

# Contents

---

<i>Preface</i>	xv
<i>About the Web Site</i>	xxi
<b>CHAPTER 1</b> Business Continuity Management Plan	1
Crisis Management	4
The Value	5
Common Failings	7
Business Continuity Goals	9
Defining a Crisis	10
Mapping Risks	11
Critical Dependencies	12
Tactical Risk Evaluations	13
Determining Risk Tolerances	15
Incident Response versus Crisis Management	15
Stages of Incident Management and Crisis Response	17
Understanding Risk	17
Immediate Response and Impact Levels	21
Risk Management	22
Response Trigger Points	24
Decision and Authority Matrixes	27
Structuring Business Continuity Management Plans	29
Resourcing	33
Design and Development	36
Integrated and Compartmentalized Policies	39
Reporting and Record Keeping	39
Implementing the Business Continuity Management Plan	39
The Communications Plan	47
Organizational Interface Plans	53
Medical Response and Repatriation Plan	58
Public Relations Plan	59
Resource and Procurement Management Plans	62
Project Initiation Plans	67
Business Recovery Plans	68
Postincident Reviews	74
Summary	75

<b>CHAPTER 2</b>	Incident Management Plan	77
	Incident Management versus Crisis Response	78
	Principles of Incident Management	79
	Incident Management Plan Risk or Threat Overview	80
	Objectives of the Incident Management Plan	80
	Incident Management Sequence	81
	Crisis Management Flow	82
	Incident Management Sequencing	82
	Incident Management Stages	84
	Macro and Micro Crises	85
	Understanding the Incident Management Plan Needs	86
	Incident Management Plan Design and Implementation	90
	Design and Development	91
	Reviewing and Testing	92
	Adjustment and Implementation	92
	Incident Management Plan Policies and Procedures	93
	Information Security	94
	Resourcing the Incident Management Plan	94
	Structuring Incident Management Plans	95
	Incident Management Plan Policies and Instructions	96
	Incident Management Plan Cover Letter	97
	Immediate Resource Mapping	98
	Incident Management Plan Communications and Tactical Resource Plan	99
	Initial Verbal Reporting	101
	Incident Management Plan Decision and Authority Matrix	102
	Incident Management Plan Alert States and Trigger Response Plans	102
	Alert Notification Systems	106
	Incident Management Plan Information Capture Reports	107
	Incident Management Plan Crisis Response Guidelines	107
	Destruction Plans	108
	Incident Management Plan Risk Assessments	109
	Summary	109
<b>CHAPTER 3</b>	Crisis Management Structures	111
	Interorganizational Management	112
	Crisis Leadership	114
	Organizational Crisis Leadership	116
	Approach Methodologies	117
	Education and Training	118
	Supporting Crisis Management Groups	119
	Response Buildups	121
	Crisis Management Structures	122
	Corporate Crisis Response Team	123
	Country Crisis Response Team	124

Program Incident Response Team	125
Project Incident Response Team	126
Special Response Teams	126
Composition of Crisis Response Teams	127
Crisis Management Team Commander	128
Crisis Team Coordinator	129
Physical and Risk Security Manager	129
Technical Security Manager	130
Special Response Team Leader	130
Administration Manager	130
Intelligence or Information Officer	131
Liaison Officer	131
Communications Manager	132
Public Relations Officer	132
Legal Counsel	133
Human Resources Department	133
Health and Safety Department	134
Stress Trauma Adviser	134
Reception Team Manager	134
Finance Officer	135
Investor Relations Officer	135
Incident Management Structures	136
Crisis Control Center	137
Monitoring Crisis Management Programs	138
Summary	139
<b>CHAPTER 4</b> Scope of Risk	141
Security and Safety Awareness	144
Crisis Management Training	145
Stages of Disasters	145
Man-Made Risks	146
Espionage or Information Security Breach	147
Kidnappings and Ransoms	149
Hostage and Hijacking Situations	152
Domestic Terrorism (Monkey Wrenching)	153
Power Blackouts	157
Road Traffic Accidents	158
Complaints	159
Muggings or Robberies	160
Missing Persons	160
Civil Unrest	161
Arrest and Detention	162
Pending Arrest or Detention and Exit Denial	163
Loss of Sensitive or High-Value Equipment	164
Unexploded Ordnance and Mines	165
Indirect or Direct Fire Attacks	166
Suspect Calls	167
Workplace Violence	168

Threats, Coercion, and Extortion	171
Facility Intrusion	172
Chemical, Biological, or Radiological Threats	173
Small Arms Fire	175
Complex or Armed Attacks	175
Medical Emergencies	176
Repatriations of Remains	177
Explosive Attacks or Sabotage	179
Suspect Packages and Letters	180
Bomb Threats	181
Vehicle-Borne Improvised Explosive Devices	182
Sabotage	183
Family Liaison	183
Media Management	184
Computer-Related Incidents	185
Disciplinary Issues	186
Office, Facility, or Hotel Fires	187
Labor Disputes	189
Natural Risks	190
Floods	191
Earthquakes	192
Pandemics	193
Tsunamis (Tidal Waves)	193
Hurricanes and Tornadoes	194
Volcanoes	195
Sandstorms	196
Landslides	196
Forest Fires	197
Summary	199
<b>CHAPTER 5</b> Incident Response Guidelines	201
Vehicle-Borne IED Incident Management	204
Incident Management Guidelines	204
Casualty Incident Management	206
Incident Management Guidelines	206
Missing Person Incident Management	208
Incident Management Guidelines	208
Road Traffic Accident Incident Management Data Call	210
Incident Management Guidelines	210
Facility Physical Security Breach Incident Management	212
Incident Management Guidelines	212
Kidnapping and Ransom Incident Management	214
Incident Management Guidelines	214
Media Management Incident Management	216
Incident Management Guidelines	216
Detention and Arrest Incident Management	218
Incident Management Guidelines	218

