# OPEN UNIVERSITY OF CYPRUS

## Hellenic *Open University*

## Faculty of Economic Sciences and Management

***ENTERPRISE RISK MANAGEMENT***

**MASTER THESIS**

# Guidelines for implementation of a Business Continuity Management Programme

**Gerasimos Tsintzos**

**Supervisor: Dr. Anastasis Petrou**

**May 2022**

# Summary

Business continuity management (BCM) has evolved since the 1970s in response to the technical and operational risks that threaten an organization's strategic recovery from hazards and interruptions. The dissertation addresses the lack of practical examples, hints & tips and of the challenges faced and managed during the realization of BCM programmes by collecting data and analytical insights from practitioner lived experiences. Collection of such data and knowledge development could ensure that both practitioners and requestors/decision makers have a common approach and understanding that will secure and justify the added value, effort and cost of the implementation of a BCM programme.

The objectives of the research are:

1. Indicate a structured approach for the implementation of a BCM programme and a way to integrate BCM in organization's operational model
2. Address challenges and gaps identified, during the implementation of such programmes, through live experience and the realization of related surveys
3. Provide guidance and examples for the implementation of all stages of BCM lifecycle in compliance with international standards and industry practices
4. Include roles, responsibilities and profiles of key stakeholders supporting such implementation

The methodology research applied in this dissertation is qualitative and involves collecting and analyzing data from the below presented sources:

a. Literature Review
b. Lived experience by the execution of projects and implementation of BCM programmes in a variety of organizations and industries
c. Questionnaire covering the entire BCM lifecycle aiming to identify and record the main challenges faced and managed by BCM practitioners and involved stakeholders during such implementations
d. Structured and unstructured interviews with BCM professionals

# Acknowledgements

I would like to express my gratitude and appreciation to all the people that support and assist me in developing this research study.

The material that was developed and collected for the materialization of this study is the outcome of many years of efforts and numerous projects and implementations in various organizations. Many of the practitioners that responded were former colleagues and associates and I greatly appreciated and enjoyed the discussions that we had during the extremely long interviews, as some of you said.

I really enjoyed very much our individual sessions.

Extremely grateful to my BC mentor that advised me wisely for certain parts.

Special thanks to my supervising professor, Dr. Anastasis Petrou for his support and understanding.

# Table of Contents

# Chapter 1

# Introduction

Many organizations believe that their investment in Business resilience, its constituent parts and their operational management is adequate. However, the experience shows they still suffer incidents, accidents, negative media exposures, costly disruptions and subsequent shareholder value, revenues and market image losses due to an inability to effectively establish Business Continuity Resilience to prevent incidents occurring or recover their critical service and business functions and/or production following an incident or corporate crisis. This message is constantly being reinforced daily by reports within the media.

These issues coupled with corporate governance, increased regulatory and legal accountability, natural disasters, global terrorist threats, cyber security attacks and the increasing awareness and business sensitivity in continuity issues has focused the attention of senior management on the appropriateness and cost effectiveness of the current Continuity integration and proven Resilience of their business.

Through the years BCM has evolved as a separate discipline and there was an increasing effort to identify and standardize its requirements and phases. Consequently, different standards have been developed starting with PAS56, BS25999 and reaching to ISO22301. A number of guidelines have also been issued by different organizations such as Business Continuity Institute (BCI), Business Continuity Management Institute (BCMI) and other bodies to provide guidance to practitioners on how to embed BCM.

An effective business continuity programme supports the strategic objectives of the organization and builds the capability to continue business operations in the event of

any disruption. The programme should include the identification of the prioritized activities and their respective RTOs & RPOs, the risks and threats, the development of the necessary response structures and the plans to address crises and disasters. The programme needs to be adaptable to any changes occurring in the internal and external operating environment and should promote continuous improvement.

Yet, additional research about BCM implementation in different organizational contexts remains of value inclusive of a focus on collecting data and analytical insights about practitioner lived experiences and by addressing the lack of practical examples, hints & tips and of the challenges faced and managed during the realization of BCM programmes.

There is paucity of understanding and indeed a strategy formulation-implementation gap in knowledge about BCM programmes in relation to the application of a new methodology's principles and requirements from the perspective of practitioner lived experience with BCM methodology implementation as core data collection method. Collection of such data and knowledge development form their analysis could be of value in ensuring that both practitioners and requestors/decision makers have a common approach and understanding that will secure and justify the added value, effort and cost of the implementation of a BCM programme.

Hence, the aim of the research is to bridge the gap between theory and practice by providing guidelines, deliverables, examples and issues to be managed in the realization of the phases of BCM programme through lived experience.

This gap often results in a number of implications that prohibits an organization to respond and recover effectively in case of any major negative event impacting its operational status. Indicatively some of these negative implications may be:

i. Confusion among stakeholders / decision makers related to the outcome & deliverables
ii. Inadequate BCM Programme implementation
iii. Lack of commitment, resources and effort
iv. Extended time-consuming projects & incorrect budget allocation
v. No scalability or clear objectives in the development of a resilient framework

vi. Failure to implement appropriate recovery solutions
vii. Failure to recover effectively from disasters resulting in major Losses (Revenue, Brand Image, Market)

Hence, the objectives of this research are:

1. Critically evaluate methodologies in available literature for the development of a BCM programme
2. Indicate a structured approach for the implementation of a BCM programme and a way to integrate BCM in organization's operational model
3. Address challenges and gaps identified, during the implementation of such programmes, through live experience and the realization of related surveys
4. Provide guidance and examples for the implementation of all stages of BCM lifecycle in compliance with international standards (ISO) and industry practices
5. Include roles, responsibilities and profiles of key stakeholders supporting such implementation

As part of this study, phenomenological analysis was also used to acquire the knowledge that is necessary to make a substantial and effective contribution to answering the research gap and to bridge the theory with the practice.

Phenomenology (Anosike Ehrich & Ahmed:2012, Neubauer, Witkop and Varpio:2019, Gill:2014) is a form of qualitative research that focuses on the study of an individual's lived experiences within the world. It can be defined as an approach to research that seeks to describe the essence of a phenomenon by exploring it from the perspective of those who have experienced it. The goal is to describe the meaning of this experience both in terms of what was experienced and how it was experienced.

The guidelines presented in this dissertation was the outcome of lived experiences (Ranse; Arbon; Cusack; Shaban; Nicholls:2020, Kempster:2006, Schwandt, Burgon:2006) of several BCM practitioners working in the implementation of BCM programmes in a variety of organizations of different sizes in many industries. The

BCM practitioners interviewed in the scope of this research are accredited professionals in the BCM discipline from different cultural and working environments with extensive experience of implementing BCM programmes in a variety of industries. The interviews and discussions made were based on a specific questionnaire constructed in a way to cover all phases of the BCM lifecycle as these are described in the various industry and international standards. The aim of those interviews and discussions were not only to identify and present the different phases and their requirements but also to provide important practical directions, advices and examples for the efficient implementation of a BCM programme.

Hence, the dissertation is structured in chapters respectively to the phases of BCM lifecycle providing requirements, approach and deliverables along with practical advices (hints & tips) and examples based on the numerous implementations done by the interviewed practitioners.

# Chapter 2

# Abbreviations & Terminology

The chapter includes some major abbreviations that are used in the dissertation along with a terminology that will assist readers to comprehend some key terms referenced in the next chapters.

## 2.1 Abbreviations

| | |
|---|---|
| **BC** | Business Continuity |
| **BCM** | Business Continuity Management |
| **BCMS** | Business Continuity Management System |
| **BCP** | Business Continuity Plan |
| **BIA** | Business Impact Analysis |
| **CM** | Crisis Management |
| **DR** | Disaster Recovery |
| **ICT** | Information & Communication Technology |
| **IM** | Incident Management |
| **IT** | Information Technology |
| **KPI** | Key Performance Indicators |
| **MTPD, MAO** | Maximum Acceptable Period of Disruption, Maximum Acceptable Outage |

| | |
|---|---|
| **POC** | Point of Contact |
| **RA** | Risk Assessment |
| **RM** | Risk Management |
| **ROI** | Return on Investment |
| **RPO** | Recovery Point Objective |
| **RTO** | Recovery Time Objective |

## 2.2 Terminology

| Terms | Definition |
|---|---|
| **Activity** | Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services |
| **Business Continuity** | Business Continuity is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. |
| **Business Continuity Management** | An holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. |
| **Business Continuity Management System** | Business Continuity Management System of an organization is part of the company's overall Management System. Its scope and objectives are to establish, implement, operate, monitor, review, maintain and improve business continuity within the organization. |
| **Business Continuity Plan** | Business Continuity Plan is documented procedures that guide ORGANIZATION to respond, recover, resume, and restore to a pre-defined level of operation following disruption. Typically this covers resources, services and activities required to ensure the continuity of critical business functions. |

| Terms | Definition |
|---|---|
| **Business Impact Analysis** | Business Impact Analysis is a process of analyzing business (operational) activities and the effect that a business disruption might have upon them |
| **Major Changes** | Changes implemented within the organization with significant impact on its operations. These include changes in key IT Systems and applications, re-organization and restructure of key departments and operations, expansion to new markets, introduction of new services, outsource of critical services of activities to third parties etc. |
| **Maximum Acceptable Outage (MAO)** | Maximum Acceptable Outage is the time it would take for adverse impacts to become unacceptable. These adverse impacts might arise as a result of not providing a product/service or performing an activity. |
| **MaximumTolerable Period of Disruption (MTPD)** | Maximum Tolerable Period of Disruption is the time it would take for adverse impacts to become unacceptable. These adverse impacts might arise as a result of not providing a product/service or performing an activity. |
| **Nonconformity** | Non-fulfillment of a requirement |
| **Products and Services** | Beneficial outcomes provided by an organization to its customers, recipients and interested parties |
| **Prioritized Activities** | Activities to which priority must be given following an incident in order to mitigate impacts |
| **Recovery Point Objective (RPO)** | Point to which information used by an activity must be restored to enable the activity to operate on resumption |
| **Recovery Time Objective (RTO)** | Period of time following an incident within which<br>• a product or service must be resumed, or<br>• an activity must be resumed, or<br>• resources must be recovered |
| **Risk Appetite** | The level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it. |
| **Risk Identification & Assessment** | The process of identifying risk events & assessing their risk exposure within existing business & support processes as well as new products/ initiatives |
| **Risk Management** | The continuous process applied across an organization to identify risks and manage them to be within its appetite to provide reasonable assurance regarding the achievement of its goals. |

# Chapter 3

# Phenomenology & Lived Experience Literature Review

The use of qualitative research methods for the data gathering and analysis has significantly increased in popularity over the past decades (Strauss & Corbin, 2006). In contrast to quantitative inquiry where representations of the world are symbolized numerically, qualitative inquiry offers representations of the world which are primarily linguistic (Heppner, Kivlighan, & Wampold, 1999). Applying a constructivist approach within this qualitative method of inquiry allows for the study of the "how-and sometimes why-participants construct meanings and actions in specific situations" (Charmaz, 2006, p. 130). This type of investigation allows for the subtleties of human experience to float to the surface. Attention to subtle and, at times, nebulous, experience requires the researcher to "sustain a fair amount of ambiguity" through flexibility and openness towards the data.

Although human experience is the main epistemological assumption for qualitative research, the concept of lived experience has special methodological significance in phenomenology (Creswell, 2014; Patton, 2015). Lived experience refers to the world of objects around humans, how they perceive them, and the experience of oneself, body and relationships. This is the interaction between the self and perceptual environments (von Eckartsberg 1998, Van Manen 1990) states that "anything that presents itself to consciousness is potentially of interest to phenomenology, whether the object is real or imagined, empirically measurable or subjectively felt".

A broad description that would be understood as faithful to its general usage is the following:

“Lived experience involves representation and understanding of a researcher or research subject’s human experiences, choices, and options and how those factors influence one’s perception of knowledge. . . . [it] responds not only to people’s experiences, but also to how people live through and respond to those experiences. . . . Lived experience seeks to understand the distinctions between lives and experiences and tries to understand why some experiences are privileged over others” (Boylorn, 2008: 490).

The aim of this study is to bridge the gap between theory and practice by providing guidelines, deliverables, examples and issues to be managed in the realization of the phases of BCM programme through lived experience. Qualitative inquiry and analysis fit this purpose with stronger sensitivity than a quantitative methodology could offer. Also there exists little research on the topic; therefore, qualitative methods are suited for this study.

## 3.1 Phenomenology

Phenomenology relies on paradigm of personal insight and subjectivity, and it places a greater emphasis on the individual's own experience and interpretation of events.

Transcendental Phenomenology: It examines the essences experienced by consciousness in the context of particular experiences and makes recommendations. The concept of reduction lies at the heart of Husserl's phenomenological approach. Husserl often used the terms "transcendental" and "phenomenology" interchangeably to refer to the unique eidetic reduction employed to explain the phenomena reported. The invariant or eidetic elements of a given occurrence are explained using the approach of creative variation (examples of instantiation and comparative investigation).

The challenge in transcendental phenomenology is to engage in the study of a person’s lived experience of a phenomenon that highlights the universal essences of that phenomenon (Brian E. Neubauer, Catherine T. Witkop and Lara Varpio, 2019). This requires the researcher to suspend his/her own attitudes, beliefs, and suppositions in order to focus on the participants’ experience of the phenomenon and identify the essences of the phenomenon. The researcher is to stand apart, and not

allow his/her subjectivity to inform the descriptions offered by the participants. This lived dimension of experience is best approached by the researcher who moves from the participants' descriptions of facts of the lived experience, to universal essences of the phenomenon at which point consciousness itself could be grasped.

Hermeneutic Phenomenology: It is concerned with the exploration of personal experience and necessitates the provision of a description or interpretation of the meanings of occurrences encountered by participants in research. In hermeneutic phenomenology, the living world or human experience as it is lived is the subject of investigation. To create meaning and achieve a feeling of understanding, the emphasis is on illuminating subtleties and insignificant components of experience that may be taken for granted in our daily lives (Wilson & Hutchinson, 2019).

Hermeneutic phenomenology studies the meanings of an individual's being in the world, as their experience is interpreted through his/her lifeworld, and how these meanings and interpretations influence the choices that the individual makes. This focus requires the hermeneutic phenomenologist to interpret the narratives provided by research participants in relation to their individual contexts in order to illuminate the fundamental structures of participants' understanding of being and how that shaped the decisions made by the individual. The hermeneutic phenomenology recognizes that the researcher, like the research subject, cannot be rid of his/her lifeworld. Instead, the researcher's past experiences and knowledge are valuable guides to the inquiry.

The most significant distinction between transcendental phenomenology and hermeneutic phenomenology is the emphasis on individual experiences rather than the idea of being. According to Reiners, the central question in Husserl's phenomenology was "what do we know about ourselves as individuals?" Because of this, Husserl devised descriptive phenomenology, in which daily conscious experiences were recorded without regard to preexisting ideas, which were either put aside or omitted entirely. On the other hand, (Cristina Lafont, 2015) asserts that hermeneutic phenomenology is a subset of transcendental philosophy in its own right. Its goal is to demonstrate that the hermeneutic circumstances of interpreting anything as meaningful are the ultimate transcendental conditions of every human experience,

regardless of the subject matter under consideration. Nonetheless, once these hermeneutic circumstances are eventually exposed, they are discovered to be fundamentally different from conventional transcendental conditions. Instead of traditional transcendental conditions, they reveal the radical facticity and situatedness of all human experience.

Existential Phenomenology: It examines one's consciousness as a conscious being. This form of phenomenology appeals to the awareness of all people everywhere. Everyone who considers themselves an existential phenomenologist believes that philosophy should not be undertaken from a detached, objectivist, disinterested, or disengaged position. This is because, according to them, some occurrences can only be seen by someone who is involved with the world in the appropriate manner (Warthal, 2006). The work of existential phenomenologists has included discussions of the meaning of being (as in Heidegger) and the function of the lived body in seeing reality.

Existential phenomenologists all share the view that philosophy should not be conducted from a detached, objective, disinterested, disengaged standpoint. This is because, they contend, certain phenomena only show themselves to one who is engaged with the world in the right kind of way (Warthal, 2006). Existential phenomenologists have included descriptions of the meaning of being (Heidegger), the role of the lived-body in perception (Merleau-Ponty).

The ground that keeps it distinct to other schools of phenomenology is its rejection of Husserl's belief of possibility of complete reduction and its firm belief on the attempt to concentrate upon re-achieving a direct and primitive contact with the world. For this, existential phenomenology stresses on the description of everyday experience as it is perceived by the consciousness of the individuals.

Interpretative Phenomenology: It aims to explore in detail how participants are making sense of their personal and social world, or how individuals make meaning of their life experiences. Interpretative phenomenological analysis is similar to other phenomenological approaches in that it examines human lived experience; however, the distinction relies on the idea that interpretative phenomenological analysis

focuses on the meanings that particular experiences, events, and states hold for participants.

Interpretative phenomenological analysis assumes that people are self-interpreting beings (Taylor & Charles, 1985), which means that they are actively engaged in interpreting the events, objects, and people in their lives. In line with Heidegger, interpretative phenomenological analysis attempts to explore personal experience with a focus on an individual's personal perception or account of an object or event, as opposed to an attempt to produce an objective statement of the object or event itself (Smith, Flowers, & Larkin, 2009).

The primary concern of interpretative phenomenological analysis researchers is to elicit rich, detailed, and first-person accounts of experiences and phenomena under investigation (Smith et al., 2009). To achieve that, the most popular method used is semi-structured, in depth, one-on-one interviews. Semi-structured interviews allow the researcher and the participant to engage in dialogue in real time. They also give enough space and flexibility for original and unexpected issues to arise, which the researcher may investigate in more detail with further questions.

## 3.2 Lived Experiences

The literature argues that there is a gap between theory and practice. However, there are multiple approaches to filling the gap between theory and practice, including the deployment of research. Moreover, data plays an integral role in filling the void between theoretical and practical situations. Lived experiences have played a pivotal part in generating the data that is instrumental in bridging the gap between practice and theory. The data from lived experiences results from the lessons and information that people accumulate when they experience phenomena. Such information is relevant to the subject under study. For example, management research or practice can reduce the gap between its theory and practice through the exploration of the lived experience of other managers, which contains crucial lessons about practical situations that have not been captured in theoretical concepts.

Literature further states that lived experiences can bridge the gap between theory and practice in two significant ways. The first value results from the exploration of other

people's lived experiences. Such a move entails documents that capture the experiences of people that have witnessed an occurrence. From such a perspective, lived experiences are part of qualitative studies. Data can be captured through the interaction with people that experienced phenomena. For example, a researcher can interview such individuals to capture data (Moser & Korstjens, 2018). However, the only difference stems from the formers and latter's exploration of practical and theoretical concepts, respectively. The second value originates from the exposure of researchers to phenomena and incidences, prompting them to collect data first-hand. When people experience events or phenomena, they enhance their personal comprehension of the phenomenon and capture experiential information that can help other studies access practical knowledge concerning a phenomenon (Attia & Edge, 2017). The two approaches to harnessing lived experiences play an integral role in reducing the gap between theory and practice because of their wealth of practical information that might have been missed in theoretical concepts.

Moreover, literature cites the value of lived experiences in turning learners into teachers. Such a phenomenon is evident among people who experience events and occurrences despite lacking a significant wealth of theoretical knowledge. While such parties have limited theoretical information concerning an incidence, they have experienced the event and can teach others practical knowledge concerning actual phenomena. For example, in a classroom setting, teachers can turn to learners and vice versa. Specifically, while teachers possess more advanced theoretical knowledge than the student, the latter might experience a phenomenon, hence acquiring more practical knowledge than the former (Luke, 2018). Hence, lived experience introduce the use of practical and witnessed knowledge in our everyday life.

Literature also cites the value of lived experiences in bridging the gap between theory and practice among organizations through the development of a contrary perspective concerning the theoretical argument. Such a phenomenon is evident among different stakeholders in the corporation (Esmail, Moore, & Rein, 2015). For example, most studies focus on organizations and businesses, often leaving out significant stakeholders such as customers. While studies might theorize customer satisfaction, the theoretical argument does not necessarily capture the client's feelings because of

the failure to incorporate the experience of the customer. Contrarily, accommodating stakeholders in studies provides a unique perspective to the study, hence capturing stakeholders' needs that cannot be captured from a contrary lens.

Apart from the development of contrary perspectives to disciplines, lived experiences also create the chance to incorporate other factors such as social structures and their effect on how people perceive events. People that have experienced events often develop meanings of such occurrences. Such meanings might include the lessons learned from the experiences (Christie et al., 2015). Noteworthy, multiple dynamics, including social structures, influence the meaning people assign to events. Learning about such meaning plays an integral role in comprehending the meaning of phenomena from the perspective of people that experienced them. Consequently, the captured data relates to the organization or agency on which the research is based. Most importantly, the meaning assigned to lived experiences by the people who witnessed a phenomenon is vital in unearthing the practical needs of a setting.

The value of lived experiences arises from the relevance of the data captured through the process. While theoretical data is universal, it does not capture the difference that results from the variation in context (Esmail, Moore, & Rein, 2015). Consequently, theoretical information turns away from practical data because of the failure to incorporate contextual variation that helps corporations deploy arguments that apply specifically to the discipline context. Moreover, the tendency of lived experiences to revolve around specific contexts and environments enables agencies and corporations to capture data that is relevant to the environment, hence narrowing the gap between theory and practice. Therefore, the information acquired through lived experiences is relevant to the context and has practical components that have not been captured in theoretical frameworks.

The value of lived experiences is evident in multiple corporate activities such as strategy, planning, and auditing. Specific to auditing, lived experiences play an integral role in reducing the void between practical and theoretical concepts. Researchers can use lived experiences of other people that have engaged in management accounting studies. Akin to other subjects, auditing is significantly affected by context and significance. Auditing, a topic of management accounting, is hardly cited in pieces of

literature from other sectors. Moreover, most accounting schools deploy multiple standard books that mostly entail abstract cases (Humphrey, 2014). Consequently, there is a wide gap between auditing theory and practice. However, the deployment of lived experiences in research activities and corporate practices helps reduce the margin because of the access to significant and context-relevant data, which stems from the lessons drawn by previous researchers in accounting and auditing studies. Due to their exposure to accounting and auditing studies, accounting researchers possess a wealth of information concerning practical aspects of the subject, across which they come during their field research.

Most accounting and auditing theoretical models only capture universal aspects of the subject, which might not necessarily capture the emotional and cultural sensitivities that affect the subjects. However, the application of lived experiences allows researchers to learn from the lessons of previous studies (Humphrey, 2014). Such information is often contextualized to a specific setting to incorporate the emotional and cultural sensitivities that affect auditing and set study environments apart from each other. Specific to auditing research, lived experiences help researchers understand practical factors that affect the process. For example, lived experiences might feed researchers with research information that lacks theoretical concepts. Most importantly, such practical information about auditing research is context-specific and applies to various environments and territories.

The value of lived experiences in auditing research stems from the practical appraisal of measurement systems used to capture data from studies. Lived experiences emerge as the literature from which a researcher gains information about the outcomes of measurement systems that previous researchers deployed to capture performance data (Agyemang & Broadbent, 2015). From such a perspective, lived experiences reduce the gap between conceptual and practical auditing research information. The approach helps subsequent researchers learn from the works of previous studies to determine the outcomes of various studies and performance measurement methods. Consequently, the lessons help subsequent study personnel to understand practical research approaches that can yield positive performance measurement outcomes.

Literature asserts that lived experiences can also be accessed from the progress and history of previous auditors. Subsequent auditors can learn from documents of the previous colleagues to learn practical concepts in the subject that miss in auditing theories. For instance, certain theoretical arguments and explanations might not necessarily be applicable in practical settings. Moreover, due to the lack of auditing practice, auditors might fail to determine the practical pointers that guide them towards audit factors in the field (Harvey & Kitson, 2015). From such a lens, lived experiences reduce the gap between auditing theory and practice through the development of a course map that guides new auditors on the auditing course. In essence, new auditors learn about the practical coordinates, anticipated contours, and potential challenges in the course of auditing practice. Most importantly, lived experiences expose auditors to auditing implementations, which are the most practical aspects of the practice. Consequently, new auditors learn from previous ones about evident processes and practices.

Therefore, the value of lived experiences is evident in the effort to improve audit systems among organizations. While the auditing conceptual framework theorizes ways of improving audit systems, they fail to incorporate multiple practical concepts. For instance, most auditing theories fail to incorporate local factors that set localities apart from each other (Harvey & Kitson, 2015). Therefore, lived experiences accommodate local standards, including local audit systems and standards. Moreover, lived experiences give organizations and new auditors the to exercise experiential learning and reflective practice. Experiential learning stems from the deployment of the lessons learned by previous auditors that have documented their experience in the auditing practice. Contrarily, reflective practice originates from the reflections of previous auditors, which help in the visualization of practical auditing concepts.

Lived experiences also assists in the development of new insights and knowledge concerning the auditing practice. While subjects unearth new information with time, the novel insights and visibilities that stem from lived experiences possess significant percentages of practical auditing information. Such a value of lived experiences is particularly evident among auditing practices that involve immigrant families. The analysis of lived experiences of the immigrants comes with the visualization of new

insights (Lehman, Annisette, & Agyemang, 2016). Most importantly, auditing lived experiences in immigration departments captures challenges that evolve and develop around immigration, including risks. Responsibilization characterizes the working of immigration practices, with governments often delegating the immigrant management responsibility to agencies. However, such a move comes with the culmination of risks. Consequently, the responsible agencies establish new auditing practices and standards that help in addressing the evolution of immigration risks. Therefore, lived experiences limit the gap between auditing theory and practice through the development of new knowledge and visualizations. Converse to conceptual information, the new knowledge originating from lived experiences is largely practical because of its origination from field practice.

Lived experiences are vital in identifying practical elements of auditing that relate to specific settings. For example, the 1986 Immigration Reform and Control Act (IRCA) sought to reduce the inflow of immigrants from Central America to the United States. The policy sought to deploy auditing practices to control and check the flow of immigrants from Central America. However, IRCA failed to reduce the inflow of immigrants from Central America to the United States. Multiple reasons led to the failure of IRCA to halt and limit immigration (Lehman, Annisette, & Agyemang, 2016). For instance, the audit system deployed by IRCA failed to effectively verify the legality of work. The policy also underperformed in the enforcement of employer sanctions. Lived experiences can develop new visions, which are also accompanied by reflective knowledge. Consequently, lived experiences result in the establishment of new practical information that can help improve audit systems. For instance, the IRCA case can help other nations, including the United States, develop better auditing systems that incorporate practical lessons as opposed to impractical or misguiding theoretical concepts.

Literature also cites the value of lived experiences in bridging the gap between planning theory and practice. In essence, lived experiences help corporations and individuals accrue practical planning knowledge that lacks theoretical concepts. Moreover, the course is pivotal in doing away with theoretical arguments that hardly apply to the field setting (Donetto et al., 2015). Specifically, lived experiences are vital

in reducing the gap between planning theory and practice in two major ways. First, they increase the range of perspectives in the planning process, hence revealing lenses that had been ignored in theoretical concepts. Lived experiences create room for participatory planning, which encompasses the inclusion of individuals that have experienced events in the planning procedure. For example, if a company seeks to plan for corporate activities, it might reduce the gap between planning theory and practice through the inclusion of all stakeholders, including clients and employees.

Lived experiences of people in an organization might reveal the ignorance in previous planning activities because it exhibits the challenges that arise from past procedures. Specifically, corporations often make plans without including vital stakeholders in the planning phase. However, the developed plans come with detrimental impacts because of the width of the gap between the planning theory and practice. However, lived experiences of stakeholders ignored by organizations in previous planning processes might help determine practical needs that such plans should seek to address (Donetto et al., 2015). Such information helps corporations determine shortcomings in previous planning activities and the subsequent strategy to establish an improved planning procedure. Moreover, the inclusion of stakeholders that have experienced the detriment of previous planning procedures plays an integral role in limiting the theory-practice gap because such individuals possess information about practical planning dynamics. Co-designed planning, which explores and deploys lived experience information, is vital in achieving harmony between theoretical and practical planning because of the inclusion of multiple stakeholders.

Social and cultural values are often ignored in the planning process due to the overreliance on Eurocentric theoretical concepts. However, the inclusion of people who have previously taken part in planning activities helps corporations learn from the challenges faced by such an individual in past planning procedures (Porter, 2016). Lived experiences help planners learn about the social constructs responsible for variation in the success level of planning efforts. Specifically, planners with prior planning experience understand the social variations that might make certain theoretical arguments impractical among certain groups of people. For example, most

planning theories are based on colonial cultures, making the developed plans inapplicable in particular settings.

The deployment of the lived experiences of people in such environments helps corporations reduce the gap between planning theory and practice because it reduces the overreliance on colonial cultures. Lived experiences play an integral role in incorporating cultural factors in the planning procedure. The gap between planning theory and practice further stems from the imposition of theoretical arguments, based on a particular group, on a contrary community. Such a move results in a cultural conflict that often results in the failure of the deployed plan (Porter, 2016). For example, teachers can hardly deploy effective teaching plans without accommodating the cultural and social factors of the learner population (Aronson & Laughter, 2016). Learners can help teachers establish effective planning by airing out their lived experiences concerning the learning process, hence exhibiting the role of cultural variation in the learning process.

The lack of society incorporation is considered as a contributing factor to the gap between planning theory and practice. However, the deployment of lived experiences allows parties to include society in the planning process. Multiple individuals in a community might have experienced the outcome of previous plans. Consequently, such parties might understand the reason for the failure of past plans. The value of lived experiences in bridging the gap between planning theory and practice stems from the inadequacy of the planning theory, which fails to include society. For instance, the American and European societies, around which the planning theory is woven, are different from other communities across the globe. Technical experts can be pivotal in providing experiential knowledge concerning planning activities. Such information reduces the theory-practice gap because it incorporates the social setting and contextualizes the planning process to suit the community that seeks to benefit from the deployed plan.

The value of lived experiences in planning is evident in the activities of non-governmental planning organizations such as the Asian Coalition of Housing Rights (ACHR) and the Shack/Slum Dwellers International (SDI). The activities of the two agencies are hardly based on theoretical arguments. Instead, the two groups learn

through processes (Watson, 2014). Succinctly, they learn by executing tasks and deploying plans. Therefore, if an individual working with any of the two corporations documents the experience they have acquired in the course of their working tenure, the information contained in such a document is relevant to the environment because of the dependence on trial-and-error approach that allows the person to give out only specified planning information, which is relevant to the context. Therefore, lived experiences create room for collaborative planning, which helps develop practical plans.

As stated earlier, the gap between planning theory and practice originates from the dependence on global North theories, which are often based on variables that exhibit a differing pattern across the globe. The deployment of lived experiences helps incorporate context in the planning process (Watson, 2014). Consequently, the information established through lived experiences is more practical than it is theoretical because it is based on a local environment as opposed to reliance on theoretical arguments based on global North variables. Most importantly, lived experiences create room for collaborative and communicative planning, which is pivotal in the universal reduction of the gap between planning theory and practice. Lived experiences help studies determine practical planning strategies that accommodate the context of an environment. Subsequently, a collaboration between several planners across the globe results in the development of universal planning practices that account for cultural and social contexts.

Lived experiences also limit the gap between planning theory and practice because of the continual acquisition of knowledge during an individual's exposure to activities and systems. For instance, a system manager could learn through interaction with customers. Such an interaction allows the system manager to acquire knowledge from the experiences of the customers that give user feedback. The system manager, through their lived experience, develops a comprehension of the client's feelings and incorporates the knowledge in the development of subsequent customer satisfaction plans (Osborne, Radnor, & Strokosch, 2016). For instance, the proof of a positive correlation between evidence-based nursing education and patient care outcomes stems from Florence Nightingale's arguments and activities, which used evidence to

advance nursing practice during the Crimean War (Mackey & Bassendowski, 2017). Nightingale deduced that the provision of proof concerning a gap in nursing practice and the use of the evidence in nursing education approaches plays an integral role in filling the identified void. Therefore, evidence-based nursing education results in positive patient outcomes. Nightingale's lived experience helped her bridge the gap between the theory and practice of nursing care through continual observation of the relationship between nursing education and patient outcomes.

Concerning strategy, lived experiences are vital because of the need to address multiple context issues that differentiate different settings. Such a finding is particularly evident in environments with diverse human resources. Lived experiences help corporations deploy strategies that optimize labor utilization. Notably, labor cultures vary across geographical settings. For example, the British and United States labor forces exhibit varying characteristics that affect the attempt of organizations to get the best returns out of the workforce (Briken & Taylor, 2018). However, most theoretical arguments do not capture such differences. Lived experiences bridge the theory-practice gap because of the reliance on findings that relate to the labor force in a company's context. Lived experiences are particularly vital in strategy establishment and deployment among multinational corporations that operate in more than one state.

Lived experiences are pivotal to marketing strategies because of the variation among marketing audiences. The communication strategy plays an integral role in achieving marketing success. However, due to the ambiguity of theoretical marketing approaches, corporations are likely to deploy models that might fail because of the lack of incorporation of a setting's context and the determination of a communication strategy that suits the intended audience (Whelan & Wohlfeil, 2006). However, lived experiences give companies access to contextual information that relates to the specified audience. For instance, companies can rely on the lived experiences of previous marketing personnel to determine the communication strategies to apply to different audiences. Such a move is prudent in achieving emotional attachment to brands, which is achieved through enhanced customer-brand relationships that are optimized by the relevance of the communication strategy.

