consultant editor: Jonathan Reuvid

irm

6th edition

Managing Business Risk

A practical guide to protecting your business

citicus

SUNGARD Availability Services

GJE

Gill Jennings & Every LLP
European Patent Attorneys
European Trade Mark Attorneys

XL INSURANCE

Close Credit Management

Field Fisher Waterhouse

sas
THE POWER TO KNOW.

umu. Applegarth

HSBC Insurance

Managing Business Risk

Flamingos curl one leg to conserve body heat.

They can't find a better way to protect against loss.
But you can. With proven risk management software and services from SAS.

www.sas.com/flamingos

SAS SOFTWARE HELPS COMPANIES ACROSS EVERY INDUSTRY DISCOVER INNOVATIVE WAYS TO INCREASE PROFITS, MANAGE RISK AND OPTIMIZE PERFORMANCE.

SAS® for Enterprise Risk Management

Visit www.sas.com/flamingos for a free ***white paper***

- Compliance
- Credit risk and scoring
- Fraud detection and prevention
- Market risk
- Operational risk
- Risk-based performance management

sas®

THE POWER TO KNOW.®

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.
© 2008 SAS Institute Inc. All rights reserved. 500558US.1008

Managing Business Risk

A practical guide to protecting your business

6th edition

consultant editor: Jonathan Reuvid

CollegeHill

SUNGARD Availability Services

MARSH

MMC MARSH MERCER KROLL GUY CARPENTER OLIVER WYMAN

KOGAN PAGE

London and Philadelphia

Publisher's note
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or any of the authors.

First published in Great Britain and the United States in 2003 by Kogan Page Limited
Second edition 2005
Third edition 2006
Fourth edition 2007
Fifth edition 2008
Sixth edition 2009

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licences issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned addresses:

120 Pentonville Road
London N1 9JN
United Kingdom
www.koganpage.com

525 South 4th Street, #241
Philadelphia PA 19147
USA

© Kogan Page and Contributors, 2003, 2004, 2005, 2006, 2007, 2008, 2009

The right of Kogan Page and Contributors to be identified as the author of this work has been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

ISBN 978 0 7494 5449 4

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Managing business risk : a practical guide to protecting your business / [edited by] Jonathan Reuvid. – 6th ed.
p. cm.
ISBN 978-0-7494-5449-4
1. Risk management. I. Reuvid, Jonathan.
HD61.M26 2009
658.15'5–dc22
2008053900

Typeset by Saxon Graphics Ltd, Derby
Printed and bound in Great Britain by Bell & Bain Ltd, Glasgow

The Institute of Risk Management

The Institute of Risk Management (IRM) is risk management's leading professional education and training body. It is a not for-profit organisation owned and governed by its members who are all practising risk professionals. Whether you see risk management as your profession or as a key skill, IRM membership can support you throughout your career.

Membership provides you with information, networking opportunities and recognition. Become an IRM member and you get all the following included in your subscription:

Information

- InfoRM, the Institute's bi-monthly magazine with a weekly e-supplement containing news, articles and job vacancies
- Free subscriptions to risk-related magazines
- Discounts on relevant activities such as conferences and events from third parties
- Unlimited access to the Institute's online Risk Library

Networking opportunities

- Membership of any of the special interest groups you want to join
- Membership of your local regional group
- Free Annual Lecture and other events focusing on the topical issues in risk management
- Discounted entry to the Risk Forum, the Institute's annual conference and dinner

Recognition

- Designatory letters (depending on your membership grade)
- The opportunity to study for an internationally recognised risk qualification

There are various grades of membership starting with Affiliate which has no entry requirements and is open to everyone with an interest in risk management. To become a member all you need to do is simply complete and return the application form from our website (www.theirm.org) or phone us on +44 (0)20 7709 9808.

The IRM provides a broad range of courses to help you build your knowledge and skills. The two-day awareness course on the Management of Risk and Uncertainty is taught across the world and throughout the year. The International Certificate in Risk Management is an introductory qualification, with no entry requirement, which is studied through distance learning.

The International Diploma in Risk Management is a postgraduate qualification for the risk management professional. It is designed to equip today's practitioners to become the risk managers of tomorrow, through the development of a solid, progressive and practical set of skills which in turn enhance career portability, personal status and reward.

Institute of Risk Management
6 Lloyd's Avenue
London EC3N 3AX
+44 (0)20 7709 9808
enquiries@theirm.org
www.theirm.org

RISK: WHAT'S YOUR UPSIDE?

There's a side of risk that's more valuable, and more rewarding. The upside. It's the insight to see risk others don't and unlock opportunities others can't. It's the know-how to optimize your insurability, and the market reach to reduce cost across your full spectrum of risk. Above all, it's confidence, allowing you to

FIND THE UPSIDE℠ MARSH

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

MARSH

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

Managing Risks in a Dynamic Industry Environment – A CMT Perspective

Marsh provides clients with the full spectrum of risk and insurance products and solutions. Our services span internationally renowned broking and placement capabilities, risk and specialty product practices, claims advocacy and related services and risk consulting.

With its focus on industry specialisation, Marsh operates a number of practices with expertise in the relevant risk issues of that particular industry. Marsh's Communications, Media & Technology Practice (CMT), for example, is the global leader in providing risk consulting and risk transfer solutions to organisations in this sector. Our dedicated professionals worldwide can help identify, measure, and manage difficult risks in an increasingly complex, highly competitive, and evolving industry environment.

Marsh delivers specialised advice and solutions designed to assist in responding to financial and operational risks, as well as providing practical steps and considerations to help a client obtain cost-effective and secure protection against the many existing and emerging risks they face.

Broking the best terms

Securing the rewards of well managed risk still eludes a great many companies, even in these challenging economic times. We help companies find that reward. Companies look for insurance and related risk management solutions throughout their operations. They want to be protected now and in the future so that they are able to realise their goals for growth. They want to achieve this as cost effectively as possible, but without compromise.

Insurance will always be part of the solution

Our broking expertise and knowledge of the insurance markets and underwriters mean we can seek the best cover at the best price, matched to a client's exact business profile. We will understand their risk profile, their appetite for risk, and their acceptable level of volatility, so that when a cost-effective solution isn't available from the markets, we will help them manage the risk in other ways.

Delivering the right solutions

We serve our clients through an industry specific lens; we want to make our clients' world our world and align our internationally renowned placement and advisory services in a way that is most relevant to each client and the industry in which they operate. This approach improves the delivery of specialised solutions to all our clients. Thanks to our strong and long- standing relationships with the leading insurance markets, we can help create cost-effective insurance products where previously there were gaps.

For example in the CMT sector, multimedia communications and content strategies, such as the distribution of content through mobile phones and personal computers, are forcing new risks to the surface. Mobile phone providers are moving rapidly from being solely distribution channels for third-party content to being exclusive content developers, modifiers, and branders, thus transforming themselves into virtual publishers, with all the risk issues this entails. CMT companies are now experiencing significant privacy and intellectual property challenges that many are arguably not yet equipped to handle effectively without expert risk advice.

Maximising the insurance investment

Buying insurance should be straightforward – certainly less taxing for an organisation than deciding which product to develop, or which market to enter.

Yet every day, cases arise where organisations find they do not have necessary insurance cover for a loss, either because of lack of limits, inadequate policy wordings, or because they have failed to identify the risk in the first place.

Just as many fail to have enough protection, we also find many cases where organisations pay too much for their limits, or are over-protecting themselves.

Clearly, insurance buying is not always a straightforward process, instead becoming an area where many mistakes can be made.

At Marsh, we are experts in helping organisations optimise their insurance spend, ensuring that policies are matched to their underlying risk exposures and that they are not over or under-insured.

We understand that the efficiency in which organisations buy insurance is linked to a range of other factors, namely their ability to assess and control risk, and make sound decisions about which risks to retain and which risks to transfer.

Marsh can help you strike the right balance in all these areas and take control of your insurance spending and make consistently better decisions in this vital business area.

The role of risk management

Risks are everywhere – but the big issue is how rigorously organisations assess, control and finance them.

There is no question that those that manage their risks better than others enjoy a significant competitive advantage. An advantage that might become critically important in today's challenging economic times.

Put simply, they have a much better chance of reaching their business objectives. They can also enjoy better relationships with stakeholder groups – many of which are applying more scrutiny to business behaviour and are less tolerant of mistakes.

Such organisations are also in a superior position to take calculated risks, due to their greater knowledge of where hazards and opportunities lie. This is a much-needed competence in today's fast-moving marketplace.

Risk management therefore makes good business sense. The benefits are numerous. Managers can make better investments, protect these investments more confidently, and have a better chance of meeting strategic objectives all at a lower total cost of risk.

Risk management is also imperative because transferring risk to the insurance marketplace is not always an available, cheap or best option.

Over the past decade the CMT sector has experienced dramatic change. The convergence theme that was so widely discussed pre-2001 is now a reality. During the past three years, we have seen pure content developers merge with content distributors, content and voice distributors acquire technology companies, and content developers merge with technology companies - and vice versa. Convergence has forced companies to adapt their strategies and business models and continues to create new business realities.

Previously separate and traditional businesses are being combined with distinct revenue models into hybrid businesses with entirely new business models. With the new type of corporate entities comes a new set of strategic, operational, financial, and catastrophic challenges and risks.

Organisations that manage risk well enjoy a 'virtuous circle' when it comes to relationships with underwriters. By controlling risks and reducing internal costs, they can enjoy discounts on their premiums and cope better in a hard insurance market.

Being more in control of their risks gives our clients the confidence to make decisions with less chance of unwanted surprises.

A clear, three-step process to help our clients succeed

We take the time to understand their pressing issues and gauge their volatility and tolerance to risk. We recommend a risk strategy to make the most effective use of your risk investment budget and to protect your balance sheet – from how much insurance you buy to opportunities for reducing your total cost of risk. Our internationally recognised broking teams and risk management advisors then deliver the best solution for your business.

Our approach ensures our clients don't invest in inappropriate areas, or use resources to manage risks that can be removed.

We use our knowledge to help clients optimise their insurability and reduce costs across the full spectrum of risk. The upside is the advantage of risk well managed.

For more information about risk and insurance services Marsh offers, please contact Matthew Hogg on T: 020 7357 2524 or E: matthew.hogg@marsh.com.

The information contained in this article provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insureds should consult their insurance and legal advisors regarding specific coverage issues.

© Copyright - 2009 Marsh Ltd. All rights reserved.

Marsh Ltd is authorised and regulated by the Financial Services Authority.

Contents

Foreword, by Steve Fowler, Chief Executive, The Institute of Risk Management (IRM) *xxix*
Contributors' notes *xxxiii*

Introduction 1

Part 1: Elements of Risk Management **3**

1.1 An appetite for risk 5
Marie-Gemma Dequae, Federation of European Risk Management Associations (FERMA)
Implementing ERM 6; Making it work 7; Building value 9

1.2 Enterprise risk management: finding the optimal blend of enterprise-wide solutions 12
Andrew Oxland, Strategic Risk Consulting, HSBC Insurance Brokers
Introduction 12; The role of ERM in the business world 13; Asset liability management and optimization of the balance sheet 13; Quantification of risk 14; Blurring of banking and insurance solutions to risk 15; Clearly defined risk appetite 15; Synthesis of the insurance and capital markets to provide enterprise-wide solutions 15; Risk solutions for emerging risks 16; Non-financial risk solutions 16; Enterprise-wide risk solutions for the upside of risk 16; Conclusion 17

1.3 Risk management in a business change environment 19
Mike Ward and John Humphries, Outperform UK Ltd
Introduction 19; Define where the business is going 20; Barriers to introducing risk management 22; Developing a risk strategy 24; Integrating the risk management strategy into

business as usual 24; A risk management process 25; Achieving 'risk-managed' business change 27; References and further reading 27

1.4 Rethinking the risk management rule book 29
Chris Woodcock, College Hill
Bridging science and communication 29; Communication networks make timely connections 30; Joined-up thinking 31; Why bother to reinvent the risk management wheel? 32; Supply chain complexities add to the momentum for change 33; The demand for reporting recalls 33; Summary 36; Note 36; Reference 37

1.5 Enterprise risk management solutions 40
Austin Trippensee, SAS Institute Inc
Introduction 40; Enterprise risk management in theory 41; Enterprise risk management in practice 44; Common challenges 46; Conclusion 48; Acknowledgements 48; References 48

1.6 Leading effective business risk management 50
Tenia Chatzinikoli and William Toner, Halcrow
Taking the appropriate risk perspective 51; Defining risk appetite 51; Integrating risk and strategy 53; Understanding key risks and vulnerabilities 54; Embedding risk management across the organization 56; Conclusion 56

1.7 Different views, the same risks: representing uncertainty, assumptions and perspective 59
Allan Robinson and Bob Hide, UMU, Appleyards
Introduction: uncertainty or risk? 59; What is uncertainty? 60; Assumptions and uncertainty 60; Uncertainty management 63; Summary 66

Part 2: Corporate Risk Concerns 67

2.1 Reputation: the all-defining asset 69
Aymen Khoury, Field Fisher Waterhouse LLP
What is reputation risk? 69; The importance of reputation 70; Threats to reputation 70; Reputation dilemmas 72; Conclusion 73

CCH is helping build intelligent businesses.

Measure, monitor, and manage risk and compliance with the most comprehensive, industry-leading ERM system, CCH® Sword. Blue chip financial institutions throughout the world use this award-winning software to support all their oversight functions, ensure compliance with regulations, limit risk within their operations, and provide assurance and security to shareholders, customers and regulators.

The Sword platform's flexible framework allows for the identification and classification of individual risks, and includes integrated tools for the measurement and monitoring of risk levels, as well as easy-to-use reporting and workflow functions which assist in the management of risk across entire organizations.

What business challenge can we help you address?

Call **+353-1-6624-233** or
visit **CCHGroup.com/SwordRisk** for more information.

CCH®
a Wolters Kluwer business

2.2 Reputational risk – king risk 74
Mark Elkins, SAS UK
Reputation matters 75; A good reputation has benefits 76; Bad reputation – the only way is up 76; Measuring reputational risk 77; Reputational risk – capital quantification 78; Managing reputation 80; In conclusion 81

2.3 Risk management: motherhood and apple pie – or real business benefit? 83
Jon Murthy, UKAS
The insurer 83; The health and safety expert 84; The business consultant 85; The manufacturer 86; UKAS 86

2.4 Credit risk management 89
Richard Brennecker, Callcredit
Introduction 89; Credit marketing 90; Application processing 90; Customer management 91; Collections and recovery 92; Summary 93

2.5 Credit risk assessment for loan decisions: a new approach 94
Clark Abrahams, SAS UK
Introduction 94; Capturing revenue opportunities in new markets with alternative credit risk management systems 95; SAS redesigns the credit risk assessment, analytics and performance management process 96; Bridging the gap between compliance and credit risk management 98; Key analytic advances 99; Summary and conclusion 100; Notes 101; Reference 102

2.6 Making risk management deliver business value 103
Ruth Murray-Webster and Peter Simon, Lucidus Consulting Limited
What does risk management really mean for business? 104; How do published standards and methods help, and how do they hinder? 104; The complication of human factors 105; Driven to precision 107; Risk management needs to be exciting, not boring 107; Walk the talk 108; Act of faith, or proven concept? 109; References and further reading 109

2.7 Risk and performance management: time for the tail to wag the dog? 111
Kelly Lehmann, Stewart Business Software
Performance management 112; Risk management 113; Combining the two approaches: creating P&RM 114; Operational considerations 115; Summary 116

2.8 New horizons for risk and reputation management 118
Chris Woodcock, College Hill
Increasing vulnerability 119; Communications in the spotlight 119; Prevention always better than cure 120; Avoiding scares 121; Transforming defensive effort into a business-shaping asset 122; Practical tips on putting the future into perspective 122; The horizon comes into focus 123

Part 3: Areas of Legal Risk 125

3.1 Litigation risk 127
Rebecca Cushing and Aymen Khoury, Field Fisher Waterhouse LLP
The risk of litigation 128; Litigation preparedness 129; Risks in litigation 129; Conclusion 132

3.2 Fight for the right? 134
Jacqueline Needle, Beck Greener
The cost and frequency of patent litigation 135; Litigation procedures 135; Is the cost of enforcement a reason to avoid protection? 136; Other countries 137; Effective use of IP 139; Avoiding litigation 140

3.3 Risk management – alternative dispute resolution 141
Rebecca Cushing and Olivia Venuto, Field Fisher Waterhouse LLP
What is alternative dispute resolution? 142; What are the most common forms of ADR used by organizations in the UK? 142; Mediation in detail 144; Costs risk in not considering ADR 145; Risk management approach to ADR 146; Notes 146; Reference 147

3.4 Corporate manslaughter: the new landscape 148
Rhys Griffiths, Field Fisher Waterhouse LLP
Introduction 148; Why has the Act been introduced? 149; The new offence of corporate manslaughter 150; Ramifications of the new Act 152; How to prepare for the new Act 152; Reference 153

3.5 Managing litigation risk: lost in translation 155
Sean McGahan, McKinty and Wright
The language of law 156; Compulsive risk assessment psychosis (CRAP1) and conspiratorial risk aversion policy (CRAP2) mistakes to avoid 158; So what should you do? 159

Field Fisher Waterhouse

Field Fisher Waterhouse LLP is a full service European law firm with offices in London, Brussels, Paris and Hamburg and affiliate offices in Italy and Spain. With more than 120 partners and over 220 other lawyers, we assist a wide range of international clients, across the full spectrum of legal issues.

We have high profile Corporate, Dispute Resolution, Finance, IP, Real Estate, Regulatory, and Technology Practices.

“ Field Fisher Waterhouse has a reputation for providing an excellent all-round service to an impressive list of UK and international clients ”

Legal 500, 2008

For further information on what our firm can do for your business please contact Rebecca Cushing at rebecca.cushing@ffw.com or 020 7861 4000.

Belgium France Germany UK

www.ffw.com

Lucidus
Consulting

Making Risk Management
Deliver Business Value

"...because there are
many more things that
might happen than
will happen."

(inspired by Plato 400BC)

apm Accredited

Lucidus Consulting are accredited providers of training for APM Risk Qualifications. For more information on our consulting services, events and publications, visit www.lucidusconsulting.com

To purchase books on Risk Management by Lucidus Managing Partners, visit www.lucidusconsulting.com

"It is no easy task to write a book which is both better than its predecessors and genuinely novel. In both tasks David Hillson and Ruth Murray-Webster have succeeded admirably: this book deserves to become the leader in its field. I truly believe that it is one of the best research books on... project management in recent years."

ISBN: 978-0-566-08798-1

This book makes the link between risk management and decision-making explicit, building on existing work from the economic and risk psychology schools but taking a pragmatic, practitioner-focused approach that is relevant to all decision-making groups in any situation.

ISBN: 13:978-0-566-08787-5

"This practitioners' guide optimises the chance for project success, because it is practical... logical... useable! David and Peter have provided the risk community with a unique, thoughtful approach to risk management."

ISBN: 13:978-1567262025

90 Long Acre | Covent Garden | London WC2E 9RZ | Email: contact@lucidusconsulting.com | Website: www.lucidusconsulting.com

Telephone: London 0207 060 2196 · Manchester 0161 939 0189 | Fax: 0207 060 2198

Supply chain complexities add to the momentum for change

Meanwhile, the global scene is also changing and diversifying fast. The burgeoning complexity of the socio-technical systems in our world has led to a torrential surge in the risks we all face every day, not least in the food and beverage arena. A typical catalyst for this is the increase in 'food miles' over the past half-century – the increased complexity inherent in sourcing food from the other side of the planet, rather than the local farm, has led inevitably to increased risks and tracking prerequisites.

Indeed, it is in the food and drink industry that the multiplication of risks has perhaps been felt most profoundly in the last few years; and various high-profile product recalls and food-related health scares have highlighted the increasingly vital role food scientists and technologists play when it comes to communicating with the public around food safety alerts.

It's a fact that we had a record number of these in the UK and Europe in 2007. In April 2007, the European Commission released its annual report, *Keeping European Consumers Safe*. It outlined some alarming statistics: in the previous year there had been over 1,000 notifications of unsafe products, more than ever before and a third higher than in 2005.

It's no exaggeration to say that communicating risk to public audiences can be a fraught business. If it's a battle between facts and emotions, emotions always win. You may be a technical manager or an operational, process-led person. But always be aware that it is a mistake to base your communications around a hazard or live crisis purely on logic, like statistics, when the emotional aspects of a risk situation can be dominant. This *can* be extremely difficult for scientists to keep front-of-mind or, sometimes, to factor in, given that their professional life demands they mostly deal with hard-and-fast facts.

Logic can falter again when inviting consumers to assess relative risks: repeatedly, research demonstrates that perceived risks from *sensational* events (explosions, aeroplane crashes, tower block fires) are vastly overestimated, while more commonplace risks (heart disease, car accidents, etc) are greatly underestimated. Statistical evidence doesn't persuade the public to hold a different view.

The demand for reporting recalls

Part of the reason for a record number of alerts in Europe and elsewhere in the world, including recalls, is the increased obligation for manufacturer reporting and transparency to protect the public.

RAPEX (Community Rapid Information System) is the European rapid alert system for dangerous consumer products. It ensures that information about dangerous products identified by national authorities is quickly circulated between the national authorities and the European Commission, with the aim of preventing or restricting the supply of these products to consumers. Thirty countries currently participate in the system.

Food or beverage alert checklists for external communications

These are some of the key questions to anticipate and make sure you can answer, bearing in mind the vagaries of risk communication as outlined in this chapter:

1. *Nature of the risk/threat:*
   - Which product/ingredient/flavour(s) is/are affected?
   - What is the problem?
   - How bad could it be?
   - How exactly are they potentially harmful (or to be more specific) to what degree?
   - How do you know?
   - What should someone who has eaten this product/flavour do now?
   - What if the person consumes it regularly?
   - What medical advice should the person seek?
   - How much of it do you have to consume for it to cause a problem?
   - Is there a number that worried customers or consumers can call?
2. *Background facts on the product:*
   - What are the names for these products, and the names by which the consumer would be more familiar with them on-pack?
   - How many batches? How widely is the product/flavour distributed and for how long?
   - Which customers/consumers are affected?
   - Which product brands?
   - Which countries/counties/stores/regions?
   - How many products that are affected have been consumed?
   - How many other products are now having to be recalled from sale or withdrawn from the customer(s)?
   - How do you know that other/similar products don't hold a similar threat?
   - How long will it take to recall all affected products?
   - How have you notified retailers and customers?
   - How can you be confident that you have identified all products affected?
3. *The operational process:*
   - Who's to blame here?
   - When did you discover this problem?
   - How did you discover this problem? (And who did?)
   - How can you have produced a flavour that was toxic/carcinogenic/potentially harmful without realizing it?
   - Surely you test all your products/ingredients/suppliers?
   - How did this one make it through the net?
   - What are you doing about it now?
   - What independent tests or advice is being sought/is available?

The recall is live – so how do you communicate it?

As we all know, even the most robust pre-emptive systems, checks and mitigation plans can't prevent a malicious contamination or the occasional physical hazard. When the worst does happen and it's been agreed that a recall is the most responsible option, having gone through a strategic decision-making checklist, then the operations team will often be drawn into the broader implications and practicalities of how and what to communicate – and when.

There are three steps to deciding how to communicate your recall, always bearing in mind that your primary aim is responsible diligence and care for stakeholders:

1. *Speed: how serious is the hazard posed by the products, and so how quickly do you need to recall them?* These questions will help you decide how to communicate your recall. A phone call is almost immediate, but an ad in a magazine can take up to three months to appear.
2. *Positioning: think of the recall as if it were a marketing exercise.* Ask yourself how you advertised your product in order to sell it in the first place. This may give you some hints on how to target the recall message.
3. *Value for money: how much can you afford to spend?* Designing and printing an in-store notice will not cost much, whereas producing and broadcasting a TV announcement could cost tens of thousands of pounds. Costs will obviously help determine the method you choose, but having recall insurance can increase your choices and allow you to act responsibly to avoid brand damage.

Presentation and style

Your recall message needs to look and/or sound serious. It needs to arrest attention. You'll probably want to present it using your own house style, but it should not look like a regular ad, as this can be confusing. Clarity, simplicity and honesty are crucial to being noticed and acted on. And this in turn will build consumer trust – the cornerstone of repeat business. Don't be tempted to try to water down the reason for the recall for fear of damaging publicity – this lack of openness can be counter-productive, as fewer consumers will respond.

Careful media buying can also help you maximize your resources. If only one region in the country is affected by the recall, notices in the local press instead of national papers will save money and avoid undue alarm.

Contacting identifiable consumers

If you have detailed consumer records, this can be a very successful and cost-effective way of telling them about a recall. Writing to, phoning or e-mailing your consumers is the most precise and responsible way of targeting your recall, and adds a personal touch to the recall programme. You can contact owners of your products using the following methods:

- website special page;
- in-store signage;
- mailshot with voucher and/or direct response mechanic.

Summary

In the 21st century, the risk management role of a technical or operations team in the food industry has become much more complicated. It's also more challenging and demands a wider range of professional skills and interaction with colleagues in other fields of the organization. Not only have the demands of the industry and the regulators multiplied, but the tools to manage the situation are much more sophisticated and the advice available is widespread. Wise managers will recognize the opportunities and avoid the pitfalls. Long gone are the days when hazard analysis critical control points (HACCP), on their own, provided the only required tick in the risk management box.

If a list of drivers like the one outlined in this chapter doesn't prompt a rethink and concerted collaboration, then nothing will. Crises strike at the core of a food or drink brand's intangible and most important asset – its reputation.

At last, the increasing collaboration between the scientists and the communicators is embracing all aspects of reputation management. Paul Slovic (2000), one of the founders of the psychological study of risk perception, summarizes the need for combining logical and emotional assessment perfectly:

> Many technologists believe that public perceptions of risk are irrational… psychometric research demonstrates that, whereas experts define risk in a narrow, technical way, the public has a richer, more complex view that incorporates value-laden considerations such as equity, catastrophic potential, and controllability. The issue is not whether these are legitimate, rational considerations, but how to integrate them into risk analysis and policy decisions.

Note

1. Campden BRI is the world's largest independent membership-based organization carrying out R&D for the food and drink industry worldwide. Contact Dr Mike Stringer, Director of Food Technology (tel: 0044 (0)1386 842 003).

Reference

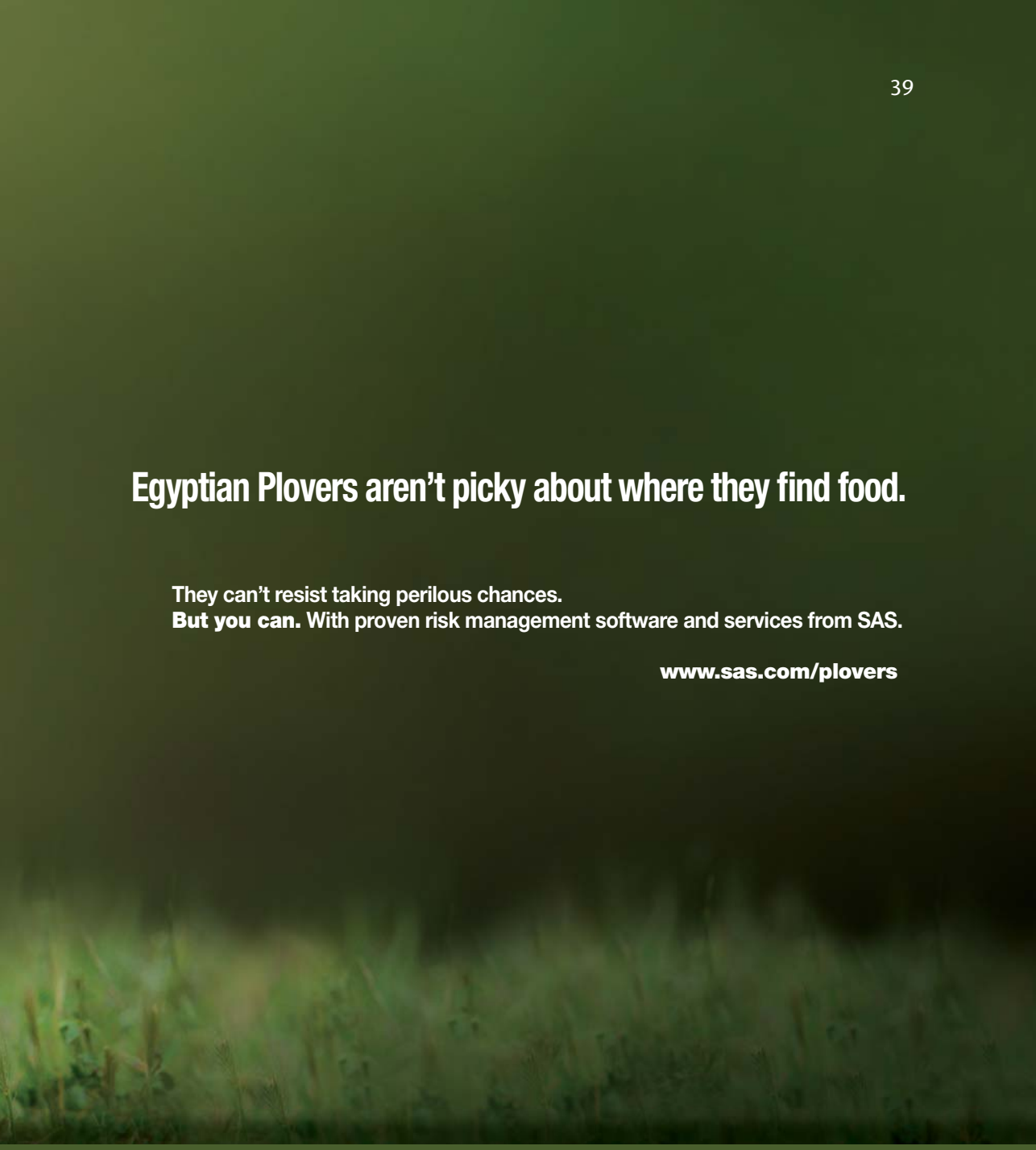
Slovic, Paul (2000) *The Perception of Risk*, p 150, Earthscan, London

SAS SOFTWARE HELPS COMPANIES ACROSS EVERY INDUSTRY DISCOVER INNOVAT

SAS® for Enterprise Risk Management

Visit www.sas.com/plovers for a free ***white paper***

- Compliance
- Credit risk and scoring
- Fraud detection and prevention
- Market risk
- Operational risk
- Risk-based performance management



SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries.
® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2008 SAS Institute Inc. All rights reserved. 500558US.1008

1.5

Enterprise risk management solutions

Austin Trippensee, SAS Institute Inc

This chapter will discuss the challenges banks face in integrating market, credit and operational risk measures. It will cover the design of a data model for the front end of your analytics, and will cover how a robustly designed repository for your output supports a robust business intelligence infrastructure. In the middle, users might want to configure proprietary measures. This chapter will also address key issues around flexibility, auditability and scalability.

Introduction

Today, banks are facing more regulatory requirements, more stringent rating agency oversight, and investor confidence issues. To meet these new challenges, many organizations are examining their policies, methodologies and infrastructure (PMI). These three building blocks form the core of any enterprise risk management environment (Crouhy, Galai and Mark, 2005).

Policies define the tolerance that an organization has for risk. The policies should be consistent with business strategy and should be communicated both internally and externally. The methodologies are the underlying mathematical models that are tied back into performance management. These models must be

properly designed, implemented and vetted. The infrastructure refers to having the appropriate people and operational processes (such as data, software, systems, etc) in place to control and report on the risks (Crouhy, Galai and Mark, 2005).

In the past 10 years, there have been countless books, journal articles and other

1.7

Different views, the same risks: representing uncertainty, assumptions and perspective

Allan Robinson and Bob Hide, UMU, Appleyards

Introduction: uncertainty or risk?

Increasingly, the word 'uncertainty' is being used in place of 'risk'. Many of the definitions of 'risk' found in risk management guidelines and standards are of the type: 'risks may represent threats as well as opportunities'. Alternatively, there are processes that deal with risks and opportunities, the two being treated as separate and distinct. This stylized representation of uncertainty limits the way risk managers record, analyse and assess risks, and constrains the relationship between the risk management process and that to which it is being applied.

Risks (and opportunities) are defined in relation to what we will call the 'base position' (cost estimate, project schedule, operational process, etc). However, how do we tell if that base position was optimistic or pessimistic, realistic or fantastic?

The answer is: we cannot, except by inference from the level of assessed risk exposure. From a strategic perspective, it is hard to understand what the results of a risk management process are telling us. Is a given project really extremely risky, or is it merely that the base cost estimate was extremely optimistic?

This issue, which relates to the context in which any risk management process is implemented, is typically dealt with through phrases like 'following good industry practice', 'benchmarking', etc, to give credibility and confidence in the base position. However, since each project is unique, and given that the same set of risks can be and are looked at from different perspectives (eg a client organization issuing a tender as against bidders competing for the work), how can we compare the risks identified by each party without understanding how optimistic or pessimistic each base position is from a strategic perspective?

Can a senior decision maker be confident that the risk management process takes the optimism or pessimism of the base position into account, particularly if the personnel taking part in the risk management process are not aware of that information themselves?

It is apparent, therefore, that many current risk management standards and processes are not sufficiently sophisticated to address the complexities, nuances and additional dimensions of uncertainty.

What is uncertainty?

Uncertainty surrounds everything, past, present and future. It represents both the limits of our knowledge of the present and our ability to predict and forecast future events. When seeking to understand uncertainty, the first and most important point is to understand from what perspective we are looking.

For example, I am trying to catch a train in the morning to go into work. I know that over the last two years it has taken me, on average, 15 minutes to drive to the train station, excluding the time it takes to walk from house to car and from car to station platform. If I plan my journey on the basis that this morning it will take only 10 minutes to drive to the station, then experience suggests that I am being highly optimistic and am likely to be disappointed. If, on the other hand, I allow 30 minutes for the car journey, then experience suggests I am being highly conservative and am likely to arrive in plenty of time (and will probably spend several minutes waiting for the train to arrive). This demonstrates that it is only possible to assess the likelihood and impact of risks in the context of the planned activity.

However, as this planned activity lies in the future, the plan also represents a whole suite of assumptions about what the future will be. Therefore, another way of looking at the process of managing uncertainty is that we are actually managing our assumptions and seeking to understand the uncertainty around them.

Assumptions and uncertainty

Any uncertainty management process is simply one of understanding the robustness of the assumptions we are making about the future. Each assumption

we make, whether explicit or implicit, also represents a risk – the risk that the assumption will prove to be incorrect. If our assumption proves to be incorrect, then understanding the impact of this failure in our assumption(s) is essential. Since we do not know which of our assumptions will fail, an uncertainty management process must consider the consequences associated with each assumption failing. This highlights that the true purpose of any uncertainty management process is to help decision makers understand the robustness and consequences of their decisions.

Figure 1.7.1 shows a graphical representation of how uncertainty relates to assumptions, and what those assumptions mean.

We can separate assumptions into three categories: contextual, normal and critical.

Contextual

These are the assumptions that form the context for the plan. For example, in the context of driving to the train station a contextual assumption is that I am going to drive to the train station, as opposed to working from home, ordering a taxi or getting a lift from someone. The important point about these assumptions is that they are believed (by the decision maker) to be: robust, where the assumption is unlikely to change; and valid, where the assumption is based around the best available information. In the context of a project, a contextual assumption represents the base plan, cost estimate or scope.

