Chapter 3
Business Continuity Management (BCM)

3.1 Introduction

This chapter elaborates on a review of BCM. As the background, it describes the historical development of BCM and its relationships with other concepts. It will be followed by reviews on BCM as a management system, BCM's main principles, and Business Continuity Planning overview. The next section will describe the implementation of BCM, related with regulations or standards that support the concept and the development of BCM level of preparedness. Several reviews on BC plans from various sectors are elaborated in the final part of the chapter, followed by reviewing the need for BCM in organizations based on its benefits and challenges.

3.2 Background

3.2.1 BCM Definition and Development

The Business Continuity Institute (Business Continuity Institute 2007b) defines Business Continuity Management (BCM) as an act of anticipating incidents that will affect mission-critical functions and processes for the organization, and ensuring that it responds to any incident in a planned and rehearsed manner. Moreover, the Singapore Standard for BCM (SPRING 2008) looked at this concept as a holistic management process that identifies potential impacts which threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. Foster and Dye (2005) similarly viewed BCM as the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change. In this

L.S.R. Supriadi, L. Sui Pheng, *Business Continuity Management in Construction*,
Management in the Built Environment, DOI 10.1007/978-981-10-5487-7_3

context, top management must take the lead in driving organizational BCM with a view to garnering the collective efforts of all individuals within the organization for this purpose (Low et al. 2008a).

The main objectives of developing and implementing a BCM in an organization are (O'Hehir 1999; Health 1999):

1. To enable a focused approach in developing a business continuity plan (BCP), using a well structured and comprehensive methodology.
2. To develop a pragmatic, cost effective, and operable recovery plan, to enable the firm to achieve critical business processes during a major disruption to the firm's operations.
3. To minimize the impact of the crisis on the firm's operations.

Moreover, Smith (2003) stated that an effective BCM strategy should be to ensure the safety of staff, maximize the defense of the organization's reputation and brand image, minimize the impact of business continuity events (including crises) on customers or clients, prevent impact beyond the organization, demonstrate effective and efficient governance to the media, markets and stakeholders, protect the organization's assets, and meet insurance, legal and regulatory requirements.

Historically, BCM was developed many years ago, where this concept is an evolution of a disaster recovery approach in a firm. Its roots lie in Information Systems (IS) protection although it is argued that it has grown a long way since then. Elliott et al. (2002) developed on these theories in more details explaining that the evolution of BCM has progressed from a focused technical aspect to a broader strategic organizational requirement. They also described the evolution as being linked to three mindsets within organizations which are technology, auditing and value based mindsets. The key features of these mindsets are:

a. Technology mindset in the 1970s—The focus was on the protection of computer systems, principally hard corporate main frame systems. During the 1970s, a common assumption was that business disruptions were triggered by a technology failure; thus priority was placed on protecting hard systems such as corporate main frame systems (Prithchard 1976; Broadbent 1979; Kuong and Isaacson 1986).
b. Auditing mindset in the 1980s—Technological changes in the 1980s which moved the IT element away from main frame to end user PC responsibility, brought with it regulations, corporate legislation and policies. Auditing was needed to ensure compliance. The major focus of the auditing perspective is still on the technology, the plan itself, and how continuity can be established through protecting essential business activities.
c. Value mindset in the 1990s—This described the value-based mindset as being focused on the needs of the business, where BCM is considered to have the potential to add value to the organization. The value-based perspective departs from the technology and auditing perspectives in the assumptions that were made about the scope and purpose of BCM. The scope is perceived as constituting the entire organization including employees, who are regarded as

presenting the biggest challenge in terms of implementation and management of the business continuity process. Organizational stakeholders are regarded as being the most important driver for change and BCM. The fundamental approach in this perspective is that business continuity is regarded as the integration of social and technical systems which together enable effective organizational protection (Swartz et al. 1995). Therefore, BCM not only protects but is also seen to contribute to the value adding process through more efficient systems or providing value-adding benefits to customers through superior responsiveness, reliability, and security.

According to Foster and Dye (2005), after the September 11 2001 attacks, an event that hit the World Trade Centers in New York City, many companies had realized that the world is now full of many unknown threats, requiring that business continuity plans be much broader than in the past. Significant threats are now not only confined in the categories of fire, natural disasters and some infrastructure breakdown. Threats such as terrorism, cybercrime, reliance on third-party vendors and suppliers have also become significant. Therefore, business continuity planning should require more robust prioritization efforts for business recovery, proactive development of new and innovative recovery strategies, and a greater dependence on the testing of plans. Furthermore, considerations that need strategic thinking are not only on the location decisions of a company's own facilities, but also the location decisions of a business partner (such as supplier). All of these environmental changes take BCM into a higher level, which is more focused on building resilience.

Smith (2003) also argued that BCM is not only about disaster recovery or responding to a crisis. It should be a business-owned and driven process that unifies a broad spectrum of management disciplines. In addition, crisis and risk management are part of the fundamentals used for developing a BCM concept.

Figure 3.1 shows the difference between the old and new BCM approach. Herbane et al. (1997) described the continuum of standard and better practice of BCM and identified a number of dimensions against which practice might be assessed. The first two dimensions refer to the types of staff employed in continuity projects and to the scope of their work. Standard practice is concerned with IT systems and employs only IT staff while better practice organizations employ staff from various backgrounds on a project which is business wide in scope. In standard practice, there was little need for new structures because IT could deal with continuity. In better practice cases, new structures of coordinators were identified with responsibility for the continuity process being delegated to each business unit and the dedicated continuity team providing a supporting role. The final group of dimensions relates to the strategy. Better practice saw continuity as a strategic issue both in terms of protecting its place in the supply chain and in marketing activities.

Based on these reviews, it shows that BCM has developed and evolved into a more holistic approach. It has progressed into a broader strategic organizational mindset which focuses on its business values. In the context of definition, it appears that SPRING's (2008) definition of BCM has incorporated all of these aspects and

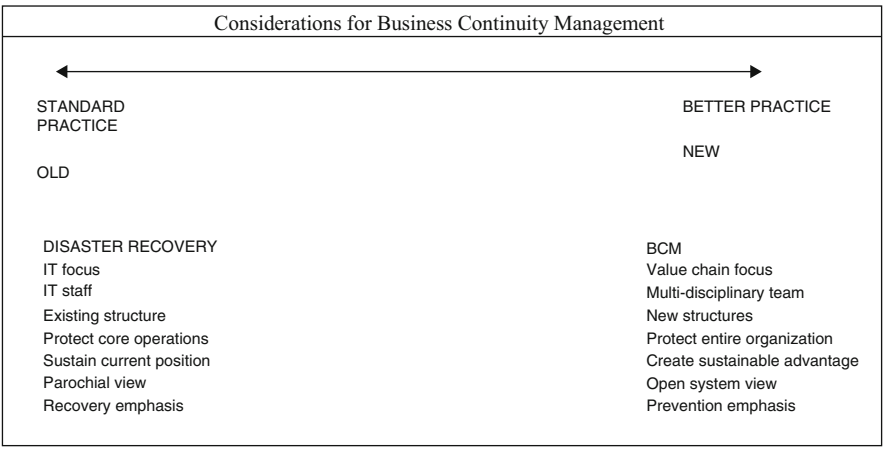

Fig. 3.1 Old and new BCM approach. Source: Adapted from Herbane et al. (1997)

represents the latest BCM mindset. Other BCM definition from BCI (2007b), Foster and Dye (2005), and Smith (2003) provide similar meanings of the BCM concept, which focuses on the keywords of: processes/procedures for the organization; response to incidents/threats/events; critical functions; and a planned and rehearsed manner. However, SPRING (2008) defined BCM's critical functions in more detailed aspects which include key stakeholders, reputation, brand and value-creating activities. Moreover, it specified the management process as holistic and the responses to threats/incidents are developed as a framework for building resilience.

3.2.2 BCM and Other Related Concepts

BCM has been considered as part of other concepts for overcoming crisis. There are relationships between BCM and these concepts, such as risk management, crisis management, and disaster recovery.