Another instrumental aspect of lived experiences in strategy establishment stems from the role of different stakeholder feelings in strategy success. Such a finding is particularly evident among customers, who are vital stakeholders because of their role in sales. However, the vast gap between theory and practice makes marketing strategies unsuccessful because of the variation of demands and preferences among clients (Whelan & Wohlfeil, 2006). However, the deployment of the lived experiences of clients helps corporations access context-relevant information that reveals customer experience, which is instrumental in developing communication strategies that seek to achieve customer-brand relationships. Lived experiences also expose companies to reality, which exhibit the shortcomings of the theoretic approach deployed, hence reducing the theory-practice gap of strategy formation. As such, lived experiences determine consumer reality notion, hence reducing the theory-practice.

Lived experiences also reduce the theory-practice gap through the recognition of the feelings of different people and settings. Such a finding is particularly evident in policies, which embody government strategies of addressing multiple social issues. The success of government policies can hardly be determined without the analyzing the feelings of the different players involved in the policy. For instance, the analysis of the lived experiences of students in the United Kingdom has shown that the Prevent Strategy, which has been deployed to address radicalization in the region, is ineffective in school settings (Taylor & Toni, 2017). The finding reduces the practice-theory gap in the strategy and helps the United Kingdom determine theoretical arguments that are not practical in different settings, including classrooms. Specific to the United Kingdom situation, lived experiences have established that the Prevent Strategy hinders vital critical discussion among learners because they fear engaging in debates. Moreover, the strategy enhances inter-group conflicts because a significant proportion of the student population is alienated and villainized. Such a gap between strategy theory and practice could only be filled through the analysis of lived experiences.

The major value of lived experiences stems from the relevance and contextualization of theoretical information. Such a move helps the experienced parties to learn about the incompatibility of theoretical concepts in particular practices. Subsequently, the

trial-and-error approach helps in the establishment of practical concepts that might be lacking or incorrectly articulated in theoretical frameworks. While the theoretical concepts might not necessarily be wrong, they are often based on American or European study populations. Consequently, they might fail to directly apply to particular settings, especially among global South countries. Nevertheless, lived experiences allow individuals to learn from prior mistakes, helping corporations and individuals reduce the gap in auditing and planning theory and practice.

# Chapter 4

# Business Continuity Management Overview

No organization can have complete control over its business environment. It is therefore essential for companies to have a Business Continuity Management (BCM) and Crisis Management capability, in case of crisis or disaster.

**Business Continuity Management (BCM)** is defined by the Business Continuity Institute (BCI) as '*an holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities'*. (BSI BS2599-1:2006:1)

The BCI's use of the term 'Business Continuity Management' rather than 'Business Continuity Planning' is deliberate because 'planning' implies there is a start and end to the process and can lead to unwanted planning bureaucracy. BCM is, by necessity, a dynamic, proactive and ongoing process. It must be kept up-to-date and fit-for-purpose to be effective.

BCM is a business-owned and driven process that unifies a broad spectrum of management disciplines. It provides the strategic and operational framework to both review and where appropriate redesign the way an organization provides its products and services whilst increasing its resilience to disruption, interruption or loss.

It is generally recognized that an organization's BCM resilience depends equally on its management and operational staff as well as technology and requires an 'out of geographical region' BCM capability.

Because of its all-embracing nature, the way BCM is carried out will inevitably be dependent upon, and must reflect, the nature, scale and complexity of an organization's risk profile, risk appetite and the environment in which it operates. Inevitably BCM has close links to risk management and corporate governance strategies.

Since the BCI's publication of the GPG in 2002, there has been a massive movement across the Globe to adopt a standard for Business Continuity Management. Within the UK this activity has led to the publication of **Publicly Available Specification 56 (PAS56)**, which then led to the **first full standard BS25999-01 - Code of Conduct**.

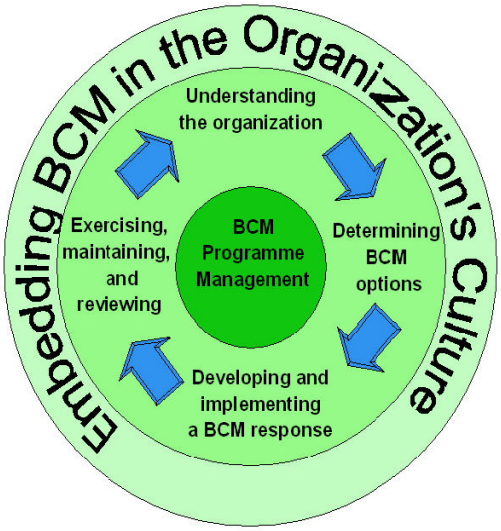



**Figure 4.1:** The BCM Lifecycle—BS 25999-1

The stages of the life cycle are set out in the scheme above, as of the BS25999-1 Standard.

Current International standards by British Standard Institution include:

- BS 25999-1:2006 Business continuity management. Code of practice
- BS 25999-2:2007 Business Continuity Management. Specification
- BS 25777:2008 Information and communications technology continuity management. Code of practice

The above standards, BCM life-cycle and good practice guidelines help to a clear understanding of what is required to achieve the needs of the business and corporate governance.

In May of 2012 the first ISO Business Continuity Standard was published:

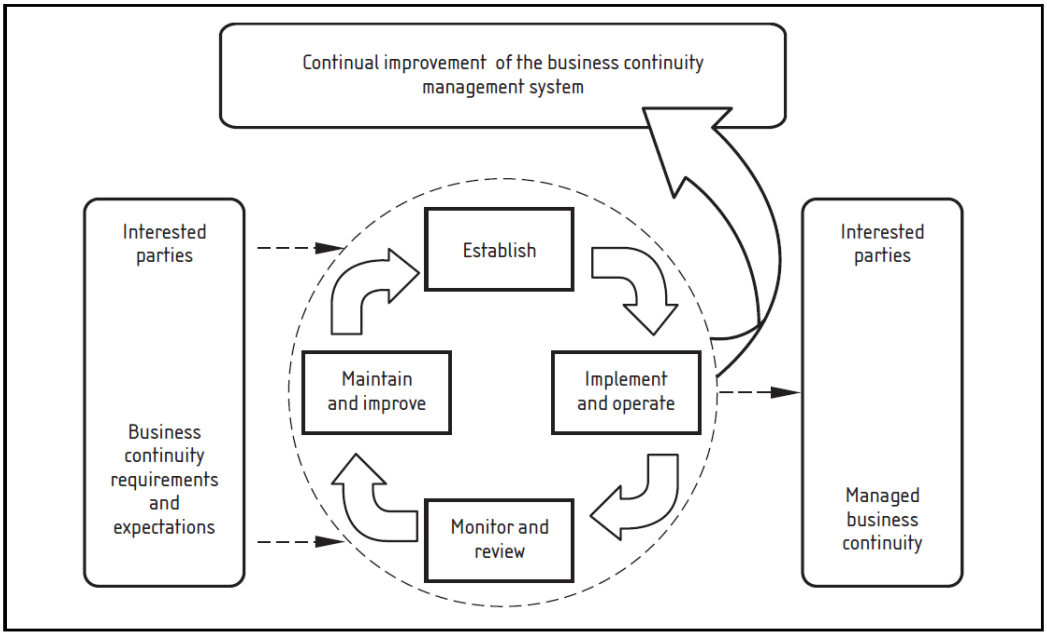
- **ISO 22301:2012(E) Societal Security – Business Continuity management systems - Requirements**.

The Standard adopts the Plan-Do-check-Act (PDCA) Model- as was the BS25999 – and specifies the requirements for setting up and managing an effective Business Continuity management System (BCMS) within an organization.

It is applied the "Plan-Do-Check-Act" (PDCA) cycle to establishing, implementing, operating, monitoring, exercising, maintaining and improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards that may exist in an organization, thereby supporting consistent and integrated

Figure 1 **PDCA cycle applied to BCMS processes**

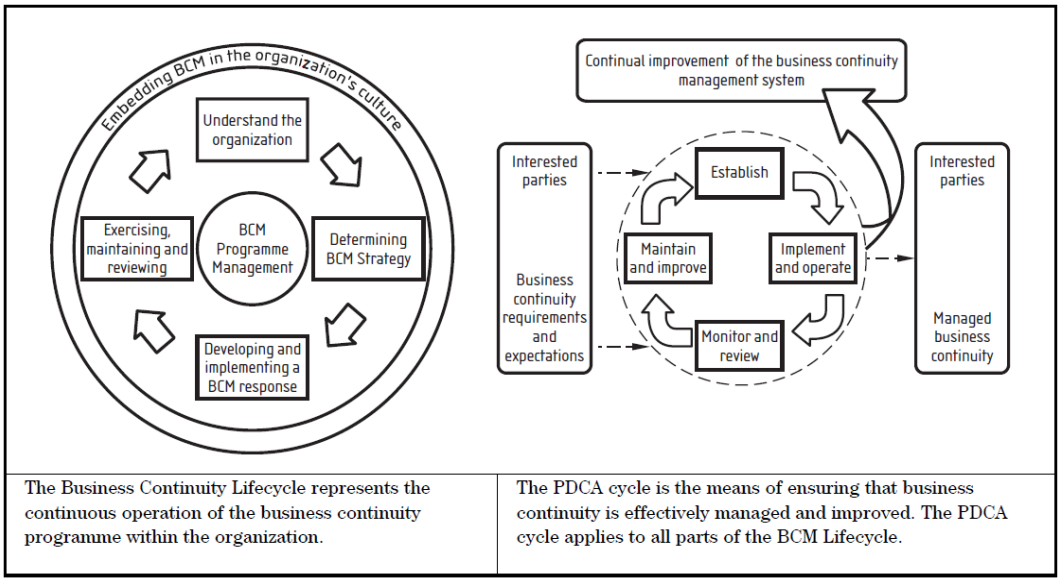



implementation and operation with related management systems. (BSI BS2599-2:2007:2)

**Plan** Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to managing risk and improving business continuity to deliver results in accordance with an organization's overall policies and objectives.

**Do** Implement and operate the business continuity policy, controls, processes and procedures.

Figure 2 **The business continuity management lifecycle**




The Business Continuity Lifecycle represents the continuous operation of the business continuity programme within the organization.

The PDCA cycle is the means of ensuring that business continuity is effectively managed and improved. The PDCA cycle applies to all parts of the BCM Lifecycle.

**Check** Monitor and review performance against business continuity objectives and policy, report the results to management for review, and determine and authorize actions for remediation and improvement.

**Act** Maintain and improve the BCMS by taking preventive and corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

In October of 2019, the ISO Business Continuity Standard of 22301 was updated.

# Chapter 5

# Methodology & Methods

## 5.1 Relevance of Phenomenology as Methodology and Methods for BCM Study

In both Husserlian and Heideggerian phenomenology research, unstructured one-to-one interviews are the most effective data collecting mode. The following researchers employed an unstructured method for their interview format: Beck (1992), Ng and Sinclair (2002), and Thornburg (2002). They began the interview by asking questions such as 'tell me about your experience' to get the conversation going. Afterward, the experiences are written down and studied for themes and meanings, which allows the experience to be comprehended better. On the other hand, Husserlian phenomenological interviewing differs from the Heideggerian method. It demands the researcher to set aside her preconceived notions about the interview topic before conducting the interview and collecting the information. So the researcher must adhere to the practice of "bracketing," which entails putting away preconceived notions.

In addition to eliciting a vivid image of the event from the interviewee, interviews have the additional benefit of facilitating the discovery of common meanings. Husserlian phenomenology has as its goal the description of people's experiences of things and how they comprehend them. This achieves this goal. But this can only be accomplished if the researcher's presence does not sway the participants. Social dialogue aims to generate a pleasant and trusting environment that should precede the interview. The researcher should next propose that the participant take a few seconds to concentrate on the event before beginning the interview thoroughly. Because it has been disclosed to the participants that the researcher is supportive and trustworthy, they can relate

their experiences without prejudice until data saturation has been attained, which is when the narratives become repetitive, and no new information is given. The sampling process will come to an end whenever data saturation is achieved.

According to Berg and Dahlberg (1998), data saturation was attained between 30 and 120 minutes, but Lundqvist and colleagues' (2002) interviews reached saturation between 60 and 90 minutes. Phenomenological interviews are almost always audiotaped, which provides a rich supply of data that can be evaluated once the interview is over. Even if the interviewer is jotting down notes throughout the interview, certain details may be overlooked. In addition, Robinson (2016) recommends that the researcher write notes after the tape recording has been completed since it is not uncommon for participants to contribute rich information at this point in the interview.

There are certain drawbacks to employing this form of data collecting. In addition to being time-consuming and labor-intensive (Christensen, Johnson &Turner, 2020), it is also expensive and necessitates highly competent interviewers. Regarding where the interview should take place, it is often in a setting where the participant spends most of their time.

Phenomenologists consider phenomena apodictic, which implies that they speak for themselves and that we should be prepared to listen to what they have to say. Bracketing, also known as phenomenological reduction, is the process of removing all of our ordinary natural assumptions about a phenomenon from consideration. For some philosophers, the reduction is a process of being as non-influential and neutral as possible in one's own experience. Researchers want to put aside their previous understanding, prior information, and preconceptions about the phenomenon to concentrate on it as it is now manifesting itself. Bridging is an approach to presenting the validity of the data collecting and analysis process commonly used in phenomenological research.

Business continuity management (BCM) entails the efforts to ensure the sustainability of corporate value in light of catastrophic and distractive events. In essence, BCM seeks to analyze risks that threaten the internal and external factors of a company,

with the intention of developing resilient frameworks that can stand such risks. Moreover, BCM aims at streamlining the recovery phase in the event of a manifestation of a firm's risk factors. Therefore, BCM is a strategic move by corporations to safeguard assets and stakeholder interests in the event of exposure of man-made and natural occurrences such as earthquakes and accidents. Despite the value of BCM, lived experiences and phenomenology can play an integral role in enhancing the role of BCM in recovery and resilience in catastrophic incidents. This chapter outlines the value of phenomenology and lived experiences in bridging the gap between the theory and practice of BCM programs.

Frequently, corporations approach and attempt to implement the theoretical BCM concept, establishing practical solutions to problems. However, there is a broad gap between the theoretical and practical BCM concepts. The gap stems from the difference between corporations and theoretical firms in the development of the BCM concept (Fischbacher-Smith, 2017). Often, organization failure and performance are practically non-linear and complex aspects that fall outside the constructs of BCM theoretical assumptions. Such differences create a gap between BCM theory and practice. There is a pressing need to fill such a margin to achieve the effectiveness of BCM programs in companies. Phenomenological studies and lived experiences offer a wise opportunity for companies and academic institutions to bridge the gap between the theory and practice of BCM.

Phenomenological studies encompass the research that seeks to capture information about phenomena through various ways, including interviews. On the converse, lived experiences entail tales by individuals that have experienced such phenomena (Errasti-Ibarrondo et al., 2018). These two research approaches can help bridge the gap between the BCM theory and practice, especially if studies focus on the performance of BCM applications in light of various phenomena and the experiences gained by the practitioners involved in the setting up and managing such frameworks or involved in the management of actual incidents.

The deployment of efficient BCM frameworks and programmes that can help an organization to cope with the impacts of a negative incident or disaster can only be achieved by such practitioners that have the actual experience of managing different

aspects and variations of the BCM theory adapted to different industries, cultural and market environments. The use of the lessons learned and the experience gained in the field by those practitioners involved and managed actual disastrous events is a key aspect that will assist in the implementation and adaptation of BCM theory into practice.

In the event of a gap between practical and theoretical concepts, connecting course and field events emerges as a wise approach to filling the gap. In the case of BCM, the theoretical concept represents the course element while the performance of BCM in practical situations is an embodiment of a field setting. Therefore, an analysis of BCM performance among companies emerges as a key way of bridging the gap between BCM theory and practice.

Research and studies offer a perfect opportunity to bridge the gap between theory and practice because they expose researchers to field environments. However, information or data is the most important outcome of studies and research. Therefore, most studies seek to reveal specific data related to a certain concept. Phenomenology and lived experience offer a way of collecting data that may be used to validate BCM theoretical concepts. Such data is then analyzed to reach conclusions that can help establish novel theories about BCM.

As stated earlier, the most significant method of bridging the gap between ant theoretical and practical concept entails venturing into the field. However, unlike other fields, the BCM field seeks to prevent immense losses incurred by companies in the case of catastrophic incidences. Therefore, there is the need to depend on the information provided by people that have experienced and managed catastrophic events. The literature states the value of change management in achieving organizational sustainability and resilience. In essence, corporate leadership needs to ensure a change in the way the company conducts its activities. Such a move is crucial to boosting the response and prevention activities done by the organization (Corrales-Estrada et al., 2021). However, the leadership needs to understand the previous occurrences to determine ways of preventing adversities and significant losses created by disasters and unexpected events. Besides, there is the need to understand warning signs that precede a disaster or risk manifestation. Lived experiences and

phenomenology records play a pivotal role in helping managers and other employees interpret disaster warning signs. For such a reason, it is vital for companies to include parties that have experienced and managed disasters in risk response and mitigation teams. There might be a vast difference between theoretical and practical warning signs of a possible disaster. However, dependence on phenomenological studies and lived experiences is similar to field exposure, which plays an integral role in bridging the gap between theoretical and practical concepts.

Hence data is important to efforts to reduce the gap between practical and theoretical concepts. However, it is hardly possible to capture the data of catastrophic events through experimentation, which is the basis of many scientific research processes. Nevertheless, there is the need to capture such information for the formulation of new theories or models. In the case of BCM, the required data entails the causes and effects of catastrophe to corporate mission, objectives, and performance. While it is hard to conduct experiments concerning catastrophes, the required data can be captured from phenomenological studies and lived experiences. There is a need for information that can reduce the gap between theoretical and practical situations. This necessary data can only be obtained by the collection of information that are extracted from the experiences of people involved and managed catastrophic events through the use of interviews and questionnaires addressing targeted areas.

However, there is the need to keep the data updated to ensure that companies are equipped and prepared to address risks as they arise and evolve (Ellitan & Anatan, 2020). Therefore, phenomenology and lived experiences play an integral role in updating crisis management information and data used by companies in BCM. They enhance the quality of data by boosting the accuracy of the data in relation to the specific risks that a corporation faces. Data plays a pivotal role in raising the effectiveness of any business process, including risk management. The approach to managing the information is equally vital in reducing the gap between BCM theory and practice. Thus, phenomenological research and lived experiences are a vital way of capturing and updating information or data concerning unexpected and unplanned incidences in companies. The change in the nature and effect of phenomena implies

that a continual practice of analyzing the data creates a continuous data update due to the analysis of different phenomena and lived experiences.

Moreover, the working of BCM theoretical concepts portrays the practice as a holistic and universal approach to addressing disturbances across a wide range of organizational risks. However, as stated previously, most organizations vary from each other. Consequently, their exposure to risks is not necessarily similar to the theoretical depiction. Such a discrepancy results in ineffectiveness in the application of BCM models (Fischbacher-Smith, 2017). As such, the deployment of the BCM model might succeed in one company and fail in another. However, the working of phenomenological studies and lived experiences implies that they deal with multiple but specific occurrences, which might exhibit multiple differences. Such a move results in the development of practical models that cater to the needs and resources of different corporations (Rezaei Soufi, Torabi, & Sahebjamnia, 2019). In essence, it reduces the gap generated by the dependence on a similar theoretical model that has not been proven to work across all corporations.

The failure of many BCM practices among companies exhibits the effect of the gap between BCM theory and practice. The change in the nature and frequency of business disruptions is primarily responsible for the failure of such applications. As such, the shift in the nature of business calamities has not been captured by BCM theories because of the difference between the development of such theoretical frameworks and the occurrence of corporate disruptions. Resultantly, the theory and practice of BCM deployment exhibit a vast difference (Krell, 2006). Nevertheless, dependence on phenomenological studies and lived experiences exposes researchers to new forms of business interference, whose transpiration differs from that explained in conservative BCM theories. Resultantly, researchers and scholars can use phenomenology and lived experiences to update the theoretical content of BCM concepts, hence accommodating new practical situations.

Lived experiences also enhance an individual's exposure to unexpected and unplanned incidences. Not only do they increase the comprehension of the transition from BCM theory to practice but also exhibit specific challenges that corporations could face due to the gap that exists between BCM theory and practice. Such an aspect

of phenomenological studies and lived experiences is particularly evident among people in leadership positions. Lived experience and phenomenology play an integral role in leadership involvement in BCM. Literature indicates the value of change management in achieving organizational sustainability and resilience. In essence, corporate leadership needs to ensure a change in the way the company conducts its activities. Such a move is crucial to boosting the response and prevention activities done by the organization (Corrales-Estrada et al., 2021). However, the leadership needs to understand the previous occurrences to determine ways of preventing adversities and significant losses created by calamities and unexpected events.

The value of prior BCM implementation experience encompasses the acknowledgement of the deployment context, which is responsible for the failure of success of BCM application in corporations. Among leaders, lived experiences enhance foreknowledge concerning BCM implementation, hence awareness of probable challenges that stem from the gap between BCM theory and practice. Such experience in itself helps bridge the gap between BCM theory and practice, especially concerning the deployment of BCM practices and models among companies.

The value of lived experiences and phenomenology also extends to the workforce. Literature states the role of the workforce in crisis management, specifically information dissemination. Notably, the onset of a crisis often results in massive turnover among companies. However, employees that have experienced similar crises are unlikely to quit their jobs because of such incidences (Krell, 2006). Moreover, phenomenology and lived experiences enhance the ability of the workforce to notice warning signs that signify the onset of a crisis. Such a pattern exhibits that lived experiences and phenomenology records can help companies address crises in two crucial ways, including early response and prevention. In such a move the company reduces losses incurred following accidents. Most importantly, lived experiences enhance the resilience of the workforce to crisis distress. Employees with prior BCM implementation experiences also reduce the gap between BCM theory and practice through the identification of practical disaster warning signs that might not have captured by theoretical BCM frameworks.

Therefore, the use of lived experiences and phenomenology records are vital to determining the outcomes of previous risk management plans, which provide room for improvement of BCM theories, hence creating a practical continuous mitigation environment. They are primarily valuable to companies and institutions because they bridge the gap between BCM theory and practice. They also play an integral role in sustainability by helping corporations avoid risks that are too costly to entertain. A reduced gap between BCM theory and practice is necessary for the success of the concept in business environments.

## 5.2 Details About the Applied Phenomenological Method with focus on Lived Experience and Design of Questionnaire and Interviews

In view of the above Phenomenological studies and their focus on data collection we will use such lessons in constructing a questionnaire and interviews for data collection about Lived Experiences of BCM Professionals. Below, I am describing the questionnaire and interview choices made in the research design for our methods.

### 5.2.1 Questionnaire

The questionnaire was developed taking into consideration the theoretical framework of the BCM methodology and was structured in a way similar to the different stages of the BCM lifecycle. One of the targets of the questionnaire was to extract, validate and expand the information related to the key areas of the BCM discipline, identify the importance of the different stages and record their respective components. The second target of the questionnaire was to collect information and viewpoints for the implementation of the BCM lifecycle stages based on the experience of the interviewers in similar programs. Both targets were successfully accomplished based on the response received.

The distributed questionnaire is included in Annex A in the relevant chapter of annexes at the end of this study. The target group included both BCM practitioners working as permanent employees in various organizations but also practitioners working as freelancer consultants. In this way both operational modes and attitudes were taken into consideration for the completeness of the study.

It needs to be noted that the practitioners that responded in the questionnaire were originated from different regions, cultural and working environments, while they have worked in a number of industries implementing BCM programmes. Therefore, their thinking, concept, approach and attitude in such implementations is considered as thorough, representative and fully aligned to the BCM discipline.

The questionnaire was sent to 39 BCM practitioners, while the total number of the people responded to the questionnaire was 20.

The outcome of the data collected through the responses received has been incorporated with the rest of the information received from the different additional resources in the subsequent chapters.

### 5.2.2 Interviews

Structured and unstructured interviews were conducted with the majority of the people that were also involved in answering the questionnaires. Although the questionnaire was an important tool for the collection of data through a qualitative approach by determining the scope, content and limitation of the research, interviews greatly assist in broadening the amount of information collected and especially in analyzing views and angles based on each interviewer's personal experiences.

Interviews employed a qualitative research methodology guided by Consensual Qualitative Research (CQR; Hill, et al, 1997; Hill et al., 2005). The analysis was reviewed and further discussed with an outside auditor for the study. The auditor is a practitioner that has over 30 years of BCM experience, one of the oldest members of Business Continuity Institute (BCI) and heading the BCI Greek & Cypriot chapter.

The selection of the people interviewed was made with the following criteria

- Expertise in the specific discipline based on the number of years involved in the implementation of BCM programmes

- The regions in which the respondents have been engaged. There has been an effort to include people from all regions in order to take into account different

cultural and working environments that may differentiate the lived experiences

- The size of organization that employers are working was another criterion. The interviewers were from small, medium and large size organization in order to include differentiations in working environments

- An additional supportive criterion was the type of employment of the people involved in the research since it was required to include both the viewpoints of persons employed in BCM functional roles in organizations but also working as freelancer consultants.

The duration of the interviews varied between 90 -120 minutes, some of them were conducted face to face and other through online applications (e.g., webex, zoom) due to the constraints of different regions. The interviews were not recorded but extensive written notes were kept and further analyzed. As it has been done with the questionnaires, an effort was made to include practitioners from different regions, industries and cultural environments to identify possible differentiations and customizations in their BCM implementation.

The structured interviews were conducted using the content of the questionnaires prepared, addressing open-ended questions covering all the stages of the BCM lifecycle. The scope of this type of interview was to further validate the response received through the questionnaire but also further expand the content and details for each of the stages discussed. In this way it was possible to further identify items and issues that were not directly addressed in the questionnaire or that have been omitted.

The unstructured interviews involved discussions with the participants related to their view, experiences, challenges and lessons learned during the implementation of BCM programmes in different industries and cultural environments.

The areas discussed and covered during the interviews is included in Annex A in the relevant chapter of annexes at the end of this study.

## 5.3 Other Data Collection Methods

Other methods and sources of obtaining the necessary data to be included in the study were:

I. BCM Literature Review
II. Lived Experience (combined with the interviews)
III. Collection and analysis of material (e.g., surveys) relevant to the above by knowledge bodies such as BCI, DRII, BC Management

### 5.3.1 BCM Literature Review

The scope of the BCM literature review is to identify the theoretical background and framework of BCM methodology and to collect information for the implementation of BCM programmes by subject matter experts.

Moreover, it was an attempt to identify whether and to what extend there was any recording of the practical experience gained during the implementation of BCM programmes.

The literature review focused on international standards (e.g., BS 25999, ISO 22301, etc.), advisory directions provided by different knowledge bodies (e.g., BCI, DRII, BCMI), internet related sources (e.g., Continuitycentral & other sites) research papers and books written by recognized experienced practitioners that assisted in the creation, development and maturity process of the BCM methodology during the past decades.

The list of all these different sources of literature review is presented in the relevant section at the end of this study.

The review of the literature resources provided the necessary theoretical framework that served as the groundwork of this study and indicated the areas that were required to be included in the questionnaires and in the agenda of the interviews.

Hence, the material related to the BCM theory and any constraints or limitations identified was used as the framework upon which the study was developed and

expanded to include the practical experience from numerous implementations and the respective lessons learned that resulted in the development of these guidelines.

On the other hand, the review indicated the fragmentation of practical guidelines and recommendations during the implementation of BCM programmes and the lack of systematic research in recording the challenges that result in their failures.

### 5.3.2 Knowledge Bodies Surveys

There are several knowledge bodies and organizations that are related to the BCM discipline and provide mentoring and support to practitioners or people interested in the specific area.

A request was made to certain of them such as BCI, BC Management and DRII to provide with any surveys conducted related to challenges identified and addressed by BCM practitioners while implementing BCM programmes and following the international standardization.

Unlike to other disciplines and knowledge bodies, e.g., Project Management & PMI or Information Security & ISACA, there are no available surveys or any evidence of systematic research conducted by BCM's knowledge bodies that include information related to the issue of challenges identified and addressed by BCM practitioners. Apart from the extensive interpretation of the theoretical framework, the deployment of aspects and components related to the BCM lifecycle that should be included in the BCM programme there are sporadic references and shreds of actual practical implementation and lessons learned.

This finding makes the outcome of the study even more current since there is a detailed theoretical framework of BCM implementation but limited data related to challenges and adaptations that need to be made for a BCM programme to be efficient and fully operational.

### 5.3.3 Lived Experience

The collection of data and lessons learned through the experience of the practitioners that have worked with BCM methodology and implemented BCM programmes in a

variety of organizations, different industries and cultural environments for a long period of time is one of the major targets of the study.

Even the author of this study is a BCM practitioner with almost 20 years of working in the specific discipline, certified by one of the most recognized BCM knowledge bodies, the Business Continuity Institute (BCI), with one of the most senior levels of expertise as Associate Fellow of Business Continuity Institute (AFBCI).

The author worked and setup successfully BCM programmes in a large number of different size organizations in different industries across many countries in both EMEA and APAC in roles both as a freelance consultant and as regular employee. He has also been involved in the certification of organizations with the relevant BCM standardization of BS 25999 & ISO 22301 (e.g., Athens Stock Exchange) by recognized certification bodies (e.g., Lloyd's Register).

Similarly, the people involved in the study through responding to the questionnaires or participating in the interviews have provided their own experiences and lessons learned in the implementation of BCM programmes, while most of them have extensive experience and many years of service in the specific discipline.

The consolidation of the BCM theoretical framework with the lived experience and lessons learned by very experienced BCM practitioners is presented in details throughout the different chapters of the study as hints & tips, practical examples and templates and in combination of the theoretical framework of each phase of the BCM lifecycle.

# Chapter 6

# Data Collection & Analysis

The chapter presents information related to the BCM practitioners that have participated in the research, their respective background, experience and history, and a preliminary analysis of the data collected through the questionnaires.

Detailed information for the different stages and components of the BCM lifecycle is included in the subsequent chapters. These chapters also include the information collected and expanded through the interviews that have been conducted along with hints, methodology and practical examples per each phase.

## 6.1 Respondents' Demographics & Background

The following tables indicate certain demographic and background details related to the practitioners that responded in the questionnaire.

