

A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance

CONTENTS:

Preface, by Senator George Mitchell

Preface, by Steve Mellish, FBCI, The Business Continuity Institute

Introduction

1. A Risk-Based Approach To Business Continuity
2. Stakeholders
3. Governance, Good Practice, Standards, Regulation and the Law
4. Culture, Strategy, Performance, Risk and Business Continuity
5. Getting Started: The Business Continuity Management Cycle
6. Introduction to the Business Impact Analysis
7. The Business Impact Analysis: A Hitch-Hikers Guide
8. Application and Uses of BIA Information
9. Technology, Exposures and Continuity
10. Dependency Management: Supplier Management, Outsourcing and Business Support
11. Opportunities and Other Applications for Business Continuity Tools and Principles
12. The People Factor
13. The Value of Insurance When Facing Potentially Catastrophic Risk
14. Communications
15. Emergency and Governmental Services
16. Rehearsals and Exercising of Plans and Risk Decision-Making
17. Maintenance, Benchmarking, Assurance and Audit
18. Developing a Plan - Putting Theory Into Practice

APPENDIX

A: British Standard PAS 56, Guide to Business Continuity Management, Annex

B: BCM Evaluation Criteria

Glossary

EXCERPT FROM THE INTRODUCTION

As business practices and sensitivities change, Business Continuity Management (BCM) is increasingly a central and crucial tool for the risk manager. Responses to the Bi-annual Risk Management and Risk Financing Survey by AON in 2005 amongst risk managers, insurance managers and finance directors of the United Kingdom's top 1,000 organisations placed business continuity as the second most important risk issue that concerns them. The greatest concern, protection of the brand value, and others in their top ten, (1) loss of reputation, (4) product liability/tamper, (5) regulatory/legislation (6) physical damage, (8) terrorism, (9) corporate governance and (10) professional indemnity, are all commercial survival issues and key elements of continuity management.

BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/430>

The consequences of damage by a risk incident might not just be quantifiable initially in monetary terms, such as in the loss of valuable assets or by destructive levels of litigation. The consequences might involve the loss of life or valuable dependencies that are necessary for the organisation's very survival. These include intellectual assets, brand values, regulatory approvals, legality, the confidence of its various stakeholders, and its ability to deliver urgent, contracted, products and services on time. Furthermore the consequence may be that the organisation has to step away from its marketplace for a period of time and give free reign to competitors to do lasting damage to the customer, supply or distributor base.

The damage, of course, may not only be within the organisation. There could be destruction of the legal or physical environment on which the organisation depends. An urgently needed "just in time" supplier or distributor might be the one directly affected by a disaster, but their failure to deliver as contracted may have an equally destructive impact on the production line of the organisation expecting urgent and key ingredients into their own products.

We set out to write this book because we have seen thinking about business continuity starting to evolve from its roots in IT back up and contingency equipment and facilities departments, typically referred to as "disaster recovery.". We believe, though, that these roots are still often the drivers for business continuity and its practitioners and that they, and too often their employers, remain within these narrow thought horizons. The modern business is much more complicated than this, is exposed to entirely new dependencies and criticalities, and, in spite of its wealth and scale is even more exposed to single, organisation-wide exposures to destruction than in earlier business models. This causes us great concern and we feel significantly exposes organisations to destruction and total failure.

In the same way that risk management has moved on from being the purchase of insurance products, business continuity needs to emerge from its silos and position itself as part of the much wider risk and strategic management framework of the organisation. This book sets out to take the reader forward and has, we believe, important messages for chief executives, directors, non-executive directors, risk managers, continuity managers, internal and external auditors, investment managers, compliance managers, finance directors, project managers, regulators, education programmes and others.

An important aspect is that different organisations - and even personalities within an organisation - can take very different views on acceptability and unacceptability of risk exposures. They will make these decisions within their different backgrounds and cultures, and also the quite different pressures upon them. A bank, servicing credit cards and cash machines 24 hours, seven days a week, will take an entirely different view on acceptable gaps in service than an organisation where customers could reasonable wait a few days for the contracted service, product or for another response. Some organisations, especially those using e-commerce distribution may have competitors who could upsize and respond incredibly quickly to any difficulties seen in another player in their marketplace. It is for this reason that the amount of time lost or "time out" from the market place is another vital consequence for the risk manager.

Equally an organisation cannot allow damage to destroy their financial and other business controls over their organisation. An insurance company may, for example, be dealing at any one time with current claims valued at many billions of pounds and will have reserved accordingly. To lose records and thus intellectual control over such a claims portfolio could totally destroy that organisation.

BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/430>

OPTIONS AVAILABLE TO THE BOARD

As always, the responsibility for risk understanding and management rests firmly with the board of directors. The board may delegate the processes for achieving risk understanding and risk management, but it cannot delegate the responsibility. Once the risks and the potential consequences are understood, the directors cannot ignore them and must make decisions around the information obtained. This is not just a regulatory issue, it is simply good management.

The decision could be that the exposure is an acceptable one. This might be a reasonable decision if the potential worst-case consequences are clearly understood and the board considers that they could not possibly have an unacceptable impact on their own people, their stakeholders, balance sheets, controls, legality, market presence, brand values, revenue accounts nor cash flows. If the exposure, however, is deemed to be unacceptable then the organisation has further choices to make:

- The board can invest resources to manage the exposure or the potential consequences down to what is considered to be the acceptable level.
- It could, of course, decide to avoid the particular activity or environment altogether.
- It can enter into a contract to transfer the risk into an insurance product or to another counterparty.
- It can prepare beforehand for the consequences of a risk incident; knowing that, with that preparation, that business critical dependencies are safe and that the strengths of the organisation can be used to manage through the consequences without unacceptable damage.

The risk manager could use one of the tools listed above, but in practice is more likely to use the most cost-effective and commercially realistic combination.

It is worth mentioning at this point the ability of the organisation's lawyers to transfer by contract the potential cost of risk to suppliers, distributors or other counterparties. There is no real value however, when a risk incident destroys a just-in-time and critical supplier or a distributor; and that it in turn by its failure damages or destroys the risk manager's own organisation's ability to remain in business. The lawyer's view needs also the additional and important dimension of business continuity. Furthermore it is interesting to recognise that the most destructive of risks highlighted by the AON survey are not insurable ones in the conventional insurance market. 'We didn't need risk management because we had insurance' is too often a cry from the corporate grave.

This book deals with the last of the four options listed above, i.e., business continuity management. The message of this book is that business continuity forms just part of a much wider and coordinated risk management programme that sets out critically to understand what the exposure is and the consequences of that exposure. We believe, in just one example, that there is a crucial role at strategic level for the business continuity manager when an organisation is considering, choosing and establishing contractual and operational relationships with a potential outsourced supplier. This book takes a view across the options available for managing any exposure, or potential impact that would be life-threatening to the organisation. It is important, though, that the reader keeps in mind throughout this much wider picture of risk and risk management that BCM as just one of the tools available to be used in isolation or in conjunction with the others. The existence of a business continuity manager, especially one whose task is only to 'recover' the organisation from a physical disaster, is very likely to be raising expectations of resilience well beyond the ability to deliver.

CONTINUITY AND ITS RISKS

We should begin with the rather obvious but important maxim that - if the organisation allows itself to die during the risk incident - the best continuity planning will provide nothing more than a mechanism for trying to revive an already dead horse.

During a potentially catastrophic disaster in a modern multinational, the board's attention is on the survival of the business. It is too easy to consider only the insurers' view and believe that the most important concern is the replacing of buildings and contents, or defending from litigation. The loss of physical operations; whether they be buildings, contents, equipment or similar are, of course, important. The risk manager's view on BCM embraces these issues but also needs to look way beyond. It is crucial to consider the foundation stones, and thus vital dependencies, that enable a modern business to survive. These can then be matched against stakeholders who, in their own way are critical dependencies. Only then, we suggest, can we see the real post-damage pressures, and what is needed to be done, before the incident too, to ensure that the organisation can be kept alive.

In recent years, there have been important changes in the way businesses deliver and market their own products; changes too in their relationships with their stakeholders, and in the risks themselves.

Many a modern organisation can fairly be described as made up of no more than a brand, miners of owned or rented intellectual assets, controls, and outsourcing contracts. These ingredients have become crucial, urgent dependencies and single points of risk for the very survival of that organisation.

STAKEHOLDERS

It is valuable to also consider organisations from the perspective of their stakeholders. We could recognise stakeholders simply as those organisations and individuals that have a 'stake' or interest in the current organisation's affairs. The stakeholders demanding the attention of the continuity risk manager are not just investors; they include internal and 'outsourced' employees, customers, suppliers, distributors, financiers and their advisors, and the political, legal and natural environment. Their needs and demands are different and in some cases contradictory.

If these are not problems enough, in the real world of damage, the problems of a company reeling from serious damage, are just beginning. All sorts of new stakeholders emerge, identified by their abilities and propensities to react to damage. These stakeholders can shift the ground even further away from underneath managers in already difficult circumstances, to keep the organisation alive. These include competitors, the media as wholesalers of confidence, the brand values, bankers, credit rating agencies and regulators. Many organisations have, of course, their own unique stakeholders in addition.

This book sets out to look at these processes, stakeholders and dependencies and places them firmly at the strategic issue end of the Board's attention. Above all, this book sees business continuity not just as something to remove a threat, but as something that is as much about opportunities for development and for enabling the much wider objectives of the organisation.

BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/430>

THE EVOLUTION OF IMPACT

Risks themselves, therefore, have not only changed, but also the potential for damage from these new risks is totally different. Furthermore, consider the potential for damage to the organisation that can occur from old risks. A fire or storm damage that occurs in a building housing a group-wide computer system causes damage that is unrecognisable from the extent of damage we could envisage in past business models from a fire in one building.

So many of these risks are not physical ones. The loss of intellectual assets, the reputation, key stakeholders walking away, a drop in credit rating raising significantly the cost of capital and destroying dependant financial models, are just a few of the impacts that would cause so much more damage than the loss of buildings and their contents. This concentration of single points of destructive risk too can cause the skills of one individual or small team to be skills on which the entire delivery of a multinational depends.

BUSINESS CONTINUITY MANAGEMENT

The issue we address is not just the individual continuity manager's own department: it is more than this. It is about ensuring, at the highest level in an organisation, that continuity is not something that is pushed aside as unimportant, but needs to be positioned, structurally, and especially in business understanding and skill levels, in the very heart of today's organisations. To do otherwise is just lip service, and creating a risk in itself, because it will raise expectations amongst stakeholders including shareholders, employees, customers and regulators, and as such is more dangerous than having no 'business recovery' position at all.

EXCERPT FROM THE PREFACE BY SENATOR GEORGE J. MITCHELL

"The escalating pace of change, a rising tide of technological innovation, almost instantaneous transmission of breaking news and the globalization of crime and terrorism, all combine to provide a heady cocktail of challenge for today's organization.

"Clear to all business watchers are the dramatic ways that businesses have responded to these challenges and reorganized themselves, as they have taken up the opportunities available. These include new uses for technology, faster and direct to customer communications, increasingly open foreign market opportunities, outsourcing and off-shoring, harnessing the power of the brand, sophisticated supply chain management, just-in-time delivery cycles, the ability to mine huge databases in milliseconds, and new relationships with the workforce.

"These elements of the modern business may offer great flexibility and a magnificent ability to relate precisely to the needs of individual customers and other stakeholders. They have, however, also given rise to critical dependencies and single points of potential catastrophic risk and failure. Organizations can upsize and respond to new selling opportunities very quickly indeed. If an organization is fighting through a crisis, its competitors will most likely be well positioned to seize any opportunities created by the distraction and diversion of attention that recovery can demand. Interestingly therefore, the risk of sudden destruction of today's modern organization, however huge, diverse, financially strong and multinational, is more likely than businesses using the models seen in the 1990s and before.

"The most critical failure points are not financial. Company boards have long established financial risk measuring mechanisms but the response to these new exposures and the growing influence of regulators are driving boards increasingly to consider non-financial risk. This is tougher to quantify, harder to grasp and consequently can give rise to boards feeling less comfortable and in control and consequently, less confident.

BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/430>

“Business Continuity Management is coming of age to respond to the new needs of its own stakeholder, the organization for which it carries the responsibility. It is indivisible from risk management and is an increasingly important tool of risk management. The Continuity Industry leaders are now looking well beyond technology and other infrastructure replacement, and see a crucial value for themselves at the very top of level of their organization’s strategy setting. They set out to understand the importance of these dependencies, measure the risk and impact in its very widest sense, and then ensure resilience and an ability to respond and recover to a level that the whole range of stakeholders are entitled to expect.

“This book is a must read for those senior managers, risk managers and continuity managers who have the vision to see both the new opportunities and the new responsibilities of business continuity management.”

George J. Mitchell, Chairman
DLA Piper Rudnick Gray Cary
Former Senate Majority Leader and
U.S. Senator for Maine
Senator Mitchell successfully chaired
the peace negotiations in Northern Ireland.

EXCERPT FROM THE PREFACE BY THE BUSINESS CONTINUITY INSTITUTE

“At last, a book for those involved in risk and business continuity management that proves beyond doubt why the traditional 'silo approach' to risk management and business continuity management must be removed and replaced with a modern day 'joined up' approach to protecting a business and the interests of its stakeholders.

“Today’s business world faces an increasing assortment of risks and threats that can have devastating effects. However we should not lose sight of those day-to-day incidents that can ultimately result in ‘death by a thousand cuts.’

“This book, written by authors with acclaimed knowledge, experience and wisdom within both risk management and business continuity management, provides clear guidance supported with a wide range of memorable and highly relevant case studies for any risk manager or business continuity manager to successfully meet the challenges of today and the future.”

Steve Mellish, FBCI, Chairman
The Business Continuity Institute

BUY ONLINE FROM: <http://www.itgovernance.co.uk/products/430>