3.2.2.1 BCM and Risk Management

There are differences between risk management and BCM. Risk management focuses on a thorough organization-wide identification and assessment of risks and evaluating risks in relation to their likelihood and impact before identifying an appropriate risk response. BCM is concerned only with events that cause a significant business disruption, where it is not mainly concerned with probability but with the impact of an event and the time required for an organization to return to

normal business operations (Collier 2009). Moreover, Goh (2010) mentioned that the relationship between risk management and BCM can be partially explained by referring to the Australian Standard for risk management. BCM efforts focus on addressing those risks which are deemed not acceptable to the organization. Subsequent BCM activities are aimed at establishing the appropriate measures to address these risks. It relegates BCM as part of risk treatment. Business Continuity has been defined "to safeguard the interests of an organization and its key stakeholders by protecting its critical business functions against predetermined disruptions" (BCI 2010, p. 3). The numbers and types of critical business functions in an organization would depend on the nature of the business and its mission as reflected in its Minimum Business Continuity Objective (MBCO). Risk management in BCM should be restricted to those instances where it affects the MBCO of the organization. It is also important to note that BCM is focused on identifying vulnerabilities within organizations, especially those linked to the underlying value they support and understanding the impact of their non-availability over time on the organization (BCI 2010; Hiles 2007). Table 3.1 summarizes the comparison between risk management and BCM.

3.2.2.2 BCM and Crisis Management

BCM has strong links with crisis management through the incident management component. In the BCM context, incidents come in different shapes and sizes and will typically invoke the BCM plan. Crisis management is often seen as the domain of communication and public relations (PR) practitioners with the BCM practitioner in a support role, if involved at all. Crisis management is also seen as responding to non-physical as well as physical events such as financial performance and reputation tarnishing incidents (BCI 2010).

Table 3.1 Comparison between Risk Management and BCM [adapted from BCI (2005, p. 6)]

	Risk management	BCM
Key method	Risk analysis and assessment	Business impact analysis
Key parameters	Impact and probability or likelihood	Impact and time
Type of incident	All types of events	Events causing significant business disruption
Size of events	All sizes and costs of events	For strategy planning: survival-threatening incidents only
Scope	Focus primarily on risks to core business objectives	Mostly outside the core competencies of the business
Intensity	All from gradual to sudden	Sudden or rapid events (although response may also be appropriate if a slower-moving incident becomes severe)

Source: Drennan and McConnell (2007)

Moreover, BCM considers any disruption holistically and determines how an organization will respond to the disruption, continue its activities and recover. BCM practitioners consider the media response to an incident or crisis to be an integral part of a full business continuity (BC) programme. Regarding emergency planning that is usually included in incident management, BCM views that this planning is not only seen as the domain of services from police, fire, ambulance and local authorities, but also for the organization in general. The company that adopts BCM would have a specific emergency response team that will coordinate with other external emergency response agencies (BCI 2010).

Other relationships between BCM and crisis management were also mentioned by Elliott et al. (2002), where BCM provides principles that use a crisis management approach. A crisis management approach may be defined as one that:

- Recognizes the social and technical characteristics of business interruption (organizations are socio-technical systems).
- Emphasizes the contribution that managers may make to the resolution of interruptions (the importance of the human response element).
- Assumes that managers may build resilience to business interruptions through processes and changes to operating norms and practices.
- Assumes that organizations themselves play a major role in "incubating the potential failure" (early detection is vital).
- Recognizes that, if managed properly, interruptions do not inevitably result in crises (the importance of preventative measures).
- Acknowledges the impact, potential or realized, of interruptions upon a wide range of stakeholders (think beyond the impact on the organization itself) (Elliott et al. 2002).

Some studies had made a distinction between BCM and crisis management. BCM refers to the planning and implementation of systems and procedures to enable an organization to sustain normal operations in the event of a disaster or other potential interruption. It is the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change. Crisis management is viewed to be a process by which an organization deals with major unexpected events that have already happened. Crisis management focuses on the immediate activities which need to be considered when the incident occurs. At most, the crisis management planning phase deals with the first couple of hours of the incident occurring, detailing who the key decision makers are, who will talk to the customers/clients/regulators and when this will be conducted (Smith 2003; Devlin 2007; Foster and Dye 2005). In addition, BCI (2007a) defined crisis management as the role that senior management have during an incident. It includes the high level command and control aspects of identifying a crisis situation, deciding how and when to respond, communicating both internally and externally, and leading and directing the recovery process.

3.2.2.3 BCM and Disaster Recovery

According to Elliott et al. (1999), the difference between disaster recovery and BCM is primarily based on its scope. Disaster recovery is a focus on technology-based problems triggered by external factors. BCM focuses more on adding value, creating an attitudinal change throughout the organization and considering its associated stakeholder groups. It is more concerned with the continuance of the whole business in the face of any unusual or unforeseen event. Moreover, disaster recovery is the implementation of a response capability to a specific type of event that impacts the continuity of the business. BCM is responsible for the overall identification of potential events, the likelihood of the occurrence of the event, and the predicted impact on the organization. BCM puts in place plans to deal with such occurrences. Disaster recovery is essentially a plan, with supporting infrastructure, which is enacted in the event of a disaster. In this way, disaster recovery is a subset of BCM, as is contingency planning, high availability planning, and the like (McCrackan 2005).

3.2.2.4 BCM and Business Resilience

BCM is a relatively newcomer to the business disciplines; however, aspects of BCM may have always been present in organizations, under different names. The vulnerabilities in the business and operating model of an organization can be considered in seven areas, which are reputation, supply chain, information and communication, sites and facilities, people, finance and customers. The nature of the BCM approach is to provide the framework to understand how value is created and maintained within an organization and establishes a direct relationship to dependencies or vulnerabilities inherent in the delivery of that value. This approach is conducted in a holistic and cross-functional manner. A successful BCM implementation would increase an organization's resilience, where it is defined as the ability to absorb, respond and recover from disruptions. This will eventually contribute to higher corporate performance (BCI 2010).

3.3 BCM as a Management System

BCM is a system that develops a framework of protocols and sets of procedures and instructions which give structure, order and stability to the particular function being managed. It is in line with the definition of a management system, stated by Griffith (1999), that sets out and describes, for a particular management function, the organization's policies, strategies, structures, resources and procedures used, within the firm to manage the processes that delivers its products or services (Griffith

2011). Based on its theory development and main principles, it can be seen that BCM adopts several management mainstream theories.

In its implementation, BCM adopts the Plan-Do-Check-Act (PDCA) methodology for achieving continual improvement. The BCM policy, objectives, processes and procedures are planned, implemented, assessed, and reviewed regularly (SPRING 2008). PDCA is a key attribute within standards-based management systems that is widely used nowadays. It was established by Deming, who propounded the view of quality management within a cycle of plan-do-check-act. The theories underpinning quality management have influenced systems development and continue to form component parts of systems applications. Historically, quality management was developed from a range of traditional organizational theories such as scientific, human and classical schools of thought. These theories are also pertinent to the evolution, development and implementation of management systems (Griffith 2011).

BCM also adopts the view of complexity theory, where an organization consists of a number of components (agents) that interact with each other according to sets of rules that require them to examine and respond to each other's behavior in order to improve their behavior (Stacey 1996). According to Griffith (2011), due to the extensive and complexity in the arrangement of business activities, processes and resourcing, a management system in an organization should establish an effective framework of responsibilities at various organizational levels. Parts of BCM principles are determining various responsibilities to the BCM members.

Based on its definition, BCM is developed and implemented in a holistic approach. The holistic perspective has much in common with systems theory. This theory viewed management system as a central part that directly supports the core business of the organization. Moreover, it is considered that a management system focuses not only on itself but also for the greater contribution that it can make to the organization (SPRING 2008; Griffith 2011; Checkland 1981).

According to Lawrence and Lorsch (1967), contingency theory suggests that organizational variables are in a complex interrelationship with one another, where environmental contingencies act as constraints and opportunities which influence the organization's internal structures and processes. Moreover, decision making are made through considerations of all aspects and situational approach (Olum 2004; Carlisle 1976). In BCM, this approach is adopted by implementing risk analysis and business impact analysis. The consideration of risk is viewed as a key element of the system (BCI 2010).

The BCM methodology has strong links with crisis management. Crisis management is often viewed as responding to non-physical as well as physical events such as financial performance and reputation tarnishing incidents. Furthermore, the domain of communication and public relations are important in crisis management. BCM considers any disruption holistically and determines how an organization will respond to the disruption, continue its activities and recover. BCM practitioners also viewed that communication and response to public are part of a full business continuity programme (BCI 2010).

