MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

Business Continuity Management

By

Eric Krell

Published by:

CMA CANADA

AICPA®

CIMA

NOTICE TO READERS

The material contained in the Management Accounting Guideline *Business Continuity Management* is designed to provide illustrative information with respect to the subject matter covered. It does not establish standards or preferred practices. This material has not been considered or acted upon by any senior technical committees or the board of directors of either the AICPA or the Society of Management Accountants of Canada and does not represent an official opinion or position of either the AICPA or the Society of Management Accountants of Canada.

MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

Business Continuity Management

By

Eric Krell

Published by The Society of Management Accountants of Canada
and The American Institute of Certified Public Accountants

1 2 3 4 5 6 7 8 9 0 PP 0 9 8 7 6

ISBN 0-87051-622-1

BUSINESS CONTINUITY MANAGEMENT

INTRODUCTION

Ten months elapsed between the conception of this *Management Accounting Guideline* (MAG) and its completion. During that time, the crucial importance of business continuity management (BCM) capabilities has been driven home, repeatedly and painfully, on a global scale

The terrorist attacks of Sept. 11, 2001, served as a gruesome wakeup call to North American corporate managers responsible for preparing their organizations to respond to disasters. The December 2004 Indian Ocean tsunami, the July 7, 2005, terrorist attacks on London's subway system and Hurricane Katrina's and Hurricane Rita's disastrous effects on large swaths of the U.S. Gulf Coast in August and September 2005 offer proof that both public and private BCM capabilities have a long way to go.

The frequency of man-made and natural disasters has increased in recent years. The nature of disasters has also changed: who could have imagined five years ago that civilian passenger airplanes would be used as a weapon of war? More important, the impacts of disasters on companies have greatly increased and intensified thanks to technological

CONTENTS

EXECUTIVE SUMMARY

In the 21st Century, organizations that fail to define and implement effective responses to disasters will be defined by their ineffective responses to disasters. Among leading companies, an IT-centric approach to disaster recovery is giving way to business continuity management (BCM). BCM capabilities enable organizations to restore their businesses to normal operations following business interruptions, which range from a simple power outage to a Category 4 hurricane. The finance and accounting managers — along with the senior-level executives, functional and operational managers and corporate directors — who read this guideline will learn how to define BCM and its essentials and processes; identify the BCM-related roles of corporate managers and directors; work through a BCM framework for developing and maintaining effective business continuity management processes; and see examples of leading BCM capabilities in practice.

advances, progressing globalization and the extension of the supply chain. Companies of all sizes are "connected" to their suppliers and customers to a much greater degree today than ever before. When a disaster occurs, its effects quickly ripple up and down the supply chain.

As a result, management teams and corporate boards face much more pressure to make their organizations more resilient when disasters, ranging from simple power outages to Category 4 hurricanes to synchronized suicide bombings, strike. To date, however, the corporate BCM capabilities necessary to establish that resiliency generally have ranged from absent to insufficient. This deficiency has a high cost: a University of Minnesota study finds that 93 percent of companies that lose critical systems for more than 10 days quickly file for bankruptcy; another study finds that 90 percent of organizations that experience a "catastrophic loss of data and equipment" without a business continuity plan in place go out of business within 24 months of the loss (Kahan, 2005).

The 9/11 Commission's exhaustive investigative research concludes that the Sept. 11, 2001, terrorist attacks revealed failures in imagination, policy, capabilities and management. The purpose of this guideline is to help organizations address and prevent those failures while providing finance and accounting managers with a foundation on which to further develop their BCM thinking, strategy and processes.

The purpose of this Management Accounting Guideline is not to fear monger (a tactic practiced by some BCM service providers that should be recognized and disregarded), but to help finance and accounting professionals enable their organizations to make the most effective and cost-efficient investment in the BCM capabilities that best meet the needs of the business.

The specific ***objectives*** of this guideline are as follows:

- To define business continuity management as a corporate capability and to identify its essential components and processes;
- To identify the drivers that make BCM a vital corporate and management competency in the 21st Century;
- To establish and define the roles and responsibilities that corporate managers and boards fulfill in developing effective BCM practices;
- To present a step-by-step framework for developing and maintaining effective business continuity management processes;
- To provide an overview of the software applications available to support BCM planning and execution processes;
- To present examples of sound business continuity management capabilities in practice.

While the ***target audience*** of the guideline is finance and accounting managers, all senior-level executives, functional and operational managers and corporate directors will benefit from its content.

DEFINITION AND SCOPE OF BUSINESS CONTINUITY MANAGEMENT (BCM)

Establishing and maintaining business continuity management processes begins with three steps:

1. Defining business continuity management;
2. Identifying and defining the key components of a viable BCM framework; and
3. Placing BCM in the context of organizational risk management

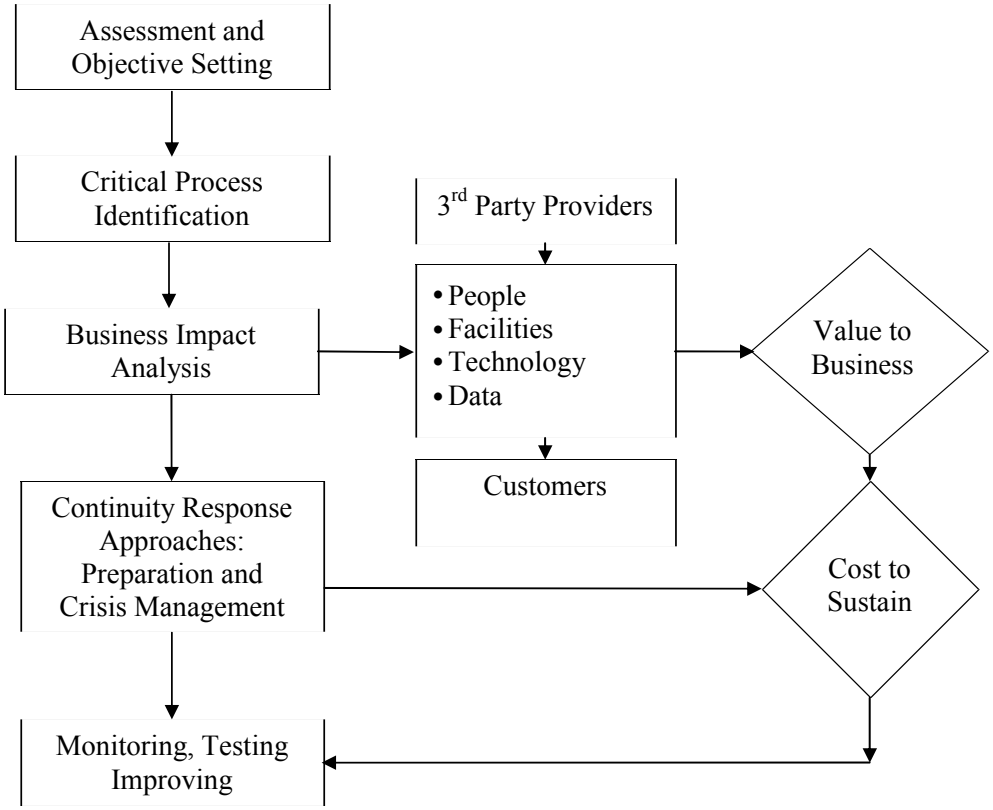
BCM Defined

This guideline agrees with the BCM definition put forth by the U.K.-based Business Continuity Institute (BCI): "Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organization, and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." This guideline defines stakeholders as employees, customers, suppliers, investors, and the community or communities in which an organization operates.

Business continuity planning is the process through which organizations establish the capabilities necessary to protect their assets and continue key business processes after a disaster — an unexpected business interruption caused by natural or man-made events — occurs.

The following framework (see Exhibit 1) illustrates the components of business continuity planning:

Exhibit 1: Business Continuity Planning



Although the discipline still has a long way to go, organizational business continuity management has evolved significantly over the past two decades. In the past, "disaster recovery" was usually centered in data processing or information technology (IT) departments. These early efforts primarily focused on getting hardware, software and data up and running again after a disruption. These days, it is generally recognized that business continuity planning efforts require a cross-company perspective and therefore should not be limited to the IT department. That said, many effective continuity tactics have emerged from disaster recovery efforts that arose in the IT function during the past decade. For example, many of the same principles that apply to data and systems backup also apply to facilities management and backup.

More recently, disaster recovery has expanded into "business continuity planning," a phrase that was primarily used to emphasize the need to move continuity efforts beyond the IT department and weave them throughout the organization. Most recently, the use of terms like "business continuity management" and "business resiliency" have increased, emphasizing the proactive nature of current continuity efforts. A business continuity plan, as the chart above illustrates, begins with executive-level assessments of an organization's continuity objectives. That assessment is followed by the identification of the organization's most important business processes. Then, finance managers and other business managers analyze the critical components of those processes: people, facilities, technology systems and the data the systems contain. The analysis should also consider how an unexpected business interruption might affect suppliers and customers.

The ensuing response processes ensure that all of the components that enable a critical business process are restored within a prudent amount of time. Defining what is prudent demands input from the finance and accounting function because it requires a comprehensive understanding of (*a*) each process' value to the business; and (*b*) the cost of restoring the process within a given amount of time.

The resulting plan should then be monitored, tested and, when necessary, adjusted or improved.

Key Terms

Business Continuity Management (BCM): Management's capability to identify potential impacts that threaten an organization and to provide a framework for building resilience and an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. Stakeholders include employees, customers, suppliers, investors, and the community or communities in which an organization operates.

Business Continuity Planning (BCP): The process through which an organization establishes and maintains business continuity management capabilities. This process includes assessments and objective setting, critical process identification, business impact analysis, and continuity response strategies, as well as monitoring, testing and improving these areas.

Disaster Recovery Planning: Often used as a synonym for BCP, but also a term associated more with IT-related responses to business interruptions.

Business Impact Analysis: The process of identifying how a specific business process, or set of business processes, would likely be affected by an unexpected interruption.

Crisis Management: A term that refers to the processes enacted after a business interruption has occurred to limit the negative effects of the interruption while returning the business to normal operating mode as effectively and efficiently as possible.

(*continued*)

BCM and Organizational Risk Management

Business continuity management is a subset of companywide or enterprise risk management (a topic addressed in the *Management Accounting Guideline* "Identifying, Measuring, and Managing Organizational Risks for Improved Performance.")

