BUSINESS CRISIS AND CONTINUITY MANAGEMENT

Gregory L. Shaw, D.Sc., CBCP
Senior Research Scientist
The George Washington University
Institute for Crisis, Disaster, and Risk Management

This chapter is focused on the private sector organizations (businesses) that support the economy at the individual, family, community, local, state and national levels. However, even with this focus, the framework and principles of for profit business crisis and continuity management (BCCM) are applicable to all organizations, be they private, public or not-for-profit. Organizations exist to provide products and/or services to their customers and should strive to maintain and/restore this capability, even in the face of highly disruptive events. Regardless of the terminology chosen as the title for organizational continuity, crisis and continuity management or continuity of operations, continuity is a strategic responsibility and function for all organizations if they are to survive and prosper.

Central to the development and maintenance of a comprehensive organizational continuity program is an understanding of the myriad functions supporting continuity and their interdependencies. Recent efforts to develop a national standard as contained in the *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2004 Edition*, is a starting point, but falls short of the detail necessary to prescribe true standards.

As an alternate to the NFPA 1600 program description, a visual framework of BCCM, with definitions is presented and explained as the foundation of an enterprise wide program of BCCM. The framework was developed to be simple enough to be understandable at all levels of an organization, yet complete enough to support the case for functional integration and management to multiple stakeholders including boards of directors, executive level managers, stock owners, and customers. The framework supporting function of risk management and its sub-functions is explained to demonstrate the applicability and benefit of the business specific functions of business area analysis and business impact analysis to any organization.

Introduction

"Business" is not just the purview of the private sector. All organizations, be they private sector, public sector or not-for-profit provide products and/or services to their customers. Along with the delivery of products and/or services, all organizations also share the possibility of disruptive events that have impacts ranging from mere inconvenience and short-lived disruption of operations to the very failure of their ability to deliver their products and/or services which are the very nature of their business. Accordingly, organizational functions supporting business

disruption prevention, preparedness, response and recovery such as risk management, contingency planning, crisis management, emergency response, and business resumption and recovery are established and resourced based upon the organization's perception of its relevant environments and the risks within those environments.

Individually, these functions can contribute to the protection of an organization and its business line. However, efficiency and effectiveness demand their integration and coordination into a comprehensive program of business crisis and continuity management. A logical starting point for accomplishing this integration is a visual framework and explanation that identifies the business crisis and continuity management supporting functions and their relationship to one another. Such a framework and its explanation are presented in this chapter. The framework, as presented, may appear quite different from the widely recognized Federal Emergency Management Agency model for Comprehensive Emergency Management which includes the phases of mitigation, preparedness, response and recovery, but the underlying philosophy and approach of both are actually quite similar and complementary.

The Term Business Crisis and Continuity Management (BCCM)

Because of the many inconsistencies in terminology found in the contemporary literature of the business community the hybrid term business crisis and continuity management has been coined and introduced as a title for an organization wide strategic program and process. It is necessary to include a brief discussion of the creation and choice of this term since much of the current literature and business practices use the individual titles crisis management or business continuity management separately and often interchangeably as an umbrella term for the multiple functions and processes supporting the mitigation of and response to business disruption.

United States based organizations such as Disaster Research Institute International (DRII 2004), ASIS International (ASIS 2004), and the Association of Contingency Planners (ACP 2004) use the terms Business Continuity Management or Business Continuity Planning as their umbrella for multiple functions and processes including crisis management. The United Kingdom based Business Continuity Institute also employs the term Business Continuity Management as its overall program title. However, noted experts such as Ian Mitroff (Mitroff and Pauchant 1992, Mitroff 2001) and Stephen Fink (Fink 1986) emphasize crisis management as the unifying structure and term for strategic business protection, response and recovery and include business continuity as one of many supporting functions.

