St. Cloud State University
theRepository at St. Cloud State

Culminating Projects in Information Assurance Department of Information Systems

5-2016

Business Continuity Management: A Holistic Framework for Implementation

Andrea Patricia Sanchez Dominguez
apsanchez@stcloudstate.edu

Business Continuity Management: A Holistic Framework for Implementation

by

Andrea Patricia Sánchez Domínguez

A Starred Paper

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science in Information Assurance

May, 2016

Starred Paper Committee
Dr. Susantha Herath, Chairperson
Dr. Dennis Guster
Dr. Nimantha Manamperi

ABSTRACT

In the last few years, different events have made organizations aware of the importance of Business Continuity Management (BCM). When first developed, BCM implementation used a traditional approach. Academically, some authors have provided frameworks for BCM implementation. However, these frameworks do not contemplate all the dimensions necessary for a holistic BCM implementation. Furthermore, globally organizations have made efforts to standardize the implementation process which resulted in the standard ISO 22301. However, standards provide only what is required for an implementation and not how to achieve this. This paper introduces the reader to BCM, the importance of BCM, and its evolution. Additionally, proposes a guide for the implementation of a holistic framework for BCM. This study applies a qualitative approach. As part of the research, a case study was performed. To gather the information, interviews were conducted. The purpose of the case study is to evaluate the BCM current state in a Latin American financial institution. Finally, an analysis of the BCM legal framework in Panama is provided.

Keywords: Business Continuity Management (BCM), resilience, holistic, implementation, frameworks, standards

ACKNOWLEDGEMENTS

Gracias por Tu presencia, gracias por Tu amor

Por haberme dado la razón de seguir

Gracias por amarme así…

I want to thank my family (my mom, my dad, and sister), especially my mother who supported me and always believe in me. Thank you to all my friends and relatives in Panama who kept sending me messages and different ways of support since my day one in SCSU. Thank you to my relatives and friends in the USA who became my family during my stay here. Thank you to my advisor Dr. Susantha Herath who guided me and helped me since I was accepted into the program. And finally, I want to thank all the people who challenged me, who believed in me, and who changed the way I see the world.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Chapter I

INTRODUCTION

1.1 Introduction

Organizations around the world are becoming more aware of the importance of Business Continuity Management (BCM). Catastrophic natural disasters and malicious activities have shown how vulnerable and unprotected we are. Many of these events are moving organizations to understand and to develop a BCM implementation with a holistic approach. Organizations know that sometimes events cannot be avoided. However, it is possible to be prepared, minimize the impact, and restore the operations in a minimum time. This e-business era requires resilience organizations with high availability and performance.

This study aims at analyzing mainly the ISO 22301 standard and other different frameworks and methodologies for the implementation of BCM, propose a guide for the implementation of a holistic framework, and present a case study to evaluate drawbacks and gaps of the BCM in a financial institution.

1.2 Problem Statement

Many organizations do not follow a framework with a holistic approach to implement BCM. It leads to business interruptions, financial and reputational losses, inability to recover from a disaster, and, in the worst case scenario, human losses.

1.3 Nature and Significance of the Problem

Business Continuity Management is not a new topic; however, in the last few years, the importance of business continuity has increased significantly. Making it necessary to know a holistic framework to implement BCM successfully. New regulations, standards, availability demands, and organizational requirements to counter the effects of crises and interruptions have made the implementation of BCM crucial.

1.4 Objective of the Study

The objective of this study is to develop and to propose a guide to perform an implementation of a holistic BCM mainly based on the standard ISO 22301 and other frameworks and methodologies related to BCM. Moreover, the study presented the results of a case study to analyze the implementation of a BCM and its current state. Finally, an analysis of the BCM legal framework in Panama is also presented.

1.5 Study Questions

1. How the implementation of a BCM holistic framework can be performed?
2. Which are the activities that should be performed in order to get a holistic framework implementation?
3. Do external factors as a legal framework can affect a holistic BCM implementation?

1.6 Definition of Terms

BC: Business continuity

BCM: Business continuity management

BCMS: Business continuity management system

BIA: Business impact analysis

COBIT: Control objectives for information and related technology

ISACA: Information systems audit and control association

MTPD: Maximum tolerable period of disruption

RA: Risk analysis

RPO: Recovery point objective

RTO: Recovery time objective

1.7 Summary

Business Continuity Management is the key to business resilience today. However, to guarantee success, it is necessary to go through a holistic framework. The integration of different dimensions in the BCM implementation is critical. Today, some organizations implement BCM without focusing on the integration of important aspects such as complete top management involvement. This study provides a guide for the implementation of a holistic BCMS. This guide is mainly based on the international standard ISO 22301, and other frameworks and methodologies. Moreover the study provides the results of a case study where a BCM was evaluated and, finally, an analysis of the BCM legal framework in Panama.

Chapter II

BACKGROUND AND REVIEW OF LITERATURE

2.1 Introduction

Business Continuity Management has been evolving especially in the last years. Some authors point to the late 70s as the beginning of BCM, when organizations started storing their backups in alternate sites. Important milestones have been used to determinate different phases in BCM evolution. While the beginning of BCM is intrinsically related to Disaster Recover, today BCM is more than that. It is a continuous process which involves the preparation of an organization to be able to restore and continue operations after a disaster. To accomplish this, an evaluation of the organizational context and involvement of the whole organization is necessary. This process has to be seen as part of the organizational culture to achieve the expected results. Nowadays, standardization has emerged as a technique to accomplish BCM embeddedness in organizations. Furthermore, academically different frameworks have been presented to assist organizations in the implementation of BCM. Some are oriented to the technological dimension, while others focus on an information system strategy or risk approach.

2.2 Background Related to the Problem

According to Bird (2011), BCM can be defined as a:

> holistic management process that identifies potential threats to an organization and the impacts to the business operations that those threats – if realized – might cause, and which provides a framework for building organizational resilience with the capability for an effective response that

> safeguards the interests of its key stakeholders, reputation, brand, and value creating activities. (Page 10)

In a more limited definition, the Business Continuity Standard BSI 25999 stated: “Business Continuity is the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level” (as cited in Hiles, 2011, p. 31). Randeree, Maha and Narwani (2012) indicated that BCM is a management process of critical assets in a way that is possible to guarantee continuity of the critical process in an organization. In the same line as the BCI, Samson (2013) defined BCM as an integrated approach to help organizations to react against any unexpected event in an effective and timely manner. However, Samson goes further in his definition. He also stated that BCM is a continuous process. In addition, this process is a compound of a series of activities as part of the preparation for an unplanned event, anticipation, and mitigation of the impact of the undesired events, recovery tasks, and evaluation of learned lessons to improve BCM. Jedynak (2013) established, BCM as a “permanent and interactive” management process oriented to assure the continuity of critical process at any time. Jedynak stresses the importance of the preparation before, during and after an unplanned event. There is some controversy in authors’ definitions about the scope of BCM. The review of BCM literature shows how BCM scope has been changing through the years. Nowadays, BCM is a management process compound of different sub-process (identification of critical assets and threats, risk management, among others) that integrates all the organizational areas for disaster preparedness. It is a never ending process characterized by the continuous updating to guarantee business resilience. Finally, the central focus of BCM is the assurance of critical business process continuity.

2.3 Importance of Business Continuity Management

Randeree, Maha, and Narwani (2012) stated that the importance of BCM resides in three aspects: supply chain disruptions, customer demands amidst rising competition, and regulation and risk. In this new era of e-business, disruptions in business processes are not tolerable. Every day, customer demands are getting higher, and the only option to guarantee fulfillment of their demands is assuring business continuity. On the other hand, regulations (SOX, HIPPA, BASEL II, among others) are requiring greater integration, and involvement of companies in BCM while new potential risks arise into our lives. Cyberwar, espionage, hacking, and other new forms of terrorism are also affecting companies. These harmful and intentional events are also creating awareness of the importance of business continuity in organizations.

2.4 Evolution of Business Continuity Management

The first sparks in the route to develop BCM as a discipline appeared in the decades of the 1950s and 1960s. During this time, organizations began to be aware of critical information. This was reflected in the activities that they performed, such as store backups of their information in alternate sites (Randeree, Maha, & Narwani, 2012). Others experts agree that BCM has its beginning in the 1970s, when different changes took place in the IT field (Jedynak, 2013).

In the last 40 years, technology has evolved by leaps and bounds. Today, the world is living a new era of “e-business” where dependencies on technology are high. “Business Continuity” and “Always On” are terms that became more and more popular.

This has created an increased interest in BCM making it evolve. Unfortunately, in some cases natural or intentional disasters also made BCM evolve.

To understand how BCM has been changing, Herbane (2010) described four phases which cover the period 1970 to 2010:

2.4.1 Phase 1 - Emerging legislation phase

This phase (mid–1970s to the mid-1990s) is characterized by the appearance of acts that were created with a purpose different than continuity management, however, these initiatives were the beginning of the development of what we know today as BCM. Flood Disaster Act (1973) and US Foreign Corrupt Practices Act FCPA (1977) were the foundations for the introduction of Disaster Recovery Plan (DRP) and BCM in organizations. Later, in the 1980s the Office of Comptroller of Currency's Banking Circular BC-177 (1983) and the US Expedited Funds Availability Act (1989) appeared. Both of them were a more formal start for the disaster recovery and business continuity plans in US banks.

Finally, in the 1990s, the establishment of new regulations required stronger control for the protection of critical assets, incident response strategies, availability of critical processes, and contingency planning.

Some of the regulations that marked milestones in this phase were:

1. Office of Management and Budget Circular A-130 (1993)
2. Health Insurance Portability and Accountability HIPAA (1996)
3. Telecommunication Act (1996)
4. Executive Order 12656 (1998)
5. Gramm-Leach-Bliley Act (1999)

2.4.2 Phase 2 - Emerging standard phase

During this period ([the] mid-1990s to [early 2000s]), there was a predominant development and awareness of standards to guide the BCM process. Worldwide, different initiatives took place. In the beginning, BCM was just part of the standards, however, over the years it took a more important role. In 1996, the IT Governance Institute and ISACA presented a new framework called COBIT. COBIT's main objective was to link business goals with IT goals. In its first version, COBIT included an objective which stated the necessity to ensure continued services (Pasquini & Galie, 2013). In 1995, the National Fire Protection Association's (NFPA) presented the NFPA 1600 Recommended Practice for Disaster Management. This document was revised, and for the 2000 year edition it became a standard. It included a total program approach for disaster/emergency management and business continuity programs (McLaughlin, 2005).

