

## **BUSINESS CONTINUITY: BEST PRACTICE, 2ND EDITION**

### **EXCERPT FROM THE FOREWORD TO THE 2ND EDITION**

The events of 9/11 have cast a long shadow over the world and led to a vital reappraisal of Enterprise Risk Management and Business Continuity Management.

The Federal Reserve Bank of New York, Federal Reserve System, the Office of the Comptroller of the Currency, the New York State Banking Department, and the Securities and Exchange Commission sponsored the Financial Industry Summit, held on February 26, 2002. I can do no better than to repeat Roger Ferguson's summary of the key vulnerabilities that regulators and institutions have to face in the aftermath:

- First, contingency planning generally did not account for region-wide events. Some firms found they lost both primary and back-up sites. There were significant concerns about the loss of or inaccessibility of staff.
- Second, concentrations, both market-based and geographic, were really evident and became a source of vulnerability.
- Third, the critical interdependencies across the industry, although understood in the context of planning Year 2000, were never so readily apparent. This was evident in the impact of the problems at key infrastructure providers on wide range of financial institutions. Even institutions far removed from New York City were significantly affected by interdependencies.

These factors apply not only to financial institutions that were particularly hit by the tragedy, but also to many other industries that could be impacted by disasters having a similar impact.

Key lessons have been painfully learned:

- People issues are paramount: staff availability, risk awareness and training are critical.
- Operations distributed over a wide geographic area have a better chance of recovering and may recover quicker. Reliance on single points of failure should be avoided.
- Focus on the outcomes of disaster rather than the causes and on the deliverables rather than on the processes of delivery.
- It is not enough to pay lip service to business continuity: planning must be whole hearted, thorough and tested. Testing may need to extend across the industry, across industries and into the supply chain, including infrastructure providers.

It is our hope that effective risk management, emergency and continuity planning may help to prevent deliberate disasters and to mitigate the consequences of those that do occur.

Andrew Hiles

## **EXCERPT FROM THE PREFACE**

**Melvyn Musson, FBCI, CBCP, CISSP**

I was very pleased to be asked to write a preface to this much-needed book. There are many books that have been written covering various aspects of hazard control, emergency response, disaster recovery and business continuity, but not one that pulls all areas together under the auspices of the individual sections of the BCI and DRII Professional Practices.

Why my interest? To quote from a letter I wrote to the National Fire Protection Association (NFPA) in 1991 when they were considering the establishment of a Technical Committee to develop a Standard on Disaster Management:

Disaster Management, or Business Continuation Planning as we prefer to call it, is a natural progression from Hazard/Loss Control through Emergency Response to the recovery process.

The best hazard/loss control programs cannot prevent emergency or catastrophic situations occurring. The emergency response procedures that most companies have developed or which may be required by law, deal with such aspects as initial fire fighting, evacuation, life safety, etc. - what one might term the stabilization of the situation. They cover the first hours of the emergency. They do not deal with the long-term recovery, which could take several months.

Disaster Management, or some other similarly named program, is needed to enable the company to institute procedures to return to normal operations as soon as possible.

That standard is now available as NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs. Within that standard are details of the BCI/DRII Professional Practices, albeit as part of the various sections of the standard and not as an individual, specific section.

In addition to NFPA 1600, other standards and guides such as BS7779 in Great Britain and the recent Australian Risk Management Standard are incorporating the Professional Practices either by specific reference or wording relating to the practices.

The advent of the Turnbull Report introduces a new consideration and need, which the Professional Practices can support.

This makes it all the more important to have a reference material that can clearly detail what should be considered in each of the ten subject areas, together with appropriate examples and details of not only the benefits but also the problems that can be expected with each of those subject areas. Andrew Hiles has been able to do so in the development of this book. In addition, since Andrew intends to issue periodic updates, this book becomes a living document, which will address both changes in the Professional Practices and developments within the industry.