BCM's rising importance and IT-based history have caused internal debates about who owns the BCM function and how BCM relates to a company's existing risk management efforts. Again, business continuity management is a subset of a larger risk management strategy. The most significant difference between risk management and business continuity management relates to the output of each process. Risk management strategies (either risk avoidance, risk acceptance, or risk mitigation — through risk reduction, risk sharing or transfer of the risk) are "pre-event" responses to perceived risks. Most BCM strategies and tactics focus on the processes that need to take place after an event or disaster occurs; the objectives of those processes are to restore the business to normal operations as efficiently and effectively as possible.

The Business Continuity Institute's "Good Practice Guidelines (2005)" present a partial, but useful, comparison of the two disciplines; a portion of this comparison follows (see Exhibit 2).

DRIVERS OF BUSINESS CONTINUITY MANAGEMENT

The need for business continuity management capabilities continues to increase due to the following drivers:

1. A rise in the number of natural and man-made business interruptions;
2. The growing impact of business interruptions on organizations due to rising business interconnectivity;
3. The essential obligation to protect, preserve and build value;
4. New regulations and guidelines pertaining to BCM;
5. The business benefits of effective business continuity management; and
6. The generally insufficient quality of existing corporate BCM capabilities.

Driver 1: A Rise in Business Interruptions

The number of terrorist incidents worldwide has escalated since the Sept. 11, 2001 attacks ushered in a new age of man-made disasters. Bombings in Africa, the Middle East, East Asia, London and Madrid have killed thousands. There were 651 "significant terrorist attacks" worldwide in 2004, according to the U.S. State Department. That figure is three times the number of attacks that occurred in 2003 (Danner, 2005).

Driver 2: The Growing Impact of Business Interruptions

Most companies now operate in a more connected business climate. Numerous organizations of all sizes are virtually tethered to a growing number of customers, suppliers and distributors through an extended web of technology systems and processes. That connectivity exacerbates the negative impact of a prolonged business interruption. Not only did large automobile companies lose millions of dollars to production delays when the U.S.-Canadian border was closed and just-in-time inventories dried up in the wake of the Sept. 11, 2001 terrorist attacks, their suppliers and their suppliers' suppliers also suffered financial setbacks.

Even "normal" disasters, such as hurricanes, power outages, earthquakes and climate change, now inflict abnormal consequences due to the ever-increasing interconnectedness of the global economy. Those consequences are virtually

EXHIBIT 2: GOOD PRACTICE GUIDELINES

	RISK MANAGEMENT	BUSINESS CONTINUITY MANAGEMENT
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact and Probability	Impact and Time
Type of Incident	All types of events, usually segmented	Events causing significant business interruption

guaranteed to continue. "Earth, by its very nature, is a prolific architect of mayhem and purveyor of calamity," a recent *Popular Science* cover story reports. "The only thing we can do to protect ourselves is strive to learn where and when such massive natural disasters will happen — because, rest assured, they *will* happen (Behar, 2005)."

The Swiss Reinsurance Company publishes an annual report detailing the human and financial tolls of natural catastrophes and man-made disasters, and 2004 was a costly year on both counts, extending what the report describes as a "discernable upward trend." The catastrophes recorded by Swiss RE caused more than 300,000 deaths worldwide and directly attributable financial losses of more than $123 billion. Property insurers covered $49 billion of that amount.

Driver 3: The Essential Obligation to Protect, Preserve and Build Value

Put simply, ensuring business continuity is one of the top priorities of any company's senior executive team. Senior management is charged with the duty of building corporate value. To do so, that value must be protected and preserved during periods of uncertainty. Effective business continuity management capabilities allow a company to return to the status quo as quickly and as cost-effectively as possible.

Driver 4: New Rules and Regulations

The fact that insurance covered only 40 percent of catastrophe and disaster costs reflects another compelling driver of business continuity management, which is why the growing number of new industry guidelines, organizational rules and government regulations on business continuity management represents, in most cases, a positive development.

On April 7, 2004, the U.S. Securities and Exchange Commission (SEC) approved New York Stock Exchange (NYSE) Rule 446, "Business Continuity and Contingency Plans." The new rule illustrates the degree to which new laws, rules and guidelines are driving the need for stronger business continuity management capabilities at a growing number of North American companies.

NYSE Rule 446 requires NYSE members and member organizations to establish and maintain business continuity plans. Those plans must "be reasonably designed to enable [the member organization] to meet its existing obligations to customers, and address the existing relationships with other broker-dealers." The plans must be reviewed at least annually and "updated whenever there is a material change in a firm's operation, structure, business, or location that affects the information set forth in the BCP."

The adjective "material" calls to mind the Sarbanes-Oxley Act of 2002, the sweeping law that affects all companies that are publicly listed on exchanges in the United States. Although the Sarbanes-Oxley Act does not mandate public companies to establish and maintain business continuity plans, many of the law's principal objectives point to the need for effective business continuity management capabilities.

Indeed, some external auditors are reviewing their clients' business continuity processes in the post-Sarbanes era. These requests make sense, according to a leading risk management firm:

> "… for SOA compliance, it is prudent to consider business continuity issues as well. An important aspect of managing a company's overall risk, including its continuation as a going concern, is its ability to effectively address business continuity and disaster recovery, particularly with respect to those business processes that are critical to the successful achievement of the company's business objectives. A company's processes, systems, and controls must make available all material information needed for fair presentation and disclosure in its SEC reports, including the update of accounting estimates with current and reliable information. On a more strategic scale, an organization's business continuity methodology and approach must be agreed to by management as the foundation for mitigating financial and reputation risk posed by business interruption." (Benvenuto and Zawada, 2004).

In the United Kingdom, Publicly Available Specification (PAS) 56 provides a guide to "Business Continuity Management." The specification is sponsored by the Business Continuity Institute, which offers the discipline's most widely respected certification, the Fellow of Business Continuity Institute or FBCI. PAS 56 will form the basis of a "British Standard for Business Continuity Management." Some experts note that PAS 56 could eventually be adopted as an ISO standard.

There are many other regulations and industry guidelines related to BCM, as outlined in Appendix 1, "BCM-Related Regulations and Guidelines."

A recent survey conducted by Deloitte & Touche and CPM Global Assurance found that regulatory

Key Terms (*continued*)

Disaster: An unexpected business interruption caused by natural or man-made forces. The interruption poses a threat to some or all of the following: employees, the company's physical assets, the company's financial position, and/or the company's brand.

Maximum Tolerable Outage (MTO): The amount of time a business process or component of that business process (usually a production facility or an information system) can be offline before the cost of that outage becomes too high for the business.

Recovery Point Objective (RPO): The point in time at which a business process, or component of that business process, will be restored following an interruption; the RPO occurs before the MTO for a process or function occurs.

compliance was the second most commonly cited driver (behind "management recognition of the problem") of business continuity in corporations.

Driver 5: Business Benefits

Companies are not only implementing business continuity plans because they have to; some are doing so because there are business benefits. According to the BCI, these include, but are not limited to:

- BCM can be used by companies to differentiate their service-delivery or product-delivery resilience to potential customers;
- Thorough business impact analyses as well as ongoing business continuity monitoring can expose business inefficiencies;
- Retaining customers following a disaster is less expensive than acquiring new customers; and
- Successful crisis management experiences can build morale among the workforce and help prevent employee turnover following a disaster.

Driver 6: Existing BCM Capabilities Are Insufficient

The most important motivator of BCM improvement may be lack of continuity preparedness at most organizations. Given the importance of this driver, more space will be dedicated to this discussion.

One expert believes that some facets of corporate BCM capabilities — including the ability to anticipate "business surprises" — are a century behind the times. "[W]hen comparing the state of real-time monitoring of weather patterns with real-time monitoring in business," writes Gartner Inc.'s Kenneth McGee, "the business world has roughly the same capability as hurricane forecasters had in 1900," (McGee, 2004).

Other sources are only slightly less pessimistic about the general state of corporate BCM capabilities. Deloitte & Touche LLP's most recent annual survey of business continuity professionals found significant weaknesses in continuity training, plan-testing frequency and other BCM areas within U.S. companies.

Two-thirds of those survey respondents indicated they still do not have a process to ensure that an appropriate BCM program is maintained. Almost 60 percent of the respondents do not provide any training for their workforce to help employees understand their roles and the required procedures following a disruptive event. Only 28 percent indicated that they know their third-party dependencies and understand the recovery capabilities of their key business partners.

Researchers from META Group (which is now a part of Gartner Inc.) also analyzed Deloitte's annual BCP survey findings and had this to say: "The real challenge, as the report notes, is the sad fact that two-thirds of respondents don't have a true BCM function, putting any BC plans and planning in limbo. Equally troubling, as we have noted in our research and as this survey points out, is that the lack of ongoing BC management and governance (very critical since BC is not a project but an ongoing process) is compounded by the lack of executive involvement," (Deloitte & Touche, LLP and CPM Global Assurance, 2004).

Nearly half of the respondents to a Fall 2004 survey of 2,000 global executives by executive search firm Korn/Ferry International indicated that their companies do not have procedures in place to respond to an act of terrorism or a catastrophic event; moreover, 11 percent of the respondents said they did not even know if such procedures existed in their organization. Those figures are more alarming given the fact that 48 percent of the same respondents reported that terrorism continues to impact the economies in which their companies operate.

Part of the problem may be cost. Small to mid-sized companies typically spend $50,000 to $100,000 to have an external consulting firm help conceive and implement a continuity plan. Although most large companies have some form of business continuity plan in place, many of those plans are outdated or were ineffective to begin with. A Fortune 500 company would likely spend $750,000 to $2 million to implement suitable business continuity management capabilities.

That instinctive resistance coupled with those hefty price tags help explain why the disaster recovery and business continuity management discipline has burned brightly on strategic radar screens at certain times in the past decade and then faded quickly. BCM was foisted to the top of executive teams' priority lists leading up to Y2K and then again immediately following the 2001 terrorist attacks on the United States, but quickly gave way to issues perceived to be more pressing (e.g., a recession) once the events passed.

The magnitude of the risk attached to insufficient business continuity management capabilities will grow significantly in coming years — not because of a likely wave of terrorist attacks or a more cutthroat generation of computer hackers, but simply because disasters will inflict farther-reaching

damage as companies' reliance on technology and an increasingly global population of vendors and suppliers continues its onward march.

