A Message from the Secretariat

Donna Brenner and Luis Fernández de Heredia, cochairs of the International Operational Risk Working Group (IORWG), are delighted to present the 10th Annual IORWG Conference Summary. It is our honor to lead the IORWG, which has grown to include 61 institutions throughout the world over the past 10 years. On April 21–23, 2015, 59 attendees from 39 central banks and international organizations convened in Cape Town, South Africa, to share best practices, create innovative new frameworks, and discuss topics such as cybersecurity, risk reporting, risk training, and building an enterprise risk management (ERM) program.

We hope that members will find the conference summary to be a useful reference tool. All of the expert group presentations are housed on the IORWG website and serve as educational references for central banks as they continue to enhance their operational risk management (ORM) programs.

We look forward to your continuing engagement within the group. For those who attended the conference in South Africa, we hope you found it meaningful and rewarding. And for those who could not attend, we hope to see you in the Philippines in 2016. The IORWG has planned a number of key initiatives for the coming year that will advance central bank risk management programs, and we seek your continued support and participation.

IORWG Conference Summary

François Groepe, deputy governor of the South African Reserve Bank, provided the welcoming remarks. He acknowledged the importance of the IORWG and the collaboration of the central banks on risk management. He noted that risk management methods are qualitative to a large extent. The IORWG emphasizes the importance of learning from each other. After 10 years, the group has achieved much with few resources. It started as an idea from two founding
François Groepe members. François expressed his enthusiasm for the conference and for the external speakers who joined us this year. He acknowledged the working groups and his interest in the Monetary Policy Risk Repository and encouraged the participants to make use of their time to expand their networks and to enjoy his home of South Africa.

Donna Brenner of the Federal Reserve Bank of Philadelphia provided an overview of the conference agenda and acknowledged the work of the IORWG. She welcomed Luis Fernández de Heredia of the Bank of Spain as the new cochair of the IORWG and acknowledged the contributions of former cochair Helena Tejero, also from the Bank of Spain. First established in October 2005, the IORWG remains committed to its original goals. Membership in the IORWG has continued to grow, and members have taken advantage of many opportunities to learn from their colleagues. Expert groups continue to provide a vehicle for networking and for exploring effective practices. Donna thanked those who led and participated in the working groups. Luis also provided introductory remarks and welcomed new members. The group then participated in roundtable introductions.

**Expert Group 1**

**ORM Trends and Best Practices**

Douglas Pereira from the Central Bank of Brazil led the discussion on ORM trends and best practices and reviewed the IORWG survey findings and conclusions. Thirty-eight of the central banks responded to the survey. The most significant advancements this year in ORM compared with 2014 focused on methodology improvement as well as training and workshops. The top challenges that central banks encountered were related to the commitment from and integration with business areas. Central banks are primarily interested in process improvement, completing the rollout of ORM programs, and risk mitigation and monitoring. Challenges continue to focus on ORM in business areas’ daily processes, integration with strategic planning, and resources and transversal risks. Best practices center on risk self-assessment, incident management, near misses, and special handling of transversal risks. A key area for improvement is related to the use of automated information technology (IT) tools. The primary objectives for next year will focus on the use of IT tools for risk management, awareness, and enhancing incident management.

Samantha Loke from the Monetary Authority of Singapore (MAS) provided an overview of her organization’s operational risk program. The MAS has a dedicated risk function that includes enterprise risk, business continuity management, and investment risk management. The MAS uses a distributed approach with department risk partners and department security officers who serve as key points of contact. Its key risk review focuses on events or issues that could have a significant impact on the MAS, the financial sector, or the economy over a one-year period. In terms of strengthening risk awareness, two of the MAS’ efforts include a robust information security campaign and an annual information security seminar. The MAS also provides an information security digest that shares case studies on operational risk incidents and conducts a two-day ERM course. Samantha also described an industrywide cyberattack exercise from 2014.