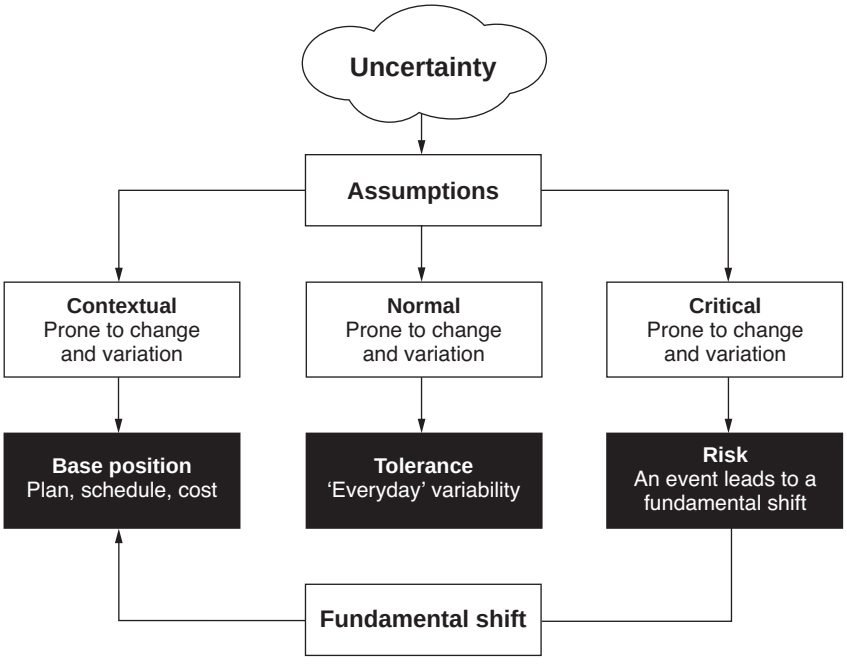


Figure 1.7.1 Relationship between uncertainty, assumptions and risk

Normal

If contextual assumptions represent the 'cast in stone' beliefs, of the 'if this changes then we're not talking about the same project' type of assumptions, then normal assumptions represent the 'usual' sort of variability, which does not require senior management involvement (in this case senior management involvement might be thought of as applying to any management actions that might require approval, support, information or assistance from a more senior level than the decision maker). In the context of driving to work, it represents me following the usual process for travelling to the train station, without the need to take exceptional or unusual action. In the context of a project, 'normal' assumptions represent those behind a particular value – they will often be evidenced based (though quite possibly subjective rather than objective evidence, eg the statement 'For years it has taken me, on average [being deliberately vague here] 15 minutes to drive to the train station' is subjective, but *may* be viewed as reliable given that I am the decision maker and I am trying to manage the uncertainty around my journey).

These assumptions therefore represent the 'normal' range of variability around a project or process. In terms of a 'heat' diagram, they represent the high-frequency, low-impact types of variability that are often not worth managing.

Critical

Critical assumptions are the opposite of contextual assumptions. These assumptions are prone to change and variation and/or have a significant impact upon the objectives of the activity or project. Critical assumptions represent the low-frequency, high-impact risks in the heat diagram, the unusual events that are outside of the norm.

Case study 1: Risks, assumptions and subjectivity

If all assumptions may lead to risks, then it follows that any uncertainty management process that hopes to be complete will have to take account of those assumptions within the process.

On a complex infrastructure programme, this led us to introduce assumptions dictionaries as a means of keeping track of all the various assumptions being made by different parts of the organization. Each of these assumptions presented a potential uncertainty, and there was also the possibility of different parts of the organization making conflicting or contradictory assumptions.

As we implemented these assumptions dictionaries, we were faced with questions as to what information needed to be included and, fundamentally, what an assumption is.

The *Chambers English Dictionary* definition is: 'that which is taken for granted or supposed'. For our purposes, we defined assumptions as the subjective beliefs, both explicit and implicit, of an individual or team about the future within a particular context. This highlights our belief that all information within the uncertainty management process is fundamentally subjective – even if a large amount of objective data is available around an area of uncertainty, the use of the data to inform (either statistically or otherwise) our view of the future is based on the often implicit assumption that the future will be the same as the past.

Recent events both in the environment (climate change) and in the financial services industry (credit crunch) demonstrate that the reason uncertainty management is important is because the future is not the same as the past.

In the context of driving to the train station, a critical assumption would be 'I assume that my car won't break down.' This sounds like a reasonable statement, but is it? On what basis can it be assumed to be 'reasonable', what information is required to provide confidence in that statement, and *what level of confidence does the decision maker require*?

Uncertainty management

The distinction between 'normal' and 'critical' assumptions – a continuum of uncertainty

There is no fixed boundary between normal and critical assumptions, ie normality or criticality is a function of the assumption(s) being made. It is also a function of the objectives and the overall context.

An assumptions management process

Given the relativity of assumptions, and their inherently subjective nature, it becomes apparent that a robust process for reviewing them is needed (Figure 1.7.2). As with most risk management processes, this process needs to be iterative, as assumptions will be changing and being modified as time passes, more information becomes available and attitudes (optimism or pessimism) change.

Uncertainty analysis

Once we have a clear understanding of the assumptions that we are making, we can then begin to assess the uncertainty surrounding those assumptions. As with the quantification of risk (cf PRAM, 2nd edition), this becomes the likelihood that the assumption is correct, and the impact on the objectives of the project, process or activity should the assumption prove incorrect.

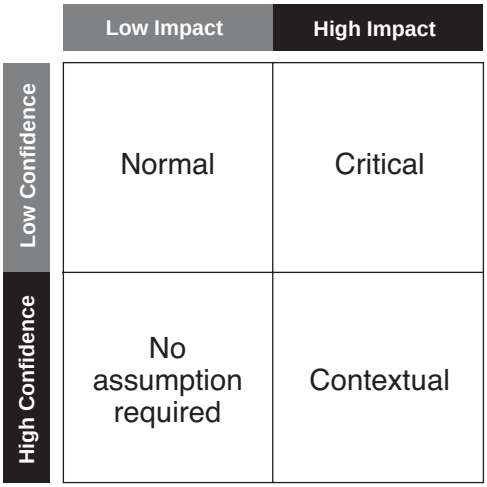


Figure 1.7.2 Assumptions analysis process

Case study 2: The limits of knowledge (or risk and quantum physics)

For a major metropolitan transport organization, one of the key issues faced is: what is the condition of our physical infrastructure assets? Where detailed information on the condition of an asset is not available, assumptions have to be made to allow the normal business processes to proceed:

> Asset A is of unknown condition. Asset B is known to be at condition X, and is of similar age and type to Asset A. Therefore, we can assume that Asset A is also of condition X, and will require work Y to be done at time Z.
>
> However, when Asset A is actually investigated, it may turn out to be in a very different condition to that assumed.

All of this is very similar to the principles of quantum physics. Schrödinger's cat faces the risk of being poisoned, with a certain probability (unknown) and impact (death of the cat). Even though the condition of the cat is decided in advance of the box being opened, our uncertainty regarding the risk cannot be resolved until the box is opened.

This reveals that the key point in time for any uncertainty and its associated assumptions is the point at which the uncertainty materializes, when we open the lid of the box to see if the cat is alive or dead.

For example:

> *Assumption 1*: The drive to the station takes 15 minutes. Well, it is actually extremely unlikely that: 1) the car journey will take exactly 15 minutes and 2) the average car journey to the station is 15 minutes.
>
> Given that this quantification (of 15 minutes) is based on my subjective judgement of what a reasonable time for that journey should be, we might say that it is 100 per cent likely that the time taken to drive to the station will be somewhere between 12 and 20 minutes, though it is most likely that it will take 15 minutes.

> *Assumption 2*: My car will not break down. The car I currently own has never broken down. However, in my experience of car ownership (let's call it 20 years) I have had two breakdowns and two accidents. So let's say there's a 4 in 4,000 (20 years × 200 driving days), or 0.1 per cent, chance of a breakdown on a given day, with the result that my journey to the station takes between two and four hours.

The first example represents a 'normal' assumption. There is some inherent variability in it (probably owing to some further unidentified assumptions – like which route I take), which is hard to manage successfully. The second example represents a 'critical' assumption. If my car breaks down it will have a significant impact on my journey. It is much easier to manage (eg have the car serviced regularly), but cannot be completely avoided even when mitigated.

From a risk management perspective, we are assessing the risk that the assumptions we are making are not in fact true.

Case study 3: How realistic is an estimate (and why are they almost always wrong)?

When quantifying the risk associated with a major PPP contract, we initially faced a challenge in understanding how realistic the base costs were. This was complicated by the fact that, owing to the scale, scope and duration of the contract, several different firms had contributed estimates for different parts of the contract.

This is a general problem: all estimates created for a business may be expected to use realistic values. Professional staff following good industry practice, taking a view on the appropriate industry benchmarks, will produce a realistic estimate. The issue for risk managers is to understand what, if any, contingency has been included within the estimate.

This leads to the question: how realistic is 'realistic'? The first step on the way to understanding how realistic was 'realistic' was to replace the single values in the estimates with 'triple-points'. The three values represent the minimum value, the most likely value and the maximum value that may be expected to occur in 'normal' circumstances. The most likely value should represent the value that would otherwise have been

used. The minimum and maximum represent the limits of normal variability, excluding the effect of any risks (or opportunities).

So why are estimates always wrong? Unless the 'triple-point' is symmetrical, the minimum being as far below the most likely as the maximum is above it, then the mean or average value will not be the same as the most likely (Figure 1.7.3).

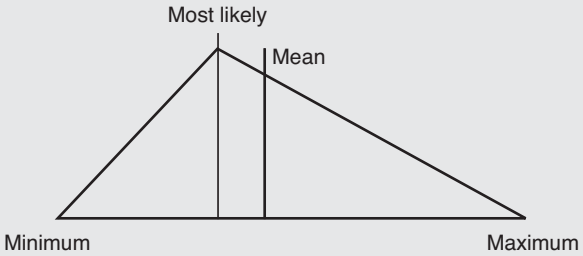


Figure 1.7.3 Relationship between mean and most likely for an asymmetrical triple-point estimate

Optimistic or pessimistic? Why not realistic?

Having assessed all the assumptions relative to our base position we are now able to assess whether, in our view, our base position was optimistic or pessimistic and, if appropriate, to adjust it to make it more realistic. However, it is quite possible that in certain circumstances an organization will choose to take an optimistic or pessimistic view, as that aligns better with the organizational objectives.

Summary

The future is uncertain, and by default we make assumptions about how the future will turn out. By examining, testing and reviewing these assumptions we:

- make the assumptions explicit, thus enabling us to ascertain whether we think they are realistic;
- are enabled to understand whether our base position is optimistic, pessimistic or realistic, and whether this is appropriate;
- are provided with a way to integrate risk management and risk analysis explicitly with the base position (or rather the assumptions behind the base position).

2

Corporate Risk Concerns

THIS PAGE IS INTENTIONALLY LEFT BLANK

2.1

Reputation: the all-defining asset

Aymen Khoury, Field Fisher Waterhouse LLP

It is widely accepted that a reputation can take a lifetime to build and a moment to tarnish, sometimes irreparably. Reputation has been described as being the culmination of many good things lost in one bad deed. But a reputation remains an intangible asset, almost impossible to quantify. It can be a nebulous concept, even more difficult to value than other intangible assets such as the knowledge or experience of employees.

Preserving and enhancing reputation are becoming increasingly difficult tasks for businesses. The very technology that once gave them a competitive edge can now be used against them. Customers and employees are more sophisticated, more discerning and more readily prepared to mobilize. Legal and regulatory developments have become a more burdensome reality to test even the most unshakable of reputations. What is clear however is that reputation is often the primary indicator of every other risk a business faces. Ultimately, it is the sum of all parts.

What is reputation risk?

Reputation can be an elusive concept, difficult to define. It means different things to different people. If it is defined as what people think of you; it is therefore a

subjective concept. The same company can have contradictory reputations depending on the age, culture and location of the minds in which it exists. The context is all defining. Perception is king. Whether that perception is grounded in fact is sometimes irrelevant. No wonder then that one can find an array of definitions for reputation risk.

Despite the ambiguities, however, risk to reputation is real. If one accepts the wisdom that reputation is ultimately amassed through the culmination of a number of deeds, then reputation risk is surely the threat to all that has been built up over the years: the collection of past actions, performance, customer base, brand association and revenue.

The importance of reputation

Protecting reputations has often been an expensive and controversial affair. In law, for example, defamation cases remain among the few civil actions that include jury deliberations and often involve an award of damages unequalled in other forms of litigation. Such is the importance placed on guarding reputations.

All people are susceptible to having their reputation damaged. In 2005, Nelson Mandela learned this when his former confidant Ismail Ayob was accused of faking and selling Mandela's artwork for considerable sums of money. Mandela filed papers in the Johannesburg High Court, but not without having his reputation damaged.

Similarly, no business is beyond having its reputation damaged. Marks & Spencer experienced this when its clothing line was considered to be out of touch with what the public expected. As with Mandela, it was M&S's strong long-standing reputation that allowed it to weather the storm and, paradoxically, shape a new one. The stakeholders (the customers, suppliers, shareholders and employees) retained a perception of M&S that bought the company time while it pursued a new direction, all the while relying on the unfaltering reputation of its food operation. In gaming terms, it had credits it was able to cash in. The key to emerging from a crisis will often depend on the degree of trust the public has for the business.

But M&S did not escape without considerable loss. The bottom line was hit and hit hard. This is the value of reputation. It can have an impact on every facet of the business and goes to the heart of its capability to generate future wealth. Reputation attracts (or repels) investors, talented employees, customers, suppliers, distributors and sponsors. Further, it has such force that it can determine the outlook of regulators and activists alike (think credits again). Ask yourself whether or not claims are easier to make against companies with poor reputations. In short, a healthy reputation determines the future capability of the business; it gives it a considerable competitive edge.

Threats to reputation

The practice of business is rapidly changing. Greater legal and regulatory intrusion is just one area to which reputations are increasingly vulnerable. In the wake of the more sophisticated threats to reputation, however, a failure to meet

the regulatory standard is likely quickly to become an exaggerated deficiency. Compliance with environmental, financial, employment or health and safety regulations gives the official green light for the company to function and ensures that action against its officers and directors is prevented. Thus compliance is the minimum expected by stakeholders, even though it achieves little more than a neutral impact on the reputation of the business. Conversely, companies faced with public regulatory investigations or litigation invariably suffer damage to their reputations, irrespective of their liability in the case. The notion of there being no smoke without a fire weighs heavily in the public's mind.

Yet threats faced by businesses are considerably greater than the 'traditional' risks to reputation. Increasingly, companies find themselves particularly vulnerable to the effect the media and internet are having on the dissemination of information. The 24-hour real-time transmission of information from 'official' channels can be intrusive enough. But businesses are now having to contend with internet chat rooms, message posting and social networking sites that can do more than cybersmear, which can often be damaging enough. The internet is a primary tool utilized by campaigners and activists, which businesses will find themselves increasingly vulnerable to, since it has the ability to mobilize like-minded individuals in relatively short periods of time. HSBC experienced the power of students using Facebook in the aftermath of its decision to scrap interest-free accounts, promptly forcing a U-turn by the bank.

The ease by which information is accessible means that it is more likely, if not guaranteed, that embarrassing associations will be revealed sooner or later. The Bank of Scotland's joint venture with American evangelist Pat Robertson in 1999, to launch a telephone and banking internet arm, proved disastrous when he characterized Scotland as a 'rather dark land' that was too tolerant of gay people. The backlash, which included commercial and private client customers closing their accounts with the bank, was swift and furious.

Evidently, the risk to reputation predominantly relates to matters in the public domain. Yet there can be a distinct lack of awareness in businesses over what is in the public domain. This may be the consequence of an assumption by business leaders that external elements pose the greatest risk to reputations, whereas in fact internal elements, particularly employees, are often most destructive. Think Barings Bank and, more recently, Soc Gen.

Yet the threats are not always as extreme as a wholesale abandonment of major rules and regulations. Smaller, more publicly visible performance (or lack of it) can have detrimental effects on business reputation, particularly if that behaviour goes to the heart of what the business does. According to the RAC's 20th annual *Report on Motoring*, the behaviour (or misbehaviour) of fleet drivers is increasingly affecting the reputation of the companies that employ them. The report called for better training of drivers, which it suggested was needed to ensure that courtesy and respect are instilled as part of the company culture from the outset. The logic is persuasive. If perception is reality, then there can be no disparity between the internal and external dynamics of a company if a healthy reputation is to be projected. A good rule of thumb is to proceed as if everything that is said and done by the business is in public.

Reputation dilemmas

Managing reputation risk is unquestionably a challenge. The difficulties of quantifying the risks of an intangible asset are obvious. Businesses, however, should be able to prepare for threats that are foreseeable. For example, aviation companies know that the biggest catastrophe they face is when an accident happens. Air France's response to one of its Airbuses crashing at an airport in Toronto in August 2005 was swift and open. As well as quickly controlling the incident itself, the airline's immediate and frank communication with the media meant it could not be accused of attempting to mitigate the damage by covering it up.

The attractions of not disclosing the full extent of a blunder are obvious. But such temptations can be disastrous. Coca-Cola and its ill-fated tap water venture, and Perrier's benzene contamination scare are probably better remembered because of the mismanagement of the crises that followed than because of the incidents themselves. Public perceptions of cover-ups are undesirable. On the other end of the spectrum is the Tylenol cyanide contamination scare in 1982, which may not be as easily remembered. This is in large part due to the effective crisis management undertaken by Johnson & Johnson, which included advertisements of the contamination in newspapers and the establishment of free telephone helplines. The incident clearly demonstrated that the extent of damage caused by a crisis is often determined by the management of the crisis that follows.

Companies clearly face a dilemma. The choice that needs to be made is often a trade-off between taking the hit to reputation in the short term to preserve the long-term reputation and possibly even survival of the business. But this extends beyond managing an immediate crisis. It can have considerable implications on the long-term strategy of the company. Classic examples are brewers and distillers of alcoholic drinks – patently aware of the need to manage their reputations – that place warnings to drink responsibly in their advertisements. Such expressions of concern extend beyond regulatory compliance. In fact, logic would dictate that asking people to drink less goes contrary to increasing turnover in the short term at least. Yet such companies are keen to project a responsible image in order to enhance their reputations and thereby ensure long-term profitability.

The contradiction can sometimes be more troublesome for companies. Burberry's reputation was tarnished by its association with 'chav' culture. While short-term sales were on the increase, newly (and inadvertently) found fans of the brand's signature check did little for its reputation as a luxury brand. The company's fears caused it to pull a number of its lines. This was a classic example of trading short-term profits to preserve long-term reputation. Similarly, Stella Artois has experienced difficulties in maintaining its self-styled 'reassuringly expensive' slogan while it was continually associated with violent behaviour that even caused the term 'Stella Defence' at law. For the company, the ability to rely on the Artois brand alone to create a separate portfolio of beers to shake off its downmarket association provides a vehicle for maintaining a certain quality to its product.

Companies are increasingly adopting sophisticated long-term policies to help enhance their reputations. Petroleum companies have gone out of their way to project an image that they invest in environmentally sustainable energies. In 2005,

BP launched BP Alternative Energy, a business unit that manages BP's investments in solar, wind, hydrogen and combined-cycle-gas-turbine power generation, at the time said to amount to up to $8 billion investment over the decade to come. Such initiatives are as much about public perception as economic sustainability. They are associated with the increased expectations of stakeholders. The shareholders may be primarily concerned with profits, but ensuring this in the long term requires a more rounded strategy. In this regard, the ethical dimension cannot be overstated. A sustainable reputation more often than not demands a show of accountability. Being seen to be responsible is just as important as being responsible.

The role of ethical policy is illustrated by the emphasis that sectors less traditionally concerned with such matters are now starting to give it. Despite the controversial shutdown by the government of the Serious Fraud Office investigation into the al-Yamamah contract with Saudi Arabia, BAE Systems was forced to admit damaging ethical lapses amid allegations of bribery and corruption. Yet, rather than close ranks, the company commissioned a report by Lord Woolf on its ethical practices. Such concern seemed to be at odds with the traditional views associated with arms trading. But BAE was fully conscious of the blow its reputation had taken. While ensuring that the report did not enquire into previous contracts entered into by the company, the report allowed the company to project the image that it was getting its house in order. It was also a clear acknowledgement that the company's reputation needed addressing as part of its long-term operation. Lord Woolf himself remarked, 'BAE can either become an ethical company that refuses to get involved in some contracts; or it does not and risks long-term reputational damage.'

The requirement to show a commitment to an ethical policy reflects the increasingly transparent environment that businesses find themselves operating in. Corporate social responsibility (CSR) initiatives are now expected to be part of the operation of most well-organized and forward-thinking companies. Such programmes can have an effect on the morale and emotion of stakeholders, employees and customers alike. Ultimately, however, they are public relations exercises that do wonders for the reputation of the businesses.

Conclusion

An old Chinese proverb says 'Don't consider your reputation and you may do anything you like.' Attractive as this notion sounds, this is simply unthinkable for businesses today, even those that may seem to have less concern for needing to project a healthy, ethical image. Traditionally, business reputations have been defined by what product or service they deliver to the public. More recently, reputations are shaped by the ability of companies to assimilate social, ethical and economic aspects into a profit-making operation. The reality is that practically everything a business says, does or is can make or break its reputation.

2.2

Reputational risk – king risk

Mark Elkins, SAS UK

> Glass, china and reputation are easily cracked, and never mended well.
>
> Benjamin Franklin

Is reputation risk a risk in itself or is it the consequence of other risk? According to an Economist Intelligence Unit (EIU) report in 2005 called *Reputation: Risk of Risks*, 52 per cent of survey respondents considered reputation risk as a risk in itself, while 40 per cent considered it a consequence of other risks. However, the report suggests there is a difference in views between corporate entities and financial services companies as to the relative importance. For the former, reputation risk is considered a risk in itself, whereas the latter consider it a second-tier risk. Furthermore, a 2008 EIU report called *The Bigger Picture: Embracing Enterprise Risk Management* highlighted that trust in financial services firms has been eroded owing to the credit crisis, resulting in reputational risk becoming more important now than ever before. In this latest EIU survey, 62 per cent of respondents say that protection against loss and damage to reputation is one of the most important benefits of an ERM strategy.

During the course of this chapter we will look at reputation risk, in itself an umbrella of risk, since any breach in operational, credit or market risk can directly

affect a company's reputation. Clearly, some risks have a greater effect on reputation than others, and these will be identified. The calculation of value at risk (VaR) will be explored, alongside various approaches that could be taken in expressing the cost that could be incurred by a particular risk were it to transpire. Finally the chapter will cover strategies and mitigation actions that have been used by financial services companies when an adverse event has taken its toll on their reputations.

Reputation matters

Of course reputation matters; but what is reputation? It is not a thing, and it is not tangible. It is about the way in which any organization is perceived internally and externally by customers, shareholders and peers. It is about its credibility as an organization and its performance – both fiscal and operational. It's about its values, culture, beliefs and interaction with society at large. Reputation is massive. A good reputation leads to recommendation and, as any marketer will tell you, that is the best method of marketing. It means a premium can be charged for goods and services. Higher margins can be achieved, as customers believe they are with a sound company.

In the financial services world, reputation is highly important. The relationship between customer and institution is based on trust, after all. Consider Northern Rock. The company raised capital on the financial markets to then lend on to home buyers, secured on existing books of business. In the United States it became evident that sub-prime books were not performing. Consumers and corporates in the United States were finding difficulty in meeting their financial commitments. The financial markets started to shut up shop, effectively not buying books or lending money to other financial institutions. Since Northern Rock was dependent on the markets for its capital to lend, it was perceived as being in trouble. Once news was leaked that it was unable to lend, the perception of the public was that it was in trouble. Its reputation plummeted. The dribble of savers withdrawing money from their accounts became a torrent, and queues formed outside Northern Rock branches up and down the country as depositors withdrew their savings. They no longer trusted the company.

Was it necessary? Was the bank really going to the wall? The bank certainly suffered as a result. The CEO left the company, the share price drastically reduced, and the bank was nationalized after protracted negotiations with potential suitors fell through.

The trouble with a bad reputation is that it rubs off on others. The Financial Services Authority (FSA) was criticized for failing to be vigilant in its supervision of the bank. Others in the sector watched their share price drop, though not so dramatically, as investors started to have concerns over the banking sector and its exposure to bad debt. Reputation clearly matters to the public, and a bad reputation sticks.

The most infamous loss of reputation occurred with the collapse of Barings Bank. Nick Leeson's actions and the bank's lack of supervision over its Singapore-based trader resulted in the bank being famously sold for £1. Both Barings and

Northern Rock could have avoided their predicaments had they put in force adequate risk procedures. In the case of Barings, it would have been operational risk systems and processes, and rigorous supervision of the processes. For Northern Rock the approach would have been stress testing and the assessment of different market conditions that could occur and being prepared with contingency plans for different scenarios.

A good reputation has benefits

As Warren Buffett so eloquently put it, 'It takes 20 years to build a reputation and five minutes to destroy it.' There are sound reasons why companies want a good reputation:

- It makes it easier for them to recruit and retain employees.
- It differentiates them in largely commoditized markets.
- It allows them to charge a premium for their goods and services, on the basis that they are known in the market for meeting customer expectations.
- It attracts investors, who see the company as low-risk, increasing share price, shareholder value and market capitalization.
- It increases the ability to raise funds on the capital markets.
- It can give them a competitive advantage, and create a barrier to market entry.
- It can soften the scrutiny of the regulators, who trust companies with a good reputation more than those without.
- In crisis mode, investors tend to give companies with a good reputation the benefit of the doubt.

However, once a good, or even an excellent, reputation has been earned, companies cannot afford to rest on their laurels. They need to ensure that their reputation at minimum is maintained, if not further enhanced. To do this they need to monitor their environment and swiftly and appropriately react to any changes in the perception of the company. Monitoring of websites, chat forums, blogs and the press, and canvassing opinion from customers and suppliers are ways by which reputation can be monitored. Additionally, companies need to promote any initiatives, performance enhancements, products, etc that could add to a positive reputation.

Bad reputation – the only way is up

Of course, the only positive to having a bad reputation is that there is only one way to go, and that's up! The following factors are indicative of a bad reputation:

- high employee turnover;
- reduction in market share;
- poor reports in the media;
- fall in customer retention;

- falling share price if publicly quoted;
- restricted financing ability as rating agencies downgrade.

This is not by any means a comprehensive list of negative associations of having a bad reputation, but clearly these issues do need to be addressed if a company wishes to remain in business.

Measuring reputational risk

Research has revealed that the amount of value attributable to an organization's reputation can run to billions of US dollars, and can represent between 40 and 70 per cent of market capitalization (Table 2.2.1).

Table 2.2.1 Value attributable to reputation

Bank	*Absolute loss (US$ billion)*	*Loss in market capitalization (%)*
Citigroup	–212.3	–70.0
UBS	–141.5	–71.4
RBS	–129.8	–65.7
AIG	–124.1	–64.1
Bank of America	–94.2	–39.1
HBoS	–91.0	–75.1
Wachovia	–89.6	–70.6
Soc Gen	–81.5	–59.6
Unicredit	–79.7	–19.9
Fortis	–75.2	–69.3
Barclays	–68.1	–56.1
Crédit Agricole	–59.9	–55.6
AXA	–50.3	–45.1
Allianz (Dresdner)	–49.0	–39.0
Deutsche Bank	–48.5	–49.7
BBVA	–48.2	–41.1
Intessa San Paulo	–47.8	–41.7
Credit Suisse	–46.6	–44.5
ING	–44.4	–39.4
JP Morgan	–43.7	–23.6
BNP Paribas	–43.0	–32.3
Lloyds TSB	–35.9	–51.9
Natbas	–34.6	–77.0
Sberbank	–31.1	–32.6
HSBC	–29.7	–13.0
Dexia	–29.0	–64.7

Source: Financial services market data, January 2007 to present.

Consider the 'credit crunch' and the effect it has had on the reputation of the banks, for example. Announcements of large bad debt write-offs, of increased impairment and arrears on loan portfolios have been well reported. Shareholder confidence has waned, reflected in the dramatic fall in share price and subsequent downslide in market capitalization. The reputation of the banks has been tarnished. They are being criticized in the media for adopting lending criteria that are too lax, and not being prudent As a result they have tightened their underwriting to such an extent that it is extremely difficult to obtain a loan. However, nobody questioned their underwriting policies at the time. Just how long will it take for their reputations to be restored?

The Intangible Asset Finance Society proposes that reputation capital (reputation value) is the sum of the value of all corporate intangible assets. Intangible assets include business processes (such as credit underwriting – see above), patents, trademarks, reputations for ethics and integrity, and quality, safety, sustainability, security and resilience. This is far-reaching in its scope and does have merit, although calculating the value of some business processes could prove challenging.

Financial institutions must start to incorporate this risk in their loss assessment surveys of the business. The risk will need to be assessed and modelled alongside other strategic operational risks. Issue and management mitigating plans and actions will need to be raised against the loss assessments to ensure the potential loss events are minimized, with a goal of zero tolerance. Advanced analytics can be used to quantify and model these risks. In particular, with the less likely events and risks, different risk modelling approaches can be used at different levels of the risk distribution curve depending upon their likelihood, frequency and financial impact. For example, for long-tail events, scenario-type analysis such as Monte Carlo simulation approaches may well be appropriate where a history of such events is not well defined.

Reputational risk – capital quantification

Looking at the benefits of having a good reputation and the drawbacks from having a bad one, there are quantifiable factors that could, through financial modelling, provide a financial number that can be aggregated to value the worth of reputation (Table 2.2.2).

The complexity of reputation modelling is increased with a further variance: where the event originated and what type of damaging event it was. Different shocks or events will have more or less impact on reputation. Severity of capital loss is dependent upon the relative value placed upon the event by stakeholders. For example, the impact on reputation of a server outage for an ATM at a bank may be less than for a breach of security on a bank's online banking facility that compromises confidential customer information!

Table 2.2.2 Valuing the worth of reputation

A good reputation…	*Metric*
… makes it easier to recruit and retain employees.	What is the cost of recruiting an employee (time, resource, recruitment fees)? What has historically happened to employee numbers when a previous piece of bad news leaked? (%) In staff surveys, is there a correlation between number of responses or level of employee satisfaction and the number of leavers?
…differentiates in a largely commoditized market.	How much of a market share lead does the company have over the competition? What is the value of that lead in economic terms? How much of that lead is down to the reputation or quality of the product or service?
… enables the charging of a premium for goods and services, on the basis that the company is known in the market for meeting customer expectations.	How much additional margin is made above the competition, and what is the unit value of that margin? What has been the effect of a piece of bad news on the company, or competitor, or sales? Have sales fallen? How much? What was the revenue impact?
… attracts investors, who see the company as low-risk, increasing the share price.	What has been the effect in the past of reputation-harming news on share price, shareholder value and market capitalization? What is the value attached?
… increases the ability to raise funds on the capital markets.	What would the impact be on the credit rating of a particular risk factor breach? What would that impact cost the company?
… can give a competitive advantage, and create a barrier to market entry.	What would the effect be of a new competitor in the market?
… can soften the scrutiny of the regulators, who trust companies with a good reputation more than those without.	What are the fines imposed by the regulators? What has happened to competitors when a compliance breach goes public? Declining share price and market capitalization? Outflow of customers? How long has that lasted for and at what cost in lost sales?

Table 2.2.2 Continued

A good reputation…	*Metric*
	What is the cost of rectifying the compliance breach? How much cost is involved in spending increased time with the regulators?
… means that, when the company is in crisis mode, investors tend to give it the benefit of the doubt.	But what's the PR cost of a crisis management agency?

Managing reputation

So, having identified what factors influence the reputation of a company, it's now a question of managing those risk factors. Prevention is better than cure, so, for example, ensuring quality is maintained in manufacturing by putting in place best-practice processes and procedures can protect the reputation of a company. It's a preventative activity, and if and when the risk factor has 'exploded' into the public domain it becomes a PR crisis management activity.

The severity of the impact on the value of reputation can be predicted, however, through the use of analytics and modelling, followed by an appropriate PR strategy to mitigate the impact.

Figure 2.2.1 does not address all the risk factors; others should also be taken into consideration. But how companies can address each of these factors can be by way of a process, and a particular process can be valued in its contribution to the reputation capital of the company. Effectively this is giving a value to the cost of conformance to a particular recognized best practice and predicting the impact, based on one's own as well as others' experience, of the cost of non-conformance – performing below par.

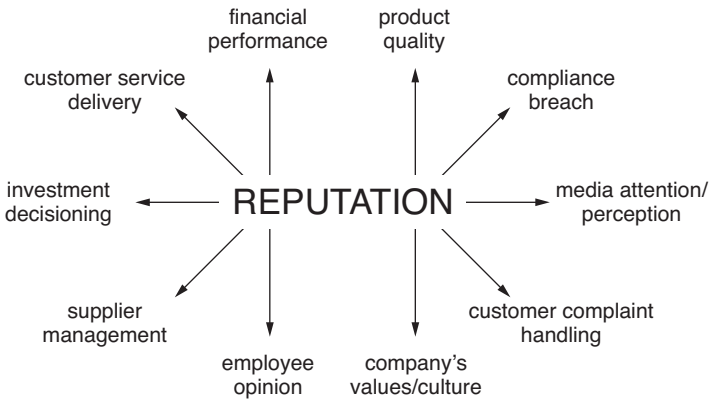


Figure 2.2.1 Influences on corporate reputation

In conclusion

The value of the impact on the reputation capital of a particular event can be modelled based upon one's own and competitive organizations' historical experience. This enables predictive analytics to assess and identify key risk areas that need to be addressed by the firm, be that in production, service delivery, complaint handling, etc. The importance of each factor varies by sector. Security will be highly valued by customers of a bank where the relationship is based upon trust that the bank is a secure custodian of one's wealth. In contrast, security will not be such a concern in a customer's relationship with a sandwich shop, but more based upon compliance with health and safety regulations.

In the finance sector banks and regulators alike have realized that reputational risk is something that can be quantified and therefore needs to be taken into consideration when establishing the level of economic capital required to support the business and in particular to protect shareholders against the likelihood and severity of unexpected losses arising from damage to reputation. With advanced risk modelling techniques, models can be constructed that allow banks to map the potential losses from reputational risk events on to the financial statement line items. Once these models mature, reputational risk management is likely to move from being an intellectual curiosity to becoming a critical business performance tool to protect shareholder value.

By managing, at source, the risk factors of key importance to customers, a reputation can be built through effective PR and word of mouth. The perception of the stakeholders can be built and expectations set, to coincide with delivery on those expectations. Reputation risk matters hugely to organizations. It's what risk is really all about: mitigating and preventing the risk of going out of business. It has been referred to as the Cinderella risk, but perhaps now, as organizations recognize its importance, Cinderella will be going to the ball!

Look for the UKAS mark

UKAS
UNITED KINGDOM ACCREDITATION SERVICE

Save Money... ...Reduce Risk

If your business uses **testing, calibration, certification** or **inspection services** in these sectors, *look for the UKAS mark* when choosing your suppliers

Hampshire County Council

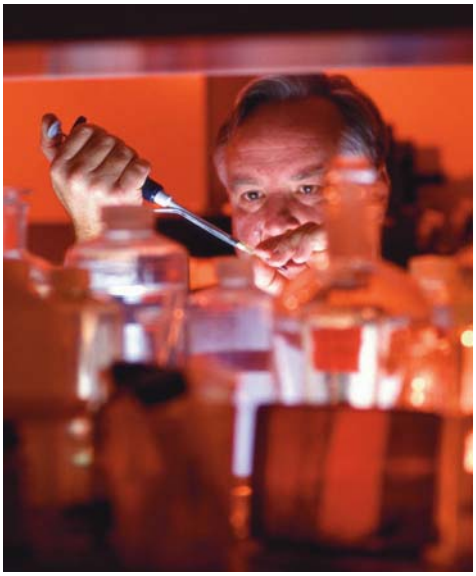
"Our supplier selection policy stipulates that a business must demonstrate financial viability, Health & Safety competence, and UKAS accreditation. As a purchaser, it is essential that we get what we ask for.

UKAS accreditation is a pre-requisite whenever we are choosing an organisation to work with to help us manage asbestos. We do not however look for UKAS accreditation in one area of asbestos management. We would look for it in all areas – for example for testing, surveying and air testing.