Regarding change management, it is also part of crisis management. Lawrence et al. (1976) stated that a visible crisis faced by an organization can be an important force for triggering behavioral change, although such change may have costs derived from it. Essentially, such crisis has an unfreezing impact on the members of the organization, causing them to review and analyze their current attitudes and behavior patterns. Managing change in an organization should be conducted in orderly phases which are diagnosing the problem, planning the change, launching the change, and following up on the change in the organization. In this matter, it appears that these phases are similar to the PDCA approach which is adopted by BCM (SPRING 2008; Lawrence et al. 1976).

In accordance with Griffith (2011), a general approach to planning, delivering and implementing any management system consists of the following key considerations, which BCM also provides:

- The needs of the customer and other stakeholders.
- The policies and objectives of the organization.
- The organizational processes necessary to fulfill the policies and objectives.
- The assignment of responsibilities to manage processes towards the objectives.
- The provision of resources to attain the objectives.
- The establishment of procedures and instructions to manage the processes.
- The monitoring of processes to determine their efficiency and effectiveness.
- The identification and elimination of non-conformities in the processes.
- The encouragement of continual improvement in management of the processes.
- The audit and review of systems to improve the overall management approach.
- The feedback on performance to improve provision to customers through improved policies and objectives.

Furthermore, the highly influential factors to be considered in implementing a management system are as follows (Griffith 2011):

- Organizational culture. Instilling a trusting and cooperative workforce is vital to embedding the system.
- Involvement, which is bottom-up involvement from grassroots level in system development is essential, as is inviting contribution and feedback to management.
- Resources, which are trained and capable managers, supervisors and workforce are essential and, as such, investments in training and system ownership should be a priority.
- Flexibility. The system should be allowed considerable flexibility in performance upon system establishment, incrementally becoming more demanding as familiarity with its operation is developed.
- Shared commitment. Management must develop a blame-free culture where learning and improvement are preferred to difficulty and blame.

These factors should be embedded in an organization for its BCM implementation effectiveness.

3.4 Main Principles of BCM

To implement BCM, each organization must identify the threats and assess their resulting impacts. BCM needs to address issues and concerns in six broad areas in the following order (SPRING 2008):

1. Risk analysis and review: The threats to an organization can be identified through a risk analysis and review of its internal operations and external operating environment.
2. Business Impact Analysis: The potential impact of these threats on an organization and its ability to continue business operations and service can be obtained by conducting a business impact analysis. This would include, where possible, the loss impact from both a number of days of business disruption and financial consequences.
3. Strategy: The organization determines the appropriate strategies to safeguard its interests. These strategies can be preventive or pre-emptive in nature.
4. Business Continuity Plan (BC Plan): A detailed business continuity plan should be formulated to indicate the resources and capabilities required of the organization to prepare, respond, and recover from potential threats.
5. Tests and exercises: An established BC plan shall be validated by implementing tests and exercises. These are done to highlight errors or omissions and verify if the resources committed are accessible, available and adequate for efficient and effective recovery. It also verifies whether the staff is familiar with recovery procedures, and whether the BC plan meets its recovery objectives.
6. Program management: The organization will demonstrate commitment in maintaining the currency of its plan through regular and systematic review of its risks and business impacts, regularly reviewing its BCM strategies and revalidating its BC plan. Program management serves to validate the capability of the BC plan to fulfill the plan's objectives. Validation aims to uncover flaws in the plan design, for example any inaccuracies and incompleteness of the design of the plan.

There are four main components that must be considered in implementing BCM in an organization, which are (SPRING 2008):

- Policies: Senior management must stipulate policies to guide BCM efforts by the staff. The policies should set out the organization's aims, principles and approach specifying what is to be achieved or delivered, and will serve as the rationale and support for all BCM areas. In addition, policies provide the rationale for establishing the processes, people and infrastructure to support BCM on an ongoing basis.
- Processes: The set of activities with defined outcomes, deliverables and evaluation criteria to attain the objectives of the BCM policies. They include formal change control and documentation processes.
- People: Participation from various business units in the firm should be established to oversee BCM efforts and the skill sets of participants are crucial

to the success of BCM. The roles and responsibilities of staff involved in the organization's BCM efforts should be clearly defined.
- Infrastructure: The organization should allocate resources to support critical business functions against potential risk events. This consistently requires a good understanding and application of available technology and equipment, and physical facilities to respond to risk occurrences.

Generally, BCM has four main processes which are developed in an organization. The processes are the initiation process (initiating the BCM concept in the firm), planning for business continuity [which produces a business continuity plan (BC Plan)], implementation (implementing the BC Plan through testing and exercising), and lastly the operational management process (maintaining and updating the BC Plan). These four processes can be divided more comprehensively into six phases which are (Pitt and Goyal 2004; Elliott et al. 2002; BCI 2010):

1. Phase one—Project initiation

   The fundamental critical activity required prior to the establishment of a BC Plan is obtaining senior management approval, support, and commitment. Having obtained management approval, the initial phase of the BC Plan will include establishment of the BC Plan objectives and requirements of the plan. A business continuity steering committee would normally be established. This committee is likely to be made up of senior staff within the organization who have the relevant strategic view of the firm's operations. It is important that they also have nominated deputies who are suitably briefed and have an in-depth understanding of the BCP process.
2. Phase two—Risk assessment/business impact analysis

   The principal objectives of phase two relate to data gathering and review of alternative courses of action. The identification and evaluation of this information will then allow senior management to make decisions on the critical aspects of the core business. Having identified the risks, a business impact analysis should then be carried out. Karakasidis (1997) identified this as a key step in protecting an organization, and identified some of the minimum objectives as being:

   - Determine critical requirements and resources and the effects a disaster may have on the people, place, process, and premises.
   - Estimate anticipated target recovery time for each core business function and service.
   - Establish core business recovery priorities.
   - Identify key personnel, equipment, and facilities needed to support core functions.
   - Estimate costs of extended business disruption.
   - Identify resources required to develop, test, and implement BC Plan.

3. Phase three—Design and development of the BC Plan

   Essential issues to be addressed at this stage include detailed scope strategy and objectives of the plan, administration procedures, formation of business

continuity committee and downstream business recovery teams, lines of communication, escalation notification and plan activation, scenario setting for plan execution, establishing BC Plan records, storage, access, and its budget.

4. Phase four—Creation of the business continuity plan

   This phase basically deals with the creation of the BC Plan. The key issues to be addressed include:

   - Emergency response procedures covering evacuation, decanting access to work areas, and access to documentation.
   - Emergency control center establishment, command and control procedures.
   - Detailed procedure for communications, delegation or designation of authority, and key stakeholders.
   - Detailed resumption, recovery, and restoration procedures.
   - External support, vendor contracts, contacts, and resources.

5. Phase five—Testing and exercising BC Plan

   In order to establish the effectiveness of BC Plan, it is essential to implement a regular testing and exercise program. The key activities to be established during the testing and exercising stage will include preparation of exercise program and objectives, the details of exercise scenarios and monitoring and recording procedures, and identification of training requirements, communication channels, and induction of new staff.

6. Phase six—Maintenance and updating

   Having established the need for testing and the degree of probability that a substantial number of plans might fail following the testing exercise, it is essential that the lessons learned and shortfalls documented are incorporated into the plans. The key issues to be addressed during this phase include:

   - BC Plan review criteria and objectives
   - Schedules and program of review
   - Plan distribution and security

In responding to the changing environment of a business from time to time, the maintenance and updating process should be done in a regular and continuous basis.

Based on this review, it is considered that BCM has evolved from a simple reactive disaster recovery planning, to crisis management principally driven by information technology, and finally to a more proactive comprehensive approach.

3.5 Business Continuity Planning (BCP)

The main process of BCM is Business Continuity Planning (BCP). BCP refers to the identification and protection of critical business processes and resources required to maintain an acceptable level of business, protection of such resources, and preparation of procedures to ensure the survival of the organization in times of business disruptions. Fundamentally, it seeks to mitigate the impact of a disaster by

ensuring alternative mission-critical capability is available when disaster strikes. The process seeks to preserve the organization's assets in the event of a disaster, which are its capability to achieve its mission, its operational capability, its reputation and image, its customer base and market share, and its profitability (Low et al. 2008; Hiles 2007). This is regarded as the main process due to its vital output for the firm in handling disruptions and overcoming crises. This planning process will be followed by regular monitoring and updates.