1. Current Employment. The table indicates whether the respondents were employed by an organization as regular employees or working in the consulting area as freelancers. There has been an effort to include both types of working models to efficiently represent possible different types of approach in BCM methodology.

| EMPLOYMENT TYPE | |
|---|---|
| **Consulting** | **Regular Employment in Organizations** |
| 6 | 14 |

**Table 6.1** Type of Employment

2. Sex. The table indicates the respondents' sex. The majority of the respondents was male.

| SEX | |
|---|---|
| **Female** | **Male** |
| 2 | 18 |

**Table 6.2** Sex Type

3. Respondents' Age Range. The table depicts the age range of the respondents. Most of the respondents were in the range of 41 – 60 years old. The age range of the practitioners that responded in the questionnaires indicates many years of working service and implies adequate experience in the specific discipline.

| AGE RANGE | | | | |
|---|---|---|---|---|
| **18 - 30** | **31 - 40** | **41 - 50** | **51 – 60** | **61 - higher** |
| 0 | 2 | 6 | 10 | 2 |

**Table 6.3** Respondents' Age Range

4. Number of years in current job. The table depicts the number of the years the respondents are working in their current role and organization. The respondents covered all ranges of employment in their current organization from relatively new to old employees.

| YEARS IN CURRENT JOB | | |
|---|---|---|
| **0 – 5 years** | **6 -10 years** | ➢ **11 years** |
| 5 | 6 | 9 |

**Table 6.4** Years in Current Job

5. Employees' Organizations. The table indicates the number of employees working in the respondents' organization. The majority of the respondents works in large size organizations. Nevertheless, the sample of the respondents is representative from all size organizations and consequently from different working environments.

| ORGANIZATIONS' SIZE | | | |
|---|---|---|---|
| **1 - 100** | **100 – 1,000** | **1,000 – 5,000** | **➢ 5,000** |
| 6 | 1 | 4 | 9 |

**Table 6.5** Employees' Organizations

6. Organizations' Regions. The table presents the regions in which the respondents' organizations operate. Most of the respondents' organizations operate in more than one region. Consequently, the respondents have worked in different multicultural environments and possibly adapted various working practices.

| REGIONS | | | | |
|---|---|---|---|---|
| **EMEA** | **APAC** | **North America** | **Central & South America** | **Oceania** |
| 15 | 12 | 8 | 7 | 2 |

**Table 6.6** Organizations' Employees

7. Experience in implementation of BCM Programmes. The table indicates the experience of respondents in implementing BCM programmes in different organizations. Based on the response presented below, it is evident that more than half of the respondents have extensive experience in the specific area.

| BCM EXPERIENCE (IN YEARS) | | |
|---|---|---|
| **0 – 5 Years** | **6 -10 Years** | **➢ 11 Years** |
| 1 | 5 | 14 |

**Table 6.7** BCM Experience

8. Certification by professional bodies (e.g., BCI, DRII, etc.). The table presents the professional bodies by which the respondents have received certification. Some of the respondents have more than one certification received from different professional bodies that are related to the BCM discipline. This indicates that practitioners in the specific area seek evidence of proof by

recognized professional bodies indicating the level of knowledge and experience in the specific discipline.

| PROFESSIONAL BODIES | | | |
|---|---|---|---|
| **BCI** | **DRII** | **ISO 22301 Lead Auditor / Implementer** | **None** |
| 10 | 9 | 5 | 1 |

**Table 6.8** Respondents' Certification

9. Areas of experience in organization / projects. The table depicts the respondents' areas of expertise that applies in the current employment and/or projects involved during their professional experience. Note that only one of the options could be selected.

| Areas of experience in organization / projects | Respondents |
|---|---|
| **1. Business Continuity** | 10 |
| **2. Operational Resilience** | - |
| **3. Organizational Resilience** | 5 |
| **4. Risk Management** | 1 |
| **5. Crisis Management** | - |
| **6. IT Disaster Recovery / IT Service Continuity** | 2 |
| **7. Operation / Facilities** | - |
| **8. Physical Security** | - |
| **9. Information Security** | 2 |
| **10. Other** | - |

**Table 6.9** Respondents' Areas of experience in organization / projects

10. Respondents per Industry. The table presents respondents' primary area of skills use as part of the organization in current role.

| Industry | Respondents |
|---|---|
| **1. Financial & Insurance Services** | 1 |
| **2. Professional Services** | 6 |

| Industry | Respondents |
|---|---|
| **3. Manufacturing** | - |
| **4. IT & Communications** | 5 |
| **5. Telecommunications** | 5 |
| **6. Transport & Storage** | - |
| **7. Retail & Wholesale** | - |
| **8. Energy & Utility Services** | 1 |
| **9. Banking** | 1 |
| **10. Other - Investments** | 1 |

**Table 6.10** Primary area of skills in current role

11. Industry Work Experience. The table presents the experience of respondents to different industries. Most of the respondents have experience of implementing BCM programmes in multiple industries, indicating the high level of expertise and adaptation required to cope with any specific industry differentiation.

| Industry | Respondents |
|---|---|
| **1. Financial & Insurance Services** | 12 |
| **2. Professional Services** | 13 |
| **3. Manufacturing** | 6 |
| **4. IT & Communications** | 10 |
| **5. Telecommunications** | 13 |
| **6. Transport & Storage** | 4 |
| **7. Retail & Wholesale** | 3 |
| **8. Energy & Utility Services** | 6 |
| **9. Banking** | 11 |
| **10. Maritime** | 1 |
| **11. Business Process Outsourcing** | 2 |
| **12. Investments** | 1 |

**Table 6.11** Respondents' Industry Experience

12. Regions Working Experience. The table depicts the experience of respondents to specific regions. Some of the respondents have working experience in more than one region, indicating the exposure of the respondents to different cultural and working environments.

| REGIONS WORK EXPERIENCE | | | | |
|---|---|---|---|---|
| **EMEA** | **APAC** | **North America** | **Central & South America** | **Oceania** |
| 12 | 9 | 4 | 3 | 2 |

**Table 6.12** Respondents' Regions Working Experience

## 6.2 Questionnaires' Content & Outcome

This qualitative study addressed the following areas in the questionnaires:

- Stages of the BCM lifecycle and their importance in the implementation of BCM programme
- Components that need to be identified and managed in each of the different stages of the BCM lifecycle
- Approaches used in the collection of the necessary data for the efficient completion of each stage
- Identification of the stakeholders involved and their characteristics
- Major challenges that need to be addressed in each of the stages but also in the implementation of the BCM programme
- Measures to maximize the efficiency of a BCM programme and Key Performance Indicators (KPIs) to monitor it

It has been requested from the respondents to identify and mark the importance of the items in each question by choosing three different levels (Low, Medium and High). In this way the practitioners participating in the survey can indicate whether specific theoretical aspects and components are considered as essential or not during the

implementation of a BCM programme. Moreover, in each of the questions there has been an option of providing additional input based on their judgement. It should be noted that the answers had derived based on the experience of the respondents and not through their knowledge of the respective theoretical framework.

The feedback received by the practitioners that responded to the questionnaires is presented in the following paragraphs. The text in blue color was the additional optional input provided by the respondents. Detailed description of the items / components recorded in the questionnaire is included in the subsequent chapters taking into consideration the level of importance marked by the respondents.

### 6.2.1 Structure of BCM

The table below presents the questionnaires' results related to the proposed structure of BCM within an organization.

| DOMAIN | QUESTION | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Structure of BCM (Roles / Responsibilities)** | Identify roles for a fully operational BCM programme in an organization | Business Continuity Management Steering Committee | 0 | 3 | 17 |
| | | BCM Unit / Manager / Consultant(s) | 0 | 1 | 19 |
| | | Business Continuity Representative | 0 | 4 | 6 |
| | | Head of Business Unit | 0 | 6 | 7 |

**Table 6.2.1** Structure of BCM

**Observation**: All respondents have recognized the necessity of existence of a BCM structure within an organization. This structure should have distinctive roles and responsibilities to be able to support efficiently the operation of the BCM programme. BCM Steering Committee and Unit have been identified as essential and critical within an organization, while the assignment of Business Continuity representatives from all Business Units greatly facilitates the effort and execution. Detailed analysis and

information for the scope and responsibilities per each role is included in Chapter 8, paragraph 8.1.

### 6.2.2 Business Impact Analysis

The table below presents the collected results related to the Business Impact Analysis stage.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Business Impact Analysis** | Importance of BIA to the Business Continuity Programme | | 1 | 1 | 18 |
| | Identify the aims of BIA and mark their importance | Products | 0 | 4 | 16 |
| | | Services | 0 | 2 | 18 |
| | | Activities / Processes | 0 | 2 | 13 |
| | Indicate the best approach to conduct a Business Impact Analysis | Questionnaires | 1 | 7 | 12 |
| | | Site Surveys | 1 | 7 | 12 |
| | | Workshops | 1 | 3 | 16 |
| | | Interviews | 0 | 1 | 19 |
| | Indicate the types of losses that need to be evaluated | Finance | 0 | 1 | 19 |
| | | Strategic | 2 | 3 | 15 |
| | | Reputation | 0 | 2 | 18 |
| | | Legal | 0 | 1 | 19 |
| | | Operational / Customers | 0 | 4 | 13 |
| | Rate the importance of deliverables in a Business Impact Analysis | Recovery Time Objective | 0 | 1 | 19 |
| | | Recovery Point Objective | 0 | 2 | 18 |
| | | MTPD | 0 | 12 | 8 |
| | | Dependencies | 0 | 1 | 8 |
| | What should be the experience and skills profile of the people involved in the execution of BIA from organization's side? | Managerial level | 0 | 4 | 16 |
| | | Technical Expertise | 0 | 6 | 14 |
| | | Business Overview | 0 | 3 | 17 |
| | | Engineer Level | 11 | 6 | 3 |

**Table 6.2.2** Business Impact Analysis

**Observation**: It is evident that the phase of Business Impact Analysis is considered as critical for the implementation of a Business Continuity Management programme. Respondents indicated that the scope of the BIA phase is to identify the services, products and activities within an organization while it is important to develop an impact evaluation matrix per specific types of losses such as: finance, strategic, reputation, legal and operational / customers.

The respondents identify a number of approaches of conducting a BIA that usually are applied complementary to each other (questionnaires, site surveys, workshops and interviews) to reach the point of the deliverables that should include recovery time objective (RTO), recovery point objective (RPO), maximum tolerable period of disruption (MTPD) and dependencies that may exist.

Finally, an important aspect of BIA is investigated. The profile of the people (managerial, technical expertise, business overview or engineer level) from the organization that need to be involved in the BIA phase is examined because it is considered as critical for the quality and completeness of the information extracted related to the organization's operational model and environment.

At the end of the BIA's part in the questionnaires there were two questions related to challenges managed during the BIA execution and critical items to be taken into consideration. The feedback received is included as "Hints & Tips" in the respective BIA section. Detailed analysis and information related to BIA process is included in Chapter 9, paragraph 9.1.

### 6.2.3 Risk Assessment

The table below presents the collected results related to the Risk Assessment.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Risk Assessment** | Do you consider the phase of Risk Assessment as critical to the Business Continuity Programme? | | 1 | 3 | 16 |
| | Provide indicative threats/risks to | Natural Disasters | 0 | 3 | 17 |
| | | Technological | 0 | 4 | 16 |
| | | Man made | 0 | 6 | 14 |

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| | be assessed during the RA. | Geopolitical | 0 | 0 | 8 |
| | | Terrorism | 0 | 0 | 2 |
| | | Cyber Attacks | 0 | 0 | 3 |
| | Indicate the outcome(s) of Risk Assessment (s) | Threats | 0 | 4 | 16 |
| | | Risk Concentration areas | 0 | 3 | 17 |
| | Indicate categories for which the risk assessment should be made. | Finance | 0 | 1 | 19 |
| | | Strategic | 1 | 4 | 15 |
| | | Reputation | 0 | 7 | 13 |
| | | Legal | 1 | 3 | 16 |
| | | Operational | 0 | 1 | 6 |
| | Do you consider history of past events and their frequency during your assessment? | Yes | 0 | 4 | 16 |
| | Indicate your preferred approach to conduct a Risk Assessment | Questionnaires | 1 | 7 | 12 |
| | | Site Surveys | 0 | 6 | 14 |
| | | Workshops | 3 | 4 | 13 |
| | | Interviews | 0 | 5 | 15 |

**Table 6.2.3** Risk Assessment

**Observation**: The phase of Risk Assessment is also considered as essential to the respondents. During the Risk Assessment, threats like natural disasters, technological failures and man-made disasters should be analyzed and evaluated for their probability of occurrence and impact in the operation of an organization. It should be noted that specific threats such as geopolitical conditions, cyberattacks and terrorism have been also referenced by the respondents indicating their current role in today's world scene.

The outcome of the Risk Assessment effort should identify all the threats and risk concentration areas that may impact the operation of an organization, while the assessment should be made taking into account the different categories of finance, strategy, reputation, legal and operation. It should be noted that the categories for

which the risk assessment is conducted may have a different importance depending on the industry and operating environment of each organization.

The important role of history and past events has been also acknowledged by the respondents since their occurrence may indicate trends or vulnerabilities to specific threats and impacts.

Respondents indicated their different and joint preferences of conducting a Risk Assessment through questionnaires, site surveys, workshops and interviews.

At the end of the RA's part in the questionnaires there were two questions related to challenges managed during the RA execution and critical items to be taken into consideration. The feedback received is included as "Hints & Tips" in the respective RA section of Chapter 9, paragraph 9.2, along with detailed analysis and information for the RA process.

### 6.2.4 BC Strategy

The table below presents the collected results related to the BC Strategy.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| BC Strategy | Do you consider Strategy as critical to the Business Continuity Programme? | | 0 | 1 | 19 |
| | List areas that should be covered within Strategy | Activities & Processes | 0 | 3 | 17 |
| | | Technology / Infrastructure | 0 | 2 | 18 |
| | | Services / Products | 0 | 4 | 16 |
| | | Sites approach | 0 | 9 | 11 |
| | | Suppliers / Vendors | 0 | 0 | 12 |
| | Identify models / approach to be reviewed and followed | Own Site | 0 | 5 | 15 |
| | | Reciprocal Site | 3 | 10 | 7 |
| | | Third Party Site | 2 | 9 | 9 |
| | | Home Base | 0 | 9 | 11 |

**Table 6.2.4** BC Strategy

**Observation**: The development of a BC Strategy is considered as critical for almost all the respondents. BC Strategies should be identified and developed to secure the seamless operation of activities and processes and the provision of services and

products, the necessary technology and infrastructure to support them. Many respondents noted the importance of developing a BC strategy for third-party suppliers and vendors to secure redundancy in organization's support by external stakeholders.

During the development of BC strategy, the organization should review and decide on the different models of redundant operation such as: alternate, reciprocal, third-party or home-based site(s).

Detailed analysis and information related to BC Strategy process is included in Chapter 10.

### 6.2.5 BC Plans & Response Structure

The table below presents the collected results related to the BC Plans & Response Structure.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Business Continuity Plans & Response Structure** | Response Structure. Indicate the importance of different levels of Response Structure | Strategic | 1 | 5 | 14 |
| | | Tactical | 0 | 4 | 16 |
| | | Operational | 0 | 3 | 17 |
| | Response Structure. Issues to be considered while developing a response structure | Size | 2 | 3 | 15 |
| | | Complexity | 0 | 4 | 16 |
| | | Geographical Dispersity | 0 | 7 | 13 |
| | Business Continuity Plans. For each level of plans indicate the difference components to be included | Strategic – Strategies to be followed | 0 | 1 | 19 |
| | | Strategic - Communication | 0 | 3 | 17 |
| | | Strategic – Mechanism for monitoring | 2 | 7 | 11 |

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| | | Strategic – Legal & Regulatory requirements | 2 | 5 | 13 |
| | | Strategic – Coordination with the different levels | 0 | 6 | 14 |
| | | Tactical – Mechanism for coordination & monitoring | 0 | 5 | 15 |
| | | Tactical – Allocation of resources | 0 | 4 | 16 |
| | | Tactical – Coordination with the different levels | 0 | 7 | 13 |
| | | Operational – Allocation of resources | 0 | 3 | 17 |
| | | Operational – Coordination with the different levels | 0 | 5 | 15 |

**Table 6.2.5** BC Plans & Response Structure

**Observation**: The development of BC plans and the creation of the response structure to manage any major incident or disaster is the outcome of all previous phases and processes. Both components are critical for an organization to secure its capability to efficiently manage any disruption or impact caused by any type of disaster.

The response and management of any crises or disasters should be deployed in different layers and levels that have distinctive roles, responsibilities and accountabilities. This differentiation in the levels of response can ensure that the organization is capable of cohesively managing any impact or disrupt in its operation.

All respondents agree that during the development of the plans and the response structure, issues related to the size of the organization, its complexity in operations and geographical dispersity should be taken into account.

Finally, the respondents were asked to comment on the importance of the different components that may exist in the various levels of response plans and structures.

Detailed analysis and information related to BC Plans & Response Structure is included in Chapter 11.

### 6.2.6 Competency Development Programme

The table below presents the collected results related to the Competency Development Programme stage.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Competency Development Programme** | List objectives for a competency development programme | Evaluation of recovery capability | 0 | 0 | 20 |
| | | Confirm competency | 2 | 7 | 11 |
| | | Achieve BIA's RTOs & RPOs | 0 | 6 | 14 |
| | | Increase awareness | 0 | 3 | 17 |
| | | Validate continuity options | 2 | 4 | 14 |
| | | Readiness | 0 | 0 | 10 |
| | Types of Exercises to Development Competencies | Scenario | 1 | 7 | 12 |
| | | Notification | 3 | 15 | 2 |
| | | Simulation | 0 | 4 | 16 |
| | | Live | 0 | 5 | 15 |
| | | Disaster Recovery Tests | 0 | 0 | 8 |
| | Role of external stakeholders in Exercises and Competencies Development | Suppliers, Vendors | 1 | 6 | 13 |
| | Frequency of Tests | Annual | 1 | 1 | 18 |
| | | Semi-Annual | 3 | 14 | 3 |
| | | Quarterly | 145 | 5 | 0 |
| | | Monthly | 20 | 0 | 0 |

**Table 6.2.6** Competency Development Programme

**Observation**: The development of an exercise programme is critical in the BCM methodology. The continuity capability of an organization cannot be considered reliable unless it has been tested. All respondents have acknowledged the importance of the exercise programme. The objectives of such program that assist in increasing

the competency of an organization to sustain any disaster or major operational outages are: Evaluation of the recovery capability of an organization that may have already implemented a number of measures, increase the awareness of the personnel, check whether the achievement of RTOs & RPOs defined in the BIA process is possible, validate the efficiency of the implemented continuity options and finally as some of the respondents outlined the readiness of the entire organization to react in such events.

Types of exercises that can be conducted are: scenarios targeting specific type of events, notification call tree tests to measure the efficiency of notifying and mobilizing the necessary resources, tests that simulate specific outages or events, live exercises and disaster recovery tests that are related to the technical infrastructure.

The role of external stakeholders in such exercises is considered as important by many respondents because not only they will need to be part of the recovery in case of an actual event but also to test their readiness and support.

Finally, most of the respondents consider that the appropriate frequency of conducting the tests, depending always on the type of tests, should be annually or semi-annually.

More detailed information is included in the chapter 12.

### 6.2.7 Maintenance of BCM Programme

The table below presents the collected results related to the Maintenance of BCM Programme.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Maintenance of BCM Programme** | Importance of the Maintenance of BC arrangements | | 0 | 1 | 19 |
| | Factors triggering the need for Maintenance | Changes in BIA, RA, Strategy | 0 | 0 | 20 |
| | | Changes in legal & Regulatory Requirements | 2 | 9 | 9 |
| | | Reviews and/or Audits | 1 | 7 | 12 |

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| | | Organizational Changes, Changes in the operational environment | 0 | 0 | 5 |
| | Frequency of maintenance of BC Programme | Annual | 4 | 0 | 16 |
| | | Semi-Annual | 4 | 14 | 2 |
| | | Quarterly | 16 | 3 | 1 |
| | | Monthly | 16 | 2 | 2 |

**Table 6.2.7** Maintenance of BCM Programme

**Observation**: One of the aspects of BCM methodology that has been also identified as important is the maintenance process of BCM programme. Per respondents' input, factors that may trigger the necessity for maintenance may be changes in any of the previous mentioned BCM stages (BIA, RA and Strategy), changes in the legal & regulatory requirements under which an organization operates or as a result of finding by both internal or external audits. Another factor that may trigger the initiation of the maintenance of the BCM programme may be major changes in the organization or in the environment that the organization operates.

According to the respondents, the proposed frequency of initiating a maintenance process is on annual basis considering that more frequent updates (semi-annually, quarterly or monthly) may not be necessary and beneficial.

Detailed analysis and information related to the factors triggering the maintenance of BCM programme and its frequency are included in Chapter 13.

### 6.2.8 Review of BCM Programme

The table below presents the collected results related to the Review of BCM Programme.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **Review of Business Continuity (BC) Programme** | Review Importance | | 0 | 0 | 20 |
| | Types of Review | Audit | 0 | 4 | 16 |
| | | Management Review | 0 | 8 | 12 |
| | | Quality Assurance | 6 | 6 | 8 |

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| | | Performance Appraisal | 5 | 6 | 4 |

**Table 6.2.8** Review of BCM Programme

**Observation**: The review of the BCM programme is considered as critical by all respondents. The review of BCM programme can be conducted through different methods such as: audits (external and internal), management review, quality assurance and through performance appraisals.

Detailed analysis and information related to the different types of review of BCM programme are included in Chapter 13.

### 6.2.9 BCM Programme KPI Metrics

The table below presents the collected results related to the BCM Programme KPI Metrics.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| **BCM Programme KPI Metrics** | Importance of KPI Metrics in BC Programme | | 0 | 4 | 16 |
| | List KPI Metrics to be used in BC Programme | BIAs | 1 | 4 | 15 |
| | | RAs | 1 | 4 | 15 |
| | | Strategies | 1 | 6 | 13 |
| | | BCPs | 0 | 3 | 17 |
| | | Tests | 1 | 2 | 17 |

**Table 6.2.9** BCM Programme KPI Metrics

**Observation**: The purpose of BCM KPI's are to monitor and measure the performance of Business Continuity programme based on the references obtained through achievement of processes or goals. Most of the respondents outlined the high importance of setting KPIs in the BCM programme. KPIs that have been listed as important are related to Business Impact Analysis (BIA), Risk Assessment (RA), Strategy, Business Continuity Plan (BCP) and Tests.

More detailed information for the KPIs that can be applied to monitor the efficiency of the BCM programme is included in the chapter 14.

### 6.2.10 BCM Programme Major Challenges

The table below presents the collected results related to the BCM Programme Major Challenges.

| DOMAIN | QUESTIONS | COMPONENTS | IMPORTANCE | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| General | Identify major challenges during the implementation of a Business Continuity Programme | Project Management | 3 | 9 | 8 |
| | | Management commitment and understanding | 0 | 3 | 17 |
| | | Poor culture on top management | 0 | 2 | 18 |
| | | Lack of engagement of all organization | 1 | 3 | 16 |
| | | Size & complexity of organization | 1 | 10 | 9 |
| | | Confusion between the implementation of a BCMS and the investments required for BC solutions | 2 | 9 | 9 |
| | | Poor theoretical and practical background | 3 | 9 | 8 |

**Table 6.2.10** BCM Programme Major Challenges

**Observation**: At the end of the questionnaire, the respondents were asked to indicate the major challenges that they have managed during the implementation of BCM programmes. Some of the major challenges that were identified were related to:

- ✓ Project management issues during the implementation of the programme
- ✓ Poor or lack of management commitment and understanding related to the value of implementing a BCM programme
- ✓ Poor culture on top management
- ✓ Lack of engagement of all organization. During the BCM effort it is necessary to involve all parties and stakeholders to secure that nothing essential was left out

- ✓ The size & complexity of the operation of the organization is an issue that should be taken into consideration and cause various challenges
- ✓ Numerous times, practitioners face the confusion that is caused to the involved stakeholders by the differentiation that exists between implementation of the BCM programme and the solutions that need to be applied to allow the organization to continue their operations in case of disasters
- ✓ One major challenge that is frequently faced is poor theoretical and practical background related to BCM framework by both non experienced practitioners or decision makers within an organization

More detailed information related to challenges and proposed resolutions is included in the chapter 7.

## 6.3 Interviews' Content & Outcome

In total 15 BCM practitioners out of the 20 that responded in the questionnaires were interviewed.

The following table indicates the areas discussed and covered during the interviews. The topics and areas discussed followed the structure of the BCM lifecycle. The material collected through the interviews is presented in details in the subsequent chapters responding to the different stages of the BCM lifecycle in the form of approach description, hints & tips, practical examples and instructions to be followed for their efficient implementation.

To further facilitate the reading of the research a column has been added in the table indicating the respective chapter in which the content of the interviews has been incorporated.

| **Topics** | **Chapter in Research** |
|---|---|
| **Section A. Business Continuity Policy & Programme Management** | |
| 1. Scope & Objectives | **7** |
| 2. Project Management | |
| 3 Initialization of BCM effort | |

| Topics | Chapter in Research |
|---|---|
| 4. GAP Analysis | |
| 5. Discuss any challenges / hints & tips / items | |
| **Section B. Governance / Structure of BCM in Organizations (Roles / Responsibilities)** | |
| 1. Indicate organizational structure to support BCM Programme in an organization | **8** |
| 2. Discuss roles and responsibilities of the organizational structure | |
| 3. Discuss Training, Awareness sessions & competencies of the people involved in the development of a BCM programme | |
| 4. Discuss any examples of structure | |
| 5. Discuss any challenges / hints & tips / items | |
| **Section C. Business Impact Analysis (BIA)** | |
| 1. Identify the aims of BIA | **9.1** |
| 2. Indicate the best approach to conduct a Business Impact Analysis | |
| 3. Indicate the types of losses that need to be evaluated | |
| 4. What are the deliverables of a Business Impact Analysis | |
| 5. What should be the profile of the people involved in the execution of BIA from organization's side? | |
| 6. Indicate some challenges dealt during a BIA execution. | |
| 7. Discuss any examples | |
| 8. List any item that you may consider as critical for the BIA execution | |
| **Section D. Risk Assessment (RA)** | |
| 1. Provide indicative threats/risks to be assessed during the RA. | **9.2** |
| 2. Indicate the outcome(s) of a Risk Assessment | |
| 3. Indicate categories for which the risk assessment should be made | |
| 4. Role of history of past events and their frequency during your assessment | |
| 5. Indicate the best approach to conduct a Risk Assessment | |
| 6. Indicate stakeholders, dependencies for the execution of this phase | |
| 7. Discuss any examples | |
| 8. List any item that you may consider as critical for the RA execution | |
| **Section E. Strategy** | |
| 1. Discuss the areas that should be covered within this phase | **10** |
| 2. Identify models to be reviewed and followed in this phase | |
| 3. Discuss pros & cons for solutions and models for implementation | |
| 4. Discuss any help items / hints & tips | |

| Topics | Chapter in Research |
|---|---|
| **Section F. BCPs & Response Structure** | |
| 1. Indicate Levels of Response Structure and discuss their responsibilities | **11** |
| 2. Issues to be considered while developing a response structure | |
| 3. Types of plans to be developed within an organization | |
| 4. Discuss any examples | |
| 5. Discuss any help items for an efficient response and plans | |
| **Section G. Exercise Programme** | |
| 1. Discuss the objectives of the exercise programme | **12** |
| 2. Types and scope of Exercises | |
| 3. Role of external stakeholders in Exercises | |
| 4. Frequency & Necessity of Exercises | |
| 5. List items to be considered in the execution of the exercises | |
| 6. Discuss any help items / hints & tips | |
| **Section H. Maintenance of BC Programme** | |
| 1. Discuss the scope of Maintenance | **13.1** |
| 2. List factors that may trigger the need for Maintenance | |
| 3. Identify owners of maintenance and frequency | |
| 4. Discuss any help items / hints & tips | |
| **Section I. Review of BC Programme** | |
| 1. Discuss the scope of Review | **13.2** |
| 2. Identify types of Review | |
| 3. Discuss any help items / hints & tips | |
| **Section K. Metrics & Performance** | |
| 1. Identify and list metrics and key performance indicators to measure the efficiency of a BCM programme in an organization | **14** |
| **Section L. General** | |
| 1. Identify major challenges during the implementation of a Business Continuity Programme. Propose mitigation measures | **7 - 14** |

**Table 6.3.1** Interviews – Areas of Discussion

## 6.4 Important Note for Readers

Each of the subsequent chapters includes the necessary theoretical framework related to the topics presented, resources collected through the relevant literature review and all information and content that has been discussed and collected through the

questionnaires and interviews conducted. In the previous paragraphs there is specific correspondence of the chapters with the related sections of the submitted questionnaires and the interviews.

The chapters have been structured in such a way to address the gap between theory and practice and to ensure the support of theory with actual knowledge gained by the experience of practitioners that participated in the research. This critical lack of practical guidelines often results in misunderstanding of the methodology, commitment and deliverables by senior management in organization and mishandling of the effort and resources required to implement the BCM programme.

The content in each chapter presents the practical approach, methodology, material and examples to efficiently manage and complete each of the phases of the BCM lifecycle and to secure the proper implementation of a BCM programme in an organization. A major effort has been made to include in each chapter / phase the most frequent and major challenges faced during their respective implementation and to provide advice on ways to manage and overcome them.

By following and implementing the guidelines that are detailed presented in the subsequent chapters the process of developing and managing a BCM programme become a structured, smooth and controlled process that ensures the maximum efficiency and avoids unnecessary overload and dispute among the involved stakeholders.

# Chapter 7

# Business Continuity Policy & Programme

The policy and programme are the key directions that indicate the organization's orientation towards Business Continuity Management and requires top management action, support and commitment. The establishment of a clearly defined BC programme is essential for building an efficient resiliency framework and promotes the value of BC as a discipline. (Hiles: 2004, Hiles: 2011, ISO 22301:2019, Snedaker, Rima:2014)

## 7.1 Business Continuity Policy

The Business Continuity Policy is the document that defines the purpose, scope, context and governance of the business continuity programme. Within the document there should be a description of the requirements of the BC programme and the reasons of its implementation.

The principles that are recommended to be considered in the creation of a policy, are:

- How the organization implements business continuity and how the programme is structured and resourced
- Assurance that the policy is approved and owned by the top management
- Indicate how it supports the strategic objectives of the organization
- It should be suitable to the size, complexity and industry of the organization taking into account the cultural and operational environment

- Identify the standards and guidelines to be used as benchmark (The BCI Good Practice Guidelines 2018:14)

While developing a BCM policy in an organization is critical, it is also very important to communicate it to all interested parties and stakeholders. The policy should be visible in organization's official website, in the internal web portal, part of the induction material and integrated in the annual training and awareness material of the organization.

In Annex B, there is an indicative sample of a BC policy.

### 7.1.1 Hints & Tips

- ❖ It is strongly recommended that the policy document should not be complicated and extended. It should focus on including what will be done and the way of implementation
- ❖ The policy should be reviewed at regular intervals or following major changes in the organization, its regulatory and legal framework or in its operational environment
- ❖ It should include a very clear top management commitment and communicated throughout the organization
- ❖ A long and complicated policy may obstruct the effective communication of business continuity management. The policy should clearly state on what the organization will do and how it will be done. Sometimes organizations use short and long version for communicating the BC policy depending on the audience

## 7.2 Business Continuity Programme

The BC policy incudes the scope of the BC programme. The following considerations should be taken while determining the scope of the programme.

- An understanding of the areas to be included in the BC programme

- An understanding of organization's objectives, strategy and operating environment. The engagement of other relevant units of the organization such as risk, security and governance are critical to avoid conflicts and overlapping
- Products and services provided by the organization
- The role of outsourced activities, vendors and suppliers in the provision of organization's products and services
- Depending on the size and complexity of the organization, the programme can be implemented in phases and partially in the beginning and expanding the scope and the coverage in other areas gradually
- Other requirements such as geographical dispersion, regulatory and legal constraints
- Maximum extent of damage and disruption in the organization

The BC Programme should be considered as an ongoing process which is adapting to the internal and external changes of the operating environment of an organization. Hence, the implementation of such programme should involve all activities and phases of the BC Management lifecycle. During its initial implementation, it is important to allocate the necessary time to complete all activities of the full BC management lifecycle. The subsequent repetitions and revisions of the BCM lifecycle will require less effort and time depending on the extend of changes applied.

The outcome of a BC programme is to build and maintain a business continuity capability and improve the operational resilience of an organization. To be effective, the implementation of all phases of the BC lifecycle is necessary.

The project management methodology greatly assists in the implementation of the BC management programme. Hence, persons familiar with PM and involved in the BC programme would ensure its successful delivery within the agreed time frame and budget.

Examples of projects as part of business continuity programme can be:

- Initial implementation of BC Management Lifecycle

- Initiate & execute projects aiming to mitigate and / or eliminate risks identified during Risk Assessment
- Managing an Exercise programme
- Developing and implementing a Training & Awareness programme

### 7.2.1 Hints & Tips

- Software options are available to be considered as useful tools to support business continuity programme. These options provide many advantages in the management of large volumes of documents and in the automation of certain activities. Therefore, the selection of such option should be carefully evaluated and planned taking into consideration the associated costs of licensing, training and maintenance

- Depending on the size and complexity of the organization, it is recommended that the implementation of the BC programme to be broken down in smaller projects for easier and more efficient management. This will also help the organization to develop in a gradual approach the necessary technical solution and infrastructure required to support the recovery options

- It is critical that trained and experienced persons should be assigned the management of the projects derived from the implementation of the BC programme. It is important to avoid usual PM failures causes as they will impact negatively BC programme image and scope. Hence, all PMI's standards and methodology should be applied (PMI PMBOK® Guide: 2018)

- It is critical that the top management should clearly understand the scope of the BC programme to be able both to support it and commit to it. Therefore, it is important for the BC professional(s) involved in the setting of the BC programme to provide evidence of the benefits and ROI derived of the proper implementation

- While deciding on which products and services should be included in the scope of the BC programme, the following indicative issues should be considered:

    - Financial or reputational loss due to not be able to deliver or produce

- Legal and/or regulatory requirements related to products and/or services
- Contractual commitments towards customers/clients
- Involved Stakeholders

❖ In some cases, there may be confusion among the decision makers in relation to the proper implementation of a BCMS and the investments that are required for the realization of the BC solutions that will be identified during the strategy phase. Such confusion may delay or suspend the BC programme as too expensive or non-applicable. The BC professional(s) should carefully design and deliver awareness session to educate the top management

❖ In the process of defining the scope of the BC programme, a variety of methods can be used, such as: Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis, Market Analysis Techniques, Cost Benefits Analysis, etc.

❖ Often the principles of DR, BC and IT continuity are regarded as identical and that results in misunderstanding or misinterpreting the scope of BC programme. BC professional(s) should clearly define and explain the scope, role and limitations of those definitions to align all stakeholders in the same understanding and expectations related to the BC programme

❖ In certain cases, due to poor culture of top management (e.g., concept of "it won't happen to us") or due to the desire to use BCM as tool that will allow an organization to access more easily various markets (e.g., RFP requirement), the scope of BC programme is limited and not operational. The BC professional(s) need to educate the top management of the benefits of a proper BC programme and provide solid evidence and examples of such implementations. BCM should not be considered a market penetration tool

❖ If external vendor(s) or supplier(s) are involved or supports product(s) or service(s) provided by the organization and within the scope of the BC programme, then it is necessary that these external organizations to be also included in the BC programme along their respective supply chains and ICT

infrastructure. It is very important to evaluate the resilience and endurability of the supply chain of an organization to avoid sudden and unexpected disruptions in the specific area when most needed during the management of a disaster

## 7.3 GAP Analysis

This phase is usually implemented in the early stages of the Business Continuity Management Programme and greatly assists the identification of the areas to be included in both policy and scope of the programme. Therefore, in case in the organization there is no previous BC effort or framework, this task will provide a clear picture of current status and analysis of the maturity of the organization's **Business Continuity Management preparation, competence and capabilities** in place, in relation to e.g., international standard ISO22301. It may be repeated in the subsequent executions of the BCM lifecycle.

It also assists the organization

- To define and decide on the roadmap and actions required to achieve its overall organization resilience and implementation plan approach.
- In redesigning effort (if and where required), in ensuring that budgets allocated are routed to and support the appropriate business needs, in relation to Business Continuity.