## **TABLE OF CONTENTS**

### **CONTENTS**

### **DEDICATION**

### **ACKNOWLEDGEMENTS**

### **CONTENTS**

### **FOREWORD TO THE 2ND EDITION**

### **PREFACE - MELVYN MUSSON, FBCI, CBCP, CISSP**

### **FOREWORD BY THE BUSINESS CONTINUITY INSTITUTE (BCI) - JOHN SHARP**

### **FOREWORD BY THE DISASTER RECOVERY INSTITUTE INTERNATIONAL (DRII) - PAUL R. THOMAS, JR. AND BENNY D. TAYLOR**

### **INTRODUCTION**

### **BUSINESS CONTINUITY ROAD MAP: INTRODUCTION**

### **1 PROJECT INITIATION AND MANAGEMENT**

1.1 DRII/BCI Unit 1 Project Initiation & Control

1.2 Business Continuity Project - Activities

1.3 Business Continuity - Project or Program?

Figure 1.1: Bc Maturity Pyramid

1.4 Defining the Need: Scope of Business Continuity

1.5 Defining the Need: What Is a Disaster?

1.6 Disaster Defined

1.7 Recovery Timescale

Figure 1.2: Time for Recovery

1.8 Communicating the Need - Awareness: the Dangers

1.9 Communicating the Need - Awareness: Benefits of Business Continuity Planning

1.10 Establish BC Policy

1.11 Establish a Planning / Steering Committee

Figure 1.3: Example of Steering Committee Structure

1.12 Project Planning

1.13 Develop Initial Budgetary Requirements

1.14 Report to Senior Management

1.15 Making it Stick - Other Motivators

1.16 Summary

Appendix a to Chapter One: Project Initiation Checklist

Appendix B to Chapter One: Examples of Briefing Information

Appendix C to Chapter One: Examples of Disaster Recovery Project

Appendix D to Chapter One: Examples of Project Terms of Reference & Scope, Business Continuity Project

Appendix E to Chapter One: Example of a Simple Business Continuity Project Plan

Appendix F: Indicative Project Deliverables and Investment -Phase 1 of Pilot Project

Business Continuity Road Map: Chapter 1

### **2 RISK EVALUATION & CONTROL**

2.1 DRII/ BCI Unit 2 Risk Evaluation & Control

2.2 Definitions: Hazards, Threats, Risks and Assets

2.3 Risk Assessment - the Need

2.4 Health & Safety - Risk Assessment

- 2.5 Control of Major Accident Hazards Regulations 1999 (COMAH)
- 2.6 System Safety Programs and HAZOP
- 2.7 Risk Management for Finance and the Finance Sector - Compliance Issues
- 2.8 Food and Drug Administration (FDA) Compliance
- 2.9 Risk Assessment in the Food Industry
- 2.10 Health Care
- 2.11 Risk Assessment in Other Industries
- Table 2.1 Risk Guidance and Compliance
- 2.12 Risk Assessment: Statutory Requirement and Duty of Care
- 2.13 Example of Risk Assessment Guidelines: the Turnbull Report
  - 2.13.1 the Turnbull Process
  - 2.13.2 Making Progress
- 2.14 Risk Requirements in Germany
- 2.15 Risk Assessment - the Process
- Figure 2.1 Schematic of Risk Assessment Process
- 2.16 Options for Risk Management
- 2.17 the Turnbull Approach to Risk Assessment
- 2.18 Critical Component Failure Analysis
- 2.19 Operational Risk Management
- 2.20 an Output Approach to Risk
- 2.21 Security and Siting - Risk Areas
- 2.22 Summary
- 2.23 Case Studies
- Appendix A to Chapter Two: Possible Threats
- Appendix B to Chapter Two: Example of a Simple Risk Analysis
- Appendix C to Chapter Two: the E-bomb: the New Threat
- Appendix D to Chapter Two: Fire Hazard from Computer Tapes
- Appendix E to Chapter Two: Possible Threats: Smoke Tests
- Appendix F to Chapter Two: Foot & Mouth: a Preventable Disaster
- Appendix G: Site, Environmental & Health & Safety Risk Assessment Checklist
- Business Continuity Road Map: Chapter 2

### **3 BUSINESS IMPACT ANALYSIS**

- 3.1 DRII/BCI Unit 3 Business Impact Analysis
- 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 Business Impact Analysis - Financial Justification for BCM
- 3.15 Grounds for Justification
- 3.16 Life and Safety
- 3.17 Marketing
- Figure 3.3 the World's Top Ten Brands
- 3.18 Financial
- Figure 3.4 Average Normalized Share Price Variation % Following a Disaster
- 3.19 Compliance / Legal Requirements
- 3.20 Quality