Before formulating the BCP framework, the following issues have to be considered thoroughly (Low et al. 2008a; O'Hehir 1999; Eternity Business Continuity Consultants 2007; Civil Contingencies Secretariat 2007):

1. Policy—formulating a policy statement at the managerial level to signify the company's attitude towards a particular risk and prescribing the objectives of such a policy.
2. Methodology—analyzing the assessment processes involved in evaluating a crisis, and promoting greater commitment for the company to proceed with the plans.
3. Accountability—establishing individual accountability for managing the risk and ensuring that the nominated person has the appropriated technical expertise and authority to manage the risk.
4. Management support—determining the company's current managerial attitude or process towards assessing and managing the risk, without which the company will not have the initiative to implement BCM in the organization.
5. Dependencies—defining the scope of the BCP clearly, so that every individual is aware of the dependencies involved, whether this is external or internal (key supplier, personnel, operating system, etc.) to successfully mitigate the specified crisis.
6. Being realistic—educating the management that a crisis brings about certain risks and to mitigate the effects, certain costs are involved. The management should be ready to accept certain risks and should be prepared to spend the necessary funds to mitigate the risks involved.
7. Future actions—determining the appropriate business processes to be implemented or to be refined, to reduce the risk to an acceptable level, and assigning responsibilities and milestones.
8. Performance measures—establishing measurement indicators to enable assessment, and monitoring the effectiveness of risk management which can be proactive or reactive. Proactive action is recommended to prevent occurrence.
9. Independent expert—appointing an internal or external, qualified, independent expert to determine the adequacy of the response to the crisis, such as through regular meetings, and reporting to higher management to signify the importance of BCM.
10. Contingency plan—establishing an alternate plan for the unforeseen circumstances not being provided for.

According to Vancoppenolle (1999) and Elliott et al. (2002), the respective elements are included in the operational flow of a company's operations, which

are: (1) Business processes (how the products and services are delivered to the client); (2) Participants (who the participants are, in the execution of the business process); and (3) Infrastructure and resources (what is used in the execution of the business process). These elements are necessary to be reviewed when analyzing a crisis during BCP.

Furthermore, upon the occurrence of a crisis, many parties could be affected (Elliott, Swartz and Herbane 2002). It could be the company management or interest groups like investors, suppliers, etc., who have direct or indirect investments in the company. The occurrence of a crisis, if not appropriately mitigated, could lead to adverse consequences such as withdrawal of funds, which is an external factor. Even though investors are not directly involved in the company's operations, they have an indirect influence on the growth of the company. Therefore, the requirements of the various stakeholders in the organization should also be considered, which include the following (Singapore Business Federation 2003):

- The ways and means of the employees' livelihood protection.
- The defined time lines for the resumption of support and services and transparency of operations in a crisis, which relate to customers and suppliers.
- The control of the situation, cost effective solutions to handle the impact of the crisis and the effects on business resumption, and transparency of operations by managers.
- Good corporate governance, protecting the image of the organization, and sharing of the company's profits that linked strongly to what investors will review on the company.

Hiles (2007) stated that the company's BCP should not be driven by eliminating risks according only to their probability, but rather be based on the effects and impacts on the business if an unexpected event were to occur. Such classification according to effects could be:

- Failure of an individual infrastructure element, including single points of failure.
- Longer-term interruption of a critical information flow.
- Longer-term interruption of a critical business activity chain or business process.
- Local longer-term business interruption.
- Complete business interruption.

These effects from an unexpected event may cascade into larger impact levels. Some examples of these effects are damages to infrastructure elements and resources supporting the business operations. The damage can result in impacts such as unavailability of infrastructure elements or resources or loss of information. Loss of information due to a disaster is not limited to data in computers. All of the information stored in binders, folders (with, for instance, customer information), contracts, property deeds, the archives, the legally required vital records, the paper client files, the business knowledge spread over the place, and others can be lost too.

Other than impacts on business operations, the long-term impacts of such crises or events may also arise, even after the business has been resumed and operations have returned to normal. The examples of long-term impacts are: loss of market

share; lower share price; lower credit rating; loss of brand value; loss of company image, public confidence and credibility; and loss of key staff. Furthermore, the rippling effects of a business interruption should never be underestimated, particularly for companies that are an integral component of a wider supply chain. When a company participating in a supply chain is hit by a disaster, this could ripple down throughout the supply chain (Hiles 2007).

3.6 BCM Implementation

Nowadays, BCM is widely used in various types of firms. Firms in banking, telecommunication, oil and gas, and retail industries had developed a BCM concept in their management systems. BCM is developed based on their respective business strategies and activities. Due to the different business environments, the firms developed different procedures for overcoming different types of crises. Some of them had also focused not only on their business continuity, but the service continuity to their customers. This shows that they had developed the program based on the value mindset (Elliott et al. 2002).

Herbane et al. (2004) also found that BCM has evolved to encompass wider participants, threats, techniques and responses. It has been applied in the financial service industry, vehicle breakdown services, gas suppliers, water utilities, supermarkets, and local authorities. All of these organizations recognize that in the face of internal and external threats to the continuity of operations, a socio-technical approach (beyond IT disaster recovery) is essential to improve business recovery from crises. They also have linked BCM to strategically important dimensions of their operations.

When implementing BCM for the first time in an organization, project management practices should be adopted. The practices of project management that may usefully be employed include the identification of deliverables, timescales and deadlines, and budget and work effort control. Other knowledge in project management such as communications, risks, procurement and human resources management are also needed for establishing effective BCM components (Business Continuity Institute 2007a).

3.6.1 Legislation and Standards Relating to BCM

Elliott et al. (2010) elaborated that the earliest legal provisions to influence disaster recovery and business continuity (BC) ideas can be found in the 1977 Foreign Corrupt Practices Act, which is the US financial services sector's provision. It is often cited as an important development in firm's reorientation of the perceived threats and impacts. Since then, the US financial services industry has developed various regulations and legal requirements to impose greater requirements on BC

provisions. Although the acts do not refer specifically to BC, they specify the importance of countering the increasing risk of external threats to digital resilience, which is one of the dependencies on BCM.

Moreover, the introduction of BCM-specific regulations in the financial services sector is not only applied in the US. The Australian Prudential Regulation Authority (APRA) Standard on BCM APS 222 (for deposit taking institutions) and GPS 222 (for general insurers) published in April 2005 (APRA 2005a, 2005b) requires Australian financial institutions to implement a whole of business approach to BCM. Elsewhere, the Reserve Bank of India (RBI) set out a requirement for Indian banks to fully implement BCP, presents a planning methodology, and further specifies a template for plan content. Banks are required to submit recovery time objectives for critical systems to RBI's Department of Banking Supervision at the end of each financial year and to report major failures and response activities or prevention measures on a quarterly basis (Parthasarathi 2005; Elliott et al. 2010).

In several countries such as United Kingdom (UK), United States of America (US), Switzerland, Australia, New Zealand and Singapore, BCM had been developed into a national standard, where every firm from various sectors is encouraged to have this system in its organization (Elliott et al. 2010). In Singapore, the SS540:2008 standard has been formally used as the standard for implementing BCM in a firm. This Singapore Standard is applicable to all organizations regardless of their size. This standard emphasizes resilience and protection of critical assets, in the human, environmental, intangible and physical domains. It focuses on continuity management and recovery of critical business functions (SPRING 2008). Up to now, Singapore is the only country in Asia that has established a BCM standard, whereas other BCM standards came from Europe, North America, and Australia (Elliott et al. 2010).

In the UK, the Business Continuity Institute (BCI) has developed a certification standard for business continuity practitioners. Besides that, a BCM standard (BS25999:1-2006) as a Code of Practice for Business Continuity Management was also published by the British Standards Institution and can be viewed as an implementation guide and a definitive text for those intending to understand BCM principles and practices in a more comprehensive manner (Business Continuity Institute 2007a). Moreover, the American Chapter of the Business Continuity Institute (BCI) and BSI America have joined forces to help businesses better prepare for disasters by encouraging the adoption of BS 25999 (Business Continuity Institute 2009). This standard is also in line with US's national standard for business continuity, which is NFPA 1600:2007 (National Fire Protection Association 2007).