Gap Analysis usually is conducted via

- Personnel interviews and workshops
- Review and Analysis of the existent framework documentation including existing procedures and working methods followed in an organization
- Sites visits
- Using templates and questionnaires

This assessment will evaluate existing BCM Framework, Operations and Processes to identify any possible gaps in the current Business Continuity Preparations, Solutions & Management system in place within an organization.

Furthermore, the current status and effectiveness of Business Continuity within the company is measured. The effort also results in determining what needs to be done to achieve best performance & compliance.

Areas to be assessed include – among other - the following

- Scope and Business Continuity objectives
- BCM policy & current implementation approach & strategy
- Needs & Expectations of interested parties
- Legal & Regulatory Requirements
- Management Commitment & Leadership
- Resources required & currently available for the establishment, implementation, operation and maintenance of the BCM, including Roles & Responsibilities
- Personnel competency
- Existence and control of required documentation and records
- Business Impact Analysis, Risk Assessment, corresponding risk treatment and Business Continuity Strategy provisions & history in place
- Current Business Continuity, Incident Management & Crisis Management planning & solutions
- Status of exercising, auditing and management review processes
- Current Status of Public Relations and Crisis Communication preparation
- Audit, change management, maintenance and improvement
- …

The outcome of the GAP assessment should be presented according to the Clauses, Contents and requirements of the international standard against which is analysed (e.g., ISO 22301), while visualization of the outcome greatly assists management to understand organization’s current status compared to standards.

The following example presents an example of the outcome of GAP Analysis in an organization along with the relevant visualization through a histogram. The scale of measuring the findings is similar to the one used during similar audits.

To facilitate the effort, for each ISO22301 requirement as defined and described in the Standard, a compliance score may be given. The following table depicts an indicative grading of the compliance score that may be used.

| SCORE | EXPLANATION | COMPLIANCE |
|---|---|---|
| 0% - 35% | Not adequate or limited compliance related to the requirements of ISO 22301 | NO |
| 36% - 55% | Partial of the existing framework, procedures, mechanism to the requirements of ISO 22301 | PARTIAL COMPLIANCE<br>may include major non conformities yet |
| 56% - 80% | Extended compliance of the existing framework, procedures, mechanism to the requirements of ISO 22301 | COMPLIANCE<br>may include (temporarily accepted as) minor non conformities |
| > 80% | Fully compliance of the existing framework, procedures, mechanism to the requirements of ISO 22301 | FULL COMPLIANCE |

**Table 7.1:** Grading of Compliance Score

**Example**

Major : Major Non-Conformity

Minor : Minor Non-Conformity

ICR : Improvement / Correction required

| ID | GRADE | FINDING | RECOMMENDATION | AREA | ISO CLAUSE |
|---|---|---|---|---|---|
| 001 | Major<br>ICR | Documentation related to the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, is not adequate and needs to be developed in all areas (activities, partnerships, supply chains, relationships with interested parties).<br>Links to other (under development) Management Systems are not addressed.<br>Management Approval of the documentation is required. | Document all organization's activities, functions, Services & products, Stakeholders (partnerships, supply chains, relationships with interested parties).<br>Services related documentation needs update & upgrade to comply with the standard's concept.<br>Typical Documentation may be included in (either separately or as one)<br>• BCM Framework (including Policy and processes)<br>• Services List / Catalog | Context of the Organization | 4.1<br>4.2.1 |

| ID | GRADE | FINDING | RECOMMENDATION | AREA | ISO CLAUSE |
|---|---|---|---|---|---|
| 002 | Major | No documentation has been identified to determine the requirements of the interested parties comprising the stakeholders.<br>No legal and regulatory requirements have been taken into consideration. No documentation was found in place.<br>BCM Scope is missing and requires to be defined. | The organization should (determine &) document the requirements of interested parties (Stakeholders List & Continuity Requirements).<br>This should include Legal & Regulatory Requirements.<br>A process to keep these updated should be in place | Context of the Organization | 4.2.1<br>4.2.2<br>4.3.2. |
| … | … | …. | …. | … | … |

**Table 7.2:** GAP Analysis Findings Log

The next table presents the evaluation of the compliance of an organization's Business Continuity Management System in relation to the ISO 22301. The items / questions used for the evaluation of the organization are strictly based on the content, structure and requirements of ISO 22301.

| TABLE OF CONTENTS | | | | | COMPLIANCE TO ISO 22301 | | |
|---|---|---|---|---|---|---|---|
| AREA | SUB-AREA | PARAGRAPH | | TOTAL NO OF QUESTIONS | Maximum Compliance Score | Compliance Score Achieved | % Compliance |
| 1 | CONTEXT OF ORGANIZATION | | | 15 | 60 | 25 | 42% |
| | 1 | Understanding the Organization and its context | | 3 | 12 | 9 | 75% |
| | 2 | Understanding the needs and expectations of interested parties | | 4 | 16 | 4 | 25% |
| | | 1 | General | 1 | 4 | 1 | 25% |
| | | 2 | Legal and regulatory requirements | 3 | 12 | 3 | 25% |
| | 3 | Determining the scope of the business continuity management system | | 7 | 28 | 11 | 39% |
| | | 1 | General | 1 | 4 | 2 | 50% |
| | | 2 | Scope of the BCMS | 6 | 24 | 9 | 38% |
| | 4 | Business continuity management system | | 1 | 4 | 1 | 25% |
| 2 | LEADERSHIP | | | 22 | 88 | 49 | 56% |
| | 1 | Management commitment | | 12 | 48 | 26 | 54% |
| | 2 | Policy | | 8 | 32 | 17 | 53% |
| | 3 | Organizational roles, responsibilities and authorities | | 2 | 8 | 6 | 75% |
| 3 | PLANNING | | | 11 | 44 | 13 | 30% |
| | 1 | Business continuity objectives and plans to achieve them | | 11 | 44 | 13 | 30% |
| 4 | SUPPORT | | | 26 | 104 | 60 | 58% |
| | 1 | Resources | | 1 | 4 | 2 | 50% |
| | 2 | Competence | | 4 | 16 | 8 | 50% |

| TABLE OF CONTENTS | | | | | COMPLIANCE TO ISO 22301 | | |
|---|---|---|---|---|---|---|---|
| AREA | SUB-AREA | PARAGRAPH | | TOTAL NO OF QUESTIONS | Maximum Compliance Score | Compliance Score Achieved | % Compliance |
| | 3 | **Awareness** | | **4** | **16** | **9** | **56%** |
| | 4 | **Communications** | | **7** | **28** | **16** | **57%** |
| | 5 | **Documented Information** | | **10** | **40** | **25** | **63%** |
| | | 1 | General | 2 | 8 | 4 | 50% |
| | | 2 | Creating and updating | 2 | 8 | 4 | 50% |
| | | 3 | Control of Documented Information | 6 | 24 | 17 | 71% |
| **5** | **OPERATION** | | | **78** | **312** | **210** | **67%** |
| | 1 | **Operational Planning & Control** | | **1** | **4** | **2** | **50%** |
| | 2 | **Business Impact Analysis & Risk Assessment** | | **15** | **60** | **36** | **60%** |
| | | 1 | General | 5 | 20 | 10 | 50% |
| | | 2 | Business Impact Analysis | 5 | 20 | 10 | 50% |
| | | 3 | Risk Assessment | 5 | 20 | 16 | 80% |
| | 3 | **Business Continuity Strategy** | | **16** | **64** | **39** | **61%** |
| | | 1 | Determination and selection | 5 | 20 | 10 | 50% |
| | | 2 | Establish resource requirements | 8 | 32 | 17 | 53% |
| | | 3 | Protect and mitigation | 3 | 12 | 12 | 100% |
| | 4 | **Establish and implement business continuity procedures** | | **39** | **156** | **114** | **73%** |
| | | 1 | General | 7 | 28 | 14 | 50% |
| | | 2 | Incident Report Structure | 9 | 36 | 36 | 100% |

| TABLE OF CONTENTS | | | | | COMPLIANCE TO ISO 22301 | | |
|---|---|---|---|---|---|---|---|
| AREA | SUB-AREA | PARAGRAPH | | TOTAL NO OF QUESTIONS | Maximum Compliance Score | Compliance Score Achieved | % Compliance |
| | | 3 | Warning and Communication | 8 | 32 | 24 | 75% |
| | | 4 | Business Continuity Plan | 14 | 56 | 37 | 66% |
| | | 5 | Recovery | 1 | 4 | 3 | 75% |
| | 5 | **Exercising and Testing** | | **7** | **28** | **19** | **68%** |
| **6** | **PERFORMANCE EVALUATION** | | | **50** | **200** | **69** | **35%** |
| | 1 | **Monitoring, measurement, analysis and evaluation** | | **17** | **68** | **20** | **29%** |
| | | 1 | General | 12 | 48 | 12 | 25% |
| | | 2 | Evaluation of business continuity procedures | 5 | 20 | 8 | 40% |
| | 2 | **Internal Audit** | | **9** | **36** | **25** | **69%** |
| | 3 | **Management Review** | | **24** | **96** | **24** | **25%** |
| **7** | **IMPROVEMENT** | | | **14** | **56** | **14** | **25%** |
| | 1 | **Nonconformity and corrective actions** | | **14** | **56** | **14** | **25%** |
| **TOTAL NO OF REQUIREMENTS EXAMINED** | | | | **216** | **864** | **440** | **51%** |

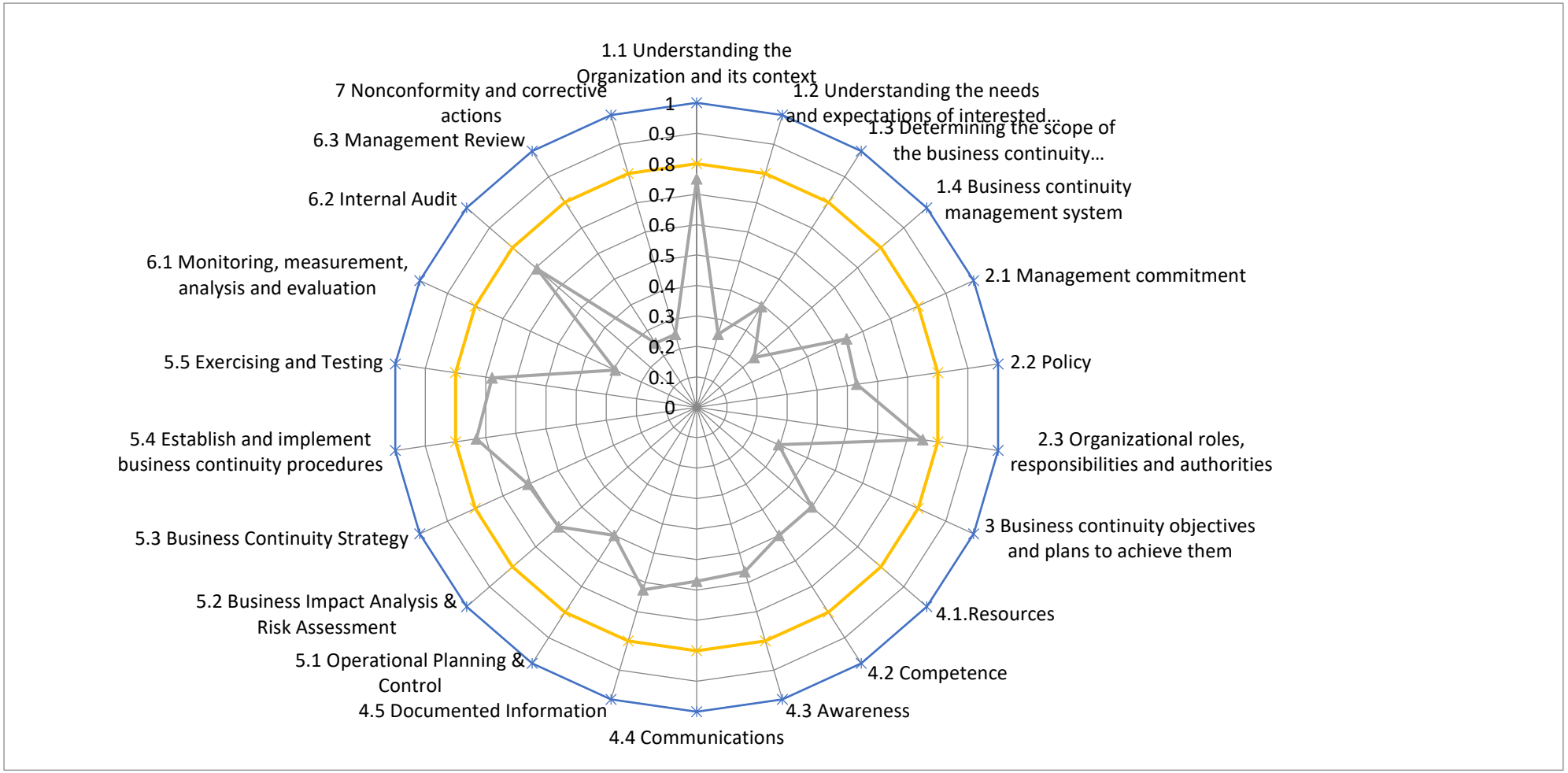



**Figure 7.1:** Histogram indicating depicting organization's compliance score in relation to each of the areas included in the ISO 22301

# Chapter 8

# BC Governance & Embedding

The efficiency of the BC programme is highly dependent on setting clearly defined roles and associated responsibilities and authorities of those involved in the programme. The chapter provides detailed information for those roles by presenting a proposed model of BCM structure in an organization.

Moreover, the chapter addresses the issue of embedding BC in an organization by proposing issues to be considered while integrating business continuity practice into the organizational culture.

## 8.1 BC Structure - Roles & Responsibilities

For an effective business continuity programme, it is critical to clearly define roles, responsibilities and authorities to manage the programme. The structure and assignment are also usually described in the business continuity policy document.

Top management should assign the accountability, responsibility and authority to teams or individuals that will properly implement the BC programme in accordance with the requirements of the policy. It is important that the roles should be allocated to the individuals with the appropriate competency and training to meet the objectives. Top management should ensure that these roles and responsibilities are communicated throughout the organization.

Even in the case that the assigned business continuity responsibilities are additional to their existing role in the organization, these new assignments should be included in the job description. Hence, their performance should be evaluated and assessed in those duties as part of the annual appraisal process.

The following model presents a proposed structure of BCM within an organization along with their assigned responsibilities.

### 8.1.1 Business Continuity Management Steering Committee

The members of the Board of Directors may act as the BCM Steering Committee. CEO is a member of this Committee, though he is the person to finally approve and sign all relevant documents and company decisions in relation to BCM, as of this Framework.

Members' responsibilities are the following:

- Ensure that this policy is adopted and implemented
- Define and approve the organizational structure of BCM within an organization
- Define and approve relevant roles & responsibilities
- Ensure that all members of the Line Management are aware of their roles and responsibilities
- Define, drive and support the BCMS implementation. Ensure compliance with this BCM Policy & Framework and the Standards, is monitored and controlled
- Review BCMS status on a regular basis (as deemed necessary)
- Review, Prioritize and approve the Business Continuity Strategies and expenditures required
- Review and respond to the annual BC Management Report submitted, and its requirements.
- Review & approve Post incident reports and recommendations

### 8.1.2 Business Continuity Manager / Head of Business Continuity management unit

The Business Continuity Manager leads BCM activities, drives and updates this framework and the mechanisms of this policy to be implemented. His/her responsibilities are:

- Ensure that all BCM activities are conducted and implemented in an agreed and controlled manner
- Select, Design, Document, Review, Improve, Update and Approve (have approved) all relevant Policies, Framework, Standards, Organization Structure, Methodologies, Procedures, Processes, standardized Templates of any kind to be used by the organization as part of the BCM System.
- Ensure that all relevant positions as of the BCM organization structure (i.e., BC Representatives) are fulfilled and personnel competences are in place.
- Achieve a BCM capability that meets changing business needs and is appropriate to the size, complexity and nature of the company
- Ensure full compliance of an organization’s BCM provisions with the requirements of all the current Laws and Regulations in relation to BCM as well as the BCM Standards adopted by the company.
- Determine, Update and Approve (have approved) the scope of Business Continuity Management
- Ensure company's Response Preparedness. Ensure that Emergency Response, Incident and Crisis Management Plans exist in order to respond effectively in case of significant incidents.
- Ensure that Business Continuity and Disaster Recovery Plans, Solutions and Documentation are in place, are applicable, approved, properly tested and maintained as per this Framework requirements.
- Supervise and ensure on an annual basis the successful completion of the overall BC Life cycle activities as defined in the relevant Framework paragraph, including
    - Business Impact Analysis
    - Risk Assessment
    - BC Strategy(ies), Incident, Crisis, Business Continuity Management and Disaster Recovery Plans

- Testing & Exercising
- Training & Awareness
- Audit & Nonconformities
- Key Performance Indicators
- Business Continuity Management System Review

Responsibility includes

- The proper preparation and roll-out of the activities (with the exception of Audit)
- the analysis of the results and the outcome of each activity, definition of changes / updates required, report preparation, presentation to and approval of the relevant Reports, Outcomes and Decisions Required for each activity to BCM Steering Committee.

- Supervise the preparation by the relevant (engaged to the incident) Business Unit, review, comment & submit to BCM Steering Committee Post incident reports and recommendations. Follow-up the implementation of Steering Committee decisions.
- Once required, facilitates and provides support, awareness and input to all teams and personnel in relation to BCM activities to ensure quality results in all efforts and activities.
- Ensures proper document management and archiving, version control and distribution of all BCM documentation

### 8.1.3 Head of the Business Unit - Line Management

The company's line management shall enforce overall compliance with the Business Continuity Management guidelines. Their responsibilities are the following:

- Identify key personnel for their Business Units, assign and train adequate resources to support BCM functions and capabilities within their unit. Appoint

a BCM Representative who is qualified to manage and co-ordinate business continuity activities in accordance with the BCM policy

- Ensure their Business Unit's Business Impact Analysis is prepared on an annual basis, approved and submitted to BC Manager
- Ensure their Business Unit's Risk Assessment is conducted on an annual basis under the existing Risk Management Framework of an organization and approved; Risks registered and relative Risk Mitigation decisions are made and are properly followed up
- Approve the Business Continuity Strategy (in relation to their area of responsibility) to be implemented
- Ensure that all BC/DR Plans of their area of responsibilities have been properly prepared. Evaluate and approve the BC/DR Plans and relevant documentation in relation to their areas of responsibilities, before they are submitted to BC Manager. Some Business units may have BC Plans for the Recovery of their Units' operation as well as BC/DR Plans for the recovery of Technology Systems they supervise
- Ensure that the annual testing Schedule of their BC/DR Plans is in place and maintained
- Ensure that their BC/DR Plans are exercised according to the annual testing schedule and reviewed either regularly or when major changes occur
- Ensure that Business Continuity Requirements are embedded in the product / service development / update / change process they supervise (if any) in order to ensure adequate planning
- Ensure that Business Continuity Requirements are included in the scope of all company projects (in relation to their areas of responsibilities) and ensure adequate budget allocation to relevant activities upon approval by the BCM Steering Committee
- When is deemed necessary and once authorized, they should ensure proper activation and implementation of their BC/DR plans

- Inform immediately the Business Continuity Manager for any issue related to the availability and applicability of their BC/DR plans

### 8.1.4 Business Continuity Representative (Business Unit)

BC Representatives are members of the company's Business Units, act as liaisons, representing the interests of their Business Units, and coordinate the Business Continuity preparation activities in their functional areas.

Their responsibilities are listed below:

- Be the focal point between the BC Manager and the Business Unit for all the BC Management issues. Approval for all his/her activities outcome is required by his/her Business Unit Head
- Coordinate and Facilitate the Business Unit effort to Prepare and document the annual Business Impact Analysis
- Coordinate and Facilitate the Business Unit effort to prepare and document the annual Risk Assessment
- Reviews and follows up (once approved and communicated) the Risk Mitigation Plan implementation in relation to its Business Unit in relation to BCM
- Coordinate and Facilitate the Business Unit effort to the development and documentation of Business Continuity and Disaster Recovery Strategies
- Coordinate and Facilitate the Business Unit effort to the development and documentation of Business Continuity and Disaster Recovery Plans
- Review, submit improvements on, Control version and maintain their own Business Unit continuity plans. Ensure proper storage of Plan copies to the designated points of availability
- Maintain the list and availability of critical staff in their Business Units and communicate any changes to the Business Continuity Manager
- Ensure the implementation of BC and DR Plans tests and exercises as well as the Pre and Post exercise reports. Submit Reports to BC Manager

- Supervise and ensure the preparation by the Business Unit and delivery to BC Manager of any Post-incident report that occurred in his/her Business Unit's area of responsibility
- Ensure that any issue related to business continuity will be reported immediately to Business Continuity Manager
- Is informed on the budget allocation and is monitoring business continuity related projects in his/her Business Unit
- Attend trainings and education sessions prepared by BC Manager. Propose to BC Manager, trainings and awareness needs and requirements for him/her and/or his/her Business Unit personnel on BCM issues

### 8.1.5 BC/DR Plan Owner

BC/DR Plan owners are the people responsible for the content of the BC/DR Plan documentation and manage the Recovery operation as of the BC/DR Plan provisions, once plans are invoked.

Each Business Unit may have several BC/DR Plan owners, depending on the number of plans (Business Unit Recovery Plan, System 1 Recovery Plan, System 2 Recovery Plan, …), yet one of them is responsible to Coordinate the overall effort at a Business Unit level.

BC/DR Plan owners are responsible to

- Prepare the content of each plan and ensure the content is accurate and provides the required information (as per the BC Manager instructions) for the recovery of the Activities or Systems.
- Review plan periodically and ensure that the content is updated and will successfully support the recovery of the relevant activities or system, once plan is invoked.
- Manage / lead the Recovery process for the specific Plan, once it is invoked, and prepare the relevant post-incident report

- Run / lead the relevant to the Plan exercises and prepares pre and post exercise reports
- Ensure that all participants within the recovery plan are adequately trained on the plan provisions, their role & responsibilities during the recovery
- Ensures that the Plan document is available at the designated location(s)

### 8.1.6 Hints & Tips

- ❖ It is strongly advised that a sponsor should be assigned for the implementation of the Business Continuity Programme. This person should be member of the upper management within an organization and ensures the success and efficiency of the implementation of the BC programme. Offers support, acts as an escalation point for issues when something is beyond BC manager's control
- ❖ Succession plan should exist for all individuals with specific roles and responsibilities within BC programme
- ❖ Those responsible to manage the BC programme should have or be working towards a professional credential from an appropriate professional body. High expertise and experience of those professionals managing the BC programme plays a critical role in the efficiency and outcome of all BC arrangements
- ❖ In the framework of BC programme implementation, it is critical that to ensure that owners have been assigned to all BCM arrangements, systems, applications, units, services and products that are involved in the scope of the BC programme
- ❖ The alternates should be fully aware of their roles and responsibilities and involved in all programme activities
- ❖ Roles and responsibilities related to BCM programme's development and management should be integrated and assimilated in the organization's structure as the rest of any functional roles

## 8.2 Embedding BC In Organization

Embedding business continuity in an organization is a critical goal that requires a collaborative approach by both top management and the BC responsible by aligning all relevant activities with the organization's strategic goals and culture. (Trebilcock:2010)

The embedment of BC management is accomplished through various steps:

- Identify all the stakeholders and parties within the organization that are required to be engaged
- Understand their key interests, priorities and concerns and identify best means to address them and engage them
- The benefits and return on investment of business continuity management should be communicated through organization's events and appropriate communication channels
- Ensure that Business Continuity is considered in the organization's strategic plans
- Include BC requirements in the planning of new products or services and in the supply management
- Include BC in the standard operating procedures used by the organization
- Include Business Continuity awareness in the standard induction process of the organization

Another important aspect of the successful embedding of BC in an organization is the building of an appropriate awareness level, continuous education and training. To accomplish that:

- Need to define the competencies and skills of all individuals involved in the BC programme
- Identify the training and awareness needs with specific outcomes for all those individuals

- Design the desired level of relevant activities to increase both awareness and competence levels
- Evaluate the effectiveness and integrate those activities as part of the continuous improvement

### 8.2.1 Hints & Tips

- ❖ The successful and efficient implementation of Business Continuity Programme requires both general management and technical skills
- ❖ Develop a network of influential individuals within the organization that understand the benefits of business continuity and resilience. These individuals will make significant contribution to the successful embedding of BC
- ❖ Seek opportunities to integrate business continuity in existing planned events such as evacuations, security drills, etc. to further promote the value of BC
- ❖ An increased number of organizations use intranet to design modules for training for specific business areas. Hence, BC should take advantage of such process to incorporate related training modules not only for individuals involved in the BC programme but also targeting all employees in an organization
- ❖ Intranet or informative / communication banners should be used in regular intervals to increase the awareness of the employees for issues related to BC within an organization
- ❖ Training required or conducted related to BC should be documented as part of BC programme and be incorporated in each individual standard training record
- ❖ Motivation is important for all areas of business. Hence, it is highly recommended that team building activities should be regularly scheduled for all individuals in the BC programme of an organization. In some organizations extra payment or other non-financial recognition is provided for individuals that are part of emergency response structure

- Typical training activities such as external training sessions, workshops, seminars and conferences should be regularly scheduled based on the training needs of the team and expenses are often covered by the organizations
- It is critical to regularly educate and increase the awareness of the top management for issues related to BC. Hence, specific effort should be made by the BC professionals towards this direction and carefully designed modules should be planned

## 8.3 BCM Process Flow

After the initial implementation, the BCM Lifecycle is an ongoing process where all of its stages are repeated usually on annually basis.

The following diagram presents a recommended indicative model of operation of a medium size organization with all phases of the BCM lifecycle with short details that are further presented and explained in the following chapters. Depending on the size and complexity of the organization there may be changes in the timeline and the involved stakeholders.

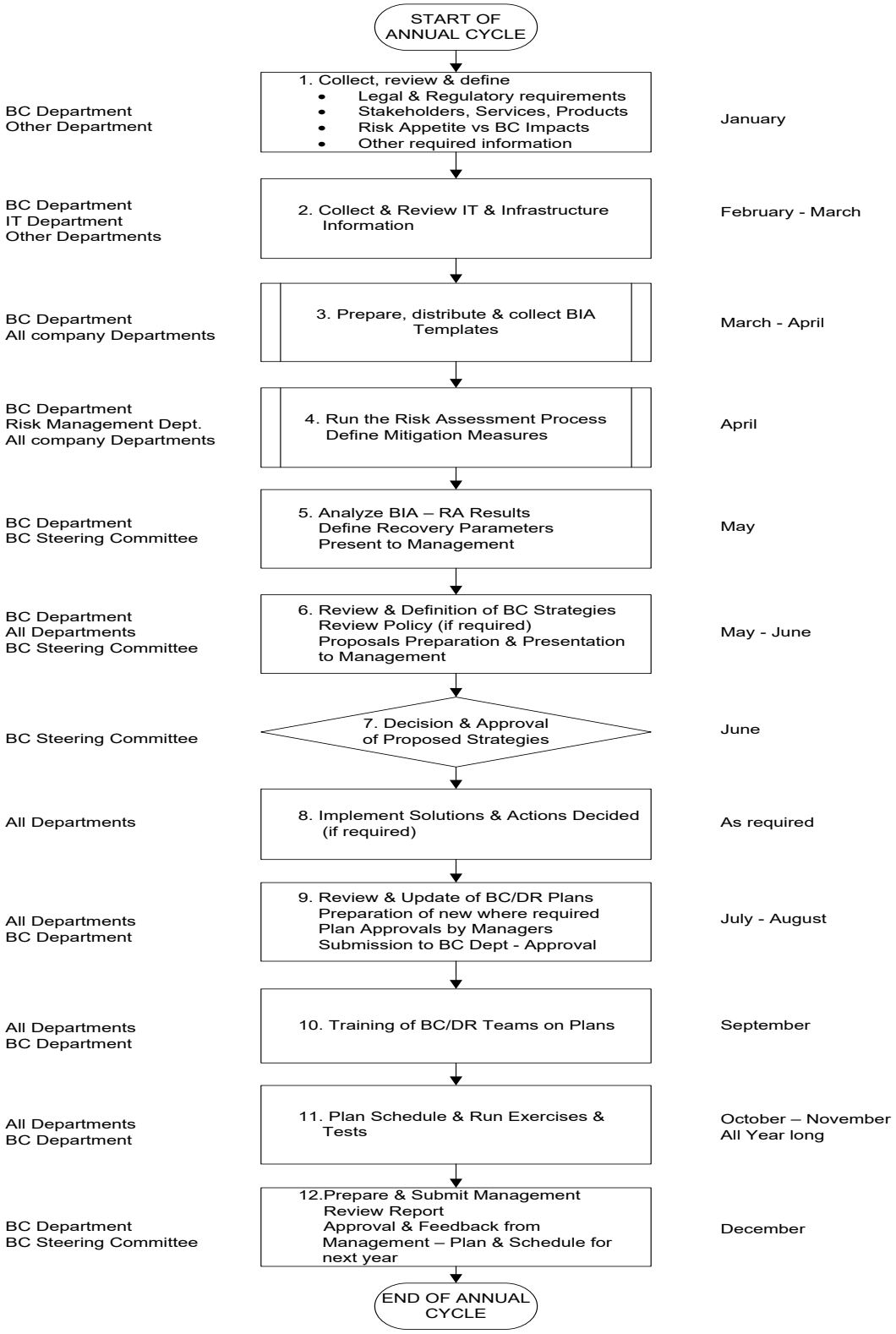



**Figure 8.1:** Indicative BCM Process Flow that incorporates the annual lifecycle

### 8.3.1 Process Description

#### *8.3.1.1 Collection, Review & definition of Business Parameters*

Organization's BC Unit cooperates with the relevant company Business Units to collect / update / review and define

- Legal and regulatory requirements for the organization in relation to BCM
- Current list of Stakeholders and their interests
- Current list of Services & Products
- Risk Appetite, Heat Matrix, Disruption & BC Impact figures
- Current related Policies (i.e., Information Security BC Policy, ITSM BC Policy, Risk Management Policy)
- Standards to be utilized (i.e., ISO22301)
- Other required information

BC Unit ensures that all Business Units of the organization have assigned their BC Representatives.

For new BC Representatives, an introductory training on BC Management is prepared and delivered by BC Unit.

| | |
|---|---|
| Process Owner | : BC Unit |
| Contributors | : Rest of the Business Units (per case, as required) |
| Deliverables | : Business environment requirements and company standards to be used |
| Delivery Period | : January |

#### *8.3.1.2 Review of current Technology Infrastructure BC/DR status*

ICT Business Unit provides an updated version of the relevant information that will allow BC Unit to have a picture on

- The BC / DR Status & Capabilities for all Applications and Systems supported (including RTOs, RPOs, Availability Status, Backup)

- The BC / DR Status and redundancy capability of IT infrastructure & Communications to support availability of organization's Services

Process Owner : BC Unit

Contributors : ICT Business Unit

Deliverables : Current picture on BC / DR capabilities of ICT-related infrastructure

Delivery Period : February - March

#### *8.3.1.3 BIA information collection*

Considering the information collected in paragraph 5.3.1.3, BC Unit reviews the previous year's BIA Collection template and prepares the current year's template to be used, according to the company (new/current) needs. New needs may include new Business Units and/or organization changes, new services, new applications, resources, new business & strategic priorities and of course new policies and procedures.

BC Unit prepares list of the Business Units / units that will participate in the BIA in accordance with organization's structure.

A training session is prepared by BC Manager and delivered to BC Representatives to explain the BIA Template and ensure their understanding of the BIA process.

BC Manager distributes to each Business Unit:

- Previous year BIA information on their Business Unit
- Current year's BIA templates
- Services list, Heat matrix, other supportive information if required

and defines timeframes for input collection.

A separate BIA response is required for every Business Unit, for every different Site the Unit operates.

BIA responses from all Business units are collected.

Process Owner : BC Unit

| | |
|---|---|
| Participants | : All Business Units with the assistance of their BC representatives and the approval of their management |
| Training | : Prepared and delivered by BC Manager to BC representatives. |
| Deliverables | : Training to BC Representatives<br>BIA responses from all company Business Units |
| Delivery Period | : March - April |

#### *8.3.1.4 Risk Assessment & Management*

BC Unit, in coordination with the Enterprise Risk Management Business Unit should run the Risk Assessment process to identify operational threats and risks exposures.

The approach should be aligned with the Risk Management Policy & Process that needs to be developed and the process for the BC-related Risk Assessment should be integrated in the annual Risk Assessment of the ERM Business Unit.

Areas to be assessed include, but not limited to

- IT Risks (i.e., current High Availability status, SLA status, DR capabilities, backup status, governance issues in relation to BCM)
- Site Infrastructure (Security, Power etc.)
- Business environment changes & requirements
- BC / DR capabilities and lack of capabilities in key areas
- Vulnerabilities in relation to Business Units activities
- Compliance to regulatory & legal requirements
- Compliance to BC Standards adopted
- Personnel issues

Based on the needs, a GAP analysis effort may be decided to be also run, that will provide the company with the picture and the relevant deviations of the applied Business Continuity Management System as per the international standards.

Process Owner : BC Unit - Risk Management

Contributors : All Business Units with the assistance of their BC representatives

Deliverables : Risk Assessment Report – Risk Treatment – Management Report, GAP Analysis Report (optional)

Delivery Period : April

#### *8.3.1.5 Analysis of BIA & RA results – Recovery parameters definition*

Input from BIAs collected as well as Risk Assessment effort outcome is reviewed, assessed, analyzed and processed by the BC Manager to prepare a company-wide picture.

