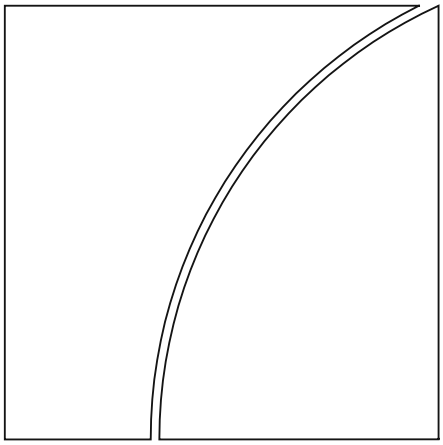
Basel Committee
on Banking Supervision



Review of the Principles for the Sound Management of Operational Risk

6 October 2014

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 92-9131-978-92-9131-554-3 (print)

ISBN 92-9197-978-92-9131-556-7 (online)

Contents

Review of the Principles for the Sound Management of Operational Risk

1. Executive summary

In June 2011 the Basel Committee on Banking Supervision published its "Principles for the Sound Management of Operational Risk"[1] ("the Principles") to provide guidance to banks on the management of operational risk. The eleven principles incorporate the lessons from the financial crisis and the evolution of sound practice for management of operational risk. The Principles cover governance, the risk management environment and the role of disclosure, and address the three lines of defence (business line management, an independent corporate operational risk management function and an independent review).

In light of the significant number of recent operational risk-related losses incurred by banks, and consistent with the Committee's greater focus on monitoring the implementation of its standards and guidance, earlier this year the Basel Committee conducted a review of the implementation of its Principles.[2] The review involved 60 systemically important banks in 20 jurisdictions and covered all 11 principles with a specific focus on the guidance related to the three lines of defence. The exercise was designed as a questionnaire by which banks self-assessed their implementation of the Principles. While it was conducted under the overall supervision of the Basel Committee and the respective supervisory authorities, the review did not involve an onsite validation of the banks' responses.

The objectives of the exercise were to (i) establish the extent to which banks have implemented the Principles, (ii) identify significant gaps in their implementation and (iii) highlight emerging and noteworthy operational risk management practices at banks that are not currently addressed by the Principles.

Key findings and observations

Overall, banks have made insufficient progress in implementing the Principles originally introduced in 2003 and revised in 2011.[3] Many banks are still in the process of implementing various principles. Systemically important banks (SIBs) have implemented the Principles and the operational risk management tools to varying degrees. Historically, implementation of the Principles was strongly aligned with the Basel Framework's approaches to calculating operational risk capital requirements such as The Standardised Approach (TSA) and the Advanced Measurement Approach (AMA). Banks applying these more advanced approaches are expected to have more advanced operational risk management

[1] Available at www.bis.org/publ/bcbs195.htm.

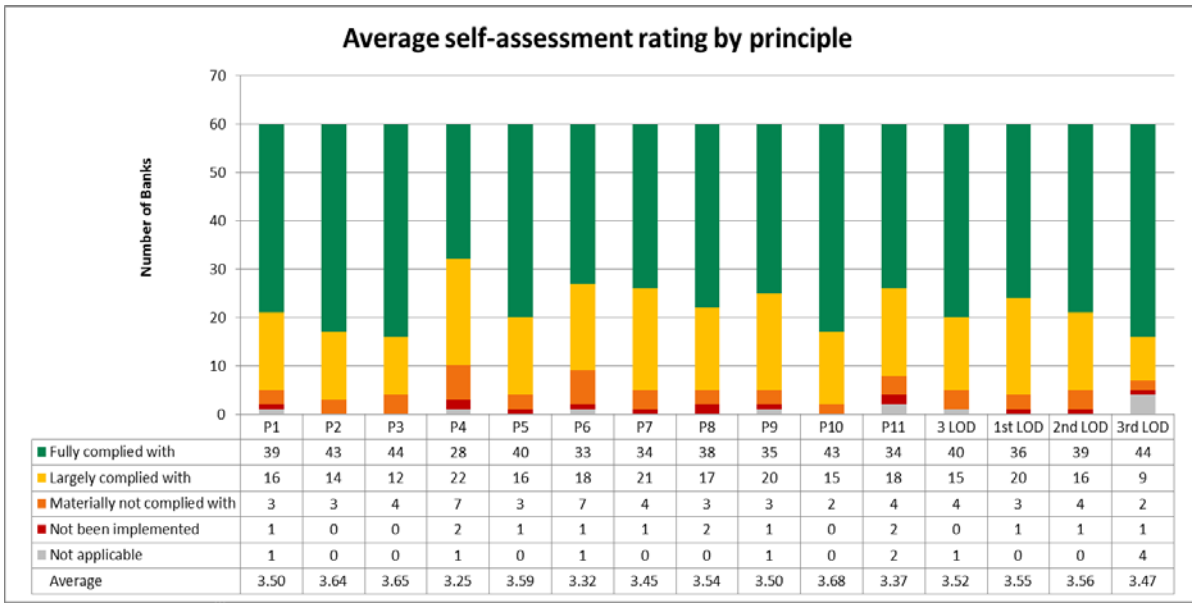
[2] In its November 2012 "Progress Report to the G20 Ministers and Governors", the Financial Stability Board (FSB) said that recent events underscored the need for supervisors to increase their focus on operational risk management, particularly for global systemically important financial institutions (see www.financialstabilityboard.org/publications/r_121031ab.pdf). In addition, the FSB recommended that the BCBS conduct a peer review on implementation of its Principles by June 2014.

[3] Throughout the report, reference is made to varying quantities of bank responses using the words 'few – typically less than10, 'some' – typically more than 10 but less than 20 and 'many' – typically more than 20.

frameworks and implement to a greater degree the operational risk management tools, which include risk and control self-assessments (RCSAs), internal loss data collection, scenario analysis, external data collection and analysis, key risk indicators (KRIs)/key performance indicators (KPIs), change management and comparative analysis.

Some SIBs, however, have yet to implement all of the Principles and do not deploy the full range of operational risk management tools. This may be because some of the banks are not subject to the most advanced approaches to operational risk and the associated higher expectations for managing the risk. Therefore, these banks may not be adequately identifying and managing their operational risk exposures. Methods for identifying and managing operational risk should be seen as complementary to the calculation of operational risk capital requirements, rather than as a consequence of that activity. Aligning the implementation of the risk management principles with the risk profile and systemic importance of banks, rather than the approaches selected to calculate operational risk capital requirements, is also be consistent with the objective of more intensive and effective supervision of systemically important banks.

The following chart summarises the average bank ratings[4,5] for each of the Principles and the three lines of defence.



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	3 LOD	1st LOD	2nd LOD	3rd LOD
Fully complied with	39	43	44	28	40	33	34	38	35	43	34	40	36	39	44
Largely complied with	16	14	12	22	16	18	21	17	20	15	18	15	20	16	9
Materially not complied with	3	3	4	7	3	7	4	3	3	2	4	4	3	4	2
Not been implemented	1	0	0	2	1	1	1	2	1	0	2	0	1	1	1
Not applicable	1	0	0	1	0	1	0	0	1	0	2	1	0	0	4
Average	3.50	3.64	3.65	3.25	3.59	3.32	3.45	3.54	3.50	3.68	3.37	3.52	3.55	3.56	3.47

This review has identified various challenges and themes within each of the principles. Four principles have been identified as among the least thoroughly implemented by banks including (i) operational risk identification and assessment, (ii) change management, (iii) operational risk appetite and tolerance, and (iv) disclosure. In addition, weaknesses have been observed in the implementation of the

[4] Rating: 1 – Not implemented; 2 – Materially not complied with; 3 – Largely complied with; 4 – Fully complied with; N/A – Not applicable.

[5] Average rating calculated using arithmetic average of ratings 1–4. Where banks rated the practice as n/a, a 0 rating was assigned.

overarching principle of the three lines of defence. The following section summarises the challenges and themes related to these principles.

Fundamental principles of operational risk management

Operational risk identification and assessment (Principle 6)

Overall, while banks have implemented some of the operational risk identification and assessment tools, others are not fully implemented or are not being effectively used for risk management purposes. Some banks indicated that the tools that had been implemented were largely used for risk measurement purposes (ie capital measurement and allocation), while others indicated that tools had not been fully implemented because they were not deemed necessary for risk measurement purposes.

In addition, a wide range of practice was reported regarding the implementation of many of these tools. For instance, while many banks have implemented distinct, multi-tiered operational risk management tools (ie RCSAs, scenario analysis, business process mapping), other banks noted that they have chosen to implement one tool that would serve the purpose of two or possibly three tools together (ie a scenario-based RCSA, a process-based RCSA etc). Furthermore, at some banks, considerable management effort will be required to ensure the bank-wide implementation of certain tools. These include key risk and performance indicators; external data collection and analysis; and comparative analysis as well as the creation and monitoring of action plans generated through the use of the operational risk management tools.

Change management (Principle 7)

Overall, there are many aspects of change management that have not been fully implemented by many of the banks. The change management principle had one of the lower average ratings assigned, indicating that banks are continuing to implement and enhance their existing change management programmes (eg new products and initiatives).

Only about two thirds of the banks have fully implemented risk and control assessments within the change management process for new products and initiatives. While the Principles define changes to include new products, activities, processes and systems, there is a wide range of practice as it relates to the policy framework for change management processes. For instance, a few banks said that their governance framework did not apply to all types of change such as outsourcing. Many banks also noted that the operational risk taxonomy is either not applied, or not consistently applied, to various changes including new products, activities, processes and systems. Alignment with the bank's taxonomy would allow for integration and aggregation of results with the overall risk profile.

Several banks noted that the roles and responsibilities relating to change management were included within either the bank's operational risk management framework or underlying change management-related policies. Many banks also noted the involvement of several control groups within the second line of defence review of risk and control assessments, such as compliance, legal, business continuity, technology, and other risk management groups. However, a number of banks continued to state that the second line of defence responsibilities were not yet fully implemented as they relate to change management.

In addition, a small number of banks noted that these other control groups were primarily responsible for performing the risk and control assessments, which is not fully aligned with the concept of the three lines of defence. Some banks also noted that the corporate operational risk function (CORF) was only involved in the process through membership in the approval and oversight committee. Participation in a committee may not fully provide for the opportunity to provide an effective challenge to the first line of defence's risk and control assessment.

In addition, many banks noted an absence of, or a partially implemented, process for monitoring of risks following the approval of the initiative, as well as an absence of a formal post-implementation review process.

Operational risk appetite and tolerance (Principle 4)

Many banks generally indicated that establishing a risk appetite and tolerance statement was more challenging for operational risk than for other risk categories, such as credit risk and market risk, and attributed this to the nature and pervasiveness of operational risk. For those banks that have established an operational risk appetite and tolerance statement, a commonly observed practice was the inclusion of a metric such as operational losses as a percentage of gross revenue. However, these metrics tended to be backward- rather than forward-looking. As a result, many banks indicated that work is under way to enhance the existing operational risk appetite and tolerance statement.

Role of disclosure (Principle 11)

Most banks said that their general quality of operational risk disclosure is fully compliant, pointing to the existence of a specific section for operational risk in the annual report or individually developed disclosure templates under the Basel Framework's Pillar 3 requirement. However, they do not disclose sensitive information relating to control gaps or issues, suggesting that these disclosures tend to be primarily high-level statements. The relative lack of information on the operational risk profile and how banks manage their operational risk may be attributable to inadequate implementation of a disclosure policy that is subject to approval and oversight by the board.

Three lines of defence

Most banks reported that they comply fully with the "three lines of defence" principle. Judging from the comments submitted, however, it is apparent that a range of practice exists relating to the implementation of the three lines of defence.

In a few cases, banks inappropriately classified responsibilities across each of the three lines of defence (eg they assigned various business line responsibilities to the second line of defence). Some banks also noted more significant challenges in the consistency of the application and their ability to substantiate the independent review of the operational risk management tools used by the first line of defence. A few banks noted insufficient resources within the CORF. In addition, a large number of banks have yet to fully develop a quality assurance programme that is applicable within the second line of defence.

Most banks indicated that responsibilities relating to the third line of defence were fulfilled. They noted that those performing review and challenge of the design and effectiveness of the bank's operational risk management controls, processes and systems are not involved in the development, implementation and operation of the operational risk management framework. Most banks also said that internal audit coverage of the framework is adequate. They added that the review of both the first and second lines of defence is sufficient and commensurate with other risk management functions where they follow a risk-based approach when determining the frequency and scope of the audit. However, almost a third of the banks noted that further enhancements were needed or planned to ensure full compliance and, as outlined in other sections of this report, some banks noted that coverage was limited to the operational risk model and its inputs, rather than the implementation of the overall operational risk management framework (ORMF).

Furthermore, most banks indicated that internal audit has sufficient resources to carry out its responsibilities as a third line of defence. However, a few banks noted that their third line of defence responsibilities needed improvement in terms of definition, execution and monitoring, and that staffing within internal audit was insufficient.

Many banks also noted that they are still in the process of implementing a more refined approach to assigning specific responsibilities to the three lines of defence.

Recommendations

Failure to fully implement appropriate operational risk identification and management practices may result in direct and material financial losses, or reputational and consequential losses, and could lead to a systemic impact on other banks, customers, counterparties and the financial system. As illustrated throughout this report, banks noted that they are at varying stages of implementation of each of the Principles. The review also highlighted several principles where, overall, banks had not adequately implemented and addressed the related risk management practices. In particular, banks should:

- improve the implementation of each of the operational risk identification and assessment tools, including risk and control self-assessments, key risk indicators, external loss data, business process mapping, comparative analysis, and the monitoring of action plans generated from various operational risk management tools;
- enhance the implementation of change management programmes and processes and ensure their effective monitoring;
- strengthen the implementation of the three-lines of defence, especially by refining the assignment of roles and responsibilities; and
- improve board and senior management oversight; articulation of operational risk appetite and tolerance statements; and risk disclosures.

2. Introduction

The *Principles for the Sound Management of Operational Risk* ("the Principles"), as updated and published in June 2011, cover (i) fundamental principles of operational risk management, (ii) governance, and (iii) the risk management environment.

In December 2012, the BCBS's Working Group on Operational Risk (WGOR) established a work stream to undertake a review of the implementation of the Principles. Conducted via a questionnaire, the review aimed to:

- identify and understand the degree to which banks have implemented the Principles;
- identify common significant gaps at banks related to the implementation of the Principles; and
- identify emerging and noteworthy practices in operational risk management that are used by banks but which are not currently addressed by the Principles.

3. Findings and observations

A questionnaire was used to solicit self-assessments from participating banks. The questionnaire contained 180 questions and was completed by 60 systemically important banks across 20 jurisdictions. The questionnaire covered all 11 Principles as well as the on the overarching guidance related to the three lines of defence. For a list of participating jurisdictions see Appendix I.

Banks were asked to self-assess and rate their operational risk management practices on a rating scale of "1" to "4" or "N/A". The four ratings were defined as follows:

1 - Principle has not been implemented

2 - Principle is materially not complied with

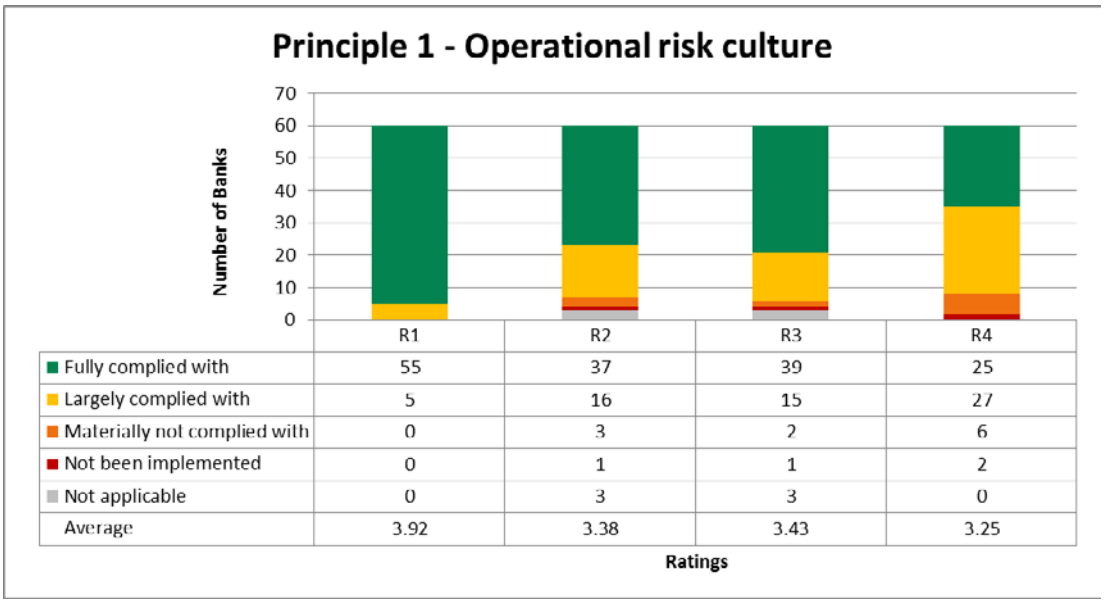
3 - Principle is largely complied with

4 - Principle is fully complied with

For further information on the guidance given to banks in completing the self-assessment ratings, see Appendix II. For a full list of Principles and criteria that were surveyed, see Appendix III.