Hostage Situation Incident Management	220
Incident Management Guidelines	220
Suspect Call Incident Management	222
Incident Management Guidelines	222
Civil Unrest Incident Management	223
Incident Management Guidelines	223
Unexploded Ordnance or Suspect Package Incident Management	225
Incident Management Guidelines	225
Suspect Letter Incident Management	228
Incident Management Guidelines	228
Destruction of Sensitive Materials Incident Management	230
Incident Management Guidelines	230
Repatriation Incident Management	232
Incident Management Guidelines	232
Domestic Terrorism or Special-Interest Groups Incident Management	236
Incident Management Guidelines	236
Espionage Incident Management	238
Incident Management Guidelines	238
Site Occupation or Sit-Ins Incident Management	239
Incident Management Guidelines	239
Sabotage Incident Management	241
Incident Management Guidelines	241
Demonstrations Incident Management	243
Incident Management Guidelines	243
Pending Detention or Exit Denial Incident Management	245
Incident Management Guidelines	245
Complaints Incident Management	247
Incident Management Guidelines	247
Blackouts and Power Loss Incident Management	249
Incident Management Guidelines	249
Loss of Sensitive or High-Value Materials Incident Management	250
Incident Management Guidelines	250
Indirect Fire and Direct Fire Attacks Incident Management	251
Incident Management Guidelines	251
Workplace Violence Incident Management	253
Incident Management Guidelines	253
Chemical, Biological, or Radiological Attack Incident Management	254
Incident Management Guidelines	254
Complex Attack Incident Management	256
Incident Management Guidelines	256
Family Liaison Incident Management	257
Incident Management Guidelines	257
Office, Facility, or Hotel Fires Incident Management	259
Incident Management Guidelines	259

Threats, Coercion, and Intimidation Incident Management	261
Incident Management Guidelines	261
Mugging or Robbery Incident Management	263
Incident Management Guidelines	263
Small Arms Fire Incident Management	265
Incident Management Guidelines	265
Floods and Tidal Waves Incident Management	267
Incident Management Guidelines	267
Earthquakes Incident Management	269
Incident Management Guidelines	269
Pandemics Incident Management	271
Incident Management Guidelines	271
Hurricanes and Tornadoes Incident Management	273
Incident Management Guidelines	273
Volcanoes Incident Management	275
Incident Management Guidelines	275
Sandstorms Incident Management	277
Incident Management Guidelines	277
Landslides Incident Management	279
Incident Management Guidelines	279
Forest Fires and Brush Fires Incident Management	281
Incident Management Guidelines	281
Summary	283
<b>CHAPTER 6</b>	
Crisis Information Capture Reports	285
Immediate Verbal Reporting (SAD CHALETS)	288
Serious Incident Reporting	288
Serious Incident Report Incident Management Data Call	290
Incident Management Plan Risk Assessment Reports	291
IMF Risk Assessment Report Incident Management	
Data Call	292
Sample Crisis Information Capture Reports	293
Vehicle-Borne IED Incident Management Data Call	294
Casualty or Injury Incident Management Data Call	295
Missing Persons Incident Management Data Call	297
Road Traffic Accident Incident Management Data Call	299
Facility Physical Security Breach Incident Management	
Data Call	303
Kidnapping and Ransom Incident Management Data Call	305
Media Management Incident Management Data Call	307
Detention or Arrest Incident Management Data Call	308
Hostage Situation Incident Management Data Call	310
Suspect Call Incident Management Data Call	312
Civil Unrest Incident Management Data Call	313
Unexploded Ordnance or Suspect Package Incident	
Management Data Call	314
Suspect Letter Incident Management Data Call	315

*Contents*

xiii

Destruction Plan Incident Management Data Call	316
Repatriation Incident Management Data Call	317
Information Security Breach Incident Management Data Call	318
Domestic Terrorism or Special-Interest Groups Incident Management Data Call	319
Complaints Incident Management Data Call	321
Mugging or Robbery Incident Management Data Call	322
Pending Detention and Exit Denial Incident Management Data Call	323
Loss of Sensitive or High-Value Materials Incident Management Data Call	325
Indirect or Direct Fire Attacks Incident Management Data Call	327
Workplace Violence Incident Management Data Call	328
Threats, Coercion, or Intimidation Incident Management Data Call	329
Chemical, Biological, or Radiological Threats Incident Management Data Call	330
Small Arms Fire Incident Management Data Call	332
Complex Attack Incident Management Data Call	333
Explosive Attack or Sabotage Incident Management Data Call	335
Family Liaison Incident Management Data Call	336
Computer-Related Incidents Incident Management Data Call	337
Disciplinary Issues Incident Management Data Call	338
Office, Facility, or Hotel Fires Incident Management Data Call	339
Espionage Incident Management Data Call	341
Site Occupation Incident Management Data Call	342
Demonstrations Incident Management Data Call	343
Blackouts and Power Loss Incident Management Data Call	345
Floods or Tidal Waves Incident Management Data Call	346
Earthquakes Incident Management Data Call	347
Pandemics Incident Management Data Call	348
Hurricanes and Tornadoes Incident Management Data Call	349
Volcanic Eruptions Incident Management Data Call	350
Sandstorms Incident Management Data Call	352
Landslides Incident Management Data Call	353
Forest Fires or Brush Fires Incident Management Data Call	354
Summary	356
<b><i>Acknowledgments</i></b>	357
<b><i>Index</i></b>	359

<http://www.pbookshop.com>