



cutting through complexity™



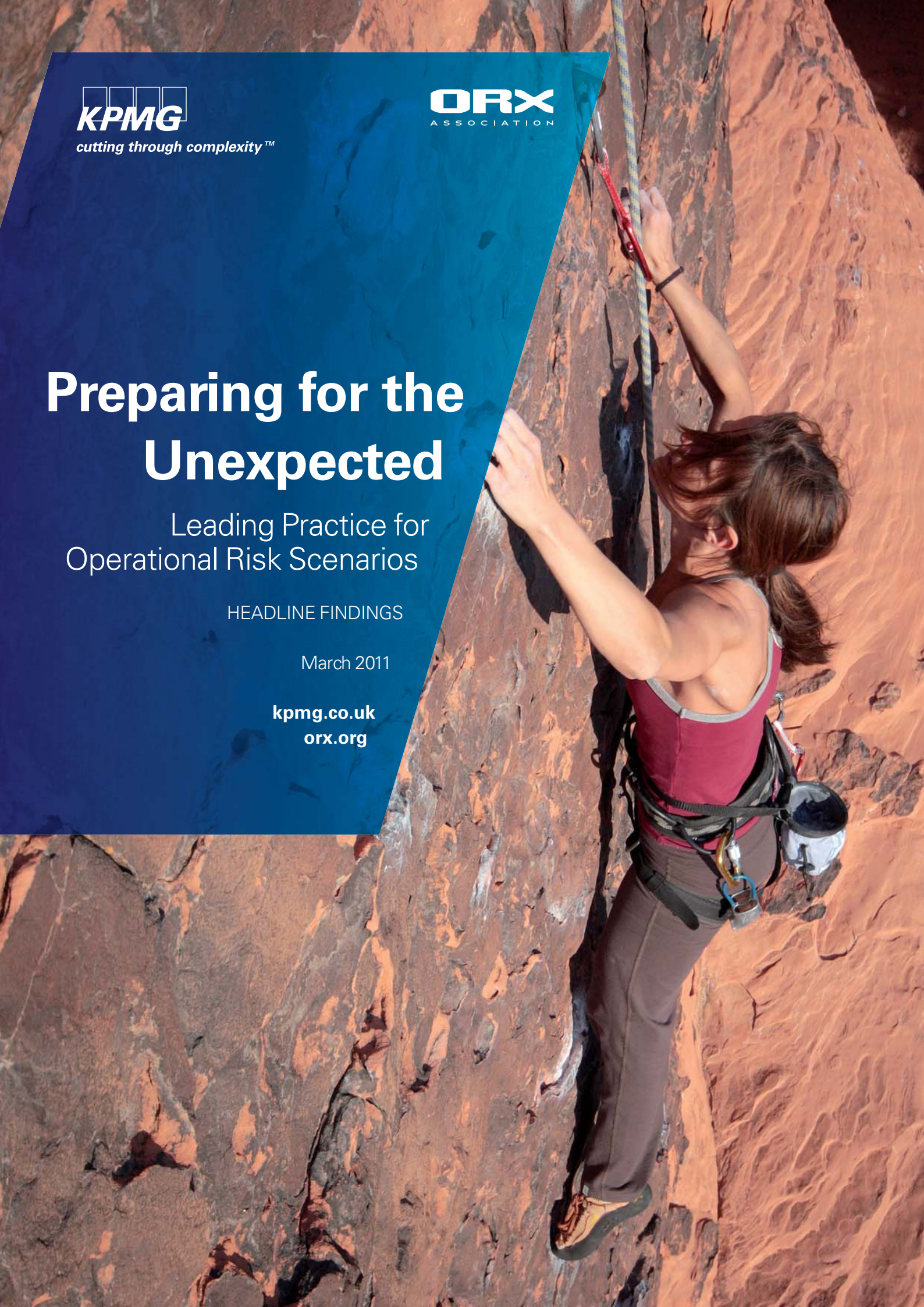
Preparing for the Unexpected

Leading Practice for
Operational Risk Scenarios

HEADLINE FINDINGS

March 2011

kpmg.co.uk
orx.org



Headline Findings

These headline findings are based on a more extensive report prepared by KPMG in the UK in conjunction with the Operational Riskdata eXchange Association (ORX) and working closely with the ORX Members. The report was prepared for the ORX Members and is the culmination of 12 months exploration of Operational Risk Scenarios, both how they are generated and their possible evolution. The full report is available to ORX Members at www.orx.org.

Scenario analysis is a technique of growing interest. It allows senior management to consider systematically the risk of extreme but plausible events they have yet to experience. This helps them to assess the risk of, for example, the next rogue trader or systems failure and proactively consider how to react quickly and decisively should the worst happen. This report explores the progress made at some of the world's leading banks in applying scenario analysis to Operational Risk.