ROLES AND RESPONSIBILITIES

The question of which corporate function should take responsibility for BCM is frequently asked. It is a good question that will be addressed below. A more important issue, however, involves defining the BCM roles and responsibilities of all corporate functions and of senior leadership. A sound BCM strategy demands broad involvement of the board of directors, senior executive team, the corporate finance and accounting function, and other corporate functions and business units.

The board of directors should:

- Understand and actively communicate the value of BCM and the risks of insufficient BCM capabilities;
- Request to review the company's business continuity plan at least once a year;
- Request updates (at least annually) from senior executives on the emergence of new BCM-related rules and regulations;
- Approve of the strategic objectives of the organization's BCM strategy;
- Direct its audit committee to determine if external auditors require annual or quarterly reviews of BCM-related documentation and processes; and
- Offer advice with regard to how investors should be kept informed in the event of a disaster.

The senior executive team should:

- Have a sound working knowledge of BCM practices and the risks to the business of insufficient BCM capabilities;
- Keep the board informed (annually, at least) of the company's BCM strategy and any significant changes to business continuity plans;
- Take responsibility for setting their organization's business continuity management objectives;
- Review and approve (initially and then annually) the critical processes identified in BCM planning exercises;
- Review and approve (initially and then annually) the business impact analyses;
- Review and approve (initially and then annually) the continuity response strategies developed and maintained by corporate functions and business units;
- Support and communicate the importance of BCM test exercises;
- Integrate BCM responsibilities into performance management process for executives and managers with key BCM responsibilities.

Other corporate functions and business units should:

- Have a sound working knowledge of BCM practices and the risks to the business of insufficient BCM capabilities;
- Participate in critical process identification;
- Participate in business impact analyses of critical business processes within their areas of responsibility;
- Help establish continuity response strategies within their areas of responsibility;
- Integrate BCM responsibilities into performance management process for executives and managers with key BCM responsibilities.
- Work with corporate finance to better understand the costs and recovery tradeoffs of their response strategies;
- Support and communicate the importance of BCM test exercises;
- Monitor and test the response strategies within their areas of responsibility;
- Review and approve (annually) the continuity response strategies developed and maintained within their areas (based in part on the results and findings of test exercises).

The corporate finance and accounting function should:

- Guide the organization's critical process identification and (subsequent) business impact analysis efforts to help the rest of the organization understand how to assess the value of various business processes;
- Help the senior executive team, other functional executives and, in some cases, the board understand the tradeoffs between cost and recovery time objectives related to specific continuity response approaches;
- When possible, enhance business impact analyses with risk analyses to help prioritize the likelihood of various business processes suffering downtime during disasters;
- Provide additional analyses of how the timing of disasters can intensify or lessen their impact on certain processes (e.g., a hurricane that

Continuity Planning Obstacles

The appearance of Category 5 hurricanes and costly Internet viruses and worms often stimulate BCM questions: *Who's in charge of our continuity planning? Where is the actual plan?* Yet, BCM commitment is difficult to sustain over time due to several obstacles that prevent companies from installing, maintaining, monitoring and upgrading business continuity capabilities, including:

1. **'Vividness Bias:'** "Vividness Bias" (Bazerman and Watkins, 2004) prevents most individuals from thinking about troubling matters and major risks unless those issues play out, intensely and repeatedly, in front of their eyes.
2. **Competing Priorities:** Many areas of an organization can be resistant to the need for continuity planning when more immediate and visible demands — such as quarterly financial performance targets, production quotas and quality objectives — bear down on them.
3. **Lack of Standards:** BCM and disaster recovery are relatively new disciplines that have undergone dramatic evolutions in recent years, but established standards are only beginning to emerge, thanks to BCI and some industry organizations. For example, the Automotive Industry Action Group (AIAG) recently published a guideline titled "Crisis Management for the Automotive Supply Chain."

closes down an oil refinery that is being restarted following a maintenance shutdown, reducing output for longer than expected; or a lengthy power outage that delays financial reporting processes near the close of a publicly listed company's fourth quarter will likely have more serious consequences to the company's share prices (and value) than an outage that occurs several weeks away from a quarterly close); and

— Glean what BCM-related documentation and processes external auditors want to review.

Who Owns BCM?

What part of the organization should actually own responsibility for BCM processes? Answers vary, but there is growing sentiment that corporate finance is the place to house BCM. There is also a growing disinclination to house BCM in IT. Doing so is often viewed as a symbol of the discipline's past, in the days when disaster recovery was concerned with backing up data and hardware — and little else.

"More progressive organizations have realized continuity planning must be a business issue," says Protiviti's Brian Zawanda, a business continuity expert. "One option is championing business continuity through the chief financial officer's organization. The CFO has a good macro view of the organization and can translate downtime into tangible financial impacts. In many organizations, risk management resides within finance, and the risk manager is a strong possibility for business continuity coordination given this person is constantly thinking in terms of risk mitigation," (Stanek, 2003).

The location of the "BCM function" sends a clear message to the organization about the importance of BCM. "Poor positioning in an organization can have a dramatic influence on success," writes Andrew McCrackan. "It's all about communicating a sense of importance and reflecting the correct profile of the function in the organization. You will never convince anyone you are running a comprehensive business continuity program from within your property management department, for example," (McCrackan, 2005).

IT appears to be a less common owner of BCM today than in years past, according to the Deloitte/CPM Global Assurance Survey, which found that the BCM function most often resides in:

- Corporate management, including corporate finance (in 33 percent of respondents' organizations);
- IT (28 percent);
- Risk management (13 percent);
- Facilities management (8 percent);
- Information security (5 percent);
- Physical security (3 percent); or
- Another area (10 percent).

Twenty-five percent of the same Deloitte survey respondents, who were evenly distributed among small, mid-sized and large organizations, reported that their companies had no budget in place for business continuity management.

Additional Contributions from Finance

Strategic financial management professionals are well schooled in the following areas:

- Cost-benefit analyses;
- The alignment of investments with high-level business objectives; and
- Identifying how organizational change affects large investments.

Sound cost-benefit analyses should be one of the essential capabilities of a business continuity management function, a point that the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" by the U.S. Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the SEC emphasizes: "The agencies recognize the importance of cost-effective business continuity planning. The costs associated with implementing the sound practices can vary substantially depending on the extent to which incremental improvements may be needed to address the risks of a wide-scale disruption."

The cost of ensuring the resiliency of processes, technology and facilities can quickly spiral out of control if those investments are not made in a disciplined manner that aligns with business needs. For example, the cost of owning and maintaining redundant facilities in another geographical location can far outweigh the benefits that the backup facility provides in the event of a disaster. A lease on a shared facility backup space might make more financial sense.

Strategic financial management professionals understand how the business generates revenue, what makes cross-enterprise projects succeed (or fail), and what type of support and understanding — from the business units and from the executive team — needs to be present for BCM investments to meet their objectives.

Many finance departments have taken lead roles in establishing processes that ensure that their organization's regulatory compliance efforts are sustainable over time. The key processes in sustaining compliance with the Sarbanes-Oxley Act, for example, echo the processes necessary to sustain BCM over time:

- The creation of an internal controls culture;
- The establishment of business-unit ownership of internal controls; and
- The integration of internal controls considerations into IT system upgrades, mergers and acquisitions, corporate reorganizations and other major changes.

Replace the phrase "internal controls" with "business continuity," and the exact same approaches ring true for effective business continuity management.

The corporate finance and accounting function may or may not own the business continuity management function, but it certainly possesses the strategic vision, risk management expertise, financial management discipline, project-management skills and macro perspective necessary to make BCM frameworks effective and efficient.

DEVELOPING EFFECTIVE BCM CAPABILITIES

There is good news for corporate managers facing the challenge of developing business continuity management capabilities.

First, information about disaster recovery, business continuity planning and crisis management processes is readily available. The high cost of ineffective business continuity management has spurred academics, consultants and other experts in the field to share information much more freely than is usually the case in other disciplines. See the "Suggested Reading" section at the end of this guideline for suggestions on information resources.

Second, the fundamentals of a sound BCM strategy are relatively simple to grasp. Professional disaster recovery and business continuity managers and consultants frequently make the point that most elements of their work "are not rocket science." The toughest part of a business continuity manager's role is overcoming organizational resistance to fund and participate in business continuity planning activities.

John Laye, the former president of the California Emergency Services Association and a business continuity specialist, offers advice on how to overcome resistance to continuity planning. Without the proper planning and capabilities, Laye notes, "a major disruptive event is likely to take on a life of its own, driving your company into decisions that will negatively [affect] plans for a bright future. Worse, it can lead to that graveyard spiral aviators know about. Event becomes crisis; crisis becomes disaster; and on down. Over the longer term, resources for expansion are consumed, employees being groomed for promotion leave, and the confidence of investors, regulators, potential partners, and customers is shaken (Laye, 2002)."

Developing business continuity management capabilities requires a five-step process. While the business impact analysis (BIA) is the lynchpin step, the BIA cannot be effectively conducted without the first two steps. Each of the five steps contains sub-steps, as outlined below:

Step 1: Initial Assessment and Objective Setting

- Establish and communicate senior executive teams' support of BCM
- Outline and communicate ensuing steps:
  - Critical process identification,
  - Business impact analysis,
  - Response approaches, and
  - Monitoring, testing and improving the plans;
- Identify the team in charge of the project and which function and which executive the team reports to;
- Review the company's strategic plan;
- Review existing plans related to disaster recovery, continuity planning, emergency preparedness and crisis management;
- Identify existing external laws, regulations and requirements related to BCM; and
- Draft and approve a formal BCM policy that outlines the objective of the business continuity plans.

Step 2: Critical Process Identification

- After reviewing the company's strategic plan, identify the company's most critical business functions;
- Identify the business objectives executed by those functions and the processes through which the objectives are executed;

- Process owners should identify key measures, components and external requirements of the process, such as:
  - Performance metrics (how the success of the process is measured and/or quantified with specific measures),
  - Contracts with external parties,
  - Regulatory and/or legal requirements (such as SEC reporting requirements, supplier contracts, accounts payable terms, payment schedules with creditors)
- Pinpoint the key resources and tools that enable the process to be executed, such as:
  - People and skills,
  - Equipment (including IT infrastructure, telecommunications, manufacturing systems, transportation vehicles),
  - Facilities (warehouses, factories, office space),
  - Software, and
  - Information, which includes electronic data and hard-copy documents.

