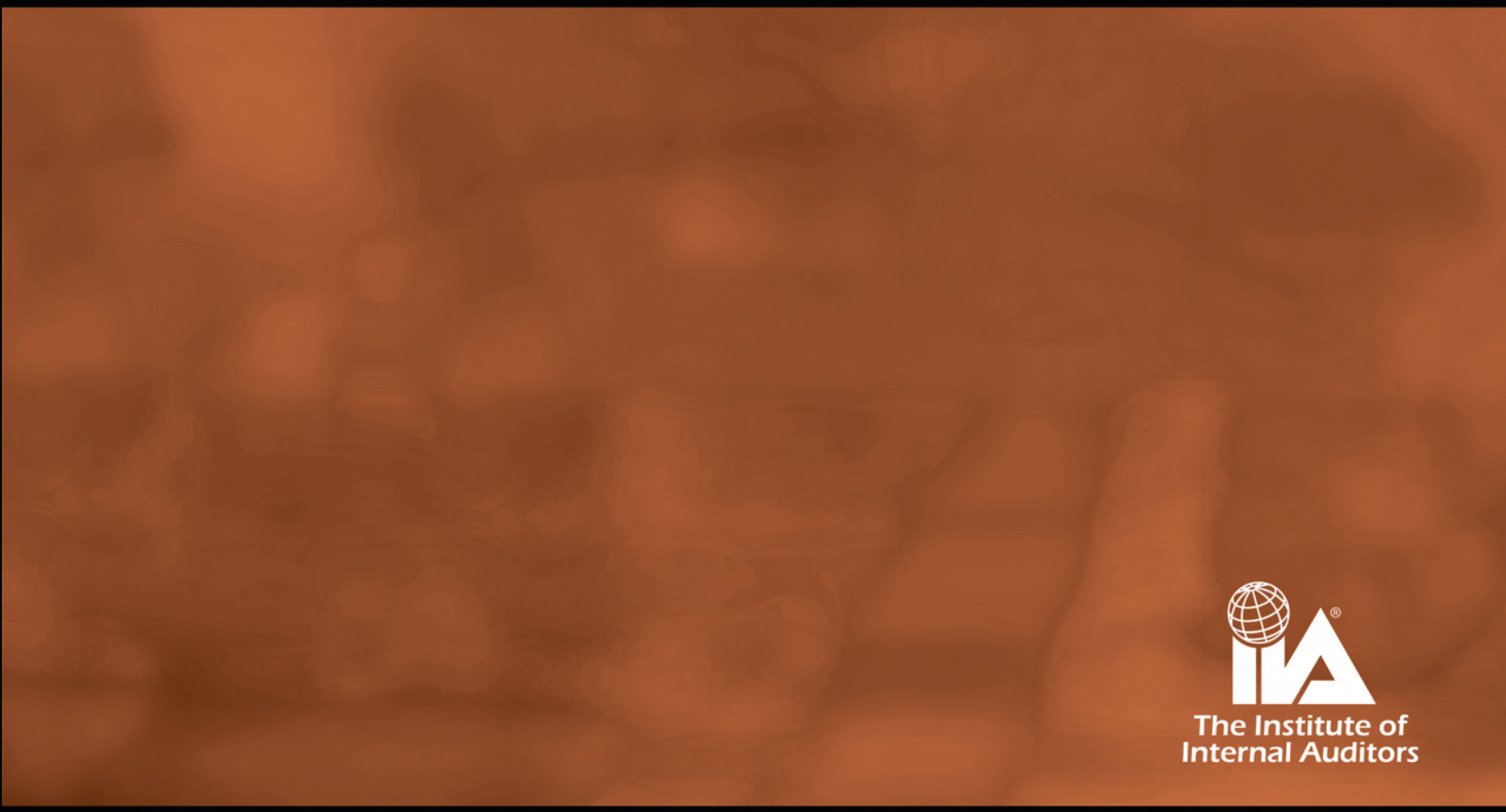
GTAG

GLOBAL TECHNOLOGY AUDIT GUIDE

Business Continuity Management



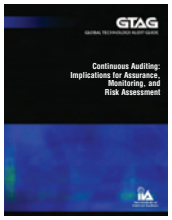
The Institute of Internal Auditors

Global Technology Audit Guide (GTAG)

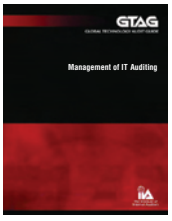
Written in straightforward business language to address a timely issue related to IT management, control, and security, the GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Information Technology Controls: Topics discussed include IT control concepts, the importance of IT controls, the organizational roles and responsibilities for ensuring effective IT controls, and risk analysis and monitoring techniques.

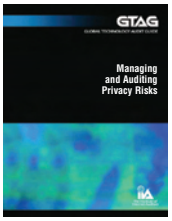
Change and Patch Management Controls: Describes sources of change and their likely impact on business objectives, as well as how change and patch management controls help manage IT risks and costs and what works and doesn't work in practice.



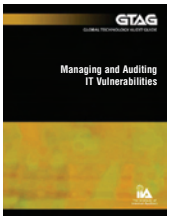
Continuous Auditing: Addresses the role of continuous auditing in today's internal audit environment; the relationship of continuous auditing, continuous monitoring, and continuous assurance; and the application and implementation of continuous auditing.



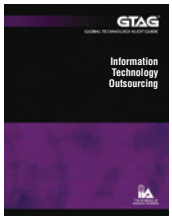
Management of IT Auditing: Discusses IT-related risks and defines the IT audit universe, as well as how to execute and manage the IT audit process.



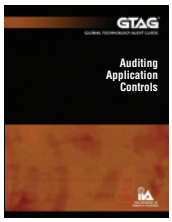
Managing and Auditing Privacy Risks: Discusses global privacy principles and frameworks, privacy risk models and controls, the role of internal auditors, top 10 privacy questions to ask during the course of the audit, and more.



Managing and Auditing IT Vulnerabilities: Among other topics, discusses the vulnerability management life cycle, the scope of a vulnerability management audit, and metrics to measure vulnerability management practices.

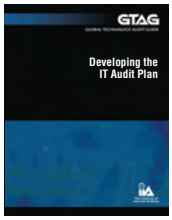


Information Technology Outsourcing: Discusses how to choose the right IT outsourcing vendor and key outsourcing control considerations from the client's and service provider's operation.



Auditing Application Controls: Addresses the concept of application control and its relationship with general controls, as well as how to scope a risk-based application control review.

Identity and Access Management: Covers key concepts surrounding identity and access management (IAM), risks associated with IAM process, detailed guidance on how to audit IAM processes, and a sample checklist for auditors.



Developing The IT Audit Plan: Provides step-by-step guidance on how to develop an IT audit plan, from understanding the business, defining the IT audit universe, and performing a risk assessment, to formalizing the IT audit plan.

Visit The IIA's Web site at www.theiia.org/technology to download the entire series.

Business Continuity Management

Authors

David Everest, Key Bank

Roy E. Garber, Safe Auto Insurance Co.

Michael Keating, Navigant Consulting

Brian Peterson, Chevron Corp.

July 2008

Table of Contents

1. EXECUTIVE SUMMARY 1

2. INTRODUCTION 3
   - 2.1 BCM Definition 3
   - 2.2 Crisis Management Planning 3
   - 2.3 Disaster Recovery of IT 3

3. BUILDING A BUSINESS CASE 4

4. BUSINESS RISKS 5
   - 4.1 Common Disaster Scenarios 5
   - 4.2 Common Disaster Impacts 6

5. BCM REQUIREMENTS 7
   - 5.1 Management Support 7
   - 5.2 Risk Assessment and Risk Mitigation 8
   - 5.3 Business Impact Analysis 10
   - 5.4 Business Recovery and Continuity Strategy 11
   - 5.5 Disaster Recovery for IT 12
   - 5.6 Awareness and Training 14
   - 5.7 Maintenance of the BCM Program 14
   - 5.8 Exercise of the Business Continuity 15
   - 5.9 Crisis Communications 18
   - 5.10 Coordination with External Agencies 18

6. EMERGENCY RESPONSE 19

7. CRISIS MANAGEMENT 20

8. CONCLUSION/SUMMARY 21

9. APPENDIX 22
   - 9.1 Sample BCP Audit Guide 22
   - 9.2 BCM Standards and Guidelines 22
   - 9.3 BCM Capability Maturity Model 23

10. GLOSSARY 32

11. ABOUT THE AUTHORS 33

1. Executive Summary

Most business professionals would agree that in the course of running a successful business, corporate executives spend a considerable amount of their time analyzing the marketplace, developing and implementing strategies, establishing performance and financial goals, developing and executing business operations plans, reporting financial results, and communicating to stakeholders. Most would also agree that prior to worldwide preparation for the year 2000, business continuity management (BCM) was not necessarily high on the priority list of every corporate executive. Although disasters in recent history have elevated the awareness of business continuity (BC) risks and their impact on corporate finances and operations, there are still companies that have failed to heed the warning signs and are underprepared for a disaster or a business disruption. Manmade and natural disruptions to businesses may be unpredictable, but the impact can be managed if an effective BCM program is part of the overall corporate governance framework.

The goal of BCM is to enable an organization to restore critical business processes after a disaster has been declared. BCM is a simple matter of risk management designed to create business continuity capabilities to match likely risks based on business value. There are large, medium, and small companies that have not adequately prepared for incidents that could render their business or part of their business inoperable for an extended period of time. Documented cases demonstrate how companies or entire industries have sustained significant financial damage due to their lack of preparedness for unforeseen disasters, including the U.S. airline industry following the Sept. 11, 2001 terrorist attacks; TfL (Transport for London) following the London bombings; and the commercial fishing industry in Sri Lanka and Thailand following the tsunami in 2004. Damage to an organization may include loss of customers, profits, reputation, government licenses/approvals, etc. The lack of preparedness exposes the business to a degree of risk that is relative to each type of business.

Whether due to economic downturns in an industry, lack of informed management, or other corporate cost decisions, BCM program champions such as chief audit executives (CAEs) often find their recommendations to executive management for improved BCM to be ignored or deferred far into the future. The CAE has the responsibility to report BCM deficiencies to management and the audit committee of the board, for example, when an audit or other discovery means reveals that management cannot provide evidence to ensure that in the event of a declared disaster, business operations and systems will be recovered in a manner that meets the organization's business, financial, and operational goals based on the likelihood of disruptive events.

This Global Technology Audit Guide (GTAG) was written with an understanding of the CAE's perspective. CAEs have been challenged to educate corporate executives on the risks, controls, costs, and benefits of adopting a BCM program. Although it is true that recent disasters around the world have motivated some corporate leaders to give attention to BCM programs, others have failed to recognize and/or address the risk. The key challenge is engaging corporate executives to make BCM a priority. On the surface, any executive is likely to express that BCM is a good idea, but when it comes to taking action, some will struggle to find the budget necessary to fund the program as well as an executive sponsor that has the time to ensure its success. This guide will help the CAE communicate business continuity risk awareness and support management in its development and maintenance of a BCM program.

As shown in Figure 1, the CAE must understand the role of BCM as one of three elements of an Emergency Management Program (Note: The term *Emergency Management Program* may be used globally in various government and business sectors, but is not necessarily a standard professional term). Emergency response (ER) is the first action that focuses on avoiding, deterring, and preventing disasters and preparing the organization to respond to a disaster. The goal of ER is lifesaving, safety, and initial efforts to limit the impact to

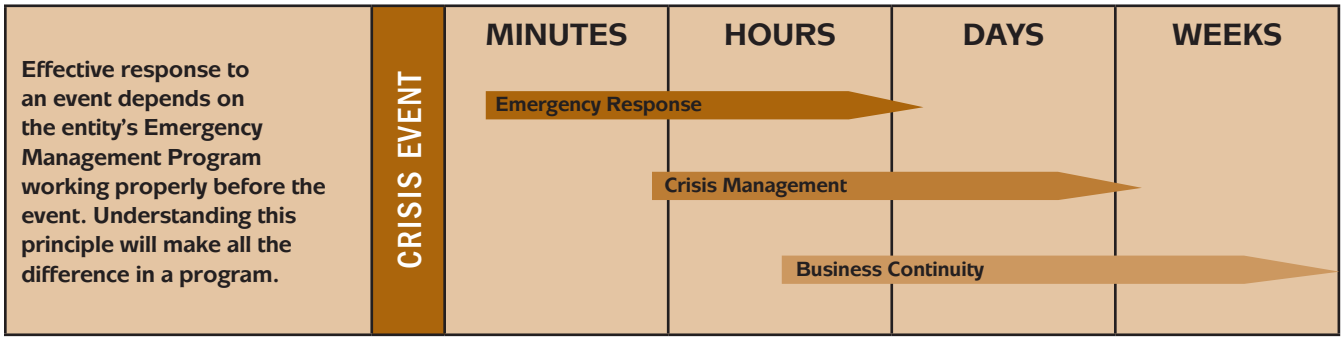


Figure 1. Emergency Management Program

asset damage. Crisis management (CM) focuses on managing external — and in some companies, internal — communications and senior management activities during a disaster. Even in an environment where ER and CM are mature and effective, BCM may remain inadequately addressed. BCM capabilities are focused on the recovery of critical business processes to minimize the financial and other impacts to a business caused during a disaster or business disruption. BCM must be integrated with ER and CM but should be a separate program.