Herbane (2010) highlighted that this period is different from the previous, especially because of two changes. First, the standards present in this phase appeared as part of the upgrade of earlier standards, and second, through the application of the ISO/IEC directives, local standards became international standards. Examples of this are ISO/IEC 17799 Information Security Management and ISO /IEC 20000 Information technology-service management. Both evolved from British standards. In these standards, Business Continuity had an important presence, however the focus of them was not only BCM. Finally, in

2000 new initiatives appeared in the United Kingdom: BS15000 and the Joint Service Publication 503 – Business Continuity Management (Herbane, 2010).

2.4.3 Phase 3 - The post-9/11 phase

One of the most dramatic events in the last few years was the 9/11 attacks. It completely changed the way people saw the world, and for Business Continuity it created a before and after (Rodgers, 2001). The attacks demonstrated how vulnerable we are, and in many cases the shortcomings in the execution of business continuity plans. Human losses, economic and psychological impact, and interruption of critical services were some of the main consequences of these attacks.

As a result of the impact of these events, the appearance of guidelines and the enactment of new regulations took place (2002-2005). Regulations were focused in some critical industries, including financial, public authorities, stock exchanges, and utilities. As with the increase of regulation, there was also a boom in the standardization of the business continuity process. Organizational resilience became an important concern, and people became more aware of BCM. It is reflected in the considerable number of legislation in different countries, such as China, Thailand, Pakistan, India, Australia, South Africa, among others (Herbane, 2010).

2.4.4. Phase 4 - Internationalization phase

This phase (2006-2010) is characterized by the desire of organizations to go beyond regulations. There is a new interest that goes beyond complying with the existing regulations, and finding new ways to acquire business resilience.

International standards arrived as a tool for organizations to satisfy regulatory requirements, while at the same time they are covering the minimum competitive criteria for BCM in the market (Herbane, 2010).

According to Herbane (2010), during this period two important processes allowed internationalization:

1. National standards became international standards
2. International organizations took a stronger role in leading this breakout.

The internationalization of standards was a new roadmap for organizations to achieve international certifications. One of the most popular standards that appeared during this period was BS 25999. It was published by the British Standard in 2006 (N.A., 2011). This standard helped organizations to start adopting a holistic BCM approach, and for many years it was an acceptable standard for BCM (Tamineedi, 2010).

2.5 Evolution of BCM in the last five years

The beginning of this period (2010-present) was characterized by the occurrence of natural disasters that struck and heavily affected some countries. The Earthquake and Tsunami in Japan (2011), and Hurricane Sandy in the US (2012) were three of the most devastating natural disasters during these years. In the case of Sandy, companies went through different difficulties, from the simplest to the most complex. They experienced failures in communications and networks, disruptions in supply chains, and even the inability to get the electricity system on. Organizations were not able to handle the storm effects, and after effects demonstrating the lack of an efficient BCM (Samson, 2013).On the other hand, new threats have appeared in cyberspace: cyberwar, phishing, credential theft, point-of-sale (POS) attacks, RAM scraper, among others. These threats may impact an organization’s finances and reputation, in other cases threats impact security and stability of nations.

The occurrence of these massive natural disasters and the appearance and increase of new cyber threats caused momentum for BCM. The term “resilience” got more and more implications among the business continuity experts, and a new standard came to supersede the BS 25999: ISO 22301 (Brennan & Mattice, 2014). In addition, to the new standard, new trends have also appeared as part of the strategies for business continuity. These emerging technologies are improving resilience, automating communication, increasing cost efficiency, and promising a decrease in recovery time and data loss. Some examples of these strategies are virtualization, cloud computing, mobile devices, and social networks (ISACA, 2012).

Today, it is not only the fact that organizations have to fulfill regulations, but the priority is to prevent disasters. Experts believe that the key for the success of a BCM is the implementation of a holistic framework, which is able to integrate all the areas of an organization. It is a complicated project, and it is important to understand that it is not only an IT responsibility. It is a joint effort that involves the whole organization.

2.6 Standardization of Business Continuity Management

As was explained, through the history of BCM few standards have been entirely dedicated to Business Continuity Management. Two of the best known are BS 25999 by the British Standards Institute and ISO 22301 by the International Standard Organization. It was released in 2012. ISO 22301 is the first international standard focused only on business continuity. This standard can be used regardless of size, region, and type of industry (Zawada, 2014).

According to Zawada (2014), this standard helps organizations to address three important issues: management engagement and organizational alignment, program scope, and project versus the program. ISO 22301 as a standard explained “what” an organization required to take into consideration for a BCM implementation. However, it does not explain the “how”. The different clauses of ISO 22301 are based on the model Plan – Do – Check- Act (PDCA), which allows organizations to go through an entire process of planning, reviews, and improvements (Young, 2015).

ISO 22301 (ISO 22301:2012) is compound of eleven (11) clauses:

1. Introduction
2. Scope
3. Normative References
4. Terms and Definitions
5. Context of the Organization
6. Leadership
7. Planning
8. Support
9. Operation
10. Performance Evaluation
11. Improvement

ISO 22301 is an answer to many BCM practitioners who were looking for a non-regional standard able to be used in any organization. It represents a change in traditional BCM. ISO 22301 also provides clauses to performance evaluation and improvement. These clauses help organizations to keep tracking, and close gaps that can be found during the testing and exercise process (Ee, 2014). As other ISO standards, ISO 22301 allows organizations to be certified by a third party, and to demonstrate to their clients that they are fulfilling a standard which is internationally accepted, in an attempt to guarantee the continuity of their critic services.

2.7 Literature Related to the Problem

According to Ee (2014), this era arrives with new threats making organizations be more and more aware of BCM. A Traditional approach to implement Business Continuity Management is now not enough. Furthermore, the traditional approach presents limitations to the organizations. Bajgoric (2014) indicated that the traditional approach usually focuses only in one aspect forgetting the different BCM dimensions. Ee (2014) stated that many organizations don’t reach business resilience. Some of the reasons are: organizations focus on past or just individual incidents, inadequate knowledges in how to conduct business impact analysis (BIA) / risk impact analysis (RIA), and use of “regional” standards for BCM application. Ee (2014) indicated that these problems can be faced through the implementation of a BCM based on the integration of relevant disciplines and using a standard approach. In this line, Zawada (2014) stated that ISO 22301 allows organizations to make a self-evaluation to determine if they are doing all the necessary actions to reach business resilience. According to Zawada (2014), the standard goes far away of the BCM planning phase. It includes an audit and corrective action sections. On the other hand, Zawada (2014) indicated that ISO 22301 as a standard only provides the “what” for a BCM, but not the “how”. This makes it necessary to adopt a framework to go into detail.

Bajgoric (2014) presented a systematic framework for the BCM implementation. This framework proposed the concept of an “always on” business. The model explained that today organizations are using continuous computing technologies to offer to their customers more availability and reliability. This framework divides the continuous computing technologies into three layers: server operating system, storage, backup and recovery technologies, and networking infrastructure. Jarvelainen (2013), argued that the traditional approach of only implementing disaster recovery techniques, and keeping backups of the information in an alternate site is not enough. Gibb and Buchannan (2006), defined a framework in terms of the phases of a project. Each phase of the framework provides inputs and outputs and emphasize in the critical activities necessary to reach the goals. The framework is a compound of nine phases, which highlight the key activities, inputs and outputs of each phase. On the other hand, Tammineedi (2010) explained the BCM’s activities critical for an organization based on a standard approach. These activities are divided into three important phases: before an event happens, during the event, and after the event happens (debrief).

Kadar (2015) introduced the concept of BCM risk index. Allowing business practitioners to measure and report the status of the BCM to top management, and align it to the organizational culture. Jarvelainen (2013) stated that different external drivers can promote the embeddedness of continuity practices in organizations. Additionally, standardization and regulations are promoting awareness in BCM. Randeree, Mahal, and Narwani (2012) stated that regulations and industry standards are forcing organizations to assure that their BCM implementations are accomplishing the maturity level required.

All these trends are making organization focus not only in the traditional approach, where disaster recovery was the key. Organizations are also focusing in the integration of different process and areas. Torabi, Rezaei, and Sahebjamnia (2014), stated the importance of understanding the organization, and its key products and processes for the implementation of a comprehensive BCM. In BCM, two processes are necessary to understand the organization: BIA and RIA. Torabi, Rezaei, and Sahebjamnia (2014), developed a framework for BIA which focuses on four main activities: identifying of key products, key products' breakdown structure, identifying of critical functions, and estimating the continuity parameters. Green (2014), established that measure "understanding the organization" is also an important part of a BCM implementation. It is relevant to demonstrate how the BCM is able to provide support and alignment to the organizational goals and strategies.

The papers mentioned, explain different frameworks based on a specific focus. However, these studies do not present a holistic approach with all the dimensions required in a BCM implementation. Today, business resilience depends completely in a holistic approach of BCM. International standards are a first guide for an organization to the implementation process. However, it is not enough.

2.8 Literature Related to the Methodology

Bailey (2015) pointed out that qualitative research is more common in today's studies especially in those related to management. A more flexible approach is becoming necessary to evaluate phenomenon or situations in complex organizations.

According to Kumar (2014), the qualitative approach allows researchers to explore focusing in description and narration of experiences, perceptions or feelings, making big samples not necessary. Furthermore, this approach supports researchers to explore in depth and gain insight of a specific circumstance. McCusker and Gunaydin (2015) stated that qualitative studies answer questions such as: “what”, “how” and “why”. In addition, these studies require a focus on the process of collecting data due to the fact that the interpretation of it is critical for presentation of results.

2.9 Summary

This chapter presented BCM definition from different authors’ perspective, why it is important and a compilation of some milestones that changed the way people perceive Business Continuity Management. It explained the evolution of BCM and some frameworks proposed in the last years. Furthermore, the chapter made a brief description of some standards related to BCM. The next chapter makes an overview of the methodology and techniques that are going to be used in this study.

Chapter III

METHODOLOGY

3.1 Introduction

Different approaches can be used to conduct a research study. According to what a researcher is interested in investigating, an approach is going to be suitable or not. This study was performed based on the qualitative approach. The study included the analysis of different frameworks and a case study performed through interviews as main tools for data collection. Furthermore, the study includes an analysis of the BCM legal framework in Panama.

3.2 Design of the Study

Amaratunga, Baldry, Sarshar, and Newton stated the “Qualitative research is conducted through an intense and/or prolonged contact with a field or life situation” (p.21). According to Maxwell (2013) qualitative approaches are suitable because allow researchers to re-design their studies while they are working. Sometimes, during the exploration of a situation, the researchers can find that a component of the study needs to be reconsidered and, it can change the development of the study. Furthermore, the data collection techniques, study questions, the developing of theories, among other components of the study are linked. If one of these changes or has to be restructured, the others also are going to be affected. Kaplan and Maxwell (2005) explained that in contrast with the quantitative approach, the qualitative approach is used when a researcher’s main objective is the analysis of a complete process or situation, how does it work, how does it interact with other subjects, which are its components, and the relations among them. Moreover, the qualitative approach allows the researcher to analyze the information gathered, and to explore experiences and perceptions (Kumar, 2014).

