CGMA TOOL

Business Continuity Management – Key Strategies and Processes

CGMA
Chartered Global Management Accountant

Powered by AICPA | CIMA

Two of the world's most prestigious accounting bodies, AICPA and CIMA, have formed a joint venture to establish the Chartered Global Management Accountant (CGMA®) designation to elevate and build recognition of the profession of management accounting. This international designation recognises the most talented and committed management accountants with the discipline and skill to drive strong business performance. CGMA® designation holders are either CPAs with qualifying management accounting experience or associate or fellow members of the Chartered Institute of Management Accountants.

CONTENTS

INTRODUCTION

Organisations around the world have been the victims of all sorts of disruptions. Over the years, man-made and natural disasters have unveiled the vulnerability of businesses on a global scale.

These unannounced and disruptive incidents usually carry a hefty price tags as property, lives and reputations are often damaged beyond repair and compensation. Incidents such as oil spills and fires, chemical plant explosions, epidemics, pollution, extreme weather events, plane crash, synchronised terrorist attacks, cyber-attacks and data breaches – to name a few – served as powerful wakeup calls for preparing organisations to respond to unexpected disasters.

With technological advances, progressing globalisation and the extension of the supply chain, the impacts of disasters on organisations have greatly increased and intensified. Businesses of all sizes are connected to their suppliers and customers to a much greater degree today than ever before. When a disaster happens, the repercussions escalate throughout the entire the supply chain.

As a result, management teams and corporate boards face much more pressure to make their organisations more resilient when disasters strike. **Business continuity management (BCM)** capabilities enable organisations to restore their businesses to normal operations following an unanticipated disaster or business interruption. To date, however, the corporate BCM capabilities necessary to establish that resiliency generally have ranged from absent to insufficient.

The purpose of this tool is to help provide finance and accounting managers with a foundation on which to further develop their BCM thinking, strategy and processes. The specific objectives are as follows:

- To define BCM as a corporate capability and to identify its essential components and processes;
- To identify the drivers that make BCM a vital corporate and management competency in the 21st Century;
- To establish and define the roles and responsibilities that corporate managers and boards fulfill in developing effective BCM practices; and
- To present a step-by-step framework for developing and maintaining effective business continuity management processes.

DEFINITION AND SCOPE OF BUSINESS CONTINUITY MANAGEMENT (BCM)

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

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

The U.K.-based Business Continuity Institute (BCI) defines BCM as "a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. (Source: ISO 22301:2012)".[1]

Business continuity planning is the process through which organisations establish the capabilities necessary to protect their assets and continue key business processes after a disaster occurs.

The BCI BCM Lifecycle model[2] includes six key categories which are also referred to as Professional Practices. The model details the various stages of activities that businesses need to go through to improve organisational resilience. These activities will be further addressed and detailed in the tool.

- Policy and Programme Management
- Embedding Business Continuity
- Analysis
- Design
- Implementation
- Validation

Although the discipline still has a long way to go, organisational business continuity management has evolved significantly over the past two decades. In the past, "disaster recovery" was usually centered in data processing or information technology (IT) departments. These early efforts primarily focused on getting hardware, software and data up and running again after a disruption.

Over the years, it is recognised that business continuity planning efforts require a cross organisational perspective and therefore should not be limited to the IT department. That said, many effective continuity tactics have emerged from disaster recovery efforts that arose in the IT function. For example, many of the same principles that apply to data and systems backup also apply to facilities management and backup.

Disaster recovery has expanded into "business continuity planning" – a phrase that was primarily used to emphasise the need to move continuity efforts beyond the IT department and weave them throughout the organisation. Most recently, the use of terms like "business continuity management" and "business resiliency" have increased, emphasising the proactive nature of current continuity efforts. In fact, BCI had recently released a position statement to enhance understanding on "the position of business continuity in the context of organisational resilience."[3]

Definition of Key Terms

Business Continuity Management (BCM):

A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats—if realised—might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

Business Continuity Plan (BCP):

A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical products and services at an acceptable predefined level.

Business Impact Analysis:

The process of analysing business functions and the effect that a business disruption might have upon them.

Crisis:

An abnormal situation which threatens the operations, staff, customers or reputation of an enterprise.

Crisis Management Team:

A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.

Disaster:

A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.

Disaster Recovery Planning (DRP):

The strategies and activities associated with the continuing availability and restoration of organisational operations.