The bottom line is that the CAE should be able to answer the following three simple and important questions related to business continuity:

1. Does the organization's leadership understand the current business continuity risk level and the potential impacts of likely degrees of loss?
2. Can the organization prove the business continuity risks are mitigated to an approved acceptable level and are recertified periodically?
3. If an unacceptable business continuity risk exists but executive management has decided to assume the risk, are the organization's owners, business partners, and other constituents aware that management has decided not to mitigate the risk? Also, has the decision to accept the risk been properly documented?

If the answer to any of these questions is "no," this GTAG can help. Specifically, this guide aims to help CAEs understand the BCM program, risks, and controls and to prepare them with information for executive- and board-level discussions. The value of this GTAG is that it provides a high-level summary in straightforward business language for executive readers and detailed guidance for internal auditors in audit assessments. This GTAG focuses on how BCM, as a program or framework, is designed to enable business leaders to manage the level of risk the organization could potentially encounter if a natural or man-made disruptive event that affects the extended operability of the organization were to occur.The guide includes disaster recovery planning (DRP) for continuity of critical information technology infrastructure and business application systems, because many business functions are predominately automated. This will help the CAE establish the basis for exercising an effective assessment and reporting key information to stakeholders.

2. Introduction

This GTAG describes the knowledge needed by members of governing bodies, executives, and internal auditors to address the effectiveness of business recovery capabilities and the impact they have on business. Other professionals may find the guidance useful and relevant as well. This guide provides information related to assessing BCM capabilities and describes the different parts of a comprehensive program and how to establish the correct plan for an organization.

2.1 BCM Definition

Business continuity management is the process by which an organization prepares for future incidents that could jeopardize the organization's core mission and its long-term viability. Such incidents include local events like building fires, regional events like earthquakes, or national events like pandemic illnesses. The key components of the BCM are:

- **Management Support** — Management must show support to properly prepare, maintain, and practice a business continuity plan (BCP) by assigning adequate resources, people, and budgeted funds.
- **Risk Assessment and Risk Mitigation** — Potential risks due to threats such as fire, flood, etc., must be identified, and the probability and potential impact to the business must be determined. This must be done at the site and division level to ensure the risks of all credible events are understood and appropriately managed.
- **Business Impact Analysis (BIA)** — The BIA is used to identify business processes that are integral to keeping the business unit functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster.
- **Business Recovery and Continuity Strategy** — This strategy addresses the actual steps, people, and resources required to recover a critical business process.
- **Awareness and Training** — Education and awareness of the BCM program and BC plans are critical to the execution of the plan.
- **Exercises** — Employees should participate in regularly scheduled practice drills of the BCM program and BC plans.
- **Maintenance** — The BCM capabilities and documentation must be maintained to ensure that they remain effective and aligned with business priorities.

2.2 Crisis Management Planning

Crisis management planning addresses how the corporate entity will inform the general public, its employees, and various stakeholders of the crisis and the steps being taken to get the business up and running again. CM consists of methods used to respond to both the reality and perception of crises, which are documented in a CM plan. CM also involves establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms. It consists of the communication that occurs within the response phase of emergency management scenarios.

2.3 Disaster Recovery of IT

Disaster recovery of information technology (IT) components supports restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (e-mail, phone, etc.), workspace, and other business processes after a disaster. A well-established and thoroughly tested disaster recovery plan must be developed in harmony with the BCM plan to increase the probability of successfully recovering vital organization records.

3. Building a Business Case

Emergency preparedness is no longer the sole concern of businesses located in earthquake- or tornado-prone areas of the world. Preparedness must now account for man-made disasters, such as terrorist attacks, in addition to pandemics and natural disasters. Knowing what to do during an emergency is an important part of being prepared and may make all the difference when seconds count. The goal of preparedness is to resume business operations with as much transparency, from the customer's perspective, as possible. Examples of recent catastrophic events affecting large and small businesses alike include:

- The worldwide SARS outbreak (November 2002 through July 2003) consisted of 8,096 known infected cases and 774 deaths. The near pandemic caused a severe customer decline in Chinese cuisine restaurants in North America, a 90 percent decrease in some cases. Most conferences and conventions scheduled in major cities were cancelled. In addition, government intervention disrupted normal business functions (e.g., travel, supply chain, etc.) for many companies in countries with known infections.
- The Sept. 11, 2001 terrorist attacks on the Pentagon and the World Trade Center were the most devastating attacks on U.S. soil since the bombing of Pearl Harbor. In addition to upsetting military processes, the Sept. 11 attacks also targeted civilian processes and U.S. businesses.
- The July 7, 2005 London bombings were a series of terrorist-planned explosions on the London public transportation system. The attacks, which were responsible for more than 50 deaths and 700 injuries, seriously disrupted London's public transportation system as well as the country's mobile telecommunications system.
- Hurricane Katrina (formed on Aug. 23, 2005) may be the costliest natural disaster in U.S. history. At least 1,836 people lost their lives in the hurricane and the subsequent floods. Katrina caused an estimated US $81.2 billion in damage, including significant damage to industrial (mainly oil, refinery, and chemical), commercial (mainly hospitality), and agricultural facilities.

Since 1983, regulatory agencies like the American Bankers Association and Banking Administration Institute have required their supporting members to exercise operational continuity practices (later supported by more formal BCP manuals) that protect the public interest. Newer standards were often based on formalized standards defined under ISO/IEC 25002.

Often, the value of a BCM program is not appreciated until it is needed. Perhaps this is because it is difficult to calculate the return on investment of a BCM program until a disaster strikes. Management needs to understand that if such a situation occurs, business must continue, but under very different circumstances. The cost of a disaster may be the end of the business. Business leaders need to weigh the cost of being prepared against the cost of closing the doors of the business for a week, a month, or forever, depending on the catastrophe. Many governments around the globe require certain industries to have a tested BCP in place. In the United States, all businesses within the financial, utility, and health care sectors are required to maintain an updated BCP. There are general and industry-specific standards and guidelines for effective BCM (see Appendix: BCM Standards and Guidelines, page 22).

During the first World Trade Center attack in 1993, Morgan Stanley (MS) learned an important lesson. None of the MS employees lost their lives, but it took four hours for all of the employees to evacuate the building. As a result, management decided that the BCP needed to be updated. MS took a careful look at its business operations and the risk of potential disasters and developed a new plan. On Sept. 11, 2001, the planning paid off. After the first hijacked plane slammed into the first World Trade Center tower, MS security evacuated all the employees. The evacuation took only 45 minutes this time, allowing MS to get on with recovering daily operations. Improvements to ER capabilities likely saved numerous lives. The BCM capabilities were also improved as part of the review.

4. Business Risks

Natural disasters happen around the world on a regular basis. Hurricanes, floods, earthquakes, and fires shatter lives and devastate businesses. Man-made disasters like fire, power failures, and terrorism are no less destructive. Together, these unanticipated events pose risks to business as usual. Sometimes the financial fallout persists for years. Some companies are never quite the same, and others simply go out of business. However, these outcomes can be avoided in almost all cases.

Almost every location in the world falls into a hot zone for hurricanes, tornadoes, earthquakes, wild fires, and/or floods. Fires can ravage a building in any city in any state. Likewise, terrorism can occur anywhere in the world.

4.1 Common Disaster Scenarios

Common disasters experienced around the world include:

Fire may occur in a single office building, a complex, or an industrial facility, or in an entire area near a forest or woodlands. Each year, more than 4,000 U.S. citizens die and more than 20,000 are injured in fires, many of which could have been prevented. Direct property loss due to fires is estimated at US $10 billion annually (in the United States alone), which doesn't include the financial loss to companies from disruption to their operations.

Pandemic is a global disease outbreak. An influenza pandemic occurs when a new influenza A virus, for which there is little or no immunity in the human population, emerges. It then begins to cause serious illness and spreads easily from person to person. Many governments around the world have begun planning for a pandemic. They have identified critical national infrastructure industries like: finance, banking, energy, transportation, government, etc. These industries are being asked to prepare BC plans to ensure critical business functions will continue to operate during a pandemic. The economic impact from a pandemic could be devastating due to unavailability of staff, which may lead to suspension of business functions. If a pandemic occurs, it is likely to be a prolonged and widespread outbreak that could require temporary changes in many areas of society, such as schools, offices, transportation, and other public services. An informed and prepared public can take appropriate actions to decrease its risk during a pandemic.

Terrorism is the use of force or violence against persons or property in violation of the criminal laws of the countries around the world for purposes of intimidation, coercion, or ransom. Terrorists often use threats to:

- Create public fear.
- Try to convince citizens that their government is powerless to prevent terrorism.
- Get immediate publicity for a cause.

Acts of terrorism include threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings, cyber attacks (computer-based), and the use of chemical, biological, nuclear, and radiological weapons. Terrorist attacks have devastated large metropolitan areas, disrupting businesses in these general areas, and have greatly impacted staffing levels for businesses in the affected region.

Biological Attacks are the deliberate release of germs or other biological substances that can make people sick. Many agents must be inhaled, enter through a cut in the skin, or be eaten to take effect. Some biological agents, such as anthrax, do not cause contagious diseases. Others, like the smallpox virus, can result in diseases that can be transmitted through people touching, coughing, etc. A chemical attack is the deliberate release of a toxic gas, liquid, or solid that can poison people and the environment. The threat of a biological attack can have a devastating impact on a business (e.g., evacuation of facilities) even if no real attack occurs.

Tornadoes are nature's most violent storms. They can appear without warning and can be invisible until dust and debris are picked up or a funnel cloud appears. Although tornadoes are more common in certain areas of the world, they can occur anywhere and at any time of the year, making advanced preparation especially important. Tornadoes can damage business facilities and lead to unavailability of staff.

Hurricanes/Typhoons are severe tropical storms that form in tropical or subtropical waters around the globe. Scientists can now predict many tropical cyclones. Organizations located in or near coastal communities impacted by cyclones must plan for an evacuation, which can significantly disrupt their operations.

Flooding is a common natural disaster in many parts of the world. However, all floods are not alike. Some can develop slowly during an extended period of rain, or in a warming trend following a heavy snow. Others, such as flash floods, can occur quickly, even without any visible signs of rain. Most parts of the world need to be prepared for flooding, but particularly locations in low-lying areas, near water, or downstream from a dam. Even a very small stream or dry creek bed can overflow and create flooding. Flooding can disrupt staff availability even if the primary business facility is not directly impacted.

The Rising Costs of Natural Disasters

Although natural disasters have taken their toll throughout history, there are strong indications that they have become more frequent and severe in recent decades and that this upward trend is set to continue. In part, this trend can be explained by growing urbanization, which has led to an increasing concentration of population in vulnerable areas (see Freeman, Keen, and Mani, 2003). It also reflects the changes in weather patterns — in particular, those associated with the rise in global surface temperatures — that appear to have increased the frequency and intensity of adverse weather events, such as hurricanes, floods, and droughts (see IPCC, 2007). With more frequent and intense natural disasters affecting increasingly densely populated areas, their costs have risen strongly over time (see below).

	1950-59	1960-69	1970-79	1980-89	1990-99	1996-2005
Number of events	21	27	47	63	91	57
(billion dollars; constant 2005 prices)						
Overall losses	48.1	87.5	151.7	247.0	728.8	575.2
Average loss	2.3	3.2	3.2	3.9	8.0	10.1

Figure 2. The Rising Costs of Natural Disasters[1]

4.2 Common Disaster Impacts

Various disasters that commonly occur may result in the loss of:

- **People.** If there is significant loss of human life or unavailability of staff, organizations may not have the proper personnel to run daily operations.
- **Facilities and equipment.** Several of the disasters described above have the potential to destroy or severely damage operating facilities, manufacturing plants, offices, and other critical business sites.
- **Communication infrastructure.** Organizations may not be able to communicate with employees, vendors, and customers.
- **Supplies.** This may include power supply, service from vendors, manufacturing supplies, etc.
- **Information and IT systems.** Critical business applications may not work properly.

[1] David Hoffman, "Innovations in insurance can help countries manage the fiscal impact of natural disasters," *Finance & Development* magazine, March 2007, Vol. 44, No. 1.

5. BCM Requirements

Figure 3 shows the action necessary to meet BCM requirements.