The reasons for using a UKAS-accredited company are manifold. Firstly, it is a way of ensuring the quality of the work. However it is not just about the quality, as we are dealing with the management of asbestos in schools and offices, and so there are clearly reputational issues at stake as well.

Using a UKAS accredited organisation is not going to necessarily increase the price of procuring a particular service. A UKAS accredited organisation will offer value for money. The cost of getting it wrong and re-working is phenomenally expensive. This would not be the best use of rate payers' money. It is much cheaper to get it right first time."

Glenn Turner,
Head of the Scientific Service,
Hampshire County Council



Visit **www.ukas.com** to find out how using a supplier accredited by UKAS will deliver real benefits for your business

Delivering Confidence

2.3

Risk management: motherhood and apple pie – or real business benefit?

Jon Murthy, UKAS

Bring together four people into one room. Make one an insurer, another a health and safety expert and the third a business consultant. The final person is a manufacturer. The subject of their discussion is risk management. Like motherhood and apple pie, risk management is deemed to be a good thing. But why? Each party will have its own view.

The insurer

Insurers are looking at risk management as an instrument that informs them as to the type of cover and premium required. Insurers are increasingly interested in developing individual risk profiles for key clients in specific areas, as a more

effective method of both underwriting and supporting client needs. Certainly, the more a client's business is understood, the more efficient the allocation of capital will be, against the understood risk. Insurers are working on the principle that the more they know about the risk the more informed the underwriting will be.

The questions then arise:

- What is the most efficient way of gauging a business's risk culture?
- What systems and processes will demonstrate good risk management?
- How can the insurer be confident that such systems and processes will be executed faithfully and regularly within the business?

In principle, there are three key areas that would need to be examined: health and safety, environmental, and management practices. Good strategies in these areas should bring down the incidence of accidents that could trigger claims. The casualty part of any insurance programme could be more confidently predicted if these areas were perhaps certified in some way. But insurers aren't in the business of assessment and certification. Their alternative, currently, is to work closely with the client's risk manager and broker so that there is a good level of information transfer – enabling a sound judgement to be made and the premiums to be decided accordingly.

The health and safety expert

The Health and Safety Executive (HSE) confidently claims that health and safety should be the cornerstone of a civilized society. Also, it wants to achieve a record of workplace health and safety that leads the world. However, it is the job of health and safety (H&S) experts to make that a reality in daily business life. They see risk management programmes as the most effective way of ensuring that health and safety matters are executed meaningfully within the workplace. However, an issue arises with the basic nature of the way businesses now work. In the old days, health and safety regulations used to be prescriptive and based on 'tick lists'. There was a comfort factor about this in that, so long as the boxes were ticked, companies felt that they had fulfilled their health and safety requirements. But there was a question as to whether this actually achieved successful health and safety management. It also left the responsibility for health and safety with the list makers rather than the businesses.

In 1972, there was a change to more broad-based, goal-setting H&S regulations. A non-prescriptive model was used, based on the view that those that create risk are best placed to manage it. In place of existing detail and prescriptive industry regulations, it created a flexible system whereby regulations expressed goals and principles and were supported by codes of practice and guidance. The aim was to place responsibility firmly with the business community to establish a culture of health and safety in a proactive rather than reactive manner.

But in the business environment of today, risk management encompasses far more than basic health and safety assessments. A modern risk programme can include sophisticated analysis of what problems and issues a company might face that could interrupt the successful and profitable provision of its product or service. There will be financial projections, costed scenario impact analysis and unit-based performance evaluation and measurement. Everything will be stripped back to its fundamentals and examined as to whether it contributes an opportunity or a risk to the business. Health and safety has to take its place alongside political, social, technical and environmental risk analysis.

However, unlike some of the other areas, health and safety risk management is a basic discipline, executed day by day within the business. The practical implementation of good health and safety management operates a long way from the boardroom and even further from the policy makers and government agencies. This is where the results are generated. The tables of statistics that reflect UK plc's performance in health and safety are based on health and safety experts being able to produce good business reasons why a particular percentage of the corporate pound should be spent on health and safety. In the past, it has simply been enough to point at the statutory or regulatory environment and say 'We have to.' Now, within the overall context of risk management programmes, the argument must be more sophisticated.

The business consultant

It is the consultant's job partly to strip away all the vested interests, look through the platitudes and business clichés and try to see what is really critical to the bottom line. It may mean taking on some sacred cows. For instance, consultants may need to take on the entire concept of risk management. Does it deliver business benefits? How do you measure the real value to risk reduction? Consultants' clients are operating in a world where there is a basic paradox. Citizens are increasingly demanding a riskless society. Most customers, however, choose to purchase products and services based on price, but will also respond to consistent brand values such as quality and value. Risk measurement? No, it doesn't appear to sell more widgets. However, if a product (such as foodstuffs) suddenly appears to present a higher risk to consumers, then certainly that risk will inhibit sales.

The risk industry is predicated upon less risk being good and more risk being bad. But consultants want to be able to break this down into a statistical scale and measure where within that scale a client should be ideally placed. It's not a black-and-white issue; nor will the profile of the scale necessarily stay still throughout a business cycle. However, it is useful for the business to be able to address and discuss risk in terms of scale. But how can this business imperative of risk reduction fit into the regulatory and statutory framework? The consultant thinks that a sliding scale is in a client's best interest. But how can this be measured and evaluated? How will this proposition play with the regulators and government agencies?

The manufacturer

Manufacturers are feeling their cheque books. They have a basic business principle. They want success, by which they mean that they want the business to make money, they want people to buy their products and, ideally, they want this to happen without drama or delay. They know that risk management plays some part in the third element of their wish list. They're not sure if or how it contributes to items one (money) and two (sales). However, they are pretty sure, at least in some areas, that it is a good thing. For instance, the broker has at least identified some practical financial benefits of risk management.

Manufacturers would like to be able to better evaluate the business benefits of risk management. Too many of their suppliers use risk management claims as a sales panacea to cover all ills. From facilities management to data recovery, insurance to engineering inspection, everyone claims to be reducing manufacturers' risk. Manufacturers think they probably do, but would like to be able to measure it a little more effectively. If there were tables that showed the correlation between share prices and risk management, that would be interesting – or tables of sales figures or market share that compared those companies with quality marks or standards to those without.

In the meantime, however, manufacturers hope that the insurers will give them a better premium because of the risk culture their companies have developed. They're buying into the idea that they should exercise good business practices because it does lessen the threat to their businesses of a consumer backlash because of health or environmental considerations. One thing that they do find an issue is the propensity of regulators and government agencies to 'cascade' information down upon the business without having the courtesy of taking feedback from the coalface. They would like to be able to work within an environment where they are applying effective and efficient standards that satisfy consumer demands while also protecting business assets – the people, property, proposition and production facilities. Those would be the real business benefits to manufacturers of a risk management programme.

UKAS

UKAS accreditation means the evaluator can show to its customer that it has been successful at meeting the requirements of international accreditation standards. UKAS is the sole UK accreditation body recognized by government to assess organizations that provide certification, testing, inspection and calibration services.

In all the cases above UKAS is interested in demonstrating that objective, independent evaluation can help evaluate and assess risk management programmes. For example, internationally recognized standards already exist for the certification of environmental and quality management systems, the provision of which can be assessed by UKAS. In other areas of business, specific sector schemes can be developed to provide meaningful evaluation that will be internationally recognized. The UKAS approach ensures that such schemes demonstrate competence and performance capability on an ongoing basis.

Beyond motherhood and apple pie, there is a fit between risk management and the accreditation process, and together they deliver real business benefits. More recently, UKAS accreditation has been recognized by the insurance industry. A number of insurance brokers, backed by well-known underwriters, have introduced dedicated schemes for UKAS-accredited organizations. Recognizing the excellent claims history of UKAS customers, these schemes provide increased coverage and reduced premiums.

what a difference a day makes

A lot can happen in one day. That's why Callcredit gives you information that's updated daily, rather than weekly or even monthly. With CallMonitor, the UK's first daily alert service, you find out faster if something about your customer changes – giving you the opportunity to act before it's too late.

Find out more at **www.callcredit.co.uk/MBR** or call 0113 244 1555

different is good

© Callcredit Limited 2008. All rights reserved.
Registered in England and Wales with company number 3961870.
Registered Office: The Bailey, Skipton, North Yorkshire, BD23 1DN. www.callcredit.co.uk

Callcredit
Part of the Callcredit Information Group

2.4

Credit risk management

Richard Brennecker, Callcredit

Introduction

One of the challenges of modern credit risk management is the application of robust analytical techniques against an ever-changing background of economic conditions, technological advances, regulatory changes and customer demands.

The current economic climate is especially demanding with the 'credit crunch'; increasing costs of essential items and falling house prices are putting a number of households under significant financial pressure. Annual bad debt losses run into billions of pounds, and recent events have put the results of most institutions under an even more intense spotlight. Increases in funding costs and regulatory pressure in areas such as fees and insurance have put further pressure on profit margins. The combination of these two factors makes the credit risk manager's job of lending to the right customers profitably even more crucial.

Given the uncertainty, many institutions have been comfortable to restrict lending over the past year; however, the pressure will soon resume to grow lending and deliver the results shareholders expect.

This article looks at the challenges currently faced by senior credit risk professionals and the role more effective data use can play in all aspects of the credit life cycle.

Credit marketing

Acquiring new customers is often the first touchpoint with a consumer and can have a major impact on portfolio quality and profitability. Customers are becoming more demanding, with a big movement to internet channels and a demand for instant decisions.

Traditionally lenders were happy to 'target' large parts of the UK population in a mass volume manner, hoping to maximize response rates and lending volumes. For many years the domains of marketing and credit risk were very separate, with differing success measures, which generated significant inefficiencies through marketing to customers who had little or no chance of passing the credit underwriting criteria. The movement to a customer value management approach adopted by institutions a few years ago started to drive more involvement for credit risk functions in the marketing area to bring more analytical rigour to the targeting function. The recent reduction in profit margins and the increased emphasis on responsible lending are leading increasing numbers of organizations to be yet more targeted in their activity to maximize the value generated by reduced budgets.

The process of pre-screening potential customers for adverse data via a credit reference agency (CRA) is now well established. More and more lenders are moving towards 'dual wash' strategies with a second CRA, or indeed champion-challenging their existing supplier. This approach ensures that lenders can access the most predictive data available to them with clients finding an additional 20 per cent of prospects who are ineligible or uneconomic to mail, resulting in reduced costs and a better overall customer experience. The use of multiple agencies also encourages creative thinking, product innovation and healthy commercial rivalry.

Application processing

Application processing was the first area to see the widespread introduction of scorecards in the industry, with a number of major institutions implementing systems in the early 1980s. These early scorecards based most of their predictive power on information supplied by the applicant on areas such as home ownership, employment and marital status, which provided a significant advance in consistency over the previous manual underwriting-based approaches.

It soon became clear that even more powerful scorecards could be produced through the introduction of credit bureau data into a lender's front-end scoring system to arrive at an accept/decline decision based on the applicants' track record with other lenders.

The next major advance came in the late 1990s when credit scoring was used for pricing decisions as well as acceptance. The drive for this change came from a desire to turn down fewer applicants and saw many institutions, particularly in the credit card market, developing new products for the underserved markets. These changes put a significant onus on credit risk professionals to take a value-based approach to optimize the risk/reward balance, not just minimize bad debt charges, but this seems to have been reversed to some degree over the past 12–18 months.

Against the current backdrop of over-indebtedness and the credit crunch, it is worth noting that lenders are finding increasingly that their traditional methods of credit scoring are missing, or at least not effectively identifying, a debt-stressed subset of the population. These people are becoming, or are already, highly over-indebted, with the crucial missing element being the affordability of the debt to individual customers.

Lenders are increasingly using new tools and strategies to identify customers with high levels of unsecured debt with what would traditionally be considered 'good' credit risk profiles (ie they are up to date with their credit commitments). In extreme cases of over-indebtedness, where the ratio of unsecured debt to net monthly income is in excess of 25 to 1, it can be seen that more than 50 per cent of consumers are up to date on their credit facilities with multiple lenders and 75 per cent have been no more than one payment down on any product in the last 12 months.

Analysis carried out in 2007 showed that a number of over-indebted customers were improving their position by accessing the equity in their property via a remortgage or second-charge mortgage. Given the tightening in lending criteria and the fall in house prices following the credit crunch, it became very difficult for customers to restructure their debt in the same way in 2008, putting additional strain on those already in difficulties. The challenge for credit risk managers is integrating this new approach into existing credit strategies. It is clear that it is not a direct replacement for traditional scorecards, but rather that indebtedness data should work in tandem with credit risk scores to deliver optimized credit decisions.

The trend towards using data from more than one CRA, often referred to as 'multi-bureau', has grown in popularity in the last couple of years as lenders strive to build as complete a picture of their customers' position as possible. Unsurprisingly, many lenders are working on developing multi-bureau strategies, not only to maximize the use of 'similar' data from multiple CRAs but also to integrate predictive variables based on indebtedness data and adopting tools that measure the affordability of additional lending for a customer.

Another growing area of technological influence is electronic verification, where external data supplied by credit reference agencies are being used to complete anti-money-laundering checks on new customers. This has the dual advantages of removing the labour-intensive document-based checks and improving the speed of the end-to-end customer process. While this may appear to be merely operational issues they have a beneficial credit risk impact, as the document-based approach tended to disincentivize good customers from completing the process.

Customer management

The changing economic landscape, with increasing utility prices and customers rolling off low-rate fixed mortgage deals, makes the ongoing risk assessment at customer level essential. It is no longer prudent to rely on scoring at application stage without updating the view on a regular basis.

To achieve this, many lenders have implemented behavioural scoring systems. The first systems in the late 1980s and early 1990s tended to be internally focused,

basing the risk assessment on characteristics such as missed payments and time on books, but now the majority are underpinned by monthly bureau data feeds from either one or multiple CRAs.

The credit strategy within customer management systems has become increasingly complex and is often made up of numerous scoring models and distinct credit strategies covering a variety of products, brands, segments and business processes. Whether it is shadow limits on credit cards, auto-pay limits on current accounts or customer-level risk indicators, the number of parameters that require maintenance and monitoring is significant.

The speed with which organizations react to changes in customer behaviour is crucial in successfully managing lending portfolios. The recent introduction of daily monitoring and alert services offers the ability to react more dynamically to changes in customer behaviour than was previously possible with traditional monthly scoring runs. Integrating this information into existing credit strategies can be complex but is certainly achievable in timescales that ensure benefits are realized and a competitive edge gained.

When the current economic conditions start to improve, the pressure to expand lending will grow and the credit risk manager will be faced with the task of identifying those customers to whom it is now more appropriate to advance additional lending. The challenge will be to identify those who are now in control of their finances again, despite some historic adverse indicators, and to adapt policies and strategies accordingly. Again, external data will be key to getting this decision right, but the benefits of being one of the first institutions to show renewed faith in a customer are significant and will make it worth the effort.

Collections and recovery

Historically, the collections and recoveries area has been less developed in relative terms, but this is changing rapidly as organizations compete to secure payments from customers who are struggling to meet all their commitments. Traditionally, collections systems have tended to be operationally focused, with contact strategies driven by balance rather than risk or probability of repayment, giving rise to significant opportunities to improve the effectiveness of the process.

Recent innovations in this area are numerous. Institutions are adopting pre-delinquency management techniques to establish dialogue with customers before they have missed any payments, and advanced multi-stage statistical modelling is now being deployed to predict the propensity to repay. Lenders are also starting to deploy tools that look at customer affordability as part of collections negotiation activity, with income data being used to identify customers who may be understating their ability to repay delinquent debts. Developments in software are also impressive, with collection platforms now incorporating decision engines, web payment portals and dialler management capabilities. Debt purchasers are also looking at daily changes to the debtors' credit file for more efficient and effective management of their assets.

UK legislation is becoming more stringent, with previous best-practice guidelines being written into enforceable legislation. The automated tracing solutions

are under particular scrutiny. The UK trade industry bodies are also keen to punish companies working outside the guidelines, and the industry momentum to be more transparent and ethical continues to increase. The UK continues to move away from the United States in terms of much stricter operational guidelines, particularly with reference to debtor information and dialling practices.

Debtors are now able to access more information and support with regard to their debts than ever before and, considering the recent increases to the cost of living, the amount of monies offered for repayment is generally lower. With the legislative changes adding a further cost to the costs of collections, the operational efficiency of most collection areas is under more pressure than ever.

The debt sale arena is growing as institutions look to sell on debt and release the regulatory capital it ties up; both sellers and buyers are benefiting from much greater use of CRA data and are deploying tracing and segmentation tools to improve performance. Secondary debt sales or 'resales' are becoming more common in the UK, and the debt purchase industry is adapting to the opportunities of accessing bureau data on their purchased portfolios. Foreign investment is still high in the UK, with some of the larger purchasers choosing to outsource the entire collection operation to UK debt collection agencies.

Taking these developments as a whole it becomes clear that the use of data in collections and recoveries is increasingly adding value to the bottom line of many organizations and that this area is now very much part of an organization's overall risk management approach rather than merely being an operational afterthought.

Summary

Credit risk management is a complex discipline covering the entire customer life cycle. The current challenges thrown up by the 'credit crunch' and subsequent events have put the credit strategies of most organizations under increased focus. The greater use of external data, particularly in areas such as indebtedness, identity verification and collections, coupled with new tools such as daily alerts and affordability measures, has the potential to equip credit risk professionals to operate successfully in this dynamic landscape, with those who lead the way by embracing these developments being the most likely to succeed.

2.5

Credit risk assessment for loan decisions: a new approach

Clark Abrahams, SAS UK

Introduction

This chapter sets out to establish the need for a comprehensive overhaul of the traditional credit assessment and underwriting practices, which have contributed to the billions of dollars of sub-prime lending losses incurred across the industry over the past two years.

Risk expert Myles Shevlane believes a number of factors were to blame for the sub-prime mortgage crisis, but a significant root cause factor was the reliance on conventional credit scoring and underwriting practices. The introduction of modern automated underwriting systems along with advancements in analytics, such as use of credit scoring and risk-based pricing, gave the banks a false level of security and encouraged a rapid expansion in sub-prime lending. So now banks face a dilemma: whether to return to a historical human-based lending assessment process or look to stick with the current highly automated scoring-based approach.

It has been recognized that development in automated underwriting technology has played a significant role in encouraging lenders to penetrate deeper into the sub-prime loan pool. To a large extent, sub-prime lenders believed any additional risk they were taking on was covered using advances in credit scoring and scoring system policy overlays. This enabled them to effectively price that risk and charge borrowers on the basis of their fully quantified creditworthiness. This has contributed to the rapid development of the sub-prime loan market[1] and has created greater access to home ownership for some segments of borrowers, such as low-income and minority households.

The magnitude of the current crisis makes it abundantly clear that there is significant room, and need, for improvement in current credit assessment approaches. There are two fundamental problems that contributed to the weakened underwriting standards and degraded loan quality.

First, credit scoring has not done an adequate job of assessing risk in the sub-prime mortgage market. The majority of the sub-prime mortgages underwriting systems were not, in fact, capturing 'the full range of risk factors in the market'.[2] In particular, their conventional risk models were applied to non-conventional loan products, which are associated with different payment terms and behaviour. Improper use of credit scoring and automated underwriting presented incomplete risk analyses and weakened underwriting standards and policy. The end result has been a drop in loan quality.[3] Lenders are now re-evaluating their lending procedures and tightening their lending standards in an effort to improve loan quality. This effort will inevitably involve underwriting technology improvement, which includes strengthening process integrity and upgrading scoring and automated underwriting system components. The system component upgrade will entail evaluation of the adequacy of data, current modelling practices and risk measurement frameworks.

Second, there is a blind spot in today's underwriting practices. That is, current practices over-rely on quantitative models and automated underwriting systems. Technology has a vital role in boosting efficiency and helping to measure and monitor credit risk. The models have their place and part to play. However, we need to control the models instead of the other way around. Loans first need to be properly classified and then risk-rated. Today's process has that back to front.

New and improved ways for addressing limitations of credit-scoring systems and evaluating credit risk will be in demand. Simply recalibrating existing models and throwing more of the same technology at the problem will not fix it.

Capturing revenue opportunities in new markets with alternative credit risk management systems

Traditional credit analysis uses human judgement to evaluate creditworthiness; the main drawbacks associated with this judgemental system are inefficiency and subjectivity. Over time, this system has been replaced by computerized statistical models, which represents a great advance in many disciplines, including credit

granting, loan portfolio management and compliance testing. To date, credit-scoring models represent the most successful application of statistical modelling methods to assess consumer credit risk. Among the many benefits that credit scoring has brought is the hastening development of the secondary market for consumer loans, which has provided needed liquidity to lenders that are able to risk-rate, price and bundle loans for sale to investors in the capital market.

In certain instances it can prove advantageous to exercise more control over the historically data-driven models, rather than letting those models dictate the outcome. Both judgemental and credit-scoring approaches bear some weaknesses and strengths. That presents a bit of a conundrum. Would you rather: 1) promote less efficient, more subjective and less consistent judgemental loan approval processes; or 2) rely entirely on data-driven scoring models?

An alternative modelling approach can take advantage of the strengths associated with human judgement and computer models by means of a *hybrid approach*. An alternative loan underwriting model will support safe and sound lending while providing a more flexible process for qualifying creditworthy consumers, many of whom currently fall outside the mainstream. The motivation for considering, and ultimately embracing, these new approaches lies beyond process improvement for granting credit to *mainstream* consumers, although the business case is compelling enough to justify it. The real thrust for the timing of this technological change is the change in the consumer population itself, and the dynamics surrounding it, on which the standard current models may not fully capitalize.

Consumer access to credit depends largely on point-scoring models that have evolved over the past several decades. A major premise of credit-scoring models is that past performance determines future outcomes. Most credit models were developed based on samples that did not include the un-banked population. This raises the question: 'How can lenders qualify certain segments of the consumer population that have not historically been users of traditional credit and hence do not have associated credit payment performance histories in credit bureau databases?'

These models implicitly assume that un-banked people have no significant differences in credit characteristics from their mainstream counterparts. This assumption is not necessarily well founded and may hinder qualified consumers from accessing fair credit and meeting their financing needs. Credit market opportunities in emerging markets will be most heavily affected, and this will further increase exposure to fair lending compliance violations. The propagation of new alternative credit models throughout the financial system will afford better, fairer, chances for all borrowers, and greater revenue for lenders, and deliver broader economic prosperity in communities across the nation.

SAS redesigns the credit risk assessment, analytics and performance management process

A comprehensive new credit risk framework is needed – a hybrid approach that combines the best that technology can offer with expert human judgement. Such

an approach can help deal with the current crisis and may lessen the extent of, or even prevent, the next one.

SAS has therefore pioneered the Comprehensive Credit Assessment Framework (CCAF), which can get the job done. CCAF provides a consistent approach by using advanced computing technology and a sound, safe model development and validation process. CCAF naturally affords a sustainable and sensible segmentation based on all primary credit factors. It then offers a systematic means for taking appropriate actions relative to those identified segments, as well as for ongoing monitoring of the impact of those actions in a comprehensive and efficient manner. Simply put, CCAF accomplishes this by:

- expanding the boundaries of information;
- appropriately segmenting loan applicants based upon primary factors;
- layering in needed secondary qualification factors;
- assigning actions for each identified segment;
- putting in place an adaptable policy mechanism that is responsive to the evolving economic climate.

More specifically, CCAF improves current credit scoring from following three perspectives:

1. CCAF ensures inclusion of primary predictive factors that cover the full spectrum of relevant qualification criteria and both determines and reveals how they combine to produce outcomes. Credit scoring, which relies on historical data, does not have this capability, nor does it possess a feedback mechanism to adjust factor weightings over time as experience accumulates.
2. CCAF determines which risk factors pertain to the lending decision within the context of each borrower's situation and the loan product parameters, and then appropriately adjusts the factor weightings to produce the right outcome. This is in stark contrast to credit scoring, which has a fixed number of factors that have a constant set of point weightings that are automatically applied to all credit applicants regardless of their qualifications. Furthermore, CCAF uses a forward-looking approach and simulates future economic conditions, and its adaptive nature makes it more predictive over time, unlike credit-scoring models.
3. CCAF systematically integrates judgemental components and proper context into the modelling process in a complete and transparent manner. Credit-scoring systems lack context because they rely purely on the available data to determine what factors are considered. Credit-scoring systems lack transparency, because two individuals with identical credit scores can be vastly different in their overall qualifications, the credit score itself is not readily interpretable, and industry credit-scoring models are maintained as proprietary, as are their development processes.

To prevent future financial crises, it is absolutely necessary to improve the borrowers' financial literacy and the lenders' process of transparency and to

better assess loan product affordability and suitability. CCAF achieves these goals through the following aspects:

- *Comprehensible classification to convey the essence of the borrower's qualifications.* This allows risk-rating credit transactions within that complete context, including transaction and borrower contours. It fosters financial education and literacy by letting the borrower know how he or she is classified and ranked according to relevant causally linked primary factors. It also shows borrowers how their proposed loan is classified against other possible loans for which they would be qualified.
- *Greater control of loan decisions.* This is through CCAF's ability to integrate expert judgement with statistically based criteria in the risk evaluation process, which encompasses not only default risk but also concentration risk, regulatory non-compliance risk and a host of other important objectives. Specific thresholds can be enforced at the segment level to limit risk exposure. As a result, significant overstatement or understatement of risk on individual loan transactions can be avoided, as can unacceptable levels of risk across all portfolio segment levels.
- *Easy identification of loans that are truly affordable relative to every borrower segment.* This drives product-offering choices relative to specific credit risk segments. The most suitable mortgage products will vary widely by segment, and they may be neither the most profitable choices for the bank nor the most inexpensive for the consumer. This is a fundamental requirement for responsible lending in the aftermath of the sub-prime mortgage crisis, and it pertains to self-certified and prime markets as well.

Bridging the gap between compliance and credit risk management

In recent years, the banking industry has seen a convergence of risk management and regulatory compliance. Over the past decade, regulatory compliance examinations have adopted more of a risk-based examination approach, especially for larger and more complex enterprises. Hence, it is important to make new connections between compliance and credit risk management that bring to light new possibilities for improving current practices.

Understanding the connection between credit access and credit risk is the key to developing a new generation of models and processes that preserve safe and sound lending while promoting inclusiveness in the credit market. The main thrust of a fair and responsible lending compliance programme is to find and fix problems associated with credit access and to effectively communicate performance to stakeholders in order to avoid, or correct, any misperceptions about the institution's lending performance. Regulators also conduct periodic safety and soundness exams to review bank underwriting standards, among other things. Lenders have credit policies that spell out those standards, which reflect

the institution's actual loan default experience and best judgement to ensure profitable, safe and sound lending. Inaccuracies in credit risk measurement can trigger predatory lending patterns, which can readily cascade into fair lending issues. Hence, failures in credit risk management will almost surely result in non-compliance with laws and regulations.

Key analytic advances

Described below are five new analysis methodologies that can help lenders more effectively and efficiently manage credit and compliance risk while maximizing their shareholder returns (Abrahams and Zhang, 2008):

- *Universal performance indicator (UPI).* This is for creating a comprehensive view of compliance and credit risks at different geographic and organizational levels. Monitoring and managing fair lending risk exposure have become increasingly important for lending institutions as regulatory agencies continue to scrutinize fair lending practices and increase the standards. Moreover, the regulatory examiners themselves, who are evaluating fair lending across their institutions, also need more effective and accurate methods to evaluate it quickly and prioritize their efforts accordingly. The analytic framework is initiated with a universal performance indicator approach. The goal is to obtain a comprehensive picture of overall compliance performance. This entails the exploration of a large amount of data and identification of risk focal points. The new methodology can help institutions evaluate overall business practices in any context with a standardized UPI that simultaneously rank-orders performance relative to all relevant factors.
- *Dynamic conditional process (DCP).* This is designed for effective compliance testing and credit risk modelling by better utilizing data and emulating business reality. DCP can help overcome some limitations inherent in traditional modelling, and DCP dynamically categorizes lending decision-related factors and captures variation in policy thresholds among loan products, markets or programmes. Conditional and interaction structures are created in order to model the variant nature of decision factors in lending decisions, while minimizing the complexity of the model specification process and model maintenance. DCP can outperform competing modelling approaches by achieving a closer fit to business reality and using the data more efficiently. DCP can also be applied to monitoring and improving override processing to reduce associated compliance risk.
- *Risk evaluation and policy formulation system (REPFS).* This represents an alternative credit risk model using either traditional or non-traditional credit information by taking the advantages of both statistical scoring models and judgemental and business criteria. A REPFS is a hybrid model that affords qualitative benefits while preserving quantitative-based decision making. This approach has particular applicability to emerging markets.

- *Multi-layered segmentation (MLS).* This is for developing integrated segmentation schemes to perform assessment for various segments, including neighbourhood and under-banked lending and investment. Proper segmentation is the key to getting good results, to validating those results and to thoroughly and concisely explaining those results to all stakeholders. The multi-layered segmentation approach can be used for risk and revenue evaluation and to formulate credit risk management strategies. The approach affords a complete and deep understanding of the driving forces behind outcomes and how those outcomes stack up against a variety of norms (historical, regulatory, market, industry, societal, economic) and both near-term and strategic goals (business, consumer, community and regulatory).
- *Credit and compliance optimization process (CCOP).* This is for integrating credit and compliance objectives within the model validation process to achieve optimal business decisions and strategies. A credit and compliance optimization process (CCOP) is offered for consideration as a unifying concept. Model optimization and validation are approached from both credit risk and compliance risk perspectives using an integrated analysis methodology. The integrated methodology uses the hybrid approach to perform a more comprehensive model validation in an intuitive way. Override analysis results and the UPI concept are also integrated into this framework for compliance monitoring.

Collectively, these advances can help lending institutions strengthen their internal controls for identifying, measuring, evaluating and monitoring risk.

Summary and conclusion

So what needs to change? Myles Shevlane believes banks need to learn from the lessons of the sub-prime crisis and take a completely fresh look at the end-to-end credit approval and credit-scoring process. This will involve a major re-evaluation of end-to-end credit assessment and lending procedures, encompassing market assessment, stress testing, analytics, modelling and scoring, risk assessment and risk-based performance management.

A comprehensive new credit risk framework is needed to address the major shortfalls in the conventional approaches to credit scoring. In response to the new demands to transform this process, SAS has pioneered the Comprehensive Credit Assessment Framework (CCAF). CCAF transforms the end-to-end credit assessment process, introducing a more sophisticated credit-scoring methodology and advances in analytical techniques and modelling. SAS has designed a much more sophisticated and all-encompassing process, and linked this with advanced modelling techniques. A key difference in the new approach is the way the SAS process allows for the reintroduction of expert judgement and knowledge of the customer in the process.

CCAF provides a consistent approach by using advanced computing technology and a sound, safe model development and validation process. CCAF naturally

affords a sustainable and sensible segmentation based on all primary credit factors, and then offers a systematic means for taking appropriate actions relative to those identified segments as well as for ongoing monitoring of the impact of those actions in a comprehensive and efficient manner.

CCAF incorporates advances on several fronts, such as:

- inclusion of additional alternative sources of information;
- inclusion of more credit applications having missing or incomplete information;
- more holistic model formulation;
- less reliance on historical samples that may not reflect the full range of possible future outcomes;
- the ability to adapt as additional loan data and policy rule changes are collected and incorporated, making CCAF more, rather than less, predictive over time.

CCAF effectively segments customers into relevant groups, enabling identification of all risk factors associated with each group in combination with customer-specific behaviour data and appropriate use of advanced analytics and credit-scoring techniques. This incorporates expert judgement and the calibration of the models to allow for changes in economic and financial markets, together with regulatory and compliance parameters.

The integration of CCAF and the aforementioned new approaches in lenders' credit risk management and fair lending compliance programmes will prove beneficial to all stakeholders, including lenders, borrowers, secondary market conduits, investors and regulators. Adoption of CCAF, in particular, will help prevent credit market disruption by forcing consideration of the full business and lending context, by not over-relying on pure quantitative models, by continuously monitoring portfolio concentrations and by imposing concentration limits when and where necessary so that risk exposures are never allowed to reach crisis proportions. Further, as CCAF adoption becomes universal, regulators will be able to better compare lending institutions, aggregate results across institutions and geographies, develop new, more effective benchmarks, and spot adverse trends in risk ratings, exposure concentrations and loan performance.

There are few endeavours more important than the quest to provide safer, fairer and profitable access to capital for qualified individuals and businesses in order to improve the quality of lives and to foster sustainable economic growth and prosperity. The comprehensive overhaul of the traditional credit assessment and underwriting practices we are proposing will take us a long way towards achieving that quest.

Notes

1. Sandra Braunstein, Director of Consumer and Community Affairs for the Federal Reserve, the House Committee on Oversight and Government Reform, *Inside Mortgage Technology*, 21 May 2007.
2. Patricia McCoy, professor, University of Connecticut Law School.

3. Ben S Bernanke, Sub-prime mortgage lending and mitigating foreclosures, before the Committee on Financial Services, US House of Representatives, 20 September 2007.

Reference

Abrahams, Clark and Zhang, Mingyuan (2008) *Fair Lending Compliance Intelligence and Implications for Credit Risk Management*, Wiley, Chichester

2.6

Making risk management deliver business value

Ruth Murray-Webster and Peter Simon,
Lucidus Consulting Limited

In this chapter we start from the position of accepting that risk management for business is a good thing, required by regulation and supported by standards (eg the IRM/AIRMIC/ALARM risk management standard or BS6079–3:2000), methods (eg the UK Office of Government Commerce's Management of Risk – M_o_R®), tools (eg @RISK or Crystal Ball) and training provided by a wide range of providers. Yet many organizations find it difficult to make a process that seems complete common sense work for them. They struggle to build the culture and working practices necessary to transform the rhetoric into reality. Why might this be? We have some experiences and insights to share that may help to make effective risk management a reality for you.

What does risk management really mean for business?

Our experience is that, to really make sense of risk management for business, it is necessary to go back to examining risk management from a life perspective. Although standard dictionary definitions of the term 'risk' and our everyday use of the term suggest potential threat (something that is uncertain, which, should it occur, would mean something bad for one of our objectives), common business parlance also embraces the notion of risk as an opportunity (uncertainties that would have beneficial impact on something that matters). If you stop to think about how we as human beings look at the uncertainties around us, then it is easy to see that the process that is going on is a weighing up of chances (probabilities or likelihoods) and consequences (impacts or effects) and concludes in a decision being made on how to proceed.

So what risk management really means for business, we suggest, is summed up by these two questions: 1) how does your organization identify and manage those uncertainties (threats or opportunities) that have the biggest impact on business value (matter the most to you), and 2) how do you use this information to make optimal decisions in uncertain situations?

How do published standards and methods help, and how do they hinder?

Published standards and methods can help in many ways. By using a common language and a step-by-step process they are able to provide a consistent, repeatable approach to risk management. This has the advantage that an organization has one way of working to teach or make people aware of and no one has to 'reinvent the wheel' every time a risk assessment is undertaken.

The UK Office of Government Commerce's Management of Risk (M_o_R) is a good example of a publicly available method. Like most other risk management methods it is based around a series of steps or stages: identify context and risks (both threats and opportunities), assess or evaluate risks, plan responses and implement responses. M_o_R also recognizes that the risk management process needs to be embedded and reviewed and that communication is essential.

With a common language and understanding of a structured method in place, businesses can move forward from random risk management, based largely on personal intuition, to a more formal process where there is a way for all interested parties to contribute to risk identification, assessment, response planning and ongoing management. Figure 2.6.1 identifies a typical risk management process.