Despite the difference in terminology, there is little debate in the business continuity and crisis management literature that crisis management, business continuity management, and their supporting functions need to be thoroughly integrated in support of overall business management. *Business Continuity Management: Good Practices Guidelines* explains the inconsistency in terminology by stating "Crisis Management and BCM [Business Continuity Management] are not seen as mutually exclusive albeit that they can of necessity stand alone based on the type of event. It is fully recognized that they are two elements in an overall business continuity process and frequently one is not found without the other." (Smith 2002)

Thus, in an attempt to emphasize the inter relatedness and equal importance of crisis management and business continuity management, Business Crisis and Continuity Management has been chosen as the umbrella term and is defined as:

> *Business Crisis and Continuity Management – "The business management practices that provide the focus and guidance for the decisions and actions necessary for a business to prevent, prepare for, respond to, resume, recover, restore and transition from a disruptive (crisis) event in a manner consistent with its strategic objectives (Shaw and Harrald 2004)."*

The Evolution of BCCM

Business Crisis and Continuity Management, as a recognized business program, has evolved over the past twenty plus years from a technology centric disaster recovery function dealing almost exclusively with data protection and recovery to a much wider holistic and enterprise wide supporting focus (Wheatman, Scott and Witty 2001). Despite some strides to evolve BCCM into a profession including a widely accepted common body of knowledge and terminology, standards of performance, and certification process, progress has been slow and is hampered by the fact that BCCM, though generally recognized as a strategic function, remains a discretionary program for all but the most highly regulated business sectors such as the financial sector and healthcare sector. Even within these regulated sectors, standards of performance for all BCCM supporting functions may not be recognized and specified in sufficient detail to insure a truly comprehensive and integrated program.

As Ian Mitroff concludes from his extensive research in the area of business crisis management (his umbrella term for an integrated BCCM program), most businesses do not have an adequate crisis management program, supported by corporate culture, individual and organizational level expertise, infrastructure and plans and procedures to fully understand, prepare for, and manage the crises they may face (Mitroff 1992). Mitroff has since updated his conclusions in the 2001 book, Managing Crises Before they Happen where he states that "The vast majority of organizations and institutions have not been designed to anticipate crises or to manage them effectively once they have occurred. Neither the mechanics nor the basic skills are in place for effective CM. (Mitroff 2001)" Mitroff's conclusions are further supported by the results of the 2001 Business Continuity Readiness Survey, jointly conducted by Gartner, Inc. Executive Programs and the Society for Information Management that found "Less than 25

percent of Global 2000 enterprises have invested in comprehensive business continuity planning. (Gartner 2002)"

This trend in BCCM acceptance is changing, however. The reality of business is that increasing and dynamic natural, technological and human induced threats, business complexity, government regulation, corporate governance requirements, and media and public scrutiny demand a comprehensive and integrated approach to business crisis and continuity management. Classic natural, technological and human induced events such as Hurricane Andrew (1992), the Northridge Earthquake (1994), the Exxon Valdez oil spill (1989), the Bhopal chemical release (1984), the World Trade Center attack of 1993, and the Tylenol poisoning case (1982) have provided lessons learned that emphasize each of these factors and the need for coordination and cooperation within and between organizations, and between all levels of government, the private and not-for-profit sectors.

These lessons have not been lost by many businesses that have reached the conclusion that integrated BCCM should be viewed as an investment rather than an additional cost that detracts from profits and have implemented their vision of comprehensive programs. The United States Business Roundtable, an association of business chief executive officers of leading corporations with the stated objective of improving public policy, explicitly recognizes the role of the Board of Directors and Management in the area of corporate governance in general, including specific business crisis and continuity management responsibilities. The Roundtable's white paper *Principles of Corporate Governance* charges the Board of Directors to periodically review management's plans for business resiliency and designate management level responsibility for business resiliency. Within the scope of business resiliency various functions are specifically mentioned and include business risk assessment and management, business

continuity, physical and cyber security, and emergency communications (The Business Roundtable 2002). However, lacking recognized standards and incentives, many businesses still consider BCCM as a burdensome cost that receives minimal and even no support.

The tragic events of September 11th, 2001 and the implications for businesses directly and indirectly impacted by the events have further reinforced the need for enterprise wide coordination of the multiple functions supporting business crisis and continuity management. Studies following the attacks of September 11th, 2001, such as the 9/11 Commission study and report have engaged the United States government, at all levels, in the process of recognizing the responsibilities of the private sector and encouraging the private sector to take adequate steps to protect people, property and business operations. Further steps, including mandated standards, may well follow beyond the current level of encouragement and voluntary compliance.