5.1 Management Support

Management support is critical to the success of BC at every organization. Senior management must ensure that there are policies in place that require management teams throughout the organization to deploy a BCM program for their business

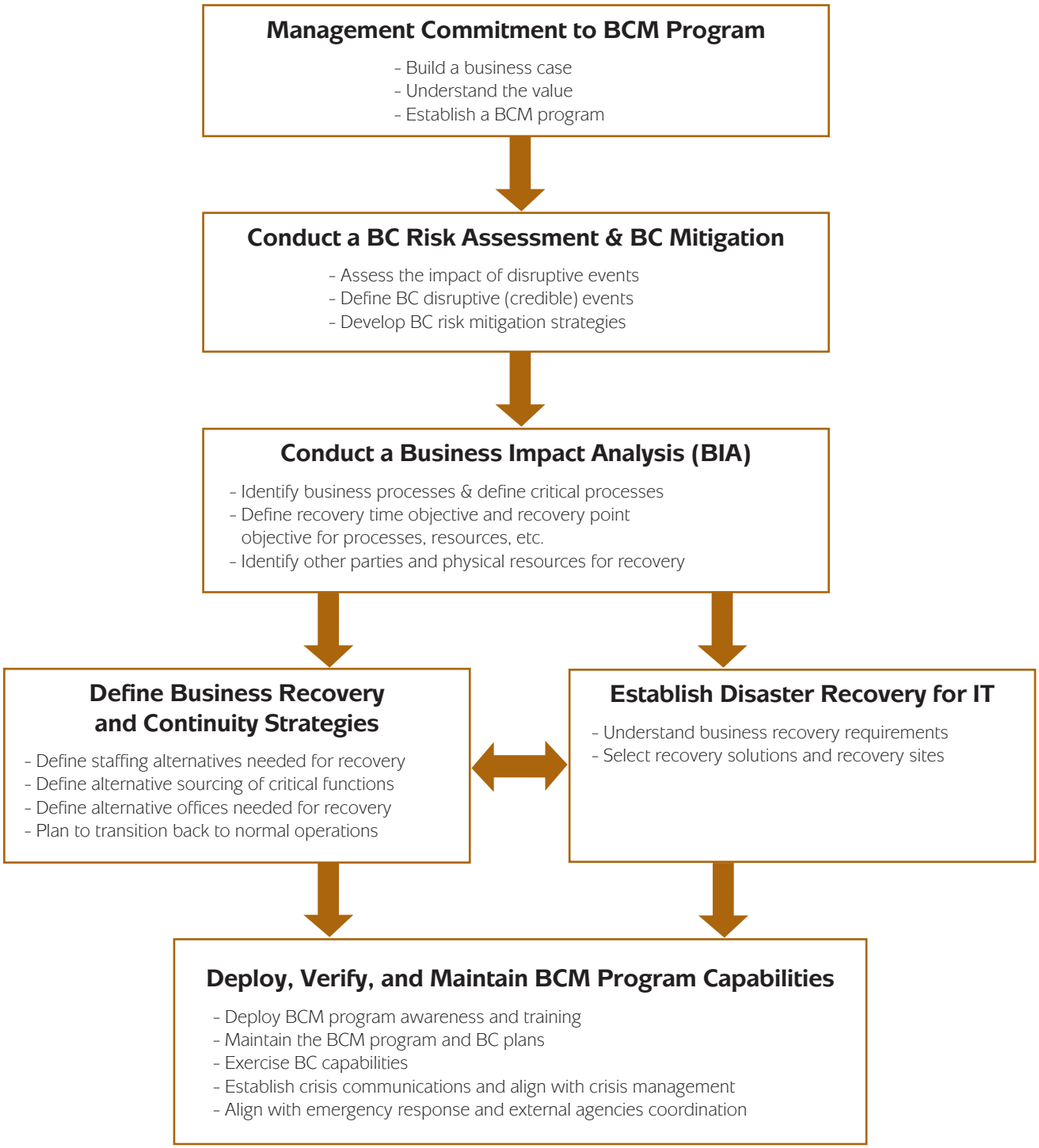


Figure 3. BCM Requirement Flow Chart

units. All emergency management policies must be aligned to ensure that CM, ER, and BCM work together during an actual disaster.

A. Senior Management Support

Senior management must display visible support for BCM and the emergency management program. This can be accomplished in various ways, including by:

- Defining a central group within the organization that is responsible for BCM and managing governance (e.g., defining required standardization), knowledge sharing, best practice coordination, consulting, and cross-business unit BCM activities.
- Creating a BCM system that each business unit (BU) must deploy.
- Ensuring appropriate funding for organization-wide BCM activities via the organization's annual business plan, testing, and ensuring BUs include funding for their BCM efforts.
- Communicating the importance of BCM and how it adds business value.
- Participating in BC exercises, training sessions, and other emergency management events.

The BCM system that each BU must deploy should include:

- A definition of BCM and its business value within the company.
- A description of the steps required to deploy and maintain a BCM program within a BU.
- The establishment of ownership for BCM by each BU (see "Business Unit Management Support" below).
- The definition of BCM metrics that can be used to evaluate progress of the program at the organization level and BU or regional level (e.g., each BU creates its own local metrics).
- Deployment of a BCM continuous quality program that can be updated by each BU to deploy and maintain BCM.

B. Business Unit Management Support

BU or regional management must also display visible support for BCM and the emergency management program. This can be accomplished in various ways, including by:

- Deploying the BCM system defined by the organization.
- Ensuring participation by all teams within the BU in the BCM effort so that they create BC capabilities to match their risk and business value.
- Identifying someone to participate in organization-wide BCM governance (e.g., define required standardization), knowledge sharing, best practice coordination, consulting, and cross-business unit BCM activities.
- Communicating the importance of BCM and how it adds business value.
- Participating in BC exercises, training sessions, and other emergency management events for the BU.
- Ensuring appropriate funding for BU BCM activities via the BU annual business plan.

In deploying the BCM system, BU or regional management should:

- Update the BCM definition section to define business value specific to the BU.
- Understand the steps that are required to deploy and maintain a BCM program within a BU.
- Establish ownership for BCM within their BU, including assigning people to key roles such as BU BCM sponsor (to arrange funding and provide leadership of BCM), BU BCM manager (to lead and maintain BCM capabilities), and BU BCM coordinator (to arrange BCM activities at the direction of the BCM manager).
- Define BU BCM metrics that can be used to evaluate progress of the program.
- Deploy a BU BCM continuous quality program.

5.2 Risk Assessment and Risk Mitigation

BU or regional management should complete a BC risk assessment for each of its business functions and associated sites (city or region). The purpose of this exercise is to identify likely risks that could disrupt critical business processes performed at specific locations of operation. The BC risk assessment is used to shape the overall BCM program scope by providing a list of likely events and associated consequences that should be addressed in a risk mitigation plan (e.g., prevention) and the BCM program. There is no way to predict all risks or to mitigate all known risks that may need to be accepted. Participants in the BC risk assessment should include individuals such as staff from the business as well as staff from the health, safety, and environment group; facilities management; legal; human resources; and personnel from the medical field.

A few disruptive events are *very likely* to occur, like hurricanes and/or utilities failures in some parts of the world, or other regularly occurring events. Specific tactical BC plans may be needed for these predictable events. Most events are *somewhat likely* to occur, such as earthquakes. Although an earthquake will occur in some regions, there is a good chance it will impact another part of the larger region. Therefore, if the site of operations is in an earthquake zone, this must be considered a likely disruptive event, which is often referred to as a *credible event*.

It is impossible to eradicate all risks from an environment and still conduct effective operations. Balance is the key to risk management of BC. When evaluating disruptive events,

it's important to identify those that are credible and look for all potential events that may impact business operations. Possible methods for predicting future disruptive events include:

- Looking at historical data associated with similar organizations in the same region.
- Using government or industry data concerning possible risks.
- Using subject matter experts when the business model changes or limited data is available to perform a detailed risk assessment.

A. Examples of Disruptive Events

Below are some examples of disruptive events that might impact critical business processes.

- Natural disasters such as earthquakes, hurricanes, rain/flooding, and lightning.
- Industrial events such as fire, explosions, spills, and contaminations.
- Supplier failures such as component provider disruptions and electricity utilities.
- Other catastrophes such as airplane crashes.
- Medical epidemic such as a pandemic or other medical risks.
- Labor disruption, including strikes, transportation disruption, and civil unrest.
- Economic or political instability, including terrorism/bombings and war.
- Human factors such as employee errors, criminal acts, and fraud.
- IT risks such as cyber-terrorism, viruses, hacker attacks, and denial-of-service attacks.
- Production and manufacturing risks such as:
  - Supplier disruptions, including power, raw materials, and critical services.
  - Production equipment failures to pipelines, boilers, and conveyor belts.
  - Unavailability of supporting utility services like treatment plants and disposal equipment.
  - Product storage, transportation, and distribution failures.
  - Unavailability of critical laboratory, testing, and/or quality control processes.
  - Process automation system (IT systems like SCADA and DCS) failures that stop production.
  - Government delays in permits, customs, staff visa, and/or certification.

B. Assessing the Impact of Disruptive Events

After identifying the credible events that could impact each of the organization's sites or regions of operations, additional work is needed to understand the event. Some of the factors that must be evaluated to better understand the scope and impact of the potential event include the:

- **Geographic extent of the impact:** A single building (e.g., fire), entire facility complex (e.g., chemical spill), metropolitan area (e.g., transportation strike), large region (e.g., earthquake), or potentially the world (e.g., pandemic flu).
- **Days of impact:** Number of days before operations will likely return to 75 percent functionality, which means 75 percent of people, resources, and production are functioning. Days of impact may be the period before the organization can replace lost resources, like renting a new building and making it functional after a building fire.
- **Availability of staff (by days):** Percentage of staff that likely would be able to work based on each likely disaster event (by days: 0, 3, 7, 14, or 30). Staff may need to go home for an extended period for some disasters like earthquakes that may damage homes.
- **Availability of operations and/or offices:** Likely percentage of operations and/or office space that is functional (during the days of impact).
- **Availability of IT (during the days of impact):** Likely availability of key IT components for each disaster event. This includes IT infrastructure (logon capabilities), IT network, IT applications, etc.

The BC risk assessment can be used to determine the impact to critical business processes. Some operating facilities, like research and development offices, may have few critical business processes performed at the site. The BC risk assessment for all sites should focus, at minimum, on the health and safety of staff, security, and potential environmental impacts to ensure that the CM and ER functions will have the resources they need to be successful.

C. Developing Risk Mitigation Strategies

Developing and deploying BC risk mitigation strategies will help to minimize the impact of disruptive events and will improve response capabilities. Examples of risks and their corresponding mitigation strategies include:

- **Safety risks for various disasters:** Leverage ER and/or Health, Safety, and Environmental team and/or operational plans.
- **Operational failures:** Leverage standard operating procedures and normal maintenance activities.
- **Loss of primary office:** Arrange to move staff members to an alternative office or enable them to work at home, assuming their home is likely to be functional (i.e. not damaged if the event is regional, and home has necessary resources like equipment, computer, network connection, etc.)
- **Loss of IT network connectivity:** Develop IT system and information recovery (disaster recovery) plans to create network redundancy or recovery.

- **Loss of IT data center:** Develop plan to manually perform work processes until IT systems can be restored. Also, develop IT disaster recovery plans to restore IT systems at alternative site.

The BCM sponsor and an appropriate team of managers must review and approve the BC risk assessment and BC risk mitigation strategies. Since management must act to address the risks, it is critical that management approve the BC risk assessment and ensure the BC risk mitigation plan is funded, implemented, and tested periodically.

5.3 Business Impact Analysis

A BIA is used to identify critical business processes that need to be recovered following a disaster event. The BIA may include an initial discussion of recovery solutions needed to resume the critical business processes (see "Business Recovery and Continuity Strategy" on page 11). Participants in the BIA should include staff from the business as well as key suppliers.

The BIA should be performed with the knowledge from the BC risk assessment that defined the credible events that could disrupt the business. Typically, BIA meetings are performed individually for each team. Then, discussions occur with the other teams identified as critical providers after each BIA meeting.

A. Identifying the Business Processes

The first step in a BIA is to identify the business processes performed by the functional team, the resources needed to perform the function, and the critical staff performing the work. The business processes initially should not be broken down into too many individual sub-processes. Business processes should be identified separately if they have different staffing (e.g., staff roles), service providers (e.g., third party, outsourcer, etc.), or resources (e.g., IT systems).

B. Determining RTO and RPO Based on Business Impact

The second step in a BIA is to identify the type of business impact if the business process cannot be performed. Below are some types of business impacts:

- Health and safety (e.g., injury).
- Environmental (e.g., spill).
- Customer service (e.g., loss of customers).
- Financial (e.g., penalties).
- Regulatory/legal (e.g., governmental action).
- Reputation (e.g., loss of image).

Then, determine a recovery time objective (RTO) based on the types of business impact. An RTO is a duration of time and service level within which a business process must be restored (after a disaster) to avoid unacceptable consequences associated with a disruption in continuity. An RTO is typically identified based on standard time markers of 0, 3, 7, 14, or 30 days. The business management ultimately determines the correct RTO for each business process. Typically, the cost of the recovery solution will rise as the RTO decreases (i.e., if the business process must be restored immediately, the cost could be very high).