We work with many organizations that have invested heavily in the adoption of a structured and standard process for risk management, yet many of these organizations perceive that this rigour gives them little more than administrative benefits. Yes, they 'tick the boxes' at audit and can be seen to be doing

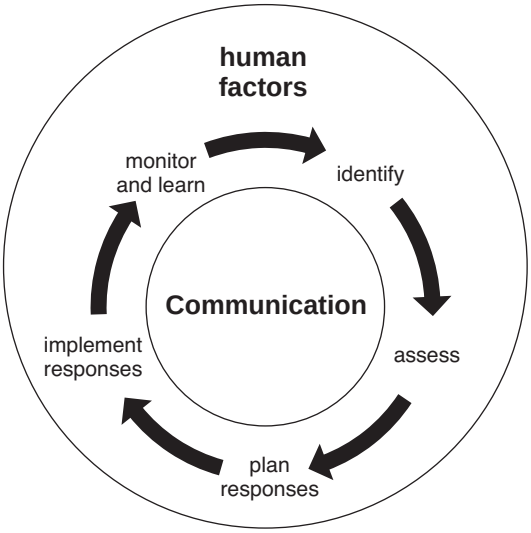


Figure 2.6.1 A typical risk management process

something – but is the risk management process working to create, or at least prevent the destruction of, tangible bottom-line business value?

Standards and methods are an essential aspect of risk management, the alternative being to make it up as we go along. However, most do not recognize two things. First, any process needs to be scalable, ie fit for use in any business context and therefore avoiding the 'sledge-hammer to crack a nut' syndrome. Second, and most importantly, any process must overtly take account of the inherent human factors in the assessment of what is risky and what isn't, and the degree to which those things matter.

The complication of human factors

In the final analysis, individual people and groups of people make business decisions in uncertain situations. When making decisions those human beings weigh up the things that they perceive could happen, the chances and consequences and make a judgement. Although most people in business would attempt to be rational and systematic about this it could be argued that despite such attempts 'risk is in the eye of the beholder'. Certainly there are some situations where there is sufficient historical evidence and data for future situations to be predicted with some confidence; but different people will still put their own personal 'spin' on the data and the decision that is made as a result. Moreover, there is never enough information to predict future situations with certainty. Unless we are talking about situations of pure variability (like throwing an unloaded die or playing the lottery) where a mathematical probability can be calculated, there will always be residual uncertainty that could matter a lot to the business. These may be 'unknown unknowns' or 'Black Swans', as

It is not only consumers who suffer the consequences of counterfeit goods. Damage to reputation and the loss of sales are of major concern to businesses.

Perhaps the most obvious risk of counterfeiting is a diversion of sales and loss of profit. Without the burdens of development, advertising and overheads, counterfeiters are able to bring their product to market quickly and in most cases are able to severely undercut the cost of genuine items. Too many consumers will also take the option of the cheaper, poor quality counterfeit where that option is available.

Unfortunately, consumers will not always be aware that the goods they are purchasing are counterfeit. This will understandably lead to an unjustified loss of confidence in the brand in question and irreparable damage to the reputation of that brand. Where a consumer is uncertain as to whether a brand is genuine or not and, as is often the case safe or not, will mean the consumer simply prefers to steer clear altogether.

Protection

Jason Lumber at Harrison Goddard Foote comments "The first logical step in guarding against piracy is to ensure that the correct intellectual property rights are put in place. Regular intellectual property audits are crucial to ensure that rights which can be protected are protected as early as possible."

Some rights, such as copyright, subsist automatically. Others, including the laws protecting trade marks and designs of products, require registration through the appropriate authorities. In many cases the existence of registered rights allows the owner to simply produce a registration certificate for the purpose of having goods detained or for the purpose of prosecuting counterfeiters.

Detection

With intellectual property rights in place, companies should develop a strategy for detecting counterfeit goods.

Customs authorities and local trading standards will often be at the front line of detecting counterfeit goods in the EU. In 2006, customs seized more than 250 million articles and were involved in 36,486 cases involving counterfeit goods.

Customs will move to seize goods on their own initiative where sufficient grounds exist for suspecting that goods infringe an intellectual property right. However, the effectiveness of Customs can be enhanced when intellectual property owners take proactive steps to increase the chances of detection. A general 'Application for Action' can be filed annually with the Customs authority at any time as a preventative measure. This application informs Customs officials of the rights owned and if available, intelligence as to potential counterfeit imports. Filing this document can greatly increase the chances of counterfeit goods being detected.

When goods are seized, a right owner has a very short time, normally just three days, in which to take action before the goods are released. Therefore it is important to have clear strategies and lines of communication through the relevant divisions of an organisation and their legal advisers.

Trading Standards can also be utilised to seize counterfeit goods in the UK. They provide a free service if counterfeit goods are located in their particular jurisdiction whereby counterfeit goods are seized and counterfeiters themselves are prosecuted.

Customs and trading standards have only limited resources and intellectual property owners should look to supplement their detection strategies with other means. Intellectual property practitioners can offer specialist investigation and watching services including, for example, internet auction watching.

Other practical preventative steps can be taken to reduce the risk of counterfeits making it to the market. Supply chains should be supervised closely to ensure that retailers do not deal in counterfeit goods. Agreements with retailers should permit unannounced audits and distribution chains should be monitored because counterfeiters often prey on weaknesses in the legitimate distribution chains. Many counterfeiters try to add their counterfeit goods in with legitimate goods for them to then pass unnoticed through Customs and regular distribution or retail channels.

Enforcement

When counterfeit goods have been detected, the available options range from requesting the destruction of goods by Customs and instructing lawyers in the preparation of cease and desist letters, right through to pre-trial remedies such as injunctions and the issuance of full court proceedings.

Aggressively pursuing litigation against those that manufacture, distribute and sell counterfeit products can have a huge deterrent effect. In addition, litigation may uncover further information which assists in finding those responsible for the counterfeit product.

Although it is difficult to reduce the risk of counterfeiting completely, it is worth implementing measures even if only to act as a deterrent. If counterfeiters can see that a company is actively aiming to prevent its goods being counterfeited then it may discourage further illegal activities.

Getting these steps right can ensure that a brand or product is not the next major counterfeit target ensuring the integrity and profitability of the brand or product.

For further information please contact either Richard Wylie (TM) rwylie@hgf.com or Sanjeet Plaha (Litigation) splaha@hgf-law.com

4

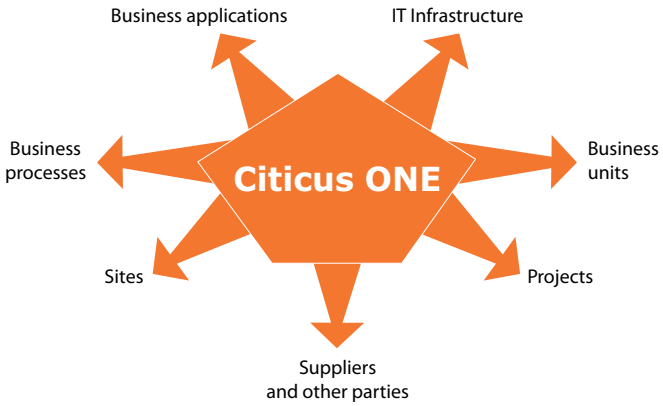
Information and Security Risk

180

citicusone

The world's most advanced software for managing information risk and other areas of operational risk:

- Tells top management what they need to know about their organization's risk status, in terms they can understand and relate to
- Enables risk to be assessed objectively and consistently using a highly-efficient and proportionate assessment process that can be applied to any area of operational risk
- Keeps track of actions needed to drive risk down
- Enables consolidation of risk ratings and remediation activity within and across risk areas
- Has been used to carry out many thousands of risk assessments in over 150 countries
- Can be installed in-house for use within organizations of all sizes or accessed via a hosted service
- Easily configurable to probe the areas of risk of greatest concern to **you**
- Full training and support available



Recent feedback from customers:

*"After I configured **Citicus ONE** to do our privacy impact assessments, it gave me goose-bumps to see how well assessments are presented."*

Risk practitioner Major US manufacturer

*"The Harm reference tables presented by **Citicus ONE** have a touch of genius about them. We can apply them to anything we wish to assess."*

Actuary Major insurer

For further information, contact Marco Kapp, Simon Oxley or Sian Alcock at:
Citicus Limited, Holborn Gate, 330 High Holborn, London WC1V 7QT, United Kingdom
Web: www.citicus.com Email: info@citicus.com Tel: +44 (0)20 7203 8405 Fax: +44 (0)20 7203 840

4.1

Managing information risk and other areas of operational risk: routes to success

Marco Kapp and Simon Oxley, Citicus Limited

In 1999, the Organisation For Economic Co-operation and Development (OECD) – a body where 30 of the most economically advanced nations of the world come together to devise policies to foster economic growth and the expansion of world trade – published its *OECD Principles of Corporate Governance*. This highly influential report argued that identifying and managing risk are a fundamental part of top management's job, and that boards of directors should:

- establish a risk policy;
- institute a system for risk management;
- be fully informed about risk (ie be provided with accurate, relevant and timely information, and training if necessary);

- deal with risk with due diligence and care;
- disclose (eg by publishing in their annual report) all material risk factors and how risk is monitored and managed by their organization.

The OECD principles were endorsed by OECD ministers in 1999 and revised in 2004. They are now the international benchmark on corporate governance for policy makers, regulators, investors, corporations and other stakeholders worldwide.

Developments over the last five years – including those presently unfolding in the home loans and banking sectors – underline the importance of strong corporate governance and effective risk management practices. Notable events include:

- high-profile collapses of firms such as Enron Corporation, WorldCom and Parmalat, which led to the US federal government passing the Sarbanes–Oxley Act 2002;
- rogue trading losses at AIB, Barings, National Australia Bank and Société Générale;
- improper disclosure of sensitive data that millions of citizens entrusted to government or private companies;
- flawed risk management practices that led to the 2008 'credit crisis' – which is still unfolding.

The OECD principles and subsequent events show that managing risk well is important because policy makers, regulators and investors *require* that it is done well. It is indeed a crucial part of good management – with the potential for *catastrophic* loss if not done well, ie loss at a level that the organization concerned cannot sustain without outside assistance, or at all.

As a result, today, annual reports report on risk management practices and highlight key risks with increasing clarity and sophistication. Given the global credit crisis, it doesn't take a crystal ball to see that the pressure to manage risk well will intensify in the near term.

What does managing risk well mean?

So what does a business need to do to manage risk well? Some businesses have excellent methods in place for managing particular areas of risk. For example, insurance companies rarely get into trouble with motor insurance business. This is because:

- motor insurers have learned exactly what information to collect to evaluate the risk to them of insuring different categories of vehicles or drivers;

- there is abundant information around on incidents and claims;
- they have systematized, repeatable processes in place to price policies and write exclusions that control their exposure;
- they can track whether these processes lead to profitable business over time;
- the vocabulary, mechanisms and procedures for measuring and managing risk are built into the fabric of the organization – and everyone complies with them.

Their success enables them to predict the likelihood of suffering claims and their magnitude with sufficient accuracy for decision makers. This is the purpose of any risk management process. Thus their practices provide a solid starting point for looking at how to manage *information risk* and other areas of *operational risk* well.

What is 'information risk' exactly?

Information risk can be defined as the 'chance or possibility of harm being caused to a person or organization as a result of a loss of the confidentiality, integrity or availability of information'. This definition has stood up to inspection for many years and has been widely adopted. It can be applied to all types of information and all means of capturing, storing, handling or transmitting it. Its use it therefore strongly commended.

How well is information risk managed at the moment?

So how well is information risk managed at the moment? Just going about your normal day-to-day life will tell you that the answer is 'not very well'. Systems go down, process information incorrectly and disclose it to the wrong people so often that it's part of the day-to-day reality of modern life.

To take a couple of incidents at random, a UK town council recently managed to publish a list of 'safe houses' for victims of domestic violence on its public website – a shocking violation of victims' confidentiality; and a glitch at the UK's main air traffic control centre led to flights being cancelled at London's busy Heathrow airport – less shocking but still pretty irritating for the travellers whose flights were cancelled or delayed.

To put the likelihood of suffering a major 'information incident' on a quantitative footing: in leading companies there is over a 50 per cent chance of a business-critical system suffering a major incident like this a year. Modern public and private sector enterprises will be supported by tens, hundreds or thousands of such systems, which is why major glitches are so evident to employees and the people who rely on their efforts.

Detailed statistical analysis reveals that the harm caused by such incidents can be minimized simply by adopting good practice (eg testing that back-ups can be restored successfully within the critical timescale of a business application, rather

than just assuming they can). Controls like these can slash the chance of suffering a major incident – and often cost little or nothing to implement. So why don't people adopt them? The answer is that:

- Security people often focus on threats like hackers and viruses rather than the more mundane and far, far more common types of event (eg human error) that lead to a loss of confidentiality, integrity or availability. The effect is to unbalance efforts to guard against incidents.
- There are too many controls that need to be in good shape for any one person to focus on all of them, so key weaknesses are often overlooked.
- There's no real consensus about what 'good practice' is.
- Increasingly, systems are connected to other systems, so weaknesses in one can foul up another.
- 'Ownership' of individual systems is often unclear – and 'owners' don't really know how to manage risk down.

The net effect is that business-critical systems that support leading organizations tend to have controls that are in 'variegated' condition: typically, in great shape in a few control areas, weak in other equally critical areas and 'average' in the rest.

Why information risk is so needlessly high?

Detailed inspection of the controls applied to thousands of systems and their experience of incidents shows that to drive risk down a very different pattern of controls is essential. Specifically, controls need to be in pretty good condition across the full spectrum of control areas. This is *the* key finding from a massive programme of research into what makes controls effective.

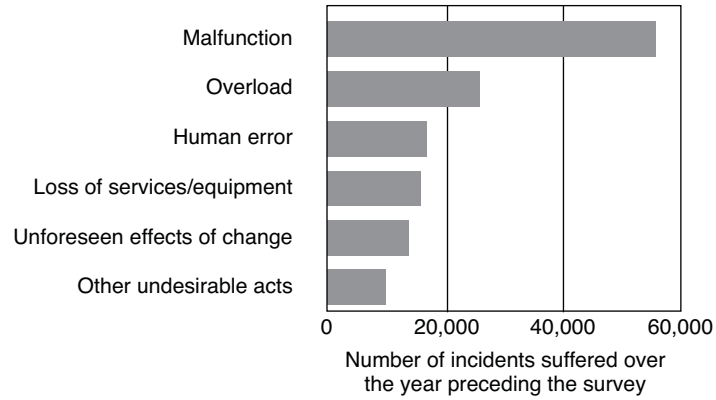
About 10 per cent of business-critical systems that support leading organizations have controls in this condition. That's why information risk is so high.

Figure 4.1.1 shows what sorts of incidents actually lead to a loss of confidentiality, integrity or availability of information and why getting controls into 'pretty good all-round condition' is worthwhile. The four charts in Figure 4.1.1 show that incidents are disturbingly common and, while most have minor impact, some can have very serious consequences. The cumulative effect of such incidents erodes profits and makes enterprises underperform.

Benefits of driving risk down

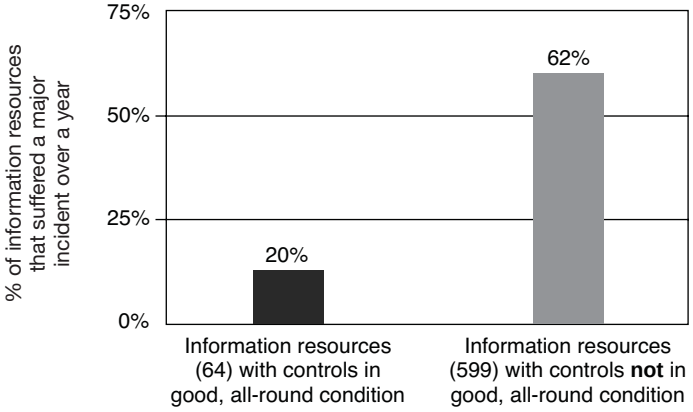
By getting controls in good shape, organizations can substantially reduce information risk. They can also significantly improve their bottom line, since good controls reduce the chance and financial impact of major incidents, and cut the number of minor incidents suffered day to day and the inefficiencies that go with them. Thus the benefits of driving risk down are substantial.

Accidents are by far the most common type of information incident suffered over a year



Source: Citicus analysis of 139,000 incidents affecting 558 'live' information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.

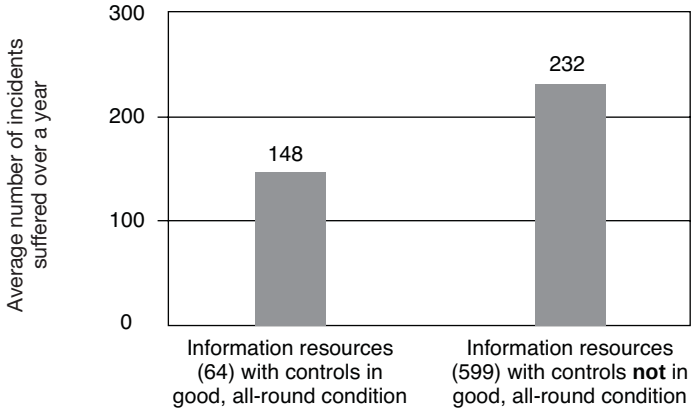
Control weaknesses massively drive up the probability of experiencing *major* incidents.



Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.

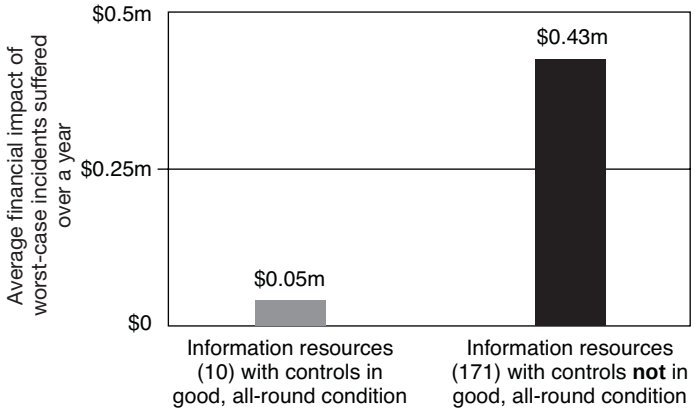
Figure 4.1.1 Statistical insights into information risk

You can expect to suffer substantially (36%) fewer incidents when your controls are in good, all-round condition.



Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.

Where controls are in good, all-round condition, the average financial impact of worse-case incidents is only a fraction of what it is elsewhere.



Source: Citicus analysis of 181 worst-case incidents affecting 181 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information status survey.

Figure 4.1.1 continued

Causes of failure in managing information risk down

To get the benefits, you have to go about managing risk in the right way, and avoid the pitfalls that lead to failure.

As part of the research we've carried out, we've examined factors that cause information risk management initiatives to fail and to succeed in a wide variety of case-study organizations.

Key causes of failure

Here are the key things to avoid:

- inability to measure risk *objectively*;
- overly complex approaches that yield results business people don't believe in or understand;
- turf wars between proponents of competing risk methodologies;
- lack of tools to automate the process in a reproducible way;
- lack of cooperation on the ground;
- lack of resources to drive and run the risk management initiative;
- immature processes and reporting structures;
- weak programme management;
- questionnaire fatigue.

Each of the above is a potential 'programme killer' – but an *inability to measure risk objectively and in business terms* will bring any programme into disrepute, so that's possibly the most crucial one to get right.

Secrets of success

The secrets of success that emerged from the research we conducted are strongly reinforced by our experience in helping organizations of different types and sizes around the world manage risk successfully. They can be summarized as follows:

- Before you start, gain top management commitment.
- Get the organizational arrangements right.
- Have a strong, personable programme manager who has the drive, skill and experience to deal with business, people, and technical issues as well as to drive a company-wide programme.
- Base your approach on a crystal-clear definition of risk that addresses what needs to be protected and both the magnitude and the probability of harm.
- Measure the five determinants or indicators of risk that your insurance company considers when assessing the risk posed by drivers (criticality or value at risk; status of controls; special circumstances, eg complexity or scale; experience of incidents; and the business impact of incidents).

- Ensure the risk management process is constructive rather than blame oriented (otherwise people will evade or sabotage the programme).
- Ensure the risk management process is continuous rather than a series of one-off evaluations (so improvements can be tracked over time).
- Make risk management a *personal* responsibility of individual business 'owners' of your 'targets of evaluation'.
- Keep evaluations simple, efficient, objective and business oriented.
- Ensure the process is proportionate (when resources are limited it makes sense to focus them where they will have the greatest payback rather than spreading them evenly across everything).
- Produce meaningful results that capture the attention of busy decision makers – particularly business 'owners'.
- Introduce an element of competition between facilitators and 'owners' (eg by publishing risk league tables).
- Cause pressure to filter down so it motivates others to act (eg by showing dependency risk).
- Embed risk management into the fabric of the organization (eg make criticality assessments become part of project approval and procurement processes).

Putting principles into practice

Over the last eight years, our company has had extensive experience with putting these principles into practice in a wide variety of organizations operating in virtually every country in the world. Figure 4.1.2 gives a quick overview of the constructive evaluation process we advocate.

Our software enables a busy business 'owner' to complete a *criticality assessment* of an information resource in minutes in a coherent, business-oriented fashion, using a company-wide 'harm reference table' to highlight the types of harm that need to be considered. Because the approach is systematized, hundreds of such evaluations can be completed in two or three weeks; thousands take a bit longer (say three to four months).

Criticality assessments focus not on the probability of a harmful event or how it might be caused (which business 'owners' are not equipped to assess through their own experience). Instead, they assess the *worst that could happen if confidentiality, integrity or availability were to be compromised for whatever reason*. This ensures that the assessment of risk takes the worst that can happen into account, which is crucial.

Once criticality has been assessed, the programme manager can decide which information resources warrant a full evaluation of risk using a *balanced risk scorecard*. Such evaluations can be conducted at a high level or in more detail using the scorecard plus subordinate checklists, thus achieving proportionality in the depth of each evaluation.

The balanced risk scorecard verifies the assessed *criticality* of a 'target of evaluation' and establishes the status of its *controls* – this is the factor that mainly determines the likelihood of suffering incidents in future. But it doesn't stop there. It also assesses three other factors that highlight or otherwise indicate risk, namely:

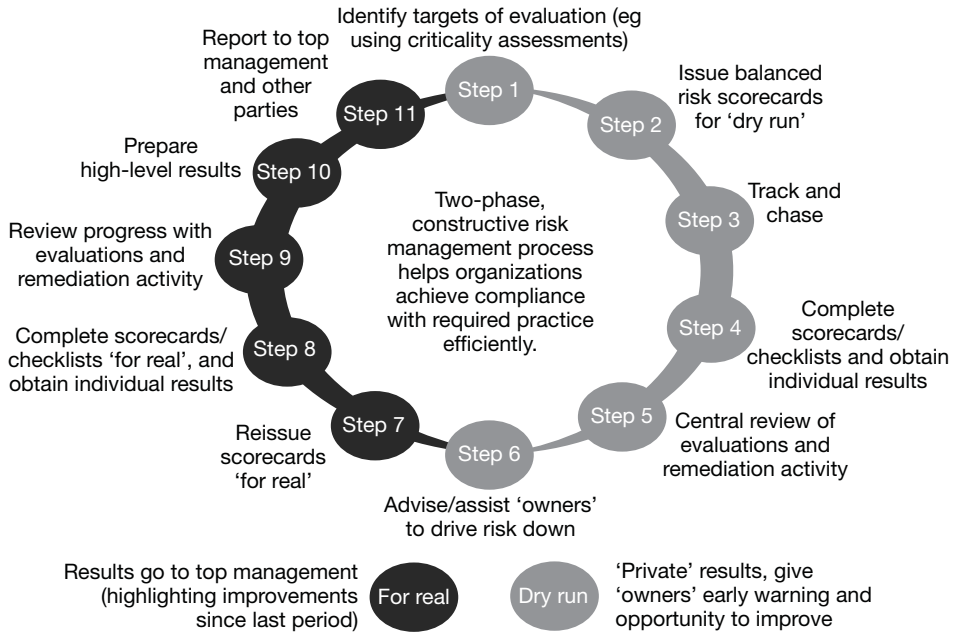


Figure 4.1.2 A constructive evaluation cycle

- *special circumstances*, such as immaturity, scale or complexity (these increase the likelihood of suffering incidents);
- *the number of incidents* suffered over the last year (these provide an independent indication of whether controls are effective and are highly predictive of the chance of suffering major incidents in future);
- *the business impact of such incidents* (these provide a business-oriented indication of what incidents have cost the organization so far).

By design, these five factors echo the ones your insurer considers when setting the price of your car insurance (eg the value of your car, its roadworthiness, your age, your occupation, where you live, and your history of driving offences and claims). Thus measuring them yields a sound, factual picture of the risk posed by individual systems, which can be aggregated for decision makers.

A full evaluation like this is usually conducted initially at a three-hour risk workshop and can thereafter be updated in minutes (eg as improvements are made that reduce measured risk).

For completeness any serious risk management programme worthy of the name also needs to keep track of remediation activity, which our approach does, and show 'owners' of individual systems the risk status not just of their own system but of the other systems it is linked to. This can be visualized using a dependency risk map such as the one shown in Figure 4.1.3.

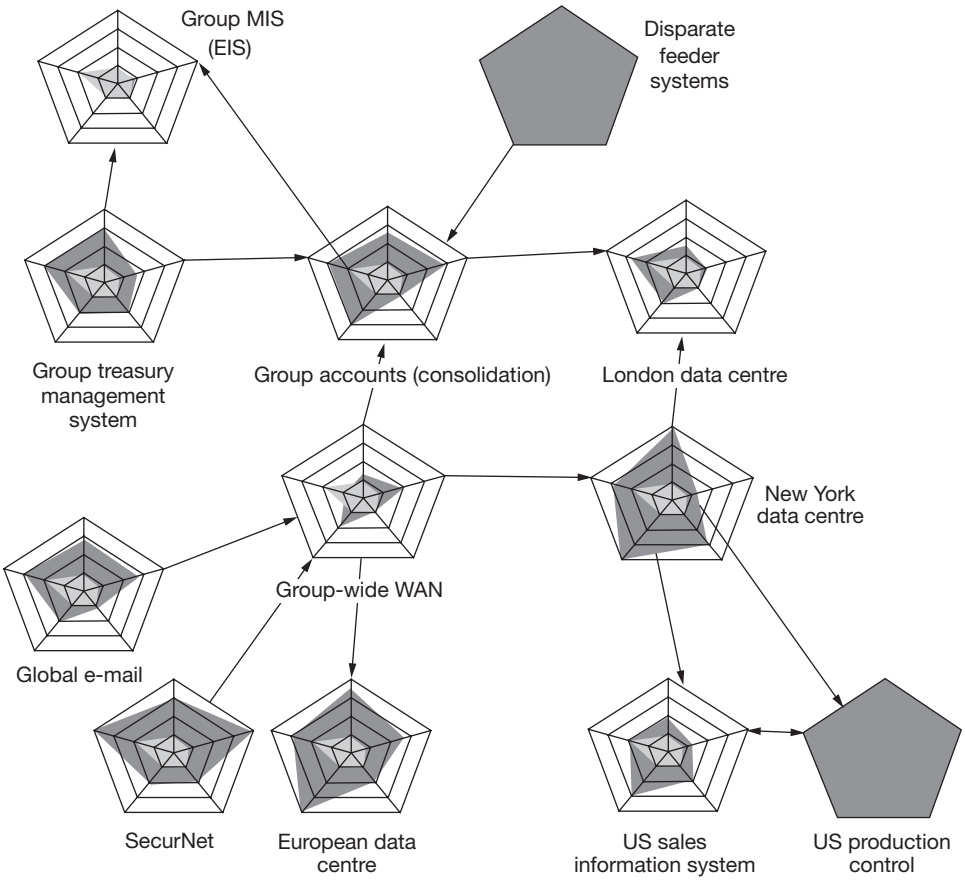


Figure 4.1.3 A dependency risk map

Benefits of a sound approach

Since we started in 2000, our software has been used to carry out thousands of evaluations, in over 150 countries. Typically, the process of managing information risk starts with a 'discovery' phase, which of itself delivers many benefits.

> When we started, we didn't know whether we had 6,000 or 60 business-critical systems in Germany alone and had only very patchy information about their 'owners'. Now we know exactly what's critical we can focus attention on the ones that matter most.
>
> Risk manager, global consumer products company

Our customers are also finding that sound risk data help in deciding which systems should be co-located and which kept separate and the precise grade of service each one needs. This can save millions when services are delivered by an outsource partner.

Extending the approach to other areas of risk

When we started, our focus was on developing a business-oriented and scalable method of evaluating information risk systematically, which could be successfully applied by organizations of all types and sizes. Since then, we've found that the same principles can be applied to other areas of operational risk; it is just the fine detail of the process that needs adjusting.

By 2008, we found that our customers and prospects were excited about applying the same approach to multiple areas of risk and focused in particular on information risk plus three other areas of operational risk, namely:

- *supplier risk*;
- *site risk* (this covers security and health and safety of employees, visitors and neighbours);
- *privacy of personal data* (this is of ever-growing importance as regulations tighten and more and more breaches emerge).

The reaction we've seen is telling us that there is pent-up demand for a method of measuring and managing risk based on sound principles. We hope this chapter has given you a good feel of what these might be and helps you plot a route to success that avoids the pitfalls others fall into.

SOME THINGS YOU CAN'T BRING BACK IN YOUR SUITCASE.

Isn't the real excitement of travel having experiences that still enthral you? At InterContinental we use our expert local knowledge to help you enjoy exactly what makes a destination unique. In Hong Kong, for example, we can get you front row seats for one of the world's most iconic skylines, a sight no one should leave without experiencing.

Do you live an InterContinental life?

For more details or to make a reservation, please call +800 1800 1800 or visit intercontinental.com

INTERCONTINENTAL®
HOTELS & RESORTS

4.2

Integrating security risk management into mainstream business

John Ludlow, Global Risk Management, InterContinental Hotels Group

Background

Historically, security management in hotels could be characterized as fragmented, uncoordinated and reactive. It was certainly not seen as central to the success of the business. Given the largely static security environment of hotels in the past, this approach was, however, probably effective enough in mitigating the security risks that confronted international hotel brands. As hotels themselves shifted from being largely individually owned to the international brands that currently populate business travellers' lodging options, sets of brand standards emerged that attempted to guarantee a consistently good hotel experience for frequent travellers across the brand. In most cases, however, the move to brand consistency had little impact on security management, which had tended to become somewhat detached from developments elsewhere in the hotel sector and had become something of an

organizational anachronism (even if still reasonably effective in responding to routine security issues).

At the same time, the risk environment in which hotels operated was changing. Developments in the political, economic, social, technological and legal spheres were presenting new challenges as well as opportunities for hotel security risk management. The most salient element of this shift was the emergence of international terrorism, and this was made abundantly clear when al Qaeda in Iraq carried out simultaneous suicide attacks against three international hotels in Amman in November 2005. This was not, however, the only element in the security spectrum that had changed. The end of the Cold War had shifted the global security paradigm in other areas that now affected hotel risk management, such as identity theft and money laundering. National catastrophes such as the Asian tsunami and Hurricane Katrina in recent years also challenged the security departments of international hotel brands to prepare and respond to significantly higher-impact events. Similarly, security (and risk) departments became the first port of call for senior hotel management when faced with events such as the conflict in Lebanon in 2006 and 2007 and newly emerging threats such as cyber-crime.

It became clear to IHG during this period that the traditional, fragmented and reactive approach to hotel security was not able to provide the desired level of sophisticated protection against a rapidly more complex and ambiguous threat environment; nor was it well placed to meet the increasing expectations placed on hotels to prevent, prepare for, respond to and recover from major risk incidents. IHG therefore carried out a far-reaching analysis of its existing security capacity set primarily against the benchmark of the international terrorist threat and developed a strategy of threat-based security risk management. The consequences of this study were to have a profound effect on the company's perception of both the security risks and the consequent mitigation strategy.

New security strategy

Perhaps the most significant aspect of the study was the conclusion that there was indeed a need for a global security risk strategy. This had not existed before and in itself was somewhat ground-breaking.

Looking at the contents of this strategy, it is worth noting that the first outcome was the requirement to understand the nature of the threats that surrounded the business and to assess their likely probability and impact. It had been concluded that a threat-based approach had been largely unnecessary in the past, since security threats tended to be of the high-volume, low-impact type, such as staff pilfering or anti-social behaviour. These were largely static in nature, and understanding them was largely a given for each hotel. There was no need for constant review of these low-impact threats, since they did not change substantially from one year to another. Similarly, there was little need for a differentiated countermeasures strategy: mitigation of basic routine security risks had evolved over

many years at a subconscious level and could be characterized as the 'locks, safes and bouncer' set of measures. Within the international hotel business these measures were generally well managed. Supervision of them could be adequately provided and addressed at the local level with the help, typically, of former police officers, benefiting from their local contacts and knowledge of local petty crime.

However, it was clear that this approach could not be scaled up to meet the newer, more complex threats. Neither, and crucially, did it make financial and business sense. While, in the past, room thefts globally could be countered by, say, the adoption of a uniform approach to guest room door locks, it made no sense, economically or otherwise, to adopt in every hotel standards of physical security to counter international terrorism. The burden on the business, both financial and aesthetic, would be unacceptable. The options therefore were to do nothing and trust to fate or adopt a differentiated approach of introducing countermeasures based on an assessment of the relative security risks at each hotel. And this could be achieved only by adopting a threat-based approach.

The question was where to find suitable models to emulate. The answer was to turn to the world of government in general and the intelligence community in particular, since the latter had developed over many years (some would argue centuries) a philosophy of national security based on constantly and systematically assessing threats and formulating appropriate and proportionate countermeasures.

Following the process of internal review, therefore, the findings were summarized as follows:

- Security risk requires a new approach that is similar to but different from the management of other operational risks, such as fire safety.
- Security risk management has to deal with changing and emerging *dynamic threats* rather than more static *hazards*.
- Direct threats are caused by individuals and organizations that have both the *intention* and the *capability* to *harm* our *assets* (this includes staff, guests, property, reputation, etc). These intentions and capabilities are *constantly* changing and need *constant monitoring*.
- There needed to be a better understanding of *indirect threats*, that is to say conditions in the hotel environment that amplified the risk associated with direct threats (eg high VVIP guest ratio, proximity to a US embassy) or reduced the hotel's ability to respond to such direct threats (eg overconfidence in local police capabilities, lack of an information security policy).
- Security risk management therefore has to be able *constantly* to *identify threats*, *assess the associated security risks* and *develop proportionate measures* to counter and prevent such threats as they emerge and change.
- Security management has to *make sense* to the business and support and be *integrated with its strategic objectives*.
- It was clear that it was not necessary, desirable or financially practical to introduce a uniform set of physical security standards to cover all eventualities. There had to be a realistic and cost-effective matching of countermeasure responses to each threat.

Key features of the new approach

So much for the history; of more interest to the current chapter is how this translates into a workable strategy and practice for the hotel industry in the 21st century. The strategy that emerged from the internal assessment contained the following key features:

- It was underpinned by the concept of *threat assessment*: this would produce a systematic requirement for assessing a range of political and security threats. It would operate both at the *strategic* level to understand medium- and long-term threats to the global business and *tactically* at the hotel level where individual threat assessments would be conducted for all higher-risk hotels.
- It was an *intelligence-led* approach to create:
  - insight and understanding of the global threat environment as well as the tactical threats to each hotel;
  - a forward-looking view to place both the global business and each hotel in a position proactively to avoid, prevent and prepare for threats.
- It sought opportunities for *cooperation and collaboration* wherever possible:
  - with security and intelligence agencies;
  - with corporate security professional bodies;
  - with other forward-looking hotel brands in non-competitive areas of security to increase the hotel sector's security values;
  - with client corporate security departments to create security partnerships.
- It recognized the *human factor* as the key to success:
  - at the corporate head office level: the recruitment of a small team of security and intelligence professionals with a balanced range of backgrounds;
  - at the hotel level: networking of previously fragmented security managers and the identification and training of security champions to translate the new threat-based approach for more traditional hotel-level security teams.
- It was a global process to classify each hotel into one of *four threat categories* and then to carry out individual *threat and vulnerability assessments* on each of the higher-risk hotels. The results of this would produce:
  - a set of affordable countermeasures and responses for each hotel according to its business profile and threats;
  - more generic countermeasures applicable to types of threats or regions (eg measures to counter vehicle-borne bombs that would not conflict with the desired guest experience).