This picture (and relevant report outcome) includes

- Activities prioritization & impact analysis
- Impact Analysis as of current business environment
- Current recovery parameters (MTPD, RTO, RPO) & priorities as a result of the above impact analysis
- Dependencies, key Suppliers and Resources required (including personnel, IT systems & applications, Communications, infrastructure, vital records)
- Gaps as of existing BC / DR Strategies and current environment assessment
- Proposals for changes to key BC parameters (i.e., RTOs etc.)

Results are documented and presented to BC Steering Committee for review approval and decision making where required.

Company recovery parameters (RTOs, RPOs, and MTPDs) are finalized and information is utilized for the next process step.

Process Owner : BC Unit

Participants : BCM Steering Committee

Deliverables : A combined BIA and RA outcomes report, including proposed recovery parameters. Company Approved Recovery Parameters

Delivery Period : May

#### *8.3.1.6 BC Strategies review & update*

BIA & RA results are communicated to all Business Units (on a need-to-know basis) together with current BC / DR Strategy that is in place (as of the previous year) as well as the company recovery parameters (RTOs, RPOs, MTPDs) that have been defined in the BIA effort.

All Business Units should review their current status – in relation to BC / DR Strategy & related requirements, update (or create new when required) and improve current if and where required and propose changes and/or improvements to BC Steering Committee.

Approach includes the ICT strategy as well.

BC Unit is responsible to review the BC strategy at company-wide level (including current provisions in Incident Management, Crisis Management, BC Invocation plans etc.) and prepare the relevant proposed changes.

Inputs and Proposals are collected by BC Unit, summarized and presented (with the contribution of each team proposing) to the BCM Steering Committee.

| | |
|---|---|
| Process Owner | : BC Unit |
| Contributors | : All Business Units with the assistance of their BC Representatives and the approval of their management |
| Deliverables | : BC Strategy approach Report at Company & Business Unit level, including ICT |
| Delivery Period | : May - June |

#### *8.3.1.7 Top management approvals and decisions of BC Strategies & Risk Mitigation*

BC Management Committee should review the Strategies and changes proposed by the various Business Units to improve BC/DR capabilities of the organization, approve and decide changes or new projects where required.

Committee also considers the key Risks identified; mitigation measures as defined / required / proposed in the outcome of the Risk Assessment Process.

Input, definitions and presentations by individual Business Units might be required and requested per case per case by the BCM Steering Committee to justify proposed changes or investments.

In several cases, decisions to implement new solutions and infrastructure systems may be required. Approval of budget allocation is expected in parallel.

BCM Steering Committee decisions are communicated to the relevant Business Units, and a company BC / DR Strategic approach is summarized.

| | | |
|---|---|---|
| Project Owner | : | BC Unit |
| Contributors | : | BCM Steering Committee |
| | | All Business Units on a need-to basis |
| Deliverables | : | Approved BCM Strategies at company & Business Unit levels |
| Delivery Period | : | June |

#### *8.3.1.8 Implementation of solutions decided*

Based on the various decisions made under the BCM Steering committee the relevant Business Units design, prepare and roll-out the Programs / Projects required to respond to these decisions. A brief Program Planning and Scheduling is communicated to the BC Unit.

| | | |
|---|---|---|
| Process Owner | : | Each Relevant Business Unit |
| Informed | : | BC Unit |
| Deliverables | : | As per the projects that have been approved |
| Delivery Period | : | As required by each Program / Project |

#### *8.3.1.9 Review & Update of BC / DR / IM / CM Plans*

This step will result in the review / update / preparation of BC / DR / CM / IM Plans of the company. The following actions should be implemented, as based on all the previous processes' outcome and decisions made:

- BC Unit should prepare / update the current Company-level BC / DR / Incident / Crisis Management Plans and the provisions therein, submit them to the BCM Steering Committee and have them approved and distributed as required.

- BC Unit may need to collaborate with several teams and Business Units to this.
- BC Unit should prepare a list of the expected revised plans (Activities and Technology) - with the collaboration of all Business Units.
- A review training workshop is prepared and delivered to BC Representatives to help them understand the requirements of BC/DR Plans preparation and used approach / process
- BC Unit distributes per Business Unit the relevant BC / DR Templates as well as the current versions of the Plans that are approved and in place.
- All Business Units, with the facilitation of their BC Representative, should
    - review existing plans
    - Update existing plans where required
    - Create new plans where required
    - Have them approved at Business Unit level
    - Submit these to BC Manager for quality assurance
- BC Unit ensures the quality on the plans delivered, ensured their compliance with the existing Company BC Standards (i.e., RTOs, RPOs etc.) and requires any adjustments from participating Business Units, so a final and approved version is in place.
- Once finalized, the Plans are distributed as described within each one, stored in the appropriate location and replace previous versions that are withdrawn and destroyed / deleted.

Process Owner : BC Unit

Contributors : All Business Units for their own Plans, BC Representatives, BC Plan Owners

BC Unit for BC / CM Plans at Company level

Deliverables : Updated BC / DR / IM / CM Plans at company and Business Unit level

Delivery Period : July - August

#### *8.3.1.10 Training of BC / DR Teams on the Plans provisions*

At the responsibility of each BC Plan Owner, the teams engaged within each Plan should be trained on the requirements of the Plan they participate, understand their roles, responsibilities and actions required once the Plan is invoked.

BC Unit will prepare and deliver a workshop / training session to explain to the teams engaged within each Company-level Plan (Crisis Management, BC Invocation and Management Plan at company level etc.) their roles, responsibilities and actions required once an incident occurs.

Process Owner : BC Unit

Contributors : All BC Representatives and BC Plan Owners to deliver the training sessions

BC Unit for BC / CM Plans at Company level

Deliverables : Trainings of all IM / CM / BC / DR Teams members on their plans

Delivery Period : September

#### *8.3.1.11 Planning, Scheduling and Running Exercises & Tests*

Based on the Plans prepared and approved, the priorities defined, test history and company requirements, BC Unit will work with the relevant teams, Business Units and management and prepare a Plan Test Strategy approach to cover organization's relevant requirements. List of Plans in need to be tested will be distributed to all Business Units (on a Plan ownership basis) identifying the tests and exercises type required (i.e., desktop, simulation, full scale etc.).

Based on this, Business Units should prepare and submit a Test / Exercise Schedule that should include all Plans within their area of responsibility (list). Schedule may extend to a 12-month time frame. Once finalized, it is submitted to BC Unit.

BC Unit should also define the Tests and exercises to be conducted at wider level (i.e., Crisis Management simulation) and prepare a relevant schedule to this.

The combined schedules of Plans tests and exercises from all company operations, Business Units will be documented by the BC Unit and presented to BC Steering Committee for review and approval.

Once approved, schedule is communicated (on a need-to-know basis) to all relevant Business Units that should proceed to implement test & exercise schedule.

Each Business Unit, under the direct involvement of the BC Plan Owners and the facilitation of their BC Representative, should prepare a pre-exercise report, to be submitted and approved by their management and the BC Steering Committee before running the exercise. Risk assessment of the exercise itself as well as the exercise process and impact that it may have on company operations should be an integral part of the preparation effort.

After each exercise is run, at the responsibility of the Plan Owner, a Post exercise report is prepared and submitted to Business Unit management and the BC Unit. Report is expected to include improvements and changes required that should be approved for action by the Business Unit Management in coordination with the BC Unit. Changes & improvements decided and approved should be implemented as soon as possible, at the responsibility of the Business Unit manager.

BC Unit keeps track of all exercises scheduled and run within the company at an annual basis.

| | |
|---|---|
| Process Owner | : BC Unit |
| Participants | : All Business Units and BC Plan Owners.<br>All BC / DR Plans team members<br>BC Unit for BC / CM Plans at Company level |
| Deliverables | : Annual Schedule of exercises & Tests<br>Annual Report of exercises & tests status<br>Post Test & Exercises Reports<br>Changes & Improvements implementation planning & delivery |
| Delivery Period | : Planning & Scheduling: October – November<br>Tests & Exercises run: all year long |

#### *8.3.1.12 Management Review*

Once a year, BC Unit should prepare a Management Review Report on the Business Continuity Management System status.

This report should provide a clear picture on the current year status and cover all aspects and areas of the BCMS including but not limited to

- Objectives
- Status
- Accomplishments
- Deviations & non-compliances
- Problems & issues met
- Recommendations to the way forward

Report should refer to the following at a minimum

- BCM Objectives – Objectives met and deviations – Mitigation measures & Suggestions for next year
- BCM Lifecycle implementation as of the current year – report on the implementation, deviations, problems & mitigation measures - improvement suggestions for next year
- BCM Performance evaluation - Key Performance indicators – accomplishments, improvements required – proposed changes to indicators (withdraw, change, define new)
- Internal Audit findings – feedback and actions implemented
- Compliance to regulatory, company & international BC standards - deviations & mitigation measures - improvement suggestions for next year
- Status and Results of Exercising and Testing
- Post incident reviews, Lessons learned and actions arising from negative incidents that occurred within the year and from relevant OIC's response performance

- Risk Assessment and Mitigation status & review – Suggestions for next year
- Follow-up actions as from previous Management Report
- Needs for changes (in policies, procedures, organization etc.)
- Opportunities for improvements

Following the report, presentation (if required) and relevant workshops requested by, BC Steering Committee should provide a feedback and approval of actions including:

- BCM Objectives for the next year
- Changes & improvements as per proposals
- Strategic projects and actions to be implemented
- Funding and Budget directions

Results of the annual Management Report as well as the decisions of the BC Steering Committee should be communicated – on a need-to-know basis – to the relevant Managers and heads of the Business Units.

BC Unit is responsible to monitor the implementation of the BC Steering Committee decisions.

Process Owner : BC Unit

Participants : BC Steering Committee
BC Unit
Business Units' Heads as per requirements

Deliverables : Annual Management Review report
Approvals given and Actions requested by BC Steering Committee

Delivery Period : December

# Chapter 9

# Analysis & Assessment

Understanding the organization is the key part of BCM. Business impact analysis (BIA) and risk assessment (RA) are two major tools of understanding the organization

in the context of BCM lifecycle. (Torabi, Giahi, Sahebjamnia:2016 pp. 201-218, Fullick: 2013, Forbes, Buchanan:2006, Priti, Sikdar:2017)

## 9.1 Business Impact Analysis

Business Impact Analysis (BIA) is a linear process and consists of techniques and methodologies that can be used to identify, quantify and qualify the business impacts and their effects on an organization of a loss, interruption or disruption of business & Operational Activities and/or their dependencies including their intra-organization and outsourced provision. (ISO 22317:2015)

The BIA is not a one-time or single stage activity. Initially, it can help clarify the scope of the business continuity programme, after which it becomes an integral part of the ongoing lifecycle to confirm business continuity requirements, leading to the determination and selection of business continuity solutions.

Effort covers information collection via questionnaires, interviews, workshops, reviewing of existing documentation etc to evaluate functions against common criteria to be proposed and agreed with an organization in order to assess potential impacts and based on the analysis results, prioritize business functions.

A subset of the organization's business functions is identified to be considered as critical and hence needs to be recovered during disasters, while other may be served on a second effort layer. Amongst others and for each of the high priority (critical) Functions, BIA effort provides Disaster Declaration Thresholds, Maximum Tolerable

Period of Disruption (MTPD), Recovery Time Objectives (RTO) and other relevant factors / characteristics in relation to Disaster Recovery and Business Continuity.

The aim of the Business Impact Analysis in an organization is:

- Identify and prioritize products and services and determine the organization's business continuity requirements at a strategic level
- Determine the process or processes required for the delivery of the organization's prioritised products and services
- Identify and prioritise the activities that deliver the most urgent products and services, and to determine the resources required for the continuity of these activities

The prioritization of products and services, processes and activities will be done by determining the Maximum Tolerable Period of Disruption (MTPD). The MTPD has been reached when acceptable levels of damage have been exceeded and the failure of the organization is imminent.

The main factors to be considered when estimating the MPTD are:

- Damage to financial value or viability
- Damage to reputation or interested party confidence
- Breach of legal or regulatory obligations
- Failure to meet the strategic objectives of the organization

(Alberto:2009, Faertes: 2015, Sikdar:2017)

The following tasks are required to be completed:

- Identify participants from all departments throughout the organization to the BIA effort. For each unit / department / sub-department / operating area selected (within the defined spectrum of business operations), BC Coordinator of the department needs to be assigned and participate.
- Prepare the relevant BIA information collection templates and documents. Distribute them to the assigned BC Coordinators and the BIAs participants for the collection of information.

- Where required, schedule various meetings with personnel from each operating area to review and discuss special functions/procedures and other considerations unique to each area. A combination of template collection, group workshops and individual interviews needs to be used to
    - Review the operations, functions and procedures
    - Identify organization's critical and less critical business functions with their recovery and contingency arrangements RPO, RTO, MTD, Data Loss, etc.
    - Identify organization's critical and less critical departments with their recovery and contingency arrangements RTO, MTD, Seats' allocation, etc.
    - Determine critical equipment requirements
    - Identify Critical Systems / applications
    - Identify SLAs for critical systems
    - Define priorities (including for processes, systems, activities, applications)
    - Identify organization's staff, suppliers and 3rd Party vendors who are critical to organization's operations
    - Identify Single Points of failure
    - Evaluate the security / availability of vital records
    - Analyse record retention policies and procedures
    - Consider the impact of the requirements identified above on business recovery planning
    - Document dependencies (location dependencies, departmental dependencies, Staff skill dependencies, Internal & external dependencies, etc.)
    - Identify the impact resulting from the loss of key operations, functions and Systems related to financial losses (direct and indirect)
    - Identify the impact (qualitative and quantitative) resulting from the loss of key operations, functions and Systems related to:
        - Employees / personnel including morale
        - Management control & Decision

        - Image, Reputation and credibility
        - Regulatory & legal impacts
        - Vendors / Service providers
        - Operational efficiency
        - Compliance
- Evaluate critical needs. When evaluating critical departmental needs, information is analysed in each of the following areas:
    - Personnel
    - Facilities and staffing requirements
    - Critical systems
    - High priority tasks
    - Data processing interruption procedures
    - Minimum equipment, forms and supplies
    - Analyse and prioritize business & IT functions, systems, and services that are critical to the organization's ability to maintain business operations through a disaster occurrence. The analysis should include the following information:
        - Services
        - Workflow Impact
        - Alternate Processing Methods

During BIA phase, information is collected on the impact on organization's operations in the immediate aftermath of a major disruption. Assessment of impact is based on Operational, Legal/Regulatory concerns, Brand image, reputation and financial exposure of the Business.

The overriding aim must be for an organization to guarantee continuity of customer service under all circumstances, thereby preserving credibility with the customers and upholding its image in the local and regional market. The approach defined, discusses the loss / disruption of operations under the combinations of Business Units, Sites, Infrastructure and Services offered to internal and external customers.

BCM addresses "one-off" events (Incidents or Disasters) which have the potential of creating continued disruption to the operation of an organization. Therefore, BCM is

mainly focused on identifying existing recovery solutions, defining recovery parameters, assisting in preparing recovery strategies and solutions in areas in need of and preparing the required Plans and Response approaches.

Day-to-Day operational issues are out of the core part of the scope of BCM (and BIA as a result), but remain under the Risk Identification and Management part of the effort. Examples include issues related to the Power alternative provisions, networking and communication improvements that could minimize risk exposure, use of good business practices and procedures to ensure quality and minimization of risks.

For the execution of the BIA phase, it is critical to identify and develop the impact metrics against which all activities, processes, services and systems are assessed. This is usually done with the cooperation and alignment of Audit / Risk Management / Finance functions within an organization. The following table depicts an indicative Impact Evaluation Matrix.

| Impact Evaluation Matrix | | | | |
|---|---|---|---|---|
| **TYPE OF LOSS / LEVEL OF IMPACT** | **(4) Major** | **(3) Moderate** | **(2) Tolerable** | **(1) Minor** |
| **Financial Loss**<br>**The realisation of an actual or potential unexpected financial loss.** | - Over 50% Impact on total client's revenues<br>- Client is considered among the most profitable ones for the organization<br>- Severe deviation between lost revenues and business Interruption insurance reimbursement | - 25 % - 50% Impact on total client's revenues<br>- Client is among the medium profitable ones for the organization<br>- Medium deviation between lost revenues and business Interruption insurance reimbursement | - 10 % - 25% Impact on total client's revenues<br>- Client is among the intermediate profitable ones for the organization<br>- Slight deviation between lost revenues and business Interruption insurance reimbursement | - Impact on total client's revenues less than 10%<br>- Client is considered as minor profitable the organization<br>- Lost revenues are covered by business Interruption insurance reimbursement |
| **Reputation & Image**<br>**Damage to the firm's reputation in the minds of anyone whose viewpoint could ultimately have direct or indirect impact on the shareholder value of the business.** | - Client's loss will severely damage organization's image<br>- Major complaints / concerns raised from client<br>- Extended adverse and sustained commentary in regional market, severe loss of confidence in capability of managing properly operational issues | - Client's loss will damage organization's image<br>- Several complaints / concerns are raised from client<br>- Medium adverse commentary in regional market, reduced confidence in capability of managing properly operational issues | - Client's loss will slightly damage organization's image<br>- Certain complaints raised from client<br>- Increased adverse commentary in local market | - Client's loss will not impact organization's image<br>- No raised / or minor complaints from client<br>- Minor adverse publicity in local market |
| **Strategic**<br>**Damage to the firm's strategic plans implementation and budget acomplishment capability** | - Competitive / strategic action that can lead to inability to attain business plan revenue targets<br>- Inability to execute organization's corporate strategy<br>- Severely impact organization's penetration to the specific market<br>- Client's brand is considered as major player in its market | - Competitive / strategic action that will lead to inability to attain strategy business plan targets<br>- Client's brand is considered as important in its market<br>- Medium impact organization's penetration to the specific market | - Competitive / strategic action that will temporarily impact organization's ability to compete in the future<br>- Client's brand is considered as of small size in its market | - Competitive / strategic action that may have a short term strategic impact<br>- Client's brand is not considered as important in its market |
| **Client's Customers Impact**<br>**Failure to provide or compromise quality in delivering services to customers (any type)** | Over than 50% of the client's customers have been impacted or do not have access to organization's services. | 25% -50% of the client's customers have been impacted or do not have access to organization's services. | 10% -25% of the client's customers have been impacted or do not have access to organization's services. | Less than 10% of the client's customers have been impacted or do not have access to organization's services. |
| **Legal / Contractual**<br>**Failure to comply with legal, regulatory, or contractual commitments** | - Severe failure to comply with the contractual Recovery Objectives (RTO & RPO)<br>- Severe Legal action on organization based on signed contract<br>- Branded Stakeholders bring claims to court. | - Medium failure to comply with the contractual Recovery Objectives (RTO & RPO)<br>- Medium legal implications with client. | - No contractual recovery requirements set by the client.<br>- Issues expected to result in regulatory censure / fines / settlements for a limited part of the business. | - No Recovery Capability possible and client is aware<br>- Limited compensation demands raised.<br>- Capable of resolution by negotiation with customers |
| **Operational Efficiency**<br>**Failure to deliver services affecting client's operations** | - Non-achievement of major service deliverables<br>- Client is hosted in numerous organization's sites | - Delays in major service deliveries<br>- Client is hosted in several organization's sites | - Inconvenient service delays<br>- Client is hosted in a small number of organization's sites | - Little Impact<br>- Client is hosted in a very limited number of organization's sites |

**Table 9.1:** Indicative Impact Evaluation Matrix used in BIA

The impact evaluation for all activities, processes, services and systems should be conducted against specific timeframes such as hours (4 Hours, 8 Hours, 12 Hours) and/or days (1 Day, 2 Days, 3 Days, 7 Days).

Another critical aspect in the BIA effort is to differentiate the Recovery Time of a technical failure and of the Recovery Time in case of a disaster. A definition is highly required to be made in order to distinguish between the Response and Recovery of a technical error or failure of an IT Application / System and the Response and Recovery of an organization to a Disaster or disastrous event that will require activation of BC Plans and full operations relocation to DR sites.

To this direction we have to define the following:

**I. RTO Time components of an Application / System / Service**


**Figure 9.1:** RTO & MTPD Relation

**II. Technical failure Incident**

Typical Technical failure incidents DO NOT REQUIRE the relocation of personnel (either IT or Users from rest of Business Units to the recovery site(s).

(1) Typically, as of the Risk Appetite, full recovery of the critical systems in case of failure should be accomplished before MTPD time frame.

This figure applies to one incident per year.

(2) The technical RTO, as of company decision, may be proposed to be set to a specific timeframe (e.g., one (1) hour) for critical systems.

(3) This timeframe of one (1) hour requires that Recovery capabilities in place of the Systems are practically on an almost high-availability / on-line / real-time synchronization status with adequate defined SLAs with the vendors

This is a very important input to the Strategic design of IT Infrastructure and relevant architecture to be implemented.

(4) This RTO includes the accomplishment of the following tasks

(a) T0 as above

(b) T2 as above (the technical part of the systems recovery) as well as

(c) T4 as above (the quality assurance of the recovered application, including the non-IT Business Units' involvement)

RTO should cover the recovery of ALL systems identified as critical or of high importance from the business users. In the case of a stoppage of the systems, recovery may require the parallel effort of several IT teams working in each of the systems. This considered, leaves very small timeframes for the technical part of the recovery of each of the systems, as significant time would be spent on quality assurance (including the participation of the rest of the non-IT Business Units users).

**III. Disaster of Operational Areas Incident**

Disastrous incidents REQUIRE the relocation of personnel (both IT and Users from rest of Business Units) to the recovery site(s).

(1) Services' MTPD may be proposed to be set to more than two (2) hours and RTO is typically less than that (2 Hours).

In order for this to be accomplished it will require the presence of specific IT personnel in the DR site(s) and the good operational status of all defined WAR(s).

(2) In the case of operational area disaster (i.e., loss of HQs site) personnel notification, travel and relocation time estimated to two (2) hours should be considered (including notification times). Time has also to be added for the recovery of the Unit's Activities in the Work area DR site (T3 above).

This limits the recovery time of applications / systems available for the personnel to the same time frames described in the II paragraph above).

The outcome of the BIA effort should include documented and detailed information related to:

- Applications used by Business Units' users.
- A list of key Business Units' vendors
- A list of Business Units' reports and their criticality
- A list of Business Units' processes dependencies ("received")
- A list of Business Units' records and their criticality

For every Business Unit the following should be documented:

- Business Activities
- Proposed (Required) Recovery Time Objective (RTO) & Maximum Tolerable Period of Disruption (MTPD)
- Highest Impact in case of interruption for each Business Activity
- Time of Occurrence of Highest Impact
- Prioritization

The prioritization of the business activities should be done based on the level of Highest Impact, RTO and MTPD. The Maximum Tolerable Period of Disruption (MTPD) is the duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed. Consequently, the Recovery Time Objective (RTO) needs to shorter than MTPD in order for the organization to have adequate time to recover and deliver the product and service prior of reaching the MTPD.

To ensure a complete and thorough impact analysis, it is recommended that the evaluation should be made both qualitatively and quantitatively, if possible. The identification and recording of the services & products provided to organization's external environment is considered critical in a BIA. The list of services provided by an organization may be defined with with the cooperation of the Finance, Marketing or other business Units and may be grouped in a number of Key Services.

The following paragraphs depict indicative examples of analysis that should be taken into account during the BIA effort and will help the organization to decide on the strategies to be followed in latter stage.

### 9.1.1 Stakeholder Impact per Service/Product

The following table presents an indicative stakeholders' impact and the relevant stakeholders in relation to an organization's Key Services / Products provided by the Business Units.

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Stakeholders Impacted | Severity of Impact as identified through BIAs |
|---|---|---|---|---|
| Service / Product Group 1 | Call Center | Service / Product 1 | Customers | High |
| Service / Product Group 2 | Legal | Service / Product 2 | Regulatory Authorities | Tolerable |
| Service / Product Group 3 | Business Development | Service / Product 3 | Banks | Moderate |
| Service / Product Group 4 | Operations | Service / Product 4 | Brokers | Low |

**Table 9.1.1**: Stakeholder Impact per Service/Product

### 9.1.2 Regulatory & Legal Impact per Service / Product

The following table presents an indicative regulatory and legal impact in relation to an organization's Key Services / Products and the Services provided by each of the Business Unit.

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Severity of Impact as identified through BIAs |
|---|---|---|---|
| Service / Product Group 1 | Call Center | Service / Product 1 | None |
| Service / Product Group 2 | Legal | Service / Product 2 | Tolerable |

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Severity of Impact as identified through BIAs |
|---|---|---|---|
| Service / Product Group 3 | Business Development | Service / Product 3 | Moderate |
| Service / Product Group 4 | Operations | Service / Product 4 | Low |

**Table 9.1.2**: Regulatory and legal impact per Service/Product

### 9.1.3 Reputation and Brand Image per Service / Product

Reputation and brand image will be greatly impacted in cases of negative incidents that will stop repeatedly or for a prolonged period the provision of an organization's Services / Products.

Depending on the market condition and business environment of the incident time, reputation impact can be Tolerable up to High. Extended adverse and sustained national and multinational media articles, comments and broadcasts will surely harm an organization's Brand Image and Reputation.

The following table presents an indicative reputation and brand image impact in relation to an organization's Key Services and the Services provided by each of the Business Unit.

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Severity of Impact as identified through BIAs |
|---|---|---|---|
| Service / Product Group 1 | Call Center | Service / Product 1 | High |
| Service / Product Group 2 | Legal | Service / Product 2 | Low |
| Service / Product Group 3 | Business Development | Service / Product 3 | Tolerable |

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Severity of Impact as identified through BIAs |
|---|---|---|---|
| Service / Product Group 4 | Operations | Service / Product 4 | Moderate |

**Table 9.1.3**: Reputation and brand image impact per Service/Product

### 9.1.4 Strategic Impact per Service / Product

Events resulting in frequent or extended operational outages can lead to inability to attain business plan targets revenue and profitability to high percentages deviations.

This will surely impact an organization's ability to compete in the future and will have a middle and long-term strategic impact on the company, its place in the local and/or regional economy and the market it operates. The organization will need quite a time to reschedule its strategies and accomplish succeeding.

The following table presents an indicative Strategic impact in relation to an organization's Key Services / Products and the Services provided by each of the Business Unit.

| Services / Products Groups | Business Units | Services / Products provided by the Business Units | Severity of Impact as identified through BIAs |
|---|---|---|---|
| Service / Product Group 1 | Call Center | Service / Product 1 | Tolerable |
| Service / Product Group 2 | Legal | Service / Product 2 | Low |
| Service / Product Group 3 | Business Development | Service / Product 3 | High |
| Service / Product Group 4 | Operations | Service / Product 4 | Moderate |

**Table 9.1.4**: Strategic impact per Service/Product

### 9.1.5 Financial (Quantitative) Impacts

Any type of negative incident is always resulting to some type of financial loss, either as a direct loss or as a loss of assets (tangible or not, including reputation and brand image).

An organization could be highly risking in stakeholders' confidence and based income unless company's ability to recover on time is ensured.

The following table depicts an indicative simplified analysis that can be made to relate revenue losses to revenue streams / services / products, and respective losses that may be generated by specific timeframes of outages. Such analysis may greatly beneficiate an organization in the strategy phase, when decisions should be made for the necessary investments to increase the organization's resilience and to prioritize the revenue loss.

| ORGANIZATION REVENUES | | | | |
|---|---|---|---|---|
| **Department / Functional Unit** | **Revenue Streams / Services / Products** | **Annual Revenues** | **Daily Revenue Loss** | **Hourly Revenue Loss** |
| Unit 1 | Service 1 | XXX,xxx | XX,xxx | X,xxx |
| Unit 2 | Product 1 | YYY,yyy | YY,yyy | Y,yyy |
| Unit 3 | …. | ZZZ,zzz | ZZ,zzz | Z,zzz |

**Table 9.1.5**: Financial Impacts per Department & Revenue Streams

Another analysis that can be made is the impact per operational site in relation to the revenue streams / services / products allocated to each individual site.

| **Site** | **Annual Revenue allocated to the Site** | **Daily Revenue Loss** | **Hourly Revenue Loss** |
|---|---|---|---|
| Site A | XXX,xxx | XX,xxx | X,xxx |
| Site B | YYY,yyy | YY,yyy | Y,yyy |
| Site C | ZZZ,zzz | ZZ,zzz | Z,zzz |

**Table 9.1.6**: Financial Impacts per Operational Sites

One of the BIA targets is to identify the chain and relation that link the business activities, the supporting systems and the generating revenue streams / services / products. In this way, it is easy to estimate any loss generated by the interruption of revenue streams / services / products or systems as presented in the next two tables.

| Operating Revenue Losses per Revenue Stream / Application | | | | |
|---|---|---|---|---|
| **Revenue Stream / Service / Product** | **Application / System** | **Annual Revenues** | **Daily Average** | **Hourly Average** |
| Service 1 | App1, App2, Sys1, Sys2 | XXX,xxx | XX,xxx | X,xxx |
| Product 1 | App1, App3, Sys1, Sys3 | YYY,yyy | YY,yyy | Y,yyy |
| …. | App2, App3, Sys2, Sys3 | ZZZ,zzz | ZZ,zzz | Z,zzz |

**Table 9.1.7**: Financial Impacts per Revenue Stream / Application

| Operating Revenue Losses per Application / Revenue Stream | | | | |
|---|---|---|---|---|
| **Application / System** | **Revenue Stream / Service / Product** | **Annual Revenues** | **Daily Average** | **Hourly Average** |
| App1 | Service1, Product1 | XXX,xxx | XX,xxx | X,xxx |
| App2 | Service 1, Product2 | YYY,yyy | YY,yyy | Y,yyy |
| Sys1 | Service2, Product3 | ZZZ,zzz | ZZ,zzz | Z,zzz |

**Table 9.1.8**: Financial Impacts per Application / Revenue Stream

Notes:

(1) The daily revenue loss is estimated taking into consideration the working days of the organization within a year or the provision time of the service / product
(2) The hourly revenue loss is estimated taking into consideration the working hours of the organization per day or the provision time of the service / product
(3) The financial figures are maintained by the financial unit of the organization
(4) All calculations should be thoroughly checked and justified based on the evidence provided

An indicative simplified Business Impact Analysis questionnaire can be found in Annex C at the Annexes chapter.

### 9.1.6 Hints & Tips

- In the early stage of BIA, it is important to clearly define the services, products and process within the organization. These definitions should be crosschecked and validated by the business owners and units of the organization.
- For some products and services in some industry sectors, a few minutes of disruption may have no impact at all, a few hours could be tolerable, but longer than a week mean failure of the business. On the other hand, in some highly competitive markets, a few hours disruption to critical services may result in major loss of positioning in marketplace.
- An aim of business continuity is to design and implement plans to ensure continuity of the organization's products and services before the MTPD is reached. BIA identifies RTOs for the prioritised products, services, activities and resources as this will enable the organization to develop solutions and plans that avoid reaching the MTPD.
- Where activities and resources support multiple products and services, the shortest time requirement of these products and services is the recovery time objective (RTO).
- A one-off contract with an outsourced service provider including significant time penalties may reduce the MTPD within the organization for the period of that contract.

- It is highly recommended that the assigned participants / BC coordinators in an organization would be of managerial level having wide expertise, knowledge and authority related to the function / unit representing.
- A combined approach to achieve an organization-wide view of key products, services and processes can make the BIA process complex and challenging. Therefore, it is necessary to incorporate all participants in the effort, present and explain the BIA process and its deliverables. A series of presentations usually greatly facilitates both the effort and the outcome.
- To facilitate the effort and to efficient manage the collection of the necessary data, it is advised that the person(s) managing the BIA phase to support the assigned organization POC(s) by scheduling short sessions of interviews and mentoring.
- The execution of BIA should be conducted through a series of sites' visits, interviews and data collection workshops with the personnel across the organization. Analysis on available information, use of checklists and the undertaking of workplace walkthroughs and inspections should also be used during the execution.
- It is very common in an organization to see that business functions have different perception and "language" compared to the technical functions. There are cases that these perceptions sometimes are opposed to each other. It is very important that these two sides should work in identifying a common perception and language especially when it comes to identify realistic recovery requirements.
- It is important for applications / systems used by an organization to correlate the Recovery Time Objective indicated in Risk Appetite, as of IT Recovery Capability through the suppliers / vendors contracts and suggested by the BIA process to identify any possible mismatches.
- It is not unusual that people in senior management roles think and operate in silos mode. The wide experience of the BCM practitioners that are assigned to

complete the BIA phase may facilitate in widening the perspective of those attitudes.

- ❖ Sometimes there is exaggeration in the estimation of the different impacts resulting in narrowing the time objectives for the recovery. Therefore, the blend of the cautiously selected organization's representatives and the experienced BCM practitioners involved in the BIA will eliminate such phenomenon.
- ❖ It is important that outcome of the BIA effort to be reviewed and accepted by all involved stakeholders. Based on this outcome all subsequent phases and outcomes are built and developed to secure organization's resilience.

## 9.2 Risk Assessment

A major part of Business Continuity Management is to ensure that the likelihood (frequency and probability) of High Priority (Critical) Business Activities and Systems, their dependencies and single points of failure being affected by the occurrence of a threat 'event' is adequately and properly managed.