Danny Vande Putte from the National Bank of Belgium provided a historical perspective of ORM development at his organization. The bank began its journey in 2007 with varied progress. In 2013, it formally organized using the Three Lines of Defense model with the appointment of an operational risk manager. The ERM policy was implemented in 2015 and defines reporting lines. Some of the bank’s key challenges include the lack of uniform business process descriptions and a misunderstanding of the Three Lines of Defense principle: Business line management is responsible for
daily controls. The bank is working with business areas to have them complete a risk analysis of all business processes and is demonstrating the added value of risk management. Further, the bank is working with business areas by using an ORM incident reporting tool and by quantifying the risk analysis. Last, it has developed working groups to deal with IT security, physical security, business continuity management, legal compliance, and strategic risk.

IORWG members discussed potential refinements to the trends and best practices survey process moving forward. The recommendation is that we develop a single profile with member information to minimize redundant information requests. There was also a discussion on differentiating survey questions in terms of the maturity of the ORM program. There is continued interest in proceeding with the work associated with trends and best practices.

**Expert Group 2**

**Maturity Model**

Douglas Pereira led this expert group that presented the pilot maturity model results. The pilot model was developed using a statistical model to choose the topics and the questions to assess the maturity model. The topics included risk culture, organization, risk reporting, risk management processes, and risk management scope and outcomes. The Delphi model was used until a response rate of 70 percent per risk category was achieved. Development of the maturity model was supported by examples of maturity tools for consideration that were shared by two IORWG members. Each of the questions had a weight assigned to it, and the scores were normalized to 100 percent. Twenty-seven central banks responded to the survey to develop the maturity model.

This model is appealing in that it is central-bank-specific. The members discussed the importance of reviewing the questions and the weights again before the model is finalized.

The Maturity Model signalizes the several stages for implementation and enhancement of the ORM framework in central banks and facilitates the discussion on how the model can help us move to where we aspire to be. The Central Bank of Brazil agreed to update the model in 2016.
Governance and Integrated Reporting

During lunch, Mervyn King, chairman of the King Commission on Corporate Governance in South Africa, addressed IORWG members on governance, 21st century megatrends, and reporting. Professor King discussed industry examples of how responsive companies are to their stakeholders. He shared guiding principles and content elements associated with effective reporting. Members appreciated his personal insights.

Breakout Session Summaries

On Tuesday afternoon, the breakout groups discussed trends and best practices as well as the development of the maturity model. In terms of trends and best practices, Marco Engel from the Dutch Central Bank reported on the group’s discussion on project management and how risk management can add value. By helping to create a framework, project and risk management add value by developing the documentation. Risk management can help develop an objective assessment, analyze risks, and manage change. During the discussion, central banks shared their roles in project risk management. The group also discussed other specialized risks such as business continuity management, physical security, and information security. Jean Goetzinger from the Central Bank of Luxembourg discussed increasing the commitment to risk management through awareness training, scenarios, and informal discussions, and covered ways to convince middle management about the added value of risk management. In terms of efficiency, he reported on the importance of focusing on immediate goals and on having skilled personnel.

External Presentation: Risk Reporting

Gert Cruywagen from the Tsogo Sun Group provided an overview on risk reporting. He discussed various frameworks, risks that can impact businesses, and the case for risk reporting. He also discussed the benefits of risk management, risk governance, and reporting. Gert shared information about King III, the corporate governance standard, stating that the board should be responsible for overseeing risk governance, determining the levels of risk tolerance, ensuring that management considers and implements the appropriate risk requirements, and validating that there are processes in place that enable complete, timely, relevant, accurate, and accessible risk disclosure to stakeholders. He illustrated the differences between board reports and executive risk reports. He shared information regarding sources of risk information, the content of board reports, and the content of executive reports. Typically, a board report will include a prioritized rank of enterprise risks, an overview of the risk program, risk response plans and progress, program initiatives, accomplishments, an outlook, and an overview of governance. Executive reports will include many of the same items as well as information about stress testing, scenario analysis results, risk tolerance and risk appetite statements,
blind spot risks, and risk culture. He also shared the templates of many types of risk reports.