In Figure 4.2.1, the overview of threat-based risk management is illustrated diagrammatically.

Threats to hotels

The threat environment of a global hotel business is both complex and ambiguous. It was clearly necessary to reduce this complexity to a manageable level. Therefore,

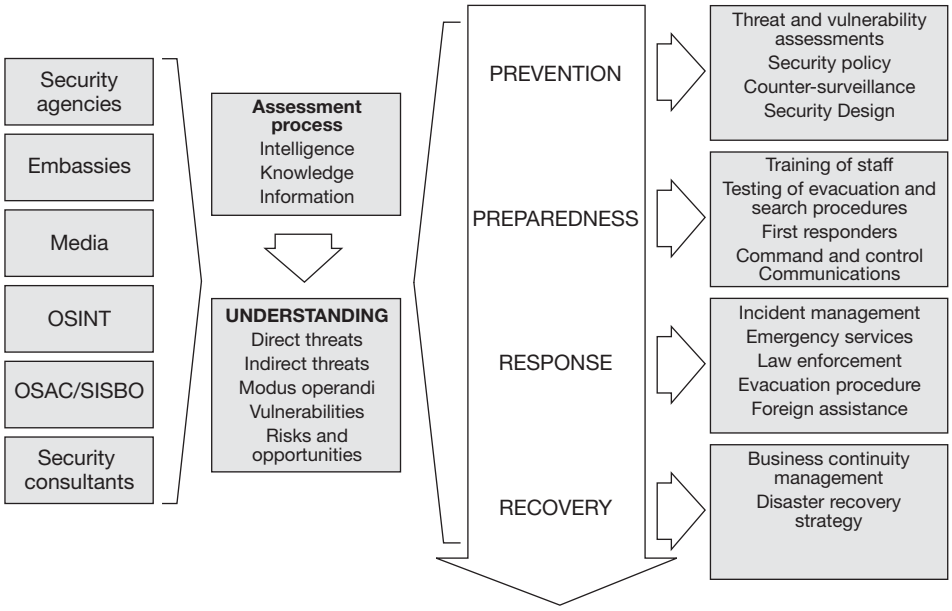


Figure 4.2.1 Threat-based security risk management overview

after identifying and analysing all security threats to IHG's hotel operations, it was agreed that they could be placed into one of three categories. Each of these categories had a set of common characteristics and a common probability/impact ratio and required a common set of basic countermeasures and responses on which to build more tailored, individual responses, summarized in Table 4.2.1.

Table 4.2.1 Analysis of threat categories

Threat level	*Threat type*	*Impact*	*Probability*	*Critical features (examples)*
Level 1	War/civil war	High	Low	Security design and engineering
Level 1	Terrorism	High	Low	Counter-surveillance capacity
Level 1	Insurgency	High	Low	Intelligence support
Level 2	Political violence	Medium	Medium	CPTED
Level 2	Civil unrest	Medium	Medium	Crisis management testing
Level 2	Organized crime	Medium	Medium	Fraud protection
Level 3	Crime	Low	High	E-learning
Level 3	Anti-social behaviour	Low	High	Extensive SOPs
Level 3	Petty crime	Low	High	Reporting integrity

An IHG approach

In 2006, IHG embarked on a counter-terrorist security programme that evolved to contain the following key elements:

- A global survey of all hotels resulting in a categorization of each hotel according to a set of criteria into one of *four major risk categories*.
- A programme of *threat and vulnerability assessments (TVA)* for each hotel in the higher-risk categories.
- Constant *horizon scanning* using intelligence techniques and inputs from a variety of commercial and government sources. Continuous security intelligence collection and analysis aimed at notifying operators of emerging and changing threats, both to maintain awareness and to inform a system of four incremental security alert/response states.
- A schedule of *follow-up consultations* by telephone and by visit where judged necessary to ensure implementation of TVA recommendations.
- The development of *security management training* courses:
  - residential courses for security managers in high-risk locations focusing on Level 1 and 2 threats;
  - online e-learning for low-risk locations focusing on Level 3 threats.
- A set of *minimum security standards* for hotels in the lower-risk category. This was further subdivided into a set of standards and responses by size and brand.
- The creation of a *technical master security plan* that contains detailed guidance and specifications on technical security measures both for new hotel building programmes and for upgrading existing hotels. The guidance and specification were scalable in line with the three threat levels.
- The introduction of *security design and engineering* to create new hotels that were 'secure by design' and to provide security engineering solutions based on latest government guidance and testing for existing higher-risk sites.
- *Web-based sets of procedures and guidance* for the full range of risks associated with security threats and natural or human-created disaster. These include up-to-date advice and detailed instructions from security experts as well as from government agencies. The web-based structure should enable swift updating and expansion.

Threat and vulnerability assessments (TVA)

Given its central role, it is worth expanding a little on the TVA process. Based on a well-established process in government security (and translated in different forms into the corporate security world), the IHG TVA process is a key tool in implementing the security risk strategy.

One of the principal objectives of the TVA process is to engage the hotel in thinking about its threat environment, in understanding the risks (including the upside risks) and in agreeing a programme of improvements. In this, the process differs significantly from an audit. The TVA does not seek to judge the hotel's

performance against a set of standards but to create a partnership for reducing risks and exploiting the consequent business opportunities.

The TVA process therefore takes place over an extended period of time and in distinct phases:

- *Phase 1:* selection of the hotel based on its ranking in the global threat assessment.
- *Phase 2:* contact with the hotel to inform it of the process and the issue of a hotel security inventory (HIS). This is a form of questionnaire passed to hotel management in which an inventory of all aspects (human, technical and policy or procedures) of hotel security is recorded. It later serves as one of the core reference documents for the hotel security manager, as well as providing an overview of current security measures and capability for the TVA adviser.
- *Phase 3:* a strategic threat assessment is carried out for each hotel, which looks at the full spectrum of threats that could potentially have an impact on the hotel. It includes potential and actual, direct and indirect threats, the political risk environment, externally originating threats, and natural and human-created disasters. This is submitted to the hotel for comment, amendment and agreement.
- *Phase 4:* having reached agreement on the details of the security threats, the TVA adviser carries out an on-site survey to identify existing vulnerabilities to the identified threats, assesses the risks on an impact/probability basis and suggests proportionate countermeasures and responses. This stage also seeks to engage the owning company and obtain its outline support and agreement.
- *Phase 5:* the detailed TVA report is submitted to all interested parties and agreement reached on the timetable for implementing recommendations along with the costing and budgeting approval.
- *Phase 6:* follow-up, review and support in meeting the timetable, and lesson learning.

Despite the initial misgivings of many hotel operators at what appears to be another form of head office audit and interference, most soon recognize the educational and supporting nature of the exercise and cooperate fully in the process.

Benefits

What does this mean for hotel operators and, importantly, the hotel guests? The benefits can be summarized as follows:

- *IHG corporate management:* confidence that major threats will be identified and mitigated in advance; no 'nasty surprises'; security risk management as an enabler for operating in higher-risk areas; cost-effective use of capital and operating funds; reduced insurance premiums or cover based on better risk control.
- *Hotel operators:* specialist advice and support available where and when needed; a security risk management approach that makes sense to guests; capital expenditure on security justified by detailed threat and vulnerability assessments; better understanding of the hotel's threat environment, allowing

for targeted expenditure; security management as a contributor to sales; better access to local emergency and security services.

- *Individual guests:* a better guest experience where security levels make sense; guests feel secure in high-risk environments and are undisturbed by lower levels of security in low-risk environments.
- *Corporate guests:* the convenience of discussing required levels of security centrally instead of on a hotel-by-hotel basis; the assurance of dealing with a leading-edge approach; the confidence of knowing that corporate travellers will be protected in line with the local threats.

The author acknowledges with thanks the contribution of Robert Ashington-Pickett to the writing of this chapter.

Don’t let anyone
tell you that
the world is flat

www.koganpage.com

Fresh thinking for
business today

You’re reading one of the thousands of books published by Kogan Page, Europe’s largest independent business publisher. We publish a range of books and electronic products covering business, management, marketing, logistics, HR, careers and education. Visit our website today and sharpen your mind with some of the world’s finest thinking.

XL INSURANCE companies are chosen by the world's leading firms for the strength of our capital and the depth of our experience. Benefit from the quality and variety of our solution-focused products created to match your insurance requirements:

PROPERTY
Global All Risk Property Damage & Business Interruption | Energy & Construction All Risk

CASUALTY
Primary Liability | Product Recall & Tamper | Workers' Compensation | Global Public & Products Liability | Excess Liability

PROFESSIONAL
Directors & Officers | Employment Practices | Financial Institutions Bond & Crime | Investment Managers Insurance | Professional Indemnity | Side A | Trustees Liability

SPECIALTY
Aviation & Space | Environmental Liability | Equine & Livestock | Marine & Offshore Energy | Fine Art | Jeweller's Block | Cash In Transit

The XL Insurance companies have one or more of the following ratings: A (Excellent) by A.M. Best, A+ by Standard & Poor's.
Experience our strength: www.xlinsurance.com

XL INSURANCE
FUNDAMENTAL STRENGTH – CAPITAL AND PEOPLE

4.3

Avoiding the global compliance trap

Jonathan Post, XL Insurance

In the present turbulent financial climate, providing consistent and globally compliant risk management solutions to multinational corporations might not be first on risk managers' to-do list, but it is unlikely to be too far down it, either. In a survey by *Strategic Risk Magazine*, 67 per cent of responding corporate risk managers saw potential compliance default as a growing risk of globalization. How can international corporations obtain integrated and consistent cover worldwide while at the same time complying with local law and market practices and accessing local coverage and loss solutions? This apparent conflict can only intensify as multinationals turn to emerging markets to supply their service and manufacturing requirements, connecting on the way with unfamiliar legal systems, and regulators who may not be geared up for their needs.

Local solutions, global consistency

Local insurance policies will provide local market standard coverages and will generally be written in the local language and governed by local law. This approach gives the advantage of familiarity for local insureds, but it does not fit well with providing globally consistent coverage. So global programme (GB) insurers provide

an additional 'wrap-around' coverage, supplementing local policies to cover the differences in conditions and limits (DIC/DIL) between those policies and the master policy. Thus subsidiaries enjoy standard local coverages in a familiar language and terms – and, at the same time, the group's global risk manager knows that if a loss is covered under the master policy it will be covered worldwide.

So far, so good. But consider a United Kingdom based client purchasing a local policy for its foreign subsidiaries from a 'passported' EU insurer. The local policies purchased for those subsidiaries are not of identical scope to the parent's master policy, and may not be issued to the same limits. As we have seen, this is where DIC/DIL coverage fills in the gaps. But outside the EU the DIC/DIL coverage wrapping around the local policies is unlicensed, and may well be illegal. By receiving unlicensed cover, subsidiaries might be acting as illegally as the insurer providing it.

Until recently, this disadvantage to the GP business model was considered to be outweighed by the advantages of global reach and consistency of cover. Besides, with a few exceptions, regulators outside the EU had not necessarily appreciated, or cared, that cover in excess of local policies was being given. But recently regulators have been taking greater interest in the potentially non-compliant provision of DIC/DIL cover – perhaps because they feel local tax authorities are missing out on local premium taxes. DIC/DIL coverage under an unlicensed carrier's master policy is no longer a risk-free product, whether for insurers, brokers or insureds.

XL Insurance has been at the forefront of insurers' attempts to resolve this issue, which it does in the following ways:

- If we abide by certain basic principles, we may provide unlicensed cover *into* many countries, without falling foul of regulatory restrictions on carrying out unlicensed insurance operations *in* those countries.
- If unlicensed insurance cannot legally be given to a subsidiary in a particular country, then we do not insure that subsidiary.

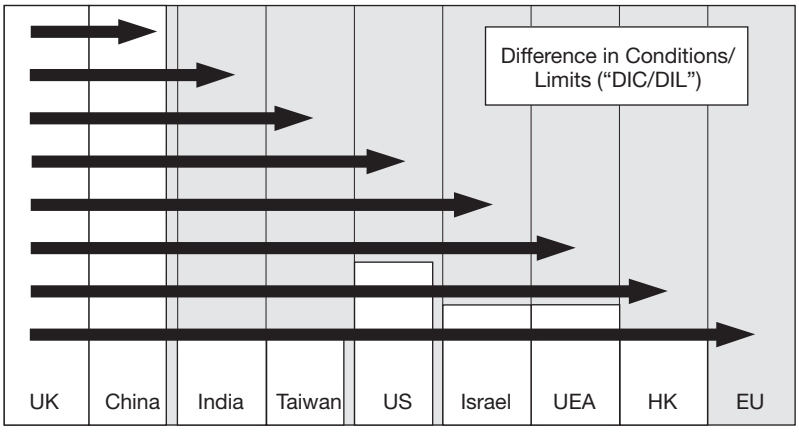


Figure 4.3.1 Global programmes – the licensing issues

- If we cannot legally insure a subsidiary, we insure the financial interest of the parent in its uninsured subsidiary upon the terms and conditions of the master policy.

That sounds simple enough in practice, but as ever the devil is in the detail.

'Permissible unlicensed' cover: asking the right questions

To ask 'Do we need a licence to offer insurance in Country A?' is, generally speaking, not helpful, because the answer will, almost invariably, be that 'Carrying on insurance business in Country A requires a licence.' It is much more useful to ask this: 'Which activities by an unlicensed insurer constitute a breach of applicable law in Country A, and which do not?' Or, put another way, 'Can we offer cover and pay claims into Country A in such a way as not to breach the relevant laws?'

The paradigm for this approach is the United States. While individual state laws provide that only domestically registered insurers may transact the business of insurance within the state, and impose strict penalties on both non-compliant insurers and brokers, federal case law, binding upon all the states, provides that where an insurance transaction takes place outside a state then that state's regulator has no jurisdiction over it. In practical terms, if the prospective insured plays no part in the placement of its insurance or, if it does, travels outside its home state to – in the jargon – 'directly procure' it from an 'alien unlicensed insurer', then its home state regulator cannot object.

For singleton insureds, the potential inconvenience of direct procurement will often lead them to purchase cover from domestic markets. But a US subsidiary of a non-US parent will generally have its cover centrally negotiated and purchased by its parent's risk manager, and does not participate in the insurance transaction. So direct procurement fits with the global programme centralized purchasing model, allowing a US subsidiary to receive cover from its parent's insurer on an unlicensed, but perfectly permissible, basis.

With the US model in mind, we wondered where else it was possible to provide cover into a country without breaching laws applicable to insurers operating in that country. Our research into over 170 countries indicated four general categories:

- Unlicensed cover is unconditionally allowed (very rare).
- Unlicensed cover may be allowed provided the insured initiates contact with the insurer and the transaction takes place outside the jurisdiction (relatively common).
- Unlicensed cover may be allowed if cover was sought from, but cannot be provided by, the domestically licensed market (relatively common).
- Unlicensed cover may be allowed if the local regulator gives advance permission (common, but in practice difficult to achieve).

These broad categories together account for a significant proportion of the countries researched, and we now know where conventional 'non-admitted' cover was actually, or potentially, compliant all along. We refer to this as 'permissible unlicensed' coverage.

Permissible unlicensed taxes

Licensing is not the only hurdle. Where we provide cover on a permissible unlicensed basis, then to achieve substantial compliance we also need to know where we or our clients face a tax obligation as a result.

For an example, let's go back to the United States. Providing directly procured cover makes the US insured liable for direct procurement tax, payable at state level. Rules vary from state to state, but a general principle emerges: within a certain number of days after inception of the directly procured cover, the insured must report the existence of the cover to its state insurance regulator, and pay a tax variously rated at between 2 per cent and 4 per cent of the premium.

This pattern repeats itself across the globe: receiving cover on a permissible unlicensed basis will sometimes expose the insured to tax. Generally this tax is not high; the trick is to know where it applies and how to pay it. Our research has identified those countries where such a tax applies, and we can pass this information to our clients. Of course, verification, registration and payment itself are up to the insured and/or its local tax adviser.

Financial interest cover

Our research has also showed that there are countries where, no matter how many different ways you ask the same question, the answer will always be 'no'. Sometimes it is illegal to purchase insurance cover other than from a domestically licensed insurer. Sometimes all insurance must be purchased through a licensed insurance broker, which may itself place risks only on the domestic market. Sometimes any insurance capable of responding to any loss occurring within that country must be placed with a domestic insurer.

Where the permissible unlicensed route is barred in this way, cover provided under master policies is potentially illegal, with consequences not only for insurers (which the local regulator will find it difficult to penalize) but also for insureds (a lot easier – because they, by definition, will be within the jurisdiction). We have set ourselves a simple rule: we will not give cover where it would be illegal to do so. But that does not necessarily prevent us from insuring our clients' interests across their entire global operations.

How do we resolve this? We start from the proposition that the parent company of a group of companies has an economic, operational and strategic interest in the well-being of its subsidiaries, and will be adversely affected by events that adversely affect those subsidiaries. A parent that has invested its and its shareholders' capital into establishing a global presence through its subsidiaries must be presumed to have an interest in retaining or reinstating that presence, an

interest that can be compensated in monetary terms. So, in cases where a parent has subsidiaries that cannot legally be covered, we do not insure those subsidiaries, but we insure the parent's financial interest in those subsidiaries.

English and some other common law systems require that a person must have an 'insurable interest' to take insurance against the possibility of an adverse event. It is the presence of that insurable interest that distinguishes a contract of insurance from a pure bet. Is financial interest coverage a bet? For the answer, we go back to classic judgments of the late 18th century; for a person to have an insurable interest in a particular thing, he or she (or it) must stand in relation to it so as to enjoy a benefit from its preservation or to be prejudiced by an adverse occurrence affecting it.

We and our external legal advisers believe that the parent company of a group of subsidiary entities has such an interest in its subsidiaries; that interest may arise out of its ownership of those entities, but equally might arise out of the fact that those entities fulfil a certain role for, and add a certain value to, the group as a whole. If a subsidiary is adversely affected by a loss, its ability to make an operational or strategic contribution to the group is likewise affected.

Agreed valuation of financial interest loss

Except in the most straightforward of circumstances, a financial interest loss may be difficult to quantify, leading to a lack of certainty. But certainty and consistency are not optional in today's market. Clients want consistency of cover. If they are to be insured in respect of their uninsured subsidiaries, they want to be indemnified on the same basis as those subsidiaries would have been if they had been insured. Likewise, insurers do not want to pay the parent where, if they were insuring the subsidiary itself, a loss would not be covered.

We need to fix the scope of coverage of the policy and the level of indemnity of the parent with sufficient precision to satisfy the need for 'contract certainty', and in such a way as to preserve global consistency of coverage and limits. We achieve this by means of a valuation clause in the master policy, which does not simply fix the value of the insured's interest; it sets out the agreed basis for calculating the insured's loss. So the parent's loss to its financial interest will be calculated on the basis of the amount that the subsidiary would have received if it could lawfully have been insured on the terms and conditions of the master policy.

In this way, a group 'virtual cover' is given that will equate in monetary terms to the coverage desired. Although there is little settled law on the question, external legal advice from our producing countries has a general theme: such an agreed valuation clause will be set aside only where the intention of the parties was fraudulent or where the indemnity principle is very substantially breached.

Repatriation of claims funds

Financial interest cover is simply another cover under the master policy, so there are no issues of payment of local 'non-admitted' taxes, as with permissible unlicensed

coverage. However, tax issues arise upon repatriation of claims funds from the insured parent to its uninsured local subsidiary.

Remember that, where financial interest cover is given, the parent is entirely free to decide what to do with the claims proceeds it receives. It may repatriate them to its uninsured subsidiary, sustaining the original uninsured loss, but it may just as well direct them to a different, or a new, beneficiary, or keep them itself. The uninsured subsidiary is dependent upon its parent's generosity. Where the parent does elect to repatriate those funds, it will have to decide how this transfer is to be achieved, because the funds are no longer 'insurance' but a gift, which may be taxed either in its hands or in those of the subsidiary.

This issue already arises in 'conventional' global programmes, but in a different context. Under a conventional global programme, insurers know that some claims may not be capable of being paid direct to the insured subsidiary, because, not to put too fine a point on it, they should not be insuring that subsidiary in the first place. So claims are paid to the parent company, even though the insured entity is its subsidiary, and the parent must then transfer those funds, which will often be taxed en route. To sweeten that pill, insurers have offered 'tax indemnity clauses' designed to ensure that, where the insurer has to settle a subsidiary's claim centrally, it will pay it a sum that, after tax deductions on transfer, will equate to the subsidiary's loss. Since the route is taken because the insurer does not want to be caught offering illegal unlicensed insurance, that seems fair enough.

Compare that, however, with the situation where financial interest cover is given. The uninsured local subsidiary has no right to be indemnified for its uninsured loss and, if its parent does decide to give it part or all of the parent's own claims proceeds, the subsidiary must treat it for what it is – a gift. Our high-level tax advice into the tax treatment of such a gift in the primary jurisdictions where we will offer financial interest cover indicates that, properly structured, such repatriation of claims proceeds may be minimized and in certain circumstances could be tax neutral. So while tax may well become payable upon a simple 'route 1' transfer, a little care and pre-planning could mitigate or even avoid that liability.

Conclusion

There is no 'magic bullet' that will automatically provide a single compliant solution to today's global programmes. Neither is there just one correct way of doing things. Rather, insurers and risk managers must work together with a suite of solutions to mitigate regulatory risk while 'leaving what ain't broke, fixed'. Permissible unlicensed cover and financial interest cover are just two of the tools we can use.

Of course, we cannot wholly guarantee compliance. It is the regulator's prerogative to move its goalposts and update legislation. But what we can say with some certainty is this: that there is a problem; that it is not going to go away; and that to take good-faith steps to address the issues, and to pay taxes when due, will probably stand insurers, the insured and brokers alike in better stead than continuing to pretend that the issue does not exist.

Close Credit Management

Credit Management - it's what we do

At Close Credit Management we provide our clients with the confidence and certainty of reliable cash flow to pursue their business objectives.

With over 37 years collections experience and as part of the UK's largest independent merchant bank, why take the risk of entrusting your credit management needs to anyone else?

- Pre Due Calling
- Early Arrears Collections
- Full Outsource Capability
- Collection Letters
- Inbound and Outbound Calling
- Scheduled and Unscheduled Field Visits
- Full Legal Process

To find out more, please call **0845 313 0864** to arrange an appointment with one of our Business Development team.

www.closecm.co.uk

At Close Credit Management we provide our clients with the confidence and certainty of reliable cash flow to pursue their business objectives.

With over 37 years collections experience and as recipients of the inaugural Commercial Debt Collection Agency of the Year award, we work with clients across a broad range of market sectors developing bespoke and productive collection services.

Our aim is simple – *to collect as much as possible, as quickly as possible as efficiently as possible.*

We offer a full, in-house range of collection and credit management tools providing;

- Development and delivery of effective **collection letter** mailings
- Management and execution of **inbound and outbound calling campaigns**
- Provision of both **scheduled & unscheduled home visits to** fully understand customers' circumstances and negotiate satisfactory solutions
- Internal management of the full **legal** process through to judgment and enforcement

As holders of the ISO 9001:2000 accreditation for process improvement and via our use of Six Sigma methodology, we will tailor these services to drive an increase to your bottom line.

Part of the FTSE 250 listed Close Brothers Group, we adhere to the relevant regulatory requirements including CCA 2006 and the principles of Treating Customers Fairly, ensuring we deliver both the service and performance you would expect from a division of the largest and most respected merchant bank in the UK.

As leaders in our field, we understand the importance of evolution. No business can afford to stand still. What worked well last year may not necessarily work well this year, but the better we understand your business, the better we can tailor and develop our services to your specific needs.

As independent specialist negotiators Close Credit Management are able to ascertain information about your customers that you may not be able to access, enabling you to understand their current situation and realistic future financial position. With a network of fully employed field based negotiators we offer nationwide coverage and deliver significant results within very tight timescales.

Our staff are our key and we understand the benefits for both of us in developing long term partnerships. We believe that by understanding your business we can develop a range of collection strategies to deliver the performance and results that your business requires, both now and in the future. So why take the risk of entrusting your credit management needs to anyone else?

4.4

Use of e-commerce in the receivables industry: added value or window dressing?

Martin Smith, Close Credit Management

In today's e-centric business world the companies that do not present themselves and their services over the internet will inevitably be viewed as archaic. However, the path to successful innovation and implementation is not a smooth one.

As consumers, we have all had experiences of misfiring websites and the frustrations they create. We have also heard of the horrors of lost or stolen data, a perpetual nightmare for anyone storing and transferring data electronically, from government departments to major retailers and banks.

The receivables industry has seen any number of attempts to use e-commerce as a service tool, one of the earliest and most obviously flawed theories being that you could set up a web interface to which clients would post debts for collection – great if you have only one to type in, but not so good if you have hundreds or thousands of them. Any large receivables agency needs referrals in

volume. Attracting low-volume clients kills efficiency and generates endless offline communications with clients anxious to know the progress of their only debt under management. This may be fine for a small agency but is entirely useless to the larger agencies, which have continued to refine and develop existing referral management technologies in association with their clients to ever greater effect.

So, if the 'pass your only debt' portal is the wrong idea for most of us, how can the industry use e-commerce to facilitate and develop its offering, and what steps should be taken to manage the risks involved?

A number of activities we undertake can clearly benefit from use of web-based interfaces. Some, like reporting and updating on accounts, are now very much standard practice. Remote workers are facilitated by systems such as Citrix that are designed to lock in security, again a well-established technology.

The biggest benefits, though, appear to present themselves in the field of debtor/customer communication. Here, the introduction of web-based payment systems giving debtors an easy-to-use 24-hour payment portal, with add-ons such as e-mail for contact and the ability to print off a statement and also change (subject to verification) address or telephone information, is proving a real winner. This same facility can be used to capture e-mail addresses, thereby giving collectors another contact point.

There is no reason why, in addition to its debtors, the company's own collectors and their third-party agents should not use the same payment site. Add automatic cash allocation to this and the creditor has a pretty much universal electronic payment platform, which saves additional administrative resource by allocating payments as well. Customers can use the same portal to place orders and request attention to queries.

Companies implementing such systems are seeing some startling e-benefits, given additional impetus when they add bespoke elements to align with their specific market and customer base. Suddenly you are presented with a piece of new technology that rapidly settles at your system's core, elbowing out previous systems such as PDQ machines but posing the big question 'What steps should be taken to manage the risks involved?'

Control it or it will control you

For many of us the construction and maintenance of websites and their attendant technologies are non-core activities in our businesses, which we buy in. In common with our normal practices as IT system users we know what we want the technology to do and we are capable of addressing the broad risks involved. However, as we also well know, outsourced services are fine when the provider is stable and experienced. They are also fine when they are doing something that we fully understand but choose not to do ourselves.

E-commerce often involves complex technologies of which we know very little. It's a relatively new and fast-developing field, and many providers are, by definition, still in the early stages of development as businesses themselves. Their

principals may well be 'techies' with limited knowledge of how to run a business or financiers with little or no technical knowledge.

So, while we may be capable of making a risk assessment on our web-based activities, how do we manage and mitigate that risk when we place a slice of this new technology close to the heart of our business?

The first element we need to understand is what the various components of the system are and who actually maintains and develops them. A typical system, as previously described, may sit initially in three boxes with three separate control points, as illustrated in Figure 4.4.1.

Add the basic functionality and the interfaces, and the possibility for breakdown becomes evident (Figure 4.4.2).

The clear risk here is that, when a technical hitch occurs (and it will), delays arise first in establishing what is wrong, then in confirming who is responsible for fixing the problem and then finally in actually restoring functionality. In the meantime your company's operatives are left to deal with the customers and others who cannot use the system. There is a fair chance that the fix is entirely out of their control.

This type of *ménage à trois* is the risk manager's nightmare; then throw in your internet service provider as well! Key to managing the situation to best effect is the choice of partners and understanding the relationships between them.

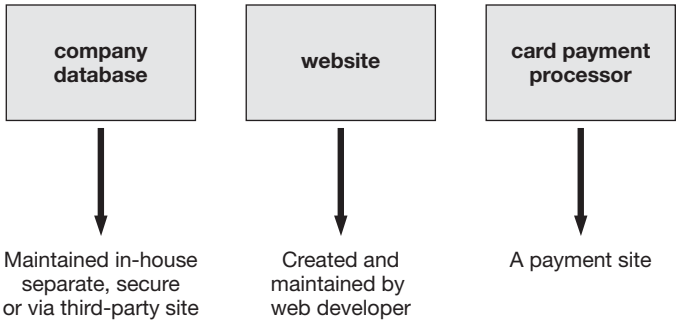


Figure 4.4.1 An e-commerce system

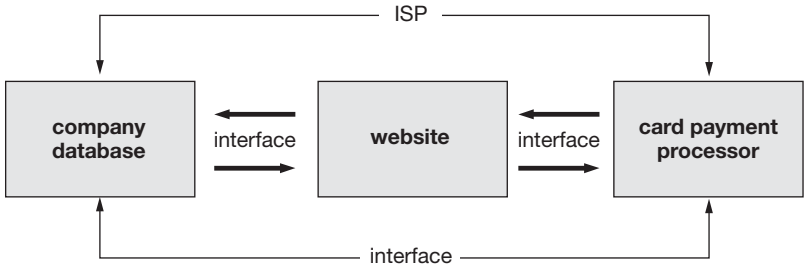


Figure 4.4.2 E-commerce system interfaces

You will probably have very different relationships with the key players in this chain of activity. Of course, you will have detailed knowledge in-house of your own systems and requirements of the project. Your website designers (if not also in-house) will be the only people with whom you will have a close working relationship – your ISP and the card payment processor will be much more remote and will do very little, if any, tailoring of their technology for you; it will be up to you and your web designers to make yours fit theirs.

Of course, if a breakdown occurs it could be your ISP or data processor that is at fault, but because of the closer relationship you will inevitably have with your website provider then almost inevitably theirs is going to be the first number to call when the system breaks. Part of your development of this relationship therefore, especially if you are a small business with limited resources, needs to take into account the extent to which you may need to rely on your website provider to help you manage the broader process. It will, not unnaturally, also expect to be remunerated for this service. What it is most important to remember here is that the chain of activity you are employing is extensive, possibly spanning continents in the case of processing servers, so you need to have a very clear policy on exactly how you are going to track down 'faults' and also deal with the various parties that will be clamouring for an explanation when they occur.

The fact is, then, that no single key partner in this enterprise has the whole process under its control. Choose the best, most reliable ISP and payment processor; then look to develop a close and detailed understanding with your website provider – choose one that can give you respectable reference contacts, and check them out before you commit, as this partnership is crucial to your management of the system risk for a very long time to come.

Data security

While this subject is not exclusive to e-commerce activities, it is, nevertheless, well worth using your e-commerce project to look at both specific and wider aspects of your data security practices.

Every country has its own laws and regulatory practices associated with data security, and it goes without saying that compliance with these is non-negotiable. Beyond this there are two obvious general exposures: deliberate fraud (external or internal), and ignorance or stupidity, which you can control only internally.

In any event, the withering criticism of government departments, banks and other businesses with regard to loss of personal financial data, which we see ever more often in the media, frequently backed by censure and fines from regulators, is obviously to be avoided at all costs. This chapter is not specifically focused on the technical aspects of encryption and firewalls; however, these should be researched thoroughly and in place at all critical points of the process to minimize risk of external leakage or theft of confidential information.

Clearly, what records you keep, particularly in dealing with personal banking or card details, is the starting point from which risk emanates. Again, local regulations stipulate what information can, or cannot, be retained for your business

purposes. However, the stupidity demonstrated by some data controllers – losing memory sticks, leaving laptops on trains, sending highly sensitive material through the post – is truly breathtaking. Why on earth card or bank details need to be taken out of their controlled, secure business environment is, rightly, entirely beyond the comprehension of the conscientious risk manager. One simple rule – don't let it happen!

However, there are other more subtle ways in which the data you acquire through your growing use of e-technologies could be under threat. For example, if you record your telephone calls, all the information, including card numbers and security codes, is available to be copied by anyone who has access to the recordings. You may not retain this information in any other way, but angles such as this are easy to miss. For this reason, the installation of a new, or upgraded, e-commerce technology should be used as an opportunity to review all the surrounding risks, both direct and indirectly associated with its use, and upgrade controls as required.

The development of the 'virtual office', where the types of e-commerce platforms discussed can play a key role, presents receivables management companies with the opportunity to spread their activities well beyond their previous geographic confines. Debtors can be given 24/7/365 access to the means to make payment in a variety of currencies. Time zones become irrelevant. Business continuity is also benefited, as the technology does not require access to a physical office in the way that has previously been necessary.

Without doubt, the receivables industry has much to gain from the development of e-technology. The key things to remember are: 1) No one controls the internet, so recognize the risk; and 2) Choose your partners carefully and especially so if your website provider is not in-house. Once you have chosen wisely, if you still identify significant risks then they are as likely to be already there in your data management controls as to have been created by the new process.

First choice for today...
...and for the future

30
years of helping our customers both large & small

+20
locations strategically placed across the UK

+10
years of winning industry awards

= / Choice

SUNGARD®
Availability Services

t: **0800 143 413** ■ e: **infoavail@sungard.com** ■ w: **www.sungard.co.uk**

10th Anniversary Award Outstanding Excellence in Business Continuity.
Business Continuity Service Provider of the Year – 2006, 2005, 2002, 2000, 1999. Finalist – 2008, 2007, 2006, 2005, 2004, 2002, 2001, 2000, 1999.

4.5

Whose risk is it anyway?

Keith Tilley,
SunGard Availability Services (UK) Limited

Over the past three decades the development of business continuity as a management discipline – business continuity management (BCM) – has been marked by its progress away from the server room and into the wider business, where it is often the responsibility of a C-level executive. We see this trend accelerating. The sea change has come about because many organizations now view BCM as being much more than just technology-centric disaster recovery and more a fundamental part of the organization's holistic approach to operational risk management (ORM).

For most organizations, BCM is the main proactive information availability (IA) strategy employed – where IA is:

> the continuum of disciplines, spanning security and infrastructure as well as business continuity and disaster recovery, allowing organisations to keep people (eg, employees and customers) and information connected at all times. As an ongoing strategy, IA provides a high degree of risk tolerance, whilst helping organisations ensure an appropriate response to interruptions as and when they occur.
>
> SunGard Availability Services

However, in some (mainly financial sector) firms ORM is used alongside, or instead of, BCM.

Lest we be accused of dealing purely in semantics, let us also define BCM and ORM. BS 25999 – the British Standard for BCM – defines the process as:

> a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

ORM, meanwhile, is defined thus:

> Managing the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
>
> Basel Committee of the Bank of International Settlements

The differences *are* subtle, but ORM is focused on the management of losses rather than the return to business as usual, which is the aim of BCM. Often the resulting activities will be similar, but not always. One major difference is that ORM focuses on ensuring that the organization has sufficient financial capital set aside to ensure that it can continue to operate during and after a crisis. Another major difference is that ORM tends to be internally focused, while BCM includes external stakeholders, such as supply chain partners.

AIRMIC, the Association of Insurance and Risk Managers, believes that ORM supports BCM:

> ORM considers all risks that support the business and some generic risks, such as failed processes and health and safety. BCM, on the other hand, is a control that goes across the whole business and beyond. It considers all types of risk, beyond those included under the ORM umbrella. ORM and BCM have grown up through different disciplines, but there is room for both. However, each profession needs to share and cooperate.

So, with this appreciation of how BCM and ORM complement one another, as companies recognize the need to be prepared for any eventuality, there is a growing tendency for the threat of business interruptions to be managed in the same way as any other risk. As with any risk, those responsible for BCM need to have access to up-to-date, accurate and relevant information so that the organization can make timely preparations and informed decisions. This allows it to make sure it has the right resources and processes in place to ensure appropriate business resilience.