Principle 1: Operational risk culture

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.



	R1	R2	R3	R4
Fully complied with	55	37	39	25
Largely complied with	5	16	15	27
Materially not complied with	0	3	2	6
Not been implemented	0	1	1	2
Not applicable	0	3	3	0
Average	3.92	3.38	3.43	3.25

The banks were asked to rate and describe to what extent the following elements of the Principles had been implemented:

(a) a code of conduct or ethics policy (R1);

(b) alignment of compensation policies with their risk appetite and tolerance etc (R2);

(c) compensation policies that balance risk and reward (R3); and

(d) availability of operational risk training throughout the organisation (R4).

As reflected in the chart above, overall, most banks indicated that a strong operational risk management culture had been implemented throughout their organisations and that the board of directors and senior management had established a culture that provides for appropriate incentives for professional and responsible behaviour.

Almost all banks reported that they have fully implemented a code of conduct or ethics policy that (i) sets clear expectations for integrity and ethical values of the highest standard, (ii) identifies business practices and conflicts, and (iii) is in compliance with all applicable laws, rules and regulations (R1). Noteworthy practices include ensuring that the code of conduct or ethics policy (i) applies to all the bank's staff including the board of directors, (ii) is regularly reviewed and attested to by employees, (iii) is regularly approved by the board of directors, and (iv) is publicly available on the bank's website. Other noteworthy practices include the establishment of a separate code of conduct specifically designed for certain roles (eg treasury dealers, senior management), a whistle-blower programme and a senior ethics committee.

Many banks noted that compensation policies appropriately balance risk and reward and are well aligned with the bank's long-term strategic direction, financial goals and overall safety and soundness (R3). Some banks indicated that their compensation policy is aligned with the *FSB Principles for Sound Compensation Practices*; they employ appropriate deferral mechanisms and claw-backs and balance the proportion of fixed and variable compensation tied to multiple factors, often including corporate performance, business performance and individual performance. However, few banks indicated that work is under way to better align the compensation policies with the statement of risk appetite and tolerance. Noteworthy practices include remuneration linked to risk-adjusted indicators.

Regarding the establishment of operational risk training at all levels throughout the organisation (R4), most banks indicated that some form of operational risk training has been established. For example, some banks have established online operational risk training modules focused on various

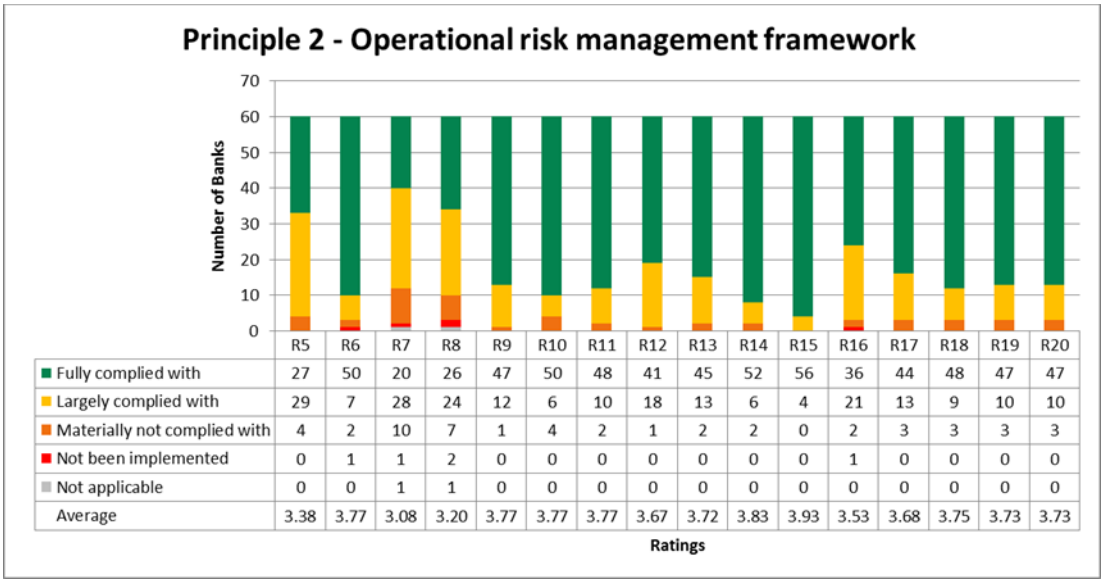
aspects of operational risk, such as "Operational risk 101" and on specific topics such as business continuity, information security or financial crime. Many banks have plans to enhance existing operational risk training, and several banks noted that plans are also in place to enhance the operational risk training and awareness for the board of directors. Noteworthy practices include the establishment of operational risk awareness for all employees, more advanced training on operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities. Other noteworthy practices include customised and mandatory operational risk training for many roles (ie business unit operations, supervisory levels, senior management and the board of directors) and strong internal monitoring of training practices in relation to requirements.

Overall, banks are encouraged to:

- continue to make progress in aligning compensation policies with the operational risk appetite and tolerance statement; and
- develop further and implement their operational risk training and awareness programmes.

Principle 2: Operational risk management framework

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.



	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19	R20
Fully complied with	27	50	20	26	47	50	48	41	45	52	56	36	44	48	47	47
Largely complied with	29	7	28	24	12	6	10	18	13	6	4	21	13	9	10	10
Materially not complied with	4	2	10	7	1	4	2	1	2	2	0	2	3	3	3	3
Not been implemented	0	1	1	2	0	0	0	0	0	0	0	1	0	0	0	0
Not applicable	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Average	3.38	3.77	3.08	3.20	3.77	3.77	3.77	3.67	3.72	3.83	3.93	3.53	3.68	3.75	3.73	3.73

The banks were asked to rate and describe their current degree of implementation for many aspects related to their operational risk management framework (ORMF), including the following:

(a) the integration of the ORMF into the overall risk management processes (R5);

(b) the application of the ORMF to all the bank's material operating groups and entities (R17);

(c) the establishment of an ORMF that includes various items such as the governance structures used to manage operational risk (R7), the use of operational risk and identification and assessment tools (R8), and the review and approval requirements of the framework itself (R6, R14, R16);

(d) the establishment of a common taxonomy of operational risk terms (R12) which should include definitions of operational risk and operational risk event types (R15); and

(e) the establishment of operational risk reporting and management information system (MIS) requirements (R11).

Regarding banks' views on the integration of their ORMFs into their overall risk management processes (R5), this requirement received one of the lowest average ratings within Principle 2. Many banks noted that reporting by the operational risk management group to the chief risk officer is consistent with other risk management groups, and that operational risk information is reported to the same officers who receive the other risk management reports. At the same time, however, many banks noted that there is further opportunity to integrate the operational risk assessment programme into the bank's strategic decision-making process. In addition, some banks noted the need to further strengthen the operational risk assessment process within the new product development and new initiative processes.

A bank's ORMF is also expected to apply to all of a bank's material operating groups and entities, including subsidiaries, joint ventures and geographic regions (R17). While overall the banks rated themselves strongly on this requirement, a few banks are still in the process of rolling out the framework to some small subsidiaries. Regarding the application of the ORMF to joint ventures, challenges were noted relating to the concept of "controlling interest". While one bank noted that the ORMF is applied to all entities with a common brand name, logo or equity investment of 30% or more, other banks apply the ORMF only where there is a greater than 50% ownership in the joint venture. Many banks noted that joint ventures are not controlled by the bank and therefore these entities are governed by a shareholder agreement that sets out its own governance programme including shareholder membership on the board, as well as agreements to share the bank's risk policies and guidelines for the joint venture to consider.

Regarding the establishment of an ORMF that identifies various aspects such as the governance structures (R7), operational risk identification and assessment tools (R8), many banks noted that these were not adequately identified within their ORMF as these items received the lowest ratings within Principle 2. In addition, while some banks were quick to update and align their ORMFs following the June 2011 release of the revised BCBS Principles, many banks were slow to respond and only recently updated their ORMFs to reflect the updated guidance.

The banks also noted that, in general, their ORMF established a common taxonomy of operational risk terms and included definitions of operational risk and operational risk event types. While some banks referenced the use of the Basel framework's operational loss event categories, other banks noted the development of a complementary operational risk taxonomy that is causal-focused, and not loss-focused. Responding banks were of the view that the frameworks had adequately established these taxonomies, though some noted that further work is needed to ensure the consistent implementation of the risk taxonomies across all business lines and operational risk tools, and these banks are focusing on the establishment of a quality assurance programme. Many banks also noted that the consistent use of an operational risk taxonomy across the bank and within the tools would allow for better aggregation of risks and issues for the purposes of updating their operational risk profiles, and for senior management and board reporting. Noteworthy practices include the creation of an operational risk dictionary that includes definitions and examples of various operational risks in the bank's taxonomy, as well as guidance related to the classification of each of the operational risks within the taxonomy, to ensure consistent identification and classification across the bank. An additional noteworthy practice was the establishment of a control library, which inventories all the controls within the bank and each of its business lines. One bank also noted that its definition of operational risk events extends beyond direct financial losses, and includes indirect losses such as forgone revenue and lost business, and overall reputational damage due to an operational risk event.

Many banks noted that their ORMFs adequately established operational risk reporting requirements (R11), and pointed to the inclusion of the nature and frequency of reporting requirements for operational risk management. In addition, many banks also noted the existence of a central operational risk system and data repository that allows for the central capture, aggregation and reporting of key operational risk data. This includes operational losses, operational risk assessments, control deficiencies and key risk indicators. However, some banks are currently self-assessing their operational risk practices against the Basel Committee's "Principles for Effective Risk Data Aggregation and Risk Reporting" guidance,[6] which was published in January 2013. Scope exists to enhance current practice as it relates to completeness and timeliness of data, as well as to enhance the current operational risk data reconciliation processes and the flexibility of operational risk reporting through improved ad hoc reporting.

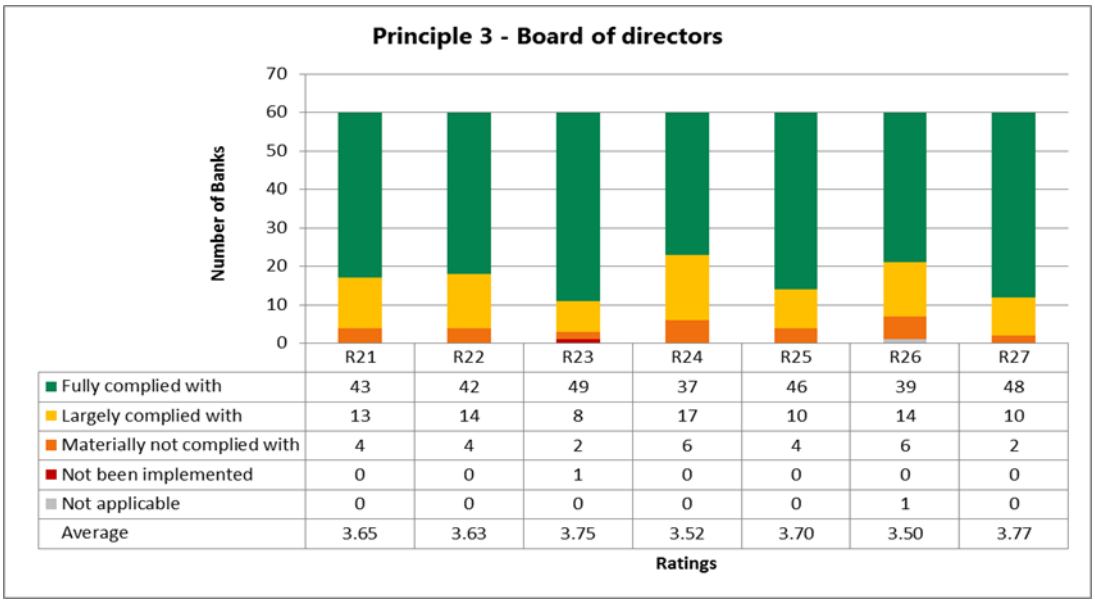
Overall, banks are encouraged to:

- further develop the integration of the operational risk management programme into the bank's strategic decision-making process;
- ensure that the ORMF or other relevant policy requires a robust operational risk assessment process within the bank's new product and new initiative approval processes;
- ensure that the ORMF specifies the use of all implemented operational risk identification and assessment tools;
- ensure that the ORMF requires the use of the bank's operational risk taxonomy in all operational risk tools to allow for the aggregation and reporting of operational risks and control issues; and
- develop a quality assurance programme to ensure that the independent challenge and review applied by the second line of defence results in consistent risk and control assessments.

Principle 3: Board of directors

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.

[6] Available at www.bis.org/publ/bcbs239.htm.



	R21	R22	R23	R24	R25	R26	R27
Fully complied with	43	42	49	37	46	39	48
Largely complied with	13	14	8	17	10	14	10
Materially not complied with	4	4	2	6	4	6	2
Not been implemented	0	0	1	0	0	0	0
Not applicable	0	0	0	0	0	1	0
Average	3.65	3.63	3.75	3.52	3.70	3.50	3.77

The banks were asked to rate and describe their current degree of implementation for a variety of board-related elements, including that the board:

(a) establishes a management culture, and supporting processes, and develops oversight of control environments (R21, R22);

(b) regularly reviews and approves the ORMF (R23, R24); and

(c) ensures the ORMF is subject to independent review and best practice (R25, R26).

As indicated in the table above, most banks said that the board was very active in establishing a strong risk management culture, and in overseeing the bank's control environments (R21, R22). Common practice includes discussion and review of operational risk management reporting at the board level, and in board subcommittees mandated with more specific risk management oversight responsibilities. Noteworthy practices include (i) the board regularly challenges senior management on the design and effectiveness of the bank's operational risk management framework, (ii) the board reviews and approves an operational risk management strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation, and (iii) the establishment of a formal communication strategy, whereby senior management underlines the importance of strong risk management practices through a variety of forums such as employee communications and training sessions.

The topic of risk culture is receiving more attention from banks and many noted that they will monitor developments and will look to implement any resulting supervisory guidance.

Regarding the regular review and approval of the ORMF (R23, R24), most banks rated practices as either compliant or largely compliant. Many banks said that the board or a subcommittee (ie the risk or audit committee) was responsible for regularly reviewing and approving the ORMF. However, a range of practice was noted as a few banks indicated that their board was not responsible for reviewing or approving risk management policies, but rather that these activities were delegated to senior management. The banks explained this variation in practice by pointing to differences in their local legal environment and in supervisory guidance or expectations. While most banks noted that such review and approval occurred at least annually or more frequently if there was a material change in risk profile, some banks noted that review and approval occurred less frequently (ie every two to three years), and one bank noted its review was performed once every five years.

As evident in the chart above, the banks also rated highly the board's role in ensuring the ORMF is subject to independent review and best practice (R25, R26). Most said that this role was

accomplished through the board's regular review of risk management reporting and internal audit reporting which included approval of the internal audit plan and review of ORMF audit reports. A common practice also noted by the banks was the participation by employees in industry working groups and conferences to remain current on leading practices. However, as it relates to the board ensuring that bank adopts best practices, only a small number said that the board had commissioned an external third party to review the design and effectiveness of the ORMF.