Next, determine a recovery point objective (RPO) for information systems. The RPO is the amount of data that can be lost if a disaster destroys the information systems. Business staff must determine how many days' worth of data can reasonably be lost and recreated manually. Data can often be recreated from other sources such as external systems that exchange data with the organization system (e.g., banking systems). The business management ultimately determines the correct RPO for each business process. Typically, the cost of the recovery solution will rise as the RPO decreases (i.e., if the business process cannot afford to lose any data, the cost of data replication could be very expensive).

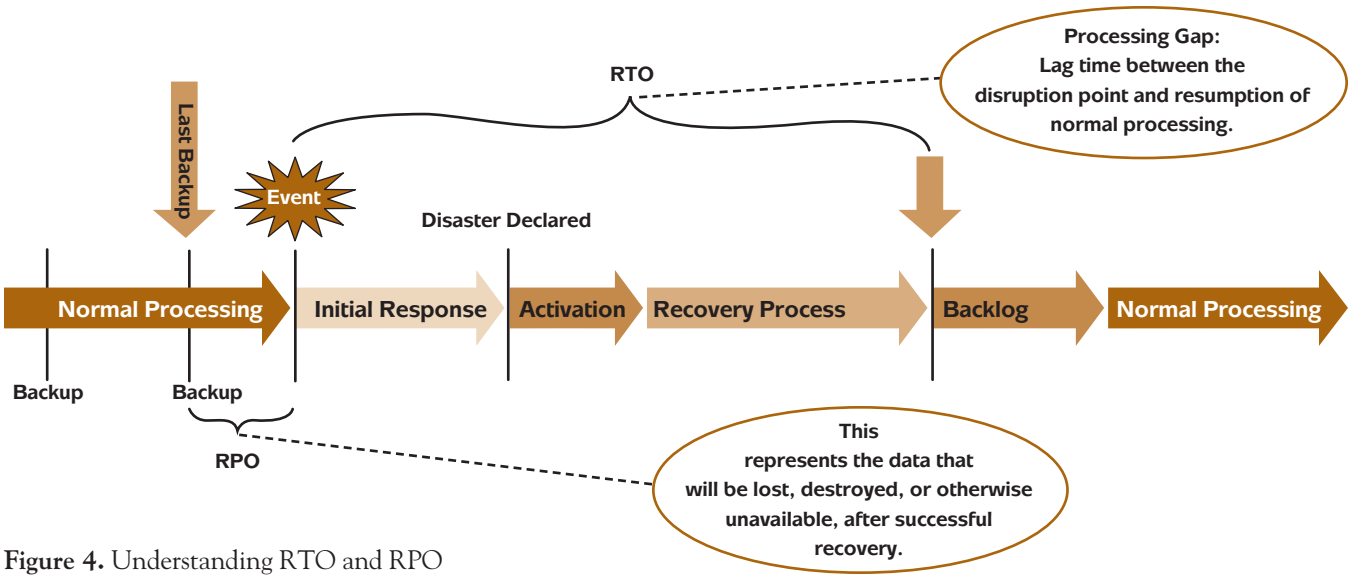


Figure 4. Understanding RTO and RPO

C. Identifying the Other Parties and Physical Resources

The third step of the BIA is to identify the other parties and physical resources that are critical to the business process, which could include other departments, vendors, other third parties, critical equipment, and physical records. A BIA may need to be performed with other parties who support critical business processes to ensure they are prepared to support business recovery.

D. Obtaining Sponsor and Manager Approval of BIA

The BCM sponsor and managers of each team must review and approve the BIA for their scope of operations. Since managers throughout the organization are responsible for ensuring the business continuity and recovery solutions are implemented, they must own the BIA for their team.

5.4 Business Recovery and Continuity Strategy

Business recovery and continuity strategies must be developed for critical business processes identified during the BIA. The BIA may include an initial discussion of recovery solutions needed to resume the critical business processes (see "Business Impact Analysis" on page 10). Participants in the business recovery and continuity strategy session may include staff from the business, key suppliers, and information systems organizations.

The business recovery and continuity strategies may include some of the following types of solutions:

- **Manual work processes:** Work can be done manually while IT systems are down.
- **Outsourcing:** Some work can be performed by external companies, competitors (reciprocal agreement), or secondary vendors.
- **Disaster recovery for IT:** An IT recovery solution will be needed for critical systems, but because these can be very expensive, manual work processes may be used initially following a disaster.
- **Alternative staffing:** Identify other staff members who can perform the job function.
- **Alternative facilities:** Identify alternative facilities where the primary staff can work.

When developing business recovery and continuity strategies, the credible events identified during the BC risk assessment must be considered along with their likely impacts to resources. Alternative facility options may be very limited for regional disasters like hurricanes, which could impact organization facilities and employee homes at the same time.

A. Staffing Recovery Activities

Because limited staffing is a likely outcome for most credible events, alternative staffing is always required for BC. The best option is to identify people outside the likely impacted area based on the credible events. If there are no people from outside the area, then consider increasing staffing levels in the primary region. If it is assumed that 80 percent of the staff will not be available if a disaster strikes, consider how many people are needed to perform a particular job and multiply that number by five:

- If one person is needed to perform the job, identify five people who could do the job.
- If two people are needed to perform the job, identify 10 people who could do the job; and so on.

Business people who normally perform the work may know of other ways to perform the critical business processes. These options may include manually performing the job functions, which may already be done on occasion when systems are down. Other options may include using existing staff at another site if the primary staff is unavailable. Some functions can be outsourced to a third party if needed.

B. Alternative Sourcing of Critical Functions

Consider various options to have the work performed by an external provider. Assess the degree of consistency and quality that is required for each critical function. In a disaster, the organization may be able to function with industrial standard products and services that do not meet exact organization specifications. Another option is to outsource internal work to other suppliers. Many functions can be performed externally by various companies that provide standard services. Consider establishing a reciprocal agreement with competitors if there are high capital costs or regulated functions that are performed consistently by numerous companies.

Many of the risks identified during the BIA may include suppliers of goods and services that are critical to the organization's overall supply chain. These vendors may provide critical raw materials, or components used to manufacture products or used in the packaging, storage, or distribution of products. Contractual terms can be used to ensure that key suppliers meet their obligations, assuming they remain in business. Alternative suppliers (supplier diversity) may be needed if the primary supplier fails.

Another option is to determine how to supply products if a complete failure occurs in production. Procuring product from competitors in a disaster may be an option, but a reciprocal agreement in advance may help control costs. Another option is to prioritize customer fulfillment based on contractual commitments, followed by future business opportunities, etc. Identifying production alternatives in advance can help maximize overall company production based on various disaster events. The data would include resource utilization, by-product production, and other factors that could be

used to optimize production based on available resources and (vendor and utility) services.

C. Alternative Offices Needed for Recovery Activities

Alternative office space may be required in nearly all disasters that require the activation of the BCP. There are many options to provide offices for staff, but the cost of these solutions varies greatly. Below are some of the alternative office space options.

- Another organization facility that is outside of the disaster zone but near the primary office is often a low-cost solution. This requires the business unit at the alternative organization office to invoke their BCP to send noncritical staff home.
- Many people today use remote access to perform many office-related functions from home or a hotel. The key requirement is that employees have the appropriate security tools (e.g., remote access token) and appropriate hardware (e.g., laptop or personal computer) they need to work remotely. When evaluating remote access solutions, the impact to productivity must be considered, particularly as it pertains to lack of collaboration and communications if a team is spread across multiple sites.
- Commercial recovery sites also offer office space, but usually at high cost and often with limited network connections to the organization IT systems.

Any alternative office space solution must be tested by users to ensure they can log on. Some volume (performance) testing also must be completed to verify the solution will support the desired number of users. Noncritical staff should be instructed to not log on during a disaster so that resources remain available for those deemed critical.

D. Planning to Transition Back to Normal Operations

A plan must be developed to transition the organization back to a normal state after the recovery solutions are no longer needed. This can be challenging because the organization operates in an abnormal state during a disaster. Manually collected data must be entered into systems once they are restored. Financial and regulatory exceptions that occurred during the disaster must be resolved by filing the appropriate paperwork and obtaining approvals. Product exchanges (borrowed) that occurred during the disaster either need to be replenished, or the other party must be paid for those products.

The BCM sponsor and an appropriate team of managers must approve the continuity strategies for their scope of operations. Because managers throughout the organization are responsible for ensuring the business continuity and recovery solutions are implemented, they must own the continuity strategies for their team.

5.5 Disaster Recovery for IT

Depending on the business functions being performed and their reliance on IT, some portion of the critical business processes can be recovered without IT or information. In other cases, IT systems and information are needed to support the recovery of some critical business processes. Each organization must determine the maximum downtime of IT systems that can occur before it becomes an issue that could jeopardize the entire organization, whether it be hours, days, weeks, or more.

Disaster recovery planning is a term used to describe IT recovery. Some companies use different terms to include the recovery of IT systems, data, information management systems and processes, and other related systems. The disaster recovery document should describe the IT and information management systems recovery strategies. The DRP should cover detailed recovery instructions that may include references to procedures, vendor references, system diagrams, and other related recovery materials. The detailed recovery procedures must be updated when system and business processes change.

Below are some examples of the components that may be recovered as part of the DRP.

- IT systems, including:
  - IT data center.
  - Applications and data needed by the organization.
  - Servers and other hardware.
  - Communications such as phone, radio, etc.
  - Network, including external (third party) connections.
  - IT infrastructure (e.g., logon services and software distribution).
  - Remote access services.
  - Process control systems (e.g., SCADA/DCS).
- Information management systems, including:
  - File rooms.
  - Document management systems (electric and manual).

A. Considerations When Selecting DRP Strategies

There are a number of things to consider when selecting IT recovery strategies:

- The DRP document should describe the strategies for recovering systems and information based on direction from staff after staff members have performed a BIA.

- The recovery capabilities of critical IT and information service providers must be assessed to ensure they meet the requirements of the business.
- The recovery of IT and information components often must be combined to create a complete system needed to support critical business processes. For example, recovery of an application may require recovery of the desktop application, server application, server hardware, server operating system, infrastructure servers, data center, third party network connections, etc.
- Internal and external service providers of IT and information services should describe the recovery services they provide, including information regarding:
  - The recovery activities the service provider is responsible for and any recovery limitations there may be.
  - The recovery activities (e.g., reconstructing lost data) the organization is responsible for.
  - The manner in which the organization and service provider will communicate during a disaster.
  - Contracts for third parties (e.g., application service providers) or service level agreements for the internal provider.
  - The scope of their recovery efforts (e.g., systems, data, network, etc.).
  - Their recovery strategy.
  - Their RTOs and RPOs.
  - The cost of their recovery solutions, services, testing, and declaration of disaster.
  - The frequency of their recovery testing.
- Components of the environment may be recovered using solutions that would not normally be used in a production data center. For example, some data may not be recovered initially (e.g., large image libraries) which means they would not be available (e.g., may generate error messages).
- Recovery strategies for each IT system or component should be developed independently without a need for consistency with other IT systems. However, it's important that components that work together to form a system be hosted in the same location or in multiple locations that have sufficient network bandwidth. For example, e-mail might be recovered at one large central data center, file replication may occur at another site on a server within the local region, some applications and services (e.g., engineering) may be outsourced temporarily during a disaster, local applications recovery may occur using a PC instead of a server, etc. The objective is to find the best and most cost-effective recovery solution for each system, even if solutions are spread around the world. The only requirement is that the systems be accessible by the users, regardless of where they are recovered, and all components of a system work together.
- Information security and compliance standards need to be considered when designing recovery solutions. Recovery solutions should not introduce unreasonable levels of security or compliance risks. Some security and compliance controls will be relaxed if a real disaster occurs, but a conscious decision is needed to understand the risks that exist in the recovery environment. Recovery solutions are intended to reduce the risk associated with the loss of availability, but must be balanced with the need for integrity and confidentiality.

B. Recovery Solutions and Recovery Sites

The following is a list of recovery solutions and recovery sites commonly used.

- Hot recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery resources are available at recovery site(s) and data is synchronized in real-time to enable the system to be recovered immediately or within hours.
  - Typical recovery time is minutes to one day.
- Warm recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery resources (e.g., nonproduction systems, spare hardware, etc.) are available at recovery site(s) but may need to be configured to support the production system when the disaster occurs.
  - Some data may need to be restored (probably from tape or other backups).
  - Typical recovery time is two to 13 days.
- Cold recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery site(s) have been identified with space and base infrastructure needed to perform the recovery.
  - Recovery resources (e.g., servers) are not available at recovery site(s) and likely need to be procured.
  - Data likely needs to be restored (probably from tape backups).
  - Typical recovery time is 14 to 30 days.
- No recovery plan/capabilities.
  - No recovery plan exists.
  - Recovery resources and data restore processes have not been defined.
  - Data backup plans exist to ensure that critical data can be restored at some time in the future.
  - A risk exists that the systems and business processes they support may never be recovered or may result in an extended delayed recovery.