Getting the balance wrong can be damaging. Overestimating what's needed may mean other areas are starved of much-needed funds, while underestimating may result in being unable to respond effectively to a business interruption. This is why the age-old principles of conducting business impact analyses, risk reviews and vulnerability assessments are so valuable a start point for any cohesive, well-engineered, holistic and relevant IA strategy.

Hence, to manage risks from a BCM perspective, more information and more detailed analysis from sources more widely spread across the organization are vital. And, given that even the most well prepared can be undone by a weak chain of supply

or less robust partner, it is also highly recommended to involve strategic partners and suppliers to get a holistic view of risk and vulnerability. When due assessment has been conducted, the business is then in a position to decide upon appropriate risk mitigation, resilience and continuity measures, and from here the organization's IA strategy can ensue. But why bother with any of this in the first place?

Considerations for 21st-century IA

Since DR was pioneered back in the 1970s, the business world has changed out of all recognition and continues to do so. It stands to reason, therefore, that BCM planners must address myriad new realities:

- The changing nature of risk. Organizations are facing new threats to the business, such as terrorist attacks and cyber-crime, in addition to the more familiar risks of power, software and hardware failure.
- Globalization has created truly worldwide markets; as a result opportunities have increased, but threats have too. Businesses are generally 'leaner', and developing the flexibility to respond rapidly to new opportunities is a key management imperative.
- Regulation and compliance. Regulation is more pervasive today, and all directors – not only those in the financial services sector – have a statutory obligation to 'exercise reasonable care in the performance of their work' and act in the best interests of the organization's stakeholders (source: Institute of Directors). Additionally, today's global businesses face myriad compliance issues, which vary across geographies but which must be met to avoid fines and prosecution.
- Reduced tolerance for failure. In today's fast-moving, highly competitive world, customers, shareholders, employees and other stakeholders are far less understanding of an organization's failure to cope in a crisis. This is one of the key factors behind the growing need to drive BCM down the supply chain.
- The advent of new benchmarks. BS 25999 is the most heavily downloaded document in the BSI's history and is set to become a prerequisite for doing business. The standard's requirement to document all management activities and decisions can create a huge administrative overhead and is likely to drive the need for increased automation. The paperwork burden may be compounded by the new risk management standard BS 31100.
- Increasing customer power has created an ever-growing threat of brand and reputation damage, and the internet has provided an effective means of coordinating and communicating customer dissatisfaction.

These factors, coupled with the increased visibility of BCM at senior level, mean that more is demanded of BCM today without a corresponding increase in resources. That means the BC professional has to work smarter. The right specialist BCM software tool can be a critical enabler in disseminating this enhanced information throughout the organization so that it can become an integral part of the BCM culture and ORM process maximizing IA investments.

Optional extra or vital tool?

Increasingly, we are seeing many of our larger customers – those with multiple sites, often in all four corners of the globe – devolving responsibility for BCM to individual business units. In such cases, there is invariably a central BC department, but its role may not be to impose uniform solutions on vastly differing business operations or to micro-manage BC plans but rather to ensure minimum standards are met, thereby acting in an advisory as opposed to prescriptive role.

Specialist software tools have been around for nearly 20 years. So why should they now be viewed less as optional extras and more as tools of vital importance? To answer that question we need only recall how the world of work has changed – and with it so too have the software tools available.

The future shape of continuity software

The new challenges faced by organizations cannot be met by traditional software solutions, much less general office automation or personal productivity tools. For instance, the planning process is now more complicated, as many more factors need to be considered, including:

- Planning for multiple scenarios. First-generation tools tend to be limited to single-scenario plans such as hardware failure. They do not have the functionality necessary to be able to perform multiple impact analyses and historical tracking to ensure availability regardless of the scenario.
- Managing complex interdependencies. Software has to be more sophisticated to take into account key relationships and dependencies within the business.
- Ensuring information availability – keeping people and information connected at all times. In today's 24/7/365 business environment, down time is a central threat. This was highlighted in a poll of companies around the world by the Economist Intelligence Unit in which 47 per cent of risk managers questioned said that more than 24 hours' down time could seriously jeopardize the survival of their entire business.
- Ease of use by end users throughout the organization, whatever their level of IT literacy. Traditional software was developed with only the business continuity manager in mind but, as BCM moves out of the IT department into the wider business, software tools need to be intuitive for all to use.
- The impact of a disaster upon the wider supply chain – and not just on the business and its customers. SunGard's *From Adversity to Availability* report, published in 2008, found that 46 per cent of businesses insist that their suppliers can demonstrate that they have contingency plans to guarantee that service levels and contractual commitments will be met, even in the event of a disaster.
- The ability to meet changing requirements as the organization grows and matures.
- The need to produce meaningful reports that can be easily understood by business managers as well as BC professionals.
- Demonstrating a clear return on end users' investment of time and effort. It is human nature to grow frustrated with business continuity tools that are used

only once or twice a year with no tangible results. If the tools are to be effective, end users need to frequently input data into a system, but they are unlikely to do so unless they can see the benefits.

These are just some of the reasons why we believe a new generation of smarter software is needed to deliver the integrated, comprehensive functionality required for effective BCM. This will cover the entire BCM life cycle, as defined by BS 25999, from business impact analysis to testing and incident management and every stage in between.

We envisage such software will contain features to increase accessibility of BCM throughout an organization, including:

- Compliance scorecards to measure compliance against BS 31100, BS 25999, Sarbanes–Oxley, any applicable FSA regulations and relevant legislation such as the Civil Contingencies Act.
- Dashboard reports to give staff at all levels an instant snapshot of their BCM preparedness, enabling them to take any necessary remedial action immediately.
- Integrated risk assessments to register and monitor operational and environmental risks that can be viewed by business process, line of business, technology and geography.
- Supply chain management – integrating key suppliers into the BCM programme.
- Workforce management – managing BC profiles of individual members of staff to ensure they are involved in testing and have been trained to undertake their personal responsibilities in the event of an invocation.
- Testing programme – scheduling, tracking and maintaining all testing requirements such as scope, results, remediation and so on.

If IA is about keeping people and information connected – then BCM's job is to keep everyone connected with the information they need, all the time, no matter what. What BCM software does is help embed this thinking into the culture of the organization by helping ensure that the right information gets to the right people, in the right way and at the right time, thereby helping them make the right decision.

SunGard predicts that the ability to anticipate and plan for the major-event types an organization might encounter will increasingly become part of the daily business agenda. The time when BCM was a niche occupation in the IT department is receding quickly. Resolving the complex, conflicting and changing requirements of corporate risk departments, senior management, customers, regulators and end users can no longer be achieved using basic office productivity tools.

What's more, in today's landscape of myriad and changing risk, a lack of strategy to enhance resilience, direct recovery or facilitate a nimble handling of emerging threat situations could be regarded as naivety at best or a dereliction of duty at worst. Organizational ability both to manage risk and to secure availability more effectively than the competition will be a key factor in separating the winners from the losers. And BCM software has its part to play in enabling this.

Case study: Smiths Group: specialist continuity software – a practical application

SunGard Availability Services client Smiths Group has first-hand experience of the value of specialist continuity software. This FTSE 100 company consists of three largely autonomous business divisions: Smiths Detection Systems, Smiths Medical and Smiths Specialist Engineering. Altogether, the group employs around 21,300 people in the UK, United States, China, Continental Europe and Mexico but, despite its size, has a lean head office team of just 200 personnel.

While Andrew Scott, head of IT services for Smiths, has responsibility for risk management, the individual operating divisions are responsible for their own operational risk management and business survival issues. So Scott faced the tough challenge of not only creating robust and workable BCM programmes for the corporate head office sites but also developing a BCM template that would prove attractive to the highly diverse business units worldwide.

Scott used specialist continuity software from SunGard to conduct business impact and risk analysis to assess preparedness across the group. The results of this exercise showed that most businesses within the group had some distance to travel in terms of improving their BCM preparedness and organizational resilience. There were two exceptions: Smiths Medical and the corporate HQ, both of which already had a long-standing history of BCM and disaster recovery in place.

Taking a pragmatic approach, Andrew Scott decided to use the SunGard software as an information management tool to create templates that could be adapted by the various divisions. This was a tall order. The common templates had to respect Smiths Group's structure, internationalism and security needs to encourage BCM best practice across all borders without compromising the remit of the business divisions. Furthermore, it could not be too unwieldy or restrictive to use if the required level of take-up was to be achieved.

SunGard worked with Smiths to build a software solution that met the demanding brief. Training and support materials were developed to help ensure a successful roll-out. To support Andrew Scott in his role, a reporting structure was established that would enable local plan reports to feed into central tracking, activity and compliance management reporting.

From a situation that could have been likened to 'herding cats', Smiths now has a system in place that:

- delivers a standard environment for BCM across the group;
- defines roles and responsibilities across the business;

- is consistent with company policy and drives high standards;
- provides a focus and repository for BCM activity.

With SunGard's help, Smiths has found a software tool that promotes ownership of BCM at all levels and enables its divisions to be responsible for their own BCM success. It is also a platform for future growth and evolution of BCM within Smiths Group's environment. It allows simultaneous plan updates and quick wins and gives management sight of BCM performance at any point in time.

THIS PAGE IS INTENTIONALLY LEFT BLANK

5

Managing Operational Risk

THIS PAGE IS INTENTIONALLY LEFT BLANK

5.1

An introduction to modelling operational risk

*David Breden, HSBC Operational Risk Consultancy**

Introduction

Operational risks are those associated with the failure of systems, people or processes, or that result from the impact of external events. Therefore it is clear that businesses have always managed operational risk. They have taken steps to prevent theft and fraud and have introduced checks and balances to pick up the basic human errors that beset all businesses. Since computers have become a commonplace of business life, we have created a dizzying array of passwords, firewalls and encryption methodologies to ensure that our data remain secure, and we have insured our business assets against fire, theft, flood, earthquake and other natural disasters. All of these actions are designed to protect us against the adverse impact of operational risk. On the whole, however, firms have not found

*The views expressed in this chapter are the author's personal views and do not necessarily represent the views of the HSBC Group.

it necessary to model or seek to quantify operational risk exposures. They have identified and ranked risks in relative terms as being high, medium or low risks, but have not sought to apply a financial value to such exposures.

For financial institutions this situation changed with the advent of Basel II, the name commonly applied to the guidance provided by the Committee for Banking Supervision of the Bank for International Settlements on the appropriate level of capital that internationally active banks should set aside to protect themselves against risk. Under the previous system (commonly referred to as Basel I), capital was set aside to cover credit risk (on the basis of a set amount to be held against money lent regardless of the quality of the borrower) and market risk. Basel II, however, seeks to create a risk-sensitive, forward-looking capital adequacy assessment that will assess levels of credit, market and, for the first time, operational risk that are present in the bank concerned and assign capital based on these levels of risk.

The Committee sets out the methodologies that banks should use to calculate their exposure to operational risk.[1] At the most basic level, capital is calculated by using a proxy (average net interest income plus average net non-interest income over the previous three years) and multiplying this value by a risk factor designed to be indicative of the level of operational risk in the market. Such methods involve no risk analysis but merely provide a number for capital adequacy purposes. The road is, however, open for more ambitious institutions to opt for the Advanced Measurement Approach and develop a modelled approach to the quantification of operational risk.

The motivation for a bank to model operational risk exposures has therefore originated through regulatory imperative, but the process has commercial benefits that flow across industry and business sectors and stretch beyond the regulated financial services sector. Let us say, for example, that we detect a flaw in a system and process that exposes us to loss and we believe the risk to be 'high'. However, the event has yet to produce a tangible loss. We want to avoid such a loss, but how will we be able to build a business case to support the level of expenditure we need to correct the flaw? Those responsible for the company purse strings are unlikely to be swayed by a red traffic light in a risk report when asked to release a possibly significant sum to resolve the flaw. It is useful in such cases to be able to indicate a monetary scale for the potential risk so that a proper cost–benefit analysis can be carried out. To produce this estimate of exposure we will need to develop an operational risk model.

The difficulties of modelling operational risk

It is not unusual for firms to model risk, and most models will involve risk managers arriving at an assessment of the likelihood or the frequency with which a loss will occur and then the impact of the risk if it should occur. However, despite requiring identical inputs, modelling operational risk has created challenges that are still subject to considerable discussion and debate amongst practitioners. Some of the issues that give rise to this debate are:

- Context dependency. Operational risk exposures change from day to day and minute to minute. The extent of any loss we suffer will depend on underlying circumstances. The impact of a theft from a retail store will depend on the amount of cash held in the till at the moment at which the theft takes place. We may normally hold only a few hundred pounds in the till, but if we have just made a large sale then the thief may get away with a much larger haul. A matter of pure chance will determine the size of the loss. Similarly if we send a payment to an incorrect destination, then our loss is likely to be determined by the size of the payment and the willingness of the beneficiary to return the sum paid in error, amongst other factors. Again an identical mistake can give rise to vastly different impacts depending upon the underlying circumstances of loss. Any model that we build to describe operational risk exposures must be capable of recognizing this significant element of uncertainty.
- Linked to the above point is the fact that in many cases there is no apparent upper limit for operational loss events. In any credit portfolio, loss can be linked to the amount of the principal amount lent or advanced on credit plus an amount for interest and possible legal costs of attempted recovery, but the same cannot be said of operational losses. If an employee perpetrates a fraud in the company, what will the loss be? It will be impossible for us to answer the question without knowing the circumstances of the loss, but simple reference to some examples will demonstrate that unauthorized activity by an employee can in extreme cases lead to the downfall of a firm.[2]
- There is no defined portfolio of operational risks to which a firm may be exposed. Most firms will create a checklist of risks to which they believe they have an exposure, but new risks emerge continually. For example, the form of external attack from fraudsters is continually evolving, and changing environments will also give rise to new threats. Meanwhile human beings will always be able to find new ways to make errors or disrupt processes. Operational risk management is beset by the impact of 'unknown unknowns'.[3]
- Much risk modelling is based on the assumption that the past is a good indicator of the future. If such a view is accepted then it is a logical step to base forward-looking models on historical data drawn from past losses within the firm. Even if we are prepared to accept the value of past events as an indicator of future operational risk events, we are unlikely to be able to gather data that will comprehensively describe our total risk environment. We will find that we have a lot of data (hopefully of small monetary amount) in certain areas to describe our exposure to petty theft or credit card fraud, but, almost by definition, firms that are trading successfully are unlikely to have suffered the sort of significant unexpected event that we are seeking to identify and address in operational risk management. If we are to build a model capable of making any approximation to quantifying such 'Black Swan'[4] events, then we will need to supplement the deficiencies and gaps left with more subjective sources of information.
- As a final complication we should recognize that not all operational events have a direct financial impact. Failure of an ATM over a holiday weekend will

give rise to little financial loss for a bank that will presumably be protected by service-level agreements with hardware suppliers for maintenance – but the impact will be felt in customer dissatisfaction and possible departure, so this will be an event that should be addressed regardless of the low initial impact, and a way will need to be found to factor such events into the model.

The parameters of the model

As mentioned earlier, the key parameters of the operational risk model will be the frequency with which the event occurs and the impact of the event when and if it does occur. In both cases we will wish to factor in uncertainty, as our aim will be to reflect the potential for unexpected events that our organization has never experienced. To do this, we will not work with absolute amounts, but rather will apply a mathematical distribution to both frequencies and impact to enable us to reflect a range of potential frequency and impacts from best case through expected and on to worst-case scenarios.

Frequency

Sometimes referred to as 'likelihood', this measure indicates the number of times an event might occur in a particular year (five times a year) or the number of years that will have to pass for the event to happen (once in 20 or 50 years, for example).

In general terms there is a degree of consensus as to the appropriate distributions to be used to model frequency. For high-frequency events we will generally use a normal distribution, as shown in Figure 5.1.1. This particular example depicts a normal distribution with a mean of 5,000 and a standard deviation of 1,000, indicating that, given these assumptions, we expect this particular event to occur between 1,910 times a year and 8,090 times a year, allowing for considerable variation in results. Greater variance can of course be achieved by increasing the standard deviation.

For rare events we will often use a Poisson distribution, which is particularly suited for events that we expect to occur infrequently. In Figure 5.1.2 we show the distribution produced by a Poisson curve applied to a risk that on average happens once a year, but may not happen in every year. As can be seen, in most years the event will happen once or not at all. However, uncertainty is produced by applying

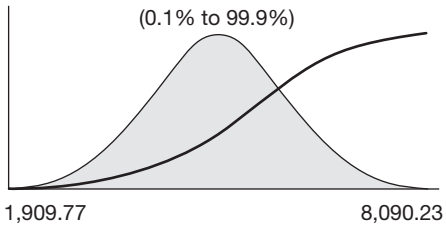


Figure 5.1.1 Normal distribution

Requiring decision makers to rate the key risks forces them to engage actively in this strategic process, considering both the hard data from the scorecards and the softer data that are ever present in an organization's environment. Complementary data and insight can also be generated through stress testing and scenario analysis processes.

The process of developing an organizational strategy map and risk map, considering both the macro (broader business environment) and the micro (individual strategic objective) level, and developing a small number of high-quality indicators (all supported by appropriate measures) is the critical first stage in becoming an execution-focused organization. Applying the methodology and, particularly, the resulting strategy maps and risk maps provides the context within which to frame future management discussions.

For a management team, the discussions around and interaction between the strategy map and risk map lead to a deeper understanding of both organizational strategy and organizational risks. Additionally, the challenge and debate that should be a hallmark of these discussions develop the capabilities of the management team and set the right tone for organizational culture.

The strategy maps and risk maps should be 'owned' by the management team responsible for delivering the objectives laid out in the strategy map at each level within the organization. As the strategic objectives are cascaded down through the business, so are the risks. Therefore the management discussions, decision making and bias towards taking action will also flow down, building organizational capability and developing culture.

When considering risks at the macro and micro level, organizations should also be considering their risk appetite, current risk exposure and risk capacity. Again, this discussion builds capabilities and culture while generating insights that enhance decision making.

Addressing the 'measurement dilemma'

To simplify the development and sustainability of the R-bp process, the methodology addresses what may be called the 'measurement dilemma'. This is the situation where organizations attempt to measure 'everything' because of uncertainty as to what should be measured and what the 'right' measures are.

This can result in organizations having hundreds of 'key' measures that provide little management or strategic insight. The R-bp methodology addresses this by:

- providing the strategic context within which to define indicators and measures;
- differentiating between different types of indicators – performance indicators, risk indicators and controls indicators – and being very specific about their use;
- differentiating between 'indicators' and 'measures' and providing clear guidance on each of their roles within the overall process.

Providing clearer, easier-to-understand information again helps generate better-quality management discussions, decision making and action taking.

Case study: Risk-based performance in action

One of the early adopters of the risk-based performance methodology was the global IT function of a London-based investment bank. In addition to the dual challenges of meeting Basel II and SOX, the global IT function was faced with delivering an enterprise-wide risk and controls project and overcoming internal cultural issues, specifically around achieving buy-in and embedding the planned processes into everyday culture.

Initially traditional risk and controls matrices were developed and implemented using ad hoc processes supported by spreadsheets. However, problems were quickly identified. As there was a balanced scorecard already in place, there was particular concern about the duplication of processes and information, and the negative impact on staff of yet another data capture process.

At this point, a more strategic and integrated approach that would build on both the existing risk and controls matrix and the global balanced scorecard was introduced. The risk-based performance methodology was introduced to guide the development of an integrated performance and risk management process supported by a specialist software application. The resulting system and processes were implemented in 32 centres around the world, providing information to multiple levels of management and also reporting to multiple regulators and external stakeholders.

Applying the principles and approaches within the risk-based performance methodology, the final solution achieved a high level of buy-in and support because the IT function was able to reduce process and reporting complexities while delivering a focused set of management scorecards, dashboards and reports. Delivering risk identification and assessment within the context of the organization's strategic objectives allowed for a reduction of the number of key risks from hundreds to tens, with similar reductions in the number of measures, indicators and volume of data while increasing the quality of management information.

In the face of tighter market conditions as a result of the credit crunch, the risk-based performance methodology has now been implemented more widely within the bank to address current performance and risk management issues.

What are the benefits?

Our research found that adopting an integrated approach to performance and risk management produces significant benefits for improving strategic execution, as well as reducing risk-related loss, cost savings, and improved management information.

The following figures highlight the opportunity to drive benefits:

- There are 40–70 per cent of organizations that fail to execute their strategy successfully.
- One study found the average short-term financial loss on large-risk events (greater than US$1 million) is US$65 million, with a tail loss after 120 days climbing by a factor of 12 – an average of US$780 million.
- Another study between 2001 and 2005 found that risk-related losses at the top 12 US banks represented 4–5 per cent of their net income.
- A study of operational risk losses at 200 financial services organizations between 1997 and 2002 found 150 cases of significant financial distress at 90 organizations.
- The three studies above generally agreed that 50 per cent of these losses were caused by factors within the organizations' control, and thus they were preventable.
- It is estimated that a 25 per cent reduction in regulatory capital can be achieved by implementing performance and risk processes and systems to meet the demands of Basel II (AMA).
- One leading expert suggests that reducing operational losses offers the potential for greater cost savings than tradition cost-cutting approaches.

Manigent's clients and research participants saw the risk-based performance methodology as an appropriate framework for enabling these benefits to be realized and for allowing many of the current issues around performance and risk management to be addressed. It is a proven approach to addressing many of the challenges financial services organizations face in relation to management information, including:

- risk-related losses;
- excessive costs due to duplicated processes and unnecessary complexities;
- poor-quality and inactionable management information;
- poor strategic execution;
- high regulatory capital and the cost of capital.

Conclusion

Following the 2007/2008 credit crisis, organizations are seeking to respond better to the fundamental challenge of all businesses – the balance between risk and reward. To do this, management teams must move beyond today's metric-focused management information frameworks, where performance and risk management are considered separately, and create a culture that enables them to manage with one eye on performance and one eye on risk on a daily basis.

The risk-based performance methodology enables organizations to integrate and align performance and risk management processes to provide a single, enterprise-wide view of performance and risk. By implementing the methodology,

management will be able to have more informed discussions and make better decisions. This in turn will enhance strategic execution and build shareholder value by exploiting opportunities and responding to risk more effectively than their competitors.

Reference

Kaplan, RS and Norton, DP (1996) *The Balanced Scorecard: Translating strategy into action*, Harvard Business School Press, Boston, MA

INCREASING CONFIDENCE IN YOUR FUTURE

Today's risk management is about delivering the confidence needed to ensure that stakeholders' expectations are met; to know that key business risks are under control and provide the security of future performance in today's uncertain world.

This is why at LRQA our approach is different. LRQA's risk management support - Business Assurance - is designed to help you ensure that your systems are identifying and driving down critical risks to deliver real improvements in the eyes of your critical stakeholders.

Business Assurance is our approach to management systems assessment. It focuses on developing effective and efficient management systems giving your business the confidence it needs to thrive and grow. By understanding your business and your goals, we are able to work with you to accurately pinpoint the key areas that need to improve, helping you turn risks into opportunities and weaknesses into strengths.

With Business Assurance, you can feel confident about your future.

To find out how LRQA can help you,
visit us at: www.lrqa.com,
contact us at: enquiries@lrqa.com
or call us at: +44 24 7688 2373

Lloyd's Register Quality Assurance is a member of the Lloyd's Register Group

LRQA
Measure the Difference

5.5

Managing your supply chain risk

Sandy Sutherland, David Lawson and Alex Briggs, Lloyd's Register Quality Assurance (LRQA)

The successful building of a brand's reputation and value requires careful and planned management. One aspect of that is the managing of risks, including those throughout the supply chain that can have a negative impact directly or indirectly on a brand. Before a brand can begin to set up its global supply chain, it first needs to determine what the critical dependencies are. In other words, what issues carry the largest potential risk? Once these have been identified, the next step is to begin ensuring that systems and processes are embedded as far up and down the supply chain as is deemed necessary to effectively manage those critical dependencies. Organizations try to transfer immediate risks to their suppliers, and in some cases succeed. Unfortunately, there's often one kind of risk you can't transfer, and that's the risk to your brand image. If it goes wrong and it's your name on it, then it's your brand that suffers, not your suppliers.

Management systems-based approach

While the task of identifying the critically dependent issues is a daunting one, it is by no means the end of the journey. Once the issues have been identified, it's vital

to have a robust and structured approach to managing the risks while maximizing the potential opportunities associated with those key areas of the business. Having a management system that is at the very heart of the business can provide the necessary platform to ensure that a brand is correctly managing the key issues. A management system is the means by which a company delivers on its policies in regard to specific areas or concerns, the most traditional of which are quality, environmental performance and health and safety (H&S). The majority of global brands now use an internationally recognized quality management system (QMS) as the basis upon which their supply chain stakeholder expectations are met and risk is sufficiently reduced. The requirement of ISO 9001 has become widespread owing to the tangible benefits it has delivered to companies around the world. Those benefits include providing a systematic approach to managing a business, consistency across the entire chain, traceability of both product and processes, and clear processes for identifying client needs and managing them.

In some cases, having a management system such as ISO 9001 may be enough to minimize risks sufficiently. But, for the majority of today's global corporations, by adding additional elements to their management system at a relatively low cost (both financially and in time) they can further reduce their risks, while offering their stakeholders greatly improved transparency and trust.

Managing environmental concerns

If managing your impact on the environment is a critical factor for you, then you'll have to look both upstream and downstream from your own business. That way you'll be considering the environmental aspects and impacts your supply chain has as a whole. You'll look at who is supplying you, who you're selling to, what happens to your goods, what materials go into them, how often they are moved and by what methods, how they are disposed of, etc – all of this has to be taken into account.

ISO 14001, the leading global environmental management system standard, is the most commonly used tool to help you manage your impact on the environment. ISO 14001 requires you to look at how your business has an impact on the environment and then implement arrangements to help you reduce that impact. This often has the additional benefit of reducing costs within your supply chain.

If your greenhouse gas (GHG) emissions are a stakeholder concern for you, then ISO 14064 is a voluntary standard that enables you to quantify your GHG emissions and can then lead to managing their reduction, with potential financial gains for organizations that use this approach.

An increasingly important issue for global brands today is measuring and communicating their carbon footprint. This can be a difficult process and often very tricky for brands, as they are unsure what part of the footprint is solely or partially theirs and which part should be carried by their suppliers. For example, if you are a toy manufacturer, do you need to factor in all or only some of your CO_2 emissions from the manufacturer that produces the packaging for your toys, or possibly the CO_2 emissions from the production of the batteries that will need to be inserted to operate them? In this case, PAS 2050, the BSI British Standards

Specification for the assessment of the life-cycle greenhouse gas emissions of goods and services introduced in late 2008, goes a long way towards providing you with the tools to address the carbon footprinting issues associated with your products, goods and services.

It may be that you are in the food industry, providing cold-water prawns that consumers want to know have been sourced in an environmentally responsible way. Here you have to think about your upstream suppliers. Are the prawns from a sustainable source? Is your product free from artificial additives, chemicals and pesticides?

But what about downstream? Typically this is a buyer, whether it's business or a person. The buyer may want to know, for example, whether you are proactively taking steps to minimize your impact on the rest of the supply chain. An example of this could be the use of recyclable packaging as well as energy-efficient distribution and transport of goods to your customers. Does your product include a carbon label, making transparent to your end customers the carbon footprint of each package? If so, then you will need verifiable data to build trust for your brand and your supply chain practices.

Resilience in the supply chain

The events of 11 September 2001 brought a new factor to the forefront for global brands and their supply chains: security. Security relates not only to the safe transport of goods but also to the speed of delivery and the control of the product throughout its journey. In today's world, with just-in-time delivery reducing storage costs significantly, it is crucial that, if a major retailer orders a container-load of goods from somewhere in the world, those goods, exactly those goods, must arrive at exactly the desired location at exactly the specified time. Any variance in the above criteria and the supply chain begins to struggle, with each link in the chain eventually suffering from the knock-on effect.

Management systems can help here too. ISO 28000 looks at security in the supply chain, including getting the goods there uncontaminated and complete. It's also about smoothing the pathway through regulatory and customs requirements. This is now one of the most important areas for organizations with global supply chains. Certainly, if you are part of the process of moving goods from one country to another, it doesn't matter which area you are in, whether this involves warehousing, distribution or receipt of goods and services by ports, containers, shipping, rail, air or movement of goods by road, supply chain management systems must now address and mitigate against potential disruptions caused by security risks.

So, if you want to look at which supply chain security management system is most applicable to your organization, it is crucial to look first at the regions of the world in which your supply chain operates. Regional schemes and regulations such as C-TPAT in North America and AEO in Europe are increasing in importance, becoming a barrier to market entry for brands looking to trade in those areas. ISO 28000 certification provides brands with the in-depth information on

their supply chain that makes meeting the security aspects of AEO or C-TPAT requirements that much easier.

Health, safety and welfare – responsible management

Health, safety and welfare are a major concern for your business if your supply chain involves any of the following:

- the use of hazardous or dangerous substances;
- work carried out in hazardous environments;
- parts of the world, organizations or industries with a poor reputation for health, safety and welfare.

Your major stakeholders in this respect are your own employees, those of your suppliers, consumer watchdogs, the visitors to your sites and possibly your neighbours. At the heart of any system are proper hazard identification and then a good risk management strategy in relation to those hazards. In supply chain terms, however, it's not just your own immediate site that you are concerned with; it is the elements that make up your supply chain, from the sourcing of raw materials through to the packaging and distribution of your product. All of them need to be taken into account in developing a transparent view of your potential exposure through your supply chain.

It is reasonable for global brands to expect their suppliers to have management systems that address health, safety and welfare. There are several options in today's workplace, including global standards, national guidance documents and industry-specific 'checklist style' certification programmes. The Occupational Health and Safety Standard (OHSAS) 18001 is the most widely used H&S standard. OHSAS 18001 and most of the national guidance documents follow similar principles and practices.

If your supply chain involves parts of the world, organizations or industries with a poor reputation for health, safety and welfare you may also need to consider and promote responsible management through the adoption of management systems based on Social Accountability Standard SA 8000. This will help you manage your supply chain exposure to organizations that may deliberately exploit and mistreat workers and protect your brand by demonstrating your support for responsible management.

If your supply chain includes small companies visiting your sites with deliveries, doing maintenance work for you and other such work, it is less likely that those smaller entities will have an H&S management system. Therefore your management system has to accommodate them, including the rules that guide their on-site behaviour and clear processes that limit your potential liability in the case of an accident.

A supply chain management system that addresses health, safety and welfare helps protect not only your people but your business too.

Conclusion

Brands today are more accountable to their stakeholders than at any point in history. What was once a one-way conversation completely dominated by the large corporations is today a two-way dialogue often initiated by the consumer, either directly or through consumer watchdog groups. Senior management are accountable to stakeholders financially as well as socially, ethically and environmentally. Achieving the level of transparency required for a business to meet stakeholder expectations and create a competitive advantage is a key driver for brands. Increasingly, brands are realizing that corporate claims need to be backed up with proof, risks need to be proactively managed, and their brand reputation is often their most valuable asset. The use of management systems to underpin their business allows companies to address the areas that are critical to the success (and often survival) of their business.

For companies at the end of the supply chain, there are three main paths they can choose. The first option is to rely on their suppliers to 'self-certify' that they are addressing the critical factors. This usually takes the form of a questionnaire that each supplier is required to answer, and it is then used to evaluate the reliability and potential risk of each supplier in relation to the key issues. The second option offers the brand at the end of the supply chain a higher level of assurance. In order to minimize their risk in the areas identified as critical dependencies, suppliers are required to prove that they are effectively addressing those issues via third-party certification. The final option, the most inclusive approach, can be described as a partnership between brands and their suppliers. Brands that adopt this approach work closely with their suppliers, even sharing employees and data, with the outcome being that both sides have a stake in the rewards and risks associated with their business.

Brands now have a responsibility to understand the risks they take on when outsourcing and constructing supply chains and to ensure there is sufficient transparency to understand the depth and breadth of potential disruptions to the supply chain. When the costs of getting it wrong are market share, shareholder value, brand image and possibly even bankruptcy, can any brand afford to ignore its stakeholder concerns?

The advantages of having a set of management systems (or an integrated management system) customized for both your business objectives and your stakeholder concerns far outweigh the minimal cost and time needed to implement additional systems. By identifying and understanding the most crucial supply chain issues in the minds of your stakeholders, you are able proactively to minimize risk, enhance brand value and create a competitive advantage.

Vision...

...can take you places you've never dreamed of, make a career choice second to none.

Opportunities...

...to become a leading professional in one of today's fastest growing professions.

Support...

...at the moment you need it most, we'll give you the confidence to keep moving forward, taking your career to new heights.

CIPS – one organisation, 50,000 members, infinite benefits

The role of CIPS is to support, represent and service the interest of its members worldwide and to promote best practice in purchasing and supply management. CIPS runs a graduate level diploma qualification for its members which is recognised worldwide demonstrating that the holder has achieved a sound technical knowledge and understanding of the subject.

THE CHARTERED INSTITUTE OF PURCHASING & SUPPLY®

For more information on a career in purchasing visit: www.cips.org email: info@cips.org Tel: 01780 756777

5.6

The role of strategic purchasing and supply management in risk management

Emma Brooks, Chartered Institute of Purchasing and Supply (CIPS)

Value generators and value protectors

Procurement's profile in organizations is on the rise. A wider spend remit is being influenced and internal barriers are being broken. Some of the most valuable assets the purchasing team can bring to an organization is due diligence of vendor rating and regular detailed monitoring of supplier performance to identify, monitor and manage enterprise-wide risks while encouraging innovation and continuous improvement. This has manifested itself through enhanced relationship-management skills in purchasing teams both internally and externally.

This resource is yet to be fully exploited and, although procurement has made some progress in influencing spend areas such as marketing, HR and legal services, the skills and value that procurement can add to the purchasing process have yet to be maximized on a company-wide scale. There are vast sectorial differences too, as procurement teams still struggle to make an impact in the service industry, while their presence is deep rooted in manufacturing and retail.

The role of purchasing and supply management (P&SM) professionals has been transformed and, in many industries, there has been a shift from a transactional, back-end administrative function to a fully embedded, cross-departmental, value-adding function. Procurement professionals are taking on a more consultative role and are working alongside business units to deliver shared goals. To become more strategically focused, P&SM professionals have begun to investigate what is important to the organization and the end customer in order to identify what delivers both customer and shareholder value. Once you have established what the important issues are, you then begin to understand the risks and vulnerable points and can start building a resilience plan. The role of procurement is that of risk management and building robust supply chains, both upstream and downstream, that can weather disruptions with minimal impact. Professor Paul Cousins, Director of the Supply Chain Management Research Group at Manchester Business School, summarizes the role of procurement as that of 'value generator and value protector'. All initiatives, including risk management programmes, must be tied back into shareholder value and customer perceptions, and procurement professionals are the custodians of this process.

However, research shows that procurement professionals still have some way to go if they are to catch up in the risk management stakes. A CIPS-commissioned report compiled by Dr Helen Peck from the Resilience Centre at Cranfield University found that:

> High-profile events such as corporate governance scandals, international terrorism and civil contingencies requirements have propelled corporate risk management and security into the headlines; although they appear to have had relatively little impact on awareness of risk management in purchasing and supply.

McKinsey's also report in their recent 'Understanding supply chain risk' global survey, that almost two-thirds of respondents said that the risks to their supply chain had increased over the past five years. As we operate in a global environment, this pattern is likely to continue and risk management will become a major focus for P&SM professionals. So why are they still struggling to get involved and noticed?

It is paramount for procurement professionals to ensure they have the ear of the board in order to play a key role in risk management strategies and prove their worth. Successful risk management programmes assess the risk in terms of likelihood and impact as well as what it means to the organization. Why is this important to my organization? How will it impact value? Until this connection is made it is difficult to obtain senior management buy-in or even to be taken seriously at all.

