

KPMG

**Operational Risk
A Storm is Coming**

Andrew Smith
June 2006

AUDIT • TAX • ADVISORY

DF026

Agenda

Charting the rise of Operational Risk

But ...

Operational Risk: RIP

KPMG

© 2006 KPMG LLP, the U.S. member firm of KPMG network, a Swiss entity. All rights reserved. This document is confidential and for circulation only and may contain information that is proprietary to KPMG network, a Swiss entity.

1

Operational Risk

The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events (BIS)

Operational risk is not a new risk however the idea that operational risk management is a discipline with its own management structure, tools and processes is new (BBA).

KPMG

© 2006 KPMG LLP, the U.S. member firm of KPMG network, a Swiss entity. All rights reserved. This document is confidential and for circulation only and may contain information that is proprietary to KPMG network, a Swiss entity.

2

OR emerged as a result of focus on controls and governance DF026

Examples

- ▶ Treadway Commission (1987)
- ▶ Federal Deposit Insurance Corporation Act (1991)
- ▶ COSO Report (1992)
- ▶ Cadbury Commission (1992/93)
- ▶ Public Oversight Board (1993)
- ▶ COCO (1994/95)
- ▶ Quality movement (Baldrige/EQA)

General Trend towards empowered, self managed work teams and flatter organisations

© 2009 KPMG LLP, a U.S. member firm of KPMG network, a Swiss entity, through member, the Swiss entity a member firm of the network and its members. KPMG and the KPMG logo are registered trademarks of the member firms of the network.

3

OR Infrastructure at a leading FS group DF026

① Internal risk profile
② Internal loss history and KRI
③ External loss history

© 2009 KPMG LLP, a U.S. member firm of KPMG network, a Swiss entity, through member, the Swiss entity a member firm of the network and its members. KPMG and the KPMG logo are registered trademarks of the member firms of the network.

4

OR Reporting at a leading FS group DF026

© 2009 KPMG LLP, a U.S. member firm of KPMG network, a Swiss entity, through member, the Swiss entity a member firm of the network and its members. KPMG and the KPMG logo are registered trademarks of the member firms of the network.

5

Agenda DF026

Charting the rise of Operational Risk
But
 Operational Risk: RIP

© 2008 APRIE LLP. All U.S. member firms of APRIE International, a Swiss corporation, through APRIE, the firm acts as a consultant to its clients and its members. APRIE and its member firms are registered providers of APRIE International, a Swiss corporation.

APRIE 6

The Problem DF026

The Banking Industry has been working hard on OR since the early 1990s. OR is now a formal capital requirement within BIS II.

But

..... the better the banks got at the traditional approach to OR, the more it became obvious that it doesn't work well!

© 2008 APRIE LLP. All U.S. member firms of APRIE International, a Swiss corporation, through APRIE, the firm acts as a consultant to its clients and its members. APRIE and its member firms are registered providers of APRIE International, a Swiss corporation.

APRIE 7

Example (1): Quantifying Operational Risk DF026

Most OR quantification is poor because

- initial input data is poor
- little delivery of consistent or effective actions
- little feedback into new input data

© 2008 APRIE LLP. All U.S. member firms of APRIE International, a Swiss corporation, through APRIE, the firm acts as a consultant to its clients and its members. APRIE and its member firms are registered providers of APRIE International, a Swiss corporation.

APRIE 8

Example (2): Key Risk Indicators (KRI)

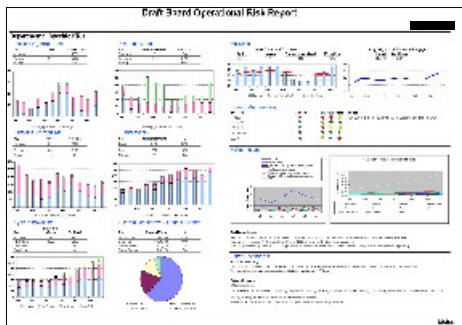
DF026

- KRI should be leading indicators of possible material change in OR environment
 - KRI are formal part of BIS II Pillar 1 OR qualitative standards
- But
- They are not a picture of the risk profile at all!
 - They are a picture of how the risk profile might be evolving because formal risk information/quantification is poor!



Example (3): Board Reporting

DF026



Audience participation (1):-

DF026

- Q1: Does senior management in your organisation care passionately about the quality of your business?
- Q2: Does senior management take operational risk management seriously using it as a key tool for effective business management rather than occasional involvement in risk registers with little follow through into actions
- ⇒ Is the fundamental problem the commitment and competence of senior management or is it the traditional operational risk concept?



Q: Is your organisation clear as to what operational risk management really means and what it should be achieving?

⇒ Real need for a clear concept for risk management customised to your organisation.

Charting the rise of Operational Risk
But ...
Operational Risk: RIP

The essence of risk management lies in maximising the areas where we have some control over the outcome, while minimising the areas where we have absolutely no control over the outcome and the linkage between cause and effect is hidden from us.