With roughly 80% of America's critical infrastructure managed by the private sector (The Conference Board 2003), The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* recognizes that the "private sector generally remains the first line of defense for its own facilities," and encourages private sector owners and operators to "reassess and adjust their planning, assurance and investment programs to better accommodate the increased risk presented by deliberate acts of violence (The National Strategy 2003)." The most recent versions of the *National Response Plan* (January 2005) and the *National Incident Management System* (March 2004) include the private sector in all phases of crisis and emergency awareness, prevention, preparedness, response and recovery planning and operations. The *National Response Plan* explicitly charges the private sector to enhance overall readiness (NRP 2005).

Supporting this goal of improved private sector readiness and intra and inter sector coordination, the 9/11 Commission chartered the American National Standards Institute (ANSI) to develop a consensus on a national standard for preparedness for the private sector (9/11 Commission 2004). Based upon its collaboration with the National Fire Protection Association (NFPA) and the research of the 9/11 Commission, the "American National Standards Institute (ANSI) recommended to the 9-11 Commission that the National Fire Protection Association Standard, NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs*, be recognized as the national preparedness standard (ISHN 2004)." The 9-11 Commission report contains the following recommendation concerning private sector emergency preparedness and business continuity:

> "We endorse the American National Standards Institute's recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard, and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security (9/11 Commission 2004)."

Following from the 9/11 Commission Report, The Intelligence Reform and Terrorism Prevention Act of 2004, signed into law on December 18, 2004 specifically states in Section 7305 – Private Sector Preparedness, that:

"Preparedness in the private sector and public sector rescue, restart, and recovery of operations should include, as appropriate –

(A) a plan for evacuation;

(B) adequate communications capabilities; and

(C) a plan for continuity of operations. (IRTPA 2004)"

The Act goes on to state that the NFPA 1600 standard "establishes a common set of criteria and terminology," and charges the Department of Homeland Security to "work with the private, as well government entities. (IRTPA 2004)" The Sense of Congress included in the Act falls short of mandating national standards for the private sector, but does encourage the adoption of voluntary standards such as those included in NFPA 1600.

The implications of the Act and the evolution of national standards on the private sector will certainly evolve over a period of time; however, there is already high level conjecture and discussions that compliance with NFPA 1600 will be established as an acceptable "legal standard of care" owed by businesses to their employees and the general public and will serve as a "safe harbor" to minimize potential legal liability. Compliance with NFPA 1600 may also find its way into insurance considerations including insurability, premium pricing, and deductible levels. Additionally, proof of adequate "preparedness" is increasingly finding its way into contractual agreements between the public and private sectors and between private sector businesses. Such requirements gained prominence in the preparations for Y2K, but lacked any real standard to demonstrate compliance. NFPA 1600 standards, though voluntary, appear to be the foundation of widely accepted national standards. Legal protection, insurance savings and contract requirements are certainly incentives for "preparedness" for all businesses and may be

supplemented by additional measures such as tax savings and other forms of preferential treatment for business to business and business to government interactions.

NFPA 1600 Standard

The NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs* (2004 edition) has gained national level attention and prominence as a result of the 9/11 Commission study and report, however, its development pre dates the events of September 11th, 2001. The original NFPA 1600 standards, published in 1995, focused on *Recommended Practice for Disaster Management.* The 2000 Edition, updated in the 2004 Edition, expanded the focus to a "total program approach for disaster/emergency management and business continuity programs (NFPA 2004)." Lacking a visual framework of the functions comprising an integrated program of Disaster/Emergency Management and Business Continuity, NFPA 1600 specifies 15 program elements as displayed in Figure 1.