Most banks are investing in Operational Risk scenario analysis. More than fifty percent of the banks participating in a recent study, on which this report is based, either have changed – or will be changing – their scenario analysis practice within 12 months. They are investing in developing an approach that best fits their individual objectives, circumstances and management views, and practice therefore differs across the industry. However, ORX and KPMG have been able to identify common building blocks, along with 'better practices' for each building block, and develop associated maturity matrices.

What matters more, however, is that banks are seeking to find the right balance between risk measurement and risk management. Scenario analysis has previously typically been focused either on group driven 'top-down' measurement models, or business driven 'bottom-up' management models. This study has identified a convergence that can close this gap. The benefits of linking management and measurement accrue on both sides, ideally resulting in scenarios that fit the current business environment and concerns whilst also being executed in a comparable manner and metric across a group. The result is a forward-looking measure of risk that both engages and makes sense to management.

This report is based on actual and evolving practice amongst some of the world's largest banks. It sets out the headline findings gathered between September and November 2010 in a study of leading practices in the creation, validation, and use of Operational Risk scenarios, undertaken by ORX and its member banks working with KPMG. About 40 percent of the top 100 banks around the globe participated in the study, either through surveys, interviews, or attendance at in-depth workshops.



“[Banks] are investing in developing an approach that best fits their individual objectives, circumstances and management views.”

From Diversity, A Common Approach

A key finding from this work is that banks maintain a broad variety of scenario analysis methods for both risk measurement and management purposes. This diversity is likely caused by the following factors:

- Bank choices and circumstances
- Regulatory influence
- The early stage of evolution of Operational Risk as a principal risk discipline.

Nonetheless, the study identifies and validates a common approach that banks can use to help gauge the relative maturity of their scenario analysis processes. The high-level building blocks that comprise the approach are:

- **Governance:**
Good governance is critical to enabling the scenario analysis process to maintain a valuable place in the suite of management tools influencing the running of the business on an ongoing basis. The role of effective governance includes ensuring that the scenario process gains support and buy-in from all important stakeholders and achieves the integrity, consistency, and longevity required for it to be fully effective.
- **Preparation:**
Scenario analysis is used in many different functions across banks. However, the key to successfully preparing and designing a scenario is the same, whether the purpose is to analyze Operational Risk, define business strategy, or identify the business impact of system failure. Everyone involved in the scenario design needs to clearly understand the objective of the exercise and the details of the well-described scenarios.
- **Assessment:**
This generally involves the assessors (either via workshops, interviews, or questionnaires) estimating frequency and severity parameters for each scenario, or combinations of them. The assessment team may be a combination of subject matter experts, business unit managers and executives, business risk managers, and representatives from group functions (e.g., HR, IT, Legal, Internal Audit). Critical to this step is an appropriate team and a well-designed assessment process.

- **Validation:**

It is essential to review the results of scenario analysis to ensure that consistent and defensible estimates and outcomes are delivered. The assessment process is inherently subjective and susceptible to bias, and, most of all, people have a recognized difficulty in specifying their beliefs in well-calibrated and consistent statistical estimations. A well-structured and systematic review and validation approach for scenario analysis is crucial to minimize and control these challenges.

- **Reporting:**

As scenario analysis is used both for risk measurement and for risk management, there are a broad range of potential channels by which, and audiences to whom, the results may be reported. Aspects of the scenario analysis process (including, but not limited to, inputs and outputs) may periodically be reported to business unit management and executive committees, local Operational Risk management, the Corporate or Group Operational Risk management function (CORF), Group executive management, and Board risk committees.

Each of these building blocks is, in turn, made up of components that can be separately described and evaluated. These components were explored in some detail in workshops, producing maturity matrices. These matrices can be used by a bank to frame a view of its current state. Each matrix is constructed with gradations, proceeding from 1, which is a basic state, to 5, which is a sophisticated, and what may be conceived as an aspirational, state. Generally, large and complex banks will be found at or around level 3.