Step 3: Business Impact Analysis

- Identify the following impacts to specific business processes and corporate functions when a disaster occurs:
  - Human resources,
  - Financial positions,
  - Reputation,
  - Physical assets,
  - Supplier relationships,
  - Customer relationships, and
  - Investor relations;
- Identify, to the best extent possible, the maximum tolerable outage (MTO) of each process;
- Identify a recovery point objective (RPO) for each process based on the MTO
  - Consider how the timing of a disaster (in the year, within a fiscal quarter, etc.) might influence the MTO and RPO

Step 4: Continuity Response Approaches

Companies can proactively limit the impacts of a disaster. And managers can speed the company's return to normal operations with effective crisis management processes. Preparation and crisis management represent the two areas of continuity response approaches.

Preparation

The following preparations focus on human resources, facilities, IT systems and data, and the supply chain (suppliers and customers):

Human Resources

- Senior and business unit management establishes the strategic importance of BCM and continuity planning through communications, disaster-response test exercises and, where applicable, the inclusion of BCM responsibilities in job descriptions and performance management processes;
- A succession plan — at the senior-management level and in each department and function — is maintained and updated;
- Management considers adopting policies that prevent a set amount (e.g., more than two) executives, managers and/or other critical personnel from traveling together on the same car, plane or helicopter at the same time;
- Disaster-response communications protocols are established and communicated to employees;
- Alternative communications (e.g., Web sites and/or telephone numbers) are maintained and provided to employees so that they and their family members can access updates if a disaster prevents employees from working in their office or family members from reaching employees at their office;
- Crisis-management protocols and reporting relationships are clearly communicated and copies (electronic or hard) of those protocols and reporting relationships can be accessed by employees outside the office; and
- Contact lists are created and maintained for each employee (and suitable backups, where possible, if the disaster renders the employee unavailable) who is required to restore a critical business process following a disaster.

Facilities

- Using the business impact analysis, identify the costs and benefits of owning or leasing alternative facilities (production facilities, warehouses, office space for employees);
- Test company-owned backup facilities at least once a year to ensure that they function as intended;
- Work reviews of the following systems into BCM testing: water-detection systems that provide early warning of leaks; systems that

detect gases, smoke and other indicators of fire or potential fire; airborne-contamination-detection systems; fire-suppression systems; backup power capabilities; and physical building security;

– Assess how long and to what extent backup facilities can host and help sustain critical business processes; and
– Review agreements with providers of backup facilities at least once a year to ensure that capacity continues to meet the company's needs;

IT Systems and Data

– Work with IT managers to ensure that system and data backup processes exist;
– Evaluate and prioritize the recovery time needs of each critical IT system;
– Conduct a cost-benefit analysis to better identify the proper balance between recovery time objective and the cost of recovering data and restoring systems within those time frames;
– In conjunction with backup facility planning, evaluate the IT readiness of each backup facility option; and
– Ensure that telecommunications backup consideration is included in these discussions.

Suppliers and Customers

– Create and distribute contingency planning questionnaires to key suppliers to raise awareness and to gauge their BCM capabilities;
– Encourage key suppliers to relay questionnaires to their key customers;
– Identify alternate suppliers in the event a disaster prevents one or more suppliers from operating beyond a maximum tolerable outage;
– Consult with key customers and then create a contingency planning questionnaires that establishes each customer's state of awareness and BCM capabilities. Encourage both key customers to do the same with their key suppliers and customers.
– Assist key suppliers and key customers by sharing knowledge of organizing for the planning and development of BCM capabilities.
– Identify emergent alternate sources of supply.

Crisis Management

The second set of disaster-response processes involve crisis management steps: the protocol an organization follows in the immediate wake of a business interruption until damaged processes are restored to full operation.

At a high level, crisis-management plans address how the company will handle its people, critical business processes, relations and communication with key suppliers, relations and communications with top customers, facility needs, technology (data and systems) needs and other operating needs when an interruption strikes. Crisis management plans also lay out how organizations will communicate with stakeholders during the disaster.

A crisis management plan should:

– Identify which executive or executives are responsible for initiating the crisis management plan;
– Identify which managers are responsible for making specific HR, facilities, IT, and supply chain continuity decisions during a disaster;
– Include a protocol for communicating with employees' family members when a business interruption puts employee safety at risk;
– Include a protocol and decision trees that indicate which executives make those decisions and the time frames within which those decisions should be made;
– In the protocol identified immediately above, identify backups or alternative arrangements if any individual in the decision tree cannot be contacted or is unable to act;
– Provide a highly detailed account of how critical processes will be restored through:
  • Alternative work schedules,
  • Backup facilities or alternative power supplies at existing facilities,
  • Backup IT systems,
  • Backup telecommunications systems, and
  • Alternative arrangements with suppliers and customers;
– Provide a detailed plan for notifying and updating the following audiences about the disaster's impact on the business:
  • Employees (and family members),
  • Suppliers and customers,
  • Investors,
  • Regulators,
  • The community(ies) in which the company operates,
  • Local, state and federal emergency response officials

- Banks and creditors, and
- The media.

Step 5: Monitoring, Testing and Improving

– Evaluate how significant changes, such as reorganizations, mergers and acquisitions, and major system implementations, affect business continuity plans, and adjust plans as required;
– Adjust business impact analyses and business continuity plans to ensure that they take into account significant organizational changes;
– Test business continuity plans at least once a year (companies in sectors with BCM regulations appear to be moving toward quarterly testing schedules).
– When conducting tests, involve operational and functional employees and managers.
– When conducting tests, strive to make the exercises resemble a "real" response to the greatest extent possible (e.g., include local, state and federal emergency response agencies in the exercises whenever possible);
– Identify weaknesses and gaps uncovered during the test exercises, and adjust plans as required;
– Develop a timeline to eliminate weaknesses;
– Report on the outcome of the tests and ensuing remediation plans to keep senior executive teams and corporate boards informed.

ADDITIONAL INSIGHTS TO HELP READERS TAILOR BCM TO THEIR ORGANIZATIONS

The above framework offers high-level, general guidance. The more detailed insights that follow are intended to help readers tailor business continuity processes to meet the unique needs of their organizations.

Human Resources

Managing human resources represents the most crucial component of business continuity management. Humans are the most valuable and most unpredictable element of any business continuity plan.

Consider the example of one business continuity consultant who recently conducted a nearly flawless hurricane-response exercise with a Florida-based client. The crisis management team executed the plan perfectly during the simulated hurricane and responded smoothly to unexpected situations that the continuity plan previously did not address.

However, when a real hurricane struck the company weeks later, the result was disastrous. Rather than report to their posts and fulfill their responsibilities as they had been trained to do, many members of the crisis response team left the office to check on the safety of friends and family members, and to assess the damage the hurricane inflicted on their personal property.

A recent analysis by the National Institute of Standards and Technology (NIST) concluded that the evacuation of the World Trade Center towers following the Sept. 11, 2001, terrorist attacks went slower than current estimates of how quickly people travel down stairwells when evacuating a building. However, those estimates are based on time measurements during non-emergency exercises. Granted, there were terrible complicating factors that slowed the World Trade Center evacuations, but the point is a clear one: practice often differs from reality, particularly in crisis response situations.

The subject of succession planning in the context of disasters is an unpleasant one: If key managers or employees die in a disaster, who will step up and fulfill their responsibilities? But discomfort is not the only reason succession planning is a generally underserved area of continuity management. Succession planning tends to be a neglected component of strategic planning in general — even outside the context of BCM:

- A study by RHR International found that 75 percent of organizations are not confident that their current talent pool will meet their future executive-staffing needs;
- 50 percent of the same respondents anticipate losing half of their senior management team within the next five years; and
- A different survey from CCH Inc., asked: If your organization's top four executives died in a car accident on the way to the airport, would your organization have a succession plan? Only 10 percent of respondents answered affirmatively and reported that their companies maintain a formal succession plan.

The preceding question begs another: What were four executives doing in the same car at the same time? Some companies, such as Teachers Insurance and Annuity Association — College Retirement Equities Fund (TIAA-CREF), limit the number of key managers who may travel together.

The psychology of crisis management usually starts and ends with discussions of the qualities

that make an effective crisis manager or emergency response team leader. The consensus is that crisis managers should possess the same qualities as senior managers and, perhaps even more important, find their work personally satisfying.

Ian Mitroff, in his most recent book, greatly expands on that conclusion. His research on crises and how organizations respond to them reaches a central conclusion that the emotional preparation for dealing with crises is the single most difficult and important factor in determining the success of crisis management efforts. It also represents a difficult concept to deal with: How can an intangible like "emotional preparation" be nailed down and woven into a documented procedure? He offers a straightforward answer: Hire advisors or counsellors to prepare to work through the powerful emotions crises spark *before* a crisis occurs.

That suggestion may be a bit too far out of the box for organizations just venturing into BCM, but Mitroff's suggestions nonetheless address an often overlooked, difficult to manage and inevitable outcome of disasters and crises in the workplace. He also encourages managers to address and mitigate organizational denial that can impede the adoption of crisis management and continuity capabilities. His description of common types of organizational resistance (see Exhibit 3) should help planners identify and diffuse the denial.

Information Technology

Protecting an organization's critical IT systems and business data in the event of a disaster can lead to highly technical discussions and terms like "asynchronous replication." In practice, however, successful systems and data continuity is all about time and money: When do the systems and data need to be back up and running, and what will it cost to establish that capability?

The major technology issues in business continuity management include:

- Assessing the value of systems and data to the organization; and
- Selecting storage/backup solutions and processes that reflect that current value

IT has generally performed well over the years in protecting companies' IT assets, which have changed and evolved dramatically over the past 15 years, during business interruptions and disasters. As continuity continues its transition from the IT function to the business as a whole, finance and accounting professionals can smooth and strengthen that transition by injecting greater financial discipline into technology continuity planning.

In a technology continuity context, time is measured as a "return to operations" (RTO) metric. Traditional methods of data backup, in

EXHIBIT 3: COMMON TYPES OF ORGANIZATIONAL RESISTANCE

TYPE OF DEFENSE MECHANISM	EXAMPLE
Denial	Crises only happen to others. We are invulnerable.
Disavowal	Crises happen, but their impact on our organization is small.
Idealization	Crises do not happen to good organizations in out-of-the-way places.
Grandiosity	We are so big and powerful that we will be protected from crises and we can handle anything that is thrown our way.
Projection	If a crisis happens, then it must be because someone else is bad or out to get us.
Intellectualization	We don't have to worry about crises since the probabilities of their occurrence are too small. Before a crisis can be taken seriously, one would have to precisely measure the odds of its occurrence and its consequences.
Compartmentalization	Crises cannot affect our whole organization since the parts are independent of one another.