Furthermore, ISO has officially launched ISO 22301, "Societal security—Business continuity management systems—Requirements", the new international standard for Business Continuity Management System (BCMS). ISO 22301 has been developed in 2012 to help organizations minimize the risk of business disruptions (St-Germain et al. 2012). This standard is similar to the previous BCM standards, but it has some improvements for BCM implementation such as (St-Germain et al. 2012; SPRING 2012):

- Greater emphasis on setting the objectives, monitoring performance and metrics;
- Clearer expectations on management; and
- More careful planning for and preparing the resources needed for ensuring business continuity.

According to Goh (2010) and St-Germain et al. (2012), the standards from various countries have similar contents. The differences are on how the standards develop the detailed components in the BCM planning process. In general, each standard has the same BCM planning methodology, which are: Risk analysis and review; Business impact analysis (BIA); Recovery strategy; BC plan development; Testing and exercising; and Programme management (some standards incorporate project management in this phase). All of the above standards have the common objectives, which are to guide the users to recover from any disasters that have occurred in their business environment and still continuously focus on the continuity of their business processes. Furthermore, the standards also help the users in identifying the potential impacts of various disruptions to the firm and be able to prioritize the efforts in aiming to achieve resilience. Table 3.2 illustrates the main aspects of the BCM concept being grouped into six categories. These aspects are summarized from various standards.

3.6.2 BCM Level of Preparedness

Regarding implementing BCM in an organization, several agencies from various countries had developed assessment levels of BCM preparedness. These levels are useful to assess whether an organization has adopted a complete BCM concept or not. From understanding the position of the company within these levels, the organization gains feedback from its current BCM preparedness level and may increase its effort for a better BCM maturity level.

Levels of preparedness assessments have been proven to be an effective evaluation method (Scott 2007). In general, this type of assessment can help the organization to verify what they have achieved relative to the topic assessed. The organization's current achievement can also be determined by describing their current activities. In addition, it can assist the organization in prioritizing the necessary improvement based on their assessment results (Peng et al. 2011; Stevanovic 2011).

The Ministry of Finance in British Columbia, Canada (MOF-BC 2007), had developed the BCM maturity assessment for every financial agency in the province. There are three levels of criteria involved, which are:

- High maturity. This level demonstrated strong executive support for BCM, the establishment of an organization-wide structure supporting the activity, and staff responsible for BCM had a strong awareness of and compliance with core policy requirements, guidelines and procedures for BCP. BC plans for mission critical processes and business priority areas were developed and updated, and testing/exercising was ongoing, with results used to make changes. Monitoring and

Table 3.2 The main aspects of BCM principles

No.	BCM principles	Description
1	Risk analysis and review	• Examine internal and external risk events and impacts (qualitative and quantitative) that can affect the critical operation's continuity • Using Risk Analysis (RA), Business Impact Analysis (BIA), and Cost benefit analysis (justification for initial treatments to prevent or reduce the effects of risks and potential losses)
2	Business impact analysis	• Examine the impact to the organization (assesses the potential impact of loss from an internal perspective), qualitatively and quantitatively, due to a disruption of business operations and processes • BIA must be conducted on a periodic and systematic basis to assess the impact of losses if the corresponding business operations and processes are disrupted in view of proposed changes
3	Strategy development	Examine the possible strategies for maintaining the operation of Critical Business Functions (CBFs). This should cover pre-incident preparedness, response and recovery
4	BC Plan development	Examine the BC plan(s) which is an action plan that guides the response and recovery actions of the organization when disaster occurs. It includes an emergency response to stabilize the situation following a disaster, the set up and operation of an Emergency Operations Centre (EOC), and specifies CBFs to be recovered within their established Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) when a disaster occurs. RTO is the period of time in which functions must be recovered after a disruption has occurred, and RPO is the point in time at which systems and data must be recovered after a disruption has occurred.
5	Test and exercises for BC plan	• Ensure that the BC plan drawn up and implemented by the organization is viable and workable • Tests are intended to verify the capability of the BC plan to attain specified objectives or established criteria • Exercises are intended to train and condition BC team members to improve their coordination and performance in executing the BC plan. Exercises also serve to highlight any weaknesses in the operation and effectiveness of the BC plan, with establishing generic corrective actions if the result falls below assessment criteria
6	Program management	• Examine the ongoing efforts and activities of the organization to maintain the effectiveness of its BCM. BCM involves firm commitment of organization's efforts and resources to safeguard the interests of its key stakeholders, reputation, brand and value-creating activities on a continuous basis. Assessment of an organization's BCM efforts should therefore be dynamic • The BC plan is operated by staff of the organizations. Staff in the organization should be familiar with the plan via appropriate awareness and training programs prior to any test/exercise of the plan. Periodic and systematic training and awareness programs should be conducted to familiarize employees to the operation of the BC plan.

Sources: Adapted from SS540:2008 (SPRING 2008), NFPA1600:2007 (National Fire Protection Association 2007), BS25999:2006 (BSI 2006), ANZ5050:2009 (Standards Australia 2009; Elliott et al. 2010), SS ISO 22301: 2012 (SPRING 2012)

reporting processes were effective and efficient, and pandemic planning had been undertaken.
- Moderate maturity. This level demonstrated strong executive support and a level of coordination within the organization to ensure progress is made towards BCM objectives, although roles and responsibilities may not be adequately defined to ensure all recovery staffs were clear on their expectations in a business interruption. Compliance with core policy was low, and BC plans for mission critical processes and business priority areas were either under construction or in need of updating. Monitoring and reporting processes were largely ad hoc and pandemic planning may have been in the commencement phase.
- Low maturity. This is the lowest level of preparedness, where typically the organization had a lower level of executive support and BCM may not have been considered a high priority. These organizations exhibited a low level of awareness of policies and guidelines and of roles and responsibilities. Compliance with core policy was also low, and BC plans were either not developed or in need of significant updating. Pandemic planning may have been initiated, although activities to date were limited to those driven by existing OHS committees.

The Australian National Audit Office (2009) had also developed characteristics of better BCM preparedness for public sector entities. There are two levels, which are (1) Basic level, that is generally found in small, non-complex or less time-critical entities and (2) Mature level which is found in large, complex, geographically dispersed or critical entities. The characteristics that are described and assessed in each level are:

- A BCM framework is in place.
- Training and awareness of BC has been conducted.
- A risk assessment has been conducted.
- A BIA has been conducted.
- Preparatory controls have been implemented.
- The entity has documented and the executive has endorsed, its BC plans and framework.
- BC testing and exercises have been conducted.
- The entity monitors BC.

Also in Australia, Lansley and McAtee (2009) had established a six-level BCM preparedness model for companies, which are:

- Level 1—Self-governed: BCM has not yet been recognized as strategically important by senior management.
- Level 2—Supported self-governed: At least one business unit (BU) or corporate function has recognized the strategic importance of BC and has begun efforts to increase executive and enterprise-wide awareness.
- Level 3—Centrally-governed: Participating BUs and departments have instituted a basic governance program, mandating at least limited compliance to standardized BCM policy, practices and processes to which they have commonly agreed.

- Level 4—Enterprise awakening: All critical business functions (CBFs) have been identified and continuity plans for their protection have been developed across the enterprise.
- Level 5—Planned growth: BC plans and tests incorporate multi-departmental considerations of critical enterprise business processes.
- Level 6—Synergistic: All BUs has a high degree of BCP competency. Complex business protection strategies are formulated and tested successfully.