Figure 1
NFPA 1600 2004 Edition Disaster/Emergency Management and Business Continuity Programs Elements

1. General
2. Law and Authorities
3. Hazard Identification, Risk Assessment and Impact Analysis
4. Hazard Mitigation
5. Resource Management
6. Mutual Aid
7. Planning
8. Direction, Control and Coordination
9. Communications and Warning
10. Operations and Procedures
11. Logistics and Facilities
12. Training
13. Exercises, Evaluations, and Corrective Actions
14. Crisis Communication and Public Information
15. Finance and Administration

The intent of this chapter is not to be overly critical of NFPA 1600, but to recommend areas of improvement. NFPA 1600, the result of a consensus process representing multiple constituencies from all sectors, is a logical and necessary first step in the development of national standards written at a level of detail that can be used to define and measure compliance. As presented in the current edition (2004) of the document provides relatively broad descriptions of the program elements with minimal detail and is open to very liberal interpretation as to what actually comprises compliance at the program and program element level. A listing of the program elements is useful, but a graphical presentation of the elements, their hierarchy and interdependency could assist in the understanding and marketing of a comprehensive program that truly integrates the component parts. Additionally, NFPA 1600 defines a Business Continuity Program as:

> *"Business Continuity Program – An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through personnel training, plan testing, and maintenance (NFPA 1600)."*

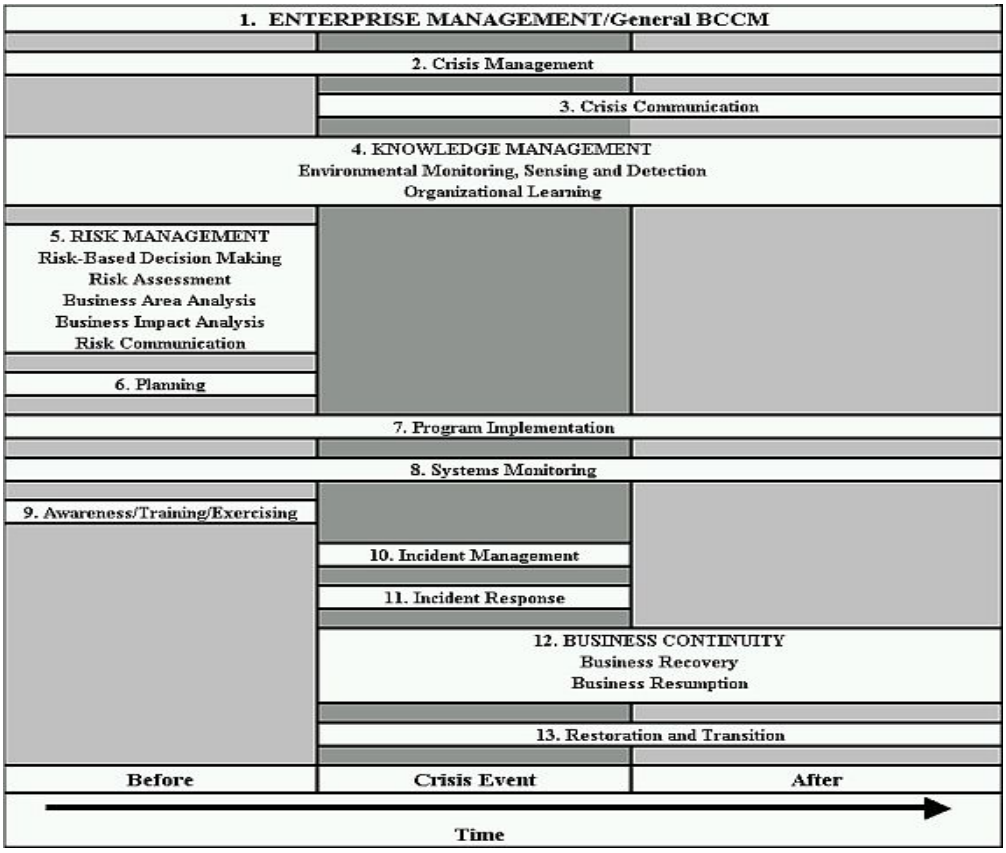
This choice of a definition stresses preparedness, response and recovery with no mention of prevention and the linkage of the program to overall organizational goals. The definition of an overall Business Crisis and Continuity Management program presented earlier in this chapter provides this necessary emphasis and relegates reactive Business Continuity to its appropriate supporting function role.