**Expert Group 3**

**Risk Reporting**

Andreas Burgstaller from the European Central Bank and Donna Brenner led the discussion on risk reporting. Donna reported on the industry scan of information from KPMG, Deloitte, and other sources. Some of the key messages focused on balancing too little versus too much detailed information, finding the right metrics for reporting, developing a coherent picture of the risk universe, balancing graphics and text to tell an informed story, and providing benchmarked information wherever possible. Overall, the key challenges are minimizing the need for manual reporting, ensuring the information is concise, creating a report that demonstrates the business value of ERM, and having a process in place to monitor mitigation. Industry experts emphasized the need to customize reports to the audience; to balance reporting with a combination of narratives, graphics, and concise conclusions, building in metrics, wherever possible; to use heat maps to clearly illustrate the risks to an organization; and to integrate risk reporting with audit, strategy, information security, project management, and other disciplines.

Andreas Burgstaller shared the survey outcomes. Thirty-three central banks responded to the survey request. The most prevalent risk report provided a bankwide summary of the operational risk across the organization. The status of mitigation is included in half the reporting. In addition, incident reports were the most widely produced operational risk reports often used by the Risk Committee. Microsoft Excel, Word, and PowerPoint are the most common tools used in risk reporting. Many central banks use benchmarking in their reports to challenge risk assessments, identify gaps, promote consistency, guide report design, and so forth. The survey results corresponded to the industry results, with respondents noting the importance of simple, timely, and accrual reports that are visual. Central bank reports should focus on the receiver and should be shared with the business area to foster risk awareness and transparency. The key challenges are providing good data quality and the appropriate amount of data to support conclusions without too many details for the reader. Central banks should consider ideas that have operational risk as a standing topic at board meetings, that improve the executive summary of reports, that increase the number of tools being used, and that expand the monitoring of mitigation activities.

**Expert Group 4**

**ORM Training Best Practices**

William Matambo from the Reserve Bank of Malawi and Trudy Bartley from the Central Bank of Ireland led the discussion on risk management training. William reported that 27 central banks responded to the survey. For more than half the respondents, training is not mandatory, and most respondents spend less than 10 percent of their time on training-related activities. He shared the survey results that included information on approaches, target audiences, maturity level, adaptability of materials, approaches, and other topics. More than 40 percent of the training delivery methods
included presentations. Risk management departments keep staff updated using electronic vehicles (such as e-mail and the intranet), publishing articles, circulating publications, conducting refresher training sessions, and holding meetings. The key challenges are related to demonstrating the value and importance of training and the funding of training-related activities. To help get top management support, central banks should consider developing incident management frameworks, developing key risk dashboards, lobbying through the board, demonstrating the value proposition, and publishing benchmarking exercise results.

He concluded by sharing the golden rules of training, which include focusing on the benefits of training, having an experienced facilitator, matching the training program to the maturity of the bank’s operational risk program, measuring the effectiveness of the training, and keeping staff advised of key changes.

Trudy Bartley reviewed training best practices at the Central Bank of Ireland. The bank’s ORM framework is aligned with the International Organization for Standardization’s ISO 31000, which highlights the need to improve reporting, stakeholder confidence, and trust. Its centralized ORM team spends about 15 percent of its time providing training via presentations, guidance booklets, briefings, a dedicated ORM intranet page, and an internal magazine. The bank introduced a coordinator forum in 2013 that meets twice a year and provides an opportunity for the coordinators to present their approach to the ORM. The centralized ORM team provides a variety of presentations, such as one-to-one, divisional, directoratewide, or to management teams. Training is tailored specifically to accommodate business needs. Some of the challenges include ensuring that the right staff is trained, that there is a correct balance between general awareness training...
and specific technical ORM training, and that the materials are up to date. Trudy noted that her team has trained more than 700 staff members.

Expert Group 5
Information Security and Cybersecurity Risks

Jean Goetzinger from the Bank of Luxembourg and Romain Balleraud from the Bank of France led the expert group on information security and cybersecurity risks. Their work was anchored in an expert group survey to which 53 percent of the members responded. The presentation began with a brief video and then outlined the biggest threats over the next 10 years, according to the World Economic Forum. Data fraud/theft and cyberattacks were both included in the list of biggest threats. The IORWG survey focused on governance, linkage to ORM, risk reduction, awareness, social engineering, mobile devices, analytics, cloud computing, virtual currencies, and biggest challenges.