This study used a qualitative approach. The method was suitable for the study because allowed the researcher to explore deeply the process of development and implementation of a Business Continuity Management framework. Furthermore, this open and unstructured approach enabled the researcher to analyze the relation, importance, and influence of the different components of the BCM process. Finally, this approach provided different tools and techniques to go through the assessment of a BCM in an organization in order to discover flaws in the BCM implementation. This assessment provided the researcher with an insight of what is or is not taken into consideration for a BCM implementation, and how it can affect an organization.

This study was divided into two sections. The first section includes the analysis of the standard ISO 22301 and the review of other frameworks and methodologies for the development of a guide to perform an implementation of a holistic BCM.

The frameworks and methodologies evaluated were:

- Information technologies for business continuity: an implementation framework by Nijaz Bajgoric
- Business continuity management: a systemic framework for implementation by Nijaz Bajgoric
- A framework for business continuity management by Forbess Gibb
- A new framework for business impact analysis in business continuity management by S.A. Torabi

- Business Continuity Management: A Standard-Based Approach by Rama Tammineedi (Based on the standard BS 25999)
- Failure Mode Effects Analysis (FMEA)
- Hazard and Operability Study (HAZOP technique)

The second section includes the assessment of a Business Continuity Management System implemented in an organization (case study conducted in a Latin American financial institution) in order to find flaws in the system and, to prove the importance of a holistic implementation. Finally, this section also includes an analysis of the BCM legal framework in Panama and how the legal matter can affect the BCM holistic implementation.

3.3 Data Collection

A case study was used as the main technique for data collection. The case study was conducted in a Latin American financial entity. This kind of organization was selected due to the fact that is one of the strongest regulated in the region. The point of contact was personnel in charge of the BCM area. The case study was focused on understanding the current BCM state in the organization. As part of the case study, different interviews were performed to collect information.

To collect data the main tool used was the case study. According to Kumar (2015), one of the main advantages of this tool is that the researcher has the possibility of exploring a situation and gaining insight into the different components of it. Along with this tool, an interview schedule was used. The interview schedule is a prepared list of questions used in person-to-person interaction. It differs from the questionnaire that during the interview schedule the participant is interacting with the researcher. If the participant has concerns, the researcher will help the interviewee to understand better. In this study, the interaction was through skype technology due to the fact that the researcher was in the US and the interviewees were abroad. The method to collect the information was interviewing. The interviews were scheduled in advance.

3.4 Data Analysis

Kumar (2015) stated that there are three ways to process data in qualitative studies. This study consisted of identifying, writing, and quoting verbatim the main themes discovered as the option for processing the collected data. Furthermore, once the information was transcribed from the interviews, the researcher validated with the interviewee. The questions in the schedule interview were divided into different sections. According to the answers provided, the sections were evaluated. Each section received an overall score and, finally the researcher presented a general result. The results of each section were combined to produce the final result.

3.5 Hardware and Software Environment

This study did not involve any special hardware or software environment. As was mention before, the Skype technology was used to conduct the interviews. Furthermore, for the documentation, Microsoft Office suite was used.

3.6 Summary

This chapter explained the approach used to develop this research and why it was suitable for this study. Furthermore, it presented the different tools and techniques used during the development of this research. The approach used for the research was the qualitative approach. The method for collecting data was interviewing and the tools were a case study and interview schedule. The chapter also covered the process used for the data analysis. This approach, method, and tools allowed the researcher to explore the implementation of a BCM in an organization because it provided an open context to perform the research.

Chapter IV

GUIDE TO IMPLEMENT A HOLISTIC FRAMEWORK

4.1 Introduction

The Standard ISO 22301 was proposed in 2012 as a new way to implement The Business Contingency Management process regardless of the size, type or location of the organization. However, it is necessary to make a deep analysis of what the standard offers to the organizations and how it is possible to use it. This Chapter makes a journey through the Standard ISO 22301 providing a complete guide for those who want to implement it but also want to go beyond it. Each clause is described, their importance is stated, activities and methodologies are proposed and explained in order to develop the clause and, finally deliverables are presented as part of the outputs of each clause.

4.2 ISO 22301 Standard

The standard 22301 is based on the model PDCA. PDCA, also known as Deming Cycle, is the acronym of Plan Do Check Act Analysis Model. This model has its origins in the 1920s. However, it was in the 1950s when Edward Deming made some improvements to the model, and it became what we know today (Gupta, 2006). This model establishes that all the activities in a management process should be divided into Plan, Do, Check and Act categories. As the Business Continuity Management involves different process, this analysis model is suitable for it.

The ISO 22301 Standard (ISO 22301:2012) explains the model as follows:

Plan: phase related to the definition of the require activities necessary to align their current BCM status with the desired status.

Do: phase related to the operation of the BCM processes.

Check: phase related to the assessments of the different BCM activities and elements in order to verify their performance.

Act: phase related to the implementation of remedies to the nonconformities found during the assessments, follow-up of these actions, and continual enhancement of the system (p.vi).

4.3 Pre-Implementation of a BCM

Prior to the implementation of a BCM, it is important to achieve some milestones such as the establishment of a BCM structure and the evaluation of the current state of the organization. These two are key points as part of the preparation for the development of a holistic BCM. In addition, in order to avoid waste of time creating everything from scratch, it is vital to check what already exists.

4.3.1 Evaluation of the BCM current state

The performance of this stage involves the evaluation of what have been done, how it is working, what needs to be improved, and what needs to be implemented. An easy and effective way to address these questions is through interviews with the key members of the organization. The assessment can be performed using as a base the different sections of the standard ISO 22301: Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement (ISO 22301: 2012). Appendix B presents a questionnaire that can be used as base to perform a gap analysis.

4.3.2 Definition of the BCM structure

This structure can vary from one organization to another. However, there are some important teams or groups that should be present in every BCM structure. These teams are going to be related to specific tasks that will be performed before, during or after an incident. These stages are linked. If a team does not perform properly, and on time their tasks all the BCM cycle is going to be affected. The importance of creating a suitable BCM structure lies in the fact that this group of people is aware of how to keep working the BCMS. Without a well-defined structure, the organization won’t be able to handle properly any kind of incident.

Generally, a common BCM structure includes the following:

- Board of Directors: responsible for the decision-making process and approval of policies and other important documentation.
- Champion: responsible for influencing the board of directors to achieve the different goals of the BCMS and for obtaining the support from the different levels and areas of the organization.
- Contingency Team: responsible for all the administrative tasks including coordination of activities, development, performance, and improvement of the BCMS.
- Incident Response Team: responsible for coordinating all the activities that allow the organization to “anticipate, detect, and mitigate the effects of an unexpected event” (Whitman, Mattord, & Green, 2014).
- Business Continuity Team: responsible for all the activities that let the organization continue operations while other team control the situation (Whitman, Mattord, & Green, 2014).
- Disaster Recovery Team: responsible for all the activities to recover the core system and other critical applications.

- Other Organizational Units: involves personnel from different units as Human Resources, Legal, Audit, Risk which also play an important role in the implementation of BCM.

Due to the fact that every organization is completely different from each other, the time that they are going to take to implement their BCMS is also going to be different. However, it is possible to estimate how much percentage of time (of the whole project) is expected to be spent in each clause. In order to do that, the following criteria have to be evaluated: size and type of the organization, the complexity of the activities necessary to complete the clause, skills required to develop the activities, the impact of the activities in the organization, and the amount of people involved in the activities. Figure 4.1 shows an approximate percentage distribution of how the time could be divided during the implementation of the whole project. This estimation is based on the criteria previously specified. The detail of the calculation can be found in the Appendix A.

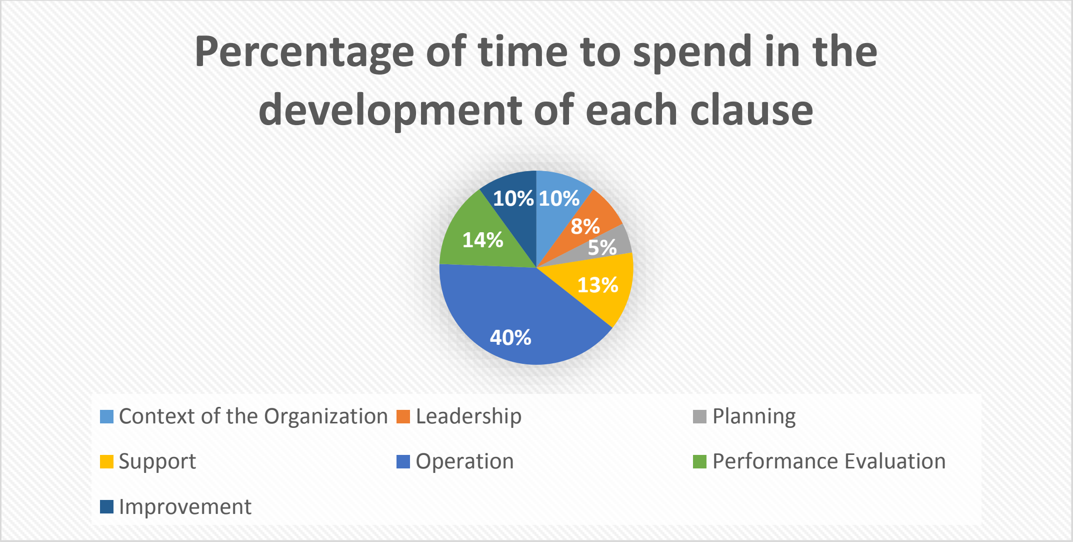


Figure 4. 1. Percentage distribution of the time in the implementation of the different ISO 22301 clauses.

To have a better understanding of the results in figure 4.1, the following sections are going to explain the clauses of the standard ISO 22301 (Clause 5 to 11), present the different activities that have to be performed and the deliverables the organization should have at the end of each clause.

4.4 Implementation of a BCM

The guide presented, for the implementation of a BCM, is mainly based on how to implement what is on the standard ISO 22301. However, as was stated previously it also included methodologies, techniques, and information about other frameworks that is not stated on the standard ISO 22301.

4.4.1 Clause 5 - Context of the Organization

To start the planning phase, it is important to have a good understanding of the organization. Wong and Shi (2015) focus on three important components: corporate analysis, threat and resilience assessment, and stakeholder and regulatory analysis.