Source: (Mitroff, 2005)

which data is stored on a tape and moved to an offsite location, typically provided a minimum RTO of 48 hours. That can be a long, long time in today's just-in-time business environment. Other backup and recovery methods provide shorter RTO, but at a premium. So, one of the key considerations that should inform storage and backup decisions is the value, or estimated business impact, of the systems and data. See Appendix 2, "Highly Detailed Data Classification."

Data asset classification must be an ongoing process, preferably performed by the business unit managers who use the data most frequently and therefore have the most accurate understanding of its value to the business. A simplified data classification scheme contains four groupings (Toigo, 2003):

Similar prioritization categories apply to networks and applications:

- **Mission Critical:** Network or application outage or destruction that would cause an extreme disruption to the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted systems or data requires significant effort to restore, or the restoration process is disruptive to the business or other systems.
- **Important:** Network or application outage or destruction that would cause a moderate disruption to the business, cause minor legal or financial ramifications, or present problems with access to other systems. The targeted systems or data requires a moderate effort to restore, or the restoration process is disruptive to the system.
- **Minor:** Network or application outage or destruction that would cause a minor disruption to the business. The targeted systems or network can be easily restored (Cisco, 2003).

Trouble often crops up when organizations select systems and data backup solutions. The default response tends to be that all of the systems and data are important (why else would we use them in the first place?), which leads to unnecessarily expensive solutions in which all or most data are stored in highly accessible formats and locations that can be restored immediately.

In truth, all systems and all data are not created equal. And the value of data and systems changes, sometimes quickly, sometimes slowly. Lower-value data should be stored in less expensive formats and locations. High-value data should be stored in highly accessible formats and at locations that allow for immediate RTO — a combination of capabilities that adds significant but prudent expense to a technology continuity strategy.

Again, the assessment of systems and data value is most accurate when conducted — and regularly revisited — by a combination of IT, finance and accounting and business-unit managers who actually rely on the data in their day-to-day operations. Once that process is in place, it makes sense to evaluate storage solutions, which, like the

EXHIBIT 4: SIMPLIFIED DATA CLASSIFICATION SCHEME

CLASSIFICATION	DEFINITION
Critical	Data/documentation that must be retained for legal reasons, for use in key business processes, or for restoration [of] minimum acceptable work levels in the event of a disaster.
Vital	Data/documentation that must be retained for use in normal business processes and that represents a substantial investment of company resources that may be difficult or impossible to recoup, but may not be required in a disaster recovery situation. Information that requires special secrecy or discretion may also fall under this category.
Sensitive	Data/documentation that is needed in normal operations, but for which alternative supplies are available in the event of a loss. Data that can be reconstructed fairly readily but at some cost could also be classified as sensitive.
Non-critical	Data/documentation that can be reconstructed readily at minimal cost, or duplicates of critical, vital or sensitive data that have no prerequisite security requirements.

(Toigo, 2003)

rest of the IT world, have evolved significantly and quickly in recent years and continue to pose challenges for the IT function.

A 2005 survey by IT trade association CompTIA found that data protection and security is the biggest challenge identified by IT professionals who manage storage networks for their organizations. *The Wall Street Journal* confirmed as much when it ran a chart in May 2005 detailing eight costly breaches of IT security that had taken place at large companies and institutions in the previous three months. When Bank of America's computer backup tapes were lost, the Social Security numbers of up to 1.2 million customers were also swiped.

In May 2005, Time Warner made headlines when it acknowledged that 40 backup tapes containing the Social Security numbers of roughly 600,000 current and former employees disappeared while being transported to an offsite data-storage location by a records management company. Time Warner's response to the loss illustrates the value of data to organizations today as well as the steep cost of mismanaging data storage: When an internal investigation did not locate the missing tapes, Time Warner immediately contacted the U.S. Secret Service; it also offered to pay affected employees (which could translate to as many as 85,000 people) for one year of credit monitoring.

The key question facing continuity planners is not whether to invest in a storage solution, but rather which storage solution to select.

Supply Chain

New York-based TIAA-CREF is one of the largest private retirement systems in the world. It serves 3 million members in the academic community and roughly 15,000 institutional investors while managing some $300 billion in assets. Members and customers want TIAA-CREF to answer a simple but critical question in the event that a terrorist attack, massive blackout or less dramatic business interruption affects the firm: *Are my retirement investments safe?*

As a result, a process for communicating with customers is an important component of TIAA-CREF's business continuity management program. Question-and-answer sessions represent an increasingly common tool in business continuity management; planners distribute questionnaires among top suppliers and, sometimes, in the business-to-business space, to large customers. The purpose of these inquiries is to gain a more accurate sense of how relationships with vendors and customers can be affected by disasters, and how interruptions at large customer and vendor locations can affect their own organization's continuity.

One of the provisions of NYSE 446 requires each member company to disclose to customers how its business continuity management program addresses the possibility of a future significant business disruption, and how the company plans to respond to events of varying scope: "Such disclosure must, at a minimum, be made in writing to customers at account opening, be posted on the member's or member organization's Internet Website and be mailed to customers upon request."

The rule also calls for a fair amount of specificity in the disclosure, recommending that the company identify scenarios of varying severity (whether the event affects the firm only or involves an entire office building, business district or region); state whether the company plans to continue business during each scenario (and provide recovery-time estimates if that's the case); and highlight its planned responses.

The Department of Marketing and Supply Chain Management at Michigan State University has developed a highly practical "Supply Chain Business Continuity Planning Framework" that in many ways parallels the overall BCM framework identified in this *Guideline*. The system includes awareness, prevention (including risk identification, risk assessment, treatment and monitoring), remediation (planning how to minimize the event's impact and duration and identify the resources needed to do so) and knowledge management (i.e., how the organization learns from the experience and strengthens its processes accordingly).

Questionnaires are commonly used to drive awareness of the need for BCM among suppliers, and to equip in-house continuity planners with a more accurate assessment of supply-chain continuity risks. The objective should be a simple one — to learn more about the continuity and recovery capabilities of select vendors — that can be easily communicated to vendors.

These questionnaires range in length from one to six pages and typically are arranged into sections that address different facets of continuity: overall continuity strategy, crisis communications, backup facilities (including data storage) and testing. The forms differ according to level of detail. For example, on the topic of mainframe and

distributed systems recovery, one questionnaire may ask whether the vendor has a recovery process in place for those systems; another questionnaire might continue that line of questioning by asking the vendor to list the type of recovery solution it uses (third party vs. in-house); and yet another questionnaire may probe the vendor on the extent to which the processing capability in the back-up facility matches the processing capability of the primary facility during normal operating conditions.

The framework is discussed in a lengthy paper that is the result of Michigan State University research of companies with established and effective supply-chain continuity processes. The research project — one of five on business continuity management the AT&T Research Foundation funded in 2003 — also establishes the 14 principles of effective supply-chain planning. The 14 principles, and select "key issues," are as follows:

1. **Create internal awareness from the bottom up and from the top down.**
   - Disruptions can have serious financial and competitive impact
   - Operational personnel are closest to the supply base and have better appreciation of risk sources
   - Top management controls the resources needed and must endorse supply-chain continuity planning
2. **Drive awareness into the supply base through the supplier selection and supplier management processes.**
   - Establish key processes for communicating with the supply base
   - Motivate suppliers to recognize and manage risks
3. **Prioritize suppliers and commodities to focus attention.**
   - Resources are limited and must be properly allocated
   - Focus efforts on critical commodities and their suppliers
   - Focus on high-risk commodities and suppliers
4. **Consider the full spectrum of resources and flows managed within the supply chain.**
   - Multiple resources (materials, information and services) flow in the supply chain and are critical to smooth operation
   - Must consider exposure related to all of these flows
5. **Understand both probability and impact of supply-chain disruptions.**
   - Risk is a function of the dimensions of probability and impact
   - In practice, disastrous impact may overwhelm low probability
6. **Eliminate/reduce exposure where feasible; buffer or mitigate where elimination is not feasible.**
   - Eliminating or reducing exposure is the ideal solution, but not always feasible
   - If exposure cannot be reduced, buffering strategies can limit impact
7. **Develop and monitor *predictive* BCP-specific indicators.**
   - Indicators are needed that will help identify changing risk levels *in advance* of a disruption
8. **Use multiple information sources to monitor risk.**
9. **Revisit these issues on a regular basis.**
   - Supply chains are dynamic
   - Sources and levels of risk will vary over time due to changes in supply-chain structure, economic developments, environmental changes and political developments
10. **Plan for disruptions**
    - It is impossible to totally eliminate the risk of supply-chain disruptions
    - It is critical to have both a *plan* and *processes* in place to deal with disruptions when they occur
11. **Manage the impact of disruptions.**
    - Consider both the *cost* and the *duration* of the disruption
12. **Take a *continuous improvement* view of supply chain continuity planning.**
    - Exposure to supply-chain disruption cannot be fixed overnight
    - Protecting the supply chain requires ongoing attention and effort
13. **Conduct a post-event audit of supply-chain disruptions as standard operating procedure.**
    - Learn from mistakes
14. **Share knowledge of supply-chain continuity planning throughout the organization** (Zsidisin, Ragatz and Melnyk, 2003).

SOFTWARE APPLICATIONS CAN HELP SUPPORT BCM PROCESSES

As demonstrated above, business continuity management is nothing if not detail-oriented and document-intensive. Business continuity software applications can help manage the information more efficiently than filing cabinets.

First-generation BCM software applications offered document management functionality and the ability to develop continuity plans, although the plans were usually limited to a generic, single-scenario cause, such as a power failure. The applications were difficult to use, targeted to users in the IT function (documenting recovery plans for systems and applications only), and demonstrated little, if any, return on investment.

Recently, a new generation of BCM software hit the market. It is generally geared toward business users, and provides functionality that can automate all or some of up to five important BCM processes:

1. Business impact analysis;
2. Documentation of an organization's process and systems relationships (mapping, for example, which database hosts the customer records that call center employees access through the customer relationship management system);
3. Continuity and recovery planning;
4. Situation management (which allows for the tracking and managing of crisis management activities in real-time); and
5. Notification (which sets rules for the type and timing of communications with employees, suppliers, customers and other vital stakeholders during a crisis).