The business risk environment

Modern organizations operate in a very commercially pressured global environment. Competition is strong, and risks must be taken in order to remain efficient and competitive. We often see risks as having a negative impact on our organization; however, with risk often come opportunities and innovation and not always threats. Like finance and auditors, procurement professionals have had a reputation for being risk averse, providing 101 reasons for not doing something. A more modern approach is to find solutions and provide a robust framework for business to operate in, allowing scope for risk takers, and closely monitoring the process step by step.

Organizations have become very lean and mostly operate on a just-in-time basis. Therefore the slightest disruption to any element of their supply chain can have devastating results. There is often no 'slack' to withstand a major movement in an organization's operations. Procurement practices such as outsourcing, low-cost-country sourcing and lean supply have exposed us to new risks but have also given us the experience to mitigate and avoid their impacts. Trends such as reducing the supply base and using sole sourcing have forged closer working relationships in order to collectively monitor and manage risks in the supply chain. BA more than anyone discovered these risks when a breakdown of relationships with Gate Gourmet resulted in their planes being grounded for several days in 2005; BA probably did not view their catering supplier as a particularly high risk at the time. Wherever possible, the purchasing organization should adopt a partnering approach to the important and vulnerable supplier relationships as a way of mitigating the risks of supply chain vulnerability. Whenever an organization is significantly vulnerable to the consequences of failure of supply, the appropriate style of relationship to manage a supplier would usually be partnership.

Industries have also become consolidated and if one major player is affected the knock-on effects can be catastrophic. Consolidation may make it almost impossible to switch to alternative suppliers who have the same capacity, especially when non-standard products are used. Generally there is no slack in these manufacturers' capacity either, so finding a supplier to switch to may be impossible. The packaging industry is one example where there are only a few large consolidated businesses. Organizations must become agile and risk aware. We need to be able to activate contingency plans at short notice.

The right tools for the job

Procurement professionals have a wealth of tools and skills that are appropriate for risk management, from close working relationships within both buying and supplying organizations to monitoring and performance measurement techniques. As procurement professionals, we are experienced in calculating savings, and this is one way of demonstrating the value we can add to an enterprise-wide risk management programme. If you are able to price a risk or disaster in terms of the cost of the loss, you are then able to cost or calculate a 'saving' on avoiding that loss.

This is indeed a powerful tool for obtaining proper attention from the board and shareholders. Successfully managed risk taking is also likely to attract attention. Showcasing examples of increased profit, innovation or sales through the successful mitigation of risks will also raise the profile of the procurement team.

As value generators and protectors, customer perception and value are considered throughout the procurement process as well as shareholder value. Dr Peck's research also looked at downstream indicators that impact on customer satisfaction to establish the level of involvement that procurement teams had in measuring and monitoring these indices. She found that, in nearly three cases out of four, respondents stated that lead time to customer is included in routine monitoring. Just over 60 per cent also indicated that availability of company products/services was also routinely included. As ever, the devil is in the detail, and marked differences appear between the sectors. Lead time to customer featured in routing monitoring in 95 per cent of public sector organizations, over 81 per cent of manufacturing businesses, nearly 65 per cent of the transport, retail and distribution sector and under 64 per cent of financial/business services.

When respondents were asked to identify the single most important factor influencing awareness of purchasing and supply risk within their own organizations, customer requirements emerged as the overall front-runner.

Through carefully monitoring supplier contracts, relationships and performance, comprehensive risk assessments can be profiled and problems foreseen and avoided, or opportunities successfully managed to fruition. Partnering and outsourcing have led to improved relationships and more prudent performance measurement tools.

Example: risk management for temporary staff

The recruitment and management of temporary labour is often a very strategic-spend category for organizations. People, their quality of work and overall attitude, integrity and appearance can have a major impact on the performance and image of your organization. For some industries, where customer-facing personnel deal with highly personal and data-protected information, the risks of getting it wrong are high. There have been several reported incidents where bank account details have been sold from customer call centres, costing one particular bank over £230,000, not to mention the reputation impact on customer security assurance.

The role of the P&SM professional is to pre-empt these risks and put processes in place to highlight, mitigate and avoid them where necessary. A starting place is thorough pre-screening of suppliers prior to contract negotiation. It is good practice to carry out site visits and screening of the supplier's internal processes. In a call centre environment, criteria such as monitoring staff calls and e-mail, the use of USB data sticks and CDs in hard drives, restricted access to reporting and the storage of customer data are just some examples of issues that should be considered, as well as system support, data back-up and business continuity plans. Critical issues such as these should be written into the supplier contract and the relevant key performance indicators logged and regularly monitored.

Once the supplier has been awarded the contract, it is advisable to regularly audit both the supplier's and the buying organization's processes. Suppliers should be encouraged to self-audit and report back with regular management information, and the buyer should carry out spot checks and regular scheduled audits. Where this level of detail and potential risk exists, a collaborative relationship should be formed. By meeting on a regular basis and implementing a process of continuous improvement of joint objectives, risks are generally reduced and often avoided. Relationships must be forged to ensure that both parties have a shared and mutually agreed value proposition, allowing scope for innovation and process improvement from both parties. Selecting the right supplier to engage with is critical: too small and its internal resources may not stand the pace, too large and it will see you as a nuisance and be less likely to employ joint initiatives.

It is not only the confidentiality and data protection issues that must be considered; issues that are perceived as more simple, such as getting the right person on site in a timely manner and reconciling accounts, are often overlooked. The aged debt for temporary staff agencies is a problem that has been around for some time. These aspects of the purchase-to-pay process are of equal importance as they have the potential to damage a strong working relationship between buyer and supplier and therefore affect security of supply. This value-adding, end-to-end risk consideration is where procurement professionals really make a difference.

Summary

The Cranfield study concluded that, when it comes to best-practice risk management in purchasing and supply, one size is unlikely to fit all. Analysis of how companies assessed and managed risk revealed a complex picture with distinct differences between sectors. For example, while recent disruptions to supply were a major influence in manufacturing, it was corporate responsibility risks that had the greatest impact in retail and the public sector. For financial services companies, it was changes in business strategy that drove change. The risk management tools, however, are more commonplace. Fixed-price contracts, collaborative relationships and closely monitored key performance indicators are common across most sectors. The role of the procurement professional is to ensure that both internal and external contacts are on red alert to monitor the identified weaknesses in the supply chain and act quickly to remedy them.

Risk management in the supply chain is more about resilience; risk is on the increase and is part and parcel of our business lives. Often it cannot be avoided, so a method for managing and minimizing its effects is the only way forward. A lack of time and resources is a common problem; therefore procurement professionals need to raise the awareness and understanding of supply chain risk management tools and techniques in order to obtain recognition at a senior management level and ensure supply chain risk is given the time and attention it requires.

5.7

Critical engineering and risk management: avoiding complacency

Paul Saville-King,
Norland Managed Services Limited

Introduction

The ever-increasing demands of customers, combined with the need to sustain competitive advantage in a global economy, have driven a pace of change that today's business has never experienced before. Challenges of 24/7 accessibility, speedier service and the drive for lower costs mean significant technology and communications investments are necessary to stay ahead. Add the result of global terrorism, the failure of trusted household names such as Enron and WorldCom, and the proliferation of international regulations such as Basel II and Sarbanes–Oxley, and the landscape is vastly different. These changes are further centralizing the role of technology in corporate strategy and increasing a company's dependency on information and communication systems, and the engineering infrastructure that supports them. One does not have to look too far for

evidence that this is affecting the world of facilities management in the design and day-to-day operation of increasingly complex buildings.

However, it appears widely unrecognized by risk managers and boardrooms just how much risk there is for business disruption caused by the engineering infrastructure. At a 2006 business continuity seminar there was not one agenda item relating to operational risk in an engineering infrastructure sense, and the hall of exhibitors had a notable absence of engineering service providers. This is the second year that this has been the case. One could assert that this is a failure of the 'risk industry' to recognize the potential for the immediate and the catastrophic impact associated with infrastructure failure.

This omission combines with the relatively high probabilities of such disruption happening in heavily technology-dependent businesses with traditional maintenance approaches. It appears that boardrooms sit in relative comfort, thinking that the engineering aspects of their operational risk profile are the most tangible and controllable risks they face. This is not the case. If your business is dependent on technology for communications, IT for its core business activity (for example Amazon) then you may be at increased risk. Take Reuters, which according to media reports was offline for 10 hours and unable to provide the market data that are their core product following a power outage. Share prices suffer from engineering complacency and under-investment, and the traditional mechanical and electrical services tender process drives out costs by encouraging savings in the most intangible yet critical elements of service design. Engineers' holidays and training are simple examples; these may be easy short-term savings for hungry contractors eager for new business but they will expose the client to long-term risks associated with increased staff attrition and low levels of critical engineering competence.

As with business continuity planning (BCP), investment banks are leading the way in managing their critical engineering systems. Banks are also adept at planning to meet the future challenges posed by increasing infrastructure complexity, even in the face of the common conflicts between IT and facilities management departments. Building owners and management should network with facilities staff and executives from this group to add a new perspective on engineering risk management and battle to convince core business leaders that these 'cost centres' require continued levels of significant investment, even in the face of competitive cost pressures.

Combine the above challenges with the increased 'risk awareness' that now permeates boardrooms, and what you get is a new horizon for the management and audit of 'operational risk'. A study by the Chartered Management Institute (CMI)[1] found that 70 per cent of respondents had concerns about IT systems failures and 64 per cent had concerns about communications failures. Actual disruptions followed a similar trend with 41 per cent of IT disruptions and 25 per cent of communications disruptions. Only 6 per cent of respondents to a BCI survey[2] selected loss of power as their biggest threat, but this is understandable in the current 'terror-focused' geopolitical context.

Why is critical engineering and risk management (CERM) important? Simply put, no power or cooling = no communications or IT = no business. The question

then is: 'What can I do to avoid catastrophic failure of my engineering infrastructure and the resulting impact to my business?'

Extensive data analysis[3] has demonstrated that around 90 per cent of catastrophic business-critical impact related to human or process error and not to the design of the infrastructure at all. Unfortunately for some, especially those of an engineering disposition, concentrating on the less tangible softer elements of managing risk takes people out of their comfort zone.

Industry estimates vary wildly about the actual costs of down time and there are tangible and intangible elements of this to consider. According to Gartner research, the costs of down time include:

1. productivity loss;
2. revenue loss;
3. damaged reputation;
4. impaired financial performance.

In financial terms alone, down time for a brokerage/trading institute can run at around $6.4 million per hour.[4] That equates to over $100,000 per minute. The London Chamber of Commerce found that 90 per cent of businesses that lost data in a major disaster were forced to shut down after two years.[5]

Without doubt Sarbanes–Oxley has spread its tentacles into many areas of operational risk but it seems not yet to have made a material difference where this risk is of an immediate and dramatic systemic nature (through the engineering infrastructure). A traditional mechanical and electrical maintenance services partner may not be equipped – or have the right culture and awareness – to deliver adequate risk protection, especially in the softer elements that produce the most significant risks. In some respects the industry as a whole is still 15 years behind the risk management and banking sectors, although some pioneering companies are attempting to change the industry.

A structured approach to mitigating engineering risk is recommended. The five fundamental pillars (see Figure 5.7.1) of critical engineering and risk management cover the most important aspects of this approach, namely:

- focus;
- consistency;
- compliance;
- visibility;
- learning and improvement.

The five pillars

Focus

Focus relates to the need to concentrate specifications, systems and processes on activities completely aligned with reducing or eliminating risk from the critical

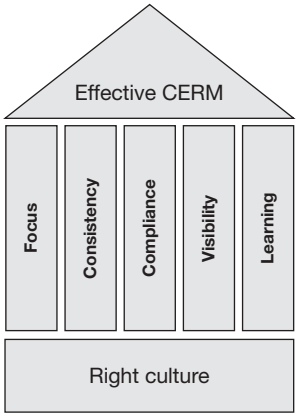


Figure 5.7.1 CERM pillars

engineering infrastructure. Examples in this respect would include challenging the norms around traditional key performance indicators (KPIs). Traditional maintenance specifications often have measures around completed maintenance tasks or reactive tasks completed on time. In reality this is often misaligned with the activities critical to keeping the customers' core business operational. Many organizations include up-time specifications within service provider contracts (such as 99.999 per cent availability) when this is recognized by industry experts[6] as impossible, even with a system-plus-system design. What does this achieve except to cause conflict between customers and supply partners even when the intent is correct? Surely it is far better to include measures and KPIs that reflect the inputs or levers that will influence the maximization of up time. Examples include many of the softer elements of service provision such as specific CERM competencies, staff motivation and levels of proactive scenario training delivery. These softer aspects pose measurement challenges, and this may be why historically many service providers and facility operators have hesitated to challenge ambiguity and define them more adequately.

Additionally, CERM best practice would recommend that the areas critical to the customer's core business are identified in a joint working group (for example the data centre or trading floors) and as a result critical engineering paths are mapped holistically. This should be in terms of geographic location, systemic interconnectivity and security/accessibility. Once completed, this review allows for a complete realignment of the planned preventative maintenance (PPM) system to focus activities on those elements of the path that are most effective for risk mitigation. This should involve new ways of working and perhaps the introduction of technologies such as hand-held units or tried-and-tested non-intrusive maintenance techniques. Around 90 per cent of existing maintenance systems can be modified without any major cost or disruption to the business.

Consistency

Consistency relates to the consistent application of 'hard earned' local knowledge, tested systems and procedures. At its most basic level, this provides a platform for measurement and benchmarking across geographic regions or even between client groups. At the more complex end of the spectrum, consistency alludes to the need to ensure that tacit knowledge[7] is transferred between team members, across boundaries and at its ultimate between homogeneous customer groups. This requires a time commitment that many incorrectly judge to be a poor investment.

Primarily, this pillar relates to the need to have consistent core processes that have passed resilience tests and deliver effective risk management from an engineering perspective, for example evolving traditional permits in use in facilities management and mechanical and electrical engineering to a system specifically designed for authorizing works relating to critical equipment and areas, thereby reducing potential risk significantly. These principles seem simple but in practice are rare in most maintenance operations.

Another essential control mechanism is the software change permit. Some senior managers have lost their jobs through failure to control the software aspects of what would otherwise have been a straightforward maintenance or project activity. In one example an 'old' revision of software – accidentally installed – on an uninterruptible power supply (UPS) protecting hundreds of trading positions caused an immediate and unplanned shutdown despite rigorous prior change management approvals. This one event cost hundreds of millions of dollars of lost revenue for an investment bank. A software control permit not only forces clarity about 'the what' and 'the when' but it also forces consideration about contingency measures and fall-back positions should things not go according to plan.

Compliance

Compliance relates to the need to ensure that critical engineering activities and measurements, and the critical processes that support them are effective. It is more than auditing although this is an essential element. It is more about stakeholder assurance and, when combined with adequate visibility, provides managers and board members with peace of mind. Traditional audit processes focus on antiquated elements of performance, usually around financial processes, statutory maintenance compliance and performance against traditional service-level agreements (SLAs). This approach is not 'critically aligned' and should be prioritized for change.

Compliance must also pick up important 'noise', which may or may not contain essential information that could prevent a future business impact. Examples include the implementation of a critical incident reporting system, which records not only detail of actual business impact but records – and more importantly encourages – the reporting of near-miss data. Most near-miss recording systems fail to differentiate those events that result in a business process change or improvement, despite this being a key ingredient for generating enthusiasm and buy-in from the engineering team.

Visibility

Visibility concerns the ability of the management team to focus on delivering or supporting the core business through having peace of mind about engineering risk. This is made possible through the accurate reporting of critical engineering exceptions and potential threats that would otherwise need to be 'mined' out of the daily furore. An example of this is the CERM risk register, which not only records current and future risks relating to the engineering infrastructure (such as design issues, union strikes and potential fuel supply shortages), but also includes a success register for risks that have been systematically eliminated. This demonstrates a progressive and unrelenting 'war on risk', especially if the unfortunate should happen and difficult questions are asked by shareholders or board members. Technology has an important role to play here, and sophisticated yet simple dependency modelling systems can facilitate effective traffic light analysis – via a web browser – of the status of all systems, processes, system capacities and competencies no matter how large or globally dispersed a company is. This is probably the most important aspect of CERM, and serious thought and investment are essential to have adequate and effective levels of visibility.

Learning and improvement

Learning and improvement demonstrate CERM as being a dynamically evolving concept. Events happen despite the best systems in the world and, apart from a reliable CERM incident response team, your service provider or expert should ensure that effective lessons-learned exercises are carried out. Structure this to reflect the McKinsey 7S model with headings of systems, structure, strategy, staff, shared values (culture), skills and (management) style. These headings provide useful insight into the concept that these elements act in harmony (or not) and that one cannot focus only on the 'hard' elements such as systems and processes. 'Soft' elements such as management style, skills, CERM strategy or 'culture' are just as likely to be complex root causes of system failure and far harder to eliminate.

The sharing and leverage of local knowledge also fall under this category. This is more difficult than it seems, and a technological solution for knowledge management will not solve the problem. Again, the 'soft' elements of critical engineering such as a risk-aware culture, CERM competencies and varied communications mediums are far more effective in this regard.

Culture and behaviours

It is clear that you can have the best systems, technology and processes in the world but, without the right culture and behaviours in the first place, these processes will be poorly applied at best, and at worst deliberately disregarded. There are several 'levers' that can be applied to driving the right behaviours and culture required for critical environments as follows:

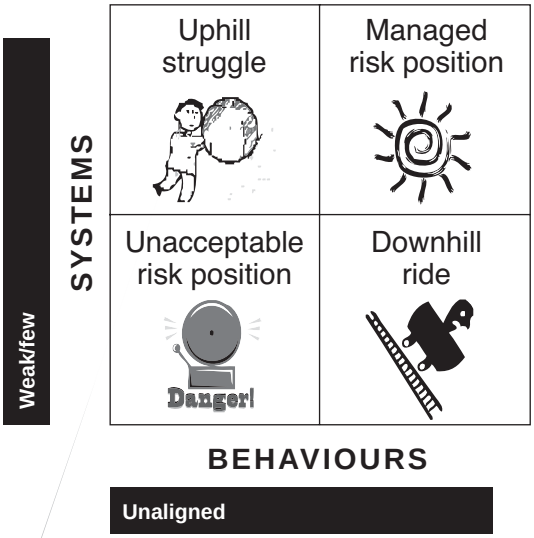
- stringent recruitment and selection in the first place based on required behaviours, not just experience and qualification;
- correct launch and communication of the need for a more robust approach to critical engineering and risk management;
- constant communication of progress and the establishment of clear metrics;
- formal training on systems and processes;
- appraisal alignment incorporating risk mitigating/highlighting behaviours;
- 360 appraisal feedback from suppliers, customers, management and peer workers;
- celebration of successes, no matter how small they seem at first;
- reward and recognition, both formal and informal;
- formal knowledge-sharing programmes.

A new model

Although the elements above are intended to provoke thought and evaluation of your current approach, it is important to select a service provider that recognizes the redundancy of traditional maintenance and is willing to work closely with you to implement a completely new model. What should be clear to you is that it is not enough to rely on systems and processes – it is the culture that counts.

This takes time, and when implementing a new CERM model – depending on the starting point – it can take up to two years to change to the desired state. Systems alone can be implemented by a proficient operator in as little as three months.

The model shown in Figure 5.7.2 provides a framework for you to assess your risk position in relation to behaviours/culture versus systems/processes. The right



6.2

Industrial pollution control – it shouldn't cost you the earth (but it could)

Fay Rushby, Environmental Health Resource Centre

Introduction

The Environmental Permitting Programme (EPP) is a joint Environment Agency, Defra and Welsh Assembly Government better regulation initiative that replaces over 40 statutory instruments with a single set of regulations – the Environmental Permitting (England and Wales) Regulations 2007, aiming to deliver more flexibility for industry, a simpler risk-based system for regulators, and continued protection of the environment and human health (EPP1). The second phase of the programme (EPP2) aims to extend the single system created by EPP1 by integrating and streamlining further environmental permitting regimes, including water discharge consenting, groundwater authorization, water abstraction and impoundment, radioactive substances regulation, and licensing

of some waste carriers and brokers. This chapter focuses on the risks and risk management associated with EPP1.

Environmental permits

For at least the last 18 years, UK and more recently English and Welsh law has required that certain 'scheduled' industrial activities must hold a permit before they are operated. Such activities (to name but a very few) include: petrol stations, print works, dry cleaners, solvent degreasers, mobile crushers, brickworks, glassworks and crematoria. The term 'scheduled' simply means that the activity or type of activity is listed in a schedule that forms part of the legislation regulating these industrial activities. The Environmental Permitting Regulations 2007 provide the current legislative framework for industrial pollution control, with many standardized permits designed to make obtaining and keeping a permit simpler and cheaper (provided you keep within the law). Get on the wrong side of the law, however, and penalties are steep; the repercussions could impact on a business much further than the initial blow to the balance sheet.

Environmental permits – do they apply to me?

This is the first and probably the most important question, the answer to which is quite definitely: yes, no and maybe. Not very helpful, I know, but if you have read Part 2 to Schedule 1 of the Environmental Permitting Regulations 2007 you will understand the sentiment. To illustrate:

- For some activities (the 'yes' activities), the need to hold a permit is absolute. Simply, if you undertake that activity (whatever 'that activity' may be) then the act of doing it means that an environmental permit is required. For example, metal foundries, dry cleaning, mobile concrete crushing, and burning waste oil in a heater (yes, really) all require a permit before the activity commences.
- For some activities (the 'no' activities), if they are not listed in the regulations then a permit is not generally required. You are however required to check the regulations and any amendments thoroughly to ensure your activity has not been recently included (this happened many times with the old PPC Regs).
- For some activities (the 'maybe' activities), the need to hold a permit and the level of permit required are dependent on operational throughput, and a permit is not required until a specific level of throughput has been achieved in any 12-month period. For these activities, such as spray painters, print works and some incinerators, operators should ensure that a monitoring mechanism is in place, along with a strategy for dealing with the application when and if it is required.

Once you have worked out if you are actually covered by the regulations, then you will need to determine to whom you apply for an environmental permit. This depends on the classification of your activity, and which 'part' of the regulations

your activity falls under. Happily, this is more straightforward, with three 'parts', known as Part A, Part A2 and Part B:

- Part A activities are the larger, more complex and potentially more polluting scheduled activities. These activities are regulated by the Environment Agency.
- Part A2 activities are large, complex and potentially polluting scheduled activities. These activities are regulated by local councils.
- Part B activities are smaller, simpler and potentially less polluting scheduled activities. These activities are also regulated by local councils.

Apply now, not later

In short, operating a scheduled industrial activity without holding a valid permit is a crime. Magistrates' court fines can be up to £50,000 per offence and/or carry up to 12 months' imprisonment (and that's hoping the council does not get clever with its prosecution strategy). Crown court fines appear to be unlimited and can carry a five-year prison sentence. Applications must be made to your regulator on a specified form and with the correct fee. The application process is relatively straightforward; however, the information required is often very detailed, and the services of a specialist consultant are highly recommended to prevent your application being delayed or even rejected. Get your application for a permit in before you start operating or reach specific operational thresholds, and get it right first time to save money and avoid being an environmental criminal.

A crushing blow for enviro-criminals

There is no such thing as 'bad publicity', or so the saying goes, but drawing the wrong sort of attention to yourself can be costly, particularly if you don't have a permit. In April 2007, the use of a mobile concrete crusher in Braintree led to a heavy deposit of dust covering 46 cars. An investigation by Chelmsford Borough Council (where the head office of the crushing operation was based) discovered that the crusher was being operated illegally. The operator did not have a permit. Chelmsford Magistrates' Court fined the operator nearly £4,000. Chelmsford Borough Council subsequently required the operator to apply for a permit (£1,470) and to pay an additional late application fee (£1,058).

Why did this happen? The operator had failed to apply for a permit and had drawn attention to the illegal activity by not controlling pollution.

A further crushing blow for enviro-criminals

So what if you haven't caused any pollution? Another unfortunate operator of a recycling operation in Wales found that even this defence was not enough. In early 2008, Rhondda Cynon Taf Council used the Proceeds of Crime Act to recover nearly £10,000 from an illegal mobile concrete crushing activity operated between March and May 2007 even though, as the Crown court was advised, no actual

pollution was caused. The operator was given a 12-month conditional discharge and was issued with a confiscation order requiring the money earned from the crushing work to be paid (as the fine) within six months or the operator would face six months in prison.

Why did this happen? The operator had failed to apply for a permit and had benefited from the crime. The council was clever about its selection and application of the law – and, while it was not believed that any environmental damage was caused, the fact no permit was attained was evidence enough.

The long arm of the law

Of course, it is easy to think of environmental risk management in isolation from all other business functions, but the implications of an enviro-crime can reach much further than the immediate interactions with the regulator. Think about your other business needs: insurance, banking and financing. Records of all convictions and cautions are held centrally by the Office of Fair Trading and are searchable by any insurer, bank or investor. A past misdemeanour could continue to hit you in the balance sheet long after you have paid your initial debt to society.

The permitting process – all change, please

The Environmental Permitting (England and Wales) Regulations 2007 (EPR) were introduced under the Pollution Prevention and Control Act 1999 and build on existing systems brought in by the Pollution and Control (England and Wales) Regulations 2000 (PPC) and Part I of the Environmental Protection Act 1990 (EPA).

Each permitting system had its own procedural nuances; fortunately, however, the permit application process of EPR is a change for the better and much more simplified than previous regimes:

1. Decide whether or not you need a permit (don't get this bit wrong – seek help if you need to).
2. Get the correct application form and any guidance you can from your regulator. If the regulator can't (or doesn't) help, get help elsewhere.
3. Fully complete your application form, including the new convictions declaration. Some of the information required is highly specialized, and unfortunately Microsoft does not do dispersion modelling computer programs. Seek expert advice where you need to.
4. Include the correct application fee. Fees and charges change annually, so make sure the regulator has got it right.
5. Wait at least 10 days for confirmation of a 'duly made application' or be ready to supply more information to support what you have already submitted. Chase the regulator for confirmation that your application has been duly made (this is particularly important for activities operating illegally, as it is the first point of recognition that you have legitimately applied for a permit).

6. Await the outcome of a 30-day public consultation period. This is the opportunity for your neighbours and competitors to be nosy and/or have a moan about you, as your application will be placed on to a public register and may be advertised locally. A separate application must be made if you want to keep commercially confidential information out of the pubic domain. The 30-day public consultation period does not apply to operators (or would-be operators) of service stations, small waste oil burners, dry cleaners or mobile plant.
7. Show the regulator around – the regulator needs to understand what you do in order to regulate you appropriately. If you can't do this, get someone in who can.
8. Review draft permit conditions. Many draft permit conditions are unworkable permit conditions; get third-party advice if you are unsure. You really do not want to saddle yourself with an unworkable permit condition that the regulator really wants to enforce.
9. Be aware of residual 'BAT', which is preventing or minimizing anything else that could pollute that the regulator forgot to write a condition about.
10. Read your permit and understand it. This includes all of the other bits – not just the operating conditions themselves. There may be many other procedural obligations that you must comply with. Ask if you are unsure.

BATNEEC, BAT and CATNIP

BAT is one of the fundamental principles of the EPR and the PPC before it. Essentially, it means 'best available techniques' and is a development of the former BATNEEC principle of best available techniques not entailing excessive cost from the EPA, except that the 'NEEC' bit has been chopped off. The subject of BAT could command a whole chapter in its own right, and covers many and varied aspects for each activity. Essentially, however, BAT is the most effective and advanced stage in the development of activities and their methods of operation that indicates the practical suitability of particular techniques for providing in principle the basis for emission limit values designed to prevent, and where that is not practical generally to reduce, emissions and the impact on the environment as a whole. Thankfully, however, Process Guidance Notes contain the Secretary of State's views on what is BAT for each category of process, and these are published on Defra web pages. The cheapest available technology not involving prosecution (CATNIP) is inviting, but usually gives more headaches than it solves problems.

Value for money or money for old rope?

So you have your permit; what happens next? Environmental permitting is a 'polluter pays' system; the price you pay is dependent on the extent to which you pollute. 'But I don't pollute', I hear you saying. Maybe not in the direct sense; however, you are still expected to cover the cost of your regulation, and in many cases you are getting excellent value for money in terms of free advice and guidance. However, not all regulators have all of the answers, and it is easy for multi-skilled officers to get lost and left behind in the masses of statutory

guidance. Also, they may be under-resourced to assist you with detailed enquiries or to help with applications or provide more technical advice. This is, of course, where the services of a specialist adviser will pay dividends and will ultimately save you time and money. Indeed, better regulation reviews now require regulators to inspect according to risk assessment. If you don't 'tick all of the boxes' during an inspection, expect to see your regulator more frequently and pay more for the privilege.

Make sure that it's the polluter that really pays

There is no escaping the fact that fulfilling your industrial pollution control responsibilities will incur an expense, but get the information you need, and at the right time, and you will see the benefits of a reduced inspection burden, cheaper subsistence charges and minimized risk liabilities through demonstrating ongoing environmental compliance.

6.3

Planning for and managing climate change

Tony Crosse, Corporate Customer Group, HSBC Insurance Brokers

Many people's perception of climate change is that it will lead to warmer conditions and that in the UK, where weather is a perennial topic of conversation, this must be a good thing. Something that many people fail to grasp is that climate change equals global warming equals disruption of the weather patterns that we have grown up with. There have been many instances of freak weather in the last hundred years or so, but generally weather patterns across the globe have been fairly stable. However, as we all know, this is starting to change.

The Gulf Stream brings warm ocean currents across the Atlantic from the Gulf of Mexico. This has a positive impact on the weather of the UK, particularly on the west side. Toronto in Canada, for example, is further south than the UK but has much more severe winters. Disruption to the Gulf Stream could mean a dramatic change in the UK's climate.

The debate about whether climate change is being caused by natural cycles or human intervention rumbles on. The knowledge of past events on our planet proves

conclusively that weather patterns go through cycles – for example ice ages – and we may be entering one of these new cycles. However, it is also certain that we have been polluting the planet to unprecedented levels since the industrial revolution, and the likelihood is that this is contributing to climate change.

Some governments and organizations have looked only at the short-term view in relation to climate change issues, but things are improving and there now seems to be a much stronger will to 'save the planet' before it is too late. Whether we have yet reached the tipping point or whether we can, or will, have any impact on reversing or slowing down climate change remains to be seen, but everyone has a moral obligation to participate in the process.

How insurance could be affected

As far as insurance cover is concerned, probably the most significant effect will be from flooding – raised sea and river levels and flash floods. More extreme weather will also have other effects, such as more hurricanes, increased storm damage, increased lightning events and more rainfall leading to local flooding owing to the inability of (sometimes antiquated) sewer systems to cope.

Extended wet conditions in areas with clay soil can lead to expansion of the soil (known as heave) that can cause damage to buildings and other structures. Conversely, extended or extreme dry conditions can lead to shrinkage of soils, which can lead to more frequent and severe subsidence damage.

Property insurance losses will increase in both magnitude and frequency as the result of climate change. Consequently business interruption losses will increase. In the future, organizations could be faced with increased deductibles, more limited availability of cover or even withdrawal of cover by insurers.

Environmental contamination will increase. Chemicals, oils and other toxic materials are more likely to spread from warehouses, factories and storage facilities if they are flooded. Hazardous materials such as asbestos may be disturbed and distributed. So, in addition to property and business interruption losses there could be considerable environmental clean-up costs resulting from flooding and other extreme weather events. There could also be an impact on other areas of insurance, for example employers' liability, health and life insurance.

What can be done to mitigate the risk

We are all aware of the plethora of measures that are now being put in place to assist in limiting damage to the environment and the campaigns to raise awareness, but organizations need to be looking at other ways to safeguard their businesses and their employees. Organizations need to be aware of their level of vulnerability at each of their locations to natural perils such as flooding. There are a number of websites, including that of the Environment Agency for England and Wales, that can be useful sources of information such as the likely vulnerability of a particular postcode to sea and river flooding.

More extremes of temperature can lead to other issues that can have an impact on organizations, employees and insurers. More sustained and colder weather conditions can lead to problems such as burst pipes, more road accidents and more slips, trips and falls. In the UK we now seem to have fewer cold spells, but other parts of the world could well be adversely affected. Carefully calculated snow loadings need to be part of the process when planning buildings in areas that are vulnerable to extensive and/or heavy snow. Increased snowfalls in some parts of the world could, in theory, lead to the collapse of buildings that are not designed to take additional weight.

Similarly, high temperatures can have various effects. Heat stress can affect people in the workplace. It may be appropriate to supply outside workers with suitable protective clothing and/or high-factor sun cream to minimize the risk of sunburn and skin cancer. Suitable precautions and procedures need to be put in place following a suitable risk assessment.

Storage areas for volatile products such as bottled gases and chemicals may need to be reassessed. Increased sunshine and higher temperatures could mean that suitable roofs or shading need to be put over such storage areas in order to keep the chemicals or gases at a safe temperature.

Equipment that is vulnerable to water damage should, where possible, be kept above ground level. Computer rooms are a good example. Some organizations in London are still installing computer and data rooms in basements. We know that the Thames barrier is being used more frequently, and this is an indication of the changing weather patterns.

The example of UK flooding

The floods in summer 2007 were unprecedented in recent times in the UK and resulted in the largest peacetime emergency response since the Second World War. The floods resulted in damage to around 55,000 properties. The UK insurance industry had a huge role to play, and the payout is expected to exceed £3 billion.

Recognizing that there are lessons to be learned, the government initiated a comprehensive review of those events. Sir Michael Pitt was appointed as the independent chair to carry out the review. His report has been published and includes 92 recommendations.

There is now a Cabinet Office Risk Register document that sets out 'our assessment of the likelihood of potential impact on a range of different risks that may directly affect the UK'. One of the sections of the 'Risk' chapter of this document looks at natural events, including sections on severe weather (storms, gales, low temperature and heavy snow, and heatwaves and drought) and flooding (coastal and inland). It also includes sections on planning by government and emergency services.

Climate change and particularly flooding will also have an effect on key services such as schools, hospitals, emergency services premises and utilities. Priority needs to be given to assessment, business continuity planning and possible mitigating actions for these key services.

Business continuity planning

The importance of up-to-date and robust emergency plans and business continuity plans (BCPs) cannot be stressed enough. Many companies that suffer serious damage and associated interruption to their business never fully recover. Many companies still do not have adequate or appropriate emergency or business continuity plans. Many more have inadequate or out-of-date plans; the latter can perversely be more of a hindrance than a help.

A well-structured BCP will have many benefits and will:

- identify and manage risks and threats to an organization;
- improve trading ability during a major incident;
- create security value for a company, its customers and its suppliers;
- give an organization a competitive edge compared to those that fail to plan;
- protect an organization's brand and image.

BCPs need to look at the risk to a business directly relating not only to an organization's own operations but also to those of customers and suppliers. For example, if a company is reliant on a key supplier, or much of its business is with one customer, then an event such as serious flooding at the supplier's or customer's premises is likely to have a financial impact on the organization in question. This risk can be assessed and mitigated in two ways: first, by taking out adequate insurance cover as an extension to the business interruption policy, for example a supplier's or customer's extension as appropriate (this can be either specified for the particular supplier or customer or as part of an unspecified extension); and, second, by finding out what precautions the supplier or customer has taken to mitigate business interruption, for example having in place a robust BCP for its own operations.

Part of the BCP process should include a business impact analysis (BIA) that analyses key risks. Many of these will not directly relate to property and business interruption damage (eg flooding), but some could have an indirect connection.

Allied to the BIA, risk assessments should be carried out in relation to the risks that could have a major impact on the business. An assessment of lightning protection on a building, for example, may identify that the lightning conductor system on the property has not been tested or inspected for several years. Any damage to the conductor or reduction in its original efficiency taking it outside of its design parameters could, in the event of a lightning strike, mean that the building or other equipment would be damaged, possibly leading to a fire. Vulnerable electrical equipment should have lightning surge protection. A lightning strike near to a building can travel through underground electric cables and up into a building and cause damage to valuable and important equipment that way.

The role of other agencies

In the UK the government, local authorities and architects, to name but a few, need to play their part in minimizing the possible effects of climate change.