Smit (2005) had studied and defined another BCM maturity model that can be applied to organizations. According to the study, there are six level of BCM maturity, described as follows:

1. BCM initiated. An organization has initiated BCM if there is formal management commitment to the organization of BCM. The responsibility for BCM is covered at a sufficiently high level within the organization and an explicit BCM policy is in effect. The deliverable of the initiated stage is BCM as an initiative.
2. BCM planned. An organization reaches the stage planned if it has performed all necessary analyses and has written all relevant plans. Therefore, this stage is characterized by a BC analysis and a BC plan. The deliverable of the planned stage is BCM as a blueprint.
3. BCM implemented. Implemented stage is reached as soon as not only the measures to assure BC are planned, but also realized. This means BCM facilities have to be realized, services have been contracted and BCM tasks have to be assigned to the right people. The deliverable of the implemented stage is BCM as an implemented project.
4. BCM embedded. On the first three stages, BCM is a project. As soon as an organization reaches the embedded stage, BCM has turned into a process instead of a project. This stage is reached as soon as a maintenance process is designed; hence a maintenance plan is developed, the plan is known and available within the organization and there is awareness regarding the importance of BCM within the organization. The deliverable of the embedded state is BCM as a process.
5. BCM controlled. At the stage of BCM embedded, an organization has developed a maintenance plan and probably formulated some BCM exercises and tests. In the next stage, BCM controlled, this maintenance process is also executed as it should and exercises are done as planned for. In addition to that, the existing BCM is audited and controlled. The deliverable of the controlled stage is BCM as business as usual. If an organization has reached stage 5, it controls its existing BCM. For some organization, a BCM process that is controlled is sufficient. However, other organizations will strive for stage 6.
6. BCM optimized. If an organization has optimized its BCM, it can use its BCM as a strategic instrument, for example to gain a commercial advantage or strive for operational excellence as a business strategy. For this, a strategic approach of BCM is a requisite. Furthermore, the organization should strive for continuous improvement of their BCM and the deliverable of the optimized stage is BCM as a strategic instrument.

Furthermore, other BCM preparedness level model from a risk consulting firm in Canada (Marsh Risk Consulting 2010) had been developed. The level of preparedness with its label, overview of the preparedness level description, and the organization's ability to respond can be seen in Table 3.3.

Last but not least, the Singapore Business Federation (2011) provided a BCM preparedness assessment, based on the company's level of understanding about business continuity. Red level shows that the organization has a minimal understanding of BC, whereas Yellow level shows the organization has a basic understanding of BC, and finally Green level describes the organization has an advanced understanding of BC. The assessment are conducted through rating the firm's understanding and preparedness towards risk analysis and review, BIA, strategy development, BC plan development, tests and exercises, and programme management.

According to a study from New York University (2006), most businesses, particularly small and medium sized ones, are lacking formal BCM programs. Only one-quarter of the companies surveyed have formal, written continuity plans. Moreover, only four in those companies provided BCM training to their employees. These four companies had prepared the concept within their

Table 3.3 Marsh BCM preparedness level

Preparedness level	Label	Overview	Organization's ability to respond
Level 5	Optimizing BCM	BCM driven by corporate strategy is subject to continuous improvement and is integrated into the overall risk management and operational strategy	Organization has sustained ability to respond to and survive strategic threats and crises—both anticipated and unanticipated
Level 4	Integrated BCM	BIA is done at divisional level and value/supply chain dependencies are understood and protected	Organization understands its business processes and has the ability to deal with crises and recover processes across sites and into the supply chain
Level 3	Established BCM	Emergency response, crisis management and BC plans are completed and linked. Training and exercising embedded in the organization	BCM response is integrated and BCM capabilities can be sustained
Level 2	Formalizing BCM	Corporate policy driving a consistent approach at site level. BIAs are done for sites and recovery strategy agreed	Key location(s) have built the ability to respond to a localized emergency and recover business
Level 1	Undeveloped BCM	Ad hoc and reactive approach—not a systematic BC	Minimum legal/regulatory requirements met providing protection for people and facilities

Source: Marsh Risk Consulting (2010)

organization due to regulatory forces, which are risks to employees and business operations, legal liability, and insurance requirements. From this study, it is recommended that an organization should analyze its own case for BCM preparedness and invest accordingly.

3.7 Reviews of BC Plan

Various sectors have developed their BC plans based on the functions of their business and impacts that may occur from certain crises. There are general principles that can be gained from these plans that may provide insights on developing a BC plan.

3.7.1 BC Plan from Financial Services Sector

As mentioned before, the financial services sector is the pioneer of developing and implementing BCM. In general, the main principles that are established in their BCM policy are as follows (Monetary Authority of Singapore (MAS) 2003; Bank *Van De Nederlandse Antillen* (Central Bank) 2010):

1. Board of Directors and Senior Management should be responsible for their institution's BCM.

   The responsibility for the state of BC preparedness of an institution lies with the Board of Directors and senior management. Senior management is responsible for steering BCM with policies and strategies necessary for the continuation of CBFs. In addition, they should demonstrate that they have sufficient awareness of the risks, mitigating measures and state of readiness by way of a confirmation to the Board of Directors.
2. Institutions should embed BCM into their business-as-usual operations, incorporating sound practices.

   Depending on the scale and complexity of the businesses, institutions could adopt sound BCM practices that include the following components:

   - Clear BCM policy, strategy and budget.
   - Well-defined roles and responsibilities for the BCM programme.
   - BC plan comprising of detailed tasks and activities.
   - Succession plans for critical staff and senior management.
   - BIA or similar process.
   - Programme for the development, implementation, testing and maintenance of BC plan.
   - Programmes for training and awareness.
   - Emergency responses.
   - External communications and crisis management coordination programmes.
   - Coordination with external parties (including authorities, interdependent parties, etc.).

3. Institutions should test their BC plan regularly, completely and meaningfully.

   It is essential to regularly test its functionality and effectiveness. Tests will also familiarize staff with the location of the recovery site, as well as the recovery procedures. Senior management and staff should participate in these exercises and be familiar with their roles and responsibilities in the event of activation. Exercises may include:

   - Desk-top-walk-through exercise to full system test.
   - Staff call-tree activation (with and without mobilization).
   - Back-up site to back-up site exercise (including with external service providers).
   - Alternative arrangements of shared services.
   - Back-up tape restoration.
   - Retrieval of vital records.

4. Institutions should develop recovery strategies and set recovery time objectives for CBFs.

   The establishment of recovery strategies enables institutions to execute their BC plan in an orderly and predefined manner that minimizes disruption and financial loss. Recovery strategies form the basis for defining recovery time objectives of CBFs. Without these clear markers, scarce resources may be inappropriately diverted to less important activities. This may adversely affect the institutions' reputation and survivability. Recovery time objectives may range from minutes to hours. The transparency and sharing of recovery time objectives would help improve service level expectations and understanding among institutions and further contribute towards the mitigation of interdependency risk.

5. Institutions should understand and appropriately mitigate interdependency risk of CBFs.

   When planning for the BC of CBFs, institutions should take into account the interdependencies of these business functions, and the extent to which they depend on other parties. Institutions should also understand the business processes of these parties that support their critical functions, including their BC preparedness and recovery priorities.

6. Institutions should plan for wide area disruptions.

   These financial services look to institutions to demonstrate that they have planned and catered for a wide-area disruption in their BCM. Some planning parameters that institutions may consider include the geographical concentration of institutions, transactional processing activities and dependencies on internal or external service providers. Institutions are responsible for deciding on the need to cater for multiple zones outage scenarios, taking into consideration their respective levels of critical business activities and prudent risk management policies. In addition, they should also consider broadening and deepening their BCM scope to cater for prolonged operational disruptions.

7. Institutions should practice a separation policy to mitigate concentration risk of CBFs.

Critical staff and information are important assets that are difficult to replace quickly. Many institutions assume that the same pool of staff would be available to recover their CBFs at the recovery sites. This may not always be true as disruptions may result in the unavailability of critical staff. Also, identifying alternates to critical staff may not always reduce the risk, especially if both the primary and alternate critical staffs are housed in the same location or zone. It is important, therefore, to find the right balance between mitigating concentration risk and not losing the efficiencies gained from the centralization of business processes and critical staff.

3.7.2 BC Plan from Education Institutions: A Case Study

On April 16, 2007, Virginia Polytechnic Institute and State University (Virginia Tech) experienced one of the most horrific events in American university history. A double homicide had occurred, followed by a mass shooting that left 32 students and faculty killed, with many others injured, and many more scarred psychologically. Families of the slain and injured as well as the university community have suffered terribly from this event. One of the main recommendations from the tragedy is to update and improve the university's emergency response plan. It is recommended that the plan should be more systematic, including conducting risk analysis (threat assessment) in advance and choose a level of security appropriate for the campus. Along with that, the university should update and enhance the plan where students, faculty and staff should also be trained annually about responding to various emergencies (Tridata Division 2009; Flynn and Heitzmann 2008).