Peter Bernstein
(Against the Gods)

Risk Management is..... DF026

A set of actions used to
contribute towards
the likelihood of achieving and surpassing
planned objectives
over a defined timeframe

© 2006 SPINA LLP. All U.S. member firms of SPINA LLP are U.S. member firms of SPINA LLP. The firm name is a trademark of SPINA LLP and its member firms. SPINA LLP and its member firms are not responsible for the content of this presentation.

15

Risk Management is DF026

The set of **actions** used to

contribute towards

the **likelihood** of **achieving** and **surpassing**

planned objectives

over a defined **timeframe**

Only things that happen make a difference

Stability

If there is no uncertainty, RM has no meaning

Outperformance

RM is part of a business, all must work together

without clarity here action ultimately meaningless

Plans are not always realistic but the scope of ambition drives the nature of the actions required

because risk = uncertainty in timescale concept is essential

© 2006 SPINA LLP. All U.S. member firms of SPINA LLP are U.S. member firms of SPINA LLP. The firm name is a trademark of SPINA LLP and its member firms. SPINA LLP and its member firms are not responsible for the content of this presentation.

16

Risk Management is DF026

A process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Enterprise Risk Management Integrated Framework
COSO 2 September 2004

© 2006 SPINA LLP. All U.S. member firms of SPINA LLP are U.S. member firms of SPINA LLP. The firm name is a trademark of SPINA LLP and its member firms. SPINA LLP and its member firms are not responsible for the content of this presentation.

17

Risk Management Culture? DF026

People/Organisations	
Will	Won't
<ul style="list-style-type: none"> ▶ Do what is important to them. ▶ Do things which demonstrably and measurably add value. 	<ul style="list-style-type: none"> ▶ Take seriously regulatory initiatives that they don't believe in. ▶ Keep doing things unless the value arising is evident.

can only achieve a risk management culture when there is alignment between the goals of risk management and the goals of the organisation.

© 2008 APRA. All rights reserved. APRA is not responsible for any errors or omissions. This document is confidential and its disclosure may be restricted. APRA and its related entities are not responsible for any errors or omissions.

18

5 Success Factors for managing OR DF026

- Operate a Total Risk programme, capturing all important risks exactly once.
- Align and customise management of risk to the way in which a (good) organisation actually works and the objectives it wishes to achieve.
- Distinguish between

- Analysis/Reports/Oversight	- "Lets do the right things"
- Action/Management	- "doing it"
- Assurance/Compliance	- "did we do what we said we would?"


© 2008 APRA. All rights reserved. APRA is not responsible for any errors or omissions. This document is confidential and its disclosure may be restricted. APRA and its related entities are not responsible for any errors or omissions.

19

Most Critical Element DF026

- Recognise that operational risk is a regulatory construct.
- It doesn't exist as a single discipline!!

Operational Risk: RIP



© 2008 APRA. All rights reserved. APRA is not responsible for any errors or omissions. This document is confidential and its disclosure may be restricted. APRA and its related entities are not responsible for any errors or omissions.

20

New Approach DF026

Objective

- To create an appropriate and effective framework and culture for the management of Operational Risk (OR) aligned with business objectives, governance framework and operating philosophy
- To enable an effective OR capital assessment through good operating risk information input
- To enable a cost effective, relevant and highly valued risk management process.

Delivery

- Work within the key success factors
- Achieve effective management of operational risk by managing its component specialist areas within an overall framework that ensures complete coverage of important risks across the organisation.
- Operational risk is delivered as a core part of the business not as an add on

© 2008 BSI. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without the prior written permission of BSI.

21

Operational Risk = Sum of Component Risk Areas DF026

<ul style="list-style-type: none"> • Financial Risk [Not OR] <ul style="list-style-type: none"> - ALM/Liquidity/Market Risk - Credit Risk - Insurance Risk - Investment Risk • Tax and Accounting Risk [Not OR] • Regulatory Risk [OR] <ul style="list-style-type: none"> - Interpretation/change - Conduct of business (new) - Public policy (new)? - Contagion Risk • IT Risk [OR] <ul style="list-style-type: none"> - Stability - Application Quality - Infrastructure Quality - Hardware - Security • Business & Strategic [Not OR] <ul style="list-style-type: none"> - Management Risk [OR?] 	<ul style="list-style-type: none"> • Operations Risk [OR] <ul style="list-style-type: none"> - HR - Legal - Fraud - Environmental Risk - Physical Security - Procurement - Health and Safety - Controls design (new) - Information Risk - Property - Project Risk - Other • CEO Advisory Areas [Not OR] <p>[OR] = BISII definition</p>
--	---

© 2008 BSI. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without the prior written permission of BSI.


22

What about the regulator? DF026

Sum of specialist risk areas

- Effective risk measurement
- Effective reporting
- Demonstrable RM process
- Co-ordinated coverage of all risk areas relevant to business

}



© 2008 BSI. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without the prior written permission of BSI.

23