Construction of buildings on flood plains has still been allowed. Even now it is reported that ministers have refused to rule out the building of the next generation of nuclear reactors in areas vulnerable to flooding. Building on flood plains not only leads to a higher flood risk for the properties being built but can also increase the flooding risk in surrounding areas. This is due to increased likelihood of water run-off and a reduction in places for water to drain away naturally because of increased areas of concrete where once there were fields.

Flood insurance is still widely available in the UK, and its availability is supported by the Association of British Insurers (ABI). However, if the government does not take more action in managing the rising flood threat we may well see the ABI's attitude change.

In conclusion

While there are clearly many possible negative impacts of climate change, there are inevitably opportunities. Businesses and insurers will need to prepare, adapt and assess the risks and opportunities available to them in an ever-changing world. Insurance will be a vital element in the efforts to adapt to climate change.

Organizations should be looking to evaluate the implications of climate change. Large companies such as HSBC are already putting significant resource into research and study of a variety of dimensions of climate change.

Some manufacturing businesses may need to look at opportunities to adapt their product range and possibly switch to alternative products, for example there is likely to be an increased demand for fixed and portable flood defence products. The construction industry, architects and planners are looking to alternative designs and methods of construction. More new buildings will be raised off the ground on stilts. Innovative designs will emerge.

The insurance industry is already looking at areas such as product ranges, public–private partnerships and other initiatives. This will no doubt result in innovative solutions.

Risk management is increasing in importance for all business sectors. The profile of risk management has been raised in recent years, and the need to protect business from the possible impact of climate change will increase its profile even more. Business continuity planning is one area of risk management that is vital for all organizations.

Climate change is inevitable. Adaptation is vital. Businesses must plan now for the new circumstances that climate change will bring and manage risks accordingly.

6.4

Dealing with the regulator

Rebecca Cushing, Field Fisher Waterhouse LLP

Introduction

Did you hear the one about the company that was fined £225,000 for failing to register under the Packaging Waste Directive? Or the one about the company charged £80,000 for running a waste business without the appropriate permit?

This is no laughing matter. Ten years ago the European Commission positioned itself as an enforcer of environmental laws rather than simply as a legislator. Since then regulatory authorities in the UK have been given increasing powers to prosecute wrongdoers. The power to investigate and penalize has seeped into local authorities and government agencies. It is no longer the sole preserve of the police to interview and charge someone whom they suspect has committed a criminal offence. Nowadays, powers once administered by the police may equally be utilized by your local health and safety officer.

While this chapter refers specifically to enforcement of breaches of environmental legislation it also has relevance for those dealing with other regulatory offences where enforcement is overseen by local authorities or government agencies. It is not possible to cover all areas in detail, but the following is intended to give a flavour of what can be expected and suggest ways of managing the risk.

The relationship between business and the regulator

The method of enforcement of environmental offences is a subject that is guaranteed to animate those who have had the misfortune to find themselves at odds with their environmental regulator. Such experiences are invariably tense and unsettling affairs, commencing with an investigation and often resulting in a criminal record. Authorities have been seen to be quick to make examples of businesses that fail to comply with environmental legislation, even in circumstances where such non-compliance was accidental. It particularly grates when the failure to comply is evidenced by non-payment of a registration fee, which is described by the Environment Agency not as omission but as 'freeloading'. Labelling a company's conduct in this way does little to promote good relations. Conversely, there has been heavy criticism that fines for wilful and deliberate breaches of environmental legislation are often too small and do not have the necessary deterrent effect. Magistrates have often been viewed as having too light a touch on such offenders.

Businesses frequently complain that no consideration by regulators is given as to how or why a company has fallen foul of the law, or to any effect that such breach may have upon its business. For some, the accidental breach of the term of a permit, or failure to register an obligated activity can have dire consequences in terms of damage to reputation or to relationships with trade affiliates, notwithstanding any separate enforcement action that may be taken (and the ensuing publicity that will invariably follow). Businesses have long maintained that regulators are too heavy-handed and impervious to justified requests for clemency.

What is enforcement?

Enforcement does not simply mean prosecution. There is a range of powers the Environment Agency can use to discipline offenders. They include the ability to issue enforcement notices, suspension and revocation notices, and improvement and prohibition notices, or to require the carrying out of remedial works. Such enforcement powers enable companies to be brought into line without the need to penalize. However, if a criminal offence has been committed then in addition to the powers set out above the Environment Agency will consider whether it should issue a warning, administer a caution or institute a formal prosecution.

Prosecution has always been considered an important part of the enforcement process, its purpose being to punish wrongdoing, to avoid a recurrence of behaviour and to act as a deterrent to others. Its application can seem obvious in cases of blatant breaches of the law, such as illegally operating a landfill site on unregulated premises, but what of the company that has unwittingly failed to register under the Packaging Waste Directive? It is difficult to see how or why the two should be treated similarly.

Evidence gathering

In many cases, the first that a company knows of its failure to comply with a piece of legislation is when it receives a letter from its regulator or local authority inviting it to provide evidence of its compliance with that legislation. Quite often the letter is accompanied by a request for a meeting. Sometimes it requests that a relevant person from the company attends an interview under caution.

It is imperative that there is someone in the business who can manage this process from the start. This means someone who not only will lead any investigation but will respond to correspondence promptly, be the preferred point of contact for the Agency and conduct interviews and investigations within the business to ascertain what has happened. If the regulatory authority knows there is someone with responsibility for conduct of the review it will invariably ease the investigative process.

The regulator's main aim in investigating a suspected offence will be to gather evidence. The regulator will want to know such things as the legal identity of the offender, where and when the offence took place, how soon corrective action was taken, and what harm occurred. This will be achieved primarily through obtaining statements and conducting interviews, as well as through physical evidence such as photographs or physical specimens. For the offending company, it is imperative for it to show that it is dealing, or has dealt, with the incident as soon as is practicable and in accordance with its own written policies. This includes conducting interviews of those involved, disciplining employees if necessary, and obtaining a clear understanding of what gave rise to the offence in question.

Make records of what was said so that there is a written account of action taken by the company. If damage has occurred as a result of the breach then the company will need to be able to document exactly what has been done to rectify the damage. This will all help to mitigate any action taken by the regulator.

If an interview under caution is requested by the regulatory authority the company should be aware that this is a formal interview carried out under the same terms as an interview in a police station; in other words, all company representatives attending the interview will be formally cautioned (using the same caution as the police use when interviewing suspects) before the interview begins. The session will be tape-recorded. The impact of an interview under caution should not be underestimated; it is a daunting procedure and can be quite intimidating for those involved. In order to get as full a picture as possible a company should ensure that it knows exactly what offence the regulator is investigating prior to interview. There should be no element of 'hijack' in the interview itself.

It is important to ensure that the right people are there to answer the questions put to them. Adverse inferences can be drawn if those representing the company are unable or unwilling to respond to questions. The interview can also be used as an opportunity for the company to put forward any material to show what has been done following the incident – mitigating circumstances, sanctioning of employees, registration with appropriate bodies, etc – and to ensure that the regulatory authority has the full facts as early as possible.

There is a serious risk in failing to attend an interview under caution, as it may amount to non-cooperation, which, if the matter does proceed to a prosecution, will be taken into account when sentencing occurs. It is also possible to ask for the interview under caution to be conducted by letter (although some authorities are moving away from allowing this); in such a case the Environment Agency will set out exactly the questions that it wants answered, and the company can then respond to them fully, again under caution.

The decision to prosecute

Once the Agency has completed its evidence gathering it will consider whether there should be a positive decision to prosecute. This is done by reference to the Code for Crown Prosecutors, a policy most usually utilized by the Crown Prosecution Service when considering whether to prosecute what one would more ordinarily consider a criminal offence. There is a two-stage test: first, is there sufficient evidence to warrant a prosecution and, if yes, second, is the prosecution in the public interest? There is a presumption of prosecution in a number of specified instances, such as incidents that involve recklessness or have significant or potentially significant environmental consequences.

If the decision is taken to prosecute then the offender will find itself answering charges in either a magistrates' or a Crown court. The court will be decided by reference to the charge. In some environmental cases the offence is one of strict liability – there is no defence to the charge – and the matter will proceed swiftly to sentencing. Aggravating and mitigating factors will be considered when setting the sentence. Thus a company that finds out that it has failed to register with an environmental regulator when it ought to have done will be treated more fairly if it admits culpability at the first available opportunity than a company that pleads guilty only when taken to court.

Sentencing

The Environment Agency is quick to name and shame those whom it prosecutes and even has a link on its website's home page directing readers to who's been 'In the Courts'. It reports that it prosecuted more people in 2007 than ever before, and it is clear that, for what are considered to be serious offences, the level of fines is on the increase. But even those companies that omit to comply (rather than wilfully cause damage) have found themselves liable to enormous fines. In February 2008, a company was fined £225,000 plus costs for failing to recycle packaging waste. The company declined to attend an interview under caution, but a response confirmed that it had failed to register for the years 2003–2005 and was unable to provide certificates of compliance for those years. The company had admitted that it had overlooked its legal obligations because of its rapidly changing business.

Fines are not the only penalty available. More use is being made of custodial sentences – seven individuals were jailed in the UK in 2007 for contravening waste

legislation alone. Suspended sentences were given to 11 defendants. The Environment Agency has also been keen to improve its ability to recover assets from those who flagrantly flout the law. The Proceeds of Crime Act 2002 allows them to do just that, permitting the confiscation of illegally obtained profits. In 2008, three such orders were made against companies that committed major waste offences. One was ordered to hand over assets of nearly £1.2 million and pay nearly £390,000 in fines and costs.

Future regulation

Over the past five years a number of initiatives examined whether there was a need to regulate more effectively and, if so, how that could be achieved. Importantly, the initiatives looked specifically at better regulation without recourse to criminal sanctions in the event of wrongdoing. Two such reviews, the Hampton Report (2005) and the Penalties Review (2006), stressed the need to ensure a model of regulation that is proportionate to risk. It was noted that reliance upon criminal prosecution failed to give regulators adequate means to deal effectively with many cases in a proportionate and risk-based way.

As a consequence of these reviews, the Regulatory and Enforcement Sanctions Act 2008 will now provide regulators with significant new powers to impose civil penalties in the field of regulatory enforcement. The Act seeks to establish a risk-based approach to regulation. As and when regulatory enforcement is necessary there will now be a number of alternatives to criminal prosecution. The Act has a number of different sanctioning powers available, such as fixed fines for various low-level offences of non-compliance to variable fines for more serious offences (which cannot exceed the maximum permissible in the magistrates' court) to notices and undertakings. If penalties are imposed then no criminal prosecution can take place. How the sanctions will be implemented in practice remains to be seen.

And is the Environment Agency finally responding to criticism? Under a new chief executive and in its 10th year of reporting, the annual *Spotlight on Business* – a review of environmental performance by businesses over the previous year – has a far more business-friendly approach than earlier editions. Where once the report focused primarily upon naming and shaming polluters, it now provides a far more rounded analysis of environmental performance within the business community. Does this reflect a more fundamental sea change in enforcing regulation?

The Companies Act 2006

Company directors should further note that the judgement of a company's environmental performance is no longer the sole preserve of the environmental regulators. Under the new Companies Act there is now a duty upon directors to promote the success of the company. Section 172 (1) states: 'A director of a company must act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole, and

in so doing must have regard (amongst other things) to… (d) the impact of the company's operations on the community and the environment'.

This requirement introduces a much wider corporate social responsibility into the decision-making process of a director. But it also means that directors will be asked to make difficult decisions that may not always seem to sit easily with shareholders' interests. Considering the environment and community may not be at the forefront of directors' minds, say, when looking to acquire new premises or take on new business suppliers.

What this means is that, even if a business manages to keep external regulators at bay, there is a residual risk that its internal regulators (the shareholders) have a right to complain if they are not happy with business policy on environmental matters. This reinforces the need to appoint personnel with responsibility for environmental matters, to have an environmental policy in place and to keep abreast of legislation. It also makes it advisable to make and retain minutes of meetings at which conflicting interests are discussed so that the discussion process is recorded in the event of there being a later challenge.

Conclusion

The present system promoting criminal prosecution of regulatory offences has surely provided a barrier to the development of a working relationship between regulators and business. The prosecuting powers given to regulators are too often wielded without sufficient consideration of the impact and effect a criminal prosecution will have upon a business and its reputation. The average business perceives little proportionality between an offence and its subsequent treatment and likely penalty. Clearly there are better ways of regulating business – the new legislation should go some way towards providing a response based upon the risk itself rather than simple wrongdoing. While the Companies Act legislation has not yet been tested by the courts, it is now even clearer that there is an important link between responsible business behaviour and business success. It is also clear that sanctions for failing to meet environmental responsibilities will no longer be the sole preserve of the regulators but will now be actionable by a company against its directors.

Appendix: Contributors' contact list

Appleyards
Appleyards House
72 Brighton Road
Horsham
West Sussex RH13 5BU
Tel: +44 (0) 8705 275201
Contact: Allan Robinson
e-mail: allan.robinson@appleyards.co.uk
www.appleyards.co.uk

Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
Tel: +44 (0) 20 7693 5600
Contact: Jacqueline Needle
e-mail: jneedle@beckgreener.com
www.beckgreener.com

Bird Goën & Co
Klein Dalenstrat 42A
B-3020 Winksele
Belgium
Tel: +32 (0) 1648 0562
Fax: +32 (0) 1638 0528
Contact: William Bird
e-mail: ipadmin@birdgoen.com

Black Diamond Risk
3478 Buskirk Avenue, #1007
Pleasant Hill
CA 94523
United States
Tel: +1 (0) 925 746 7186
Contact: Robert M Mark
Tel: +1 (0) 925 212 7348
e-mail: bobmark@blackdiamondrisk.com
www.blackdiamondrisk.com

Callcredit
One Park Lane
Leeds
West Yorkshire LS3 1EP
Tel: +44 (0) 113 244 1555
Fax: +44 (0) 113 234 0050
Contact: Louise Rodgers
e-mail: louise.rodgers@callcredit.co.uk
www.callcreditgroup.com

Chartered Institute of Purchasing and Supply (CIPS)
Easton House
Easton on the Hill
Stamford PE9 3NZ
Tel: +44 (0) 1780 756777
Fax: +44 (0) 1780 751610
Contact: Liz Lees
e-mail: liz.lees@cips.org
www.cips.org

Citicus Limited
Holborn Gate
330 High Holborn
London WC1V 7QT
Tel: +44 (0) 1306 742072
Contact: Marco Kapp
e-mail: marco.kapp@citicus.com
www.citicus.com

Close Credit Management
2 Jessops Riverside
800 Brightside Lane
Sheffield S9 2RX
Tel: +44 (0) 114 242 6628
Contact: Martin Smith
e-mail: info@closecm.co.uk
www.closecm.co.uk

College Hill
The Registry
Royal Mint Court
London EC3N 4QN
Tel: +44 (0) 20 7457 2020 or +44 (0) 1869 353 800
Fax: +44 (0) 20 7866 7900
Contact: Chris Woodcock
e-mail: corporate@collegehill.com
www.collegehill.com

Environmental Health Resource Centre
13 Oak Lodge
50 Eversley Park Road
London N21 1JL
Tel: +44 (0) 78 0234 9581
Contact: Fay Rushby
e-mail: fay@ehrc.org.uk
www.ehrc.org.uk

Federation of European Risk Management Associations (FERMA)
Avenue Louis Gribaumont
1B – 1150 Brussels
Tel: +32 (0) 27 61 94 32
Fax: +32 (0) 27 71 87 20
Contact: Florence Bindelle
e-mail: info@ferma.eu

Field Fisher Waterhouse LLP
35 Vine Street
London EC3N 2AA
Tel: +44 (0) 20 7861 4000
Fax: +44 (0) 20 7488 0084
Contact: Rebecca Cushing
e-mail: Rebecca.Cushing@ffw.com
www.ffw.com

Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH
Tel: +44 (0) 20 7377 1377
Fax: +44 (0) 20 7377 1310
Contact: Peter Finnie
e-mail: pjf@gje.co.uk

Halcrow Group Limited
Vineyard House
44 Brook Green
Hammersmith
London W6 7BY
Tel: +44 (0) 20 7602 7282
Fax: +44 (0) 20 7603 0095
Contact: Tenia Chatzinikoli
e-mail: chatzinikolit@halcrow.com
www.halcrow.com

HSBC Enterprise Risk Management
Bishops Court
27–33 Artillery Lane
London E1 7LP
Tel: +44 (0) 207 661 2410
Contact: Andrew Oxland
e-mail: andrewoxland@hsbc.com
www.insurancebrokers.hsbc.com

HSBC Insurance Brokers
Bishops Court
27–33 Artillery Lane
London E1 7LP
Tel: +44 (0) 7941 20551
Contact: Gavin Temple
e-mail: gavintemple@hsbc.com
www.insurancebrokers.hsbc.com

HSBC Operational Risk Consultancy
Bishops Court
27–33 Artillery Lane
London E1 7LP
Tel: +44 (0) 735 7661 2853
Contact: David Breden
e-mail: davidbreden@hsbc.com
www.hsbc.com

Institute of Risk Management (IRM)
6 Lloyd's Avenue
London EC3N 3AX
Tel: +44 (0) 20 7709 9808
Fax: +44 (0) 20 7709 0716
Contact: Ian Fraser
e-mail: ianfraser@theirm.org
www.theirm.org

InterContinental Hotels Group, Global Risk Management
Broadwater Park
Denham
Buckinghamshire UB9 5HR
Tel: +44 (0) 1895 512 272
Contact: John Ludlow
e-mail: john.ludlow@ihg.com
www.ihg.com

Lloyd's Register Quality Assurance (LRQA)
LRQA Centre
Hiramford
Middlemarch Office Village
Siskin Drive
Coventry CV3 4JF
Tel: +44 (0) 24 7688 2387
Fax: +44 (0) 24 7630 6055
Contact: Sarah-Jayne Whitworth
e-mail: sarah.whitworth@lrqa.com
www.lrqa.com

Lucidus Consulting Limited
90 Long Acre
Covent Garden
London WC2E 9RZ
Tel: +44 (0) 20 7060 2196
Fax: +44 (0) 20 7060 2198
Contact: Ruth Murray-Webster
Mobile: +44 (0) 7974 943443
e-mail: ruth@lucidusconsulting.com
www.lucidusconsulting.com

McKinty and Wright
5–7 Upper Queen Street
Belfast BTI 6FS
Tel: +44 (0) 28 9024 6751
Fax: +44 (0) 28 9023 1432
Contact: Sean McGahan
Direct line: +44 (0) 28 9041 2820
e-mail: sean.mcgahan@mckinty-wright.co.uk
www.mckinty-wright.co.uk

Manigent
117 Waterloo Road
London SE1 8UL
Tel: +44 (0) 20 7921 0022
Contact: Andrew Smart
e-mail: andrew.smart@manigent.com
www.manigent.com

Norland Managed Services Limited
454–460 Old Kent Road
London SE1 5AH
Tel: +44 (0) 20 7231 8888
Contact: Paul Saville-King
e-mail: paul.saville-king@norlandmanagedservices.co.uk
www.norlandmanagedservices.co.uk

Outperform UK Ltd
The Long House
Assembly Road
Coedpoeth
Wrexham LL11 3SS
Tel: +44 (0) 870 116 1293
Fax: +44 (0) 871 750 3386
Contact: Andy Murray
Direct line: +44 (0) 77 7630 1602
e-mail: andy.murray@outperform.co.uk
www.outperform.co.uk

SAS UK & Ireland
Wittington House
Henley Road
Medmenham
Marlow
Buckinghamshire SL7 2EB
Tel: +44 (0) 1628 486933
Fax: +44 (0) 1628 483203
Contact: Mark Elkins
e-mail: mark.elkins@suk.sas.co
www.sas.com/uk

Stewart Business Software
Russet House
39 Main Road
Middleton Cheney
Oxfordshire OX17 2ND
Tel: +44 (0) 1295 712955
Contact: Kelly Lehmann
Mobile: +44 (0) 79 1025 4288
e-mail: kelly@stewart-software.co.uk
www.stewart-software.co.uk

SunGard Availability Services (UK) Limited
Units 12–13 Bracknell Beeches
Old Bracknell Lane West
Bracknell
Berkshire RG12 7BW
Tel: +44 (0) 800 143 413
Contact: Piper Anna Shields
e-mail: piper.shields@sungard.com
www.sungard.co.uk

UKAS
21–47 High Street
Feltham
Middlesex TW13 4UN
Tel: +44 (0) 20 8917 8493
Contact: Jon Murthy
e-mail: jon.murthy@ukas.com
www.ukas.com

XL Insurance Group
XL House
70 Gracechurch Street
London EC3V 0XL
Tel: +44 (0) 20 7933 7000
Contact: Donal Kelly
e-mail: donal.kelly@xlgroup.com
www.xlinsurance.com

Index

application processing 90
asset liability management, and ERM 11

bridging science and communication 29
business change environment, risk management in 19 *et seq*
  business strategy 20
business consultant 85
business continuity management 217
  future considerations (1A) 219, 221

claims funds, repatriation 207
climate change, planning and managing 301 *et seq*
  business continuity planning 304
  insurance considerations 302
  risk mitigation 302
  UK flooding 303
collections and recovery 92
communication networks 30
communications, importance 119
Comprehensive Credit Assessment Framework (CCAF) 97
compulsive risk assessment psychosis (CRAP1) 158
conspiratorial risk aversion policy (CRAP2) 158
corporate manslaughter 148 *et seq*
  new Act
    preparation 152
    ramifications 152
    new offence 150
counter-terrorist security programme 183
credit marketing 90
credit risk assessment/loan decisions 94 *et seq*
  SAS system 97
credit risk management 89 *et seq*
  capturing revenue opportunities 95
  and compliance 98
  analytic advances 99
customer management 91

data security 214
defensive effort to business-shaping asset 122
disposal and discharge of waste 291
dispute resolution, alternative (ADR) 141, 142
  common UK form 142
  cost risks 145
  determination, mediation 143, 144
    risk management approach 146

enterprise risk management (ERM) xxix, 6
  effective 50 *et seq*
  implementing 6
  measurement 8
  in practice 44
  role in business 11
  solutions 40 *et seq*

in theory 41 *et seq*
environment management systems 292
environmental criminality 297
environmental offences
enforcement 307
evidence enforcement 308
prosecution decision 310
and the regulator 307
environmental permits 296
permitting process 298
environment permitting programme (EPP) 295
environmental risk 287 *et seq*
key legislation and directives 288 *et seq*
regulation 288

financial interest cover 206
agreed valuation 207
financial scandals, effects of 5

global compliance trap, avoidance 203 *et seq*
disadvantages 204
global programmes 203
local solutions 203

health and safety expert 84
health, safety and welfare management 268
horizon scanning 123
hotel security risks 196, 199
human factors 105

industrial pollution control 295 *et seq*
information risk management 181 *et seq*
failure, causes of 187
principles into practice 188
insurance and capital market synthesis 13
insurers, and risk management 83
intellectual property risk, business 161
acquisition 162
due diligence 165
exploitation, monitoring, enforcement 163
IP rights, effective use of 139
IP risk estimation and management, patents and patent portfolios 168 *et seq*
commercial risks 169
patent auctions 174
patent portfolio 172
SMEs 173
third-party infringement 174

job boundary abolition 31

litigation risk 127 *et seq*, 128, 129
avoiding 140
costs 129
law, language of 156
managing, language of 155 *et seq*
preparedness 129
the team 131

operational risk
capital, upper boundary 242
definition 236
earnings volatility method 238
financial institution investment decision 236
tail event method 240
operational risk framework 235 *et seq*
operational risk management 227 *et seq*
data sources 232
modelling 227 *et seq*, 233
difficulties 228
parameters 230

patent litigation 134
cost and frequency 135
enforcement cost 136
procedures 135
other countries 137
permissible insurance cover 205
permissible unlicensed taxes 206

receivables industry, use of e-commerce 211 *et seq*
control 212
reporting recalls 33

reputation
  as asset 69 *et seq*
  bad 76
  benefits 76
  dilemmas 72
  importance 70, 75
  managing 80
  risk 69, 74 *et seq*
    measurement 77
    capital quantification 78
  threats to 70
risk
  banking and insurance solutions 13
  embedding 56
  emerging, solutions 16
  enterprise-wide solutions 16
  non-financial, solutions 14
  ownership 217 *et seq*
  and performance management 111 *et seq*, 112
    combining (P &RM) 114
    operational considerations 115
  perspective 51
  quantification of 14
  strategy 24
    integrating 53
  tools 55
  risk appetite 51
risk-based performance 255 *et seq*
  in action 261
  and risk management 257
  as solution 258
risk identification and team coherence 248 *et seq*
  methodology 250
  programme organization 251
risk-managed business change 27
risk management 113
  barriers to introduction 19
  business benefit 83 *et seq*
  creative techniques 107
  and critical engineering (CERM) 276 *et seq*, 253
    compliance 280
    down time losses 278
    new model 282
  delivering business value 103 *et seq*
  manufacturers' 86
  process 25
  published standards and methods 104
  strategy, introduction 21
risk and reputation management, new horizons 118
risks, key, and vulnerabilities 54

scares, avoiding 121
security risk management, integration of 193 *et seq*
  hotels, threats to 196
  new strategy 194
strategic purchasing and supply risk management 271 *et seq*
  business risk environment 273
  temporary staff 274
supply chain complexities 33
supply chain risk, managing 265 *et seq*
  environmental concerns 266
  supply chain resilience 267
  trial process, planning 159

threat and vulnerability assessments 198

UKAS 86
uncertainty 60
  graphical representation 61
  management 63
  or risk 59

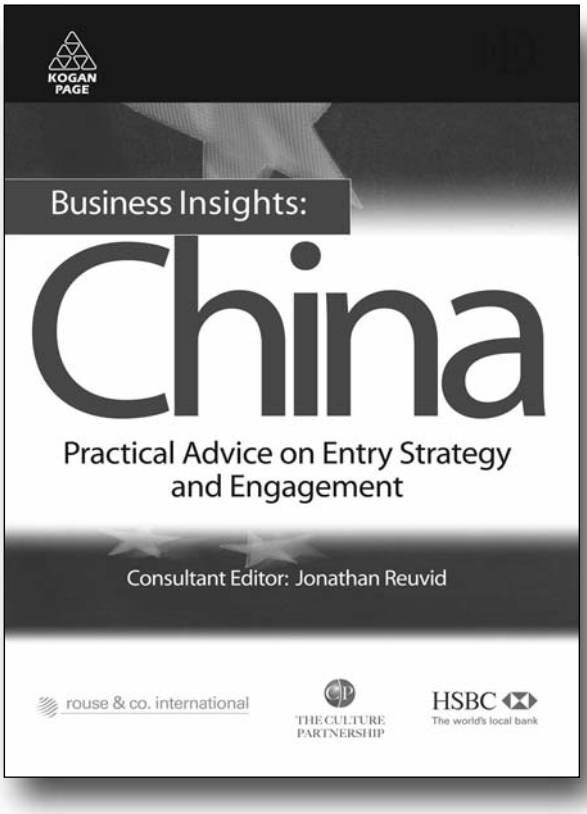
value, building of 9
value generators and protectors 271
vulnerability, company 119

Index of advertisers

Appleyards 58, 247
Beck Greener 133
Bird Goën & Co 167
Callcredit Ltd 88
CCH – A Wolters Kluwer business xv
CIPS 270
Citicus Ltd 180
Close Credit Management 209–10
The Copyright Licensing Agency Ltd xxv–xxviii
Environmental Health Resource Centre 294
Field Fisher Waterhouse xviii, 286
Gill Jennings & Every LLP viii
Halcrow 49
Harrison Goddard Foote 176–78
HSBC Insurance Brokers Ltd 10–11
Intercontinental Hotels & Resorts 192
IRM v–vii
LRQA 264
Lucidus Consulting xix
Manigent 254
Marsh ix–xii
McKinty and Wright Solicitors 154
Outperform 18
Risk Consulting Ltd xxiii–xxiv
SAS ii, 38–39
Stewart Business Software 110
Sungard Availability Services 216
UKAS 82
XL Insurance 202

ALSO AVAILABLE FROM KOGAN PAGE

"For any business thinking of doing business in China, the information in this book will make it a 'must read'. The practical advice it contains, written and edited by experts, will be of enormous assistance – and I commend it to you."
Miles Templeman, Director General, Institute of Directors



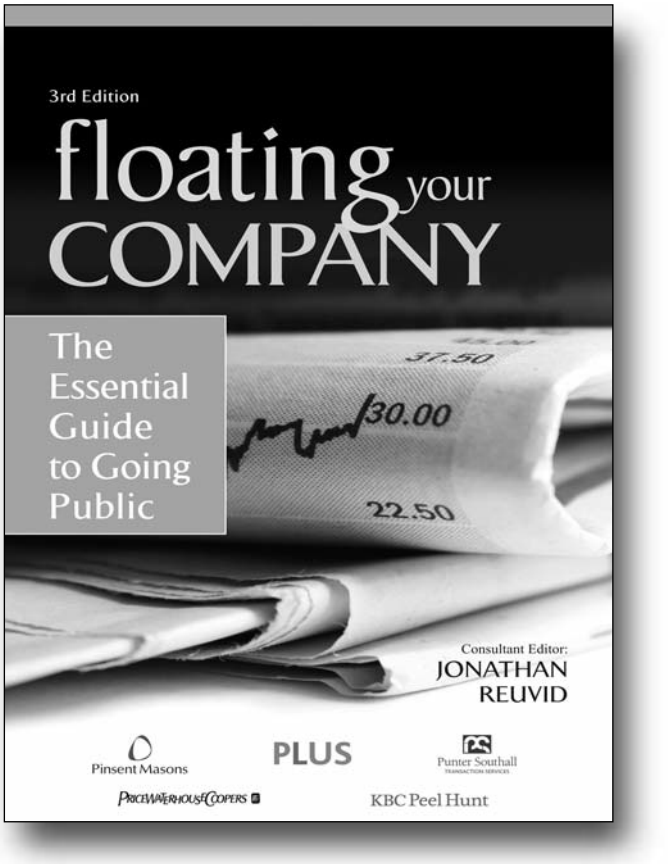
ISBN: 978 0 7494 5062 5 Hardback 2008

Order online now at www.koganpage.com

Sign up for regular e-mail updates on new Kogan Page books in your interest area

ALSO AVAILABLE FROM KOGAN PAGE

"A detailed explanation of the whole floatation process."
Commerce and Industry



ISBN: 978 0 7494 5056 4 Hardback 2007

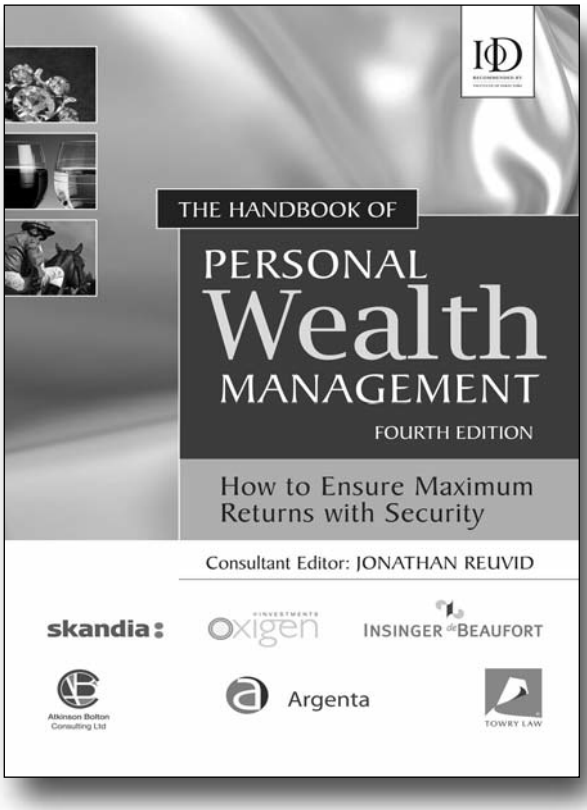
Order online now at www.koganpage.com

Sign up for regular e-mail updates on new Kogan Page books in your interest area

ALSO AVAILABLE FROM KOGAN PAGE

"Offers jargon-free advice on how to manage your personal and business-related finances and covers all aspects on wealth management in clear and comprehensible language."

Pensions World



ISBN: 978 0 7494 5060 1 Hardback 2008

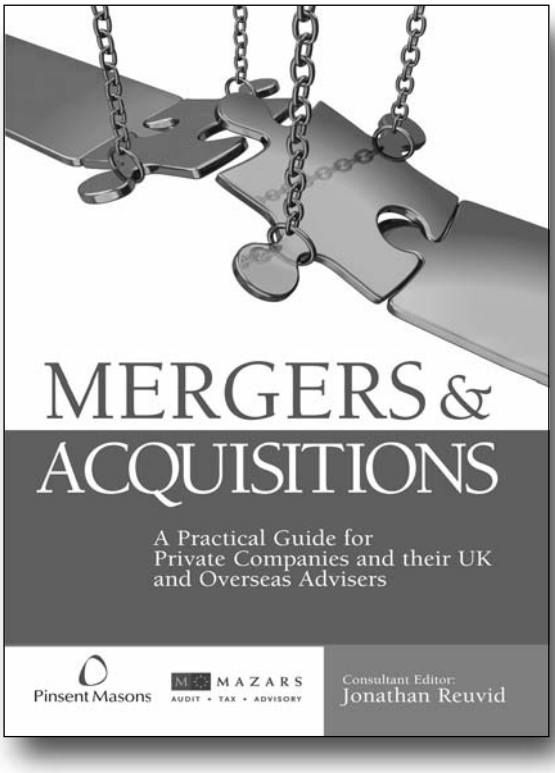
Order online now at www.koganpage.com

Sign up for regular e-mail updates on new Kogan Page books in your interest area

ALSO AVAILABLE FROM KOGAN PAGE

"This handy guide provides a detailed explanation of the options for those companies considering merging with or acquiring another business, and the often rather convoluted process."

Securities and Investments Review



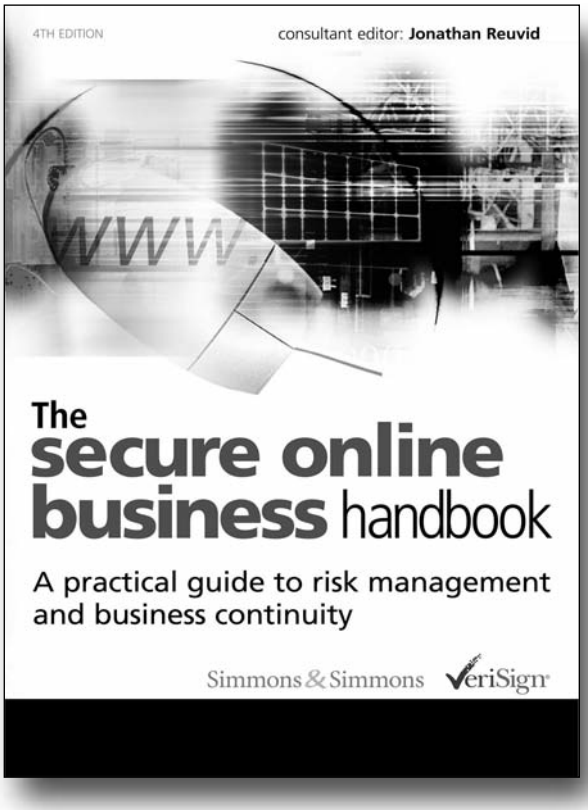
ISBN: 978 0 7494 5269 8 Paperback 2008

Order online now at www.koganpage.com

Sign up for regular e-mail updates on new Kogan Page books in your interest area

ALSO AVAILABLE FROM KOGAN PAGE

"A practical guide for managers in developing and implementing appropriate strategies for online risk management."
Management Services



ISBN: 978 0 7494 4642 0 Hardback 2006

Order online now at www.koganpage.com

Sign up for regular e-mail updates on new Kogan Page books in your interest area