Some BCM software applications contain the full range of these capabilities. Stand-alone solutions also exist. A recent Gartner report projected that 75 percent of global 200 companies will have implemented emergency notification applications (either as a hosted application or in-house) by December 2007.

The report identifies seven advantages automated notifications hold over manual calling trees, including:

- Quicker notification times (minutes vs. hours);
- Ability to guarantee delivery of a consistent message;
- Ability to use multiple forms of communication (land line, cellular phone, pager, e-mail and instant messaging via a computer or handheld device, or fax); and the ability to confirm the message's receipt (Noakes-Fry and Witty, 2005).

Additional information about the selection and use of BCM software applications is included in Appendix 3, "BCM Software Usage Survey."

BCM IN ACTION: EXAMPLES OF "GOOD" PRACTICES

Implementing BCM software may one day materialize as a legitimate best practice — once best practices emerge. Even the highly respected Business Continuity Institute shies away from the phrase. Instead, it offers up "Good Practice Guidelines."

Leading business continuity management processes are more likely to exist in companies that operate in highly regulated industries and sectors. Today, financial services leads the way, followed (distantly, in most cases) by healthcare.

A published interview with NASDAQ executive vice president of operations and technology and CIO Steve Randich illustrates the challenge of identifying best practices in this emerging discipline. The equity exchange had just completed a disaster recovery test with 50 of its member companies. Despite the interviewer's attempts to elicit information from Randich, the most he offered was "this thing went very well." Asked if the exercise produced any insights, Randich answered, "Not really." (Mearian, 2004)

Who could blame him? If the tests had exposed shortcomings, NASDAQ would only rattle its customers' nerves by publicly acknowledging its continuity vulnerabilities. The same holds true for other companies, especially those wary of alarming investors and analysts. As a result, practitioners have to hire consultants and scour book appendices, academic white papers, Web sites (including http://www.continuitycentral.com, http://www.thebci.org/ and http://www.drj.com), and published transcripts of DR and BCM conferences to glean good practices.

During a 2004 roundtable discussion attended by the financial services industry's top continuity executives, the CEO of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) offered up this advice: "Whatever you do, make sure it has the support from the very top of your organization, or it just won't get implemented. Business continuity can no longer be a staff function buried low in the organization…it's a line of business now." (SunGard, 2004)

While that sentiment echoes the same point almost every BCM service provider hammers, it carries a bit more weight coming from a CEO.

More Good Practices

A 2003 Deloitte & Touche study examined the business continuity management progress leading financial services companies had achieved since Sept. 11, then distilled that field research into five activities that characterize effective practices:

1. Making the BCM effort a top management priority led by senior executives;
2. Making continuous availability, rather than disaster recovery, the ultimate objective of the program;
3. Focusing on the business impact of potentially disruptive events rather than basing plans on the frequency of past events;
4. Broadening the scope of events beyond technology system failures to include any failure that could affect the availability of employees, working facilities and important records; and
5. Extending BCM considerations to include potential interruptions to third-party providers of critical services, such as telecommunications, security exchanges, public transportation, and energy providers.

In 2002, AT&T invested some $250,000 to identify examples of best practices in business continuity management. The money funded extensive BCM research at five U.S. universities, including Michigan State University, which produced the supply-chain continuity research cited earlier in this *Guideline*. The research produced five white papers that examine business continuity practices from different angles and in different industries; together, that research pinpoints six practices that companies should follow if their executives seek to implement advanced BCM capabilities (AT&T uses the term "business continuity planning" (BCP)):

1. **They do more than concentrate on tangible assets such as systems, networks and physical assets.** Effective BCP isn't simply a matter of keeping critical data in more than one location or building redundant systems. It addresses equally important aspects of organizational discontinuity such as employee education, alternative work processes and communication with customers. Training is a critical element in any BCP plan.
2. **They learn from their mistakes.** The Michigan [State] researchers observed that when supply-chain disruptions occurred, for instance, the best firms learned from them. "A serious disruption requires a post-incident audit that identifies important lessons learned — things that went right and things that went wrong," says Dr. Zsidisin. But even within the company that was most advanced in the use of audits, the process was managed by the buying organization, not the supply-chain partner where the actual disruption occurred. Unless the suppliers take responsibility for the audit's execution, an audit has limited utility as a tool for self-improvement.
3. **They are open to using third-party providers.** Outsourcing BCP functions to third-party providers that store critical company data and make available alternative facilities to continue such operations in the event of a disruption can provide significant protection — particularly when IT processes are not a firm's core capability. Using managed service providers can also enable companies to keep pace with rapidly changing IT environments and continuity needs.
4. **BCP is integrated across firms.** The increase in complex interactions among applications across an organization and its partners means that disruptions at one point may propagate rapidly throughout an organization in ways that may not be easily and quickly understood. Rather than asking business units to handle BCP within their own silos, an integrated approach is needed. That doesn't just mean handing the job to the IT department — functions such as human resources and customer service need to be in the loop.
5. **Plans are tested and updated on a regular basis.** Companies with untested plans may face as much risk as those with no plans at all. Where testing was observed in the universities' research, it was often limited to the evaluation of system or data backup and restoration, and not the actual restoration of business functions. The research identified cost concerns as the major impediment to regular and comprehensive testing, but saving money in this way is a false economy — an outdated or ineffective BCP program has next to no value.
6. **Above all, BCP is perceived as more than a cost.** Despite their relatively advanced BCP programs, even executives in the financial services industry see BCP primarily as merely a cost of doing business — a kind of insurance. "BCP was not seen as value-added activity that might be used to garner competitive advantage in any of our case studies," says Amitava Dutta, professor of Management Information Services in the School of Management at George Mason University (AT&T, 2004).

Financial services companies tend to be clustered in large cities, like New York, where many of the top organizations in the industry experienced the Sept. 11, 2001 terrorist attacks firsthand. Yet, it was the blackout that struck much of North America in August 2003 that showed how well the harsh lessons of Sept. 11 along with business continuity fundamentals have worked their way into the procedural fabric of many financial services companies.

For example, TIAA-CREF treats its "resiliency program" as an ongoing process that is woven into most aspects of business planning. The firm:

- Opened operations centers in different regions of the United States that can assume greater workloads in the event of an unexpected interruption at another office location;
- Generally requires executive management and business unit leaders to work from alternative locations as frequently as once a week;
- Constantly tracks the whereabouts of top executives; and

- Mandated that no more than 75 percent of senior managers can be in one office location at the same time.

The Bank of New York elevated its business continuity group from a mid-level function within the technology group to a spot on its organizational chart beside the chief technology officer.

The bank's customer communications task force treated the North American blackout of 2003 as a learning laboratory, emerging with insights that continue to shape the continuity group's strategy:

1. The realization that telecommunications continuity is paramount in financial services;
2. A greater appreciation for the value of geographic diversity as a continuity tool; and
3. The understanding that responsibility for business continuity must extend beyond IT, throughout the business.

The "process not a project" mantra resonates throughout organizations with the most effective business continuity management processes in place.

Like many other enterprises, Charlotte, N.C.-based Duke Energy established an internal group to assess the global company's existing disaster recovery and business continuity capabilities in the wake of Sept. 11. The business continuity management program that the assessment launched is instructive.

The cross-functional group's six-month review identified 42 recommendations for improvement. Three months later, in June 2002, the company opened its business continuity and crisis management program office and expanded its previous emergency-response policy to include an expansive definition of business continuity and to incorporate crisis management as a corporate accountability. By the end of 2002, 35 of the 42 recommendations had been implemented, and business units are now held accountable for weaving continuity considerations into process implementation.

Duke's managing director of business continuity and crisis management and its manager of crisis communications report that their new office emphasized the "what" over the "how" to ensure that the business units had the flexibility to introduce business-continuity elements into their operations in a way that was most appropriate.

The program office then developed an enterprise-wide, three-tiered approach that involved participation from all levels of the organization to respond to emergency incidents. Later, the program office integrated the separate functions of business continuity, crisis management and corporate security into a new organization: "continuity, insurance and security services."

Today, Duke Energy's business continuity director reports that crisis management and business continuity have become embedded in the company's culture — another characteristic frequently identified in companies with strong business continuity management practices. (Bowman and Mobley, 2005).

CONCLUSION

Natural disasters and other unexpected business interruptions occur more often and inflict greater damage on companies than they have in the past.

Business continuity management enables organizations to reduce the negative impacts of disasters and to return to normal operations sooner. To date, the general state of BCM capabilities among North American companies has been insufficient.

The gap between the financial toll of worldwide catastrophes and the amount of that toll covered by insurance in 2004 was about $74 billion. The loss of life attributed to those catastrophes topped 300,000. Those figures seem like a compelling motivator for better business continuity management. But they are not the only drivers. New regulations with specific BCM mandates are also emerging.

The epidemic of business continuity plans suffering from dust-inhalation on the shelf is being cured by the growing number of regulations and industry guidelines — along with more requests from external auditors to review the plans.

The development of sufficient BCM capabilities requires:

- An understanding of the roles and responsibilities of corporate managers and boards in implementing effective BCM practices;
- Adherence to a framework for developing and maintaining effective business continuity management processes;
- An understanding of the ways in which finance and accounting managers can apply their unique skills and experience to the execution of BCM practices;
- An understanding of the tools that can help automate and support BCM processes; and

- Knowledge of emerging "good practices" among companies with more sophisticated BCM capabilities.

Much of that knowledge has arisen from insight into insufficient responses to disasters and business interruptions. Just as the 9/11 Commission "looked backward in order to look forward," so, too, should companies learn from lessons of the past to ensure that they will not suffer through the same mistakes — or absorb similar costs — when future disasters strike.

BIBLIOGRAPHY

AT&T. 2004. Achieving Resilience — Best Practices in Business Continuity. AT&T, April.

Barnes, James C. 2001. *A Guide to Business Continuity Planning.* Chichester: John Wiley & Sons Ltd.

Bazerman, Max H., and Watkins, Michael D. 2004. *Predictable Surprises: The Disasters You Should Have Seen Coming and How to Prevent Them*. Boston: Harvard Business School Press.