In terms of governance, 94 percent of cybersecurity is part of ORM. The most commonly used standard is the ISO. Most of the central banks provide quarterly reporting, and less than 40 percent of the respondents do not use key risk indicators (KRIs). In terms of risk reduction, only 40 percent of the respondents have data loss protection, while 80 percent have logging and monitoring tools in place. There are a number of mechanisms related to training and awareness, which include videos, PowerPoint presentations, face-to-face sessions, and other vehicles. For central banks, the security staffing number varies between two and 63 staff members. As far as mobile computing is concerned, almost 70 percent of the central banks have a mobile security policy and one-third of the respondents do not allow employees to use their own devices in the workplace. All central banks have to manage stolen or lost devices. As for risks, criminals use big data to identify potential targets or to improve social engineering attacks. No central banks make use of virtual currency. The top three challenges are dealing with mobile devices, awareness, and human resources.

Enterprise Risk Management at the Reserve Bank of New Zealand

Steve Gordon of the Reserve Bank of New Zealand provided an overview of his bank’s ERM model, its journey to implement ERM, and seven key principles associated with its program. The bank’s reporting model integrates internal audit and incident management data with identified enterprise risks. Environmental factors are identified, and their impact on inherent risk ratings is periodically assessed. The bank has regular board reporting; has engagement to ensure that identified risks are current and have been assessed and have relevant treatment plans; has an empowered staff that can make informed decisions; and has a continuous monitoring process. Its ERM program is based upon seven key principles: executive buy-in, enterprise risk management with a capital “E,” engagement and communication, institutional fit, strategic alignment, business integration, and a focus on what really matters.

The Reserve Bank of New Zealand was recognized with several awards such as excellence in building risk
management capability and a central banking award, which clearly illustrates the progress that has been made.

Breakout Session Summaries

Breakout session discussions were held on training best practices, cybersecurity, and risk reporting. Jonathan Senner from the Board of Governors reported on training. His group discussed benchmarking against other central banks, whether training should be mandatory, and how central banks could leverage the use of technology in providing training sessions. Daniel Wang from the Monetary Authority of Singapore reported for the cybersecurity group. He discussed the challenges of employees’ preferences, balancing efficiency and confidentiality, supplier diversity with mobile devices, and the changing demographics in the workforce. During the reporting breakout session, Otmane Amrani shared risk reporting examples from the Central Bank of Morocco. The group then discussed reporting practices and challenges, which included a discussion on loss quantification, strategic objectives, and performance indicators.

End-of-the-Day Activities

During the evening of the third day, participants continued networking as they dined at a local restaurant. The event was hosted by the South African Reserve Bank.

Compliance Management at the South African Reserve Bank

André Bezuidenhout, head of risk management and compliance at the South African Reserve Bank, provided an overview of the bank’s approach to compliance. The key challenges are related to the nature of the business of a central bank and the risk of unwanted and unintended sharing of sensitive information. The bank uses a hub-and-spoke model for compliance management. The departmental coordinators have a functional direct reporting line to their respective departments and have a dotted line reporting to the central compliance office. André shared that the bank’s vision is to be a trusted advisor with respect to compliance management.

Cloud cover shrouds the mountains along the Victoria and Albert waterfront.
Compliance Management Survey Results

Donna Brenner reviewed the minicompliance survey results. Approximately 60 percent of the central banks responded to the survey. Some of the key observations were as follows:

- The average number of full-time equivalents ranged from one to two to 50.
- The main categories of the program address ethics, insider trading, data protection laws, terrorist financing laws, fraud, and antimoney laundering.
- The compliance function generally devotes time to training and awareness, identification and assessment of risk, monitoring, testing and reporting, and developing policies and procedures.
- The key challenges are establishing the right indicators, setting up incident management processes, training staff, setting up a new program, and striking a balance in reporting. It is a challenge to expect 100 percent adherence to rules and regulations.
- Other challenges include limited staff resources, the unique nature of central banks, and limiting exposures associated with noncompliance.
- Best practices focus on providing training and awareness programs, using e-learning for training, having experts in the business areas to support compliance, cultivating a strong collaboration between the compliance function and the lines of business, providing coverage of compliance risks at risk management meetings, and using the Three Lines of Defense model.
- Central banks have been successful in addressing compliance risks using centralized, decentralized, and hybrid models. Several banks are in the process of setting up compliance risk programs, and the key is to have effective coverage over the areas of compliance risk.