A Framework for Integrated BCCM

Consistent with the philosophy of an integrated BCCM program is the need for a visual framework identifying the component functions and their relationship to one another. A visual framework should be simple enough to be understandable at all levels of an organization, yet complete enough to support the case for functional integration and management to multiple

stakeholders including boards of directors, executive level managers, stock owners and customers. Such a framework, the synthesis of several existing frameworks as described in the paper *The Core Competencies Required of Executive Level Business Crisis and Continuity Managers* (Shaw and Harrald 2004), is presented as Figure 2. This framework displays a hierarchy of the functions (from top to bottom) and the temporal nature of each (from left to right).

Figure 2
Business Crisis and Continuity Management Framework



It must be emphasized that the BCCM framework, as presented, is in no way intended to prescribe a model organization chart for any business. It is merely the representation of multiple functions that require integration and coordination for the sake of program effectiveness and

efficiency. Definitions for each of the functions are provided as a common point of understanding since there is significant disparity in the various glossaries of Business Crisis Management and Business Continuity Management found in sources such as NFPA 1600, The Business Continuity Institute, Disaster Recovery Institute International, and the Business Contingency Planning Group.

Enterprise Management – *The systemic understanding and management of business operations within the context of the organization's culture, beliefs, mission, objectives, and organizational structure*.

Crisis Management – *The coordination of efforts to control a crisis event consistent with strategic goals of an organization. Although generally associated with response, recovery and resumption operations during and following a crisis event, crisis management responsibilities extend to pre-event mitigation, prevention and preparedness and post event restoration and transition.*

Crisis Communication – *All means of communication, both internal and external to an organization, designed and delivered to support the Crisis Management function.*

Knowledge Management – *The acquisition, assurance, representation, transformation, transfer and utilization of information supporting Enterprise Management.*

Risk Management – *The synthesis of the risk assessment, business area analysis, business impact analysis, risk communication and risk-based decision making functions to make strategic and tactical decisions on how business risks will be treated – whether ignored, reduced, transferred, or avoided.*

Planning – *Based upon the results of risk management and within the overall context of enterprise management, the development of plans, policies and procedures to address the physical and/or business consequences of residual risks which are above the level of acceptance to a business, its assets and its stakeholders. Plans may be stand alone or consolidated but must be integrated.*

Program Implementation – *The implementation and management of specific programs such as physical security, cyber security, environmental health, occupational health and safety, etc. that support the Business Crisis and Continuity Management (BCCM) program within the context of Enterprise Management.*

Systems Monitoring – *Measuring and evaluating program performance in the context of the enterprise as an overall system of interrelated parts.*

Awareness/Training/Exercising – *A tiered program to develop and maintain individual, team and organizational awareness and preparedness, ranging from individual and group familiarization and skill based training through full organizational exercises.*

Incident Management – *The management of operations, logistics, planning, finance and administration, safety and information flow associated with the operational response to the consequences/impacts (if any) of a crisis event.*

Incident Response – *The tactical reaction to the physical consequences/impacts (if any) of a crisis event to protect personnel and property, assess the situation, stabilize the situation and conduct response operations that support the economic viability of a business.*

Business Continuity – *The business specific plans and actions that enable an organization to respond to a crisis event in a manner such that business functions, sub-functions and processes are recovered and resumed according to a predetermined plan, prioritized by their criticality to the economic viability of the business.*

Restoration and Transition - *Plans and actions to restore and transition a business to "new normal" operations following a crisis event.*

Even though this framework of integrated BCCM and its accompanying definitions of supporting functions is similar to NFPA 1600 in falling short of the details for defining true standards, it is proposed as a more comprehensive basis for actual standards development. The actual examination of those details within the framework and all of the functions goes beyond the scope of this chapter. The next section will, however, briefly describe the function of Risk Management and its supporting sub-functions and its applicability to all organizations in all sectors.