The BCM sponsor and an appropriate team of managers must approve the IT recovery solutions for their scope of

operations. Because managers throughout the organization are responsible for ensuring the BC and recovery solutions are implemented, they must own the IT recovery solutions for their team.

5.6 Awareness and Training

Education and awareness are effective in preparing staff for recovery. Awareness training should be given annually, at minimum, to ensure that staff members understand their BC roles and the emergency response activities at their site or region. CM training, including leadership team decision-making and managing communications, is also vitally important.

The BCM program requires varying degrees of knowledge based on the role of the participating individuals and the sourcing strategies. Below are some of the roles and the knowledge level needed for each role:

- BCM sponsor should:
  - Understand BCM concepts and the value proposition for BCM.
- BCM manager should:
  - Understand emergency management (CM, ER, BCM).
  - Earn a Certified Business Continuity Professional (CBCP) certification from DRI International (DRII), Business Continuity Institute (BCI), or equivalent. (This qualification is optional for business unit BCM managers, but is required for the organization-wide BCM manager.)
  - Create BCM program and/or process deployment (best if aligned with organization methodology like operational efficiency, safety, and/or other related processes).
- BCM coordinators should:
  - Possess a strong knowledge of organization BCM process methodology (typically delivered via organization or external training).
- BCM consultant (internal or external) should:
  - Earn a CBCP or Master Business Continuity Professional (MBCP) certificate from DRII, BCI, or equivalent.
  - Have extensive experience performing the following: BCM risk assessment, BIA, recovery planning, exercises, etc.
- BCM staff should:
  - Understand BCM concepts and the value proposition for BCM.
  - Understand emergency communications procedures.
  - Know the ER for their site or region.

Exercises are the primary methods of training staff on the actual execution of the recovery plans and their roles, as well as identifying gaps and weaknesses. See "Exercise of the Business Continuity" (page 15) for a description of different types of exercises.

5.7 Maintenance of the BCM Program

One of the most common obstacles preventing organizations from obtaining BC readiness is neglect. Frequently, organizations invest great time and expense in developing plans that are never maintained thereafter. Like any operational plan, BC and CM plans atrophy over time and become less effective as changes in business priorities, people, processes, technology, and operating environment fail to be reflected in the plans. In some cases, "maintenance" is limited to changing the dates on a plan without changing the content. In all cases, the focus of the internal audit group should be on the maintenance of the BC/CM capability, not simply updating a document.

Some techniques to evaluate the maintenance of BC include:

- Evaluating the document change history to determine whether updates to the document are recorded.
- Reviewing maintenance requirements to ensure component maintenance is assigned to specific individuals and management provides guidance to enable the individuals to be effective at maintaining BC capabilities.
- Reviewing BC assumptions to ensure they align well with current operating requirements. BC assumptions should change to address new issues such as additional locations, new concentrations of risk (e.g., a new disaster scenario becomes credible), reliance on new/different third parties, or operations in new countries.
- Reviewing changes in BC assumptions to ensure each change has a basis.
- Reviewing the date of the BIA to ensure the foundation for the BC plans is current enough to provide adequate direction.
- Contacting people responsible for tasks in the plan to determine their understanding of the requirements and confidence that they can perform well. In many cases, people named in plans (especially plans that have existed for several years) are simply replacements for their predecessors in name only and have not been provided the same training as when the BCM program and/or BC plan was initially introduced.
- Reviewing the BC document structure/setup to determine how accurately it reflects the current organizational model and structure.
- Scanning for words such as "current" and "today's" and evaluating whether the associated content is truly keeping pace with the organization, especially if a document is available electronically.

- Reviewing exercise/test results and associated action reports for exceptions (e.g., gaps) requiring remediation.
- Assessing the BCM program and BC recovery capabilities to ensure they have been updated to correct necessary gaps and have been implemented effectively.

5.8 Exercise of the Business Continuity

Exercises, or tests, are generally considered the most effective way to keep a BCM program and BC plans current and executable. Some organizations differentiate the terms *exercise* and *test*, but there is no requirement to use these terms in specific circumstances. Regardless of vernacular, the emphasis on plan testing should be to improve the organization's performance in an actual event. It is important to note that there are many types of exercises, which, when used appropriately, can provide assurance and add value. All major BC standards require some sort of exercise/test regime to be an integral part of the BCM program. Generally, a large-scale exercise of the BCM programs and BC plans should be conducted at least annually. More frequent testing may be required for complicated environments and those with great impact (e.g., loss) to the organization. Several component tests should also be scheduled at regular intervals throughout the year.

Exercise/test requirements should be documented either inside the plan itself or in the entity-level BCM policy. Most of the standards used to govern BCM programs require three basic elements of a testing regime:

- Tests must be held at periodic intervals. The actual period between the events is determined by the BCM Steering Committee and is based on the program goals and objectives.
- Tests should address a variety of threats/scenarios and different elements within the BCM program. It is possible to address these issues in a series of broadly-based annual exercises or through more targeted site or component-level testing.
- There must be some method to track issues and gaps uncovered in the test and track their resolution.

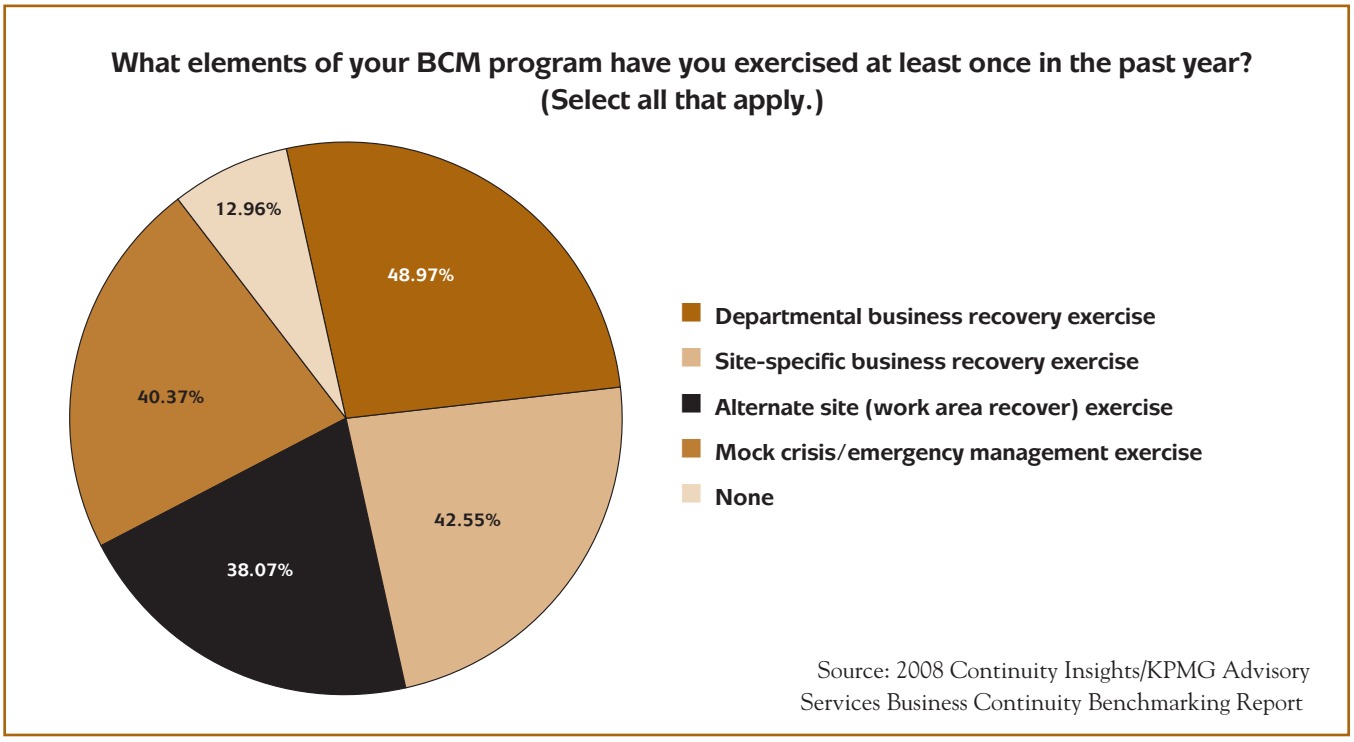


Figure 5. Exercising BCM Program Elements

A. Types of Exercises

Exercise Type	Description and Objectives
Desk Check or Plan Audit	This is the least invasive type of exercise/test generally still considered a test. A desk check normally involves only the plan owner and perhaps a disinterested third party. The goal of this type of effort is simply to ensure that content inside the plan is not outdated (e.g., contact information) and that the general thrust of the plan is still relevant. It normally includes a simple page-by-page reading and updating of the plan itself. **Objectives:** • Ensure team members are accurate. • Ensure internal and external contact numbers are current.
Orientation or Plan Walkthrough	Especially after a BC or CM plan has been recently adopted or significantly enhanced, it is helpful to walk through the document informally with those expected to implement it. The effort would include a team meeting facilitated by a designated team leader. Normally, this type of low-intensity event does not constitute a "test" in terms of an organization's BCM policy requirement. **Objectives:** • Ensure team members understand their new/updated roles. • Ensure team members understand basic plan content and format.
Tabletop Exercise (Boardroom Style Exercise)	In many cases, it is helpful to bring the entire BC/CM team together for a session to work collaboratively through a realistic scenario to identify challenges and build rapport in solving them together. Generally, these exercises last two to four hours and are facilitated either by the BC/CM manager or an independent third party. The effort concludes with a formal exercise critique detailing whether pre-established exercise objectives were met and outlining gaps uncovered in the event with a remediation timeline as well as next steps to be performed. **Objectives:** • Help team members understand the importance of their roles and responsibilities. • See the benefit of solving continuity/crisis challenges as a team. • Identify specific planning/training gaps across functional areas.
Communication Testing	Communication is a key component of a BCM process. In fact, failure to communicate accurately to key stakeholders is a frequent cause of failed crisis responses. These tests vary widely depending on the scope of communications planning and level of automation used in the crisis communications process. Companies that have deployed a mass notification tool realize a double benefit from their exercise: evaluating the tool's performance and exposing participants to how the notification will be received. Normally, this type of event involves actually contacting business partners and employees, not simply reviewing contact list information. **Objectives:** • Validate the contact information of key stakeholders. • Train participants in how to use mass notification and any role they have in the response. • Properly configure mass notification tools. • Identify communication gaps/bottlenecks where timely communication could falter in an event.

Exercise Type	Description and Objectives
IT Environment (Systems and Application) Walkthrough	This test involves conducting an announced or unannounced disaster simulation and executing documented system recovery procedures. Many IT environments are extremely complicated, and plans may be built around recovering specific applications or systems rather than the entire data center loss. In these circumstances, testing the loss of a data center could be highly disruptive and expensive. A well-designed walkthrough can be an effective exercise to bring disparate parties together in the only way that can be accomplished practically. **Objectives:** • Verify that critical systems and data can be recovered in a large-scale event. • Determine whether internal resources in individual system or application plans are able to fulfill their responsibilities, given the loss of multiple systems/applications. • Coordinate the use of response/recovery resources across multiple locations/lines of business. • Ensure the adequacy of supporting resources (e.g., human resources, procurement) to the IT response.
Alternate Site Testing	This test of all restoration/recovery components at an alternate site should include a test of the organization's ability to relocate staff to the alternate site, as well as a validation that recovery processes and IT assets operate at the alternate site, as designed. **Objectives:** • Demonstrate the actual capability to continue key processes at the alternate site. • Identify whether privacy, security, and financial controls can be maintained in the alternate operating environment. • Train participants on any revised procedures to complete key processes at the alternate site. • Evaluate the sufficiency and effectiveness of IT assets at the alternate site. • Ensure the plan to transport employees is reasonable based on the likely disaster scenarios identified in the BCM risk assessment.
End-to-end Testing	This test of alternate site facilities should include both business and IT. An end-to-end test differs from an alternate site in that critical suppliers/business partners and customers — internal or external — are included within the scope. This test typically validates connectivity to the organization's production site. **Objective:** • Demonstrate the ability to perform key processes at a pre-determined level without significant issues. It is not necessary to demonstrate 100 percent operational capacity in end-to-end testing; however, the leading practice would be to reconcile the effective capacity of the continuity strategy with the performance expectations assumed or documented in the continuity plan.

B. Exercise Frequency

Internal audit executives often wonder whether there is a "right" frequency of exercises/tests for the BCM program. Frequency of exercises alone is not the answer, because conducting the same test twice a year will quickly lead to stagnant outcomes and bored participants. As in many control areas, the generally accepted leading practice is for the frequency to be sufficient to ensure that the program is becoming progressively more mature. The majority of mature organizations test business continuity processes one or two times a year; however, this can be increased by such factors as:

- Changes in business processes.
- Changes in technology.
- A change in BCP team membership.
- Anticipated events that may result in a potential business interruption (for example, the onset of hurricane season or the perception that a pandemic could be imminent).