3.21 Summary: Financial Loss  
Table 3.5: Cost of Disaster - Causes  
3.22 Designing an Impact Matrix  
Table 3.6: Simplified Impact Analysis  
3.23 Time Window for Recovery  
Figure 3.7 Risks and Outage  
Figure 3.8 Time Window for Recovery  
3.24 A Tiered Approach to Business Continuity Planning: Relationship of Business Continuity and Service Level Agreements  
Figure 3.9 Tiered Availability  
3.25 Resource Requirements  
Figure 3.10 Effect of Coincident Workload Peaks  
Figure 3.11 The Backlog Build-up  
3.26 Summary  
Appendix A to Chapter Three: Resource & Timescale for Provisioning  
Appendix B to Chapter Three: Example of Risk & Impact Analysis  
Appendix C to Chapter Three: Example of a Service Level Agreement Using Tier Rating  
Business Continuity Road Map: Chapter 3

## **4 DEVELOPING CONTINUITY STRATEGIES**

4.1 DRII / BCI Unit 4: Developing Continuity Strategies  
4.2 Vital Materials and Back-up  
4.3 Business Continuity Strategy: Options  
4.3.1 Bunker  
4.3.2 Continuous Processing  
4.3.3 Distributed Processing  
4.3.4 Alternate Site  
4.3.5 Quick Resupply  
4.3.6 Off-Site Storage  
4.3.7 Working from Home  
4.3.8 Reciprocal Arrangements  
4.3.9 Buying-in or Outsourcing  
4.3.10 Buffer Stock  
4.3.11 Other Recovery Services  
4.4 Option Comparison  
4.5 Contractual Arrangements for Recovery Services  
Figure 4.1: Recovery Options and Recovery Timescale  
4.6 Lateral and Creative Thinking  
4.7 the Role of Insurance  
Figure 4.2: Insurance Relationships  
4.8 Using Consultants  
4.9 Summary  
Appendix A to Chapter Four: Example of a BC Project  
Business Continuity Road Map: Chapter 4

## **5 EMERGENCY RESPONSE & OPERATIONS**

5.1 DRII / BCI Unit 5: Emergency Response & Operations and Unit 10 Coordination with Public Authorities  
5.2 Types of Emergencies  
5.3 Coordination with Public Authorities (DRII /BCI Unit 10)  
5.3.1 DRII/BCI Standards  
5.4 International Coordination  
5.5 US Department of Homeland Security  
5.6 National Incident Management System  
5.7 National Interagency Incident Management System  
5.8 The US Federal Emergency Management Agency (FEMA)  
5.8.1 About FEMA

- 5.8.2 FEMA's Role in Anti-Terrorism
- 5.8.3 FEMA's Powers
- 5.8.4 US State Emergency Authorities
- 5.9 Office of Critical Infrastructure Protection and Emergency Preparedness Canada
- 5.10 Emergency Management Australia
- 5.11 Local Incident Control and Escalation
- Table 5.3 UK "Blue Light" Services: Command Structure
- 5.12 UK National Arrangements for Responding to a Disaster
  - 5.12.1 Overview
  - 5.12.2 Roles
  - 5.12.3 Combined Response
- 5.13 Public Relations & Crisis Communication (DRII/BCI UNIT 9)
  - 5.13.1 DRII/BCI Competencies
  - 5.13.2 Crisis Communication
  - 5.13.3 Role of Media Management
  - 5.13.4 Communication with Stakeholders
- 5.14 Salvage and Restoration
- 5.15 Summary
- Appendix A to Chapter 5: Example Emergency Plans
- Appendix B to Chapter Five: Emergency Response Acronyms
- Business Continuity Road Map: Chapter 5