Illustrative Maturity Matrix component from the Validation building block

Validation	Maturity levels				
Assessment Category	1	2	3	4	5
Techniques and data used for validation	<ul style="list-style-type: none"> No data is used to validate SA inputs and outputs Only SA parameters are reviewed Validation relies on an informal third party (4 eyes principle) subjective review of assessment responses 	<ul style="list-style-type: none"> Elements of AMA framework (ILD, ELD, RCSA) are used to cross-check assessment results on ad-hoc basis Third party review (4 eye principle) is subjective 	<ul style="list-style-type: none"> In addition to ILD, ELD, and RCSA, range of internal sources are used to inform the evaluation / validation process (e.g., audit report, IT security assessment) Validation of scenario assessment is performed using a subjective approach coupled with benchmarks against a well-defined set of indicators (e.g., ILD particular to risk / BU under investigation). However, the analysis may not be uniformly applied across the organization Clear data quality guidelines, controls, and tests 	<ul style="list-style-type: none"> Structured and documented process for review of SA outcomes, which may include use of decision tree or other analysis schemes Clear data quality guidelines, controls, and tests In addition to loss / risk / controls data, economic and financial indicators are also used as benchmarks (e.g., Basel BIA or TSA capital requirement, Gross Income) Structured and comprehensive backtesting program is applied granularly Formal process to investigate why the largest realized loss(es) were not anticipated in the SA process 	<p>In addition to the criteria in level 4:</p> <ul style="list-style-type: none"> Benchmarking against a well-defined set of indicators, including industry data Advanced techniques are used to support outcome validation, which may include non-standard approaches derived by "opinion poll"; e.g., <ul style="list-style-type: none"> - Introduction of "control" questions - Resampling of evaluations - Profiling of assessors

The example table above sets out the maturity level criteria for one assessment category of the 'Validation' building block, detailing the different degrees of sophistication using the various maturity levels. At the most basic level for this component, validation focuses only on a subjective review of the scenario analysis parameters (e.g., severity, frequency). In contrast, at level 3 the validation process is grounded on data from a range of sources, including ILD, ELD, RCSAs, audit reports, and IT assessments. At level 5, several additional elements are considered that include

predominantly qualitative techniques focused on expert opinion, as well as quantitative benchmarking against industry data. This latter technique is desirable, albeit currently aspirational because there is no appropriate industry data set that can serve as a benchmark. Moreover, it should be noted that workshop participants caution that level 5 may not be appropriate in all cases, due to the disproportionate cost against the marginal return in benefits, particularly given the understood difficulties in demonstrating 'value'.

“The approach is robust when risk measurement and management are tightly aligned.”

“Best For Bank”

How a particular bank approaches the scenario analysis process and where it places emphasis may be heavily influenced by a range of factors, including size, business model, product offerings, geography, and national regulator expectations. For example, where scenarios are used for regulatory capital calculation, there is greater emphasis on objective measurement, and usually the process needs to be approved by a regulator. This affects factors including the rigor of the process, documentation, and validation.

Many banks agree that the amount of time, energy, and resource that a particular bank invests into its scenario analysis process, and thus its maturity, should be “Best for Bank,” in that it should be tailored to the bank’s individual needs.

Further, a highly sophisticated approach that is not broadly understood and designed to be used as an integral part of risk management may add less value than an unsophisticated, well-understood and applied approach. For example, what may be right for a large, universal bank may be wrong for a much smaller, regional retail bank.

Moreover, the study suggests that time and experience are important distinguishing factors, as senior executives and business managers need to develop their levels of comfort with, and confidence in, the process in order to effect adjustments and successfully embed the process within the business. Where a better scenario analysis approach can be conceptualized, it cannot be truly effective until some real experience is applied to it.

Better Practices

That being said, the following are amongst the better practices in scenario analysis:

Governance

- Transition scenario analysis ownership and execution from the Group or corporate Operational Risk function (CORF) to business units, with Group oversight
- Establish a clearly defined escalation process to resolve differences and disputes amongst stakeholders
- Promote strong buy-in from the executive management, setting the correct “tone from the top.”

Preparation

- Source a variety of relevant information to inform scenario development (e.g., internal and external loss event data; key risk indicators; emerging risks)
- Solicit business unit management consensus on the topics for scenarios that have been selected
- Apply a defined and regular process for triggering, replacing, and changing scenarios.

Assessment

- Provide information that brings to life the scenario being assessed for the business, and assists in estimating loss parameters
- Strengthen the credibility of the assessment results by securing participation of business and functional experts
- Clearly document the assessment process in order to ensure both verification that the process was correctly followed and validation of the results.

Validation

- Provide a substantive independent challenge process
- Engage an independent party to verify the conduct of the overall scenario analysis process.

Reporting

- Present both to executive and business line management the results of the assessments in a manner that allows them to make informed decisions
- Ensure that the results of the scenario analysis process flow into a continuous improvement process and provide meaningful insight and benefit to the institution.

Bias Mitigation

- Use available empirical internal and external data in the preparation and assessment phases
- Ensure transparency in the assessment phase
- Maintain a strong validation process.

MindThe Gap – Risk Measurement And Risk Management

Unsurprisingly, in the wake of the recent global economic crisis and the ensuing emphasis placed on risk appetite and risk capital calculations by managers and regulators, many banks report that risk measurement has been the dominant focus of their scenario analysis activities.¹ As risk managers focused on ensuring that sufficient capital was held for certain risk profiles, less resource and consideration was devoted to scenarios for risk management purposes. Crucially, however, this is already beginning to change. There has been a notable shift in regulatory attention towards the importance of risk management, which is matched internally by bank management.