Together with the Business Impact Analysis, a Risk Assessment provides information to enable the business to determine its Risk Appetite. (Graham, Kaye: 2006)

Risk Assessment will determine the events and environmental (internal and external) surroundings that can adversely affect the organization and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss.

Here are some types of threats that may be taken into consideration during the RA effort.

- Natural (e.g., Earthquakes, Floods, Fire, etc)
- Technological (e.g., Power loss, Communications failure, IT infrastructure failure, Viruses, Security of Information Systems, Devices' failures, etc)
- Man-made (e.g., Sabotage, Large Incidents / events, Human errors, Terrorism, Process errors, Fraud, Bad Project Management, etc)

- Social
- Et al

Risk Assessment should apply on the organization processes and operations, focusing on operations, processes, activities and resources (systems, work area, technology etc)

**The Purpose of the Risk Assessment study** in an organization should be:

- To identify the internal and external threats, vulnerabilities, liabilities and exposure, that could cause the disruption, temporary or permanent interruption or loss to organization's High Priority (Mission Critical) Operations, Activities, Resources, Systems and Applications, including but not restricted to
    - Internal resilience and reliability of infrastructure (e.g., weak points for network, sites, staff)
    - External threats such as partners failures, weather conditions, natural disasters, accidents, sabotage
    - Threats from other interconnected networks
- To identify Risk Concentrations, points of failure (including single points of failure) and weaknesses of all resources required for continuing operation of every critical activity
- To identify the likelihood (probability or frequency) of a threat occurring, exposure and the vulnerability to the identified threats and assessment of their effect on the operation of the network and the provided services taking into account the vulnerable points and weaknesses identified
- To provide a basis for the organization to establish a risk appetite and risk mitigation and management control program and action plan

### 9.2.1 Risk Assessment approach

Once the key operations, Business Critical Activities, services, resources etc have been defined and their business values and recovery priorities have been set (through the

BIA execution), the Risk Assessment approach should include the following classic steps:

- Step 1 - Identify and Characterize Threats
- Step 2 - Identify and Characterize Existing Protective and Mitigation Measures
- Step 3 - Identify and Characterize Vulnerabilities
- Step 4 - Estimate probabilities and Consequences
- Step 5 - Estimate and Assess Risks

Mission critical activities / areas and services will be analysed to determine the degree of risk associated with the various types of disasters.

Considerations in assessing risk may include:

- Frequency of particular types of disasters (often versus seldom)
- Speed of onset (sudden versus gradual)
- Existing and required redundancy levels throughout the organization to accommodate critical systems and functions, including:
    - Hardware
    - Communications
    - Information
    - Personnel
    - Services
- Other important criteria

Usually during the RA effort, there is need of a series of onsite inspections and technical assessments across organization's facilities & infrastructure to be conducted.

The aim of the onsite inspections will be to identify and assess threat & risks for location and address (at the later task of Mitigation measures) any enhancements they might require and must cover.

Apart from the onsite surveys, specific questionnaires and templates may be used and filled-in to ensure risk identification in critical areas (i.e., Power, Physical Security and Facility Management).

Information Technology infrastructure, Data Centres, IT Systems and networks should be also assessed to identify risk exposures and areas in need of improvement.

Similar to the BIA effort, a Risk Impact Matrix should be used for the evaluation of the Risk Findings for both probability and impact.

The following tables depict indicative matrices for both probability and impact ratings that should be used in the RA effort.

| PROBABILITY RATING | | | | |
|---|---|---|---|---|
| **5** | **4** | **3** | **2** | **1** |
| Risk which will most likely to happen | Risk is known to occur occasionally at a frequency of about once a year | The frequency of occurrence is once every 2 – 5 years | The probability of occurrence is estimated to be about once every 5 – 10 years | The possibility of occurrence of the event is estimated to be less than once every 10 years |

**Table 9.2:** Indicative Probability Rating Matrix used in RA

| | IMPACT RATING | | | | |
|---|---|---|---|---|---|
| | **5 Catastrophic Loss** | **4 Heavy Loss** | **3 Moderate Loss** | **2 Tolerable Loss** | **1 Mild Loss** |
| **Financial** | Impact on profit > amount | Impact on profit between amounts | Impact on profit between amounts | Impact on profit between amounts | Impact on profit less than amount |

| | IMPACT RATING | | | | |
|---|---|---|---|---|---|
| | **5 Catastrophic Loss** | **4 Heavy Loss** | **3 Moderate Loss** | **2 Tolerable Loss** | **1 Mild Loss** |
| **Regulatory / Legal** | Loss of credibility due to<br>■ Failure to uphold xxx Regulators<br>■ Threat of revocation of franchise from Regulator<br>■ Failure to ensure safety of staff (loss of lives, severe injuries) | ■ Severe Legal / Regulatory action on the organization<br>■ High penalty by xxx regulators or other authorities<br>■ Branded Stakeholders bring claims to court | ■ Warning issued by regulator / legal authority<br>■ Legal implications with some key stakeholders<br>■ Impact on regulation / Medium fine by xxx regulators or other Authorities | ■Issues expected to result in regulatory censure / fines / settlements for a limited part of the business. Does not affect operations | ■ Little impact on regulation/ low fine by xxx regulators or other Authorities |
| **Strategic** | Competitive / strategic action that can lead to<br>■ Inability to attain business plan target revenue and profitability by more than 50%<br>■ Serious compromise of organization's strategic objectives | Competitive / strategic action that can lead to<br>■ Inability to attain business plan revenue targets by more than 15%<br>■ Inability to execute organization's corporate strategy | Competitive / strategic action that<br>■ Will lead to inability to attain business plan targets by more than 5% | Competitive / strategic action that<br>■ Will impact organization's ability to compete in the future | Competitive / strategic action that<br>■ May have a long-term strategic impact |

| | IMPACT RATING | | | | |
|---|---|---|---|---|---|
| | **5 Catastrophic Loss** | **4 Heavy Loss** | **3 Moderate Loss** | **2 Tolerable Loss** | **1 Mild Loss** |
| **Reputational Damage** | ■ Extended adverse and sustained national and multinational media coverage accompanied by extended stakeholder action | ■ Severe loss of confidence of the public at large and/or market and/or demonstrable damage to image / credibility / Brand | ■ Adverse and extensive commentary in national media accompanied by stakeholder action and/or reduced confidence in A RANGE of Services | ■ Adverse commentary in regional / national media accompanied by limited stakeholder action and/or reduced confidence. Impact can be resolved in short time | ■ Minor Adverse publicity in local media |
| **Customers / Stakeholders** | ■ Major part of the Customers (of any kind) has lost access to the services they get.<br>■ Call Centre siege.<br>■ Loss of big number of customers | ■ A big part of Customers (major, key or common) has lost access to the services they get for significant time frames<br>■ Big number (>10X) of complaints<br>■ Loss of customers | ■ Significant (>5X) increase in complaints<br>■ Increased percentage of Major (> 10%) & key customers do not have service | ■ Increase in complaints 1X to 5X<br>■ A percentage of Major (< 10%) & key customers do not have service | ■ Limited number of common and Major & key customers have lost access to services. |

**Table 9.3:** Indicative Impact Rating Matrix used in RA

Based on the findings, a number of recommendations and proposals to the organization should be raised so they may be able to proceed to decision making on the required controls, measures and solutions to be implemented to deal with the risks traced.

Typical Risk Mitigation options include

- Risk Avoidance
- Risk Acceptance

- Risk Control and
- Risk Transfer

The Risk Assessment outcome should include:

- An awareness of the range of potential threats that could disrupt the organization's activities
- A list of prioritized threats based on the risk of disruption to the organization's activities
- Identification of single points of failures and of unacceptable risks
- Potential measures to reduce probability or scale of impact of the prioritized threats

An indicative Risk Registry as an outcome of the RA effort may have the following format.

| Risk Registry | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (NAME OF BUSINESS UNIT/ SUPPORT UNIT) | | | | | | | | | | | | | | |
| Process | Risk # | Risk Event Description | Inherent Risk Assessment | | | Control Assessment | | | | Residual Risk Rating | Mitigation | | | |
| | | | Impact | Likelihood | Risk Rating | Control Description | Design Effectiveness | Operating Effectiveness | Control Rating | | Mitigation Action Plan / Control | Due Date | Action Owner | Action Priority |
| | | | A | B | C=A*B | | D | E | F=D*E | G=C/F | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Table 9.4:** Indicative Risk Registry

While an overall Risk Matrix of the findings always helps to visualize the vulnerability of an organization and the issues to address with high priority. Indicatively:

| RISK ASSESSMENT FINDINGS MATRIX | | | | | | | |
|---|---|---|---|---|---|---|---|
| Impact | 5 | Catastrophic Loss | | | | | |
| | 4 | Heavy Loss | | | | | |
| | 3 | Moderate Loss | | 1.2 | | 1.1 | |
| | 2 | Tolerable Loss | 1.3 | | | | |
| | 1 | Mild Loss | | | | | |
| | | | Very Low | Low | Medium | High | Very High |
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | Probability | | | | |

**Table 9.5:** Indicative Risk Assessment Matrix

The Risk Assessment process should be ongoing and the methods used should be regularly reviewed at pre-agreed intervals or following significant changes in the organization.

The Annex D includes an indicative Risk Questionnaire that may be used during the collection of the data. The specific questionnaire addresses issues related to Facility Management, Physical Security and Administration. Similar questionnaires may develop to address other areas such as IT, Infosec, Connectivity, etc.

### 9.2.2 Hints & Tips

- Risk Assessment should consider short time frames relevant to the organization planning process. Disruptions extremely rare (a 1 in 100-year frequency), even with a high impact may not be taken into consideration.

- Access to information contained in the organization's risk registry should be provided during the effort. Collaboration with the risk management unit of the organization is required.

- Business Units usually maintain their own type of risk registry, issues that are considered to impact their operational status. It is strongly recommended that interviews should be conducted with the heads of those units to discuss and identify their concerns

- Many organizations carry out horizon scanning at pre-agreed intervals. Horizon scanning is an activity used to monitor and identify potential threats to an organization and considers longer term change and underlying trends. Information provided by the horizon scan is useful when undertaking a risk assessment as part of the business continuity programme. The organization can consider the use of a monitoring or system, news websites and social media as part of its horizon scanning activities.

- Risk Assessment information may include information about the frequency and impact of past disruptions. A risk matrix may be available where impact ratings are grouped into impact categories that relate to the organization. Care should be taken to ensure that the impact ratings are appropriate to describe the consequences of disruptions.

- Any history of negative incidents impacting the operation, infrastructure & services of an organization should be taken into consideration during the RA effort. Such history of incidents may indicate underlying root causes and/or specific vulnerabilities.

- The grouping and presentation of the Risk Findings is important not only for their comprehension by the stakeholders but also for the efficient implementation of the relevant controls and mitigation measures.

- As in the case of BIA, it is important that outcome of the RA effort to be reviewed and accepted by all involved stakeholders. Based on this outcome

there may an efficient prioritization of the threats and implementation of the proper mitigation points along with the respective control points.

- The experience of the persons conducting the RA is important for the outcome, especially in the case where no RM unit exists in the organization. The well-defined risks, the proper setting of probability and the understanding of the impact are critical to the success of RA. Exaggeration or mistreatment or lack of adequate information are factors that distort the RA outcome.

- Senior management support and commitment is crucial in the effort to identify possible hidden threats and underlying consequences in the RA effort. Therefore, it is critical for the practitioners conducting the task to explain in details the process and outcome of RA to the senior management and make them part of the team and effort.

# Chapter 10

# BC Strategy

Following the completion of the previous stage of BIA and RA the next step to be done is the definition of the BCM strategy. The scope of this phase is to identify the necessary BCM arrangements that will enable the organization to improve its availability, recovery capabilities and recover its Prioritized Systems & activities within their recovery time objectives. (Tucker: 2015, pp. 107-128)

The effort should:

- Define an incident response structure that will enable an effective response and recovery from disruptions;
- Determine **on high-level approach** how it will recover each critical operation / system / activity within its recovery time objective and the BCM arrangements
- Determine how it will manage relationships with parties involved in the recovery.

The **key areas** that should be considered include

- Services continuity options
- Activity continuity options (appropriate tactics for each activity required to deliver a service)
- Resources options
- High-level relevant systems & technology & Infrastructure
- Key suppliers & third parties

Alternate solutions proposed should be based on the current infrastructure according to best practices on this area.

High-level mitigation (Strategy) proposals should be made to:

- Provide recommendations for enhancements to your organization's IT infrastructure, Systems, Applications, Technologies
- Review organization's critical suppliers and 3rd Party vendors' contracts and recommend type of arrangement with those vendors in case the event of a crisis.

Strategy is an advisory phase and does not require the acceptance & commitment of an organization to the approaches described therein. This applies specially in the cases that several technologies & solutions may be available and decision on the final technology to be used may not be applicable to be made at this stage.

The team acting as a facilitator in this phase plays a very important role. Not only knowledge of BCMS framework is required but also creativity and management of creative supporting techniques to stimulate the involved stakeholders. (Cyzewski: 2012) The main objectives of a "creative thinking process is to think beyond existing boundaries, to awake curiosity, to break away from rational, conventional ideas and formalized procedures, to rely on the imagination, the divergent, the random and to consider multiple solutions and alternatives," (Michalko: 2011)

## 10.1 Recovery Strategy approach

The objectives of this effort should be

- To define and propose strategy (ies) which will best meet the recovery requirements that have been defined in the BIA effort
- To provide feedback & discussion base towards the different strategic options as far as the feasibility, desirability, and benefits of the different approached considered
- To cover all areas of technology related, individually and in coordination with each other, as well as operations activities and personnel resources

- To ensure that the overall approach has considered the current status of the organization's operations resiliencies, solutions and arrangements in place.

The overall strategy development approach and process is used to identify, quantify and qualify the recovery options in respect of sites, business areas, sub-units in relation to the systems, elements and activities that are critical to the delivery of the organization's goods and services.

Also, the development of a Resource Recovery Strategy will enable the implementation of each strategy option at a sub-unit level. This enabled a range of strategies and tactical options to be evaluated thereby allowing an appropriate strategic response to be chosen for each site, system, element and/or activity to be recovered to an acceptable level of operation in terms of functionality and performance.

The development of the strategy is advised to be based on the following key assumptions:

- The Strategy is based on the total loss of a site of the organization, considering a worst-case scenario
- It is proposed that a **business continuity operational risk appetite of 3-5 days** to be considered whereby only business activities within this timeframe would be considered critical and subject to ongoing strategy development. All other activities will be recovered on a best endeavours basis
- The simultaneous loss of more than one site of an organization would complicate the recovery strategies to be applied. Therefore, is advised before proceeding to such options, to be discussed with the senior management of the corporation

It is advised that the methodology followed to include intra-organization options and the provision of outsourced services:

- Identify the type of strategy or combinations of strategies e.g., site

- Review of the Business Impact Analysis and Risk Assessment findings. During this process I reviewed and validated the following which included a series of interviews with company's heads and personnel:
    - Business Critical Activities for Business Units and operations
    - Business and Operations Priorities
    - Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) and Business Continuity Level (BCL) for each Operation and related Systems
    - The use, location and protection of critical information and documentation
    - The final requirements for workspace and personnel resources for critical business activities
    - The final communications requirements of the critical business activities
- Identify any existing business continuity strategy, systems redundancy and/or countermeasures
- Develop a gap analysis
- Identification of strategy solutions
- Conduct a resource recovery requirements analysis to provide a Resource Recovery Strategy e.g., essential personnel, infrastructure and premises requirements necessary for the organization to recover and deliver the agreed level of business continuity
- Conduct a Cost Benefit Analysis in respect of strategy solutions versus the following types of impact at a site and business level:
    - Brand Image
    - Loss of Revenue
    - Legal/Regulatory and Contractual
    - Customer

- Section and Prioritization of solutions

The identification of business continuity strategy enables a range of options and models to be evaluated. This allows an appropriate response to be chosen for each critical product or service so the organization can continue to deliver those products and services at an acceptable level of operation during a disruption.

Within this context there is a number of strategic options and models that should be considered individually and in combination for each product and service. Both time and acceptable operating levels in terms of performance and functionality will determine the most appropriate strategy or strategies.

The following options should be considered as a part of the strategy development phase:

- Do Nothing: A “do nothing” business continuity strategy may be acceptable within an organization’s risk appetite.

- Best Endeavours: The risky development of an emergency strategy post a disaster or business continuity incident

- Terminate: Deciding to end a service, product, function or process should be considered as part of the process strategy within the BCM process. This approach is most likely to be seen where a product has a limited lifespan.

- Insurance: Provides financial recompense/support in the event of loss, where the loss can be quantified. It does not provide protection against a loss of reputation, stakeholder value and/or damage to brand image.

- Business Continuity Planning: The improvement of an organization’s controls, facilities and preparedness to minimize loss, disruption or interruption to its critical business activities to ensure they continue at an acceptable minimum level.

- Activity Transfer: The diversion of a critical business activity to another organization or alternative part of the host organization.

- Loss Mitigation/Risk Reduction: The implementation and management of risk controls and action plans to reduce, minimize or counteract any potential impact.

- Alternate Supply: The provision of an alternative supply of a product or service to the organization.

- Change: Deciding to change a service, product, function or process should be considered as part of the activity recovery strategy within the business continuity process. This approach is most likely to be seen where a product has a limited lifespan.

Most frequently the business recovery models that are considered as a part of the strategy development effort are:

- Active/Backup Model is having an “active” operating site with a corresponding backup site for both data processing and business operations. It relies on relocating staff from the active to the backup site and maintaining backup copies of technology and data.

- Active/Active (split operations) Model relying upon two or more widely separated (geographically) “active” operational/production sites for critical business activities that inherently backup for one another.

- Alternate Site Model having an “active” operating/production site with a corresponding backup site which periodically functions as the primary site.

- Contingency/Redundancy Model is where a technical system or element of a system automatically provided and alternate method of achieving the system and/or element and/or activity function e.g., system rerouting

- Displacement Model relies upon the displacement of a non-business critical activity that is currently being carried out at another site owned by the organization and replaced by a business-critical activity which is subject to a business continuity incident.

## 10.2 Work Area Continuity Options

In the majority of the cases a relocation of certain personnel and related Business Units is required as a Continuity Strategy.

A number of alternatives are open to an organization for provision of their continuity requirements. These options are focused on establishing an alternate work office location at a secondary site. All options involve the relocation of staff and varying levels of re-building office infrastructure and IT services. An overview of the options is presented below. (Alexander, Alberto 'A Methodology for Developing a Business Continuity Strategy' Continuity Central, 2016)

### 10.2.1 Own Site

This option refers to relocating selected staff to a site owned and maintained by an organization. Communications and general infrastructure would be in tune with the exact operational requirements.

### 10.2.2 Reciprocal Arrangements

This option refers to an arrangement with a similar organization. Each party should provide arrangements mutually agreed in case the other party suffers from a negative incident and therefore required invocation of the Recovery plan. The option may be applied for similar business units of an organization operating in different sites.

### 10.2.3 Third-Party Co-location Centers

This option is implemented through a third-party contract to use existing, equipped workplaces at a fixed location. The standard market offers include furnished rooms with standard infrastructure, local area networks and in many cases the potential to link into wide area networks.

Certain customizations apply on demand. Set-ups of desktop equipment may take place so site can be available almost immediately upon request.

Main advantages of such an approach are

- The ability of an organization to negotiate a contract for co-hosting its Disaster

Recovery Technology solutions (if any) in the same site with its personnel, as the majority of co-location centers provide both services

- The ability of an organization to use the same single site to respond to all loss scenarios for all its sites and buildings. Site can also be used to support the contingency plans for specific Business Units and operations
- Cost is fixed and known in the majority of the cases

Main disadvantages of this solution than needs to be taken into consideration are

- The fact that (unless paid for exclusivity, that will require very high rates) there is a risk of concurrent disaster declaration from more than one customer (as a standard, collocation centers rent the same office area to more than one customer, assuming that the risk of concurrent use is small versus the high rent price of exclusivity)
- The fact that relocation contracts refer to a limited time-frame presence of organization's personnel in the alternative location (typically this frame is usually 1 – 2 months max) and specific extra fees should be paid in case of contract extension

### 10.2.4 Company Controlled Recovery Site

This could be a site / building / industrial room (e.g., a large warehouse or a block of flats) that could be prepared and equipped with the following

- Alternate Data Center Facilities
- Office room to host the maximum number of people to be relocated in case there is a loss of a site
- Furniture, LAN, office equipment and personnel hosting facilities
- Communication networks pre-installed to ensure connectivity to all systems and elements and sites to ensure resilience in case of the loss of a site

Security should be one of the key parameters to be considered in such a case, plus the cost and consideration of the site maintenance and management.

### 10.2.5 Home Based Personnel

It is recommended that the Planning effort should include the case of working from home, yet this scenario analysis must include the flexibility to communicate under all site losses scenarios and assess all security concerns. This is an option widely explored and used during the COVID19 pandemic by many organizations worldwide.

Information Security issues as well as Labor relevant Regulations and Legislation should be considered.

In Annex F there is a detailed Pandemic Planning template that can be used by an organization to properly manage the impact of such incident. The template includes detailed activities and information for all stages of a pandemic.

An indicative example of the personnel summary recovery requirements is presented below.

| Sites | Business Unit | Normal Operation | Personnel Relocation Requirements | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ≤ 1 hour | ≤ 2 Hours | ≤ 4 Hours | ≤ 1 Day | ≤ 2 Days | ≤ 3 Days | ≤ 4 Days | ≤ 5 Days | TOTAL |
| A Site | A Unit | xxx | | | | | | | | | |
| | B Unit | xxx | | | | | | | | | |
| | C Unit | xxx | | | | | | | | | |
| B Site | D Unit | xxx | | | | | | | | | |
| | E Unit | xxx | | | | | | | | | |
| | F Unit | xxx | | | | | | | | | |

**Table 10.1:** Identifying Personnel Recovery Requirements

Apart from the personnel recovery requirements, the deployment of all supportive necessary equipment (e.g., workstations, laptops, printers, headsets, etc.) along with the software and applications (licenses) required should be taken into consideration when planning the recovery options and solutions.

## 10.3 Systems & Elements Continuity Options

This phase is about developing a Business Continuity Strategy for the critical systems and elements of an organization. This phase follows the initial Business Impact

Analysis (BIA) and Risk Assessment (RA) efforts and findings. The BIA & RA phases are very useful inputs that will be used extensively in developing the strategic options.

During the course of the BCM Strategy work, a series of discussions should be organized with organization's IT team. The aim of these discussions was to be aligned in terms of business and technical requirements; assuring compatibility of each strategic option of a technical area with another area that affects or is being affected by it.

The aim of the entire BCM strategy work is to provide input to an organization's senior management in order to prioritize, according to organization's specific criteria and considerations, all necessary actions and decisions that lead to the mitigation of several risks associated to the total loss of primary site(s).

Analysis and the subsequent BCM Strategic options for the recovery of the primary IT systems and elements hosted in primary site comply with the following guidelines:

- Focus is on the total loss of the site(s) and not on the isolated elements of the site(s). This means that when an organization loses a site, it loses all IT equipment hosted in this specific site
- The primary focus of analysis is on "saving" the revenue generating services as well as specific elements linked to services or activities of importance to the organization
- The strategic options provided, in many cases, present more than one solution to a catastrophic event, ranging from 100% redundancy without interruption of operation to a more cost sensitive approach accepting reasonable performance degradation

### 10.3.1 Network Approach

To avoid any loss of critical connectivity serving an organization's site(s), the following options are recommended:

- Establish alternative routing for each site in order to accomplish connectivity of the affected site with all other organization 's sites. This can be accomplished through a variety of solutions, such as:

i. A topology of two nodal points with respective links towards the other sites is proposed. That means that each site has a direct connectivity and connectivity with another organization's site through which the connectivity of the affected site with the rest of organization's sites can be restored.

ii. Implementing link connectivity towards two different vendor's exchanges, so in case of an outage in one of vendor's exchange the other one will serve organization's network

- Using a different media of transmission (i.e., in case leased line is in place, use microwave link or vice versa, ISDN, etc.).
- Vendor's service outage may be caused by wide area infrastructure or technology related damage. The possibility of involving an alternative communication vendor should be thoroughly investigated as a solution to be implemented.

In all proposed solutions the existence of the appropriate bandwidth is considered as prerequisite.

### 10.3.2 System / Application Approach

The approach takes into consideration the outcomes of the Business Impact Analysis, the systems / applications that have been identified as of high importance either by IT, business users or both.

The following indicative table summarizes the categorization of systems based on criticality, that may be provided by both IT and business users and their respective RTO & RPO during the BIA effort.

| Applications | Criticality identified by IT | Criticality identified by BUs | RTO | RPO |
|---|---|---|---|---|
| Application A | Critical | High | ≤ 2 Hours | Zero |
| Application B | Critical | High | ≤ 4 Hours | ≤ 2 Hours |
| Application C | Medium | High | ≤ 2 Hours | ≤ 2 Hours |
| Application D | Medium | Low | ≤ 1 Day | 1 Day |
| Application E | Medium | Low | ≤ 1 Day | 1 Day |
| Application F | Low | Low | ≤ 2 Days | ≤ 3 Days |

**Table 10.2:** Categorization of criticality of systems/applications

### 10.3.3 Services / Products Approach

This approach provides an overview of the systems / applications involved in the delivery of an organization's products groups. This is a further enhancement to the previous layer since within the Business Impact Analysis effort the severity of impact of non-delivering of each group of products already exists. Since an overall approach and implementation of a Disaster Recovery Solution is not always possible and easy due to various restrictions (i.e., budget), gradual implementation may be selected by deciding which product group is more valuable to an organization and how efficiently and easily ROI is achieved.

The relationship of the critical applications with the products or services provided by an organization in combination with the revenues of each service and the identified recovery requirements provides a proposed hierarchy of the Disaster Recovery Solution.

Another issue that is considered critical in the implementation of the Disaster Recovery Solution is the capacity of the system / application compared to the primary / production site. In order to decide on this issue, the Operational Risk Appetite (ORA) should be taken into consideration. This ORA dictates the organization's maximum acceptable losses and unavailability related to systems, services and activities. Since the current ORA requires redefinition and further enhancements, it is not easy to define and design the capacity of the DR solution in objective terms.

The full capacity of the decided to be implemented systems in the DR site is the desired target but often the reality dictates a more reduced scope. Nevertheless, it is absolutely necessary that the capacity implemented in the Disaster Recovery Solution will meet the business recovery requirements (RTO, RPO) that have been identified through this project. Scalable or gradual increase of the capacity may be selected having direct impact to the fulfilment of the recovery requirements.

### 10.3.4 Model Approach

Provisions must be considered in order for all critical systems to be recovered in case

a DR scenario is invoked. The standby state of equipment in the recovery site depends on the recovery requirements.

Disaster Recovery model may be classified in the following categories, which result to different computing power and storage requirements:

| Classification | Description | When to use (indicative figures) |
|---|---|---|
| Cold | In the DR site, only floor space is reserved for the equipment needed in case of a recovery. In case of a disaster, equipment needs to be purchased or brought in using a Recovery contract. | RTO > 48 hours<br>or<br>RPO > 48 hours |
| Warm | Equipment is already available in the recovery site but not dedicated to the recovery (in use for other purposes). Resources need to be freed up before recovery can start. | RTO < 48 hours<br>or<br>RPO > 48 hours |
| Hot | The recovery equipment is up-and-running in the recovery site, waiting to be activated for the recovery. In case of storage, this storage is already in use (active), using data replication. | RTO < 4 hours<br>or<br>RPO 15 minutes |
| Active | In this case the production environment is distributed in production and recovery sites. In case of a failure of 1 site, operation is continued with the remaining equipment (sometimes leading to a decreased performance until additional equipment is added to the configuration). Distributing environments over multiple (long distance) sites lead to increased response times due to network latency, similar to synchronous data replication and should therefore (as a general rule) not be implemented over longer distances. | RTO: zero or in seconds |

**Table 10.3:** Model Classification

Based on to the recovery requirements determined from each system, an organization may choose a mixture of the methods outlined above in their DR Data Centre.

### 10.3.5 Connectivity Approach

Connectivity in the DR site must meet two main requirements:

- It must meet the bandwidth needs for continuous data replication from the production site or sites to the DR servers and/or storage arrays, if such technology is used in order to ensure data availability and currency
- It must be able to handle remote connectivity of users and applications in the case of a disaster

Depending on the technological solution chosen for the data replication to the DR environment, the Recovery Point Objectives of an organization and the required user connectivity capabilities, the bandwidth and acceptable latency requirements can be calculated. The DR site will have to meet or, preferably, exceed these requirements.

### 10.3.6 Location Approach

The location of the DR site must be selected so that it is not affected by the same risks as the sites for which it will assume operations. Any site in a distance more than 50 Km from the affected one may meet the requirements for assuming operations.

It must also be assured that, in the case of a disaster, the DR site can be reached by all the necessary people to guarantee its operation. Any special circumstances that may occur during a disaster should be taken into account, which may result into usual means of transport being slower or unavailable.

### 10.3.7 Infrastructure Approach

The infrastructure supporting the equipment in case of a disaster must provide an appropriate level of availability based on an organization's business needs. Data Centre appropriate tier level (or hybrid solutions) should be present in the DR site (Tier I: Basic Site Infrastructure, Tier II: Redundant Site Infrastructure Capacity Components, Tier III: Concurrently Maintainable Site Infrastructure, Tier IV: Fault Tolerant Site Infrastructure).

Indicatively:

| Tier Level | Requirements |
|---|---|
| 1 | • Single non-redundant distribution path serving the IT equipment<br>• Non-redundant capacity components<br>• Basic site infrastructure with expected availability of 99.671% |
| 2 | • Meets or exceeds all Tier 1 requirements<br>• Redundant site infrastructure capacity components with expected availability of 99.741% |
| 3 | • Meets or exceeds all Tier 2 requirements<br>• Multiple independent distribution paths serving the IT equipment<br>• All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture<br>• Concurrently maintainable site infrastructure with expected availability of 99.982% |
| 4 | • Meets or exceeds all Tier 3 requirements<br>• All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems<br>• Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995% |

**Table 10.4:** Locations Classification

### 10.3.8 Design Requirements Approach

Whether the Disaster Recovery solution is hosted in an organization's owned or outsourced managed environment, there are certain design issues that need to be taken into consideration. Indicatively these issues are:

1. Design programming
   - ✓ Facility topology design (space planning)
   - ✓ Engineering infrastructure design (mechanical systems such as cooling and electrical systems including power)
   - ✓ Technology infrastructure design (cable plant)
2. Modeling Criteria

   Modeling criteria are used to develop future-state scenarios for space, power, cooling, and costs.
3. Design Recommendations

- ✓ Critical Power Capabilities
- ✓ Overall data center power requirements
- ✓ Mechanical cooling capacities
- ✓ Kilowatts per cabinet
- ✓ Raised floor space

4. Mechanical engineering infrastructure designs
   - ✓ Heating, ventilation and air conditioning (HVAC)
   - ✓ Humidification and dehumidification equipment
   - ✓ Pressurization
5. Technology infrastructure design

   Cabling is grouped and depends on the technology used. Voice, modem, and facsimile telecommunications services, premises switching equipment, computer and telecommunications management connections, keyboard/video/mouse connections and data communications etc.
6. Site Selection

   Aspects such as proximity to available power grids, telecommunications infrastructure, networking services, transportation lines and emergency services can affect costs, risk, and security while a wide array of location factors should be taken into account (e.g., flight paths, neighboring uses, geological risks).
7. Modularity & Flexibility

   These are key elements in allowing for a data center to grow and change over time and need to be carefully taken into consideration.
8. Environmental control
9. Electrical power
10. Cable Routing
11. Fire Protection
12. Security

The Annex E includes indicative templates that can be used to facilitate data collection and ensure the quality of the collected data for the phase. Such templates should be

distributed to the BC POCs in an organization and their content can be validated and discussed during organized sessions.

### 10.3.9 Hints & Tips

- The selection of solutions can be also influenced by legal or regulatory requirements or a commercial decision to gain competitive advantage.
- Service level agreements can be put in place with suppliers to support the selected solutions. Such agreements can offer some assurance that the organization will be notified of any changes in the supply chain to avoid undesirable consequences.
- In practice, there is always compromise between cost and speed of recovery. Generally, the shorter the RPO and RTO, the more expensive the solution is. Ultimately, the goal should be to balance continuity capability against reasonable and affordable costs.
- For the technology part, IT workshops need to be facilitated with the organization's technical teams to define contingencies and most suited scenarios covering all areas. Best practice solutions and approaches will be taken into consideration, in order to submit best advice.
- An alternate location solution that is pre-equipped and can be activated in a very short time frame can be also referred to as a "hot site". This can be an expensive solution as it means having resources in place but unused until they are required for business continuity purposes.
- A warm site standby solution may be suitable for lower priority activities which can be temporarily suspended after a disruption occurs to allow time for the warm site to be reactivated and prepared for occupation.
- Organizations usually find the best outcome in combining business continuity solutions, so that the solutions reflect the priority and RTOs of the processes and activities. This combined approach also allows limited resources to be allocated in advance to the continuity solutions that support the highest

priority activities, while providing low, or no up-front cost solutions for lower priority activities.