Maximum Tolerable Outage (MTO) or Maximum Acceptable Outage (MAO):

The duration after which an organisation's viability will be threatened if service cannot be resumed.

Recovery Point Objective (RPO):

The target set for the status and availability of data or capacity at the start of a recovery process. It is a point in time at which data or capacity of a process is in a known, valid state and can safely be restored from.

Additional definitions can be found at www.thebci.org/glossary.pdf

DRIVERS OF BUSINESS CONTINUITY MANAGEMENT

BCM and Organisational Risk Management

Business continuity management (BCM) and enterprise risk management (ERM) are clearly connected although they have emerged from different disciplines, resulting in the two functions often being undertaken by different teams, using different processes and terminology.

In very broad terms, the key difference between BCM and ERM is that the former will focus first on identifying and prioritising the critical processes and resources that are fundamental to keeping the organisation operational. The key objective is to restore the business to normal operations after an event or disaster occurs as efficiently and effectively as possible.

In contrast, ERM will typically start from the organisation's overall objectives and seek to identify all the potential threats and opportunities that could affect the achievement of these objectives so that appropriate controls and responses can be put in place to address these uncertainties. From this perspective, BCM can be regarded as one of the controls to be implemented when a risk materialises.

However, what both share in common is a growth in scope and development over recent decades and it makes sense for organisations to take an integrated approach to BCM and ERM as much as possible to avoid overlaps and inefficiencies.

Six Key Drivers of Business Continuity Management

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

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

Driver 1: A Rise in Business Interruptions

The number of natural and man-made business interruptions has escalated within the decade. Recent CGMA research revealed that over 60% of respondents from all over the world indicated that the volume and complexity of risks had increased 'mostly' or 'extensively' over the last five years and in addition, for 38% of respondents, their organisations had faced a significant operational surprise in the past five years, suggesting that the increasing volume and complexities of risks are impacting their ability to operate.[4]

Driver 2: The Growing Impact of Business Interruptions

Most organisations now operate in a more connected business climate. Numerous organisations of all sizes are virtually tethered to a growing number of customers, suppliers and distributors through an extended web of technology systems and processes. That connectivity exacerbates the negative impact of a prolonged business interruption. Even "normal" disasters, such as hurricanes, power outages and earthquakes, now inflict abnormal consequences due to the ever-increasing interconnectedness of the global economy. Those consequences are virtually guaranteed to continue. The 2011 Japanese Fukushima Daiichi nuclear disaster is an example of the ripple effect an incident of such magnitude would have on the country's environment, economy and infrastructure – not counting the unknown health effects.

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

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

Driver 4: New Rules and Regulations

The growing number of new industry guidelines, organisational rules and government regulations on business continuity management represents, in most cases, a positive development.

In 2012, the International Organisation for Standardisation (ISO) released ISO 22301:2012, *Societal security – Business continuity management systems – Requirements.*[5] ISO 22301 "provides a framework to plan, establish, implement, operate, monitor, review, maintain and continually improve a business continuity management system (BCMS). It is expected to help organisations protect against, prepare for, respond to, and recover when disruptive incidents arise".[6]

In 2010 the U.S. Securities and Exchange Commission (SEC) adopted *Rule 4370. Business Continuity Plans and Emergency Contact Information* by the Financial Industry Regulatory Authority (FINRA).[7]

There are many other regulations and industry guidelines related to BCM. Refer to the Business Continuity Institute (BCI)[8] and Disaster Recovery Journal (DRJ)[9] for additional and updated practices.

Driver 5: Business Benefits

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

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

Driver 6: Existing BCM Capabilities Are Insufficient

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

The magnitude of the risk attached to insufficient BCM capabilities will grow significantly in coming years because disasters will inflict farther-reaching damage as organisations' reliance on technology and an increasingly global population of vendors and suppliers continues its onward march.