4.4.1.1 Corporate analysis

It includes the identification of all the information that can give an overall idea of how the organization works. It should take into consideration the mission and vision of the company, strategic goals, project portfolio, services, products, partnerships, and external relationships. This information should be documented. If the organization does not have it, it would be a good practice to start on it.

4.4.1.2 Threat and resilience assessment

Once there is a clear idea of the organization, the next step is to understand how the organization perceives the risk. It is going to be necessary to review the criteria existent for risk tolerance and risk appetite. If it is not available this is the moment to discuss it.

4.4.1.3 Stakeholders and regulatory analysis

It includes the identification of the different stakeholders and regulations (or legal implications) that can apply to the organization regarding the continuity of their services and products.

Once there is an understanding of how the organization works and what is important to them, the next step is to align the BCMS with the business organizational strategy. This alignment is possible through the establishment of a BCM scope which includes every aspect important for the continuity of the organization. The scope can be divided into five sections: building (premises), equipment (including critical documentation), technology, human resources, and third parties. In addition, this scope should take into consideration regulations that can apply to the organization and relations with stakeholders that need to be covered. As it would be expected, the scope of the BCM will vary among organizations and also according to the risk appetite that the organization is willing to accept. A good practice, to achieve a scope that covers all that is really important, is linking the corporate analysis, stakeholders and regulatory analysis with the business strategy and business plan (short and long-term goals and plan to achieve them). This documentation can be used to perform the first scope draft. Later, when the BIA is performed, the scope can suffer changes. It is important to clarify that the scope is not static. It is actually dynamic and it can be changing according to the organization change or new regulations appear. At this point, in the BCMS development, the scope can be an initial idea which is going to be more mature once the BIA is performed.

Deliverables: BCM scope, risk scale.

4.4.2 Clause 6 - Leadership

As part of the result from the previous section, the organization should already have defined the BCM scope. The next step is to define actions that guarantee the commitment of the top management in the BCMS. It is important because, without a high level of commitment, it is not going to be possible to achieve the drivers to promote the BCMS along the organization. Once these actions have been defined, the next step is assess and measure the level of commitment of the top management with the BCMS. Evidence of the commitment can be the designation of dedicated resources for the BCMS (people, budget, technology), existence of documentation related to business continuity (BC policy), and an established organizational structure for the BCMS. The organization structure should be reviewed and updated it (in case a BCMS is already in place) or created it during the pre-implementation process in case it does not exist already. It is very important that the organizational structure should include a champion. This person is going to be the link between the top management and the contingency team. The champion is going to be in charge of the implementation of the BCMS and encouraging the BCM culture along the whole organization while guaranteeing the support from the top management. Following the establishment of the structure, it is necessary to develop a BC policy. It should be created by the contingency team. Once the policy has been created it should be transmitted to all the organization. Top management commitment can be perceived through the support of the performance of all the activities related to the operations of the BCMS, assessment of these activities, and improvements of them.

Deliverables: BCM structure with clear roles and responsibilities, BCM policy.

4.4.3 Clause 7 - Planning

Once the scope of the BCM has been established and there is a clear BCM structure is possible to continue with the BCM objectives. The BCM champion can be the person in charge of the definition of the different objectives. The objectives reflect the goals that the organization wants to achieve related to the performance of the different elements of the BCMS. Gibb and Buchannan (2006) supports that the objectives “should be specific, measurable, attainable, relevant, and time-based (i.e. SMART)” (p.131). These characteristics will help the organization to evaluate the degree of success in the accomplishment of the different goals. Once the objectives have been stated, the organization should evaluate the risks and threats that would affect the accomplishment of these goals. An option to start, the development of the objectives, is link the BCM scope, with actions that will allow the organization to cover the defined scope. The following is an example of a BCMS objective:

- Guaranteeing the continuity of the critical operations during an adverse event through the invocation and implementation of the business continuity strategies (technological strategies and alternate processes).

Deliverables: BCM objectives.

4.4.4 Clause 8 - Support

As was mentioned previously, the allocation of resources plays a crucial role in the development of the BCMS. Top management should assign the adequate resources to allow continuity of operations. These resources include dedicated budget, personnel, and technologies. In the case of the personnel, top management should ensure that the members of the different business contingency teams have the knowledge and skills to perform their tasks. Furthermore, all of the organization's members should be aware of the importance of the BCMS, how their job can impact it, and how to act in the case of a disruption.

This clause makes special mention about the enforcement of competence and awareness. It is important to state the difference between competence and awareness. Competence can be defined as the skills needed to perform a specific activity while awareness, according to the BSI Institute (2011) refers to "create understanding of basic BCM issues and limitations" (p.6). In order to guarantee the adequacy of the BCMS implementation and its constant improvement it is necessary the definition of minimum requirements of knowledge and skills of the people involved directly in the activities to support the BCMS. This information should be displayed on the jobs description. Furthermore, it is necessary to ensure their preparedness according to the requirements defined. This is possible through the design and execution of a competence program. Wong and Shi (2015) stated the importance of the application of a Training Needs Analysis (TNA). It will help the organization to know where their people are and where they need to focus on. Furthermore an awareness program also should be created to promote a BCM organizational culture. This program should be directed to all the organization to raise awareness of the importance of BCM and, to make the workers understand how their activities and attitude can impact the whole BCM.

Following competence and awareness, the clause mentions a third element to consider: communications. Creating a communication plan will help the organization to structure how to communicate the different messages during and after an incident. This plan should include at least what has to be communicated, when it has to be communicated, and to whom. On the other hand, another option for the communication management is outsource this activity. This option will help the organization, during the occurrence of an adverse event, to focus on the implementation of other activities such as the execution of business continuity strategies, recovery strategies, and in the process of return to the normal operations.

Finally, as part of the different activities to support and strengthen the BCMS, there should be implemented a documentation management process. Having a documentation management process allows the organization to keep control of the documentation of the BCM processes and to improve it in regular basis. A document management process includes a complete lifecycle of the overall documentation (creation, access, protection, retention, storage, and maintenance). This process should be aligned with the existent procedures for manage documentation in the organization.

Deliverables: Training Needs Analysis template, Competence and Awareness Program, Communication Plan, Policy and procedure for document management.

4.4.5 Clause 9 - Operation

It is not possible to highlight one phase as the most important. All the phases represent an important part of the overall system. However, this phase can be considered as one of the cornerstones of the whole project. This is because it covers some of the complex activities: Business impact analysis (BIA), Risk analysis (RA), Developing a Business Continuity Strategy, Establishing and Implementing Business Continuity Procedures, and Exercising and Testing the Business Continuity Procedures. It is important to mention that the Standard ISO 22301 does not indicate the order of performance of the BIA and RA. It establishes that the order will depend on the methodology used to perform the analysis. This guide suggests to perform first the BIA and then the RA.

4.4.5.1 Business Impact Analysis – BIA

Performing a BIA provides several benefits to the organization. The analysis offers a complete overview of the organization. It covers three main goals. First, identification of processes which, once stopped, will strongly affect the delivery of critical products and services impacting the organization. It is necessary to include their timescales indicating how long the organization can operate without these processes and when they should be recovered (MTPoD, RPO and, RTO). Second, identification of the impact (financial, non-financial and operational) that an incident (worst case scenario) could cause to the organization. Third, the prioritization of the critical processes, which means the order in which these processes should be recovered after an outage. Furthermore, the BIA should specify the minimum level of resources needed to keep the processes working and internal/external dependencies. The BIA is a very important analysis which should be done very carefully. It is the input for other analysis as Risk Assessment and the Business Strategies.

To get a BIA with real information a good practice is to start is creating a processes map. The processes map should be performed taken into consideration all the locations, of the organization, where processes take place. This map should include:

- Premises: all the business units of the organization and their respective processes.

- Resources and Requirements: legal requirements, single points of failures, technology, dependencies (internal and externals), and people who are involve in the processes.
- Times: critical period of time when the processes should be performed in order to deliver a product or to comply with a regulation, contract or service.
- Impact (financial / non-financial / operational): specify the impact of the non-performance of the processes.

Once the map has been completed, the next step is the identification of the critical processes. Critical processes are those that once stopped will impact negatively the organization (financial/reputational) and/or those who represent important agreements with third parties (regulators, stakeholders, suppliers, among others). Finally, RTO, RPO, and MTPoD need to be identified for each critical process. Tammineedi defined RTO as “target time set for resumption of product, service or activity delivery after an incident” and RPO as “the point in time to which a system’s data must be restored after an outage” (p.42). In addition, the Dictionary of Business Continuity Management Terms (2011) defines MTPoD as “The duration after which an organization’s viability will be irrevocably threatened if a product or service delivery cannot be resumed” (p.32). The organization should start with the identification of the MTPoD of the critical processes and then continue with the RTO and RPO. These measures are crucial for the organization because enable them to be aware of how fast the operations need to be resumed to avoid adverse impact to the organization. The definition of this measures will depend in certain aspects of the organization such as their technological platform and the cost the organization is willing to pay to recover without suffer the impact of an adverse event.

The information presented in the processes map can also be used to review the BCMS scope already defined. It is possible to find information in the processes map that should be included in the scope. In that case, this is a good moment to update the scope.

4.4.5.2 Risk Assessment – RA

The main purpose of this analysis is the identification and the assessment of all the threats that could affect the critical elements of the BCMS. The Risk Analysis process includes the identification of threats, evaluation of the likelihood and impact of these threats, application of countermeasure to avoid, handle or mitigate the risks, and finally actions in order to monitor and review that the controls are in place and the protected assets are safe (Whitman, Mattord, & Green, 2014).

To start the Risk Assessment it is important to identify and categorize the different threats and hazards that could affect the organization. The NFPA 1600 provides a list of hazards that could be used as a starting point. However, the organization should evaluate other threats that are specific to them. Once the organization has identified the risks, a methodology to implement the risk assessment needs to be selected. This study proposes the use of the combination of two methodologies: HAZOP (Hazard and Operability Study) and FMEA (Failure Mode and effects analysis). Li, Gupta and, Alloco stated that both methodologies help organizations to identify failures in their process and countermeasures to minimize the impact of these failures (p. 6). The combination of these two methodologies will allow the organization to work with a qualitative analysis (HAZOP) and quantitative analysis (FMEA).

Stamatis (2003) explained that for every risk three components need to be evaluated: severity (S), Occurrence (O), and the detecting rating (D). To evaluate these parameters a scale from 1 to 10 can be used. Through the equation S x O x D it is possible to calculate the Risk Priority Number. The result of this calculation will help to prioritize the order in which the risks should be addressed. To have a more accurate prioritize list of risk is possible calculate the criticality doing S x O. Risks with a higher criticality should be address first. This methodology (FMEA) is also used by Tammineedi (2010) for the assessment of Site Risk Assessment during the implementation of BCM through a standards-based approach.