- Working remotely has the benefit of isolation during a pandemic-based incident or crisis. It is also effective when being at work or commuting to work is no longer reliable or safe (e.g., industrial action, terrorist attack or severe weather)

- Care should be taken to ensure consolidated solutions do not conflict with other common or unique individual solutions, organizational policies, supplier accreditation or legal and regulatory constraints

- Assessing the suitability of a supplier's continuity options or selection of any outsourced service providers should occur prior to any contract being agreed or as part of ongoing relationship management with the supplier. When seeking evidence of an effective BCP, the specific time objectives offered for the service should be requested (RTOs, MBCO and MTPDs). These objectives should align with the business continuity requirements of the organization

- While implementing alternative routing to increase redundancy, it should be carefully taken into account the last mile connectivity. Different vendors and routings may be used for a large portion of the route but it is usual to observe that the same last mile part is common for all. Hence, in case of a problem in the last mile route you have to manage a single point of failure

- Before deciding on the location / sites to be used as work area recovery and/or disaster recovery solutions, careful review and study of the area for adequate time should be done. Seasonal patterns, accessibility or other issues may cause unpleasant surprises after investments are made

- To facilitate the data collection in this effort, it is recommended that templates / questionnaires to be prepared that will ensure the quality of the data. These templates / questionnaires should be distributed to assigned POCs having incorporated the data collected from the previous phases. Afterwards a

validation of the collected feedback is proposed through discussion in a series of interviews.

# Chapter 11

# Business Continuity Plans & Response

## 11.1 Response Structure

Disruptions may have a broad impact on the operational status of an organization and may require the activation of several response plans by different management units. For example, there may be plans for evacuation, health and safety, ICT service continuity, physical security, crisis communication and information security.

A response structure needs to established to secure that the organization has a effective mechanism for responding to an incident, regardless of its cause. The response structure should include command, control and communication systems to manage the incident and minimize the impact.

The response structure should be capable of managing different types of disruption. There are two types of disruption:

- An incident is defined as event that can be, or could lead to, a disruption, loss, emergency or crisis
- A crisis is defined as “unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment”

Consequently, incidents and crises are linked but they require a different level of response.

There may be different types and levels of response teams depending on the size, complexity and type of an organization. It may be appropriate to have three levels of teams such as strategic tactical and operational ones. (Alexander, Alberto:2016)

- Strategic: Team focuses on issues impacting organization's core objectives, products and services and is led by top management. It is often called crisis management team and primarily address any crisis impacting the organization. The team requires to have a creative response and the authority to mobilize organization's full resources during the response. The management of events damaging organization's reputation and image are among the crises that the team should manage. Hence, communication plans and media response should be included. The team may provide guidance and communication support to the rest of the teams for less severe events

- Tactical: The team manage the continuity of the processes that are required to deliver the products and/or services impacted by the incident and to allocate the necessary resources for remediation. It assesses and manages the sort and medium-term effects of an incident while providing a framework to coordinate strategic goals with the operational response team
- Operational: The team deals the continuity of the activities that maintain the processes of delivering the products and services. It manages the immediate effects of an incident and its consequences

### 11.1.1 Hints & Tips

- ❖ The organization should develop a structure that meets its own needs that is closely aligned with the existing management structure. Hence, it is recommended the use of organization's terms such as team names, titles and roles.

- ❖ It is recommended that all business units of an organization should have appointed representatives in the response structure with duties and responsibilities directly related to their functional operation

- ❖ Disruptions may be obvious but may also develop slowly over time and result in crisis. The response structure should include a mechanism to promptly identify an incident and its capabilities of becoming a crisis using experienced, trained and authorized personnel.
- ❖ Depending on the size and complexity, some organizations may merge one or more levels in a single team
- ❖ It is critical that all members of the team should have the required competencies and skills for their roles and supported by the appropriate training and awareness
- ❖ Backup people for all roles should always be identified and involved in the management of the incidents and crises

## 11.2 Business Continuity Plans

Business Continuity Plans can be developed to address the strategic, tactical and operational requirements of an organization while the type of plans depends on the solutions agreed during the strategy phase, its size and its complexity of operational model. (Tucker: 2015, Watters:2010, Timms:2018)

### 11.2.1 Strategic Plans

A strategic level (crisis management) plan is a high-level plan that includes how strategic issues resulting from a crisis should be managed by the top management of an organization. Since there may be some incidents that do not involve disruption to the organization, these incidents may require a strategic level response such as negative media exposure that threatens an organization's reputation. In such incidents it is always necessary to involve the strategic team as the situation may escalate.

This type of plans should address strategic issues that impact the organization's core objectives, the need to communicate all involved interested parties and should not encourage micro-management of an incident. The strategic level team is responsible

for the organization's stability and reputation. Hence the following should be included in the plan:

- The strategic objectives of the incident or crisis response
- Setup short-, medium- and long-term strategies addressing different types of crises or incidents
- Manage communications (communication plan) with all involved parties including the media
    - Identify internal and external involved parties, communication requirements and expectations
    - Define the available methods and channels of communication and include a selection of such methods to secure availability of at least one method. Assign the person(s) to be responsible to deliver communication through the specific methods
    - Assign the role of organization's spokesperson and ensure that he/she is well trained and easily available during crises or incidents
    - Secure the existence of designated persons from different functional units to support the spokesperson with their expertise
    - Setup process to issue media statements and to monitor and review the response of the involved parties during the communication to adjust if required
- Setup a mechanism to monitor the response to the crisis or incident
- Ensure that the response is in line with the long-term strategy of the organization and complies with the legal and regulatory requirements of its operation
- Define the end of crisis or incidents and communicating it to the involved parties

### 11.2.2 Tactical Plans

They coordinate the response to an incident and ensure the continuity of the prioritized activities. The plans should include a mechanism to assess the impact of the disruption, apply the necessary solution and provide updates to the strategic (crisis) team while they address the response from the initial alert to the point where the disrupted activities are restored.

- The tactical plans should include:
- Mechanism for the coordination and monitoring of the operational teams
- Provision of support services to the operational teams (IT, HR, Finance, Admin)
- Allocation of resources such as:
    - Employees of the organization
    - Welfare Services
    - Security Services
    - Transportation and Logistics
    - Suppliers and alternate vendors
    - Resource requirements for each prioritized activity
- Adapting the priorities and response actions based on the conditions
- Management and progress updates from operational teams
- Reporting to the strategic team
- Focal point for the mobilization of service providers

### 11.2.3 Operational Plans

The operational level plans define the involvement of the individual business units of an organization in the incident response. They support the continuity of the prioritized activities from the start of the incident till the recovery of the agreed levels of operation and the return to business as usual.

Such plans may include the restoration of the operation of a business unit, of services or recovery of applications.

The following should be considered while developing operational level plans:

- A Point of Contact per each business unit should be appointed during the development of their plans
- It is recommended to use standardized templates to facilitate their population but always keep in mind variations depending on industry and complexity
- The individuals assigned to specific roles within the plan should have the necessary competencies to fulfill their tasks
- Communication and information interdependencies with the tactical teams should be considered and taken into account
- Draft version of the plans should be distributed to the business units for review, feedback and approval

There are numerous templates that are used for the population of a Business Continuity Plan and their format highly depends on the complexity and the size of the business units and/or activities to be included. In Annex G, there is a sample of BCP document that includes all aforementioned levels of requirements (strategic, tactical and operational).

### 11.2.4 Incident Management Example

The following diagram depicts a simplified chart of incident management. Depending on the size and the complexity of the organization, this type of diagrams may be more complex and detailed. Explanatory details for the different phases of the incident are presented below.

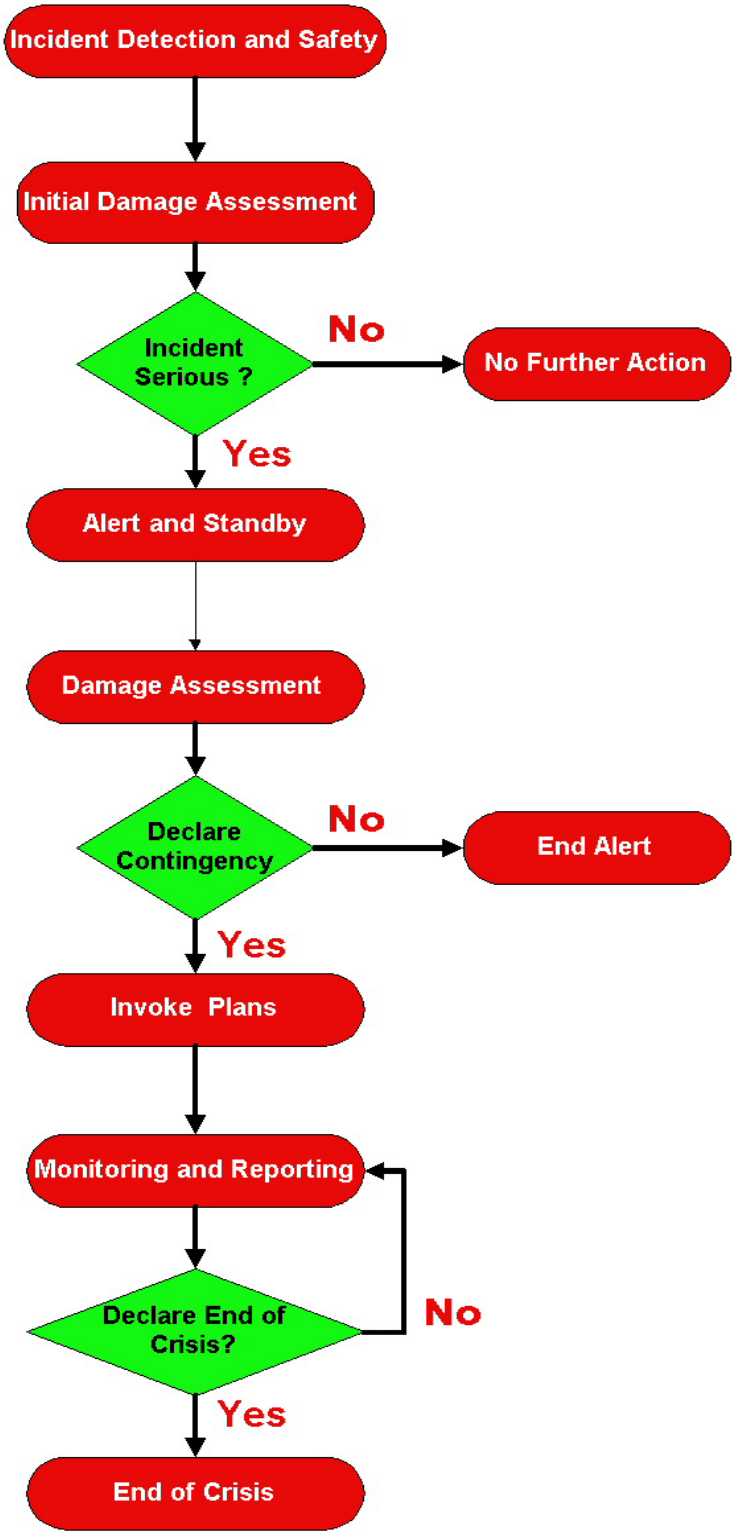



**Figure 11.1:** Indicative Incident Management (IM) Flow Chart

***Incident (Crisis) Management Activities within Phases***

*11.2.4.1 Incident Detection and Safety*

| Owners | # | Actions | Tick when done |
|---|---|---|---|
| Security Services & Guards | 1. | Immediately contact Site Manager | |
| Site Manager / Evacuation leader & team | 2. | If necessary, invoke site Evacuation Plan if there is any risk to the health and safety of the staff - ensure the safe evacuation of staff | |
| | 3. | Contact General Administration Head and report the incident | |
| | 4. | Contact Logistics/Damage Assessment Team Leader and report incident | |
| General Administration VP | 5. | Contact CEO (IMT (CMT) Leader) and report the incident | |
| Data Centre Manager and/or ICT personnel | 1. | Immediately contact Infrastructure Manager | |
| Infrastructure Manager | 2. | Contact the ICT Head & Logistics/Damage Assessment Team (if necessary) and report the incident | |
| ICT Head | 3. | Contact CEO (IMT (CMT) Leader) and report the incident | |

*11.2.4.2 Initial Damage Assessment*

| Owners | # | Actions | Tick when done |
|---|---|---|---|
| Logistics/Damage Assessment Team Leader | 1. | Conduct an initial damage assessment and impact on the site | |
| | 2. | Notify the CEO (IMT (CMT) Leader) of the damage and possible crisis situation | |
| ICT Head | 1. | Notify the CEO (IMT (CMT) Leader) of the outage of the system / Main Data Centre damage and possible crisis situation | |
| IMT (CMT) Leader | 3. | Discuss situation with IMT (CMT) members | |
| | | No further action is required if the situation is not serious | |
| | | Proceed to section Alert & Standby if situation is serious | |

*11.2.4.3 Alert and Standby*

| Owners | # | Actions | Tick when done |
|---|---|---|---|
| IMT (CMT) Leader | 1. | Notify the Chairman (if necessary) | |
| | 2. | Notify IMT (CMT) members to be on standby, and to ask their respective specialist and recovery teams to be on standby | |
| IMT (CMT) ICT Member | 3. | Notify the IT Coordination Team Leader to be on standby | |
| | 4. | Notify the Disaster Recovery Centre's (DRC) Manager to be on standby | |
| | 5. | Notify the offsite storage team to be on standby | |
| IMT (CMT) HR Member | 6. | Notify the Human Resources Team Leader to be on standby | |
| IMT (CMT) General Administration Member | 7. | Notify the Logistics/Damage Assessment Team Leader to be on standby | |
| IMT (CMT) Business Units Members | 8. | Notify the affected Business Units Coordination Team Leaders to be on standby | |
| IMT (CMT) Communications Member | 9. | Notify the Communications Teams Leader to be on standby | |
| IMT (CMT) Business Continuity Member | 10. | Notify the Business Continuity Coordination Team to be on standby | |

*11.2.4.4 Damage Assessment*

| Owners | # | Actions | Tick when done |
|---|---|---|---|
| Logistics/Damage Assessment Team Leader | 1. | Continue to assess the damage, and to provide regular status reports to the IMT (CMT) Leader regarding the extent of damage at agreed intervals | |
| | 2. | Consult with public safety authorities, police, fire and rescue units to ensure that the site is safe and secured | |
| | 3. | Ensure the staff's safety | |
| IMT (CMT) HR Member | 4. | HR to expedite medical treatment where necessary | |
| Infrastructure Manager | 1. | Continue to assess the damage, and to provide regular status reports to the IMT (CMT) Leader regarding the | |

| Owners | # | Actions | Tick when done |
|---|---|---|---|
| | | extent of damage at agreed intervals | |
| IMT (CMT) Leader | 5. | Monitor and discuss the situation with IMT (CMT) members until decision can be made to either declare a Crisis or cancel the alert. | |
| IMT (CMT) Communications Member | 6. | Prepare press briefings | |
| IMT (CMT) Leader | 7. | Discuss situation/decisions with the Chairman | |
| IMT (CMT) Leader | 8. | If the decision is to declare a state of CRISIS, then go to section Invoke Plans) | |
| | 9. | If the decision is to end the alert then go to section End Alert | |

*11.2.4.5 End Alert*

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| IMT (CMT) Leader | 1. | Notify all IMT (CMT) members on the end of the alert | |
| IMT (CMT) IT Member | 2. | Notify the IT Coordination Team Leader on the end of the alert | |
| | 3. | Notify the DRC Site Manager on the end of the alert | |
| | 4. | Notify offsite storage team on the end of the alert | |
| IMT (CMT) HR Member | 5. | Notify the Human Resources Team Leader on the end of the alert | |
| IMT (CMT) General Administration Member | 6. | Notify the Logistics/Damage Assessment Team Leader on the end of the alert | |
| IMT (CMT) Business Units Members | 7. | Notify the affected Business Units Coordination Team Leaders on the end of the alert | |
| IMT (CMT) Communications Member | 8. | Notify the Communications Team Leader on the end of the alert | |
| Business Continuity Member | 9. | Notify the Business Continuity Coordination Team Leader on the end of the alert | |

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| | 10. | Collect data, prepare and submit management report | |

*11.2.4.6 Invoke Plans*

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| IMT (CMT) Leader | 1. | Declare a state of Crisis and notify all affected IMT (CMT) members to invoke their respective plans where relevant | |
| IMT (CMT) IT Member | 2. | With the assistance of the IT Coordination Team instruct the involved Recovery Coordinators to invoke their Recovery plans | |
| | 3. | Instruct the IT Coordination Team to assist the Recovery of all other affected BUs | |
| | 4. | Contact the DRC Site Manager and notify (him or them) of possible recovery of IT systems | |
| | 5. | Inform offsite storage to ship all pertinent containers (if necessary) | |
| IMT (CMT) HR Member | 6. | Instruct the HR Resource Team Leader to invoke relevant HR directives including relevant recovery plans | |
| IMT (CMT) General Administration Member | 7. | Instruct the Logistics/Damage Assessment Team to commence salvage / repairs | |
| | 8. | Instruct the Logistics/Damage Assessment Team to assist the Recovery of all other affected BUs | |
| | 9. | Commence collection of data for insurance claims etc. | |
| IMT (CMT) Business Units Members | 10 | Instruct the affected Business Unit Recovery Coordination Team Leaders to invoke their respective and relevant plans | |
| IMT (CMT) Communications Member | 11 | Instruct the Communication Team Leader to go to the scene (if not already there) and prepare to deal with any media issues. | |
| Business Continuity Member | 12. | Notify All IMT (CMT) Members to meet at the chosen Management Centre, if this was instructed by the IMT (CMT) Leader. | |

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| | 13. | Record a declaration of Crisis in the activity log | |
| | 14. | Record details of all Business Units and technical recovery plans that have been invoked | |

*11.2.4.7 Monitoring and Reporting*

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| Business Continuity Member | 1. | Document and display recovery schedules & status in a visible place (whiteboard or power point) | |
| | 2. | Establish regular scheduled status meetings at defined intervals | |
| | 3. | Track progress of plans that have been invoked | |
| | 4. | Receive and consolidate all reports and recovery logs from all teams | |
| | 5. | Review and analyse logs, and prepare management reports | |
| | 6. | Submit status reports to IMT (CMT) members at agreed intervals | |
| | 7. | Keep recovery teams informed of all decisions made | |
| IMT (CMT) IT Member | 8. | Provide status reports to IMT (CMT) on progress of systems recovery | |
| IMT (CMT) General Administration Member | 9. | Ensure the staff's safety at all times | |
| | 10. | Ensure that the security is not compromised | |
| | 11. | Continue with salvage operations and repairs | |
| | 12. | Submit insurance claims | |
| IMT (CMT) HR Member | 13. | Monitor the need for human resources by various recovery teams. | |
| IMT (CMT) Communications Member | 14. | Gather information about the incident | |
| | 15. | Monitor what the press is saying about the incident and the organization | |
| IMT (CMT) Leader | 16. | Prepare and release communications as directed by IMT (CMT). | |

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| | 17. | Review reports and provide advise/direction/support as needed | |
| | 18. | Monitor/approve submission of insurance claims | |
| | 19. | Keep the IMT (CMT) members and the Chairman informed | |
| | 20. | Review the status with the CMT members, and when appropriate declare end of Crisis (go to section End of Crisis) | |

*11.2.4.8 End of Crisis*

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| IMT (CMT) Leader | 1. | Notify all the IMT (CMT) members on the end of the Crisis | |
| IT Coordination Team | 2. | Verify with respective teams that all activities and services have been restored | |
| | 3. | Ensure that details of the actions taken in resolving the incident are recorded | |
| | 4. | Report team's actions to the IT Coordination Team Leader | |
| | 5. | Update the invoked plans | |
| IT Coordination Team Leader | 6. | Ensure/confirm that all services have been restored | |
| | 7. | Inform the ET EVP (IMT (CMT) Member) | |
| | 8. | Compile the IT Coordination Team reports into one report and submit the report to the BC member | |
| Business Continuity Member | 9. | Notify all interested parties that the Crisis phase has ended | |
| | 10. | Receive status reports from all of the IMT (CMT) Members | |
| | 11. | Hold post Crisis workshops with IMT (CMT) members and team leaders | |

| Owner | # | Actions | Tick when done |
|---|---|---|---|
| | 12. | Prepare management report with recommendations and submit to IMT (CMT) Leader for approval and further action | |
| | 13. | Update Incident (Crisis) Management Plan and track agreed actions | |
| | 14. | Ensure plan owners update their respective plans where necessary (lessons learned) | |

### 11.2.5 Crisis Communication Plan

Crisis and issue management approaches start from the promise that good management can turn event to your advantage or head off the likelihood of a potentially damaging situation before it becomes serious. A crisis averted is a tribute to good media communication work. A sound plan and good preparation may help to avert disaster or at least to limit damages.

The crisis communication plan is to provide clear steps for communication within an organization and with the stakeholders outside the organization. The goal of this crisis communication plan is to establish a communication roadmap for variety of risk potential situations. The objectives of the plan are:

a) To identify and inform parties involved

b) To communicate facts about the crisis

c) To minimize rumors and restore confidence

Usually, the ownership of the crisis communication plan is assigned to the Media & Communication Business Unit of an organization that is responsible for implementation of the crisis communication plan. The document should be reviewed and updated regularly and at least on a quarterly basis while contact details should always be current.

When crisis is declared and the nature of crisis is identified by the IMT (CMT), the following questions should be made:

- **What precisely has happened?** Do we all have the same understanding of the situation? Could this incident call into question the reputation of the organization?
- **Is there more to come?** Are there likely to be more of these events which will worsen the problem?
- **Who will be affected and what will they think?** What would the organization look like from the outside in the eyes of local community, the officials and other audiences especially the Media
- **What is the likely time scale?** How long before the various media interested in the story start to run the story? Do we have a holding statement?

Once crisis is identified and the source is known and established, the main focus should be on the Stakeholders; internal & external. Clear messages needs to be communicated to all stakeholders.

Depending on the audience and stakeholders addressing, the communication means used may be multiple and different. Indicatively:

- **Phone Communication:** Organization's CEO should contact organization's board using a more direct approach to the communication. The first call should be very short and precise one and only for notifying and alerting them about the incident in progress. Once the main cause of the problem and the severity of the impact are identified further information is provided to them related to the estimation of the time needed to fix and resume organization's affected operations.
- **Email Communication:** Legal / Compliance / Regulatory Business Unit should send e-mails to Regulatory and Legal Authorities, to inform them about the incident. This e-mail should be very short with promise that more details will be provided as soon as the incident is fully investigated with real time estimate to resume the organization's operations.
- **Automated Call Announcements:** In case of unavailability of Call Centre announcements should be activated and released through an IVR system. The

content of these announcements will need to be prepared by the Marketing & Communication Business Unit, based on the solution that has been decided to be implemented. The announcements need to be pre-recorded and ready for use. Further announcements may need to be recorded on specific purpose, depending on the incident, impact and duration of unavailability. This needs to be decided by the IMT (CMT) and approved by its leader.

- **Call Centre:** It is certain that external stakeholders (customers, media etc.) will try to communicate the organization in the event of a disaster to know more details. It is highly essential that the information communicated outside organization should be controlled, especially in the early stages of the incident, until statements are provided by organization's spokesperson. In order to avoid confusion and mishandling, organization's Call Centre should respond in such queries in a predefined manner and direct the external stakeholders to the official organization's announcements through organization's spokesperson. No other information or details need to be announced by Call Centre.
- **Public Announcement through organization's Web Site:** Announcements should be released in the web site. The content of these announcements will be prepared and released by the Marketing & Communication Business Unit.
- **Newspaper Statement:** Marketing & Communication Business Unit may prepare a statement to be distributed to the media. This statement will cover all details about the incident and all extra measures that organization has taken to protect the organization in the future. This statement will be released at the end of the incident's day.
- **Press Conference:** The organization may call a media press Conference if:
    - There is a major crisis and the entire organization cannot not resume on the same and/or next day. Or
    - There has been damage to any of organization's site(s) that has resulted in casualties. Or

- There have been media reports for incorrect or inaccurate information handling impacting reputation of the organization

The designated organization's spoke person will lead the Press Conference.

- **TV Interviews:** In certain situations, it may be necessary to organize a live TV interview with selected channels. When it is required, this will be done by the designated spoke person and should be brief (3-5 minutes). It should be scheduled after the initial investigation is completed.

Following any or more of the aforementioned ways of communication, it is strongly recommended that the Marketing & Communications BU will be responsible to monitor the media response to the incident by watching TV channel, scanning related websites and newspapers. Updates should be provided during the day and a Report should be produced next day detailing all comments, criticism and recommendation came out as result of the incident. The report should be distributed to all IMT (CMT) members.

### 11.2.6 Hints & Tips

- Plans should be held in secure locations accessible to all involved stakeholders. It is recommended that they should be available in both electronically and hard copy format
- Although there may be a number of plans related to different business units within an organization, it is advised that their copies should be stored and maintained centrally
- Automated notifications systems can help an organization to contact and communicate with its employees more easily
- Social media (e.g., WhatsApp, Viber, Facebook) can be also used to notify and mobilize the necessary resources of an organization. This method of notification requires careful preplanning and information security approval
- The tactical response team prioritises and coordinates the response activities per the agreed priorities and solutions directed by the top management. This

may involve the activation of multiple operational level plans with a specific sequence

- Strategic, tactical and operational level plans should be reviewed regularly in line with each other in a predefined frequency or after a major change in the organization
- It is advised that the operational level plans to be detailed to facilitate the personnel that is not familiar with the activities to be followed or the systems to use. The details should also include manual workaround procedures that are used as a recovery of automated procedures
- For small size enterprises the different levels of plans may be consolidated into a single one
- It is recommended that assigned spokespeople should be very well trained to manage media under pressure
- There are several hints & tips regarding the communication during a crisis. Indicatively:
    - Since the rise of digital and social media, stakeholders expect a quick response to any issue that arise. Late response may generate false conclusions to the audience such as that the organization is guilty or that it does not control the situation. It is recommended that any response should primarily use the same channels where the crisis was initially announced.
    - It is advised that an organization to build strong relationships with external stakeholders. It is necessary to establish a strong rapport with the audience communicating with the organization and maintain a good relationship. Then, in time of crises people tend to be more susceptive to the justification provided.
    - When a crisis occurs, you're under a microscope; every move you make is going to be judged by the public. It's better to be upfront and transparent than plead ignorance or stonewall. If there's additional,

related information that could paint the company in a negative light, it may be better to share it. The news will leak eventually, and you have a better chance of controlling the message. The more information you hide, the guiltier the company will look.

- Although it's near impossible to anticipate everything that could happen, brainstorm potential scenarios with the team and map out how someone would react, so if the situation does occur, the team will be better equipped to handle it. Focus on situations that align with organization's product, services, and industry—particularly on areas where the likelihood and impact of something going wrong are high.
- When a crisis occurs, it is required to make sure that all teams company-wide are addressing the issue in a cohesive manner. It should be kept in mind that employees are organization's ambassadors when a crisis hits. It is recommended that a one-page sheet to be created and shared across the organization that outlines the actions each department should take if a crisis occurs.
- It is recommended to avoid pointing to possible culprits. Although always in the start of the crisis people tend to place the blame, it is necessary and essential to prioritize the audience and their feelings.

# Chapter 12

# Development Of Exercise Programme

The continuity capability of an organization cannot be considered reliable unless it has been tested. Only realistic exercises can validate how well designed are the continuity solutions of an organizations and identify issues that require attention. Only through exercising the continuity arrangements can the business continuity management capabilities of an organization be improved, while the lessons learned during the exercising activities will be integrated into the planning of the future activities. (Flynn: 2008, GM Heng:2006, Paton & Jackson:2002)

## 12.1 General Principles

The scope of an exercise programme is:

- Evaluation an organization's capability in the continuity activities
- Ensure the achievement of the agreed RTOs and RPOs
- Validate the continuity solutions and the assumptions that have been made
- Verify the completeness and accuracy of the business continuity plans
- Verify the adequacy of the resources required for the restoration of the organization
- Identify areas for improvement
- Confirm the competency of the personnel with the relevant roles and responsibilities

- Increase the awareness of personnel related to Business Continuity arrangements

The exercise of BC arrangements is not an activity that is conducted only once. It should be designed and scheduled in a way that it will ensure that an organization will be able to gradually improve its continuity capability and secure the efficiency of its continuity solutions.

The exercising program may use a combination of exercising methods to ensure that the expected outcomes are achieved and increase the awareness of the involved personnel.

The exercises should be realistic in order to confirm the proper operation of systems, communication lines (all types), infrastructure and procedures that support the business activities, the Business Units or the entire organization's operation.

Each exercise should have specific and clear anticipated purpose and outcome.

The following should be anticipated through an exercise:

1. All involved parties should have a clear understanding and knowledge of the plans, the scenario to be tested along with their roles.
2. To confirm that all activities and components of the exercise plan are realistic and functional while all systems, communication and infrastructure in the alternative area are operating as it has been anticipated.
3. To confirm that all prioritized business activities have been recovered to the predefined level within the Recovery Time and Point objectives that each involved Business Unit has identified in the BIA process.

It is essential that a different scenario needs to be elaborated each time, in order for all the parameters of the involved plans to be tested.

An exercise should not expose organization at any irrational risk, but needs to be practical and functional in order to build trust in the existing plans.

## 12.2 Preparing An Exercise

A soon as the Exercise Program has been approved and published, all involved Business Units will be required to proceed with the preparation of their plans exercise.

The main responsibility of the preparation of the exercise lies in the involved Recovery Coordinators with the assistance of the Business Continuity Unit.

The Exercise is prepared with the collaboration and coordination of all involved Business Units.

Each Exercise should be carefully designed taking into consideration the following issues:

- Exercise aims and objectives

Both aims and objectives should be clearly defined and may be related to the activities of a Business Unit and/or systems, applications and infrastructure that are required for the adequate operation of the organization

- Scenario

Brief description of the scenario and of the risks identified along with action in the event of unforeseen circumstances

- Business Units and personnel to participate
- Third Parties

All external parties such as vendors, suppliers, observers, authorities etc.

- Systems and Infrastructure to be tested

Business Systems, communication lines and infrastructure necessary to ensure OIC's recovery.

- Success Factors

The exercise document should include:

    - The specific parameters and factors to be tested (i.e., comprehension of the roles, time to reach alternative areas etc.)

    - Recovery Time & Point objectives as these have been identified through the BIA process
    - The acceptable level of operation of systems, applications and activities involved in the test
- Detailed Implementation Plan of the Exercise

It should include the scheduling, date and time, the individual steps that need to be performed, the involved parties (both internal and external with contact details) etc.

It is also required to include the description of all preparatory activities prior to the actual execution of the exercise.

- Management of Exercise's Impact

Any effort should be made to ensure that no impact will be caused in any of OIC's operation during the exercise.

- Results Recording

In each exercise document there should be recording of the evaluation criteria in order to measure the effectiveness of the outcome along with actions related to the follow-up of the conclusions that emerged the execution of the actual exercise

Upon completing the design and documentation of the Exercise Plan, organization's Business Continuity Unit sends it to the BC Steering Committee for review and approval.

## 12.3 Conducting An Exercise

Organization's Business Continuity Unit has the overall coordination of the implementation of the Exercise. He/she is responsible to command the start and the end of the Exercise.

He/she communicates the detailed time plan of the exercise to every third party that will participate in the execution of the exercise with the support of the involved Business Units' Recovery Coordinators.

Observers from the management of the organization may participate in the execution of the exercise.

During the exercise all actions and comments should be recorded on the responsibility of organization's Business Continuity Unit. This recording will help in the introduction of potential improvements and the update of the plans.

At the end of each exercise all involved Recovery Coordinators ensure the evacuation of the alternative facilities, the safe removal of involved staff and visitors, the cleaning of the used spaces and the proper arrangement of the infrastructure in order to be ready for use when necessary.

Upon the completion of the exercise the Recovery Coordinator of each involved Business Unit should complete a report with the results and observations (targets have been achieved or not, outcome assessment, recommendations, changes of the existing plan, etc.) and deliver it to the Business Continuity Unit.

Based on the relevant reports delivered by the involved Recovery Coordinators and the results of the Exercise, the Business Continuity Unit

- Prepares a post Exercise report related to the outcome and results of the exercise, inform the Business Continuity Management Steering Committee of the problems or difficulties encountered, deviations recorded, improvements required etc. This report will be integrated into the annual evaluation report of the Business Continuity Unit to the Business Continuity Management Steering Committee
- Enables the process of updating the Business Continuity and/or Disaster Recovery Plans if it is required
- Archives all documentation related to the Exercise

## 12.4 Types of Exercises

There are several types of exercises with different levels of involvement, complexity and risk. (Alexander, Alberto 'Planning and Managing Exercises for Business Continuity Management Arrangements' Continuity Central, 2016) Indicatively:

### 12.4.1 Scenario Exercise

It is a discussion-based activity that usually address a specific scenario within a specific time frame. It requires that the involved participants should have familiarity with the

plans tested and their roles by demonstrating their understanding and response as the scenario unfolds. Usually, assessment check lists and practical outputs may be produced by the teams involved. Such exercises can be realistic, cost effective and efficient.

### 12.4.2 Notification Exercise

Call tree is a method of dependable communication between members of a group such as employees in an organization. Such test may be used to respond to an emergency, prepare for a natural disaster or in the event of any disaster. It can be automated through system that contacts individuals using a landline, email, cellphone, text / data message. It may also be done manually in which each person who receives a call is responsible for calling others in a tree-way.