ROLES AND RESPONSIBILITIES CHECKLISTS

A sound BCM strategy demands broad involvement of the board of directors, senior executive team, the corporate finance and accounting function, and other corporate functions and business units. Below are the roles and responsibilities for the following corporate functions:

Board of Directors	YES	NO	N/A
Understand and actively communicate the value of BCM and the risks of insufficient BCM capabilities			
Request to review the organisation's business continuity plan at least once a year			
Request updates (at least annually) from senior executives on the emergence of new BCM-related rules and regulations			
Approve of the strategic objectives of the organisation's BCM strategy			
Direct its audit committee to determine if external auditors require annual or quarterly reviews of BCM-related documentation and processes			
Offer advice with regard to how investors should be kept informed in the event of a disaster			

Senior Executive Team	YES	NO	N/A
Have a sound working knowledge of BCM practices and the risks to the business of insufficient BCM capabilities			
Keep the board informed (annually, at least) of the organisation's BCM strategy and any significant changes to business continuity plans			
Take responsibility for setting their organisation's business continuity management objectives			
Review and approve (initially and then annually) the critical processes identified in BCM planning exercises			
Review and approve (initially and then annually) the business impact analyses			
Review and approve (initially and then annually) the continuity response strategies developed and maintained by corporate functions and business units			
Support and communicate the importance of BCM test exercises			
Integrate BCM responsibilities into performance management process for executives and managers with key BCM responsibilities			

Corporate Finance and Accounting Function	YES	NO	N/A
Guide the organisation's critical process identification and (subsequent) business impact analysis efforts to help the rest of the organisation understand how to assess the value of various business processes			
Help the senior executive team, other functional executives and, in some cases, the board understand the tradeoffs between cost and recovery time objectives related to specific continuity response approaches			
When possible, enhance business impact analyses with risk analyses to help prioritise the likelihood of various business processes suffering downtime during disasters			
Provide additional analyses of how the timing of disasters can intensify or lessen their impact on certain processes (e.g., a hurricane that closes down an oil refinery that is being restarted following a maintenance shutdown, reducing output for longer than expected; or a lengthy power outage that delays financial reporting processes near the close of a publicly listed company's fourth quarter will likely have more serious consequences to the organisation's share prices (and value) than an outage that occurs several weeks away from a quarterly close)			
Glean what BCM-related documentation and processes external auditors want to review			

Other Corporate Functions and Business Units	YES	NO	N/A
Have a sound working knowledge of BCM practices and the risks to the business of insufficient BCM capabilities			
Participate in critical process identification			
Participate in business impact analyses of critical business processes within their areas of responsibility			
Help establish continuity response strategies within their areas of responsibility			
Integrate BCM responsibilities into performance management process for executives and managers with key BCM responsibilities			
Work with corporate finance to better understand the costs and recovery tradeoffs of their response strategies			
Support and communicate the importance of BCM test exercises			
Monitor and test the response strategies within their areas of responsibility			
Review and approve (annually) the continuity response strategies developed and maintained within their areas (based in part on the results and findings of test exercises)			

Who Owns BCM?

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

Additional Contributions from Finance

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

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

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

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

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

- The creation of an internal controls culture;
- The establishment of business-unit ownership of internal controls; and
- The integration of internal controls considerations into IT system upgrades, mergers and acquisitions, corporate reorganisations and other major changes. Replace the phrase "internal controls" with "business continuity," and the exact same approaches ring true for effective business continuity management.

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

STEP-BY-STEP FRAMEWORK FOR DEVELOPING EFFECTIVE BUSINESS CONTINUITY MANAGEMENT CAPABILITIES

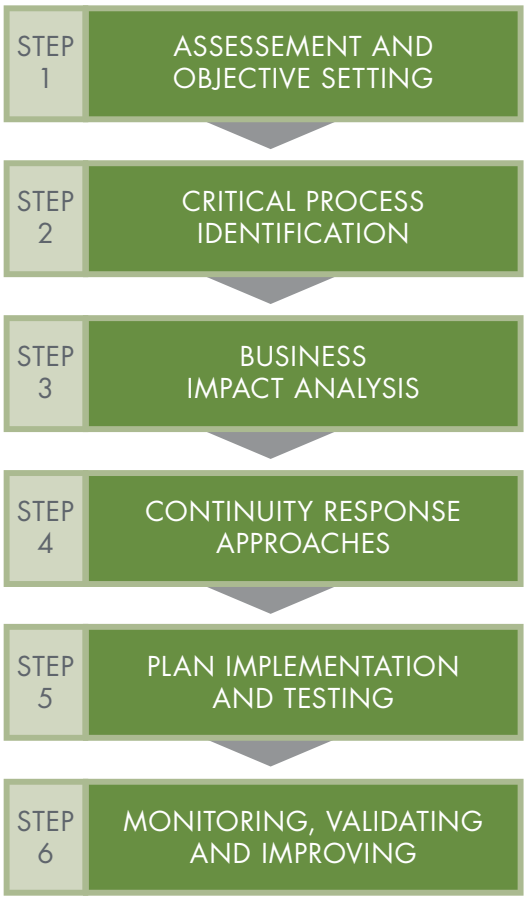
There is good news for corporate managers facing the challenge of developing business continuity management capabilities.

