ENTERPRISE RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS
BEST PRACTICES - excerpt from the foreword

“This book is intended to provide guidance and examples for the identification, management and control of risks. Wherever practicable, we have used case studies and examples to illustrate the points.

“It is impossible to cover every industry, every process and every activity in a work of this sort. We have therefore made the work as comprehensive as practicable and focused particularly on those risk areas of generic value to the reader, while providing references and case studies relevant to specific market sectors.

“Many examples are provided throughout this guide: these all have their roots in real cases and come heavily laden with pragmatism. Over fifteen years experience in blue chip environments, large and small, public and private, has gone into developing some of the methods described. Others come with a respected pedigree from a variety of industries. Your own "right way" for risk management means picking, matching and tailoring from the cases and examples provided and building on existing best practice within your organization.

“Where practicable we have provided examples of different methodologies so that the one most appropriate to the reader's organization's business continuity maturity and culture can be selected. The author is also conscious that it can only be a partial picture of what is a global business continuity industry. However, we have tried to be representative as far as practicable, illustrating issues, approaches and requirements from various countries.”

ANDREW HILES, FBCI
Oxon Bagpuize, England
January, 2002

HOW TO USE THIS BOOK

This book is laid out in the logical sequence of Risk and Impact Analysis activities:

Section 1 provides a general introduction to risk management and impact analysis
Section 2 covers risk evaluation and control and provides practical examples
Section 3 addresses impact analysis as a pragmatic blueprint
Section 4 covers risk and continuity theories and strategies, illustrating some of the science, math and methodologies behind risk assessment
Section 5 deals with insurance issues and insurance as part of the risk management mix
Section 6 shows how to write a risk and impact assessment report
Section 7 offers a guide to organizations that can provide further help and identifies sources of further information
Section 8 identifies tools for risk assessment and business impact analysis

Buy online from www.itgovernance.co.uk/products/124
Each Section is backed up by an Appendix that provides explicit information, examples and helpful documents. The Acknowledgments and Bibliography list where further information may be found. If you have a general interest in risk management, or if you are a manager responsible for that function and just need a quick overview of the subject, simply read the Introduction and Summary to each Section. This will help you to decide how much more detail you need. If anything in the Summary is not clear or obvious, turn back to the Table of Contents for the relevant section - this will show you where to look for more depth.

If you are recently appointed to have risk management responsibilities for a particular area, scan the Table of Contents to identify where the particular aspects of risk appear (e.g. Project Risk, Health & Safety etc).

If you are a student of risk or want to understand the A-Z of risk, the book is laid out in a logical order - go through each chapter in sequence for the theory and general practice. You can then return to each Chapter for checklists, forms etcetera. These are provided in the Appendices to each section.

If you are a seasoned risk professional, use the book as a source of reference and to spark new ideas. Flick through the Table of Contents and dip into the book, selecting topics of interest and examples from the Appendices that jump out at you. Also look at the way other industries, market sectors or countries approach risk and decide how portable they are to your specific situation.

Whatever your interest level and experience, we believe there is something of interest and value for you in the pages that follow.

---

**EXCERPT: WHY THIS BOOK?**

“Some fourteen years ago I was founder and Chairman of Survive, the international user group for business continuity management. Almost ten years ago Survive gave birth to the Business Continuity Institute (the industry's professional association). Both bodies were concerned with the issues of recovering from business disasters. Typically the recovery involved doing something different: alternate locations, operations, equipment, IT and telecommunications facility. It all implied a hiatus - an interruption, a period of uncertainty and disruption, before a semblance of normality was restored.

“The Business Continuity profession included the disciplines of risk management and an understanding of the impact on the business, should those risks actually occur. But then, so did many other functions within the business. Maybe the IT Disaster Recovery function was separate from business contingency planning. Operational Risk Management then had a fairly narrow role, typically looking at specific operational functions. Insurance was something else, often the remit of the Finance Director or someone called a Risk Manager who was, in fact, mainly concerned with

Buy online from www.itgovernance.co.uk/products/124
insurance aspects. There was usually someone else responsible for compliance issues, while yet another person was accountable for health and safety issues. An audit function was responsible for fraud. Typically, the organization had no overall view of risk and no individual with overall responsibility for it: fragmentation was normal.

“Then, a few years ago, there appeared an emerging tide of acknowledgment that these risk-related functions should be brought together. The reason may not always have been logic: sometimes, it stemmed from downsizing and a putting together of these functions for productivity, rather than strategic reasons. For some, Y2K projects created a sense of urgency and an impetus that promoted this as pragmatic logic. Some companies had the vision to take a holistic approach to risk management and to create what we have come to call Enterprise Risk Management.