## **6 DEVELOPING & IMPLEMENTING THE BCP**

- 6.1 DRII/BCI Unit 6 Developing and Implementing Business Continuity Plans
- 6.2 Introduction
  - Figure 6.1 the Anatomy of BC Plan Development
- 6.3 Plan Introduction
- 6.4 Identify Teams
  - Figure 6.2 Example BC Organization
- 6.5 Tasks, Actions and Functions
- 6.6 Roles and Responsibilities
- 6.7 Alternative Locations (Standby Locations)
- 6.8 Contact Details for Internal and External Contacts
- 6.9 Vital Documents and Materials
- 6.10 Resource Requirements
- 6.11 Reporting Processes and Requirements
- 6.12 Audit Trail
- 6.13 Confidentiality Status, Version Control and Document Configuration Management
- 6.14 Structure of the Plan
  - Figure 6.3 Example Organization and BC Plan Structure
- 6.15 Interim Plans
- 6.16 Software Tools for Plan Development
- 6.17 Summary
- Appendix A to Chapter 6: Example Office Services Plan for a Professional Practice
- Appendix B to Chapter 6: Example Contents of Generic Bc Plan Appendices
- Appendix C to Chapter 6: Business Continuity Planning Software
- Appendix D to Chapter Six: BC Software Checklist
- Business Continuity Road Map: Chapter 6

## **7 AWARENESS & TRAINING PROGRAMS**

- 7.1 DRII/BCI Unit 7: Awareness & Training Programs
- 7.2 Establishing Objectives and Components of the Program
- 7.3 Identifying Functional Awareness and Training Requirements
- 7.4 Developing the Training Methodology
- 7.5 Acquiring or Developing Training Aids

7.6 Identifying External Training Opportunities  
7.7 Identifying Vehicles for Corporate Awareness  
7.8 The Macquarie University Report  
7.9 Summary  
Appendix A to Chapter Seven: Staff Skills Assessment Matrix  
Appendix B to Chapter Seven: Disaster Management Internet Hot List  
Emergency Services News Groups  
Emergency Services Mailing Lists  
Catalogues, Publication Lists, Computer Data Bases  
Business Continuity Road Map: Chapter 7

## **8 MAINTAINING & EXERCISING THE BCP**

8.1 DRII/BCI Unit 10: Maintaining & Exercising the BCP  
8.2 BC Plan Audit & Review  
Table 8.1 Bc Plan Audit Areas  
8.3 the Need for Exercise  
8.4 Exercise Strategy  
8.5 Exercise Methods  
8.5.1 Talk Through  
8.5.2 Walk-through  
8.5.3 Role Play Scenario  
8.5.4 Disaster Drill: Pull the Plug  
8.6 A Structured Approach to Plan Exercising  
8.7 When to Exercise  
Table 8.1 Exercise Checklist  
8.8 Post Exercise Reporting  
8.9 Summary  
Appendix A to Chapter Eight: Example of Notes of an Exercise Planning Meeting  
Appendix B to Chapter Eight: Scenario for a Plan Walk-through  
Appendix C to Chapter Eight: Example Brief for Observers  
Appendix D to Chapter Eight: Test Scenario - Initial Briefings and Situation Reports (Sitreps)  
Business Continuity Road Map: Chapter 8

## **9 STANDARDS AND GUIDELINES**

9.1 Introduction  
9.2 USA: NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs  
9.2.1 Introduction to NFPA 1600  
9.2.2. NFPA 1600 Content  
9.2.3 Compliance with the NFPA 1600 Standard  
9.3 US Federal Emergency Agency (FEMA) Disaster Planning for Business and Industry  
9.4 Federal Financial Institutions Examination Council (FFIEC) Guidelines  
9.5 Canadian Standards Association CAN/CSA-7731-M95, Emergency Planning for Industry, a National Standard for Canada  
9.6 South Africa Disaster Management  
9.7 British Standard BS 7799 Standard in Information Security Management  
Table 9.1: BS 7799 Controls  
9.8 Australia AS4444 Standard in Information Security Management  
Table 9.2 AS 4444 Sections and Objectives  
9.9 Australia: Australian National Audit Office Better Practice Guide, Business Continuity Management, Keeping the Wheels in Motion  
9.10 Standards Australia OB/7 Working Group Business Continuity Management Guideline Draft Version 2.1  
9.11 UK Defence Council Instruction DCI GEN 170/98 Business Continuity  
9.12 UK Office of Government Commerce Bc Planning Guide

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/683>

9.13 ISO 17799

9.14 Summary

Appendix A to Chapter Nine: Sources of Standards and Guidelines

GLOSSARY

BIBLIOGRAPHY