First, information about disaster recovery, business continuity planning and crisis management processes is readily available. The high cost of ineffective business continuity management has spurred academics, consultants and other experts in the field to share information much more freely than is usually the case in other disciplines.

Second, the fundamentals of a sound BCM strategy are relatively simple to grasp. Professional disaster recovery and business continuity managers and consultants frequently make the point that most elements of their work "are not rocket science." A key competency is a painstaking attention to detail combined with a methodical, systematic approach. The toughest part of a business continuity manager's role is overcoming organisational resistance to fund and participate in business continuity planning activities.

Developing BCM capabilities requires the following steps. Each of these steps contains sub-steps, as outlined on the right.

FIGURE 1: The steps to developing BCM capabilities



STEP 1: INITIAL ASSESSMENT AND OBJECTIVE SETTING

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

STEP 2: CRITICAL PROCESS IDENTIFICATION

- After reviewing the organisation's strategic plan, identify the organisation's most critical business functions;
- Identify the business objectives executed by those functions and the processes through which the objectives are executed;
- Process owners should identify key measures, components and external requirements of the process, such as:
  - Performance metrics (how the success of the process is measured and/or quantified with specific measures),
  - Contracts with external parties,
  - Regulatory and/or legal requirements (such as SEC reporting requirements, supplier contracts, accounts payable terms, payment schedules with creditors, etc.);
- Pinpoint the key resources and tools that enable the process to be executed, such as:
  - People and skills,
  - Equipment (including IT infrastructure, telecommunications, manufacturing systems, transportation vehicles),
  - Facilities (warehouses, factories, office space),
  - Software, and
  - Information, which includes electronic data and hard-copy documents.

STEP 3: BUSINESS IMPACT ANALYSIS

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

STEP 4: CONTINUITY RESPONSE APPROACHES

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

Preparation

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

Human Resources

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

Facilities

- Using the business impact analysis, identify the costs and benefits of owning or leasing alternative facilities (production facilities, warehouses, office space for employees);
- Test company-owned backup facilities at least once a year to ensure that they function as intended;
- Work reviews of the following systems into BCM testing: water-detection systems that provide early warning of leaks; systems that detect gases, smoke and other indicators of fire or potential fire; airborne-contamination detection systems; fire-suppression systems; backup power capabilities; and physical building security;
- Assess how long and to what extent backup facilities can host and help sustain critical business processes; and
- Review agreements with providers of backup facilities at least once a year to ensure that capacity continues to meet the company's needs.

IT Systems and Data

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

Suppliers and Customers

- Create and distribute contingency planning questionnaires to key suppliers to raise awareness and to gauge their BCM capabilities;
- Encourage key suppliers to relay questionnaires to their key customers;
- Identify alternate suppliers in the event a disaster prevents one or more suppliers from operating beyond a maximum tolerable outage;

- Consult with key customers and then create a contingency planning questionnaires that establishes each customer's state of awareness and BCM capabilities. Encourage both key customers to do the same with their key suppliers and customers;
- Assist key suppliers and key customers by sharing knowledge of organising for the planning and development of BCM capabilities; and
- Identify emergent alternate sources of supply.

Crisis Management

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

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

A crisis management plan should:

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

STEP 5: PLAN IMPLEMENTATION AND TESTING

Testing the plan is crucial to ensure that the staff is familiar with the steps to take in the event of a disaster. Equally important in the testing process are opportunities to identify gaps and inconsistencies in the plan (detailed in step 6). After all it is optimal to identify problem areas in a test than in a real disaster.

- Test business continuity plans at least once a year (organisations in sectors with BCM regulations appear to be moving toward quarterly testing schedules);
  - Apply processes and procedures identified in the BCP;
- When conducting tests, involve operational and functional employees and managers;
- When conducting tests, strive to make the exercises resemble a "real" response to the greatest extent possible (e.g., include local, state and federal emergency response agencies in the exercises whenever possible);
- Ensure time sensitive processes are recovered to the minimal acceptable level;
- Resume and stabilise business operations within the timeframe acceptable to the entity.