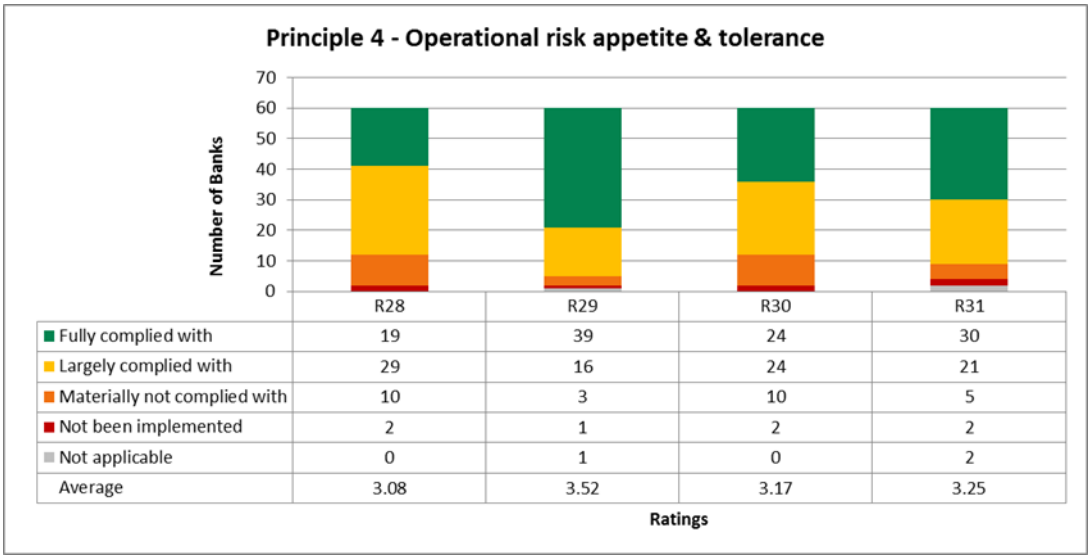
There were also a few banks that noted that internal audits of the ORMF were infrequent (ie between three and five years). In addition, a few banks said that the focus of internal audit's ORMF reviews were on the operational risk capital model, rather than a full implementation of the framework. A noteworthy practice identified was the inclusion of ORMF reviews within business unit audits, to complement the overall audit of the ORMF.

Overall, banks are encouraged to:

- ensure the scope of internal audit is on the full implementation and execution of the framework, rather than being limited to the operational risk capital model;
- ensure the scope of internal audit includes review of the effective implementation and execution of the ORMF at the business unit or legal entity levels, to complement the overall audit of the ORMF; and
- consider periodically engaging a benchmarking analysis of the bank's operational risk management framework with the assistance of independent external advisors, as part of the regular assessment of the ORMF's design and effectiveness.

Principle 4: Operational risk appetite and tolerance

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.



	R28	R29	R30	R31
Fully complied with	19	39	24	30
Largely complied with	29	16	24	21
Materially not complied with	10	3	10	5
Not been implemented	2	1	2	2
Not applicable	0	1	0	2
Average	3.08	3.52	3.17	3.25

The banks were asked to rate and describe to what extent they have implemented the following elements related to operational risk appetite and tolerance:

(a) the risk appetite and tolerance articulates the types and levels of operational risk the bank is willing to assume (R28);

(b) the board approves the risk appetite and tolerance (R29);

(c) the board reviews the appropriateness of limits, considering many factors (R30); and

(d) the board monitors management's adherence to the operational risk appetite and tolerance (R31).

As reflected in the chart above, some banks said that they have established an operational risk appetite and tolerance statement that is reviewed regularly and approved by the board of directors or a delegated authority, while others noted that this is currently under development. Many banks indicated that establishing a risk appetite and tolerance statement was more challenging for operational risk than for other risk categories such as credit risk and market risk, and attributed this to the nature and pervasiveness of operational risk. As a result, many banks indicated that work is under way to enhance the existing operational risk appetite and tolerance statement.

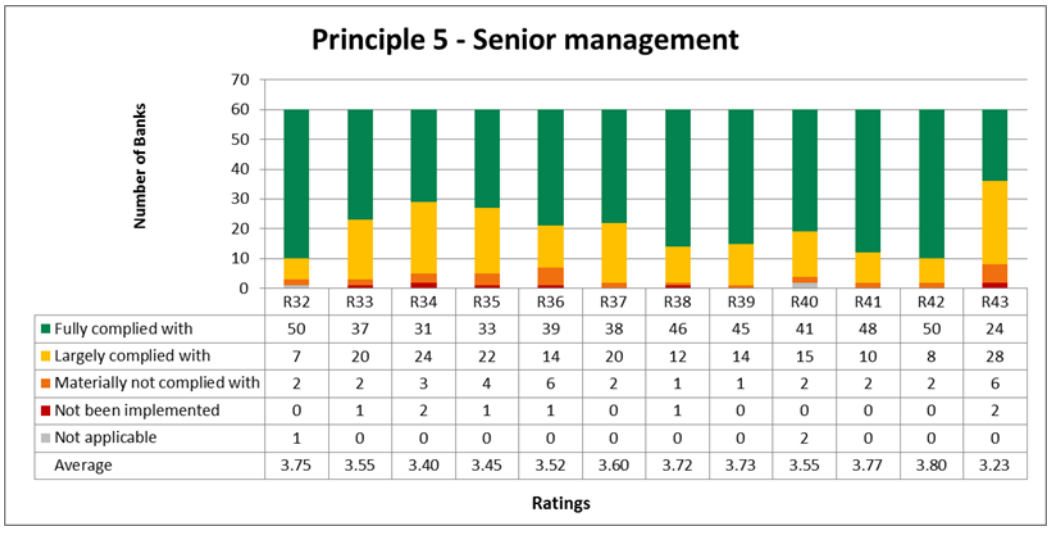
For those banks that have established an operational risk appetite and tolerance statement, a commonly observed practice was the inclusion of a metric such as operational losses as a percentage of gross revenue. However, these metrics tended to be backward- rather than forward-looking. Noteworthy practices include defining operational risk appetite and tolerance at both a divisional and a taxonomy level, utilising both quantitative and qualitative components, and setting limits based on established key risk indicators such as loss metrics, deficiencies, events and residual risk assessments from operational risk identification and assessment.

Overall, banks are encouraged to:

- continue their work to further articulate and implement enhanced and forward-looking operational risk appetite and tolerance statements.

Principle 5: Senior management

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 the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.



	R32	R33	R34	R35	R36	R37	R38	R39	R40	R41	R42	R43
Fully complied with	50	37	31	33	39	38	46	45	41	48	50	24
Largely complied with	7	20	24	22	14	20	12	14	15	10	8	28
Materially not complied with	2	2	3	4	6	2	1	1	2	2	2	6
Not been implemented	0	1	2	1	1	0	1	0	0	0	0	2
Not applicable	1	0	0	0	0	0	0	0	2	0	0	0
Average	3.75	3.55	3.40	3.45	3.52	3.60	3.72	3.73	3.55	3.77	3.80	3.23

The banks were asked to rate and describe the extent to which they have implemented the following elements of Principle 5:

(a) senior management establishes and supports an appropriate operational risk governance structure (ie governance structures, lines of responsibility, sufficient corporate operational risk function (CORF) stature and an operational risk committee) (R32, R36, R39);

(b) senior management ensures effective development and implementation of the ORMF and other operational risk policies through the recruitment of experienced and technical staff, ensuring appropriate level of resources and operational risk training, and effective communication and coordination of risk management responsibilities (R34, R35, R37, R43);

(c) senior management ensures effective implementation of challenge mechanisms, issue resolution processes and the three lines of defence roles and responsibilities (ie business line management, CORF and internal audit) (R33, R38); and

(d) senior management establishes an operational risk committee that is functioning effectively (ie receives regular inputs from country, business or functional area, meets at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making, and maintains records of committee operations that allow for review and evaluation of committee effectiveness) (R40, R41, R42).

Almost all banks reported having an independent and dedicated CORF to oversee the implementation of the bank's ORMF and also an internal audit group that assumed the responsibilities of the third line of defence. In most cases, the CORF is responsible for reporting all operational risk-related matters in the bank to the appropriate senior management/committees. The CORF is also typically staffed with tenured individuals with the appropriate seniority and experience and the title, stature and compensation of operational risk staff is commensurate with that of other risk functions.

Most banks also reported having an overall ORMF, which was supported by specific policies (ie loss data collection, risk and control self-assessment (RCSA), key risk indicators (KRI), loss modelling, scenario analysis etc), and that these policies are developed by senior management and approved by the board of directors. In some banks, the board's risk committee or operational risk committee approves these various risk-related policies.

At most banks, the ORMF and operational risk policies outline the scope, mandate, membership and hierarchy of relevant governance structures and forums, roles and responsibilities, linkages to organisational units, reporting lines, as well as escalation and resolution mechanisms. Also at most banks, the ORMF is applicable across the bank including overseas branches and regions, ensuring clear accountability and responsibility for management and mitigation of operational risk, developing a common understanding of operational risk, and helping the business and operation groups to improve internal controls. However, as noted in Principle 2, many banks said that joint ventures are not controlled by the bank and that therefore these entities are governed by a shareholder agreement which sets out its own governance programme including shareholder membership on the board, as well as agreements to share the bank's risk policies and guidelines for the joint venture to consider.

At most banks, senior management oversees operational risk in the same manner as other risks, including credit risk and market risk, in terms of identification and proposal of management policies, budget, action, and investment plans in line with the strategic goals and scope of the bank.

Regarding training (R43), as mentioned in Principle 1, most banks indicated that some form of operational risk training had been established. For example, some banks have established online operational risk training modules. However, many banks indicated that plans are in place to improve existing operational risk training, and several banks plan to improve operational risk training and awareness for the board of directors.

Most banks also noted that there is some coordination between the CORF and other risk management functions (R35). For instance, the banks typically ensured that reporting by credit, market and operational risk is aligned and consistent with the risk management committee and that there is some coordination and communication between operational risk officers and other risk colleagues across initiatives. However, some also indicated that there is room for improvement in coordination activities.

In most banks, senior management has established an operational risk committee (R39) that reports to the board's risk management committee, which is mandated to oversee the enterprise operational risk management strategy and framework. These operational risk committees direct and coordinate the implementation of the ORMF and, in most banks, membership of that committee consists of the first line of defence, the CORF and other second line of defence control functions (eg business continuity management (BCM), compliance etc). A few banks also noted that membership of the operational risk committee includes some board members or other senior and executive management for effective discussion and appropriate decision-making. Most banks also noted that the operational risk committee meetings are convened regularly (R41), minutes are prepared (R42), and action items are tracked to completion.

Regarding operational risk resources, most banks noted that the resourcing and training requirements of operational risk staff are monitored by human resources, and that succession plans have been established to ensure continuation of critical operations and maintenance of expertise.

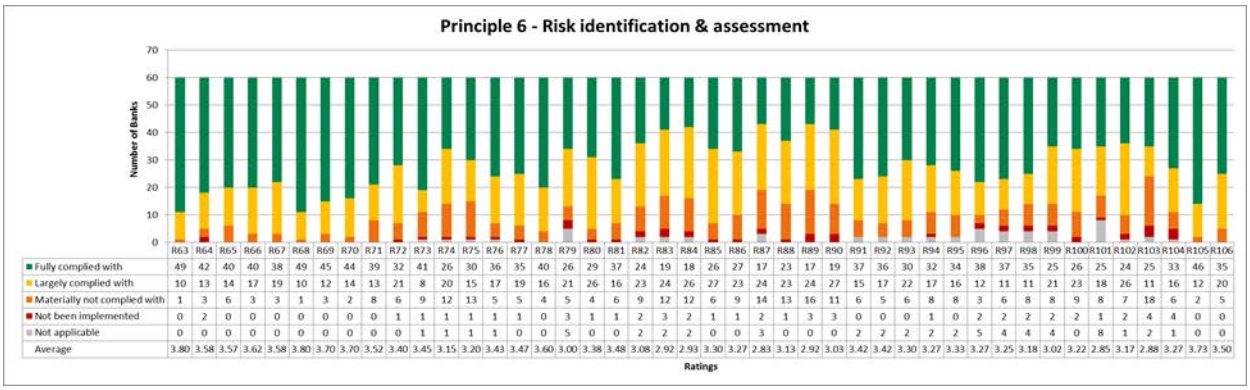
While the majority of banks rated themselves as largely or fully implemented, some banks noted that the quantity and quality of reporting on operational risk to the board could be improved, as could the board's or the risk management committee's focus on operational risk. In addition, a few banks said that they have a relatively small corporate operational risk frameworks and have not yet established an operational risk committee. Furthermore, a few banks have not yet established a formal process to gather inputs for reporting purposes from business or functional areas.

Based on the above observations, banks are encouraged to:

- ensure that the ORMF is approved by the board or a committee of the board;
- ensure that the CORF has sufficient stature, resources, and infrastructure, in relation to other risk management functions, to implement the ORMF;
- ensure that an operational risk committee is established;
- ensure that an effective independent challenge is applied by the second line of defence; and
- further develop and implement their operational risk training and awareness programmes.

Principle 6: Risk identification and assessment

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.



	R63	R64	R65	R66	R67	R68	R69	R70	R71	R72	R73	R74	R75	R76	R77	R78	R79	R80	R81	R82	R83	R84	R85	R86	R87	R88	R89	R90	R91	R92	R93	R94	R95	R96	R97	R98	R99	R100	R101	R102	R103	R104	R105	R106
Fully complied with	49	42	40	40	38	49	45	44	39	32	41	26	30	36	35	40	26	29	37	24	19	18	26	27	17	23	17	19	37	36	30	32	34	38	37	35	25	26	25	24	25	33	46	35
Largely complied with	10	13	14	17	19	10	12	14	13	21	8	20	15	17	19	16	21	26	16	23	24	26	27	23	24	23	24	27	15	17	22	17	16	12	11	11	21	23	18	26	11	16	12	20
Materially not complied with	1	3	6	3	3	1	3	2	8	6	9	12	13	5	5	4	5	4	6	9	12	12	6	9	14	13	16	11	6	5	6	8	8	3	6	8	8	9	8	7	18	6	2	5
Not been implemented	0	2	0	0	0	0	0	0	0	1	1	1	1	1	1	0	3	1	1	2	3	2	1	1	2	1	3	3	0	0	0	1	0	2	2	2	2	2	1	2	4	4	0	0
Not applicable	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	5	0	0	2	2	2	0	0	3	0	0	0	2	2	2	2	2	5	4	4	4	0	8	1	2	1	0	0
Average	3.80	3.58	3.57	3.62	3.58	3.80	3.70	3.70	3.52	3.40	3.45	3.15	3.20	3.43	3.47	3.60	3.00	3.38	3.48	3.08	2.92	2.93	3.30	3.27	2.83	3.13	2.92	3.03	3.42	3.42	3.30	3.27	3.33	3.27	3.25	3.18	3.02	3.22	2.85	3.17	2.88	3.27	3.73	3.50

The banks were asked to rate and describe the extent to which they have implemented the following operational risk identification and assessment tools:

(a) audit findings (R63–R65);

(b) internal loss data collection and analysis (R66–R72);

(c) external data collection and analysis (R73–R75);

(d) risk and control self-assessments (R76–R81);

(e) business process mapping (R82–R84);

(f) risk and performance indicators (R85–R90);

(g) scenario analysis (R91–R95);

(h) comparative analysis (R100 and 101); and

(i) other risk identification and assessment activities such as external benchmarking and creation and monitoring of action plans (R102 and R106).

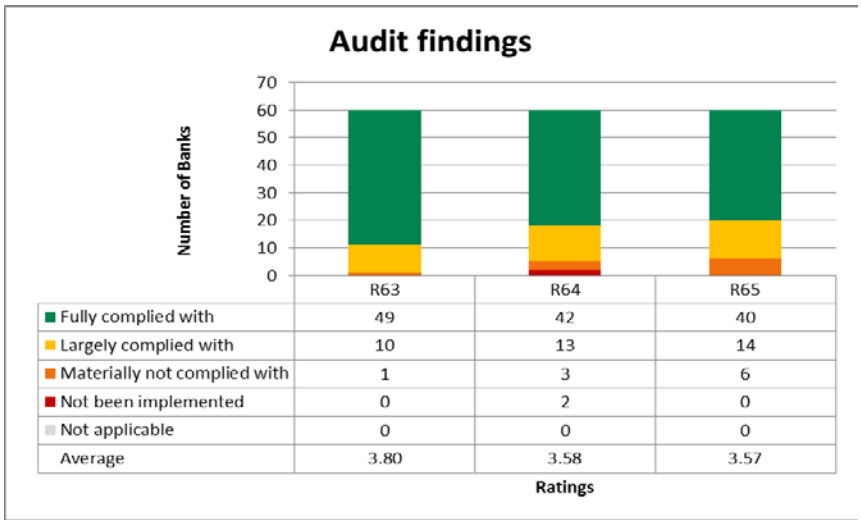
Overall, while banks have implemented many of the operational risk identification and assessment tools, many of these tools are not fully implemented or are not being effectively used for risk management. Some banks indicated that the tools that had been implemented were largely for risk measurement purposes, while others indicated that tools had not been fully implemented because they were not deemed necessary for risk measurement and capital calculation purposes.