“We have been privileged to help a number of companies through this process and facilitate the creation or enhancement of their risk resilience: in short, helping them move from an expectation of disruption and subsequent recovery to a position where effective risk management all but eliminates the disruption.

“Several years ago, I was presenting a workshop on disaster recovery planning to an international audience and a German in the front row was looking increasingly puzzled. At the coffee break, I asked him if, perhaps, I was using unfamiliar terms or whether I was not making myself clear. "No," he said. "I understand perfectly what you say. It's just that, in Germany, we are not allowed to have a disaster." Now, many years later, it is evident that he had a point. While we cannot legislate disasters, we can seek to minimize them. Of course, the unimaginable can always happen (as we have learnt from recent horrific events) and we have to be prepared to deal with the human and business consequences of it. But increasingly foresight can prevent many situations that previously may have become unexpected disasters.

“This book results from a wish to share best risk management practice - not from the perspective of a theorist, but from a practitioner's viewpoint.”

TABLE OF CONTENTS

PREFACE
FOREWORD
HOW TO USE THIS BOOK

SECTION ONE: INTRODUCTION
1.1 What is Risk Management?
1.2 Why Risk Management
1.3 Why This Book?
1.4 Risk Management and Quality
Category 1 Leadership
Category 2 Business Information Management & Analysis
Category 3. Business Planning
Hiles – more information

Category 4. Human Resource Development and Management
Category 5. Process Management
Category 6. Customer and Market Focus
Category 7. Business Results
1.5 The Importance of Business Leadership
1.6 Enterprise Risk Management

SECTION TWO: RISK EVALUATION & CONTROL
2.0 Introduction
2.1 DRII/ BCI Unit 2
2.2 Definitions: Hazards, Threats, Risks and Assets
2.3 Risk Assessment - The Need
2.4 System Safety Programs and HAZOP
2.5 Health & Safety - Risk Assessment
2.6 Control of Major Accident Hazards Regulations 1999 (COMAH)
2.7 Risk Management for Finance and the Finance Sector - Compliance Issues
2.8 Gramm-Leach-Bliley Reports
2.9 Food and Drugs Administration (FDA) Compliance
2.10 Risk Assessment in the Food Industry
2.11 Health Care
2.12 Risk Assessment in Other Industries
Table 2.1 Risk Guidance and Compliance
2.13 Risk Assessment: Statutory Requirement and Duty of Care
2.14 Project Risk
2.14.1 Project Risk Factors
Figure 2.1: The Project in Context
2.14.2 Project Management Organization Structure
2.14.3 Project Roles
2.14.4 Project Management Methodology
Figure 2.2: Example of Project Management Methodology
2.14.5: Why Projects Fail
Figure 2.3: Causes of Project Failure
2.15 Example of Risk Assessment Guidelines: The Turnbull Report
2.15.1 What is Turnbull? Why?
2.15.2 The Turnbull Process
2.15.3 Making Progress
2.16 Risk Requirements in Germany
2.17 Risk Assessment - The Process
Figure 2.4 Schematic of Risk Assessment Process
2.18 Options for Risk Management
2.19 The Turnbull Approach to Risk Assessment
2.20 Critical Component Failure Analysis
2.21 A Swedish Approach
2.22 Operational Risk Management
2.23 An Output Approach to Risk
2.23 Security and Siting - Risk Areas
2.26 Supplier and Outsourcing Risk
2.26.1 The Increasing Supply-Side Risk

Buy online from www.itgovernance.co.uk/products/124
2.26.2 Outsourcing Issues
2.26.3 Getting Outsourcing Right
2.26.4 The Importance of Service Level Agreements
2.26.5 Vendor Evaluation Criteria
2.26.6 Relating Contract Type to Service
Figure 2.5 Contract Relationships
2.26.7 Lessons from Experience
2.28 Condition Assessment & Financial Condition Assessment
2.28.1 What is Condition Assessment?
2.28.2 Financial Risk Assessment in the Insurance Industry
2.29 US Banks: Risk-Based Assessment System
2.30 Causes of Business Interruption
Figure 2.6: Analysis of Business Interruptions
2.31 Automating Risk Management
2.32 Summary
Appendix A to Section Two: Possible Threats
Appendix B to Section Two: Example of a Simple Risk Analysis
Appendix C to Section Two: Example Health & Safety Risk Checklist
Appendix D to Section Two: The E-Bomb - The New Threat
Appendix E to Section Two: Risk Analysis in IT Projects
Annex 1 to Appendix F: IT Project Risk Assessment
Appendix G to Section Two: Infrastructure Project Risk Management Framework
Annex 1 to Appendix G: Example High Level Risks for an Infrastructure Project
Annex 2 to Appendix G: A Major Infrastructure Company Approach
Appendix H to Section Two: Cost Items to Consider in Financial Authority
Appendix I to Section Two: Example of a Risk Management Database
Appendix J to Section Two: Example Assets
Appendix J to Section Two: Example Assets
Appendix K to Section Two: Murphy Rules!