Finally, in order to develop the countermeasure the organization should apply the HAZOP methodology. Hyatt (2004) stated the following steps in order to apply HAZOP:

- Develop a breakdown of the critical process
- Describe the design intent of all the parts of the process that could be affected (expected behavior of the component selected)
- Select a process parameter (parameter that is important for the expected behavior of the component)
- Apply a guide word (word, used to imply an unexpected behavior, such as more, less, too early, too late, among others)
- Determine the cause of failure (link this with the risks already identified)
- Evaluate consequences/problems

- Recommend actions

4.4.5.3 Business Continuity Strategy

The purpose of the establishment of different business continuity strategies is to decrease the impact of an incident and, as its name says, to “continue” operations while the incident is taking place. With the BIA and RA results in mind, the organization should develop their BC strategies. The strategies can be classified into actions to mitigate the risk of occurrence, technological strategies, and alternate processes.

- Actions to mitigate the risk of occurrence: these actions can be applied to the different resources of the BCM such as premises, equipment, technology, human resources and, vendors. The strategies developed here are actions in order to avoid or minimize the impact of an event. For example: emergency evacuation tests, installation of fire extinguishers, and training in the use of them, among others.
- Technological strategies: steps to follow in order to recover the core system and other critical applications during an adverse event (Disaster Recovery Plan).
- Alternate processes: activities that would be performed to recover the continuity of the operations. Some examples of alternate processes are allow an outsourcing to continue with the critical operations or performing the critical operations manually.
- Alternate site: there are different options to move the operations to an alternate site. These options include: cold site, warm site, hot site and companies’ agreements. The organization should stablish which option is feasible for them.

4.4.5.4 Business Continuity Procedures

The Business Continuity Procedures are all the actions required in order to identify and face an adverse event, respond to the event, operate in contingency, and finally recover and return to the normal operations. These procedures can be divided into three phases: activation of the procedures, operations from alternate site, recovery of the critical processes, and return to normal operation. The organization should establish an incident response structure which will be in charge of the identification of the adverse events, alert the organization and, for the escalation of the incident.

- Activation of the procedures: the contingency team should approve the activation of the contingency state.
- Operations from alternate site: accordance to the nature of the event, the business continuity team should determine if it is necessary or not to move to an alternate site (this site should be defined in the alternate site strategy) and continue operations from there.
- Recovery of critical Process: the previous stage allows the responsible teams of performing the strategies pre-established to work in contingency (technology strategies and alternate processes). Parallel to these activities, other teams should be working in performing the steps to fix damages caused by the incident.
- Return to normal operation: once the damages were fixed it is possible to perform the activities to return to normal operation.

During these phases, the organization should be executing their communication plan which should include the workflow of communications, pre-established messages and, the interested parties who need to be considered.

The Business Continuity Plan is a document where is going to reside all the information related to the organizational structure in charge during an incident, roles and responsibilities, continuity strategies, business continuity procedures, and communication procedures.

4.4.5.5 Exercising and Testing

The only way to be close to guaranteeing that all the continuity process are going to work during a disaster is through exercise and testing. These activities should be done on a regular basis. Sometimes, it can be believed that testing some procedures can be chaotic due to the fact that it involves interruptions in the daily functions. However, there are different kinds of exercises that help to train the critical staff without interrupt the organization's operations. Wong and Shi (2015) stated that exercises can be classified into five categories: orientation, desktop, drill, functional exercise and full-scale exercise. The last two involve complex scenarios. These tests need more time to be designed and the risk level that they present to the organization is higher than the first three. Furthermore, any of these tests will require dedicated resources (time and staff) to be performed. Like any other activity, exercises and tests should be planned, coordinated, and performed. Once they have been performed the lessons learned have to be discussed among all the participants and, finally, documented. These activities will help the organization to know the improvements that are needed in the different procedures and recommendation to achieve the level required for an effective BCMS.

Deliverables: BIA, RA, BC Strategies, Incident Management Structure, Incident Management Policy and Procedures, Business Continuity Plan, Disaster Recovery Plan, Exercise and Testing Plan.

4.4.6 Clause 10 - Performance Evaluation

The importance of this phase lies in the fact that without measurement it is impossible to know how the system is working or even if it is working or not. Due to this fact, this phase proposes to “check” or to evaluate the actual BCMS. According to the necessities of every organization different factors of the BCMS can be assessed. In order to do this, the organization should establish their measurement process and the implementation of internal audits and management reviews.

4.4.6.1 Establishment of Measures

The evaluation criteria will vary from organization to organization. However, many organizations can agree on common evaluation criteria. Wong and Shi (2015) stated that some factors to be used as measures, metrics or performance indicators can be business continuity leadership, contribution to critical operations, the design of the BCM, BCM teams and individual’s performance, and adaptability of the BCMS. From a technical perspective, the measures and metrics can be based on uptime, scalability, reliability, availability, recovery time, and recovery point of the technological systems (Bajgoric, 2014).

Bajgoric (2014) stated the necessity of continuous computing technologies as part of a systematic framework for the implementation of BCM. The main purpose of these technologies is to improve the availability, reliability and scalability of information infrastructure. In addition, Bajgoric (2014) stated that these technologies can be implemented into three layers: server operating system (layer 1), storage, backup, and recovery (layer 2), and networking infrastructure (layer 3). Taking this into consideration the organization should specify the expected normal behavior of these component in order to measure and control it.

To guarantee continuity of the different services it is important that the organization establishes performance indicators, which include the management and the technical side. In the case of the technical metrics, the organization should previously evaluate their technological platform. Based on this, the measures for reliability, availability, and scalability should be indicated.

4.4.6.2 Implementing an Internal Audit Process

The audit process should be performed by an independent entity. If the organization does not have an audit department it can be performed by a third party. The auditing process should be accompanied by the proper planning and coordination stages. It must be performed on a regular basis and also taking into consideration the results of the previous audit. This will allow the auditors to perform follow-ups. The audit should include the evaluation of the design and operational effectiveness of the BCMS. Furthermore, the metrics and measures established in the previous step should also be assessed.

4.4.6.3 Performing Management Reviews

The importance of these reviews lies in the fact that they allow the organization to perform the necessary changes in the BCMS (scope, plans, and improvements in processes or performance indicators, among others). These reviews let the BCMS be updated because it keep them in contact with the external enablers as new regulations appear or new risks arise. Furthermore, these reviews help to perform follow-ups of the nonconformities found during the audits.

Deliverables: Performance Indicators, Performance Indicators Report, Audits Report, Management Review Reports.

4.4.7 Clause 11 - Improvement

This phase concentrates on the analysis of nonconformities, evaluation and implementation of countermeasures to handle and/or delete the nonconformities found and, follow-ups of these countermeasures. The final purpose of this continual improvement cycle is to remediate nonconformities and to allow constant enhancement of the BCMS. The nonconformities can be categorize into documentation, leadership, process and procedures, training and awareness, among others. For example, the inexistence of a communication plan is a nonconformity related to documentation. These nonconformities are identified in the previous stage, performance evaluation, through any of the different assessments. The organization should develop and implement a remediation procedure in order to be able to analyze, evaluate, and correct the nonconformities detected. This procedure should explain the steps to follow in order to be able to propose, approve, and implement countermeasures or correction actions.

Deliverables: Policy and Procedures for Remediation of BCM Nonconformities

Appendix D includes a list of the different activities proposed to perform for the implementation of a holistic BCM, and the period when these activities should be performed.

Appendix E includes a list of additional resources that can be used to perform the activities established for the implementation of the holistic BCM.

4.5 Summary

This chapter presented an analysis of the ISO 22301 standard and how to use the standard, other frameworks, techniques, and methodologies to implement a holistic BCMS. This chapter goes step by step covering the different clauses of the standard. Moreover, the reader has the opportunity of learning the activities per clause that need to be performed. Furthermore, at the end of every clause are provided the deliverables or outcomes. It will help the reader to understand what is the result or product of each phase. The next chapter will provide the results of a BCMS analysis performed in a financial entity in a Latin American country.

Chapter V

CASE STUDY IN A LATIN AMERICA FINANCIAL INSTITUTION AND BCM LEGAL FRAMEWORK IN PANAMA

This case study does not provide any information regarding the name of the institution where the study was performed, specific location of the entity or contact information of the interviewees in order to protect their privacy and the image of the institution. Today neither in the future this information will be disclose.

5.1 Introduction

A case study "can provide insight into the events and situations prevalent in a group from where the case has been drawn" (as cited in Kumar, 2014, p. 155). To analyze a BCMS's current state, a case study is a suitable technique. It helps to understand different aspects across the organization. In addition, because only one organization is evaluated more information can be gathered. The case study presented in this section was developed in a Latin American financial institution. It helps to illustrate some of the BCM flaws that can be present in this kind of organization. Finally, the research performed an analysis about the BCM legal matter in Panama.

5.2 Case Study

An analysis of the current situation of the BCMS of a financial entity in Latin America was performed. The purpose of this analysis was to discover weaknesses or flaws in the organization's BCMS. To achieve this goal interviews were performed. The tool used to get the information and to conduct the interviews was a questionnaire with open and closed questions. The questions were divided into the 7 operative sections (clauses of the standard ISO 22301): the context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. The questionnaire was based on the book “Business Continuity Management System: A Complete Guide to Implementing ISO 22301” by Wei Ning Zechariah Wong and Jianping Shi, and in the guide presented in this study. To evaluate the results of each category some indicators were taken into consideration: is the organization fulfilling specific requirements, is the organization aware of the importance of the section in evaluation, is the organization mature enough, among others. The scale rate used to evaluate the different sections were 1 to 6, where 1 was the lowest score and 6 was the highest.