In addition, a wide range of practice was reported regarding the implementation of many of these tools. For instance, while many banks have implemented distinct, multi-tiered operational risk management tools (ie risk and control self-assessments (RCSAs), scenario analysis, business process mapping etc), other banks have chosen to implement a single tool that can serve the purpose of two or possibly three other tools (ie a scenario-based RCSA, a process-based RCSA etc). Furthermore, some tools need considerable more focus to ensure full implementation throughout the bank including key risk and performance indicators, external data collection and analysis, comparative analysis as well as the creation and monitoring of action plans generated through the use of the operational risk management tools.

The following section summarises the observations for each of the operational risk management tools.

Audit findings

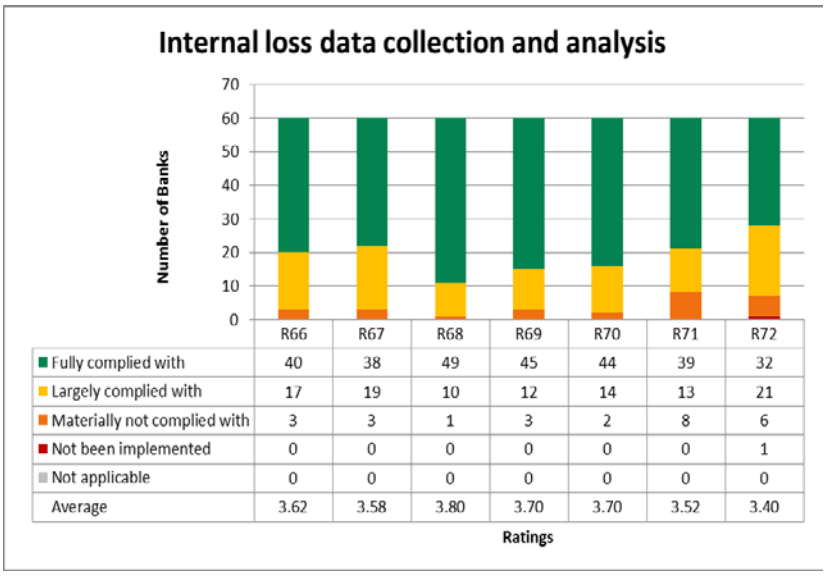
As it relates to the use of internal audit findings (R63–R65), overall, a wide range of practice was reported, and only two thirds of the banks indicated that the use of audit findings was fully implemented.



One of the noteworthy practices was the consideration of internal audit findings as an input to the various operational risk management tools, with this occurring most often in regard to the bank's risk and control self-assessment. Some banks also reported that internal audit findings are used to compare management's risk and control assessments with the various tools, and that they are also used as an input to the regular updating of the bank's operational risk profile. An additional noteworthy practice was the monitoring of the number of open and overdue internal audit issues as a key indicator. However, several banks noted that internal audit findings are not fully considered, and a few banks noted that the operational risk management function does not have direct access to internal audit findings.

Internal loss data collection and analysis

The ratings relating to the use of internal loss data collection and analysis (R66–R72) show that, while internal loss data collection and analysis processes are more fully implemented than the other operational risk management tools, approximately one third of the banks have not yet fully implemented the underlying tool. Most of the banks have a well-established process to collect internal operational loss data, with some collecting loss data above a threshold (eg $10,000 or €10,000), while some banks collect data on all operational losses, and have not established an internal threshold. These operational losses are commonly included within risk management reports and include supporting trend analysis. However, only a few banks collect and analyse information relating to all internal operational risk events, including losses, near-misses and profitable events.



	R66	R67	R68	R69	R70	R71	R72
Fully complied with	40	38	49	45	44	39	32
Largely complied with	17	19	10	12	14	13	21
Materially not complied with	3	3	1	3	2	8	6
Not been implemented	0	0	0	0	0	0	1
Not applicable	0	0	0	0	0	0	0
Average	3.62	3.58	3.80	3.70	3.70	3.52	3.40

A noteworthy practice identified by only a few banks was the establishment of an internal threshold (eg $100,000 or €100,000) whereby any operational risk event (ie losses, near-misses and profitable events) was subject to an exhaustive and standardised root cause analysis by the first line of defence, which in turn was subject to independent review and challenge by the second line of defence. These banks noted that the operational risk management function provides the business line with supporting guidance and a standardised template to ensure a consistent approach. Some banks also noted that the process involved embedding the bank's operational risk taxonomy into the template, so that this information could inform the use of the other operational risk management tools.

Additional noteworthy practices include the first line of defence leading the root cause analysis and creating action items to address any identified control deficiencies, the second line of defence closely monitoring and tracking those action items, and escalating the details of the root cause analysis and resulting action plan for items above a higher internal threshold to senior management or an operational risk committee for review. Another noteworthy practice was the establishment of a common operational risk event template and supporting guidance to ensure a consistent approach is taken by the first line of defence across the bank's divisions. In addition, some banks have developed a process to share details of operational risk events across business lines and geographies and encourage a similar approach to remediation where applicable. Also, one bank noted that it uses its 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 evaluated improperly.

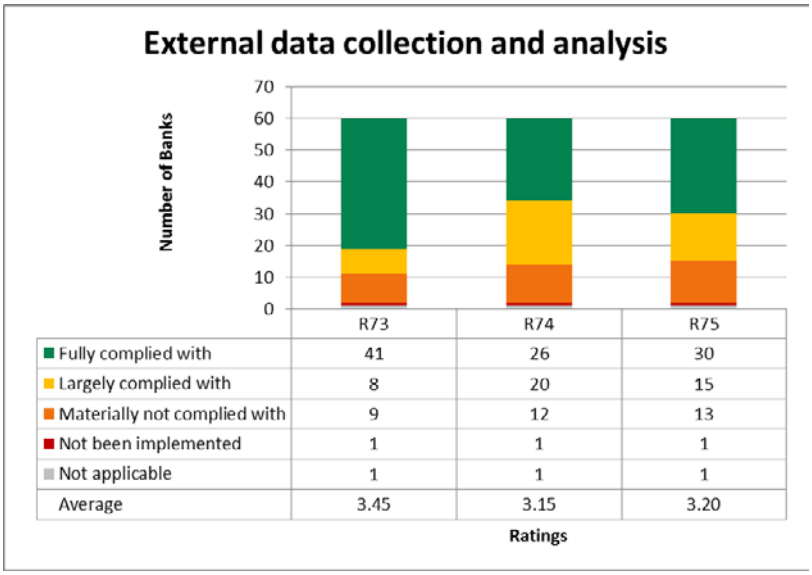
One challenge noted by some of the banks was the inability to aggregate their operational risk event data consistently in accordance with the principles referenced in the BCBS's risk data aggregation and risk reporting guidance. While many banks have implemented central repositories for operational risk event data, others are still in the process of implementing such a repository, and that the aggregation of operational loss data remains somewhat manual. In addition, some banks noted that, while the data are available by business line and region, they are not fully available by legal entity. In addition, ensuring the completeness of operational risk event data remains a challenge for many banks. While many banks have implemented a monthly reconciliation of operational losses to the bank's general ledger, a regular management attestation is commonly used that states that all business lines have reported all known events.

As it relates to the capture and analysis of operational risk boundary events (R72), some banks have established a process to collect operational loss data from market and credit risk events to gain a more holistic view of their operational risk and to support a standardised root cause analysis. At many banks, however, this has not yet been fully implemented and such banks indicated a preference for

additional guidance on the definition of an operational loss boundary event. One bank defines operational/credit boundary events as a lending loss that would not have otherwise occurred resulting from an internal failure of people, processes, and systems. It also defines operational/market boundary events as a loss that would not have otherwise occurred resulting from an operational event due to an internal failure of people, processes and systems, and which amounts to the realised difference between the initial value and the mark-to-market value at time of remediation. A noteworthy practice is the establishment of 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

The ratings relating to the use of external data collection and analysis (R73–R75) show that fewer banks have implemented the recommended practices for using *external* data, as compared with the practices pertaining to the use of *internal* loss data. In addition, while some banks use external data for risk management purposes such as benchmarking their internal losses against external standards, as well as for key inputs into their RCSAs and scenarios, many noted that the primary and sometimes the only use of the data is for risk measurement purposes. In a few cases, banks have not implemented the use of external loss data in their risk management programmes because they are not subject to AMA requirements.



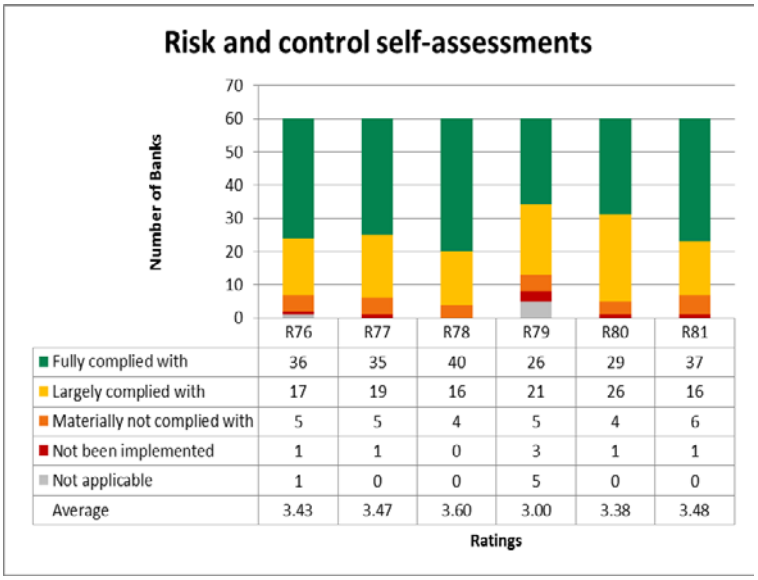
	R73	R74	R75
Fully complied with	41	26	30
Largely complied with	8	20	15
Materially not complied with	9	12	13
Not been implemented	1	1	1
Not applicable	1	1	1
Average	3.45	3.15	3.20

Many banks are members of industry consortia that provide data that are used as an input for their operational risk measurement models. The banks use these data to benchmark and assess their own internal loss data, and also as key inputs for both the scenario analysis and RCSA tools However, a few banks noted that their jurisdiction does not yet participate in such consortia.

Some banks also noted that, in the absence of consortium data or to supplement such data, they gather operational risk event data from other sources such as industry associations or media. However, many of the banks noted that this process was performed on an ad hoc basis and could become more formalised. A noteworthy practice was the distribution by the operational risk management function to business lines and operational risk officers of a monthly newsletter that lists all significant industry events. Another noteworthy practice is a monthly thematic review, whereby examples of external losses are reviewed to assess whether similar gaps exist within the bank's own business lines.

Risk and control self-assessments

While most banks have established a risk self-assessment, or a risk and control self-assessment (RCSA), many indicated that the tool has not yet been fully implemented or was currently undergoing some form of change or enhancement (R76–R81). More specifically, fewer than half the banks indicated that the RCSA was implemented on an enterprise-wide basis (R80). There also appears to be a very wide range of practice as to the design and implementation of these tools. For instance, some banks noted that the RCSA is a distinct tool that is supplemented by a distinct scenario analysis tool and a business process mapping tool, while some noted that their RCSA was process-based and that they have therefore not implemented a separate business process mapping tool. Others noted that their RCSA was scenario-based, and that they had therefore not implemented a separate scenario analysis tool.



	R76	R77	R78	R79	R80	R81
Fully complied with	36	35	40	26	29	37
Largely complied with	17	19	16	21	26	16
Materially not complied with	5	5	4	5	4	6
Not been implemented	1	1	0	3	1	1
Not applicable	1	0	0	5	0	0
Average	3.43	3.47	3.60	3.00	3.38	3.48

The following observations are further evidence of the wide range of practice on the design and implementation of the RCSA:

- some banks noted that the approach of their RCSA was top-down, others noted theirs was bottom-up, while others noted a multi-tiered approach (ie at the bank-wide, divisional and business line levels);
- some banks noted that the scope of the RCSA applies to current and existing functions and activities, while others indicated it applies only when there are changes made within the business unit;
- some incorporate the concepts of inherent risk, control assessment, and residual risk, while some indicated they do not incorporate all three concepts; and
- many noted that the RCSA is applied only to business units, and not control functions such as risk management, compliance and internal audit, while some noted that the RCSA applies to all groups except internal audit, and others noted that it is applied enterprise-wide to all groups including internal audit.

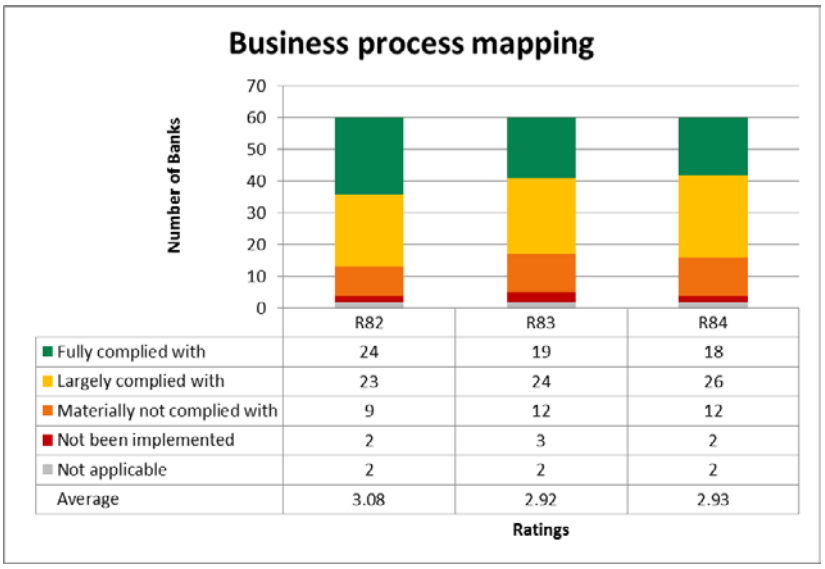
In addition, while the majority of banks indicated that all RCSAs are formally reviewed at least annually or more frequently if prompted by significant events (eg a significant operational risk event, implementation of change initiative, unsatisfactory internal audit); some banks noted the RCSAs are reviewed less frequently. Only a small number of banks noted that their review of RCSAs follow a risk-

based methodology, meaning that higher-risk businesses are reviewed more frequently than lower-risk businesses.

Noteworthy practices include the review and challenge of the RCSAs by the second line of defence, the aggregation of bank-wide themes and issues identified through the RCSAs, the embedding of the bank's operational risk taxonomy within the RCSA to ensure alignment with other tools and to allow for aggregation of a risk profile, and the completion of RCSAs not only by business unit but also for key shared business functions or processes. One bank's methodology also involved the categorisation of residual risk into one of four categories: treat, tolerate, terminate or transfer.

Business process mapping

Overall, the use of business process mapping is one of the less implemented operational risk management tools (R82–R84). In their responses, many banks noted that, outside their financial reporting processes, they do not use business process maps as an operational risk management tool. Some raised concerns that full implementation of this tool may require extensive effort and resources and were somewhat sceptical whether this tool would provide more value than the other operational risk management tools already implemented. However, other banks noted that they had partially implemented this tool, although most had yet to implement it systemically across the bank.



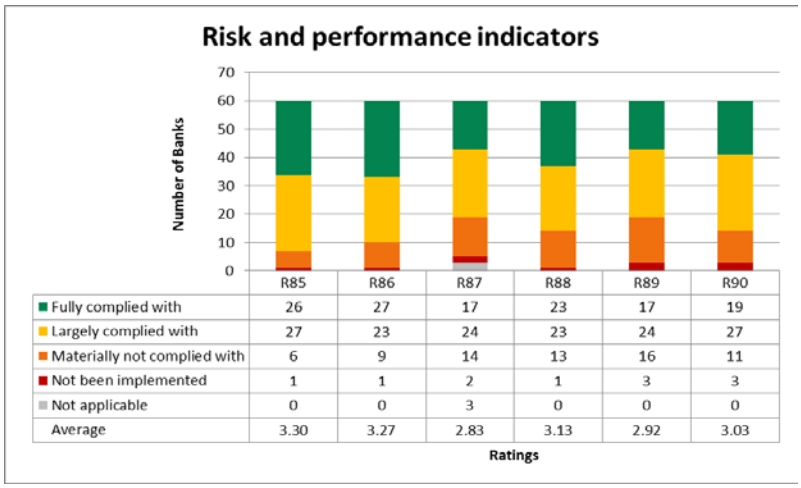
	R82	R83	R84
Fully complied with	24	19	18
Largely complied with	23	24	26
Materially not complied with	9	12	12
Not been implemented	2	3	2
Not applicable	2	2	2
Average	3.08	2.92	2.93

Noteworthy practices include the implementation of a business process architecture framework that provides guidelines for the creation of business process maps, the mapping and assessment of significant and high-risk processes rather than all business processes within the bank, the establishment of a central repository for all business process maps, and the incorporation of the bank's operational risk taxonomy into the business process with a view to mapping methodology for aggregation and comparisons against the operational risk profile. In addition, a few banks noted that the creation of relevant business process maps was the responsibility of the first line of defence, and that the second line of defence would review and apply an effective challenge to these assessments.