Regardless of the actual frequency of exercises/tests, the CAE's focus should be to ensure that the exercises/tests performed contribute to the continuous improvement of the program.

5.9 Crisis Communications

Crisis communications planning is an integral part of a holistic BCM program, and is most often coordinated by corporate communications, public relations, or another department staffed with professional communicators. Where crisis communications plans exist, they frequently address how to manage the media messaging following a crisis event. In all cases, the crisis communications process should be a subordinate function to the overall CM process, rather than a standalone effort.

Unfortunately, addressing the media is only a small fraction of the amount of crisis communications that occurs in a real event. Although the media contact is important and very public, failures in "lesser" elements of crisis communication can be equally devastating if poorly managed or executed.

Effective crisis communications plans are designed to communicate proactively an integrated message to varied stakeholders in a manner that is relevant to the individual audiences. Communication points relevant to the financial community may not be as relevant to employees or neighbors; however, the core message must be consistent. Although it is impossible to anticipate every aspect of crisis communications to be deployed during an event, some audiences that should be addressed in plans and preparedness efforts include:

- Members of the organization's response team.
- Managers responsible for continuing operations and interfacing with employees.
- Line employees whose understanding of the broader issues may be less complete than the management team.
- Family members of employees, especially family members of employees directly impacted by the event or the organization's response.
- National media, including financial media, whose interest in the organization is principally focused on management of the current event.
- Local media, both print and broadcast, that cover the organization regularly on a broad variety of topics.
- Investors, especially institutional investors, who desire transparency in the short- and long-term ramifications of an incident.
- Local and state/provincial governments that are interested in the long-term viability of the tax base and other benefits the organization brings to their constituents.
- Regulatory agencies responsible for ensuring continued compliance even when operating in recovery mode.
- Neighbors who may be adversely affected by the event, the organization's response, or the authorities' efforts to minimize overall community impact.

5.10 Coordination with External Agencies

None of the aspects of BCM can exist in a vacuum. In addition to coordinating the various disciplines amongst themselves, it is imperative that coordination points with external entities are reflected in the planning process. Government entities are interested in properly prepared private-sector organizations. For example, the United States passed Public Law 110-53 in 2007, which mandates the creation of a voluntary emergency preparedness standard by which private sector organizations can measure their efforts to prepare for a crisis. The UK Civil Contingencies Act addresses the ways in which authorities will work differently with the private sector during a state of emergency. Other governments have similar laws addressing their expectations of themselves and the private sector during a crisis. There is no "right" way to document each of the touch points with these external agencies, but at a minimum, the planning should address the following questions:

- Which governmental entities are required to be contacted following an event?
- What thresholds exist for mandatory notification, and under what circumstances would the organization make a voluntary notification?
- What areas of concern will each agency have, and how will they be different or similar?
- How can the organization engage governmental entities during the planning or exercise process to benefit from their experience without compromising the organization's independence?
- What BCM program requirements exist from regulatory agencies, and how does the organization communicate its compliance?
- Are there external agencies that must review or approve continuity strategies such as temporarily producing products in an uncertified facility, performing regulated functions out of a separate geography, or altering the way raw materials or finished products enter the country?
- Within the organization, who will interface with each governmental entity and how?

Generally, the best way to address these and other concerns is to ensure that management is responsible for the BCM program and is actually talking with external agencies about this topic. The fact that external agencies have not expressed their expectations for BCM performance to management does not mean that they do not have expectations. Communication and coordination with these entities in advance is a crucial step to securing their partnership during an actual event.

6. Emergency Response

Emergency response is generally described as the tactical planning and practical activities designed to protect life and property immediately following some type of event. Most industrialized nations have some requirement to develop ER plans for larger organizations, and specific requirements related to industries abound. In many cases, government agencies define specific requirements, but there are many guidelines from national or international industry groups that address ER issues. Some of the key elements of an ER program include:

- Evacuation planning and assembly.
- Escalation protocols.
- Damage assessment and reporting.
- Hazmat response and spill control.
- Medical response.
- Salvage and reclamation.
- Specialty issues such as fire brigades, first aid, high angle or confined space rescue, etc.

The CAE is generally not asked to review this aspect of preparedness as a standalone item. Therefore, the essential aspect to address in any BCM review or consultation is proper levels of integration and cooperation with those internal resources responsible for ER. Because many BC events begin with an ER effort, failure to coordinate plans and activities not only impedes the organization's ability to address all the immediate impacts of an event, but also makes the long-term decision-making process more difficult by needlessly omitting a key piece of information about the source and characteristics of the interruption.

Because many ER plans focus on life safety issues — almost to the exclusion of any other considerations — one of the common challenges in coordinating the continuity and ER efforts is determining how those responsible can incorporate each others' priorities without diluting their primary focus. This is an area where internal auditing can add value because of its neutrality and consultative approach. In most cases, BC teams can use information already being gathered by an ER team to augment the BC plans, and ER teams can be better informed about how their actions affect the operational, financial resilience, and reputation of the organization.

Organizations with significant ER needs due to the nature of their operations almost always employ a structured approach to managing the response effort. One popular mechanism is the Incident Command Team model, in which an incident commander is chosen to oversee all aspects of the ER, including logistics, planning, situational reporting, and operational response. Most organizations that use an Incident Command Team model customize their approach to the organization, but retain the key principles of unity of command and clearly defined roles and responsibilities. Additional information on the Incident Command Team model can be found at http://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

If coordination of the BC and ER programs is to be included in an audit plan, some key questions should be considered:

- How frequently do the program owners meet to discuss program issues and concerns?
- Have the program owners jointly met with local ER authorities to build a consensus on how events of various magnitudes can be managed best for both immediate and long-term impacts?
- Does the ER coordinator have sufficient influence to alter BC strategies if warranted, and vice versa?
- Has senior management approved a clear delineation for the responsibilities of ER versus BC in an organization?
- Are there concrete handoff protocols for information and external relationships as the ER phase draws down and BC increases in priority?
- If an Incident Management Team model is used, does the leader of the BC program have a role on the team?

7. Crisis Management

Crisis Management is easily one of the most misunderstood words in the entire BCM field. In some organizations, it is the extremely tactical planning we just described as *emergency response*. Some organizations use it to cover events related to physical security problems. Some organizations define it as being the executive-level plan to address major events at the entity level, but in reality, their plans only address crisis communications issues. For the purposes of this GTAG, we will use the term to describe entity-level planning designed to address the immediate and high-level impacts to an organization.

Most crisis management plans are designed to be activated for any incident, regardless of impact. In many cases, specific thresholds are established in advance across various types of impacts to eliminate the subjectivity often associated with escalating an event. These escalation criteria should include human, financial, and operational impacts and be straightforward enough to allow management-level employees anywhere the organization operates to know whether an escalation to the crisis management team is necessary or not. Similarly, consistent use of the thresholds across the entity helps the crisis management team be confident that if it has not yet been contacted, an event has not exceeded the pre-established thresholds.

Another key advantage of these thresholds is the value they provide in separating a BC event from an entity-level crisis. A small fire or the loss of a key supplier may be a significant impact for one line of business or operating location, but that does not necessarily constitute an entity-level crisis that warrants crisis management team activation. Properly developed thresholds empower business unit (or regional) managers to act on the business resumption issues without wondering whether they will be second-guessed by senior management.

One consistent theme across most companies who operate mature crisis management programs is a well-defined and rehearsed command and control capability. During an actual event, especially a complicated one, chaos abounds. There isn't enough reliable information at management's disposal early in the event to make completely accurate decisions 100 percent of the time. Organizations pursuing excellence in crisis management develop and test a system in advance that can intake available information, filter out the "noise," disseminate information quickly and securely, and maximize decision-making capabilities.

In addition to escalation protocols and command and control of people, processes, and information, other aspects of effective crisis management programs include:

- Incorporating specialty disciplines such as product extortion/recall, security incidents (especially international incidents), and industry-specific (e.g., aviation) emergency incident response to the overall crisis management program. Generally, companies with exposure in these areas will develop some plans to address them, but they may not be linked to the entity-level crisis management program.
- Assisting employees affected by a disaster, which may include providing mental health support, family support, or financial assistance during regional events. Assistance may also include incentives to travel or temporarily relocate in an emergency.
- Incorporating board expectations in an incident response and board reporting during the response.
- Managing shareholder issues and liability following an event, including the errors and omissions and directors and officers liability issues.
- Testing CM and BC jointly so that each program can build on the strengths of the other and the overall effort can mature in a unified way.
- Delineating authorities when some operations are managed as a joint venture and/or exist in multiple countries. Legal liability may be transferred from a joint venture or another country if decisions are made by another legal entity or in a different country. This issue is very important if the CM team is in the United States because of the country's litigious environment.

8. Conclusion/Summary

BCM is an important risk management program designed to protect companies from potential significant consequences related to events that can disrupt critical business processes. The CAE can help the organization understand the risks and the options to create an effective BCM program. Managers throughout the organization must be held accountable for appropriately managing the risks associated with disruption of the business operations and associated functions within their organization.

A BCM program provides the framework for making appropriate risk mitigation decisions and building organization resilience. Critical business processes must be recovered to support the recovery of critical business operations. The BCM program enables an organization to maintain recovery capabilities, including organizational capabilities and knowledge, systems and information recovery, resource restoration and procurement, supplier management, and alignment with emergency management processes.

The BCM program should be designed to maintain and grow the business continuity capabilities continuously. Effective maintenance of the BCM capabilities must include regular training of staff, periodic exercises (including resolution of any identified gaps and management commitment to the program), audit assessments of the BCM program and business unit capabilities, and continual improvement of the BCM program.

9. Appendix

9.1 Sample BCP Audit Guide

The Federal Financial Institutions Examination Council has an excellent Business Continuity Planning Booklet (March 2008). The guide can be found at the council's Web site, www.ffiec.gov. Below are the major objectives discussed within the booklet.

- Determine examination scope and objectives for reviewing the BC planning program.
- Determine the existence of an appropriate enterprise-wide BC plan.
- Determine the quality of BC plan oversight and support provided by the board of directors and senior management.
- Determine whether an adequate BIA and risk assessment have been completed.
- Determine whether appropriate risk management over the BC process is in place.
- Determine whether the BC plan(s) include(s) appropriate testing to ensure the business process(es) will be maintained, resumed, and/or recovered as intended.
- Determine whether the IT environment has a properly documented BC plan that complements the enterprise-wide and other departmental BC plans.
- Determine whether the BC plan(s) include(s) appropriate hardware backup and recovery.
- Determine whether the BC process includes appropriate data and application software backup and recovery.
- Determine whether the BC plan(s) include(s) appropriate preparation to ensure the data center recovery processes will work as intended.
- Determine whether the BC plan(s) include(s) appropriate security procedures.
- Determine whether the BC plan(s) address(es) critical outsourced activities.
- Discuss corrective action and communicate findings.

9.2 BCM Standards and Guidelines

Organization/Governing Body	Standard	Description of Standards
Business Continuity Institute (BCI)		Business Continuity Institute's 10 Competencies
International Standards Organization (ISO)	ISO 9000	Quality Management
	ISO 14001	Environmental Management System
	ISO 25002	Code of Practices for Information Security Management — Business Continuity Management section
British Standards Institute (BSI) includes: • **United Kingdom** • **Australia** • **New Zealand**	AS/NZ 4360	Risk Management — (AS/NZ: Australia / New Zealand Standards)
	HB221	Guide to Business Continuity Management — handbook supplement to 4360
	AS/NZ 4390	Records Management
	AS/NZ 4444	Information Security with Business Continuity Management
Publicly Available Standard (PAS) UK and Commonwealth nations	PAS 56	Guide to BCM — (PAS — UK)

Organization/Governing Body	Standard	Description of Standards
U.S. Office of the Comptroller of the Currency (OCC) Bulletins apply to financial service functions — specifically, to IT issues	Bulletin 97-23	Corporate Business Resumption and Contingency Planning
	Bulletin 2001-14	Resilience
	Bulletin 2003-18	Business Continuity Planning and Supervision of Technology Providers
New York Stock Exchange (NYSE) / Financial Industry Regulatory Authority (FINRA)		Joint Interagency White Paper published by the U.S. Securities and Exchange Commission, Office of the Comptroller of the Currency, and Board of Governors of the Federal Reserve System on Sound BCP Practices http://www.sec.gov/news/press/studies/2006/soundpractices.pdf
American National Standards Institute (ANSI)	ANSI / ARMA 5	Vital Records Program (identification, management, and recovery of business critical records) (2003). ARMA: American Records Management Association
American Society for Industrial Security (ASIS)	ASIS GDL BC 10	Business Continuity Guideline: A practical approach to emergency preparedness, crisis management, and disaster recovery (2004 draft)
U.S. National Institute of Standards and Technology (NIST)	NIST SP 800-34,45	Contingency Planning Guide for IT Systems (2002)
U.S. National Fire Protection Association (NFPA)	NFPA 1600	Standard on Disaster / Emergency Management and Business Continuity Programs (referenced as a standard for BCP)

9.3 BCM Capability Maturity Model

Although the following BCM Capability Maturity Model does not match precisely to this GTAG, it is consistent with both the GTAG and BC industry practices and standards. It is provided solely as an example of one way to evaluate the maturity of a BC program.