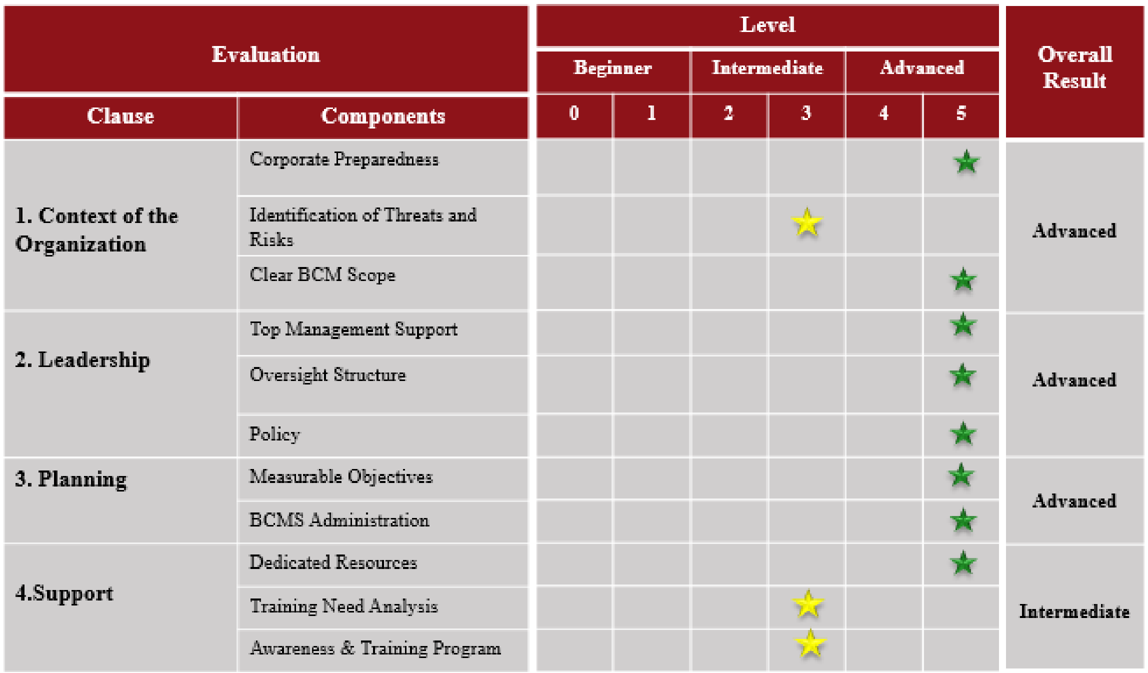
Level 1 and 2 are considered the beginner levels, level 3 and 4 are considered intermediate levels and, level 5 and 6 are considered the advanced levels.

Beginner level: the organization has a low level of maturity. The organization is not aware of the importance of the different operations/process evaluated. There is no documentation about them.

Intermediate level: the organization is aware of the importance of the operations/process evaluated. There is documentation, however, there are some activities that are not covered by the organization.

Advanced level: the organization is completely aware of the importance of the operations/process evaluated. It can be perceived through the presence of documentation, clear metrics and support from the top management.

5.3 Summary of Results



Evaluation		Level						Overall Result
		Beginner		Intermediate		Advanced		
Clause	Components	0	1	2	3	4	5	
1. Context of the Organization	Corporate Preparedness						★	Advanced
	Identification of Threats and Risks				★			
	Clear BCM Scope						★	
2. Leadership	Top Management Support						★	Advanced
	Oversight Structure						★	
	Policy						★	
3. Planning	Measurable Objectives						★	Advanced
	BCMS Administration						★	
4.Support	Dedicated Resources						★	Intermediate
	Training Need Analysis				★			
	Awareness & Training Program				★			

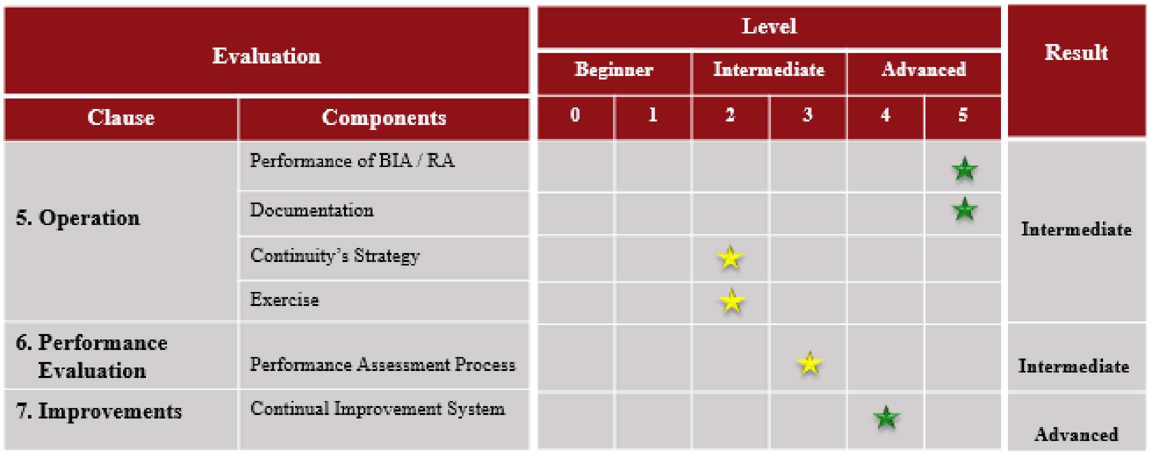
Figure 5. 1. Results (Clause 1 to 4). This figure illustrates the different components evaluated, their rates and the overall result per area.

Figure 5.1 shows that the organization is in an “Advanced” state in the clauses of the context of the organization, leadership, and planning. On the other hand, figure 5.1 also shows that the organization is in an “Intermediate” state in the support area. The reasons for these results are the following:

- *Identification of threats and risks:* Even when the organization has an established process to identify threats and risks, this process is only performed every two years. This process should be done every time a major change in the organization occurs or a new threat/risk is discovered.
- *Training Need Analysis*: Even when the organization has an annual performance assessment for the organization’s employees, and the supervisor evaluates their

training needs it is necessary to do it more deeply. For example, the analysis should include gaps, requirements, arrangements, adequacy, and priorities.

- *Awareness and Training Program*: Even when the organization has an awareness and training program in place, it is necessary that it works more to create a BCM culture in the whole organization. Today, this program involves only the BCM teams. It is possible to achieve this through the performance of more activities related to the BCM awareness, such as: workshops, educational fair, lunch time talks, mentoring, among others.



Evaluation		Level						Result
		Beginner		Intermediate		Advanced		
Clause	Components	0	1	2	3	4	5	
5. Operation	Performance of BIA / RA						★	Intermediate
	Documentation						★	
	Continuity's Strategy			★				
	Exercise			★				
6. Performance Evaluation	Performance Assessment Process				★			Intermediate
7. Improvements	Continual Improvement System					★		Advanced

Figure 5. 2. Results (Clause 5 to 7). This figure illustrates the different components evaluated, their rates and the overall result per area.

Figure 5.2 shows that the Improvements clause is in “Advanced” level. In addition, figure 5.2 also shows that the clauses operation and performance evaluation are in “intermediate” state. It is because of the following reasons:

- *Continuity Strategy*: The organization has high redundancy in their technology equipment, however, it does not have an alternate data center or a strategy to continue working if their primary site is gone. It is important that the institution evaluates the development of a continuity strategy that is economically feasible to their size and the amount of transactions that they perform.

- *Exercise*: the organization has only performed drill exercises. In addition, these exercises are focused in specific critical processes of the BIA. However, other procedures as the incident management in case of a security incident has not been discussed or tested among the incident management team. To remediate this, a more complete testing and exercise program should be developed.
- P*erformance Assessment Process:* even when the organization has a performance assessment process in place it is not strong enough. The audits performed are directed to the Risk Area and not specifically to the Business Continuity Area. A result of this is that many key indicators are not assessed such as: design of the BCMS, BCM teams or their adaptability to BCMS, BCM policy framework, review of skills and capabilities of staff, among others. To remediate this, the audit scope should be increased and it should include the features of the BCM that are not currently taken into consideration.

The overall result of this evaluation indicates that the current BCM state of this organization is at an intermediate level. However, as was stated, there are some improvements that should be performed. The implementation of some of them (support, performance evaluation clauses) does not represent any financial impact to the organization. However, the development and implementation of a continuity strategy for the critical technological platform could represent a financial impact for the organization. In this case, the pros and cons of different options should be evaluated.

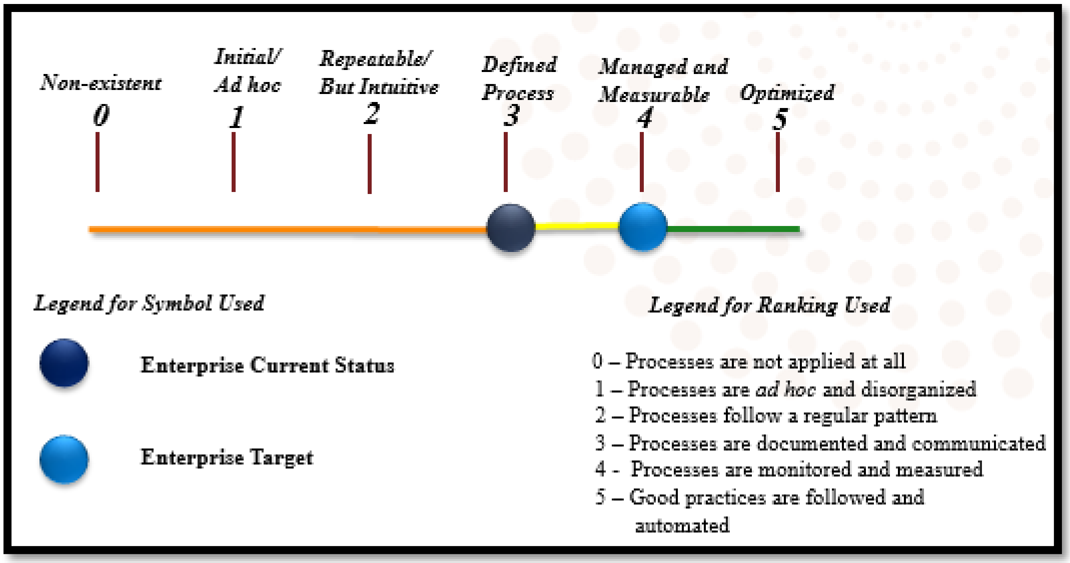

Non-existent
0
Initial/ Ad hoc
1
Repeatable/ But Intuitive
2
Defined Process
3
Managed and Measurable
4
Optimized
5
Legend for Symbol Used
Enterprise Current Status
Enterprise Target
Legend for Ranking Used
0 – Processes are not applied at all
1 – Processes are ad hoc and disorganized
2 – Processes follow a regular pattern
3 – Processes are documented and communicated
4 - Processes are monitored and measured
5 – Good practices are followed and automated

Figure 5. 3. Graphic representation of the final result. This figure illustrates the current status of the organization and the target status.

Appendix B includes the information provided by the organization evaluated.

5.4 BCM Legal Framework in Panama

Panama was selected to do this analysis due to the fact that their bank system is considered an international finance center. Unlike developed countries such as the United States, in Panama there is only one industry that is in any way regulated regarding BCM: the bank industry. There are important laws enacted that control the way banks perform their operations. The entity in charge of guarantying the proper operations of banks in Panama is called the “Superintendency (sic) of Banks of Panama”. According to their website:

> Among the main duties of the Superintendent are: to watch for the stability of the banking system; supervise banks and those economic groups whereof they make a part; grant and cancel banking licenses; order corrective measures concerning banks (appointment of advisors, interventions, reorganizations,

> compulsory liquidations, imposition of fines, etc.); as well as authorizing bank mergers and the administration of the daily tasks of the Superintendency (About the SBP, Superintendency of Banks of Panama, 2015).