Risk and performance indicators

Overall, the ratings for the implementation of key risk and performance indicators were the lowest of all operational risk management tools (R85–R90). Most banks noted that the development of key indicators was still under way across the bank, and more than half indicated that these indicators were not yet fully implemented across all business lines (R88). In addition, a few banks have not yet implemented key risk

and performance indicators in their risk management programme because they are not subject to AMA requirements, indicating that they have not considered using the tool for risk management purposes.



	R85	R86	R87	R88	R89	R90
Fully complied with	26	27	17	23	17	19
Largely complied with	27	23	24	23	24	27
Materially not complied with	6	9	14	13	16	11
Not been implemented	1	1	2	1	3	3
Not applicable	0	0	3	0	0	0
Average	3.30	3.27	2.83	3.13	2.92	3.03

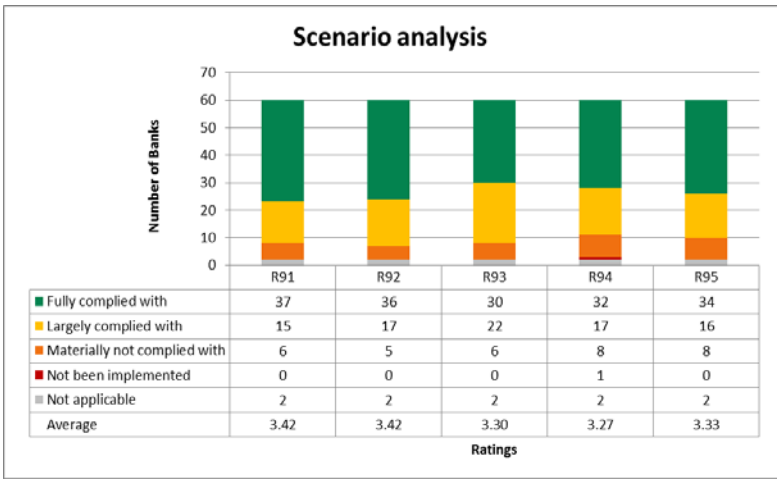
Generally, there appears to be broad range of interpretation for both key risk and key performance indicators. While some banks consider key risk indicators and key performance indicators to be the same set of metrics, some banks clearly recognise that key risk indicators are metrics designed to measure inherent risk, while key performance metrics are designed to measure the adequacy of underlying processes and controls. In addition, many of the banks noted challenges with the aggregation of common indicators as implemented in their various divisions and business lines.

Many banks that have implemented, or are upgrading this tool, said that they seek to ensure that the metrics for key operational risks (R86–R87), are regularly monitored (ie monthly or quarterly), and are measured against pre-established triggers or thresholds (R89) that often indicate the status of the risk (ie green, yellow or red). A significant number of banks also noted that further enhancements were needed to establish a more regular review process for the selected indicators and their thresholds (R90).

Noteworthy practices include the establishment of key risk and performance indicators at multiple levels throughout the bank, including at the group-wide level, the divisional level, and at the individual business line level. Again, most banks explained that implementation was incomplete because key risk and performance indicators for business units were still under development. Additional noteworthy practices included the first line of defence creating action plans for metrics that breached the respective thresholds, and close monitoring and challenge of indicators, thresholds, and action plans by the second line of defence.

Scenario analysis

Overall, many banks actively use scenario analysis as a key operational risk tool (R91–R95). However, some banks use scenario analysis on an ad hoc basis, while others use it only for risk measurement and not for risk management. Some banks also noted that the second line of defence leads and develops the scenario process, while others noted that the first line of defence and relevant topical experts, lead the scenario analysis, with guidance and challenge provided by the second line of defence.



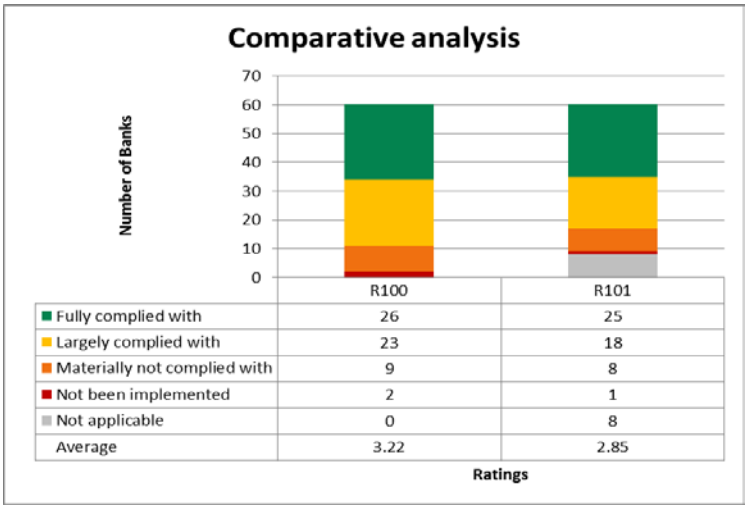
Noteworthy practices indicated included implementation at the bank-wide, divisional and business unit levels, the use of scenarios to assess existing controls, the opportunity to identify the additional controls required to mitigate the associated risks, and the development and monitoring of appropriate action plans. However, overall, few banks develop action plans from their scenario analyses (R93).

Other noteworthy practices include the use of scenarios to supplement the RCSA and other operational risk management tools by focusing on low-probability but high-impact events that the other tools may have missed. In addition, some banks said they use scenarios to compare the control environment, and help assess the completeness and adequacy of assessments in other tools (ie RCSA). A developing practice is the use of operational risk scenarios for enterprise-wide risk assessment purposes. For example, some banks have developed scenarios related to earthquakes and other catastrophic events such as a cyber-attack to assess not only the operational risk exposures (ie business continuity costs, fraud losses, lawsuits etc) but also other risks such as credit risk (ie increased defaults, devaluations of collateral), market risk and general economic conditions (ie lower revenues).

One bank noted that the operational risk function annually reviews the universe of scenarios, and creates a plan to develop, update, retire, reclassify or maintain the scenarios over the course of the year. In addition, some banks have established a scenario governance committee to oversee the overall scenario programme.

Comparative analysis

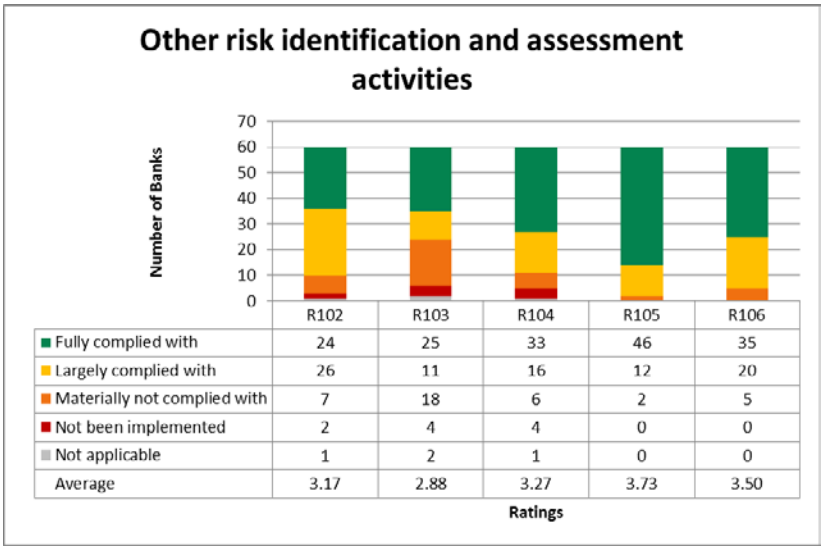
While comparative analysis is identified in the Principles as an operational risk identification and assessment tool, the chart shows that it is not widely implemented (R100). Comments from the banks suggest that this may be because (i) the definition and guidance provided in the Principles is limited, and (ii) a bank needs to have most of its tools fully implemented to support a comprehensive comparative analysis programme, and as noted above, most banks are still in the process of implementing most of the tools. But many banks indicated that they plan to enhance the quality and quantity of their comparative analysis.



Noteworthy practices include using the assessments and outputs of each of the tools to assess the effectiveness of other tools, comparison of tool assessments and outputs across similar business lines and geographies (ie RCSAs, operational risk events, scenarios etc), and the establishment of a formal process to conduct this comparative analysis by both the first and second lines of defence.

Other risk identification and assessment activities

Formal benchmarking of practices is not fully implemented at most banks (R102). While banks generally noted their participation in industry forums and conferences, many said that specific practices are not generally disclosed, and only a few indicated that they conducted formal reviews by engaging a third party or by some other means.



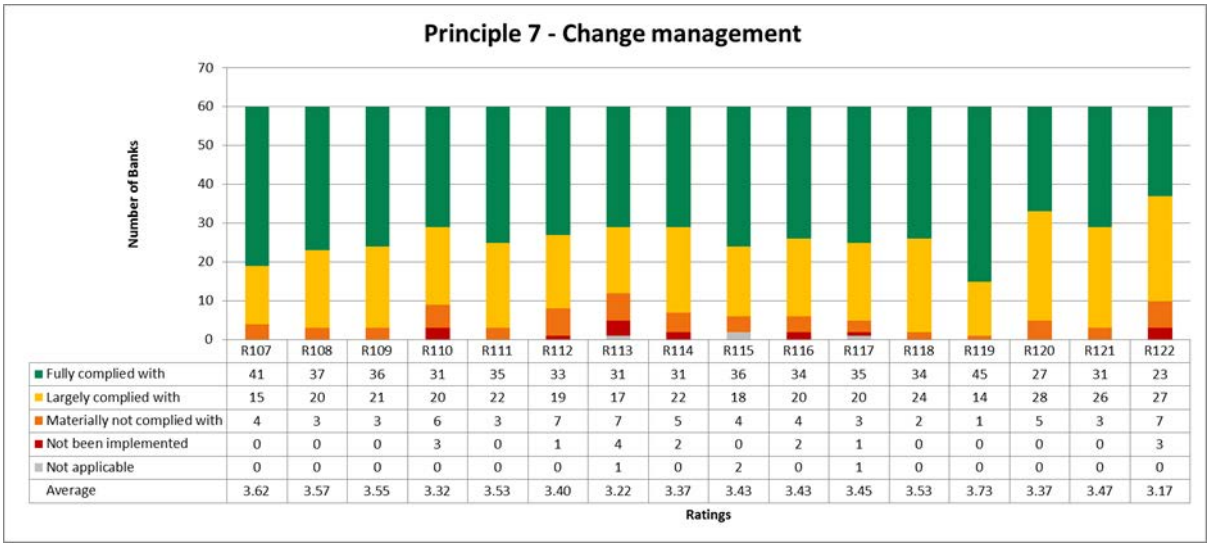
In addition, the Principles are focused primarily on the use of operational risk identification and assessment tools for risk management rather than risk measurement exposure. While many banks indicated that they have implemented a number of tools, or are in the process of implementing them, many noted that the creation, monitoring and remediation of action plans are not fully implemented (R106).

Overall, banks are encouraged to:

- increase their use of external data for the purposes of risk management;
- participate in industry consortia, to enhance the availability of external loss data for all jurisdictions;
- further implement the use of business process mapping as an operational risk management tool;
- further implement the use of key risk and performance indicators;
- further develop and implement comparative analysis processes that compare outputs from each tool to assess the effectiveness of other tools within business lines, as well as that of tool assessments and outputs across similar business lines and geographies;
- use operational risk scenarios for enterprise-wide risk assessment purposes;
- ensure that action plans from the operational risk identification and assessment tools are monitored;
- ensure that there is a formal process to create, monitor and remediate action plans derived from all tools; and
- consider more formal processes for benchmarking of operational risk management practices externally.

Principle 7: Change management

Senior management should ensure that there is an approval process that fully assesses operational risk for all new products, activities, processes and systems.



	R107	R108	R109	R110	R111	R112	R113	R114	R115	R116	R117	R118	R119	R120	R121	R122
Fully complied with	41	37	36	31	35	33	31	31	36	34	35	34	45	27	31	23
Largely complied with	15	20	21	20	22	19	17	22	18	20	20	24	14	28	26	27
Materially not complied with	4	3	3	6	3	7	7	5	4	4	3	2	1	5	3	7
Not been implemented	0	0	0	3	0	1	4	2	0	2	1	0	0	0	0	3
Not applicable	0	0	0	0	0	0	1	0	2	0	1	0	0	0	0	0
Average	3.62	3.57	3.55	3.32	3.53	3.40	3.22	3.37	3.43	3.43	3.45	3.53	3.73	3.37	3.47	3.17

Banks were asked to rate and describe the extent to which they have implemented the following aspects of change management:

(a) change management risk and control assessment, and approval process (R108–R115, and R117);

(b) roles and responsibilities (R116); and

(c) post-approval monitoring and post-implementation reviews (R120–R122).

Overall, many aspects of change management have not yet been fully implemented. The change management principle was assigned one of the lower average ratings, indicating that banks are continuing to implement and enhance their existing change management programmes.

New product and initiative assessment and approval process

Risk and control assessments within the change management process for new products and initiatives are in a fully implemented stage in only about two thirds of the banks (R109–R114). While the Principles reference changes to include new products, activities, processes and systems, there is a wide range of practice as it relates to the policy framework for such change management processes. For instance, a few banks said that their governance framework did not apply to all types of changes such as outsourcing. This may be due the absence in the guidance of a holistic definition of what constitutes a "change".

In addition, some banks have a bank-wide policy for their approach to change management, which is supported by underlying new product and new initiative policies within the various divisions. At other banks, the policies and processes for change management are more decentralised, so that these programmes consist of various underlying policies and processes that may not be completely aligned, updated and consistently applied, resulting in an ad hoc approach. Several banks are currently in the process of centralising the responsibility for overseeing the process and its implementation in the various divisions and business lines.

At many banks, the operational risk taxonomy is either not applied, or not consistently applied to various changes including new products, activities, processes and systems (R117). Alignment with the bank's taxonomy would allow for integration and aggregation of results with the overall risk profile.

Noteworthy practices included a formal project governance programme that involves several approval or points or "gates" throughout the life of the project, the identification of controls or actions required either pre- or post-implementation that are monitored by the second line of defence to ensure remediation, and properly coordinated oversight committees responsible for monitoring the implementation of the framework and for providing various approvals for new products and initiatives.

An additional noteworthy practice was a risk-based approach to the application of requirements for risk and control assessments, as well as approvals. More specifically, the extent of governance oversight required would be dictated by established criteria such as risk ratings, change to risk profile, cost, cross-organisational impact, reputational risk, compliance with regulatory requirements etc. Generally the products with the potential for higher risk and impact would be subject to higher degrees of assessment and oversight.

Specific to product risk governance, a noteworthy practice identified included a product risk framework that sets forth requirements at the various stages throughout the product life cycle (eg development, change, grandfathering and closure), and the maintenance of a central list of all the bank's products.

Roles and responsibilities

Several banks noted that the roles and responsibilities relating to change management were included within either the bank's ORMF or underlying change management-related policies. Many banks also noted the involvement of several control groups within the second line of defence's review of risk and control assessments, such as finance, compliance, legal, business continuity, technology, and other risk management groups (eg fraud management groups). However, a number of banks said that the second line of defence responsibilities were not yet fully implemented (R116), or were inadequately structured and coordinated.

In addition, a small number of banks noted that these other control groups were primarily responsible for performing the risk and control assessments, which is not fully aligned with the concept of the three lines of defence. Some banks also noted that the CORF was involved in the process only

through membership in the approval and oversight committee. However, participation in a committee may not fully provide for the opportunity to provide effective challenge to the risk and control assessment completed by the first line of defence.