### 12.4.3 Simulation Exercise

Such exercise may involve different level of teams (strategic, tactical, operational) across all locations of an organization. The scope is to simulate a real incident and the participants are asked to manage, develop and implement a response to the unfolding scenario. This type of exercises allows to rehearse all aspects of Business Continuity plans (notification, assessment, decision making, communication) along with the resources or even external stakeholders required to support the teams.

### 12.4.4 Live Exercise

This type of exercise can vary from a rehearsal of a part of the response during a disaster to full scale practice of the whole organization, with the participation of all involved parties including external stakeholders. Such exercises are the most useful since they are most realistic way to train the involved personnel and identify gaps and omissions that may not be visible in the other types of exercises.

Nevertheless, they may be extremely costly, time and effort consuming while extra consideration should be taken to avoid disruption or any impact in the organization's operation and services.

### 12.4.5 DR Test

Such tests involve mainly equipment, systems, applications, etc. that are related to the recovery procedures, technology and infrastructure supporting business activities, services and products. They are critical to validate the RTOs and RPOs and in most cases the participation of vendors and suppliers are required.

The exercise programme should include the objectives that need to be achieved, the methods that are required, the resources to be allocated along their training requirements.

The Annex H includes indicative test reports templates for different types of exercises conducted.

## 12.5 Hints & Tips

- Depending on the complexity, the scale of involvement of the personnel of an organization, the resources required and the risk level, some exercises may be conducted more frequent than others. It is generally recommended that exercises should be done on at least annual basis
- As in other BC arrangements, the exercise should be reviewed and updated regularly at agreed intervals or following a major change in the organization (systems, services, products, etc.)
- Adding realism in the exercises is critical to test the procedures and methods as in a real event and greatly helps to check the validity of the plans and increase the awareness of the involved personnel
- Exercises should be regarded as small projects with careful and detailed planning especially the ones that are riskier and more complex. As the continuity capability of an organization is further improved along with the confidence and maturity of the personnel grow, some of the exercises may be conducted without any warning
- The people responsible for planning and managing exercises should:

- Any disruption or impact that may be caused by the exercise is agreed, controlled and minimized
- Top management fully comprehends and accepts the risk of something going wrong during complex exercises
- There should always be control points and fallback procedures in case it is required.

❖ The involvement of suppliers and outsourced partners is considered an important part of an organization's recovery capability. Hence, they should be involved in the exercise programme as part of both ongoing relationship and of contractual agreement

❖ An independent to the exercise resource is needed to be assigned as an observer to monitor and record the progress of the conducted exercise and any issues identified. Lessons learned after each exercise should be discussed with all involved stakeholders and used for future improvements

# Chapter 13

# Maintenance & Review

## 13.1 Maintenance

The maintenance of the business continuity programme in an organization is critical since it maintains all BC arrangements updated and valid. It is only way to ensure that an organization maintains its readiness to respond effectively to any disastrous incident despite any periodic or major organizational and/or technological change.

The maintenance should be conducted through a formal process and be incorporated into the organization's change management process. (Snedaker, Rima:2014)

Usually, the trigger for any maintenance activities is caused by any of the following reasons:

- Changes in the organization structure, infrastructure, services, products or processes
- Any review or audit (internal or external)
- Lessons learned through the exercise programme or through a real incident
- Changes through the Business Continuity Management Lifecycle (BIA, RA, Strategy)
- Changes to the environment that the organization operates (legal, regulatory, marketing, vendors and suppliers, etc.)

### 13.1.1 Hints & Tips

- ❖ It is recommended that the responsibility for the maintenance should be assigned to the functional unit representative for business continuity. In this way, the maintenance can be less time consuming and more efficient.
- ❖ Regular reporting indicating progress of maintenance, weaknesses identified and recommendations for improvement can greatly assist in managing the maintenance process more efficiently
- ❖ The management of the maintenance of the BC documentation can also be done through proprietary BC tools and applications that have automated processes for the tracking, reporting and follow up to secure the update of all BC arrangements
- ❖ The maintenance process and its intervals should be defined within the business continuity policy
- ❖ Business Impact Analysis, Risk Assessment and Strategy phases are recommended to be conducted on annual basis

## 13.2 Review

The scope of review is to evaluate the effectiveness, suitability and completeness of the Business Continuity Programme in an organization.

Indicative review types are:

- Audit (internal and external)

  The audit analyses an organization's business continuity programme and verify it against specific standards and criteria (e.g., ISO22301, ISO27001, etc.). The outcome of the process indicates whether the BC programme is compliant with industry standards and may generate an action plan of improvements

- Management Review

  The BC programme is reviewed by the top management ensuring that it is aligned with organization's objectives. It also provides the opportunity to

underline top management's commitment to Business Continuity Management Lifecycle while supporting its governance

- Self- Assessment

  The scope is to review and assess the implementation of the business continuity programme against specific predefined targets, objectives and milestones

- Suppliers' Performance

  The review of Suppliers' Performance should be conducted against contractual Service Level Agreements related to their business continuity programme. Primary prerequisite is that the organization has identified its level of dependency on suppliers and the respective expectations have been defined in relation to BC

- Performance Appraisal

  This process may be part of the regular personnel appraisal process or only to review individual performance of their roles and responsibilities in the BC programme. The process helps in integrating BC programme as an important part of organization's operation

- Quality Assurance

  The process of quality assurance determines the business continuity programme meets the organization's requirements. It is an ongoing process throughout the entire business continuity lifecycle

The outcomes of all review types implemented in an organization should be documented in formal reports.

### 13.2.1 Hints & Tips

- ❖ All review types should not only be considered as measurement of the efficiency of the Business Continuity Programme but also as a major tool for its further improvement and maturity

- Prior to the actual audit, the audit evaluation criteria should be clearly defined, while the audit framework should take into account any legal or regulatory requirements
- It is recommended that the Suppliers' Review performance to be conducted for key suppliers of an organization. Their performance and capability can be efficiently measured through involvement in their exercise activities
- As the rest of BC arrangements, each of the implemented review types should be reviewed at regular intervals
- Management Review should identify adaptations to be implemented in the BC programme due to changes to the external and internal environment

# Chapter 14

# BCM KPI Metrics

The purpose of BCM KPI's are to monitor and measure the performance of Business Continuity programme based on the references obtained through achievement of processes or goals. These indicators are used to help organization evaluate its progress and / or performance (in terms of efficiency, effectiveness, robustness, and so on) of its BCM processes while pursuing short term, medium term and / or long-term goals / plans.

Depending on the size, complexity, maturity and dispersity of the organization there are numerous indicators that could be defined to control and measure the performance of a BC programme. A well-managed KPI dashboard gives the senior management information on how BCM program is managed across the organization and what corrective actions should be implemented.

Indicatively some of the metrics that can be included in such dashboard are:

1. Senior management support: Senior management promotes continual improvement of the program by:
    - Conducting management reviews
    - Requiring regular programme audits
    - Confirming that employees are continuously trained
    - Validating that test are being conducted regularly
    - Reviewing test results for successes and opportunities
    - Validating that the program is regularly updated

2. Business Impact Analysis: A Business Impact Analysis is conducted at regularly planned intervals for business units and associated activities that support the organization's products and services. The outcome (report) should be reviewed and signed off by the senior management. An example of a KPI related to BIA may be the number of Department-Specific Business Impact Analyses Completed/Updated Compared to Total Expected (organized by business unit)
3. Risk Assessment process: The risk assessment process systematically identifies, analyzes, and evaluates the risk of disruptive incidents to the organization on a regular basis, at least annually. The outcome (report) should be also reviewed and signed off by the senior management.
4. Risks identified through the Risk Assessment process: Based on their impact and criticality should be assigned to specific units/persons. Mitigation plans with specific timelines should be prepared and monitored. The dashboard needs to provide the number of risks identified, mitigated risks and residual risks those needs action.
5. BC management program training & awareness: Training is multi-tiered and addresses employees, recovery team leaders and members, the crisis management team, and senior management and generally all people involved in the BC programme. The following exhibits the KPI of target vs achieved.
    a. Number of BCM awareness session
    b. Number of BCM Tool training (if applicable)
    c. Number of First Aid & Health Training
    d. Number of Media and communication training
6. Business Continuity Plans: The plans address the recovery procedures and arrangements to secure the operational resilience of the organization in all levels. Therefore, they need to be updated in the agreed regular intervals to ensure that their content is valid and accurate. The introduction of a KPI that

measures whether the BCPs are updated and approved in a timely manner is critical to the resilience of the organization.

7. BCM Exercising: The BCM exercise is one of the important activities that verifies the readiness of the BCM program across an organization. The BCM exercise has to be set with certain objectives as per the readiness plans. The BCM exercising KPI measures the success of the exercise and corrective steps to be taken to mitigate the failures. The dashboard has to provide number of business units, total functions, those business units tested success or failed against objectives such as RTO and RPO. It is important to depict possible variances that may exist between the recovery requirements identified in the BIAs and the ones actually achieved during the BC exercises. In this way corrective actions and plans should be implemented to eliminate these possible variations
8. Applications / System Recovery Tests: The testing of the applications and/or systems supporting the recovery of the business units and consequently of the organization is critical. Their recovery objectives (RTO & RPO) should be measured and evaluated against the ones that have been identified in the BIA process. Any variation may severely impact the recovery chain of the organization and should be analyzed to identify the necessary corrective actions
9. Alternate work strategies: Business units follow an approved mix of alternate work strategies (e.g., work from home, from another company facility, or at a third-party site) established by the business continuity management unit that are based on the recovery time objectives derived from the BIA. The dashboard should record these strategies per each unit of the organization along with the agreed recovery requirements and their readiness
10. Audits Findings: Auditing conducted both internally or externally is a very useful tool that measures the performance and maturity of the BC programme. The audits of the BC programme are usually conducted against international industry standards (e.g., ISO 22301, ISO 27001, etc.) and their

findings and recommendation are considered as important metrics for the quality and efficiency of the BC programme

11. Suppliers / Vendors Business Continuity Assessments: Since the role of suppliers / vendors is critical to any recovery, it is important that regular assessment should be made for their business continuity capability. In large and complex organizations, the number of these vendors / suppliers may be high. Therefore, it is recommended that such assessments should be made in the ones categorized as critical or important through the BIA process

The aforementioned metrics are relatively simplistic in their design, but they can require a significant amount of effort to be reported against and meet the guidelines for quality metrics. Organizations may not have the processes or maintain documentation necessary to develop and report this level of detail. However, once initially developed, quality metrics should provide an ongoing method for communicating performance, progress and escalating issues that answer executive questions about program performance and recoverability.

The following tables depict some indicative simplistic metrics dashboard for measuring the performance of a BC programme.

| Criticality | Business Unit A | | | | |
|---|---|---|---|---|---|
| | Process | BIA Updated per agreed timeline | Recovery Plan Updated per agreed timeline | RA Updated per agreed timeline | Tested per agreed timeline |
| High | Cash Collection | YES | YES | YES | YES |
| Medium | Accounts Payable | YES | NO | YES | NO |
| High | Payroll | NO | NO | NO | NO |

| Business Unit | Type of Tests | | | | |
|---|---|---|---|---|---|
| | Work Area Recovery Test | Notification Call Tree Test | DR Test | VPN Test (WAH Users) | Other Test |
| Finance Administration | YES | YES | NO | NO | NO |

| Business Unit | Type of Tests | | | | |
|---|---|---|---|---|---|
| | Work Area Recovery Test | Notification Call Tree Test | DR Test | VPN Test (WAH Users) | Other Test |
| Human Resources | NO | YES | NO | YES | NO |
| Marketing | YES | YES | NO | NO | NO |

| Criticality | Application / System | RTO per BIA | RTO per recent test | GAP Identified |
|---|---|---|---|---|
| **High** | **Application 1** | 4 Hours | 8 Hours | + 4 Hours |
| **Medium** | **Application 2** | 12 Hours | 11 Hours | -1 Hour |
| **High** | **Application 3** | 4 Hours | 4 Hours | 0 Hours |

**Tables 14.1:** BC Programme Indicative Metrics Dashboard

# Chapter 15

# Conclusion

The guidelines presented in the research are applicable in any organization independently of size, industry, market and operational / cultural environment. Based on the feedback received from the BCM practitioners that have responded to the questionnaires and participated in the interviews, it was made clear that such approach is required to further enhance and evolve the BCM methodology.

Although there is an extensive and detailed literature review for the theoretical framework of BCM lifecycle, there is also a critical gap in recording the practical experience and knowledge received from the implementation of BCM programmes in organizations belonging to a wide spectrum of different industries and operational models. This has been made very clear, when I have approached the different knowledge bodies related to BCM, asking information, surveys conducted or resources presenting the practical aspect of BCM programme implementation. Moreover, while reviewing the relevant literature, I came across with fragmented and not integrated evidence of practical knowledge and guidelines provided by experienced practitioners.

On the contrary, there are numerous templates, questionnaires and forms produced by almost everyone in the web addressing different aspects of BCM methodology lacking the essential bond of practical approach, methodology, deliverables and interdependencies.

Such approach has resulted in poor understanding and great confusion among decision makers related to BCM lifecycle and deliverables and its relation with other disciplines resulting often in an inadequate BCM programme implementation. BCM practitioners find themselves very often trying to educate and alter a false perception

created among critical stakeholders and decision makers while implementing a BCM programme.

Lack of such common understanding among stakeholders often results in inadequate programme implementation and consequently failure to apply the appropriate recovery solutions. The absence of those solutions may lead to major losses in terms of revenues, brand image or market share and sometimes eventually to organization's closure. The following picture depicts eloquently the organization's response depending on their level of BCM programme.

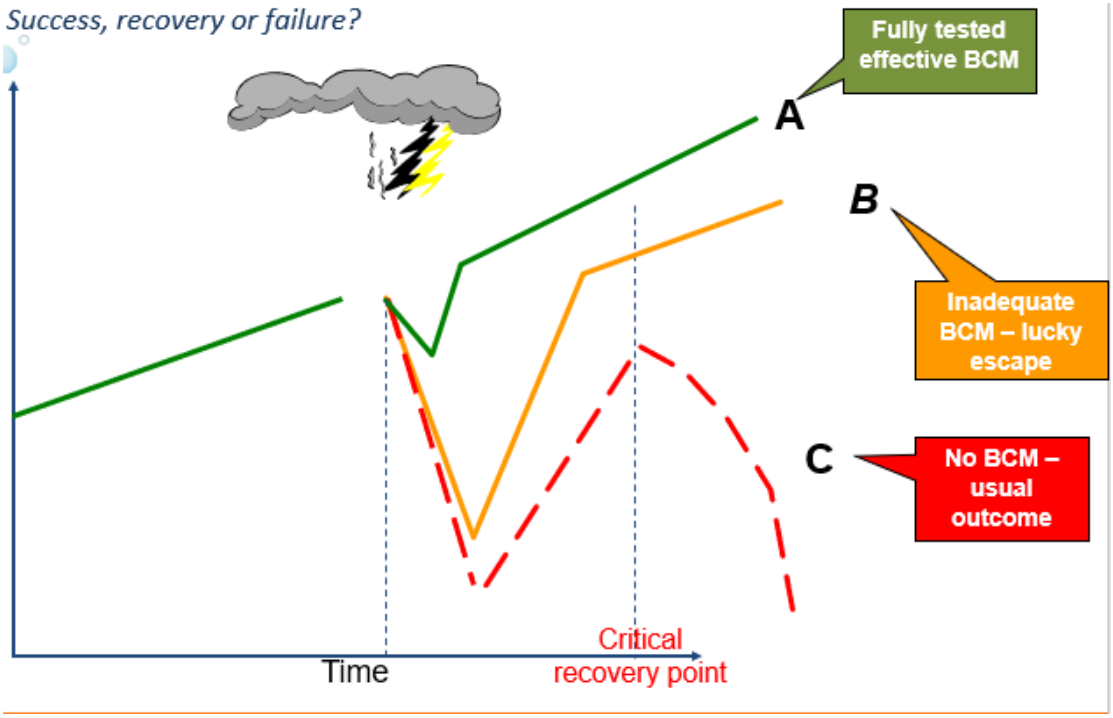



Figure 15.1: Organizations' response depending on level of BCM programme

The outcome of this research and the respective deliverables will greatly assist in recording a structured and consecutive approach of implementing BCM programmes, proposing the integration of BCM organizational structure within an organization and provide the tools, templates, methodology for a holistic approach.

The material provided, the analysis made and the different interdependencies between the phases but also between the different requirements within the same phases will greatly assist in the comprehension of the structural and gradual process

that needs to be followed to reach a desired level of operational resilience that may be different in each organization depending on its strategy.

Organizations' senior management and decision makers may now have the capability of reviewing the content of BCM methodology, the related phases and deliverables to evaluate the best approach of developing a structured and gradual methodology that will help their organization to build their operational resiliency. In this way both BCM practitioners and requestors / decision makers may beneficiate from sharing a common understanding of BCM methodology and outcomes.

By addressing the identified and presented challenges of this research, BCM practitioners may educate all involved stakeholders, including the less experienced BCM practitioners, for the effort, time and commitment required for such an effort and clearly differentiate and outline the relation and boundaries of BCM with other disciplines such as Information Security and Enterprise Risk Management.

Hence, the research has focused on providing the guidance, material, justification and detailed analysis necessary to ensure the development, deployment and management of a fully operational BCM programme that will assist an organization to manage effectively a disaster and guarantee its successful recovery. In this way apart from displaying and explaining on how an organization can beneficiate from such implementation it also assists in developing and building a common ground and understanding among BCM practitioners and decision makers on how to apply a holistic and universal methodology of implementation.

A fully integrated and comprehensive approach that has presented in this research will secure the fulfillment of the **key objectives** of an effective BCM programme that are:

- **Ensure the safety** of staff;
- **Maximize the defence** of the organization's reputation and brand image;
- **Minimize the impact** of business continuity events (including crises) on customers/clients;
- **Limit/prevent impact** beyond the organization;

- **Demonstrate effective and efficient governance** to the media, markets and stakeholders;
- **Protect the Organization ‘s assets**;
- **Meet insurance, legal and regulatory requirements**; and
- **Create a resilience framework adaptable** to any kind of crises and negatives events

It is highly recommended that this effort should be further developed and enhanced to integrate and embrace various adaptations and customizations that have been implemented during the course of years, because BCM is a journey that worth the price.

# Annexes

## Annex A

### BCM Programme Questionnaire

The attached document includes the questionnaire that was distributed to the BCM practitioners. The questionnaire covered the theoretical framework of the BCM lifecycle.

BCM Programme Questionnaire.docx

## Annex B

### BC Policy

The attached document is an indicative sample BC policy that provides details for the scope of BC programme and its governance within an organization.

Business Continuity Policy_Sample.docx

## Annex C

### BIA Questionnaire

The attached document is an indicative simplified BIA questionnaire that may be used for the collection of data in the framework of the BIA phase.

BIA Questionnaire Sample.doc

# Annex D

## RA Questionnaire

The attached document is an indicative RA questionnaire that addresses issues related to Facility Management, Physical Security and Administration.

Risk Assessment Questionnaire.xlsx

# Annex E

## BC Strategy Templates

The attached documents are indicative templates to be used for the collection of data for the development of the relevant BC Strategies for both processes/activities and systems/applications.

Activity Recovery Strategy Template.xl

Systems Recovery Strategy Template.d

# Annex F

## Pandemic Plan Template

The attached document includes detailed information related to the management of a pandemic. Depending on the structure and complexity of the organization, these activities can be assigned to specific functional units.

Pandemic Plan Template.docx

# Annex G

## Business Continuity Plan Template

The attached document includes a Business Continuity Plan template addressing strategic, tactical and operational requirements of an organization.

Business Continuity Plan Template.DOCX

# Annex H

## BCM Test Reports Templates

The attached documents include indicative test reports templates for different types of exercises conducted.

Notification Call Tree Test Report Template

Notification Call Tree Test template.d

Site Link Failover Activity Report Template

Site A Link Failover
Activity Report Temp

# References

Adams, C. A., & Larrinaga, C. (2019). Progress: engaging with organisations in pursuit of improved sustainability accounting and performance. Accounting, Auditing & Accountability Journal.

Adhikary, R. W. (2019). Globalization, Governance and Teach for Bangladesh: Understanding social enterprises in education policy. Unpublished PhD thesis, University of Queensland.

Agyemang, G., & Broadbent, J. (2015). Management control systems and research management in universities: An empirical and conceptual exploration. Accounting, Auditing & Accountability Journal.

Alexander, Alberto 'A Methodology for Developing a Business Continuity Strategy' Continuity Central, 2016

Alexander, Alberto 'Operations Resumption Planning: A Managerial Approach' Continuity Central, 201

Alexander, Alberto 'Planning and Managing Exercises for Business Continuity Management Arrangements' Continuity Central, 2016

Alexander, Alberto. "A Methodology for Business Impact Analysis: The BS 25999-2:2007 Approach" The Business Continuity Journal, Volume Three, Issue Four, 2009 UK

Annells M. (2016). Hermeneutic phenomenology: Philosophical perspectives and current use in nursing research. Journal of Advanced Nursing, 23, 705–713 2.

Anosike, P., Ehrich, L., & Ahmed, P.,(2012). "Phenomenology as a method for exploring management practice". International Journal of Management Practice

Aronson, B., & Laughter, J. (2016). The theory and practice of culturally relevant education: A synthesis of research across content areas. Review of Educational Research, 86(1), 163-206.

Attia, M., & Edge, J. (2017). Be (com) ing a reflexive researcher: A developmental approach to research methodology. Open Review of Educational Research, 4(1), 33-45.

BCI The BCI Good Practice Guidelines 2018

Beck CT (1992) The Lived Experience of Postpartum Depression: A Phenomenological Study.

Berg M, Dahlberg K (1998) A phenomenological study of women's experiences of complicated
childbirth. Midwifery 14: 23–9

Boaz, A., Hanney, S., Borst, R., O'Shea, A., & Kok, M. (2018). How to engage stakeholders in research: design principles to support improvement. Health research policy and systems, 16(1), 1-9.

Boylorn, R. M. (2008), 'Lived Experience', in Given, L. M. (ed.) The Sage encyclopedia of qualitative research methods, Vol. 2, Thousand Oaks: Sage

Brian E. Neubauer, Catherine T. Witkop and Lara Varpio How phenomenology can help us learn from the experiences of others. Perspect Med Educ. 2019 Apr

Briken, K., & Taylor, P. (2018). Fulfilling the 'British way': beyond constrained choice—Amazon workers' lived experiences of workfare. Industrial Relations Journal, 49(5-6), 438-458

BSI BS2599-1:2006 Business Continuity Management. Code of Practice

BSI BS2599-2:2007 Specification for Business Continuity Management

Charmaz, K. (2007). The Sage handbook of grounded theory. London: Sage Publications.

Charmaz, K. (2007). The Sage handbook of grounded theory. London: Sage Publications.

Christensen, L.B., Johnson,R.B &Turner,L.A (2020). Research methods, design, and analysis
(11th ed.) Boston.MA: Allyn & Bacon

Christie, M., Carey, M., Robertson, A., & Grainger, P. (2015). Putting transformative learning theory into practice. Australian journal of adult learning, 55(1), 9-30

Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodriguez-López, J. E. (2021). Sustainability and Resilience Organizational Capabilities to Enhance Business Continuity Management: A Literature Review. Sustainability, 13(15), 8196.

Creswell, J. W. (2014). Research design: Qualitative, quantitative,and mixed methods approaches (4th ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. W. (2013). Qualitative inquiry & research design: Choosing among five approaches. Los Angeles: SAGE Publications

Cristina Lafont (2015) Transcendental versus Hermeneutic Phenomenology in Being and Time

Crook, M., Short, D., & South, N. (2018). Ecocide, genocide, capitalism and colonialism: Consequences for indigenous peoples and glocal ecosystems environments. Theoretical Criminology, 22(3), 298-317.

Cyzewski, Ed. Creating Space: The Case for Everyday Creativity. Penguin 2012, San Francisco

Daoust, L., & Malsch, B. (2019). How ex-auditors remember their past: The transformation of audit experience into cultural memory. Accounting, Organizations and Society, 77, 101050.

Davison, L.T (2014) Phenomenological research using a staged multi-design methodology. International Journal of business, humanities, and technology.vol4 No 2

Denise Faertes, Reliability of Supply Chains and Business Continuity Management Open Access Procedia Computer Science, Volume 55, 2015, pp. 1400-1409

Donetto, S., Pierri, P., Tsianakas, V., & Robert, G. (2015). Experience-based co-design and healthcare improvement: realizing participatory design in the public sector. The Design Journal, 18(2), 227-248.

Ellitan, L., &Anatan, L. (2019). Achieving business continuity in Industrial 4.0 and Society 5.0. International Journal of Trend in Scientific Research and Development, 4(2).

Errasti-Ibarrondo, B., Jordán, J. A., Díez-Del-Corral, M. P., &Arantzamendi, M. (2018). Conducting phenomenological research: Rationalizing the methods and rigour of the phenomenology of practice. Journal of advanced nursing, 74(7), 1723-1734.

Esmail, L., Moore, E., & Rein, A. (2015). Evaluating patient and stakeholder engagement in research: moving from theory to practice. Journal of comparative effectiveness research, 4(2), 133-145.

Euene Tucker, Business Continuity from Preparedness to Recovery, 2015, pp. 129-159

Eugene Tucker, Mitigation and Business Continuity Strategy, Business Continuity from Preparedness to Recovery, 2015, pp. 107-128

Fischbacher-Smith, D. (2017) When organisational effectiveness fails: business continuity management and the paradox of performance. Journal of Organizational Effectiveness: People and Performance, 4(1), pp. 89- 107.

Flynn, Dennis. Delivering Successful Business Continuity Management Exercises Crisis Solutions, London, 2008.

Fullick, Alex Business Impact Analysis. Stone Road Press, Ontario, 2013

Gibb Forbes, Buchanan Steven A framework for business continuity management, International Journal of Information Management 26 (2006) p.128-141

Gill, M. J. (2014) 'The Possibilities of Phenomenology for Organizational Research', Organizational Research Methods

Giorgi, A. (2015). Phenomenology and psychological research. Pittsburgh, PA: Duquesne
University Press.

GM Heng, Testing & Exercising Your Business Continuity Plan

Graham, Julia. Kaye, David. A Risk Management Approach to Business Continuity. Rothstein Associates, Inc. Connecticut, 2006

Harvey, G., & Kitson, A. (2015). Implementing evidence-based practice in healthcare. Taylor & Francis.

Heppner, P. P., Kivlighan, D. M., & Wampold, B. E. (1999). Research design in counseling (2nd ed.). Belmont, CA: Wadsworth.

Heppner, P. P., Kivlighan, D. M., & Wampold, B. E. (1999). Research design in counseling (2nd ed.). Belmont, CA: Wadsworth.

Hiles, Andrew. Business Continuity: Best Practices. Rothstein Associates Inc, Connecticut, 2004

Hiles, Andrew. The definitive Handbook of Business Continuity Management. Third Edition. Wiley, 2011, London.

Humphrey, C. (2014). Qualitative research–mixed emotions. Qualitative Research in Accounting & Management.

ISO 22301:2019 Societal Security-Business Continuity Management Systems-Requirements

ISO 22317:2015 Business continuity management systems — Guidelines for business impact analysis (BIA)

Krell, E. (2006). Business Continuity Management. NY: American Institute of Certified Public

Lehman, C., Annisette, M., & Agyemang, G. (2016). Immigration and neoliberalism: three cases and counter accounts. Accounting, Auditing & Accountability Journal.

Luke, A. (2018). Regrounding critical literacy: Representation, facts and reality. In Theoretical models and processes of literacy (pp. 349-361). Routledge.

Lundqvist A, Nilstun T and Dykes A (2002) Both Empowered and Powerless: Mother's Experiences of Professional Care When Their Newborn Dies. Birth 29(3): 192–9

Mackey, A., & Bassendowski, S. (2017). The history of evidence-based practice in nursing education and practice. Journal of Professional Nursing, 33(1), 51-55

Michalko, Michael. Creative Thinking: Putting your Imagination to Work, 2011. Mc Graw, N.Y.

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. European journal of general practice, 24(1), 9-18.

Netolicky, D. M. (2020). School leadership during a pandemic: navigating tensions. Journal of Professional Capital and Community, 5(3/4), 391-395.

Neubauer, B.E., Witkop, C.T. & Varpio, L. How phenomenology can help us learn from the experiences of others. Perspect Med Educ 8, 90–97 (2019).

Ng M, Sinclair M (2002) Women's experience of planned home birth: a phenomenological study. RCM Midwives Journal 5(2): 56–9

Nursing Research 41(3): 166–70 Beck CT (1994) Phenomenology: its use in nursing research.
International Journal of Nursing Studies 31(6): 499–510

Osborne, S. P., Radnor, Z., & Strokosch, K. (2016). Co-production and the co-creation of value in public services: a suitable case for treatment?. Public management review, 18(5), 639-653.

Paton, D. & Jackson, D., 2002. Developing disaster management capability: an assessment centre approach. Disaster Prevention and Management, 11(2), pp. 115 - 122.

Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice (4th ed.). SAGE Publications.

Plant, K., Barac, K., & Sarens, G. (2019). Preparing work-ready graduates–skills development lessons learnt from internal audit practice. Journal of Accounting Education, 48, 33-47

PMI PMBOK® Guide – Sixth Edition

Porter, L. (2016). Unlearning the colonial cultures of planning. Routledge.

Priti, Sikdar Practitioner’s Guide to Business Impact Analysis, CRC Press, New York, 2017

Ranse, Jamie; Arbon, Paul; Cusack, Lynette; Shaban, Ramon Z; Nicholls, Daniel. Obtaining individual narratives and moving to an intersubjective lived-experience description: a way of doing phenomenology. Qualitative Research (QUAL RES), Dec2020

Robinson A., (2016). Phenomenology. In Cluett ER, Bluff R eds. Principles and practice of midwifery research. Churchill Livingstone Elsevier, Edinburgh: 187–200

S. Ali Torabi, Ramin Giahi, Navid Sahebjamnia An enhanced risk assessment framework for business continuity management systems Safety Science, Volume 89, 2016, pp. 201-218

Smith, J. A., Flowers, P., & Larkin, M. (2009). Interpretative phenomenological analysis: Theory, method and research. Sage.

Stephen Kempster. Leadership learning through lived experience: A process of apprenticeship? Journal of Management & Organization , Volume 12 , Issue 1 , June 2006

Strauss, A. C. & Corbin, J. (2006). Basics of Qualitative Research: Second Edition: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks, CA: Sage Publications

Strauss, A. C. & Corbin, J. (2006). Basics of Qualitative Research: Second Edition: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks, CA: Sage Publications.

Susan Snedaker, Chris Rima, Business Continuity and Disaster Recovery in Financial Services Business Continuity and Disaster Recovery Planning for IT Professionals, 2014

TA Schwandt, H Burgon. Evaluation and the study of lived experience. Handbook of evaluation: Policies

Taylor, C., & Charles, T. (1985). Philosophical papers: Volume 2, philosophy and the human sciences (Vol. 2). Cambridge University Press.

Taylor, L., & Soni, A. (2017). Preventing radicalisation: a systematic review of literature considering the lived experiences of the UK's Prevent strategy in educational settings. Pastoral Care in Education, 35(4), 241-252.

Thornburg P (2002) "Waiting" experienced by women hospitalized during the antepartum period. American Journal of Maternal Child Nursing 27(4): 245–8

Timms Paul, Business continuity and disaster recovery – advice for best practice, Network Security Nov. 2018 p 13-14

Trebilcock, P., 2010. Case Study: Embedding BCM into the culture. The Business Continuity Journal, 4(1), pp. 47 - 54

van Manen, M. (1990). Researching lived experience: Human science for an action sensitive pedagogy. State University of New York Press

Van Manen, M. (2011). Researching lived experience: Human science for an action sensitive pedagogy (2nd ed.). Canada: The Althouse Press

von Eckartsberg, R. (1998). Existential-phenomenological research. In R. Valle (Ed.), Phenomenological inquiry in psychology: Existential and transpersonal dimensions (pp. 21–61). Plenum Press

Warthhall, M. A. (2006). Existential phenomenology. In H. L. Dreyfus, & Wrathall, M. A. (Eds.), A companion to phenomenology and existentialism (pp. 229–239). Oxford: Blackwell Publishing Ltd

Warthhall, M. A. (2016). Existential phenomenology. In H. L. Dreyfus, & Wrathall, M. A. (Eds.), A companion to phenomenology and existentialism (pp. 229–239). Oxford: Blackwell Publishing Ltd.

Waseem, D., Biggemann, S., & Garry, T. (2018). Value co-creation: The role of actor competence. Industrial Marketing Management, 70, 5-12

Watson, V. (2014). Co-production and collaboration in planning–The difference. Planning Theory & Practice, 15(1), 62-76.

Watters, J., 2010. The Business Continuity Management Desk Reference: Guide to Business Continuity Planning, Crisis Management & IT Disaster Recovery, USA: Leverage Publishing.

Whelan, S., & Wohlfeil, M. (2006). Communicating brands through engagement with 'lived'experiences. Journal of Brand Management, 13(4), 313-329.

Wilson, H., & Hutchinson, S. (1991). Triangulation of qualitative methods: Heideggerian hermeneutics and grounded theory. Qualitative Health Research, 1, 263-276.

Wilson, H.S., & Hutchinson, S.A. (2019). Triangulation of methods: Heideggerian hermeneutics and grounded theory. Qualitative Health Research, 1, 263-276