SECTION THREE: BUSINESS IMPACT ANALYSIS
3.1 DRII/BCI Unit 3
3.2 What is BIA?
3.3 The BIA Project
3.4 BIA Data Collection Methods
3.5 Critical Success Factors: Definitions
Figure 3.1: Critical Success Factor / Business Process Matrix
3.6 Key Performance Indicators
3.7 Process Flows
3.8 Outputs & Deliverables
3.9 Activity Categorization
3.10 Desk Review of Documentation
3.11 Questionnaires
3.12 Interviews
Figure 3.2: Summary of BIA Interview Data
3.13 Workshops
3.14 Observation
3.15 Business Impact Analysis - Financial Justification for BCM

Buy online from www.itgovernance.co.uk/products/124
3.16 Grounds for Justification
3.17 Life and Safety
3.18 Marketing
3.19 Financial
Figure 3.3 Average Normalized Share price Variation % Following a Disaster
3.20 Compliance / Legal Requirements
3.21 Quality
3.22 Summary: Financial Loss
Table 3.1: Cost of Disaster - Causes
3.23 Designing an Impact Matrix
Table 3.2: Simplified Impact Analysis
3.24 Time Window for Recovery
Figure 3.4: Risks and Outage
Figure 3.5: Time Window for Recovery
3.25 Resource Requirements
Figure 3.6: Effect of Coincident Workload Peaks
Figure 3.7 The Backlog Build-up
3.26 Summary
Appendix A to Section Three: Resource & Timescale for Provisioning
Appendix B to Section Three: Example of Risk & Impact Analysis
Appendix C to Section Three: Marketing Protection
Appendix D to Section Three: The Cost of Lost Data
Appendix E to Section Three
Table 1: Cost of Downtime
Appendix F to Section Two: Background Information for BIA

SECTION FOUR: RISK & CONTINUITY THEORY & STRATEGIES
4.1 Introduction
4.2 Valuation of Risk and Flexibility
4.3 Techniques for Valuing Risk and Flexibility
4.4 Stochastic Processes
4.5 General Risk Theory
4.6 Investment Risk
4.7 Random Finite Abstract Sets (RFAS) Theory
4.8 Sensitivity Analysis
4.9 Quantitative Risk Analysis
4.10 Qualitative Risk Analysis
4.11 Boolean Simulation
4.12 Bayes Theorem
4.13 Monte Carlo Simulation
Figure 4.1: Example of Monte Carlo Model
Table 4.2: Contacts for Monte Carlo Analysis Tools
4.14 Decision Tree Analysis
Figure 4.3 Example of Decision Tree Analysis
4.15 Dependency Modeling
4.16 Computer Risk Assessment and Management Methodology (CRAMM)
Figure 4.4: CRAMM Principles
4.17 Value at Risk
4.18 Risk Methods and Techniques: Conclusion
ANDREW HILES, FBCI, is founder and Chairman of Survive, the international user group for business continuity planning and was a founding Director of the Business Continuity Institute, the international body for certification of business continuity professionals. He is a founder Director of Kingswell, international consultants. Having commenced his management career with the Royal Air Force, he pioneered IT systems before leaving to take up a position within the Finance Department of London Transport. Subsequently in their Central Productivity Unit he was a Senior Projects Manager and later became responsible for the business re-engineering function, implementing new services and major technical projects. He left to take up a position with the UK Post Office as their first Business Systems Consultant responsible for major projects. Andrew then joined the UK Atomic Energy Authority at the Harwell Laboratories where he managed the supercomputing, mainframe and other bureau and facilities management services.

Andrew was a founding director of Kingswell, an international consulting company with a blue chip client base specializing in Enterprise Risk Management, Business Continuity, and Disaster Recovery and in Service Management. Andrew is a pragmatic global consultant and trainer in these areas.

Andrew is an international speaker on risk management, business continuity and contingency planning and has featured on conference programs in the USA, Southern Africa, Europe, the Middle East and the Pacific Rim. He has presented workshops and seminars on these topics for Frost & Sullivan (Europe), IIR/ IFF (Europe and Middle East), AIC (South Africa), CEL (Hong Kong), UPOM (Saudi Arabia) and other companies having also lectured at Ashridge, Cranfield, GEC Dunchurch and Henley Management Colleges in the UK. He has broadcast on radio, TV and on Internet webinars.


Andrew is a Fellow of the Business Continuity Institute, a Member of the British Computer Society and a Freeman of the City of London.

Buy online from www.itgovernance.co.uk/products/124