Behar, Michael. 2005. When Earth Attacks! *Popular Science*, May.

Benvenuto, Nicholas and Zawada, Brian. 2004. *The Relationship Between Business Continuity and Sarbanes-Oxley*. Protiviti.

Bowman, Tom and Mobley, Michael. 2005. Case Study: Duke Energy Recognizes the Value of Convergence, April. CPM Global Assurance.

Business Continuity Institute. 2005. Business Continuity Research, February.

"Business Continuity Software Survey Results," 2005. *Continuity Central*, March. Portal Publishing Ltd.

Childs, Donna R. and Dietrich, Stefan. 2002. *Contingency Planning and Disaster Recovery: A Small Business Guide*. Hoboken: John Wiley & Sons.

Cisco Systems. 2003. Disaster Recovery: Best Practices White Paper. 1992–2003 Cisco Systems Inc.

Croy, Michael. 2004. The Business Value of Data. *Disaster Recovery Journal*, Summer.

Danner, Mark. 2005. Taking Stock of the Forever War. *New York Times Magazine*, September.

Deloitte & Touche, LLP and CPM Global Assurance. 2004. Entering the Mainstream Business Continuity 2004.

Goff, John. 2005. Who'll Stop the Rain? *CFO*, April.

Goggins, Kelley. 1999. Contingency Planning 101. *Contingency Planning & Management Magazine*, March.

Honour, David. 2003. U.S. Regulators Hit the Right Note. *Continuity Central*, April. Portal Publishing Ltd.

Kahan, Stuart. 2005. Disaster Recovery is a Numbers Game. *WebCPA*, April.

Kean, Thomas H. (chair), and Hamilton, Lee H. (vice chair). 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company.

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

McCrackan, Andrew. 2004. *A Practical Guide to Business Continuity Assurance*. Boston: Artech House.

McCrackan, Andrew. 2005. Is Business Continuity a Subset of Risk Management? *Continuity Central*, February. Portal Publishing Ltd.

McGee, Kenneth G. 2004 *Heads Up: How to Anticipate Business Surprises and Seize Opportunities First*. Boston: Harvard Business School Press.

Mearian, Lucas. 2004. Nasdaq's Tests Showed No Weaknesses, CIO Says. *ComputerWorld*, May.

Mitroff, Ian I. 2005. *Why Some Companies Emerge Stronger and Better from a Crisis*. New York: Amacom.

Mitroff, Ian I., and Alpaslan, Murat C. 2003. "Preparing for Evil." *Harvard Business Review*, April.

Noakes-Fry, Kristen and Witty, Roberta J. 2005. Automated Emergency Notification Will Speed Disaster Recovery. February. Gartner Inc.

Ramsey, Scott. 2004. The Evolution of Business Continuity Management: The Process of Ensuring Continuous Operations of Mission Critical Business Functions. CTG, 2004.

Schmerken, Ivy. 2003. Wall Street Goes Dark: Blackout 2003. *Wall Street & Technology*, October.

Stanek, Steve. 2003. Who Owns Business Continuity Management? www.KnowledgeLeader.com. Protiviti, 2003.

SunGard. 2004. Industry Roundtable: Models of Resilience. *Dialogue*, First Quarter.

Swiss Reinsurance Company. 2005. Sigma: Natural Catastrophes and Man-Made Disasters in 2004.

Thomas, Glyn. 2005. The Changing Role of Business Continuity Software. *Continuity Central*, April. Portal Publishing Ltd.

Toigo, Jon William. 2003. *Disaster Recovery Planning: Preparing for the Unthinkable*; third edition. Upper Saddle River: Prentice Hall.

United States Government Accounting Office. 2004. Report to the Committee on Energy and Commerce, House of Representatives: Financial Market Preparedness. GAO-04-984.

Wallace, Michael and Webber, Lawrence. 2004. *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*. New York: Amacom.

Zsidisin, George A., Ragatz, Gary L., and Melnyk, Steven A. 2003. Effective Practices in Business Continuity Planning for Purchasing and Supply Management. Michigan State University, June 2003. www.bus.msu.edu/msc/research.html.

SUGGESTED READING

Publishers of books, magazines and Web sites are responding quickly to the growing demand for business continuity management information. Organizations devoted to BCM, such as The Business Continuity Institute, have generously shared useful information about the emerging discipline. John Wiley & Sons, Prentice Hall, Harvard Business School Press, Amacom and other leading business-trade book publishers are releasing new titles on BCM and its components each year. And publications, such as the Disaster Recovery Journal, have played strong roles in stimulating and furthering discussions and debates on how organizations can establish better business continuity management capabilities.

What follows is a supplement to this guide's bibliography. This section is intended to provide more details on specific resources that will sharpen readers' searches for additional information.

Online Recommendations

The Business Continuity Institute (BCI) www.thebci.org is one of the world's foremost authorities on BCM issues. The BCI's current (2005) version of its "good practice guidelines," is required reading for any manager involved with BCM. The guidelines are available for free via download at the site: **www.thebci.org/gpg.htm**.

The Disaster Recovery Journal Web site, www.drj.com, provides several free samples of continuity and recovery plans (most are from universities and non-profit organizations) along with an example of a questionnaire companies can provide to vendors to assist with the process of gauging the BCM capabilities of supply chains. The site also contains a page with a lengthy list of links to other BCM resources: **www.drj.com/freelinks/links.html**.

The information clearinghouse Continuity Central, www.continutycental.com, also provides a comprehensive collection of links to other BCM articles, sites and resources: **www.continuitycentral.com/basicbc.htm**.

DRI International, www.drii.org, offers education and certifications in business continuity management; its site also provides (for free) one of the best BCM glossaries available: **www.drj.com/glossary/drjglossary.html**.

A hard copy of the Disaster Resource Guide (currently, in its 10th edition) is available ($20) at **www.disaster-resource.com**. The guide contains dozens of articles on most facets of BCM as well as a lengthy products and services directory. The Web site contains links to free articles and other resources.

Philip Jan Rothstein is an influential voice in disaster recovery issues. His firm's Web site, **www.rothstein.com**, contains links to hundreds of books (for sale) and articles (free) related to BCM topics. Rothstein also provides brief reviews of books available through his firm.

Book Recommendations

If you buy one guidebook to assist with your organization's BCM efforts, Jon William Toigo's *Disaster Recovery Planning: Preparing for the Unthinkable* (Prentice Hall, 2003) is a sound investment. Toigo has written for numerous publications, including ComputerWorld and Scientific American. His past experience as an executive in financial services companies is clearly evident in his detailed advice on building management consensus for BCM. The rest of the book's nearly 500 pages delve into every facet of business continuity management. It concludes with a discussion of the testing and maintenance of plans.

If Toigo's book is the definitive BCM text book, James C. Barnes' *A Guide to Business Continuity Planning* (John Wiley & Sons, 2001) qualifies as the best set of Cliff Notes on BCM. The relatively slim book contains more than 150 pages of checklists and forms, with a few paragraphs of analyses thrown in for good measure.

The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets (Amacom, 2004) by Michael Wallace and Lawrence Webber is a good second or third choice for overarching BCM

guidance. The book comes with a CD-ROM that includes a PowerPoint presentation with an overview of the business continuity planning processes and more than 45 forms and checklists to assist with various components of BCM.

Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes (John Wiley & Sons, 2002) offers fewer checklists and a greater emphasis on BCM principles. The fourth chapter offers advice and observations specifically targeted to senior managers responsible for BCM.

This final set of book recommendations focuses on three titles that provide more targeted information about specific components of BCM. Each of the following books would be better suited to readers who are seeking to elevate the sophistication of existing BCM strategies and processes:

- Ian I. Mitroff, who has overseen two decades of research at the University of Southern California's Center for Crisis Management, would likely dispute a categorization of his book, *Why Some Companies Emerge Stronger and Better from a Crisis* (Amacom, 2005), as "more targeted." Mitroff views risk management, business continuity planning and "crisis communications" as ultimately incomplete approaches to guiding companies through disasters. He prefers the term "crisis management" as a more encompassing description. His approach to crisis management is grounded in technical risk-management approaches but also addresses the psychological and spiritual effects, in the context of employees and the collective organization, that abnormal disaster sparks.
- *Predictable Surprises: The Disasters You Should Have Seen Coming and How to Prevent Them* (Harvard Business School Press, 2004) examines how vividness bias — why humans often do not act on knowledge — hampers organizational BCM efforts. The book identifies how companies can identify emerging threats (future disasters) earlier in their development. The book also contains an excellent 10-point crisis-response plan in its second appendix.
- In a similar vein, *Heads Up: How to Anticipate Business Surprises and Seize Opportunities First* (Harvard Business School Press) makes the case that disasters and other "business surprises" can be anticipated and responded to in ways that reduce their negative impacts. The book, authored by a Gartner Group vice president, applies many of the concepts involved in business intelligence and business performance management to business continuity management.

A Book for Small Businesses

Contingency Planning and Disaster Recovery: A Small Business Guide (John Wiley & Sons, 2002) is aimed at owners and managers of small companies (generally, those with annual revenues below $10 million).

Small companies crafting contingency plans for their IT assets typically do not need to delve into such complex areas. Continuity and recovery solutions are simpler for small business owners, although not all vendors who target that market recognize the need for simplicity. "Do not be persuaded by the colourful marketing brochures and impressive brand names with tantalizing promises of corporate-calibre disaster protection," note co-authors Donna Childs and Stefan Dietrich. "You need to establish a good balance for your business between your particular needs and the scale and cost of your solution."

The co-authors advise small business managers to group their needs into "basic" and "robust" categories. The former is designed to address the most frequent business interruptions: human error, equipment failure and third-party failures. Robust contingency covers those three business interruptions and provides more protection against weather-related disasters, terrorism and sabotage. A rough equipment cost estimate for each brand of small-business contingency approach is also provided. Basic contingency capabilities roughly translate to $5,000 in initial equipment costs plus about $1,000 annually in replacements and upgrades. Robust contingency capabilities cost about $10,000 in initial equipment costs and roughly $5,000 annually in replacements and upgrades.

APPENDIX 1: BCM-RELATED REGULATIONS AND GUIDELINES

Although there has been no "Sarbanes-Oxley equivalent" for business continuity management, the number of new continuity rules, regulations and guidelines that have accumulated in different industries, countries and government organizations in recent years, and particularly since Sept. 11, 2001, is large and constantly growing, as the following (partial) list illustrates:

- The Foreign Corrupt Services Act in 1977 required U.S. publicly held companies to provide "reasonable protection for information services," and holds corporate management accountable for doing so.