Post-approval monitoring and post-implementation reviews

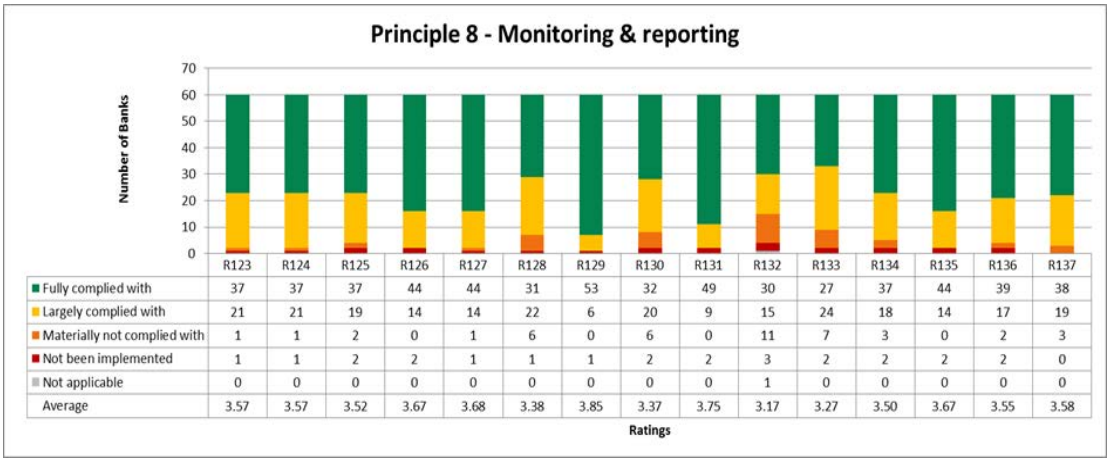
Many banks noted an absence of, or a partially implemented, process for monitoring of risks following the approval of the initiative (R121), as well as an absence of a formal post-implementation review process (R122). However, some banks did note that operational risk officers were responsible for monitoring and escalating any unforeseen issues or risks that arise post-approval. In addition, many banks that had implemented a formal post-implementation review said that the process allowed them to assess the realisation of anticipated benefits such as cost reduction, revenue generation and risk reduction prior to the formal closure of the project.

Overall, banks are encouraged to:

- further improve their change management programmes so that they are comprehensive and fully implemented;
- ensure that the roles and responsibilities for change management processes are fully implemented and aligned with the principle of the three lines of defence; and
- ensure that post-approval monitoring and post-implementation reviews are full implemented.

Principle 8: Monitoring and reporting

Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms that support proactive management of operational risk should be in place at the board, senior management, and business line levels.



	R123	R124	R125	R126	R127	R128	R129	R130	R131	R132	R133	R134	R135	R136	R137
Fully complied with	37	37	37	44	44	31	53	32	49	30	27	37	44	39	38
Largely complied with	21	21	19	14	14	22	6	20	9	15	24	18	14	17	19
Materially not complied with	1	1	2	0	1	6	0	6	0	11	7	3	0	2	3
Not been implemented	1	1	2	2	1	1	1	2	2	3	2	2	2	2	0
Not applicable	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Average	3.57	3.57	3.52	3.67	3.68	3.38	3.85	3.37	3.75	3.17	3.27	3.50	3.67	3.55	3.58

The banks were asked to rate and describe the extent to which they have implemented the following elements related to monitoring and reporting:

(a) quality of the reporting (ie comprehensiveness, accuracy, consistency and appropriateness of volume) (R123 and 124);

(b) timing and frequency of reporting (R125–129);

(c) specific items to be included in reporting (R130–136); and

(d) periodic review of sufficiency of data capture and data reporting processes (R137).

Overall, many of the banks responded that they were in full compliance with this principle, reflecting practices such as the establishment of enterprise guidance for risk reporting, regular reviews of adherence to these guidelines, and the establishment of a bank-wide data warehouse for operational risk data. However, some of the banks noted they are planning to improve the existing operational risk reporting to ensure the information is useful, concise and actionable.

Regarding the timing and frequency of reporting (R125–R129), most of the banks consider themselves as fully or largely compliant. Many banks produce quarterly operational risk reports, but a few banks produce them on a monthly basis. Some banks also noted that their reporting includes an appropriate balance of information related to both the changes of business environment and operational risk data (loss data, KRIs).

Many banks noted challenges with both the timeliness of reporting (R125) and the inclusion of suggested information relevant to decision-making (R128). Specific challenges included:

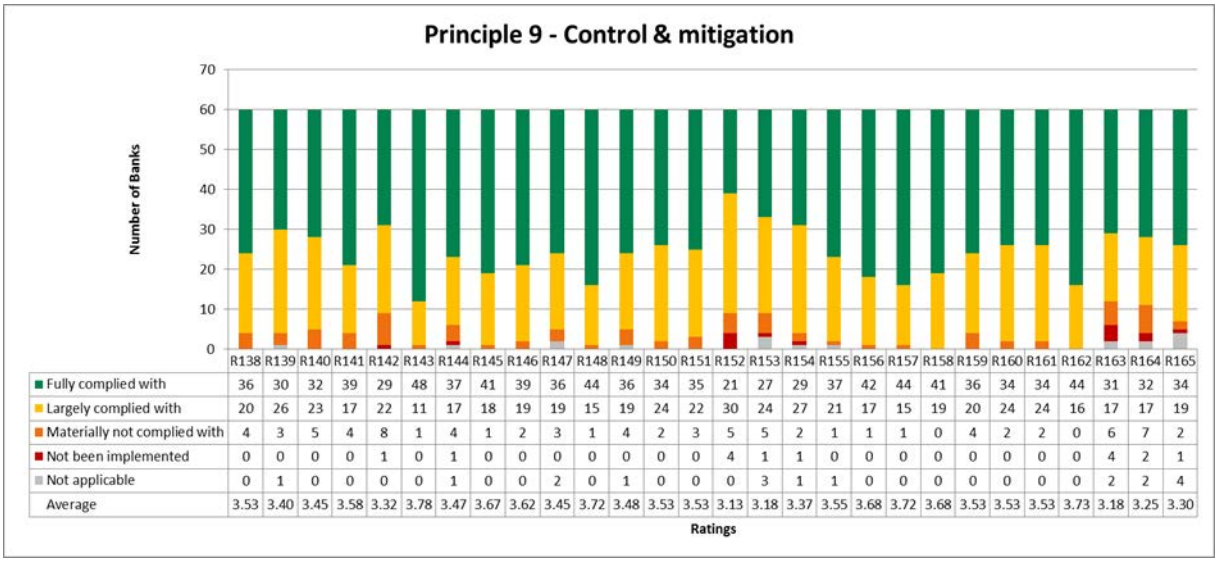
- the timeliness and effectiveness of data gathering and aggregation in a stressed condition need to be developed or tested;
- flexible processes to extract data on demand need to be further developed; and
- the quality and timeliness of information related to external events or environments need to be improved.

Regarding the specific items to be included (R130–R136), many banks noted that they were not fully compliant. However, this does not necessarily indicate that many banks have a deficiency in reporting, but rather that they need to further develop the underlying resources (ie operational risk appetite and tolerance definitions, external loss data etc).

Noteworthy practices include quarterly reporting relative to the established operational risk appetite and tolerance, and the use of an operational risk profile, or other items such as risk maps, trends and a listing of top operational risks.

Principle 9: Control and mitigation

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



	R138	R139	R140	R141	R142	R143	R144	R145	R146	R147	R148	R149	R150	R151	R152	R153	R154	R155	R156	R157	R158	R159	R160	R161	R162	R163	R164	R165
Fully complied with	36	30	32	39	29	48	37	41	39	36	44	36	34	35	21	27	29	37	42	44	41	36	34	34	44	31	32	34
Largely complied with	20	26	23	17	22	11	17	18	19	19	15	19	24	22	30	24	27	21	17	15	19	20	24	24	16	17	17	19
Materially not complied with	4	3	5	4	8	1	4	1	2	3	1	4	2	3	5	5	2	1	1	1	0	4	2	2	0	6	7	2
Not been implemented	0	0	0	0	1	0	1	0	0	0	0	0	0	0	4	1	1	0	0	0	0	0	0	0	0	4	2	1
Not applicable	0	1	0	0	0	0	1	0	0	2	0	1	0	0	0	3	1	1	0	0	0	0	0	0	0	2	2	4
Average	3.53	3.40	3.45	3.58	3.32	3.78	3.47	3.67	3.62	3.45	3.72	3.48	3.53	3.53	3.13	3.18	3.37	3.55	3.68	3.72	3.68	3.53	3.53	3.53	3.73	3.18	3.25	3.30

The banks were asked to rate and describe the extent to which they have implemented the following:

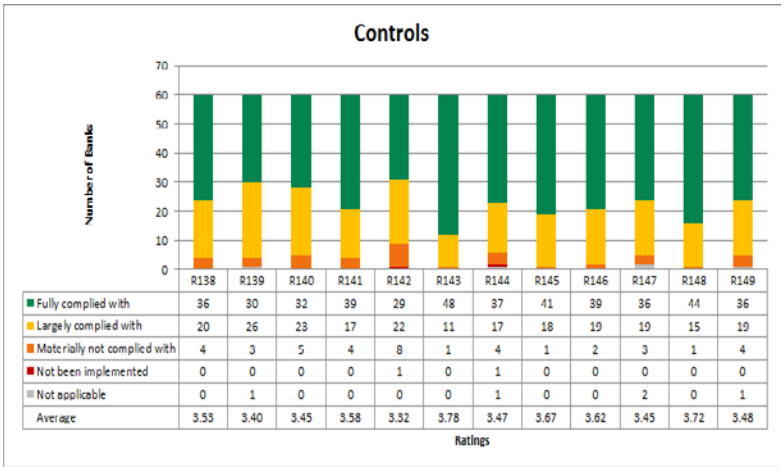
(a) control processes and procedures that include a system for ensuring compliance with policies (R138–R142);

(b) traditional internal controls that address operational risk (R143–R149);

(c) risk management policies and activities to identify, measure, and manage technology risks (R150–R155);

(d) risk management policies and activities that encompass outsourcing (R156–R162); and

(e) consideration for the use of risk mitigation including insurance (R163–165).

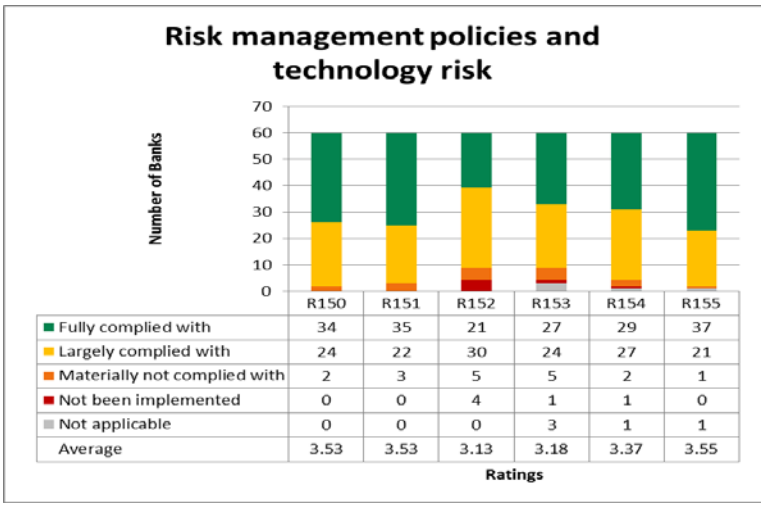


	R138	R139	R140	R141	R142	R143	R144	R145	R146	R147	R148	R149
Fully complied with	36	30	32	39	29	48	37	41	39	36	44	36
Largely complied with	20	26	23	17	22	11	17	18	19	19	15	19
Materially not complied with	4	3	5	4	8	1	4	1	2	3	1	4
Not been implemented	0	0	0	0	1	0	1	0	0	0	0	0
Not applicable	0	1	0	0	0	0	1	0	0	2	0	1
Average	3.53	3.40	3.45	3.58	3.32	3.78	3.47	3.67	3.62	3.45	3.72	3.48

Regarding control processes and procedures including a system for ensuring compliance with policies, only half the banks said that they had fully implemented a formal process to verify management controls (R139) and a process to track exceptions to approved thresholds and limits, management overrides or other deviations from policies. The banks that indicated they had a sufficient process noted various practices including:

- regular verification of compliance by the second line of defence and/or the third line of defence;
- the existence of a specific monitoring unit to track exceptions; and
- a regular process to review, monitor and follow up processes and procedures.

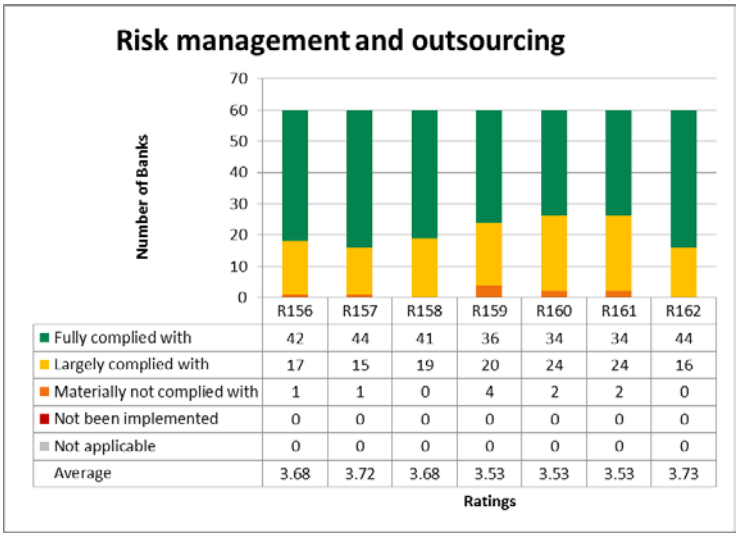
Regarding the implementation of traditional controls that address operational risk (R143– R149), most banks noted that these controls were generally well established. Many banks noted that the basic controls such as approval authorities, monitoring of adherence to limits, and vacation policies had been previously implemented due to other financial and regulatory requirements. However, there appears to be a slight discrepancy between these ratings and the lower ratings assigned to the establishment of processes that ensure compliance with policies (R138–R142).



	R150	R151	R152	R153	R154	R155
Fully complied with	34	35	21	27	29	37
Largely complied with	24	22	30	24	27	21
Materially not complied with	2	3	5	5	2	1
Not been implemented	0	0	4	1	1	0
Not applicable	0	0	0	3	1	1
Average	3.53	3.53	3.13	3.18	3.37	3.55

Some banks noted challenges with the close monitoring of adherence to assigned risk thresholds or limits (R144) as well as with ongoing processes to identify business lines and products where returns are out of line with reasonable expectations (R147). For instance, banks noted that the establishment of thresholds or limits are based on the severity of a single loss event, the accumulated loss amount of a certain period or a KRI figure, but they are still considering enhancements to the monitoring of such limits. Noteworthy practices included the use of metrics for comparison of returns (by business unit or 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.

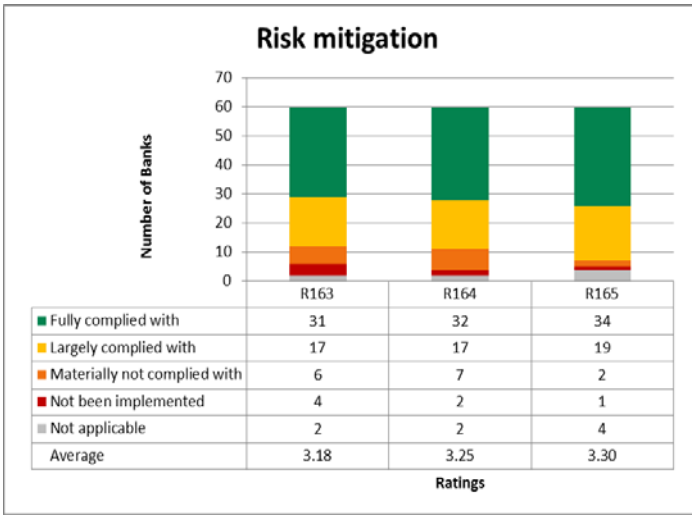
Generally banks noted some implementation and conceptual challenges pertaining to information technology risks (R150–R153), such as the establishment of a risk appetite and tolerance statement applicable to IT risk, as well as the establishment and monitoring of specific IT limits. However, a large number of banks designed their IT policies so as to adopt local and international standards for IT controls (eg COBIT, ITIL and ISO 20000/27000s).