As the website stated, the superintendent is in charge of keep an environment of control in the banking system.

In addition, to the laws enacted by the Legislative Assembly in Panama, the Superintendency of Banks creates regulations (rules, circulars, and resolutions) that promote an environment of control in the bank industry. In an interview with Vielka de Licona, the Manager of IT Risk for the Superintendency, explained that there is not a law dedicated only to business continuity in Panama. Ms. Licona pointed out that while this is true, Business Continuity which is article 54 of the Banking Law (2008) states:

> Banks shall have policies, regulations, and procedures to ensure that their principal operations can be maintained or recovered in a timely manner, in order to minimize the effects of any significant interruption that might affect their operational capability. The Superintendency may issue regulations applicable to this issue (p. 27).

As Ms. De Licona stated, an individual law, constructed solely for Business Continuity, does not exist, a clause in the general law is dedicated to this topic.

In order to guide the organizations in this topic, The Superintendency of Bank created the rules: 6-2011 (Whereby the guidelines on E-banking and Related Risk Management are established), 7-2011 (Whereby the rules on Operational Risk are established), and 3-2012 (Whereby the Guidelines for Managing Information Technology Risks are provided). However, during the review of these rules, it was possible to notice that they are not very specific in their implementation. Due to the facts that the country does not have a specific law for BCM, the size of the Panamanian banking system, and the economical acquisition power sometimes it is difficult to assess banks in the BCM matter. Furthermore, because the Panamanian banking system is really varied there is not a uniform way to assess their BCMS. The Superintendency of Banks take into consideration different aspects such as:

- Shareholding (determine the dependence by the shareholding: branch, subsidiary or headquarter)
- Type of bank license
- How is their technological platform administered?
- Is their technological platform outsourced?

Despite all the differences that can be found in the banking system in Panama the Superintendecy requires, at least, a contingency plan and the results of tests performed to guarantee the continuity of their services during an adverse event (V. de Licona, personal communication, March 17, 2016).

It is necessary to organize in a formal way the BCM in Panama. A specific law for it is required in order to help the Superintendency of Banks to state more specific rules and assessments. The enactmet of a law will allow having a stronger banking system able to recovery from serious incidents or disasters. It is known that because of the size of the banking system in Panama and the acquisitive economic power of banks sometimes it is difficult for the board of directors to acquire new technologies in order to achieve stronger continuity strategies. However, with the enactment of a BCM law it could change.

5.5 Summary

This chapter presented the results of a case study implemented in a financial institution in Latin America. The case study was divided into seven sections, these sections correspond to the different clauses of the standard ISO 22301. The purpose of the implementation of the case study was to evaluate the BCM current state of the institution. The results of this study help to understand which are some of the areas where an organization should focus on and, where the organization should make improvements. Finally, at the end of the chapter, a brief analysis was provided of what already exists and what is needed in the legal framework related to BCM in Panama.

Chapter VI

CONCLUSION

Business Continuity Management is not a new field. But it was in the last few years that it took a new and stronger momentum. This momentum was due to different facts such as terrorist attacks, new laws, and natural disasters, among others. All of these events required organizations to look forward and to seek for the strategies to continue their operations during the worst case scenario. In this route, many organization lose their path. Many people believe that BCM is related only to technology and that only the IT personnel are in charge of it. The truth is completely different.

This research demonstrated that there are several areas involved in the implementation of a BCMS and that people throughout the organization should actively participate in it. While some of them need to participate in the whole cycle, such as the administrators of the BCM system, other’s participation is required in specific moments. Furthermore, this report stated how a holistic framework can be implemented in an organization. The guide presented can be used as a starting point for the implementation, however, specific details of each organization have to be taken into consideration to make a successful implementation possible. The guide provided different activities and deliverables that can be implemented in order to achieve a holistic BCM. The deliverables presented enable the personnel involved in the BCM process to have a better understanding of what has been done and what needs to be done.

The case study presented in the report helps readers to understand how a gap analysis can be implemented in any organization. It allows readers to have a better understanding of how it is possible to evaluate the current state of a BCM and, how different aspects can affect the performance of the BCMS. Furthermore, the case study provided recommendations to fix the flaws discovered. Finally, the study presented an analysis of the legal framework related to BCM in Panama. This analysis demonstrated the impact that external factors have on the implementation of a BCMS.

This paper is not directed only to one kind of audience. Different people can perceive the benefits of the information presented in this study. However, the main purpose of this document is to help any IT/InfoSec professional interested in business continuity management to learn about it, to understand it and, to be able to perform a holistic implementation. Moreover, this paper gives tools to achieve a holistic implementation. Finally, this paper wants to create awareness in the Panamanian society about the importance of the enactment of a law dedicated to BCM.

Future work

1. Frameworks evaluated: new frameworks can be analyzed in order to include new methodologies to achieve a robust holistic framework. Furthermore, it will allow readers to manage different options when they are going to implement a BCMS.
2. Questionnaire to assess current BCM state: the questionnaire presented in this paper can be improved through the addition of more specific questions in order to have a greater understanding of the BCM’s current state. The researcher would include more questions especially related to the IT platform.
3. New methodologies in the Operation clause to develop BIA and RA: this work proposes some methodologies to work in this clause however, it is possible to

develop new methodologies or make a comparative analysis of which methodology is the best to be implemented.

4. Development and enactment of a legal framework for BCM in Panama: due to the lack of a legal framework in the BCM field, a deep research about it can be performed. In addition, the development of a project to enact a law can be presented in order to help the improvement of BCMS in the banking system in Panama.
5. The case study can be performed in different locations in order to know different external factors that can affect the implementation of a holistic BCM implementation.

BIBLIOGRAPHY

Hyatt, N. (2004). *Guidelines for Process Hazards Analysis, Hazards Identification & Risk Analysis.* Ontario: CRC Press.

Kaplan, B., & Maxwell, J. (2005). Qualitative research methods for evaluating computer information systems. In J. Anderson, & C. Aydin, *Evaluating the organizational impact of healthcare information system* (pp. 30-49). Springer.

Kumar, R. (2014). *Research Methodology a step by step guide for beginners.* London: SAGE Publications Ltd.

Maxwell, J. (2013). *Qualitative Research Design an Interactive Approach.* Los Angeles: SAGE.

Stamatis, D. (2003). *Failure Mode and Effect Analysis FMEA from theory to execution.* Milwaukee: ASQ.

Wong, W., & Shi, J. (2015). *Business Continuity Management System.* London: Kogan Page.

Whitman, M., Mattord, H. & Green A. (2014). Principles of Incident Response & Disaster Recovery. United States of America: Course Technology, Cengage Learning.

REFERENCES

Amaratunga, D., Baldri, D., Sarshar, M., & Newton, R. (2002). Quantitative and Qualitative Research in the built environment: Application of "mixed" research approach. *Work Study*, 17-31.

Bajgoric, N. (2014). Business continuity management: a systemic framework for implementation. *Kybernetes*, 156-177.

Bird, L. (2011, September). *Dictionary of Business Continuity Management Terms.* Retrieved from Business Continuity Institute: http://www.thebci.org/glossary.pdf

Brennan, J., & Mattice, L. (2014). Resiliency: Survival of the Fittest. *Security*, 26-27.

Ee, H. (2014). Business Continuity 2014: From traditional to integrated Business Continuity Management. *Journal of Business Continuity & Emergency Planning*, 102-105.

Gibb, F. & Buchannan, S. (2006). A framework for business continuity management. *International Journal of Information Management.* 128-141.

Green, C. (2014). Measuring business continuity programmes in large organisations. *Journal of Business Continuity & Emergency Planning.* 71-81.

Gupta, P. (2006). Beyond PDCA- A New Process Management Model. *Quality Progress*, 45-52.

Herbane, B. (2010). The evolution of Business Continuity Management: A historical review of practices and drivers. *Business History*, 25.

Hiles, A. (2011). *The Definitive Handbook of Business Continuity Management.* United Kingdom: John Wiley & Sons.

ISACA. (2012). Business Continuity Management: Emerging Trends. *ISACA Journal*, 1-15.

ISO 22301: Societal Security - Business continuity management systems - Requirements. International Organization for Standardization, Geneva, Switzerland. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038 (accesed 21st March, 2016)

Jarvelainen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 583-588.

Jedynak, P. (2013). Business Continuity Management The Perspective of Management Science. *International Journal of Contemporary Management*, 85-96.

Kadar, M. (2015). Development and implementation of a business continuity management risk index. *Journal of Business Continuity & Emergency Planning.* 238-251.

Li, X., Gupta, J., & Allocco, M. (2015). Hazard and Operability (HAZOP) Analysis of Safety-Related Scientific Software. *International Journal of Reliability, Quality and Safety Engineering*.

McCusker K. & Gunaydin S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion.* 537-542.

McLaughlin, P. (2005). NFPA 1600: ground rules for disaster-preparedness. *Cabling Installation & Maintenance*, 38-40.

N.A. (2011). *ISO 22301 World*. Retrieved from BS 25999 and ISO 22301 Introduction: http://www.25999.info/

Panama. Ministry of Economy and Finance.(2008).*Executive Decree No 52.* Panama, Panama. Ministry of Economy and Finance.

Pasquini, A., & Galie, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. *Symposium from Young Researchers*, (pp. 67-76). Budapest.

Randeree, K., Maha, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal*, 472-492.

Rodgers, J. (2001). A Sense of Urgency. *Bank Systems and Technology*, 33-34.

Samson, P. (2013). Beyond the 48 hours. *Financial Executive*, 54-57.

Singh, K. (2015). Creating your own qualitative research approach: selecting, integrating and operationalizing philosophy, methodology and methods. *SAGE.* 132-146.

Tammineedi, R. (2010). Business Continuity Management: A Standards Based - Approached. *Information Security Journal: A Global Perspective* , 36-50.

Torabi, S.A., Rezaei, H., & Sahebjamnia,N. (2014). A new framework for business impact analysis in business continuity management (with a case study). *Safety Science.* 309-323.

Young, R. (2015). Survival of Prepared, not the fittest energy company: . *Oil, Gas & Energy Quarterly*, 411-432.

Zawada, B. (2014). The practical application of ISO 22301. *Journal of Business Continuity & Emergency Planning*, 83-90.