Risk Management

Risk management is the foundation of a comprehensive BCCM program and drives the decisions impacting all of the other functions contained in the framework. Although portrayed as occurring in the time period before a specific crisis event, risk management is a continual and iterative process. It requires dialogue with multiple stakeholders, and monitoring and adjustment in light of changes to the environment and the economic, public relations, political and social

impacts of BCCM related decisions. All organizations in all sectors operate with constrained resources and have the responsibility to allocate available resources in a manner that best supports overall enterprise wide goals and objectives. The protection of personnel, property and reputation and the ability to recover, resume and restore business operations according to a reasoned and defendable plan are inherent in these goals and objectives and follow from a risk-based decision making .process. A private sector model of risk management, including the supporting steps of business area analysis and business impact analysis, can provide an analytic approach to risk-based decision making that is also applicable and potentially beneficial to public and not-for-profit organizations.

Business area analysis, in its basic form is an understanding of the products and services provided by a business and how they are produced and delivered. Depending on the complexity of the business and the product and service, business area analysis can be as simple as merely observing and documenting how the business operates. At the other extreme, it can involve the decomposition of business functions to the process and even task level to understand interdependencies and points of potential failure. Removed from the context of a Business Crisis and Continuity Management program, business area analysis is still a necessary component of business operations in all sectors and supports general business efficiency and effectiveness. Regardless of the complexity of the business area analysis process, what is important is that decision makers fully understand their business and what is necessary (critical) to deliver its products and services.

Business impact analysis matches the results of risk assessment (the identification of hazards and a determination of their probability of occurrence and the consequences of their occurrence) to the business area analysis to determine the impacts of the hazards on business

operations and to identify the potential interventions (controls) to protect business operations based upon their criticality. Taken together, the business area analysis and business impact analysis provide an analytic and economic basis for risk-based decision making and the allocation of resources supporting the overall risk management function. Beyond this analysis, other very legitimate considerations including political, social and environmental realities exist that impact the risk management process. They are, however, overlays to business area and business impact analysis and should not be the starting point for making risk management based decisions.

Risk management also includes the sub function of risk communication which is an essential component of risk management. Risk communication is a two way exchange of the risk related information, concerns, perceptions, and preferences within an organization and between an organization and its external environment that ties together overall enterprise management with the risk management function. The two seminal National Research Council documents, Improving Risk Communications (National Academy Press. Washington, DC. 1989) and Risk: Informing Decisions in a Democratic Society. (National Academy Press. Washington, DC. 1996) provide a comprehensive description of risk communication and perception, their application and lessons learned, and the derivation of principles and guidelines applicable to organizations from all sectors.

Conclusion

This chapter describes Business Crisis and Continuity Management as a strategic program with supporting functions and sub-functions that must be integrated for the sake of overall effectiveness and efficiency. A functional framework and definitions are presented to visualize the structure and inter dependencies of the components of such a program and are

proposed as a logical basis for developing national standards for organizations from the private, public and not-for-profit sectors. All organizations, from all sectors, are in fact businesses to the extent that they provide products and/or services to their customers. Protection of the ability to provide these products and/or services is a strategic imperative that must be understood and supported at all levels of any organization.

References

Association of Contingency Planners – International. Web Site. Oak Creek, WI. 2004. http://www.acp-international.com/.

ASIS Commission on Guidelines. *Chief Security Officer (CSO) Guideline.* Alexandria, Va. 2003. http://www.asisonline.org/guidelines/guidelineschief2003.pdf

ASIS Commission on Guidelines. *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery. Draft Guideline.* Alexandria, VA. July 12, 2004. http://www.asisonline.org/guidelines/guidelinesbusinesscon.pdf

Barton, Laurence. Crisis in Organizations: Managing and Communicating in the Heat of Chaos. South-Western Publishing Co. Cincinnati, OH. 1993.

Borge, Dan. The Book of Risk. John Wiley and Sons, Inc. New York, NY. 2001.

The Business Round Table. *Principles of Corporate Governance.* A White Paper from the Business Roundtable. 2002.

Continuity Central. *What's Under the Business Continuity Umbrella?* July 14, 2004. http://www.continuitycentral.com.

Cronin, Kevin P. *Legal Necessity*. *Disaster Recovery World II* [CD ROM]. Disaster Recovery Journal. St. Louis, MO. 1993.