In 2010, the school had developed a comprehensive emergency response and continuity plan. The brief description of the plan is as follows (Virginia Polytechnic Institute and State University 2010):

- General purpose

  The plan outlines procedures for managing major emergencies that may have threatened the health and safety of the campus community or disrupt business operations on the local campus. It identifies individuals and departments that have a direct or supporting role in emergency response, and it provides a management structure for coordinating and deploying university resources to handle the event.

  This plan consists of the basic plan, the appendices, and the emergency support function and incident annexes. The basic plan provides an overview of the university's approach to emergency response and operations. It explains the policies, organization and tasks that would be involved with the response to an emergency. The annexes and appendices give definition to the terms and acronyms used throughout the basic plan, and are the location for any supporting figures, maps and forms. The emergency support function appendices focus on detailing the specific responsibilities, tasks and operational actions to complete a specific emergency operations function, while the incident annexes focus on any

additional special planning or response needs beyond the basic response plan for particular event scenarios.

- Scope

  This plan applies to all of the university's students, facilities, staff and visitors. Surrounding community in addition to the campus may be impacted by major emergencies, and if this happens, the university will further cooperate with local, state, and federal officials in their delivery of emergency services. Categories of emergencies or hazards are identified through risk assessment with significance ranking that are most likely to impact the university.

- Priorities

  The plan's response priorities are (1) to protect life safety; (2) to secure critical infrastructure and facilities (in priority order: buildings used by dependent population; buildings critical to health and safety; facilities that sustain the emergency response; classroom and research buildings; administrative buildings); (3) to resume teaching and research programs.

- Response phases

  The university response to a disaster or emergency will generally involve the following phases:

  1. Planning and mitigation. The process of evaluating exposures and developing or refining response plans that will assure an orderly and effective response to an emergency, and for identifying and mitigating areas of vulnerability.
  2. Response. The reaction(s) to an incident or emergency in order to assess the level of containment and control activities that may be necessary.
  3. Resumption. The process of planning for and/or implementing the resumption of critical business operations immediately following an interruption or disaster. During this phase, more in-depth forecasts of the impact will be available, and university-wide priorities for program resumption will be determined.
  4. Recovery/restoration. The process of planning for and/or implementing recovery of non-critical business processes and functions after critical business process functions have been resumed, and for implementing projects/operations that will allow the university to return to a normal service level.

- Emergency notification systems protocols

  The university provides an Emergency Notification System (ENS) which is intended to rapidly circulate emergency information on an incident, and give instructions to the campus population.

- Emergency operations command structure

  The university's emergency response and continuity plan had been coordinated with the town's agencies, local government and organizations. The functional groups in delivering the response and continuity process are:

1. The policy group, which is composed of lead administrators. It establishes policies and procedures as needed to support emergency operations, and determines business recovery and resumption priorities.
2. The Emergency Response Resource Group (ERRG) directs resources in support of emergency response operations, assures the continuity of critical business functions, and implements business recovery and resumption activities. The ERRG convenes at the Emergency Operations Center (EOC).
3. Satellite Operations Centers (SOCs), located in the administrative headquarters. Deans, Vice Presidents and Vice Provosts, gather emergency impact data from their constituent departments, account for their personnel, transmit reports to the EOC, disseminate emergency instructions to constituents, and develop and implement business continuity, resumption and recovery plans.

In addition to these groups, there are also essential roles who will direct these groups, supported by essential personnel.

- Business recovery

  Even when emergency response activities are nearing completion, business recovery activities may continue for weeks or months after the event. Business recovery activities include reestablishing complete services and functions following a major incident and recovering extraordinary costs caused by the event. Furthermore, recovery priorities should be established as follows:

  1. Immediate recovery (true continuity) is essential;
  2. Recovery required within 24 hours;
  3. Recovery required between 24 and 72 hours;
  4. Recovery not required within 72 hours.

- Exercises and training

  Trained and knowledgeable personnel are essential for the prompt and proper execution of the plan. All personnel will be provided with the necessary training to execute those responsibilities in an effective and responsible manner. Training on university-level emergency response roles and the incident command system will generally be coordinated by the Director of Emergency Management.

  Exercises will be conducted as needed which allow all persons involved in emergency response to practice their roles and to better understand emergency operations and their responsibilities under emergency conditions. University-wide exercises will be held at least once per year, and will consist of tabletop, practical and full-scale staged events as deemed appropriate.

3.7.3 BC Plan for Influenza Pandemic: A Review

A pandemic is an epidemic or outbreak of infectious disease that spreads through populations across a large region; for instance a continent, or even worldwide. A flu

pandemic could occur when a new flu virus emerges and starts spreading as easily as normal seasonal flu. As the virus is new, the human immune system will have no pre-existing immunity. This makes it easier for people to contract the new flu and experience more serious symptoms than that caused by normal seasonal flu. Current viruses that had spread across a large region (particularly in Asia) are the influenza A (H1N1), the SARS incident in 2003, and the avian flu (H5N1) (SPRING 2009).

According to some studies, no one could predict when a flu pandemic will occur. When it does occur, the impacts may be felt in various ways. Regarding its possible general impact, public gatherings may be discouraged, people with flu-like symptoms may not be allowed in public places, public transport may be disrupted and regular updates and clarifications may be necessary. As for the business impact, supplies may be disrupted, the number of customers may drop, likely increase of electronic communications use which may lead to overloaded communication systems and some staff in any organization may be absent from work (SPRING 2009).

Based on these likely impacts, companies are encouraged to ensure their business remain viable in the event of an outbreak. BCP should be developed with further considerations on how to operate their business with minimal face to face contact between staff, staff and customers, and with suppliers; how to operate business effectively with key members of staff being absent from work; and how to operate if supply chains are disrupted. Moreover, the key risks to the company that need to be addressed in BCP are (SPRING 2009):

- Employees
- Processes and business functions (e.g. production, sales and marketing, etc.)
- Business infrastructure (e.g. offices, shops, factories, equipment, etc.)
- Stakeholders (shareholders, suppliers, customers, etc.)
- Communications, both internal and external

The Singapore government had proactively taken an approach to overcome this crisis through initiatives such as the Flu Pandemic Guide for small and medium-sized enterprises (SMEs) in 2006. The BC guideline developed by a Singapore standards agency provides these contents particularly for handling flu pandemic (Low et al. 2010a; Singapore Business Federation 2006; SPRING 2009):

3.7.3.1 Annex section

This section describes:

- Information about personal hygiene awareness, as an example: correct hand washing procedures; basic information on sanitization such as disinfectants, recommended use and their precautions.
- Contact list of key customers, key suppliers/vendor/contractors and others.
- Contact list of key personnel and key organizations for information and assistance on flu pandemic.
- Description about roles and responsibilities of the Flu Manager.

- Procedures upon detection of visitors and staff who are unwell. These include procedures of (1) Visitor detection and isolation; (2) Staff unwell at workplace; (3) Staff unwell outside workplace and (4) Contact tracing.
- Forms such as temperature screening, notification form (for suspected flu case at work), and body temperature monitoring log.

3.7.3.2 BC Plan for Flu Pandemic Contents

- Description about the alert level code. There are five levels of codes, which consist of:

  1. Green—isolated overseas or local cases of animal-to-human transmission. Threat of human-to-human infection remains low.
  2. Yellow—slight human-to-human transmission. A small risk of it being imported here, but has not resulted in sustained spread.
  3. Orange—evolves into human disease. WHO confirms several outbreaks in one country, spreading to other countries. Deaths are expected. Local confirmation of new cases and evidence of more than one transmission has occurred.
  4. Red—widespread infection. Increase in deaths has occurred. Healthcare system likely to be overwhelmed and essential services are added to ensure full operational capacity.
  5. Black—high death rates reported. Economic activities are severely disrupted, as panic sweeps through the community.

- Description of recommended actions for companies

  1. Priority tasks for various levels:

     (a) Green—to set up a team to oversee BCP.
     (b) Yellow—appoint a Flu manager.