International Monetary Fund (IMF)

Ashraf Khan from the IMF discussed its role and the importance of central bank governance. He shared information about the technical assistance programs he has worked on at various central banks. He also discussed nonfinancial risks as they relate to ORM. Nonfinancial risks relate to people, processes, systems, and external events. Operational risks are more complex than financial risks. He shared information about the toolkits used in risk management. Ashraf expressed his enthusiasm for the work performed by the IORWG and the opportunities that he sees for the IMF and the IORWG working together.

Expert Group 6
Continuing the Operational Risk Repository for Central Banks

Luis Fernández de Heredia from the Bank of Spain has been leading the risk repository initiative since 2011. The areas of focus have included bank notes, market operations, communications, infrastructure, legal, human resources, bank supervision, payment systems, statistics, research, monetary policy, budgeting, and facilities. Since 2011, 45 central banks have supported the development of the risk repository. The foundation of the repository is aligned with the Three (3+1) Lines of Defense Model (business line management, operational risk management, independent review, and external auditors and key stakeholders). This year’s focus was on monetary policy, budgeting, and facilities.

There were five monetary policy risks identified; however, none were considered high risks (likelihood and highest impact). The risks reported were the potential for misuse of secret/confidential information and economic policy being negatively criticized by the media.

The budgeting function reported seven risks. Again, none were considered high risks. The most relevant risks (highest impact and likelihood) were the risks of errors in financial statements and the lack of compliance with tax, accounting, or budgetary rules. The facilities, premises, and health and safety function had six risks reported, with the highest-rated risks being intrusion, theft, or misappropriation of bank assets and errors in the personnel health and safety compliance framework, processes, and measures in place.

Donna Brenner presented the annual report and reminded attendees about the goals of the IORWG. She acknowledged that, since 2006, there have been more than 36 expert groups covering a variety of topics and sharing a wealth of knowledge that can be used by newer IORWG members. The IORWG’s next steps are to plan for the 2016 conference; review the feedback from this year’s conference; continue to enhance activities, establish new working groups, and engage members to share good practices; and welcome new members and representatives. The IORWG has continued to grow over the past year.

Donna and Luis expressed their deep appreciation to the South African Reserve Bank for hosting, planning, and administering the conference. They also acknowledged the support from the expert groups and leaders. They discussed the next steps in developing future expert groups based upon the survey data captured during the conference, developing future working papers, and expanding the IORWG website.

End-of-the-Conference Activities

After the conference, members had an opportunity to continue networking by participating in a sightseeing tour of South Africa.

Expert Groups and Conference Feedback

In Cape Town, the IORWG was committed to establishing new initiatives and expert groups for 2016, based on the attendees’ preferences. The topics for the expert groups will be:

- Key Risk Indicators (Advancement of Central Bank Practices)
- Integration of Business Continuity Management into Operational Risk Management
- Risk Management and Linkage to Strategic Planning
- Cybersecurity Continuation
- Operational Risk Quantification for Capital Adequacy

In parallel, there are three initiatives that will provide the opportunity for active member participation:

- ORM Trends/Best Practices and Building an ORM Maturity Model (ongoing)
- Collection of Sound Principles and Good Practices (first working paper)
- Light Update of the Risk Repository (ongoing)

The survey results were summarized after the conference, and the results are as follows:

- Members provided positive feedback and commented that the conference was well designed and covered a relevant range of topics, provided a valuable mechanism for effective networking, and met members’ expectations. The breakout sessions were useful, and the ideas and outcomes of the meeting were considered transferrable to participants’ work. Participants appreciated that the external speakers’ presentations provided different perspectives. Members were highly appreciative of the
hospitality extended by the South African Reserve Bank.

- Opportunities for conference enhancements include the following: (1) increasing the involvement of expert group participants during all phases of the process; (2) focusing expert group outcomes more on the research of practical examples rather than presenting the quantitative data from the aggregation of surveys; (3) including more time for Q&As for each item of the agenda, thus encouraging presenters to be more interactive and dedicating more time for discussions; (4) spreading the expert group work over the course of the year; and (5) allowing more time for breakout discussions.

- Members have continued to be interested in having a combination of members and expert group presentations, breakout sessions, and external speakers for future conferences.