	R156	R157	R158	R159	R160	R161	R162
Fully complied with	42	44	41	36	34	34	44
Largely complied with	17	15	19	20	24	24	16
Materially not complied with	1	1	0	4	2	2	0
Not been implemented	0	0	0	0	0	0	0
Not applicable	0	0	0	0	0	0	0
Average	3.68	3.72	3.68	3.53	3.53	3.53	3.73

Regarding the management of outsourcing risk (R156–R162), most banks are largely compliant and have in place a formalised policy that governs outsourcing risk management requirements. However, a gap noted in a few responses included limiting the outsourcing risk management activities to internal or related-party providers. Noteworthy practices include clear assignment of both first and second line

of defence responsibilities for the assessment and control of outsourcing risk, the use of operational risk management tools (ie RCSAs, KRIs etc) to help manage outsourcing risks and develop contingency plans and backup arrangements.



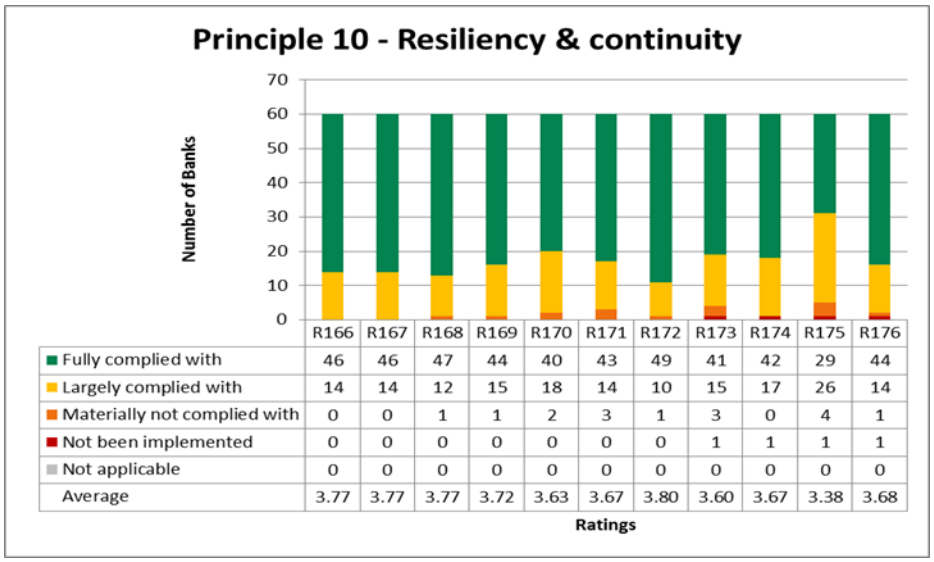
While slightly more than half the banks said that the board performs an annual review of the bank's risk and insurance management programme, many noted that the board does not perform such a review and is not engaged in such oversight. In a very small number of cases, banks also noted that senior management does not perform an annual review of the bank's risk and insurance management programme.

Overall, banks are encouraged to:

- broaden the scope of outsourcing oversight beyond internal or related-party providers;
- further develop the consideration of IT risk within the operational risk appetite and tolerance statement; and
- ensure that the bank's risk and insurance management programme is subject to regular board and senior management oversight.

Principle 10: Business resilience and continuity

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.



	R166	R167	R168	R169	R170	R171	R172	R173	R174	R175	R176
Fully complied with	46	46	47	44	40	43	49	41	42	29	44
Largely complied with	14	14	12	15	18	14	10	15	17	26	14
Materially not complied with	0	0	1	1	2	3	1	3	0	4	1
Not been implemented	0	0	0	0	0	0	0	1	1	1	1
Not applicable	0	0	0	0	0	0	0	0	0	0	0
Average	3.77	3.77	3.77	3.72	3.63	3.67	3.80	3.60	3.67	3.38	3.68

The banks were asked to rate and describe the current level of implementation of the following:

(a) business continuity plans commensurate with the bank's nature, size and complexity (R166);

(b) business continuity plans that cover all business and groups of the bank (R167);

(c) consideration of disruptive scenarios, contingency strategies, and tests to ensure that recovery objectives are met (R168–R172, R174); and

(d) regular business continuity training and awareness programmes (R173).

Most banks have said that they have established a business continuity programme that is commensurate with their nature, size and complexity (R166). A noteworthy practice includes a business continuity framework or policy that establishes the requirements for the bank's overall business continuity programme. Most banks also said that business continuity plans have been developed for all their businesses and groups (R167). However, some banks noted that this has not yet been achieved due to inconsistent application across certain business lines, units or subsidiaries (eg foreign entities or non-banking entities).

Many banks also consider disruptive scenarios, establish contingency strategies, and conduct tests to ensure that recovery objectives are met. However, a small number of banks do not participate in testing with key service providers (R175). Noteworthy practices include a well established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, the establishment of thresholds for activation of business continuity plans (eg maximum tolerable outage etc), as well as the integration of such disruptive scenario analysis into other risk management tools and processes (eg KRIs, Pillar II etc).

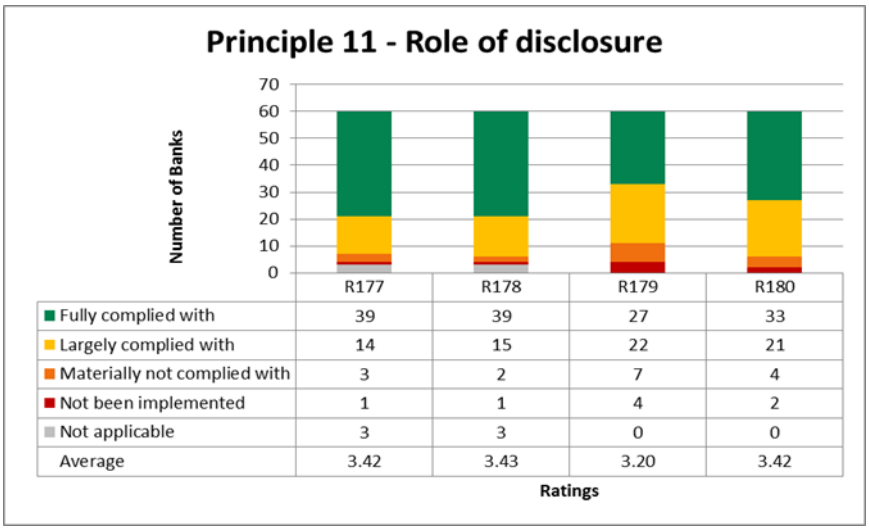
Most banks have established training and awareness programmes for all staff. Noteworthy practices include the provision of customised business continuity training to staff according to their specific roles, as well as regular review of the training to ensure its applicability.

Overall, banks are encouraged to:

- ensure that all businesses and groups are subject to the BCM programme; and
- increase, using a risk-based approach, their participation in disaster recovery and business continuity testing with key service providers.

Principle 11: Role of disclosure

A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.



The banks were asked to rate and describe the extent to which they have implemented the following:

(a) general quality of disclosure of operational risk management (R177);

(b) adequacy of operational risk disclosure for stakeholders (R178);

(c) the disclosure policy addresses operational risk disclosures (R179); and

(d) implementation of a process to review and verification of disclosure (R180).

As reflected above, most of the banks said that their general quality of operational risk disclosure is "fully compliant" (R177). A common practice is to integrate the disclosure into either the annual report or the individually developed disclosure templates under Pillar III. However, those rated below "largely compliant" have not provided sufficient comments for existing gaps.

Regarding the adequacy of operational risk disclosures for stakeholders (R178), most noted that there is a dedicated section for operational risk in external reports, which are regularly updated. However, since most banks don't disclose sensitive information relating to control gaps or issues, these disclosures tend to be primarily high-level statements. In addition, one bank indicated that its disclosure includes specific details about operational losses.

Regarding the disclosure policies that address operational risk disclosures (R179), most banks said that they are not fully implemented. Despite a wide range of ratings, it could be summarised that most participating banks have in place, or will shortly have in place, a disclosure policy. However, a number of banks indicated that their policy is not prescriptively approved by the board, though some have their disclosure policy approved by other committees of the board or senior management.

In addition, some banks have yet to implement a process to review and verify operational risk disclosure practices (R180).

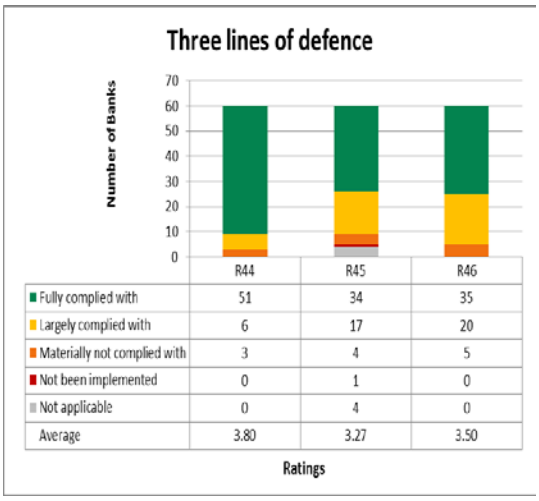
Overall, banks are encouraged to:

- develop a comprehensive disclosure policy that is subject to approval and oversight by the board, and is also subject to independent review; and

- enhance disclosure on how the bank manages its operational risk exposures, and the status of the operational risk management programme.

Overarching principle of the three lines of defence

The bank has established the roles and responsibilities of the three lines of defence, including (i) business line management, (ii) an independent corporate operational risk management function, and (iii) an independent review.



Most banks said that they fully comply with the above paragraph (R44). However, based on comments submitted, a range of practice is observed with respect to the implementation of the three lines of defence. In a few cases, banks have inappropriately classified responsibilities across each of the three lines of defence (eg various business line responsibilities have been assigned to the second line of defence).

A noteworthy practice was a well-documented and clearly articulated set of responsibilities for each of the three lines of defence as follows:

First line of defence responsibilities include using operational risk management tools to identify and manage risks, assessing and enhancing controls, monitoring and reporting the operational risk profile, ensuring that the operational risk profile adheres to the established risk appetite and tolerance, complying with policies, standards and guidelines, and promoting a strong risk culture.

Second line of defence responsibilities include designing operational risk management tools used by the business to identify and manage risks, applying "independent challenge" to the use and output of the operational risk management tools by the first line of defence, developing and maintaining policies, standards and guidelines, reviewing and contributing to the monitoring and reporting of the operational risk profile, designing and providing operational risk training and awareness, and promoting a strong risk culture.

Third line of defence responsibilities include independently verifying that the ORMF has been sufficiently well 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 and output of the operational risk management tools, reviewing the monitoring, reporting and governance processes, and promoting a strong risk culture.

Overall banks are encouraged to:

- ensure that an effective three lines of defence model is implemented to appropriately identify and manage operational risk.

For complex banking structures, the bank has implemented a more refined approach to assigning more specific roles and responsibilities of the three lines of defence among relevant departments (eg business unit (1a), business unit ORM (1b), other corporate subject matter experts (2a), corporate ORM (2b) etc).

As shown in the chart, many banks are still in the process of implementing a more refined approach to assigning specific responsibilities for the three lines of defence to the relevant departments.

A noteworthy practice was the involvement of corporate control groups with relevant expertise (eg compliance, legal, business continuity, technology risk management etc) in supporting the second line of defence with various operational risk management tools.

Overall banks are encouraged to:

- assign roles and responsibilities for the three lines of defence to relevant departments such as business units, business unit ORMs, other corporate experts and ORMs.

There is a strong risk culture and good communication between the three lines of defence for ensuring good operational risk governance.

Only about two thirds of the banks said that they fully comply with this principle, explaining that they are still in the process of building a strong risk management culture. This is most likely because various operational risk management tools are still only partially implemented. Banks also reported obstacles in communication and training that have hindered the development of a stronger corporate culture.

Overall banks are encouraged to:

- reinforce their operational risk management culture through an active communication strategy.

First line of defence

By industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

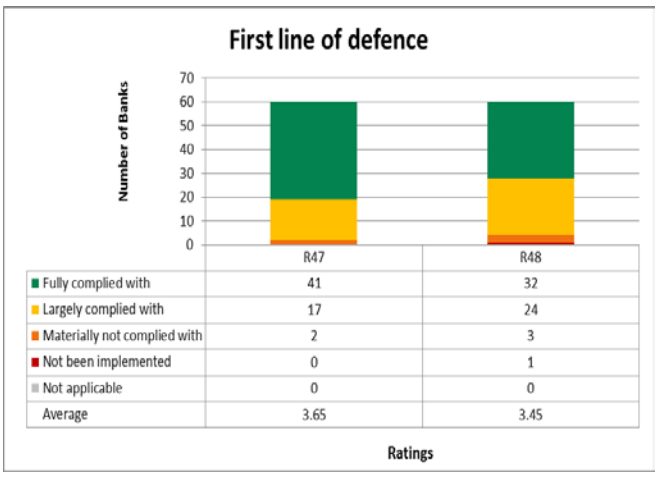
The banks were asked to rate and describe the extent to which they have implemented the following aspects of the first line of defence:

(a) responsibility to business line management has been assigned for identifying and managing the operational risks inherent in all products, activities, processes and systems for which line management is accountable (R47); and

(b) adequate resources, tools and training have been provided to business line management to ensure awareness of all operational risks and effectiveness of assessments (R48).

As reflected in the graph, overall, banks assessed themselves as largely or fully compliant with the first line of defence principles.

Most banks said that their business units are responsible for identifying and managing the operational risks inherent in the products, processes, services, and activities for which the units are responsible and that business line responsibilities regarding risk management are described in the bank's risk management policy and the ORMF. Furthermore, most banks indicated that business line management has expert resources to assess and manage operational risks in relevant products. However, some banks noted that the assignment of responsibilities needed further refinement and enhancement.



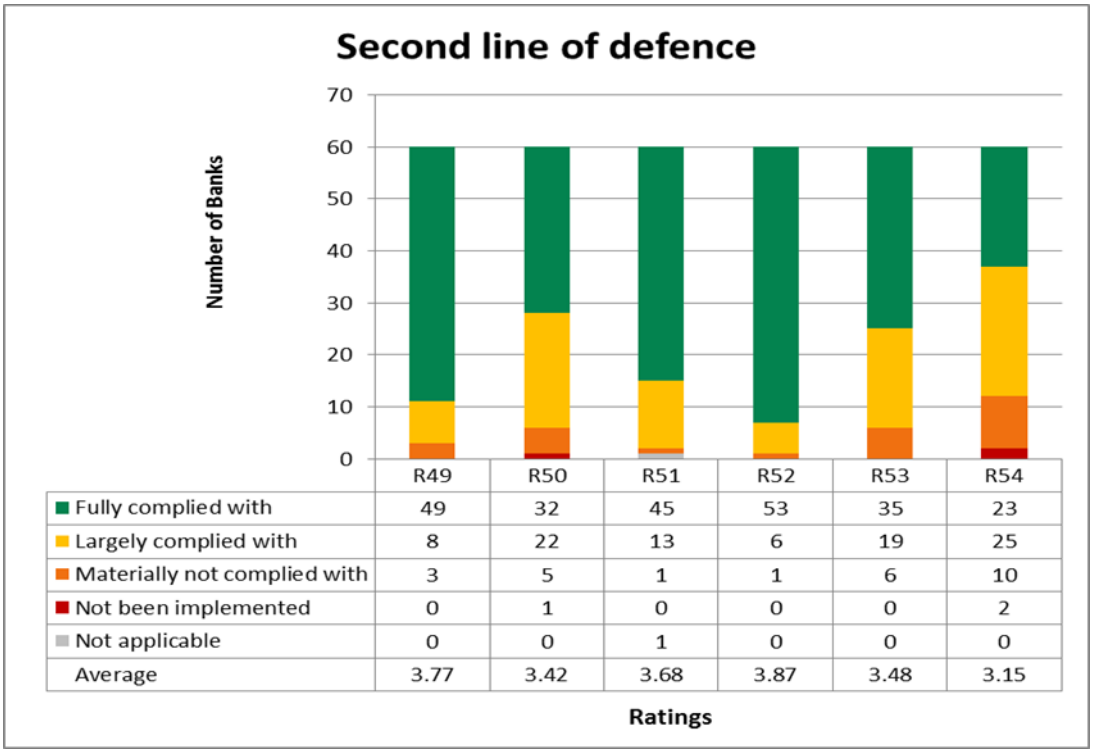
While many banks consider that the relevant resources and tools are adequate (R48), some indicated a need for greater resources. In most cases, business line management training is regularly provided to key elements of the ORMF, and is provided ad hoc for tool updates and framework changes. Training takes the form of electronic learning, comprehension tests, and seminars. However, it is not clear for most banks whether refresher/follow-up training is provided.

Overall, banks are encouraged to:

- further refine and enhance the roles and responsibilities for business line management; and
- ensure that refresher or follow-up training is provided to business line management.

Second line of defence

The second line of defence responsibilities that are assigned to the corporate operational risk function include challenging the business units' inputs to, and outputs from, the bank's operational risk management tools, operational risk measurement activities, and operational risk reporting systems.