  2. Action plans are written for every alert level.

3.8 The Need for BCM

According to a survey on trends in business continuity, it was found that BCM has become mandatory to maintain customer confidence and a competitive edge. The threat of interruption and the need to respond promptly has manifested itself, where a vast increase in regulatory requirements and a mandate from customers for BC plan development has occurred. Organizations are expected to manage the BC process more collaboratively, be driven to complete their BC plans and include it in Requests for Proposals (RFP) and Requests for Information (RFI) (BUCORIM 2008).

There are several sources of external influence that are encouraging an increased focus on business continuity. According to respondents questioned for a report conducted by the Economist Intelligence Unit (EIU 2007), customers are the stakeholder that is viewed as most important in driving decisions about business continuity, with 59% citing them as a significant influence. Moreover, in the supply chain relationships that are getting complex and more dependent, customers will most likely ask about a detailed scope of BC plan, whether the supplier has it in place and would request evidence of compliance with particular policies.

In addition to customers, pressure from regulators is also becoming more distinct. Regulators are viewed as the second most important external influence over decisions about BC, with 58% seeing them as significant in the regard. This figure rises to 72% from respondents who are in the financial services sector (EIU 2007).

3.8.1 Benefits of BCM

Previous section of this chapter had described the relationships between BCM and other concepts. Table 3.4 summarizes the distinction between these concepts based on their main focus and key methods.

Whilst BCM is able to help firms to have a response for major disruptions that may threaten their business activities, the Business Continuity Institute (2007a) found that there are other benefits that can be gained by embracing BCM as a management discipline in an organization. Firstly, BCM will help address some key risks in the firm and help them achieve compliance. Secondly, BCM can be used as a competitive advantage to gain new customers and to improve margins by using it as a demonstration of "customer care". Thirdly, a thorough review of the business through Business Impact Analysis (BIA) can highlight business inefficiencies and focus on priorities that would not otherwise have come to light. And last but not least, firms providing services or goods recognize that keeping customers through a more reliable service is cheaper than tempting back the deserters after an interruption. Other studies have also found various benefits of implementing BCM in an organization. Table 3.5 shows the BCM benefits from various studies. In addition, the table shows that BCM's main focus and key method of conducting Business Impact Analysis plays an important role and provides positive implication for an organization that implements BCM.

Table 3.4 BCM distinction with other related concepts

	BCM	Risk management	Crisis management	Disaster recovery
Main focus	BCM is concerned only with events that cause a significant business disruption, where it is mainly concerned with the impact of an event and the time required for an organization to return to normal business operations	A thorough organization-wide identification and assessment of risks and evaluating risks in relation to their likelihood and impact before identifying an appropriate risk response	Crisis management focuses on the immediate activities which need to be considered when the incident occurs. At most, the crisis management planning phase deals with the first couple of hours of the incident occurring, detailing who the key decision makers are, who will talk to the customers/clients/regulators and when this will be conducted	Disaster recovery is a focus on technology-based problems triggered by external factors
Key method	Business impact analysis; and identifying critical business function (CBF) and minimum business continuity objective (MBCO)	Risk analysis and assessment; identifying risk response	Risk analysis and contingency planning; the sensing of early warning signals that announce the possibility of the crisis	Contingency planning; emphasize on recovery of the core operations

Sources: Collier (2009), Drennan and McConnell (2007), BCI (2007a), Foster and Dye (2005), Devlin (2007), Smith (2003), Elliott (1999), McCrackan (2005)

3.8.2 Challenges in BCM

Although BCM is considered as necessary to be implemented in organizations, there are several issues regarding the challenges of its implementation. Robinson (2009) viewed that the recent economic recession would be a challenge in implementing BCM. Recession has delayed or reduced BCM uptake; with top management viewing it as a discretionary spend. Moreover, only a minority will recognize that recession increases the need for BCM, with cutbacks reducing operational resilience and scarce liquidity eroding financial tolerance. Nonetheless, when a senior management team still has a strong commitment in sustaining its business resilience, and perceiving the recession-BCM link being strong enough, these can be a strong contributory factor to maintain its BCM. Moreover, Molinier (2009) opined that these economic conditions should be viewed as an opportunity to demonstrate how the companies can provide resilience whilst streamlining processes and adopting a cost-benefit approach that demonstrably support business objective.

Table 3.5 BCM benefits

Description	References
Firms that invest in developing a BC tend to create value for the firm, particularly maintaining their stock price. For global 1000 firms, there is a high probability of a crisis resulting in substantial decline of stock price during any 5 year period	INTERCEP (2007), FM Global (2003)
Effective BCM by corporate management can actually lead to an increase in shareholder value	Knight and Pretty (1996), Knight and Pretty (2005)
Corporate resilience will be a competitive advantage in the twenty-first century. Globalization, technological complexity, interdependence, terrorism, climate and energy volatility, and pandemic potential are increasing the level of risk that societies and organizations now face. Risks also are increasingly interrelated; disruptions in one area can cascade in multiple directions. The ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption will be a competitive differentiator for companies and countries alike in the twenty-first century. Moreover, it is a contributor to profitability, shareholder value and competitiveness	Van Opstal (2007), Council on Competitiveness (2006)
Implementing a BC plan may also have legal significance for a corporation. Because BC recognizes risk and mitigates it, the creation and implementation of such a plan may help a corporation discharge its corporate governance responsibilities to customers and shareholders alike. BC is a strategic investment, and its dividends will be evident during an attack, and economically and legally, in the aftermath of a terrorist event	Directors and Boards Magazine (2006)
The business impact of crises can run into the billions. The 1990 Wall Street Blackout and the 1992 Chicago flood are two examples. The article argues that initiating a BIA can have positive implications for the bottom line, especially in the event of a disaster	Watkins (1997)
Rewards of corporate resiliency through BCM • Increased productivity and innovation often supported by more effective internal communications, streamlined processes, more adaptive workplaces, better workflows and increased employee morale • Protected revenue flows as a result of plans to protect key assets—Inventory, property/plant, equipment and intellectual property—as well as sustain core operations • Expanded customer base and increased customer retention, as both individual consumers and organizations place an increasing focus on safety, security and preparedness • Lower operating expenses as a result of lower insurance and legal costs, less theft, reduced employee turnover and more competition among suppliers • Reduced cost of capital as both equity and debt markets (including key rating agencies) increasingly evaluate	Raisch, Statler and Burgi (2007)

(continued)

Table 3.5 (continued)

Description	References
corporate preparedness and resiliency • Stronger reputation, as a result of both the application and communication of resilience • Better regulatory compliance and governance both internally and in terms of external review	
When made known to insurance companies, a corporate preparedness program can result in relatively lower insurance premiums and better policy terms	Raisch and Statler (2006)
BCM can help to avoid losses of important business data, which can result in significant losses in terms of both existing and future business as well as liabilities to customers, investors and legal authorities. IT downtime costs can range from $1 million to over $6 million annually for companies that focus on database in its business	Hinton (2000)

In accordance with Continuity Central's survey to BC professionals (Continuity Central 2011), the biggest challenge in implementing BCM was lack of resource for the implementation. The second biggest challenge was the difficulties in obtaining senior management support and input. Thirdly, getting the wider organization to buy-in to BC and to provide support to the process was another challenge that needs to be considered. Following these top three challenges, other reasons are: organizational cut backs and changes; technology issues; testing and exercising issues; compliance, regulations and auditing; and culture change. These findings provide important feedbacks to those who have implemented BCM and who are in the phase of initiating it.

3.9 Summary

This chapter provided a review on BCM, starting from its historical development, its relationships with other concepts, its main principles and methodology, to its implementation in various sectors that shows the necessary need of the concept in an organization.

As an act of anticipating incidents that will affect mission-critical functions and processes for the organization, and ensuring that it responds to any incident in a planned and rehearsed manner, BCM has evolved from a technology-based disaster recovery approach to a value-based drive for business resilience. It is also viewed as a unifying process that includes various concepts for overcoming crises.

BCM is considered as a management system that, similar with other management systems, needs influential factors such as organizational culture, involvement, resources, flexibility and shared commitments for its effectiveness. Moreover, these approaches are embedded in its main principles and methodology.

Currently, BCM is widely adopted in various firms from various sectors. Regulations and international standards have been developed for this concept and methods in assessing the level of BCM preparedness have also been established. The need for BCM is currently supported by various drivers and although there are some challenges in implementing the concept, the benefits of BCM are worth mentioning.