Source: Protiviti Inc. (www.protiviti.com). Adapted from the "Capability Maturity Model: Guidelines for Improving the Software Process," Carnegie Mellon University Software Engineering Institute, 1994.

Assessment Objective: Executive Management Support and Sponsorship Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	BCM capabilities are improved continuously and systematically. Senior management utilizes BCM capabilities to drive other efficiencies internally and build strategic relationships externally.	BCM strategies are aligned with strategic objectives and customer expectations. Senior management ensures that BCM planning operates as a core business function, chartered with clear accountability and responsibility.
Managed	Senior management has defined key metrics, in line with regulatory requirements and industry guidelines. These metrics are used to measure the effectiveness and quality of BCM capabilities. Management participates in testing and training activities, and reviews exceptions to internal policy and test results.	Senior management is committed to manage the quality of BCM program execution. Metrics are collected and managed to ensure the quality of BCM strategies and plans. BC-related objectives are noted in performance goals.
Defined	A BCM steering committee is established, and it is led by a member of the non-IT senior management team. The steering committee is the ultimate decision-maker regarding BCM strategies and solutions. A dedicated BCM budget and required resources are allocated to ensure the effectiveness of BCM capabilities, and BCM disciplines are integrated to provide an overall BCM solution for the organization.	Senior management is fully involved in BCM decision-making through a steering committee function. In addition to the BCM policy, the organization has defined specific frameworks to ensure integration of business resumption, CM, and IT disaster recovery capabilities, as well as appropriate maintenance, testing, and training processes.
Repeatable	Senior management supports the BCM program; however, limited involvement in process execution persists. Although coordination of CM, BC, and IT disaster recovery are assigned to middle management, overall coordination of BCM is ad-hoc or missing. Failure events are recognized and corrected after they occur.	Senior management is aware of the need for BCM capabilities. A BCM policy has been created, and BCM efforts are driven based on the results of a BIA (formal or informal).
Initial	Senior management sponsorship of BCM efforts is informal or absent. At this stage, BCM capabilities rely on individual efforts and "heroics," and mostly focus on IT systems backup and restoration, and ER such as building evacuation procedures.	These efforts are led by middle management and executed without proper funding and sufficient resources. Consequently, any existing continuity capabilities are defined as tactical measures.

Assessment Objective: Risk Assessment and Business Impact Analysis (BIA) Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	The results of the risk assessment and BIA drive continued enhancement to recovery strategies. The execution and review of risk assessments and BIAs are coordinated with organizational and technology change management/due diligence processes.	Senior management performs as a steering committee to identify and approve risk and impact conclusions. The steering committee recommends changes to the risk assessment and BIA process, based on the needs and requirements of the business itself.
Managed	Senior management supports the formal approach to the risk assessment and BIA. The establishment of objectives and effectiveness are measurable. Both recovery time objectives (RTO) and recovery point (data loss tolerance) objectives (RPO) are established, as is the capacity/capability at the RTO. The risk assessment process takes into account controls assessment. These processes are repeatable and are executed on a regularly scheduled basis.	The results of the risk assessments and BIAs drive the definition and development of recovery strategies and solutions. Core business processes and IT applications/systems have been addressed and are reviewed during the regularly scheduled risk assessment and BIA updates. Senior management uses these results to measure and manage enterprise-wide risk.
Defined	A more formal approach has been implemented regarding assessing risk and business impact. Management has identified an approach to define levels of criticality, supporting a methodology to collect/estimate business impact data. Recovery time objectives have been defined, and strategies have been selected to meet these requirements. Management reviews and approves risk assessment and BIA results.	As part of a formal BC strategy selection and implementation process, a defined risk assessment, or BIA approach, is established. The strategy selection process also includes recovery objectives tied directly to levels of criticality and impacts to the organization. Executive management formally drives and approves these analyses.
Repeatable	Management has informally developed risk assessment conclusions and recovery priorities, typically as a result of discussions and facilitated sessions, as opposed to formal analysis. Priorities are normally focused on the component level. Management may be unable to fully justify recovery strategy funding, given that business impact information (financial or nonfinancial) remains incomplete.	Business and/or IT management have discussed and summarized continuity/availability risks or perceived impacts associated with business interruptions. Preliminary/high-level recovery objectives are agreed upon; however a process to measure the effectiveness and reasonableness of these objectives is absent.
Initial	Neither a formal nor informal risk assessment or BIA has been performed. Business and IT management may have developed recovery priorities, but these conclusions are potentially limited to perceived levels of importance (focus on their isolated knowledge of the business). The organization has not estimated the impacts (financial or nonfinancial) associated with business interruptions.	Business and/or IT management developed "ad hoc" recovery priorities based on perceived levels of importance. Failure scenarios and controls assessments remain incomplete. Measurement criteria have not been established.

Assessment Objective: Business Continuity Strategy and Design Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	BC strategies are reviewed as part of strategic decision-making and organizational/technology change management. Strategies are refreshed on an as-needed basis.	Senior executive strategy sessions and/or change management committees drive the design, selection, funding, and implementation of BC strategies.
Managed	The results of the risk assessment and BIA drive the selection of BC strategies. A multi-disciplined steering committee evaluates CM, business resumption, and IT disaster recovery options in light of a cost-benefit analysis. BC strategies are reviewed on a periodic basis, typically every 12 months (following a risk assessment and/or BIA refresh).	A BC steering committee drives the selection of the BC strategies based on a cost-benefit analysis. This multi-functional team evaluates and selects complementary business and IT solutions.
Defined	Point solutions or discipline-specific strategies are designed and implemented based on management direction. The organization has not taken advantage of the benefits associated with organization-wide strategy selection that integrates CM, business resumption, and IT disaster recovery. The organization continues to move closer to implementing strategies that meet established recovery objectives.	The information technology organization (ITO) retains decision-making regarding IT disaster recovery strategies. CM and business resumption strategy design and selection is addressed separately, driven by risk management, security, internal audit, or even the ITO. Coordination between the business and ITO is often overlooked.
Repeatable	Cost control is the primary driver of BC strategy selection. Strategies normally rely on cold site arrangements (internal or third party) and vendor drop-shipped resources. The organization remains at risk given the probability that BC strategies may fail to meet more aggressive business objectives.	The organization does not allocate budget for BC strategy implementation and maintenance. Instead, the perceived minimum is implemented, and if funding is needed, these issues are treated as budget exceptions.
Initial	BC plans lack recovery strategy and resource definitions due to poorly defined BC program ownership or accountability. The organization places a heavy reliance on vendor support following the crisis or business interruption.	Management relies on ad hoc actions or untested response and recovery strategies. The design of response and recovery strategies is not preplanned; instead, management expects that experiences, creativity, and ingenuity will prevail when faced with a crisis situation.

Assessment Objective: Business Alignment Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	BCM is present during change management review sessions, as well as during business strategy sessions, in order to keep the organization abreast of all the changes that may have an effect on existing response and recovery strategies. The BCM steering committee meets quarterly to assess the reasonableness of existing and proposed strategies as well as spending when compared to the rest of the industry.	BCM takes advantage of more advanced business strategy and change management processes in use throughout the organization.
Managed	A BCM steering committee takes into account customer requirements and/or formal service level agreements when evaluating BIA results and BC strategy investment. Internal auditing is involved in the BCM effort as an advisor, and reviews the program in light of the internal policy and regulatory requirements (if applicable). When the organization tests its BC strategies, the business/IT solutions are jointly tested.	BCM is viewed as a key control, and internal auditing drives compliance with the existing documented policy. All aspects of the BCM lifecycle are implemented in a joint business/IT manner. BCM is used as a competitive advantage within other business initiatives.
Defined	The organization has integrated the three BCM disciplines, and a single BCM steering committee makes decisions regarding strategies and solutions. A BCM budget has been developed. A BIA and formal cost-benefit analysis drive decision-making. Internal and third-party response and recovery strategies are formally evaluated, with selections based on results from the risk assessment.	Accountability for the BCM program is moved outside of the data center. An executive with the ability to influence the entire organization sponsors the effort. BCM objectives appear on the annual performance objectives of business unit management.
Repeatable	The organization developed a formal BCM policy to drive design, implementation, and execution of BC. Although coordination among CM, business resumption, and IT disaster recovery processes is immature or absent, they exist and are positioned to assist in response and recovery operations. A BIA drives the design of BCM strategies.	Although the scope of the planning effort has expanded to include the business, ownership and accountability remains within IT, or internal auditing emerges as the driver of the BCM effort. The BIA is the primary tool used to design BCM strategies.
Initial	The organization's BC program addresses ER and/or IT disaster recovery, but fails to address strategic CM and/or business process recovery.	BC solutions, which may be limited to tactical ER and system restorations, is led at a middle management level and executed with existing excess funding (or available internal resources).

Assessment Objective: Plan Development and Strategy Implementation Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	Crisis, disaster recovery, and business resumption plans are integrated in planning and execution. Team membership is cross-functional and cross-regional. Expectations are clearly understood by all stakeholders. Plan maintenance is tightly integrated with organizational change management processes.	Senior executive strategy sessions drive the planning priorities and alignment. Standardized training and awareness programs featuring BCM content are delivered to all planning participants. Plan development responsibilities rest with those closest to the issues, and plans are vetted for content and alignment. Expert independent review is scheduled and drives both tactical and strategic change.
Managed	Coordination among CM, business resumption, and IT disaster recovery plans and teams is well defined. Plans are maintained on an as-needed basis, as opposed to a minimal standard (e.g. annually). Plan documentation is reviewed by a central authority, or signed off by senior management. Testing results and day-to-day experiences drive plan improvement. Documentation is appropriately secured and disseminated on an as-needed basis.	A combination of centralized and decentralized planning efforts exists, with all personnel trained regarding their plan documentation roles and responsibilities. Plan updates are driven by organizational and technology change, as well as test/exercise results.
Defined	CM (including ER and crisis communications), business resumption, and IT disaster recovery plans are documented and include organizational detail. All plans are updated annually. Although roles and responsibilities are clear, coordination among the plans is poorly defined.	Each plan is assigned an owner who is responsible for its development and maintenance (using an organization template standard as a starting point). The appropriate parties drive content of the plans, and quality control remains with the plan owner. Scheduled maintenance drives plan updates. Internal auditing is seen as a BC planning partner and is part of the continuous improvement process.
Repeatable	The focus of the planning effort is IT disaster recovery documentation and ER planning (building evacuation, first aid, etc.). Some CM documentation exists, but its focus is on IT incident response. The primary reason for plan documentation is to avoid audit comments. Plans are often updated in an ad hoc manner.	Plan documentation is driven by internal or third-party audit findings. The technology leadership team is leading the plan documentation effort; therefore little exists outside of IT.
Initial	Where plans exist, they are developed in silos, lacking detailed business and technology procedural details. BCM stakeholders do not know their roles and responsibilities or, in some cases, even their involvement in response and recovery execution. Plans are often out of date. Response and recovery relies on memory, and execution is often ad hoc and led by a few key employees.	Produced by a lack of understanding and focus on BCM. Plans often start with publicly available or software-based templates, and little is done to customize the content. Plans often focus on ER and the theory of recovery planning.

Assessment Objective: Training and Awareness Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	A deep understanding of the BCM program and its impact on daily operations is understood by all layers of the organization. Those responsible for performing BCM tasks are active in training others. BCM strategies are evaluated in terms of their impact to enterprise value. BCM training is included in performance evaluations (e.g., balanced scorecard).	Team members are specifically trained on how to be a BCM proponent. BCM leadership carefully coordinates BCM objectives with high-profile business objectives to exploit their publicity. Team members who have been cross-trained are provided opportunities to exercise outside their normal responsibilities.
Managed	Management has a broad understanding of how BCM elements work together. Employees know their immediate responsibilities in an actual event, and many know their long-term activities. Team members can articulate their individual responsibilities, as well as how their element interfaces with other BCM elements and the company's business objectives as a whole. BCM issues are considered in all business initiatives.	All team members are trained on their tasks as well as the broader program. BCM leadership provides program updates to senior management on a regular basis. Training and awareness programs are budgeted separately, including outside resources if necessary. Team members participate in third-party or case study training. Training includes issues surrounding how to execute the plan in the midst of an event that extends beyond the company.
Defined	A structured program to communicate BCM program goals and objectives is developed with all elements participating. Employees beyond the planning and execution teams understand the program goals and objectives. A general awareness of the multi-faceted approach to BCM exists within management.	A structured approach to BCM training exists, with management in each line of business understanding the program. Task-related training is mandatory for those throughout the organization who are listed as primary or backup team members. Existing resources, such as the company intranet or new-hire orientation are used to promote general awareness of the program.
Repeatable	Some limited training or awareness is present within a program element, but no cross-training among crisis, business resumption, and disaster recovery exists. Specific program components may have designated backups, and team members are included in casual communication regarding the program.	Middle management with tactical responsibility for program elements understands the danger of relying on one person to perform a critical BCM task. BCM tests and/or updates are a period topic in department staff meetings. Formal training on specific tasks is provided for those required to do them, but nothing else. Training is limited to participation in exercises.
Initial	No formal training or awareness program exists. Only those with immediate responsibility know program goals and objectives. No cross-training among crisis, business resumption, and disaster recovery is present. Regulatory issues drive the training and awareness efforts.	Produced by a combination of planning silos. Is present where extraordinary individual efforts are the foundation for BCM. Training, where present, is limited to ER activities.