	R49	R50	R51	R52	R53	R54
Fully complied with	49	32	45	53	35	23
Largely complied with	8	22	13	6	19	25
Materially not complied with	3	5	1	1	6	10
Not been implemented	0	1	0	0	0	2
Not applicable	0	0	1	0	0	0
Average	3.77	3.42	3.68	3.87	3.48	3.15

The banks were asked to rate and describe the extent to which they have implemented the following in relation to the second line of defence:

(a) appropriate evidence for an independent challenge that is applied to operational risk management tools, measurement activities, and reporting systems (R50);

(b) the responsibilities have been clearly assigned to other internal control groups or centres of competence (eg BCM, compliance, legal etc) (R51);

(c) the responsibilities assigned include development and ownership of operational risk management policies (R52);

(d) the CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities (R53); and

(e) the CORF has implemented a quality assurance programme that ensures that an independent challenge is consistently applied to the operational risk management tools, measurement and reporting systems (R54).

As shown in the graph, many banks are in the process of implementing a more refined approach to assigning specific responsibilities for the three lines of defence to the relevant departments (R51). A noteworthy practice is the involvement of other corporate control groups (eg compliance, legal, business continuity, technology risk management etc) as experts to assist with second line of defence responsibilities.

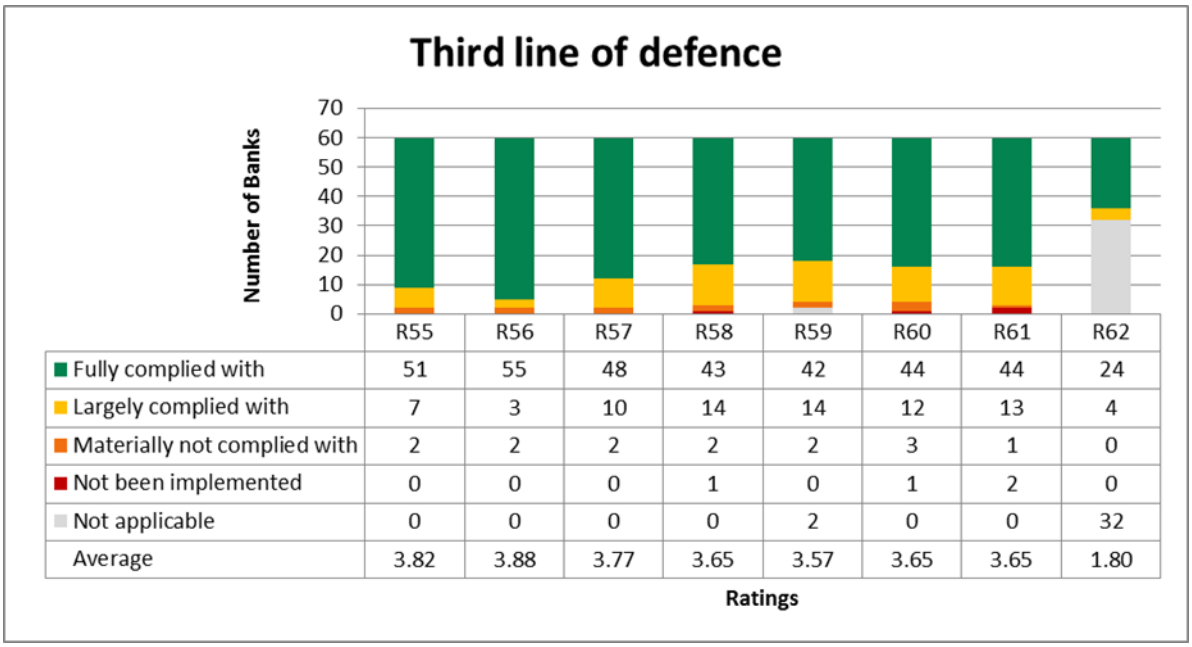
Some banks also noted significant difficulties in consistently applying and evidencing the independent challenge to the use of the operational risk management tools by the first line of defence (R50). In a few banks, there are insufficient resources within the CORF (R53). In addition, many banks have not fully developed a quality assurance programme that is applicable within the second line of defence (R54).

Overall banks are encouraged to:

- assign roles and responsibilities for the three lines of defence to the relevant departments such as business units, business unit ORMs, other corporate experts and corporate ORMs; and
- implement a quality assurance programme within the second line of defence to ensure that an independent challenge is consistently applied.

Third line of defence

The third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.



	R55	R56	R57	R58	R59	R60	R61	R62
Fully complied with	51	55	48	43	42	44	44	24
Largely complied with	7	3	10	14	14	12	13	4
Materially not complied with	2	2	2	2	2	3	1	0
Not been implemented	0	0	0	1	0	1	2	0
Not applicable	0	0	0	0	2	0	0	32
Average	3.82	3.88	3.77	3.65	3.57	3.65	3.65	1.80

Banks were asked to rate[7] and describe the extent to which they have implemented the following elements of the third line of defence:

(a) the responsibilities including an independent review and challenge of the design and effectiveness of the bank's operational risk management controls, processes and systems (R55);

(b) those performing review and challenge of the design and effectiveness of the banks operational risk management controls, processes, and systems are not involved in the development, implementation, and operation of the operational risk management framework (R56); and

(c) internal audit or other independent parties have sufficient resources to carry out their responsibilities as the third line of defence (R57).

As reflected in the graph above, most banks said that the third line of defence responsibilities are fulfilled (R55) and that those performing the review and challenge of the design and effectiveness of the bank's operational risk management controls, processes, and systems are not involved in the development, implementation, and operation of the operational risk management framework (R56). Furthermore, most banks indicated that internal audit or other independent parties have sufficient resources to carry out their responsibilities as a third line of defence (R57). A few banks noted that their third line of defence responsibilities need improvement in terms of definition, execution, and monitoring, and that staffing within internal audit is insufficient.

Internal audit coverage should be capable of independently verifying that the framework has been implemented as intended and is functioning effectively. Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the appropriateness of relying on an outsourced audit function as the third line of defence.

The banks were asked to rate and describe the extent to which they have implemented the following aspects of internal audit:

(a) internal audit or other independent parties' coverage is adequate to independently verify that the operational risk management framework has been implemented as intended, and is functioning effectively (R58);

(b) the frequency and scope of independent parties' review of both the first and second line of defence are sufficient and commensurate with other risk management functions (R59); and

(c) where independent review activities are outsourced, senior management considers the effectiveness of the underlying arrangements and the appropriateness of relying on outsourced independent review as the third line of defence (R62).

As reflected in the graph above, most banks said that internal audit coverage of the framework is adequate (R58) and that the review of both the first and second line of defence is sufficient and commensurate with other risk management functions (R59) where they follow a risk-based approach when determining the frequency and scope of the audit. However, almost a third of the banks noted that further enhancements are needed or planned to ensure full compliance, and as referenced in other sections of this report, some banks noted that coverage is limited to the operational risk model and its inputs, rather than the overall ORMF.

[7] R62 – a significant number of banks responded "not applicable". Excluding these responses, the average rating would result in an average rating of 3.85.

Approximately half the banks indicated that the outsourcing of independent review activities was not applicable (R62) as these activities were not outsourced, but for the banks that indicated they do outsource this function, most indicated that they were fully compliant.

Internal audit coverage should include judgement on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply test for compliance with board-approved policies and procedures, but should also evaluate whether the framework meets organisational needs and supervisory expectations. For example, while internal audit should not set specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

The banks were asked to rate and describe the extent to which they have implemented the following elements of internal audit:

(a) internal audit or other independent parties' coverage includes judgement on the overall appropriateness and adequacy of the ORMF and the associated governance processes across the bank (R60); and

(b) internal audit or other independent parties do not simply test for compliance with board-approved policies and procedures, but evaluate whether the operational risk management framework meets organisation needs and supervisory expectations (R61).

As reflected in the graph, most banks said that they were fully compliant, in that the audit scope of internal audit includes judgement on the overall appropriateness and adequacy of the operational risk management framework and the associated governance processes in every department (R60). Furthermore, many banks noted that internal audit does not simply test for compliance with board-approved policies and procedures, but also evaluates whether the ORMF meets organisational needs and supervisory expectations (R61).

However, some banks indicated that, although internal audit issues an assurance statement on governance, internal control, and risk management for the bank, this does not provide comprehensive assessment to opine on the implementation of the ORM framework.

Overall, banks are encouraged to:

- ensure that there is sufficient focus and coverage within the audit plan for the ORMF; and
- enhance the execution and monitoring of the third line of defence responsibilities.

4. Recommendations

Failure to fully implement appropriate operational risk identification and management practices may result in direct and material financial losses, or reputational and consequential losses, as well as systemic impacts on other banks, customers, counterparties and the financial system. As shown in this report, banks are at varying stages of implementing the Principles. The peer review also highlighted several principles for which, overall, banks had not adequately implemented or addressed the relevant risk management response.

See comments in the executive summary.

The following summarises the specific areas of operational risk management practice where, overall, the most scope for improvement exists.[8]

Banks are encouraged to:

(a) Risk identification and assessment

(i) increase their use of external data for the purposes of risk management;

(ii) participate in industry consortia, to enhance the availability of external loss data for all jurisdictions;

(iii) further implement the use of business process mapping as an operational risk management tool;

(iv) further implement the use of key risk and performance indicators;

(v) further develop and implement comparative analysis processes that compare the outputs of each of the tools to assess the effectiveness of other tools within business lines, as well as that of tool assessments and outputs across similar business lines and geographies;

(vi) use operational risk scenarios for enterprise-wide risk management assessment purposes;

(vii) ensure that action plans from the operational risk identification and assessment tools are monitored;

(viii) ensure that there is a formal process to create, monitor and remediate action plans derived from all tools; and

(ix) consider more formal processes for benchmarking operational risk management practices externally.

(b) Change management

(i) ensure that their change management programmes are comprehensive and fully implemented;

(ii) ensure that the roles and responsibilities for change management processes are fully implemented and aligned with the principle of the three lines of defence; and

(iii) ensure that post-approval monitoring and post-implementation reviews are fully implemented.

(c) Three lines of defence

(i) ensure that an effective three lines of defence model is implemented to appropriately identify and manage operational risk;

(ii) assign roles and responsibilities of the three lines of defence to relevant departments, including business units, business unit ORMs, other corporate experts and ORMs; and

(iii) reinforce their operational risk management culture through an active communication strategy.

[8] While the Committee expects banks to implement all these recommendations, their implementation may be prioritised in the order shown here if resources are limited.

(d) First line of defence

(i) further refine and enhance the roles and responsibilities for business line management; and

(ii) ensure that refresher or follow-up training is provided to business line management.

(e) Second line of defence

(i) assign the roles and responsibilities for the three lines of defence to relevant departments, such as business units, business unit ORMs, other corporate experts and corporate ORMs; and

(ii) implement a quality assurance programme within the second line of defence to ensure that an independent challenge is consistently applied.

(f) Third line of defence

(i) ensure that there is sufficient focus within the audit plan on the ORMF; and (ii) enhance the execution and monitoring of the third line of defence responsibilities.

(g) Operational risk appetite and tolerance

(i) continue their work to further articulate and implement enhanced, and forward-looking operational risk appetite and tolerance statements.

(h) Operational risk management framework

(i) further develop the integration of the operational risk management programme into the bank's strategic decision-making process;

(ii) ensure that the ORMF or other relevant policy requires a robust operational risk assessment process within the bank's new product and new initiative approval processes;

(iii) ensure that the ORMF specifies the use of all implemented operational risk identification and assessment tools;

(iv) ensure that the ORMF requires the use of the bank's operational risk taxonomy in all operational risk tools, to allow for the aggregation and reporting of operational risks and control issues; and

(v) develop a quality assurance programme to ensure that the independent challenge and review applied by the second line of defence results in consistent risk and control assessments.

(i) Board of directors

(i) ensure the scope of internal audit is on the full implementation and execution of the framework, rather than being limited to the operational risk capital model;

(ii) ensure the scope of internal audit includes review of the effective implementation and execution of the ORMF at the business unit or legal entity levels, to complement the overall audit of the ORMF; and

(iii) consider periodically engaging a benchmarking analysis of the bank's operational risk management framework, with the assistance of independent external advisors, as part of the bank's regular assessment of ORMF's design and effectiveness.

(j) Senior management

(i) ensure that the ORMF is approved by the board or a committee of the board;

(ii) ensure that the CORF has sufficient stature, resources and infrastructure, in relation to other risk management functions, to implement the ORMF;

(iii) ensure that an ORC is established;

(iv) ensure that an effective independent challenge is applied by the second line of defence; and

(v) further develop and implement operational risk training and awareness programmes.

(k) Monitoring and reporting

(i) the timeliness and effectiveness of data-gathering and aggregation in a stressed condition need to be developed or tested;

(ii) flexible processes to extract data on demand need to be further developed; and

(iii) the quality and timeliness of information related to external events or environments need to be improved.

(l) Control and mitigation

(i) broaden the scope of outsourcing oversight beyond internal or related-party providers;

(ii) further develop the consideration of IT risk within the operational risk appetite and tolerance statement; and

(iii) ensure that the bank's risk and insurance management programme is subject to regular board and senior management oversight.

(m) Business resilience and continuity

(i) ensure that all businesses and groups are subject to the BCM programme; and

(ii) increase, using a risk-based approach, their participation in disaster recovery and business continuity testing with key service providers.

(n) Operational risk culture

(i) continue their work to further align compensation policies with the operational risk appetite and tolerance statement; and

(ii) further develop and implement their operational risk training and awareness programmes.

(o) Role of disclosure

(i) develop a comprehensive disclosure policy that is subject to approval and oversight by the board, and also subject to independent review; and

(ii) enhance disclosure on how the bank manages its operational risk exposures, and on the status of the operational risk management programme.

Appendix I – Participating jurisdictions

Bank questionnaire	1	Australia
	2	Belgium
	3	Brazil
	4	Canada
	5	China
	6	France
	7	Germany
	8	India
	9	Italy
	10	Japan
	11	Netherlands
	12	Russia
	13	Saudi Arabia
	14	South Africa
	15	Spain
	16	Sweden
	17	Switzerland
	18	Thailand
	19	Turkey
	20	United States

Appendix II: Guidance for bank questionnaire ratings

The following guidance was provided to the banks regarding the rating scale within the questionnaire.

For the purpose of this exercise, the "implementation" comprises formulation of internal policy by the bank with the approval of its board of directors to implement the principles, dissemination of the policy to all relevant functions in the bank, periodic review of the policy, execution of the policy by those responsible, compliance with the policy by various departments and functional units of the bank, as well as monitoring and review of compliance by the board and senior management.

Rating	Description
4 – Principle is fully complied with	The bank is entirely compliant with the principle, there is evidence to substantiate the assessment, and there are no outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
Example – Para 39 (b): Internal loss events are analysed to provide insight into the causes of large losses and information on whether control failures are isolated or systemic. The bank uses a consistent approach to perform root cause analysis and analysis of control effectiveness for material losses, as well as for monitoring of developed action plans. Rationale: The bank's operational risk management policy requires a root cause analysis to be performed for all operational risk events > $100,000, using a standardised template that facilitates an assessment as to whether other bank units may also be subject to a similar event. The practice is mature, there are no outstanding audits or self-identified issues, and there is a verification process in place to ensure that all events > $100,000 are in fact investigated in line with this policy requirement.	
3 – Principle is largely complied with	The bank is non-compliant in only minor aspects of the principle, the non-compliance is not deemed to be material overall and there may be some minor outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
Example – Para 28 (b): The board of directors should approve the policies of the operational risk management framework. Rationale: The bank's operational risk management policies and framework are regularly reviewed and discussed by the board, but the board does not provide explicit "approval" of the operational risk management policies and framework.	
2 – Principle is materially not complied with	The bank is non-compliant in major aspects of the principle, and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
Example – Para 39 (e): The bank uses business process mapping to identify key steps and risks in business processes, activities and organisational functions. Rationale: The bank uses business process mapping for identifying key steps and risks within financial reporting process for Sarbanes-Oxley (SOX) purposes, but does not use business process mapping across other business groups and/or functions, nor does it consider other operational risk types within the bank's operational risk taxonomy.	
1 – Principle has not been implemented	The bank is entirely non-compliant with the principle and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
Example – Para 27 (b): The bank has an operational risk management framework that describes each of the eight operational risk identification and assessment tools and describes how they are used. Rationale: The bank's operational risk management framework contains no reference to any of the operational risk identification and assessment tools, nor does it include a description as to how they are used.	

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

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.