- The Internal Revenue Service (IRS) 86-19 contains legal requirements for the backup and recovery of computer records containing tax information.
- The Computer Securities Act of 1987 required U.S. federal agencies that rely on electronic support, and the private-sector companies with which the agencies conduct business, to establish and maintain recovery plans.
- Presidential Decision Directive 63 (PDD 63) was signed by President Clinton in 1998, and contains language and guidance that now sounds eerily prescient, as the inter-agency and public-private cooperation the directive calls for resembles what is now the U.S. Department of Homeland Security. "Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States," the directive reads. "Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy." PDD 63 called on companies in certain industries (information and communications, banking and finance, energy, transportation and vital human services) to establish, monitor and upgrade disaster recovery and business continuity plans.
- The Comptroller of the Currency and the Office of Thrift Supervision have issued several regulations for the financial services industry, including BC-177, a 1980s-era requirement that banks develop and maintain business recovery plans.
- The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" was finalized by the U.S. Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the SEC in April 2003 after a contentious drafting process, which at one point contained language dismissed as "draconian" by critics. The final paper, which addresses companies that are involved with clearance and settlement activities for the wholesale financial system, contains several "sound practices" intended to ensure that the targeted financial institutions implement and maintain sufficiently robust BCM capabilities that "provide useful guidance to business continuity planners in all types of companies, not just those in the financial sector" (Honour, 2003). These include: (1) Determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets; (2) Maintain sufficient geographically dispersed resources to meet recovery and resumption objectives; (3) Routinely use or test recovery and resumption arrangements.
- The "Contingency Planning Guide for Information Technology Systems" contains "recommendations" from the National Institute of Standards and Technology (NIST), which provides instructions and considerations for government IT contingency planning in the United States. The document outlines a seven-step contingency planning process, which, while geared toward IT continuity, echoes most of the same processes put forth as leading practices by business continuity management experts: (1) develop the contingency planning policy statement; (2) conduct the business impact analysis; (3) identify preventative controls; (4) develop recovery strategies; (5) develop an IT contingency plan; (6) plan testing, training and exercises; and (7) maintain the plan, which "should be a living document that is updated regularly to remain current with system enhancements."
- NFPA 1600, a standard of the National Fire Protection Association (www.nfpa.org), has been made an American National Standard, which is a national subset of the International Organization for Standardization (ISO). Although critics have questioned the standard's teeth, its most recent iteration contains a robust BCM component, which includes 10 key competencies mentioned by several other guidelines.
- The American Society for Industrial Security (ASIS) has developed a comprehensive business continuity guideline, "A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery," which is accompanied by step-by-step implementation instructions in a 48-page document available on the Web site of the international organization for security professionals: www.asisonline.org/guidelines/guidelinesbc.pdf.
- Section 1910.38 of Part 29, Code of Federal Regulations, Occupational Safety and Health

Administration (OSHA) requires companies to establish emergency action plans that address employee safety. The plans should address emergencies "that employers may reasonably expect in the workplace," such as fire, toxic chemical releases, hurricanes, tornadoes, blizzards, floods and others.

- The Detroit-based Automotive Industry Action Group (AIAG) recently released a guideline, "Crisis Management for the Automotive Supply Chain," which its executive director said was necessary because "as recent crises suggest, the supply chain is vulnerable. A domino effect in the supply chain may be created when disruptions occur at any single point."

This list of regulatory and guideline drivers is not complete; rather it is intended to illustrate the wide range of organizations, government agencies, industries and business processes (i.e., supply-chain management) in which business continuity management's profile is rising.

APPENDIX 2: IT: HIGHLY DETAILED DATA CLASSIFICATION

Some IT disaster recovery experts present highly detailed data-classification frameworks. These frameworks can help organizations make more cost-effective decisions about how and where they back up and store their business data:

CLASSIFICATION	DEFINITION
Mission Critical	Frequently used, immediate availability, significant and immediate financial impact
Business Critical	Regularly used, reasonably available, significant long-term financial impact, significant operational impact over time, eventual compliance impact
Essential	Periodically used, available within defined time frame, potential long-term financial impact, probable operational impact over time, probable compliance issues
Consequential	Occasionally used, available within extended time frame, possible but not likely financial impact, possible operational impact over time, probable compliance issues
Non-Critical	Rarely used, limited availability, unlikely financial impact, doubtful operational impact over time, potential compliance impact
Inconsequential	Used only on request, limited availability, no financial impact, doubtful operational impact over time, potential compliance impact
Disposable	Never used, no need for availability, no financial impact, no operational impact, no expected compliance impact

Source: Croy, 2004

APPENDIX 3: BCM SOFTWARE USAGE SURVEY

A recent survey of global business continuity professionals conducted by Web site Continuity Central found that nearly 60 percent of respondents use BCM software. The most frequently cited reasons for using BCM software are, in order of priority:

1. To manage and update business continuity plans;
2. To manage and coordinate crisis management response;
3. To train personnel; and
4. To evaluate the adequacy of existing capabilities.

The most frequently cited continuity management processes respondents use BCM software to automate were the following:

- Call lists (75 percent)
- Business impact analysis (59 percent)
- Testing and exercising (55 percent)
- Crisis team development (47 percent)
- Crisis management (42 percent)
- Risk assessment (42 percent)
- Project management (40 percent)
- Online access (40 percent)

- Dependency modeling (37 percent)
- Linking to standard databases (32 percent)
- Training (29 percent)
- Gap analysis (27 percent)
- Automated crisis communications (16 percent)
- Strategy selection (9 percent)

The most important criteria and components that will guide future BCM software purchases are, in order of priority:

- The ability to import and link existing information (people, resources, etc.) into the software application;
- The ability to customize the tool to reflect the purchaser's organizational structure and standards;
- ease of use (including an in-application coaching module);
- The ability to create plans in universal document formats, such as PDF; management reporting capabilities;
- a database controlled by plan owners;
- the ability to produce a full audit trail for reporting purposes;
- The ability to link to external databases;
- Robust security;
- Web-based capabilities; and
- The ability to dynamically build process and systems relationships and interdependencies.

APPENDIX 4: RESPONDING TO A BLACKOUT

The response of financial services companies to the North American blackout of 2003 is detailed vividly in a "Wall Street Technology" article (Schmerken, 2003). The story reflects several realities: smaller firms face larger cost and resources obstacles when establishing basic business continuity management capabilities; no amount of planning can ever cover all of the challenges live events deliver; and business continuity management programs require constant updating and adjustments. These lessons are evident in the real-life BCM case studies that Schmerken's reporting uncovers:

- The American Stock Exchange's offsite backup generators were delivered hours after the blackout struck Thursday at 4:10 p.m., and the exchange's trading systems were back online by the open of business Friday morning; however, the operation of the exchange's trading floor air-conditioning and heating system requires steam, which was unavailable until the New York City Office of Emergency Management located a portable boiler shortly before close of business Friday.
- The NYSE's business continuity plan worked well — almost too well. The exchange converted to a generator hours after the blackout struck and opened for business as usual the next day; however, security protocol sealed off entrance to the exchange's building. When one trader stepped outside to inform his ride home that he would be staying late to fulfill his BCM-related responsibilities, he was almost denied re-entry into the building.
- One of Lehman Brothers' post-Sept. 11 continuity initiatives, calling trees, were used to inform employees who worked in the one office tower that did not successfully transfer to backup power (the firm's main trading floors and data centers in Lower Manhattan and New Jersey were up and running within hours) via diesel generators that they should work from home on Friday. On the other hand, office space that Lehman Brothers does not own in another part of the city did not maintain backup generators and was closed the following day.
- NASDAQ's primary data center in Connecticut only experienced a brief power disruption before its diesel generator fired up. The electronic exchange also contacted most of the 300 firms it provides services to, the "vast majority" of which were able to connect with NASDAQ thanks to a fully redundant telecommunications network (Schmerken, 2003).

This *Management Accounting Guideline* was prepared with the advice and counsel of:

Barry Baptie, MBA, CMA, FCMA
Board Director and Business Consultant

Kenneth Biggs, MBA, CMA, FCMA
Board Director and Business Consultant

Dennis C. Daly, CMA
Professor of Accounting
Metropolitan State University

Alphonse M. Galluccio, CMA, FCMA, CFE
Vice President Internal Audit
The Jean Coutu Group (PJC) Ltd.

William Langdon, CMA, FCMA
Vice President, Knowledge Management
CMA Canada

Melanie Woodard McGee, MS, CPA, CFE
Manager of Accounting Joint Venture Controller
American Airlines/Texas Aero Engine Services, LLC

John F. Morrow, CPA
Vice President, The New Finance
American Institute of Certified Public Accountants

Robert C. Sweeting, BSc, PhD, FCA
Professor
Manchester Metropolitan University Business School

David L. Tousley
Chief Financial Officer
PediaMed — The Pediatrics Company

Kenneth W. Witt, CPA
Technical Manager, The New Finance
American Institute of Certified Public Accountants

Eric Krell, author

Mr. Krell, who is based in Austin Texas, is the author of hundreds of articles and columns on corporate finance, corporate governance, human capital management, risk management and other topics for magazines and media outlets. He writes for *Business Finance*, where he is also a columnist; *Consulting Magazine*; *HR Magazine*; *1 to 1 Magazine* and several business school reviews. His writing has also appeared in consumer outlets, including National Public Radio affiliate KUNC in Colorado and *Rolling Stone*. Krell holds a B.A. from the College of William and Mary. Eric@erickrell.com

For additional copies or for more information on other products available contact:

In the U.S.A.: **American Institute of Certified Public Accountants**
1211 Avenue of the Americas
New York, NY 10036-8775 USA
Tel (888) 777-7077, FAX (800) 362-5066
www.aicpa.org
Visit the AICPA store at www.cpa2biz.com

In Canada and elsewhere: **The Society of Management Accountants of Canada**
Mississauga Executive Centre
One Robert Speck Parkway, Suite 1400
Mississauga, ON L4Z 3M3 Canada
Tel (905) 949-4200
FAX (905) 949-0888
www.cma-canada.org

AICPA Member and
Public Information:
www.aicpa.org

AICPA Online Store:
www.cpa2biz.com

ISO Certified

030002