Continuity Central. *Developing a Comprehensive Open-Source Business Continuity Model.* Continuity Central. London, UK. June 27, 2003. http://www.continuitycentral.com/feature017.htm Last accessed August 14, 2004.

Department of Homeland Security. *National Incident Management System (NIMS).* Washington, DC. March 1, 2004.

Department of Homeland Security. *National Response Plan (NRP) Final Draft.* Washington, DC. June 30, 2004.

Disaster Recovery Institute International. *Introduction and Professional Practices for Business Continuity Professionals.* DRI International. Falls Church, VA. 2004. http://www.drii.org.

Drabek, Thomas and Hoetmer, Gerard (Editors). Emergency Management Principles and Practice for Local Government. ICMA. Washington, DC. 1991.

Federal Emergency Management Agency. *Emergency Management Guide for Business and Industry*. Federal Emergency Management Agency. Washington, DC. 1996.

Fink, Steven. *Crisis* Management: Planning for the Inevitable. Authors Guild Backprint Edition. 1986, 2002.

Gartner 2002 press release. *Gartner Says That Less Than 25 percent of Global 2000 Enterprises Have Invested in Comprehensive Business Continuity Planning.* October 8, 2004. http://www3.gartner.com/5_about/press_releases/2002_10/pr20021008a.jsp

Harrald, John R. *A Strategic Framework for Corporate Crisis Management.* The International Emergency Management Conference 1998 (TIEMS '98) Proceedings. Washington, DC. 1998.

Hiles, Andrew. Business Continuity: Best Practices. Rothstein Associates Inc. Brookfield, CT. 2002.

Hiles, Andrew. Enterprise Risk Assessment and Business Impact Analysis: Best Practices. Rothstein Associates Inc. Brookfield, CT. 2002.

Industrial Safety and Hygiene News (ISHN) Online. *NFPA 1600 to Become the National Preparedness Standard?* April 30, 2004. http://www.ishn.com/CDA/ArticleInformation/news/news_item/0,2169,123889,00.html

Laye, John. Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes. John Wiley and Sons, Inc. Hoboken, NJ. 2002.

Lerbinger, Otto.The Crisis Manager – Facing Risk and Responsibility. Lawrence Erlbaum Associates. Mahwah, NJ. 1997.

Mitroff, Ian I., Pauchant, Thierry, C. Transforming the Crisis-Prone Organization. Jossey-Bass, Inc. San Francisco, CA. 1992.

Mitroff, Ian. I. Managing Crises Before They Happen: What Every Executive and Manager Needs to Know About Crisis Management. Amaco. New York, NY. 2001.

9/11 Commission Report. U. S. Government Printing Office. Washington, DC. 2004.

NFPA. *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs*. 2004 Edition. Quincy, MA. 2004.

National Research Council. Improving Risk Communications. National Academy Press. Washington, DC. 1989.

National Research Council. *Understanding* Risk: Informing Decisions in a Democratic Society. National Academy Press. Washington, DC. 1996.

Saraco, Don. White Paper - *BC Management: A Marriage of Craft and Technology.* MLC & Associates, Inc. Irvine, CA. Nov. 1999.

Shaw, Gregory. L. and Harrald, John. R. *Required Competencies for Executive Level Business Crisis and Continuity Managers*. Journal of Homeland Security and Emergency Management. Jan. 2004.

Smith, David, J. Editor. *Business Continuity Management: Good Practices Guidelines*. The Business Continuity Institute. London, England. 2002. http://www.thebci.org .

Standards of Australia Ltd. *A Handbook on Business Continuity Management: Preventing Chaos in a Crisis*. Consensus Books. Sydney, Australia. 2002.

Standards of Australia Ltd. *Draft Business Continuity Handbook.* Sydney, Australia. 2003.

United States Government. *Intelligence Reform and Terrorism Prevention Act of 2004*. Section 7305. Private Sector Preparedness. Washington, DC. 2005.

Wheatman, Vic, Scott, Donna, Witty, Roberta. *Aftermath: Business Continuity Planning.* Gartner Top View. AV-14-5138. September 21, 2001. http://www.gartner.com .

White House Administrative Office. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC. February 2003.