STEP 6: MONITORING, VALIDATING AND IMPROVING

- Evaluate how significant changes, such as reorganisations, mergers and acquisitions, and major system implementations, affect business continuity plans, and adjust plans as required;
- Adjust business impact analyses and business continuity plans to ensure that they take into account significant organisational changes;
- Identify weaknesses and gaps uncovered during the test exercises, and adjust plans as required;
- Develop a timeline to eliminate weaknesses; and
- Report on the outcome of the tests and ensuing remediation plans to keep senior executive teams and corporate boards informed.

CONCLUSION

Natural disasters and other unexpected business interruptions occur more often and inflict greater damage on organisations than they have in the past. Business continuity management (BCM) enables organisations to reduce the negative impacts of disasters and to return to normal operations sooner.

The development of sufficient BCM capabilities requires:

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

FURTHER RESOURCES

Online Resources

Business Continuity Management/Disaster Recovery Planning Resources (aicpa.org)

DRI International www.drii.org

The Business Continuity Institute (BCI) www.thebci.org

The Disaster Recovery journal www.drj.com

The Information Clearinghouse Continuity Central www.continuitycentral.com

World Economic Forum – The Global Risks Report 2015 – 11th Edition

Publications

Faster Disaster Recovery (aicpa.org)

Principles and Practices of Business Continuity: Tools and Techniques (aicpa.org)

SOURCE

The information herein was adapted from the Management Accounting Guideline entitled *Business Continuity Management* by Eric Krell. Copyright © 2006 by The Society of Management Accountants of Canada (CMA Canada), the American Institute of Certified Public Accountants, Inc. (AICPA) and the Chartered Institute of Management Accountants (CIMA).

Note: The Society of Management Accountants of Canada is now Chartered Professional Accountants of Canada.

REFERENCES

1. www.thebci.org/index.php/resources/what-is-business-continuity
2. BCI's BCM Lifecycle model
3. BCI Position statement on organisational resilience
4. Global State of Enterprise Risk Oversight, 2nd Edition, CGMA 2015
5. www.iso.org/obp/ui/#iso:std:50038:en
6. www.iso.org/iso/news.htm?refid=Ref1587
7. finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=8625
8. www.thebci.org
9. www.drj.com

American Institute of CPAs

1211 Avenue of the Americas
New York, NY 10036-8775
T. +1 212 596 6200
F. +1 212 596 6213

Chartered Institute of Management Accountants

The Helicon
One South Place
London EC2M 2RB
United Kingdom
T. +44 (0)20 7663 5441
F. +44 (0)20 7663 5442

CIMA REGIONAL OFFICES:

Africa

4th floor, 54 Melrose Boulevard
Melrose Arch
Melrose North
Johannesburg, South Africa
T: +27 (0)11 788 8723
F: +27 (0)11 788 8724
johannesburg@cimaglobal.com

Europe

The Helicon
One South Place
London EC2M 2RB
United Kingdom
T: +44 (0)20 8849 2251
F: +44 (0)20 8849 2250
cima.contact@cimaglobal.com

Middle East, South Asia and North Africa

356 Elvitigala Mawatha
Colombo 5
Sri Lanka
T: +94 (0)11 250 3880
F: +94 (0)11 250 3881
colombo@cimaglobal.com

North Asia

1508A, 15th floor, AZIA Center
1233 Lujiazui Ring Road
Pudong Shanghai, 200120
China
T: +86 (0)21 6160 1558
F: +86 (0)21 6160 1568
infochina@cimaglobal.com

South East Asia and Australasia

Level 1, Lot 1.05
KPMG Tower, 8 First Avenue
Bandar Utama
47800 Petaling Jaya
Selangor Darul Ehsan
Malaysia
T: +60 (0) 3 77 230 230/232
F: +60 (0) 3 77 230 231
seasia@cimaglobal.com

CIMA also has offices in the following locations:

Australia, Bangladesh, Botswana, China, Ghana, Hong Kong SAR, India, Ireland, Malaysia, Nigeria, Pakistan, Poland, Russia, Singapore, South Africa, Sri Lanka, UAE, UK, Zambia and Zimbabwe.

cgma.org

April 2016

Association of International Certified Professional Accountants

AICPA | CIMA