While the building blocks for both risk measurement and risk management purposes are generally the same across banks, there are observable differences in the focus of the respective processes. For example, scenarios primarily for risk management uses are generally:

- Created bottom-up and owned, assessed, and validated at a lower point in the organization, closer to where the risk resides
- More granular in terms of event types and business unit levels
- More qualitative in analysis
- Undertaken with a greater degree of causal factor analysis, identifying discrete, linear risk indicators
- More focused on expected loss
- More likely to be linked to performance scorecards and cost-benefit analysis.

In contrast, scenarios used primarily for risk measurement and capital uses are generally,

- Subject to a process owned at the Group level
- Fewer in number created, usually by orders of magnitude
- More tightly focused on strategic and emerging risks, and are created at the Group level, or one or two levels below
- More likely to be centrally-defined, consistent, transparent and repeatable
- Less susceptible to bias – in particular, motivational and gaming bias – than risk management scenarios, due to rigor in the process
- Closely linked to higher order concerns of regulatory and economic capital, enterprise risk appetite and tolerance, and risk-adjusted return on capital.

To the extent that a maturity gap may have developed between the scenario analysis processes for risk measurement and risk management, banks anticipate a convergence that will drive a robust, integrated risk management platform. As this transition takes place, risk managers expect the center of gravity for the scenario analysis process will lower from CORF to the business unit level, where the risk ownership resides. They also expect that the risk management process will rise in the opposite direction (from business units to group level), where standardization can take place and risk management information can be captured and shared across the organization. The approach is robust when risk measurement and management are tightly aligned.

An Evolving Future

In a business world where the best prepared invariably come out strongest, scenario analysis already has a firmly-established role in the toolkit of the Operational Risk manager. As techniques evolve and mature with experience, scenario analysis and the value it brings will strengthen, making banks and their executives better prepared than ever before to cope with the unexpected.

¹ Stress testing is a special case of scenario analysis. In banking, the scenario analysis process generally consists of defining a scenario with extreme event potential around a particular risk (e.g., a pandemic) and calibrating risk factors around a business or organisation in terms of likelihood (frequency) and impact (severity). In a stress test, only a severity estimation is sought, as the test asks what is the impact assuming that the specified risk occurs (i.e., the probability of occurrence is certain).

“As techniques evolve and mature...scenario analysis and the value it brings will strengthen, making banks and their executives better equipped than ever before to cope with the unexpected.”



Contact us

KPMG key contacts

Jeremy Anderson

T: +44 (0)20 7311 5800

E: jeremy.anderson@kpmg.co.uk

Jane Leach

T: +44 (0)20 7694 2779

E: jane.leach@kpmg.co.uk

Mike Ritchie

T: +61 (2) 9335 8251

E: mikeritchie@kpmg.com.au

Jitendra Sharma

T: +1 212 872 7604

E: jitendrasharma@kpmg.com

www.kpmg.co.uk

ORX key contacts

Simon Wills

Executive Director

T: +44 (0)1225 430 391

E: simon.wills@orx.org

Mark Laycock

Senior Advisor - Standards

T: +44 (0)1225 430 393

E: mark.laycock@orx.org

www.orx.org

About this document. This document extracts the key findings from the February 2011 report *Preparing for the Unexpected: Leading Practice for Operational Risk Scenarios*. The Report has been prepared by KPMG LLP in the UK (described in the Report as "KPMG"), in conjunction with the Operational Riskdata eXchange Association ("ORX"), for use by ORX, as a body, for the reasons summarised in the Executive Summary. The Report is derived from information provided to KPMG or available from public sources but the accuracy or completeness of any such information has not been verified by KPMG. Recognising that ORX is performing a service for its members by commissioning the Report, in order to support ORX, but without accepting or assuming any responsibility or liability to any member or members of ORX in connection with the Report, KPMG has not charged any fee for preparation of the Report. The Report is not designed to provide any benefit, or to be of any use, to any of the various parties interested in the topic of operational risk except for ORX, as a body. Limitations on the nature of KPMG's work are set out in the Introduction section of the Report. In preparing the Report, KPMG has not had regard to any considerations specific to individual members. KPMG has taken an objective and impartial approach. In the Report KPMG does not advocate or promote any particular approach or strategy regarding the creation, validation, and use of scenario analysis for operational risk. The Report is not suitable to be used or relied on by any party wishing to acquire rights against KPMG other than ORX, as a body, for any purpose or in any context. Any party other than ORX that obtains access to the Report or a copy, whether with the knowledge of KPMG or otherwise, and chooses to use or rely on the Report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG does not assume any responsibility and will not accept any liability in respect of the Report to any party other than ORX, as a body.

© ORX 2011. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.