PROCESS MATURITY

Assessment Objective: Testing and Plan Maintenance Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	BC testing is unannounced. Simulations are developed using probable risks that were identified in a risk assessment. Tests are primarily measured by an expected recovery. Entire departments work at an alternate site for a defined period of time using backup systems and resources. Third-party business partners and vendors participate in testing. Updates to the plan are automatically integrated through a maintenance process.	Team members become thoroughly trained, and their response is merely a reaction. Minimal planning is performed in preparation for tests, and the planning that is performed is done secretly by a few individuals. Response and recovery team members have minimal reliance on plan documentation aside from some technical procedures or contact lists that are up-to-date. Automated tools are employed to maintain plans and keep them current and reflective of the business operations.
Managed	Full BC testing, for business and IT, are regularly performed. Simulations are developed using probable risks that were identified in a risk assessment. Tests are measured by the rate of recovery of critical components or functions such as connectivity, application usage, or transaction processing. Plans are maintained off site and updates are made at the conclusion of testing. Internal auditing observes the exercise and ensures plans are updated.	Test planning encompasses CM, business resumption, and IT disaster recovery. Team members are cross-trained on all relevant procedures. There is little reliance on plan documentation, although procedural and contact list inaccuracies should be addressed in a timely manner. Internal auditing monitors test planning, execution, and action items resulting from the test. Plan updates should be the responsibility of the process owners, with oversight from internal auditing.
Defined	BC and IT disaster recovery tests are sometimes performed together, but the focus is typically on component recovery. Continuity procedures are discussed using facilitated sessions to identify planning gaps. Tests are primarily measured using an expected timeframe for recovery and overall effectiveness. Entire departments work at an alternate site for a defined period of time, using backup systems. Lessons learned are documented, and plan updates are made on a scheduled basis.	Business and IT personnel conduct regularly scheduled BC tests, designed to address business process and IT asset recovery. Users test connectivity and access to applications. The planning process for these tests is extensive and involves internal and external personnel as facilitators and/or monitors. Internal auditing participates in testing exercises and monitors the process for updating plans based on test results. Plan updates are the responsibility of the process owner, with central coordination.
Repeatable	Testing is focused on IT disaster recovery and may involve end user validation of the recovered environment and/or the test results. In some organizations, management engages in scenario-drive, tabletop exercises of its CM capabilities. IT disaster recovery tests are focused on component recovery. Internal auditing reviews continuity procedures, if this function exists. Plan updates are made on a scheduled basis.	IT personnel conduct regularly scheduled IT disaster recovery and component recovery tests. The planning process for these tests is extensive and should involve internal and external personnel as facilitators and/or monitors. Internal auditing participates in testing exercises and monitors the process for updating plans based on test results. One individual is responsible for plan updates.
Initial	IT component testing takes place internally within the IT department, with limited knowledge of management and no participation from the user community. A formal testing schedule is not established, and test results are rarely documented. Testing does not result in amendments or improvements to response/recovery procedural documentation. Plans may not be well maintained or up-to-date because the BCM process is new.	BC planning successes, normally limited to IT, are present where extraordinary individual efforts are the foundation. Training, where present, is limited to ER (first aid, evacuation, etc.) and IT component recovery activities. Plan updates are the responsibility of the process owners and do not follow a standard, monitored process.

Assessment Objective: Compliance Monitoring & Auditing Maturity Evaluation		
	Characteristics of Capability	**Method of Achievement**
Optimizing	Internal auditing, risk management, and the general counsel all review plan documentation on a regular basis and also sponsor third-party audits of BCM capabilities, including testing activities. The organization engages in industry discussions regarding regulatory compliance and regularly reviews benchmarking analyses. A risk assessment and BIA are performed and regularly refreshed to ensure that plans reflect business reality and the regulatory environment.	Proactive contact is maintained with regulatory bodies. A dedicated team leads BCM activities supported by a cross-functional business and technology team, which includes internal auditing and outsource providers for specialized services. A risk assessment (by location) and BIA (by process) should be conducted and used as the foundation for building plans. They should also be refreshed periodically.
Managed	Cross-functional teams, including the general counsel and internal auditing perform regular assessments of business conditions and regulatory requirements. Internal auditing, risk management, and the general counsel also review plan documentation, in some capacity, on an annual basis. A risk assessment and BIA are used to ensure that plans reflect business reality and focus on the most likely and severe risks and impacts.	A dedicated team leads BCM activities supported by a cross-functional business and technology team, which includes internal auditing and outsource providers for specialized services. A risk assessment (by location) and BIA (by process) should be conducted and used as the foundation for building plans. They should also be refreshed periodically. Internal auditing focuses on BCM program execution as opposed to plan content.
Defined	Regulations related to BCM are considered and incorporated into BCM plans. The responsibility to monitor the regulatory landscape resides with the general counsel, who communicates with the BCM steering committee. Internal auditing monitors the plan maintenance process and influences when regulatory changes warrant updates to the documentation. A risk assessment and BIA that consider the regulatory environment have been performed within the past two years.	A small, cross-functional team is in place, and the internal audit function is actively involved in the actions of this team. A risk assessment (by location) and BIA (by process) is conducted and used as the foundation for building plans and identifying the impact of regulation on plan development.
Repeatable	Regulations related to BCM are considered and incorporated into BCM plans when financially practical. Internal auditing reviews the relevance of the documentation in accordance with a long-term audit plan and may request evidence of plan testing.	Internal auditing, risk management, or general counsel shares regulatory updates with the BCM team or those responsible for BCM.
Initial	Regulatory requirements or industry standards related to BCM are seldom considered and incorporated into BCM plans, or are viewed as too costly to implement. Internal auditing's attention does not extend beyond ensuring traditional IT disaster recovery plans are documented.	An IT disaster recovery planning process exists. An internal audit function is in place, and disaster recovery is in the annual or bi-annual audit plan.

10. Glossary

BC — business continuity

BCM — business continuity management

BCP — business continuity plan

BIA — business impact analysis

BU — business unit

CAE — chief audit executive

CBCP — Certified Business Continuity Professional

CM — crisis management

DRII — DRI International

DRP — disaster recovery planning

ER — emergency response

GTAG — Global Technology Audit Guide

IT — information technology

MBCP — Master Business Continuity Professional

RPO — recovery point objective

RTO — recovery time objective

11. About the Authors

David Everest, CISA

David Everest is a vice president of Technology Risk Review for Key Bank in Cleveland, Ohio. Everest concentrates on providing inside consulting expertise to the technology division within Key Bank. His specialties include infrastructure and networking projects. Prior to joining Key, he was a technology auditor with General Motors in Detroit, MI. Everest has an extensive IT background, both technical and strategic, and has worked in data centers and managed IT departments.

Everest has a BS in Computer Information Systems from Baldwin Wallace College in Berea, Ohio and an MBA from The Weatherhead School of Management at Case Western Reserve University in Cleveland.

Roy E. Garber, CIA, CISA

Roy Garber is the director of Application Development at Safe Auto Insurance Co. and is responsible for the project management office (PMO) and delivery of enterprise IT application solutions. His current responsibilities also include the implementation of IT governance principles and best practices.

Garber has more than 20 years of IT, financial, and operational risk management experience. In his prior internal audit role, he was a corporate officer responsible for providing leadership over corporate IT audit services for an international insurance company. In his prior external audit role, Garber managed IT assurance services engagements in large, medium, and small companies and partnered with client executives to help them meet their IT risk management needs.

Michael Keating

Mike Keating leads the business continuity management practice for Navigant Consulting. Prior to joining Navigant Consulting, he held various leadership positions in the crisis management and business continuity consulting arena, including nearly four years as the Midwest Practice leader for the world's largest insurance broker and four years as the Southeast BCM Practice leader for a prominent internal audit and consulting firm. Keating also developed the American Red Cross BICEPP program, the first program of its kind to help organizations prepare for disasters.

His specialty is in enterprise-wide business continuity programs, and he has assisted clients of nearly every size and industry prepare to minimize the impact of business interruptions.

Brian Peterson

Brian Peterson is the team leader of the Global Information Risk Management Consultant Team at Chevron Corp. and is responsible for the delivery of consulting services to Chevron companies throughout the world. His current responsibilities include managing consultants in four countries who perform risk management consulting. Peterson has more than 25 years of IT, project management, and risk management experience. He has worked in 55 countries assisting Chevron business units with various risk management initiatives. Peterson developed several tools and processes that are used throughout Chevron to manage information risks.

Peterson helped establish the LOGIIC (Link the Oil and Gas Industry to Improve Cyber-security) consortium that is a partnership between government and industry and currently acts as the project manager.

Reviewers

The IIA thanks the following individuals and organizations who provided valuable comments and added great value to this guide:

- Professional Practices Committee:
  - Advanced Technology Committee
  - Board of Regents
  - Committee on Quality
  - Internal Auditing Standards Board
  - Professional Issues Committee
  - Ethics Committee
- Lily Bi, The IIA
- Larry Brown, The Options Clearing Corp., USA
- Faisal R. Danka, London, UK
- Christopher Fox, ASA, Delta, New York, USA
- Nelson Gibbs, Deloitte & Touche, LLP, USA
- Markus Künzel, Medizinische Universität Wien, Austria
- Lemuel Longwe, Ernst & Young Chartered Accountants, Zimbabwe
- Steve Mar, Resources Global, USA
- Tom Margosian, Ford Motor Co., USA
- James Reinhard, Simon Property Group Inc., USA

PROTIVITI

A LEADER IN

INDEPENDENT RISK CONSULTING

Protiviti is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC. Protiviti's highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues. Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

To learn more about our services or to download complimentary copies of our publications, please visit protiviti.com.

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.®

RISK

AND WHY KNOWING WHERE IT IS IN YOUR BUSINESS PROCESS IS THE KEY TO

A GOOD NIGHT'S SLEEP

Many executives spend sleepless nights wondering when and if their critical systems and business processes will falter. This is not surprising, considering that today's organizations require multiple suppliers, technologies, processes and people to work in concert to deliver the continuous service customers expect. To address this challenge, organizations around the world and across industries are turning to Protiviti. At Protiviti, we take a pragmatic approach to business continuity planning and evaluate the risks inherent in all the interdependent processes and players of your operations. We then work with you to engineer practical solutions and processes for managing the incidents that can undermine your financial performance and reputation. This gives you an advantage over competitors who try to manage interruptions due to human mistakes, errant software and unreliable suppliers through point solutions and process manuals. It also means while they're up worrying, you'll be sleeping like a baby.

To learn more about Protiviti's capabilities and download a complimentary copy of our Guide to Business Continuity Management 2nd edition, *visit protiviti.com/bcm.*

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.®

GTAG

Business Continuity Management

This GTAG focuses on how business continuity management (BCM) is designed to enable business leaders to manage the level of risk the organization could potentially encounter if a natural or man-made disruptive event that affects the extended operability of the organization were to occur. The guide includes disaster recovery planning for continuity of critical information technology infrastructure and business application systems.

Chief audit executives (CAEs) have been challenged to educate corporate executives on the risks, controls, costs, and benefits of adopting a BCM program. Although it is true that recent disasters around the world have motivated some corporate leaders to give attention to BCM programs, the implementation of such programs is far from universal. The key challenge is engaging corporate executives to make BCM a priority. Although most executives are likely to agree that BCM is a good idea, many will struggle to find the budget necessary to fund the program as well as an executive sponsor that has the time to ensure its success. *Business Continuity Management* will help the CAE communicate business continuity risk awareness and support management in its development and maintenance of a BCM program.

Visit www.theiia.org/guidance/technology/gtag/gtag10 to rate this GTAG or submit your comments.

Order Number: 1045
IIA Member US $25
Nonmember US $30
IIA Event US $22.50

The Institute of Internal Auditors
www.theiia.org

ISBN 978-0-89413-623-8
53000
9 780894 136238