APPENDIX A

The following table present the different activities recommended in this study for each of the ISO 22301 clause. The criteria used were: complexity of the activity, impact of the performance of the activity in the daily operations, and possible amount of time involved in the development of the activity. These criteria were evaluated through the assignation of a weight. This weight can vary from 1 to 5, where 1 represent the lowest score and 5 represent the highest. To get the percentage of time in the implementation the total score per activity was summarize, then all the total amount per activity were summarize per clause, and finally this formula was used:

(Total score per clause * 100) / (Total score of all the activities)

CLAUSE	***ACTIVITIES RECOMMENDED***	Complexity of the Activity	Impact of the Activity in the Daily Operations	Time Involved in the Development of the Activities	Total Amount Per Activity	Total Amount Per Clause	Percentage of time in the Implementation
Context of the Organization	Perform Corporate Analysis	2	1	1	4	16	10
	Perform Threat & Resilience Analysis	2	1	1	4		
	Perform Stakeholder & Regulatory Analysis	2	1	1	4		
	Define Scope (Alignment of BCM with Business Strategy)	2	1	1	4		
Leadership	Determine the Resources for BCMS	2	1	2	5	12	7.5

CLAUSE	***ACTIVITIES RECOMMENDED***	Complexity of the Activity	Impact of the Activity in the Daily Operations	Time Involved in the Development of the Activities	Total Amount Per Activity	Total Amount Per Clause	Percentage of time in the Implementation
	Document the BC policy	1	1	1	3		
	Define Roles & Responsibilities	2	1	1	4		
Planning	Define the BCM objectives	4	1	3	8	8	5
Support	Perform a Training Needs Analysis	2	2	3	7	21	13.13
	Define the Training & Awareness Program	2	1	3	6		
	Document a Communication Plan	2	1	1	4		
	State a Document Management Policy	2	1	1	4		
Operation	Perform BIA	5	4	4	13	64	40
	Perform RA	5	2	4	11		
	Define BC Strategies (DRP)	5	2	4	11		
	Define the BC Procedures (IR)	5	2	4	11		
	Document the Exercise & Testing Plan	3	1	3	7		
	Implement the Exercise & Testing Plan	4	4	3	11		
Performance Evaluation	Establish Measures & Performance Indicators	3	1	3	7	23	14.38

CLAUSE	***ACTIVITIES RECOMMENDED***	Complexity of the Activity	Impact of the Activity in the Daily Operations	Time Involved in the Development of the Activities	Total Amount Per Activity	Total Amount Per Clause	Percentage of time in the Implementation
	Perform Management Reviews	3	2	2	7		
	Implement Internal Audit	3	3	3	9		
Improvement	Develop a Plan for Remediation of Nonconformities	3	1	2	6	16	10
	Implementation of the Plan	4	3	3	10		

APPENDIX B

BCM CURRENT STATE ASSESSMENT

Name of the Organization:

Location:

Date of the Evaluation:

Clause 5: Context of the Organization

Does the organization perform an assessment of the current BCMS status?

Answer:

Does the organization identify threats and risk to their critical assets and processes?

Answer:

Is there any regulatory requirement related to BCM that applies to the organization?

Answer:

Does the organization identify its stakeholders? (Staff, customers, and shareholders, other organizations, media, government)

Answer:

Is the scope of the BCMS defined?

Answer:

Does the organization defined and documented their mission, vision, strategic goals?

Answer:

Clause 6: Leadership

Does the BCMS have support from top management?

Answer:

Is a designed member of the organization in charge of the BCMS?

Answer:

Does the organization have a clear Business Continuity Structure?

Answer:

Does the organization have a BC policy?

Answer:

Clause 7: Planning

Does the organization have clear and measurable BCM objectives?

Answer:

Clause 8: Support

Does the organization have dedicated resources (budget, personnel) for BCMS?

Answer:

Is a training needs analysis performed? Does it addresses gaps, requirements, arrangements, adequacy, and priorities?

Answer:

Are the skills of the BCM professionals assessed?

Answer:

Does the organization have an awareness and training program in place?

Answer:

Which methods of delivery is the organization using for awareness and training activities?

Answer:

Does the organization have a communication plan which includes internal/external communications and media communication?

Answer:

Clause 9: Operation

Does the organization have a BIA and RA?

Answer:

Which are the key factors considered when the critical processes are defined?

Answer:

Does the BIA cover the following key areas?

Functions	**Impacts**	**Recovery Timescales**	**Resource Requirement**	**Dependencies**
Processes	Operational	Maximum Tolerable Periods of Disruption (MTPD)	Building Equipment Technology Human Resources Vendors	Internal
Deliverables (products and services)	Financial	Recovery Time Objectives (RTOs)		External
Delivery Time	Non-Financial	Recovery Point Objectives (RPOs)		Suppliers and Stakeholders

How does the organization assess operational and financial impacts?

Answer:

For each critical function, were MTPD, RTO and RPO defined?

Answer:

How does the organization identify the recovery timescales?

Answer:

Does the organization have a priority list of the activities that should be recovered?

Answer:

For every critical process, does the organization develop an analysis of the required resources?

Answer:

Which methodology was used to develop the Risk Assessment Process?

Answer:

How does the organization categorize the risks?

Answer:

Does the organization have an Incident Management Structure?

Answer:

Does the organization have the following key documents?

Plan	Organization
Incident Management Plan	
Crisis Communication Plan	
Business Continuity Plan	
Disaster Recovery Plan	

Which exercises does the organization perform and how frequently?

Answer:

Clause 10: Performance Evaluation

Does the organization have a performance assessment process in place?

Answer:

If your answer is yes please answer the following:

- Which factors does the organization have identified as key to the effectiveness of the BCMS?

  Answer:

- How are these key factors assessed?

  Answer:

- What is included in the audit scope?

  Answer:

Clause 11: Improvement

Is there any BCMS control system in place?

Answer:

If your answer is yes, please answer the following:

- Which assessment criteria is the organization using?

  Answer:

- Which methods of assessment is the organization using?

  Answer:

- How frequently does the business continuity manager review the adequacy of the control system?

Answer:

- Which monitor controls does the organization have in place?

  Answer:

How does the organization identify and correct nonconformities?

Answer:

Has the team found any nonconformities in the last review?

Answer:

Does the organization document the nonconformities found?

Answer:

How does the organization eliminate/remediate the non-conformities and follow it up?

Answer:

Which are the areas where continual improvement focus?

Answer:

APPENDIX C

QUESTIONNAIRE PERFORMED IN A LATIN AMERICAN FINANCIAL INSTITUTION

Clause 5: Context of the Organization

Does the organization perform an assessment of the current BCMS status?

Answer: *In late 2015, the organization contracted an outsourcing company to perform an analysis of the actual maturity of the organization in terms of continuity. This study assessed different areas of the organization focusing on TI, Marketing (communications), Continuity Department, among others. Some of the issues that were addressed include IT alignment with the Business, assessment of the different impacts and the continuity strategies. All the subsidiaries of the organization were evaluated.*

Does the organization identify threats and risk to their critical assets and processes?

Answer: *Yes, it does. Every two years the organization re-assesses the threats and risks.*

Is there any regulatory requirement related to BCM that applies to the organization?

Answer: *Yes, there is.*

Does the organization identify its stakeholders? (Staff, customers, and shareholders, other organizations, media, government)

Answer: *Yes, the organization does. This information is included in the Crisis Plan.*

Is the scope of the BCMS defined?

Answer: *Yes, it is.*

Does the organization defined and documented their mission, vision, strategic goals?

Answer: *Yes, the organization does.*

Clause 6: Leadership

Does the BCMS have support from top management?

Answer: *Yes, it does.*

Is a designed member of the organization in charge of the BCMS?

Answer: *Yes, it is. There is a Vice-president who reports to the Risk Committee and, this committee reports to the Board of Directors.*

Does the organization have a Business Continuity Structure?

Answer: *Yes, it does.*

Does the organization have a BC policy?

Answer: *Yes, it does.*

Clause 7: Planning

Does the organization have clear and measurable BCM objectives?

Answer: *Yes, it does.*

Clause 8: Support

Does the organization have dedicated resources (budget, personnel) for BCMS?

Answer: *Yes, it does.*

Is a training needs analysis performed?

Answer: *As part of the performance evaluation a training needs analysis is also performed every year. According to the results the leader of the continuity area will recommend different trainings.*

Are the skills of the BCM professionals assessed?

Answer: *Yes, during the performance evaluation.*

Does the organization have an awareness and training program in place?

Answer: *Yes, it does.*

Which methods of delivery is the organization using for awareness and training activities?

Answer: *Posters, e-mail messages, free gifts inscribed with key messages, pamphlets, instructor – led sessions, web-based training, and customized training packages*

Does the organization have a communication plan which includes internal/external communications and media communication?

Answer: *Yes, it does.*

Clause 9: Operation

Does the organization have a BIA and RA?

Answer: *Yes, it does.*

Which are the key factors considered when the critical processes are defined?

Answer: *Corporate objectives and obligations, products and services required to achieve the corporate objectives and obligations, period of time when the corporate objectives and obligations should be achieved, impact of non-compliance of objectives and obligations, personal responsible for delivering corporate objectives and obligations. In addition, today the organization is taken into consideration "income left to perceive" as a new key factor. For example, the "collection process" wasn't considered as a critical process. However, if this process is not done properly or it stops working, it will impact the financially the organization.*

Does the BIA cover the following key areas?

Functions	Impacts	Recovery Timescales	Resource Requirement	Dependencies
Processes ☑	Operational ☑	Maximum Tolerable Periods of Disruption (MTPD) ☑	Building Equipment Technology Human Resources Vendors ☑	Internal ☑
Deliverables (products and services) ☑	Financial ☑	Recovery Time Objectives (RTOs) ☑		External ☑
Delivery Time due ☑	Non-Financial ☑	Recovery Point Objectives (RPOs) ☑		Suppliers and Stakeholders ☑

How does the organization assess operational and financial impacts?

Answer: *through meetings with the process owners to know more about the process, how much it generates and critical frames where these processes should be working.*

For each critical function, were MTPD, RTO and RPO defined?

Answer: *Only were defined RTO and RPO.*

How does the organization identify the recovery timescales?

Answer: *It is identified according to the critical periods.*

Does the organization have a priority list of the activities that should be recovered?

Answer: *Yes, it does.*

For every critical process, does the organization develop an analysis of the required resources?

Answer: *Yes, it does.*

Which methodology was used to develop the Risk Assessment Process?

Answer: *The methodology used for the RA follows 5 steps: identification, evaluation, mitigation, monitoring, and review. The Risk Assessment Process is made by a third party. The third party performs the identification and evaluation phases while the organization performs mitigation, monitoring, and review.*

How does the organization categorize the risks?

Answer: *the categorization of risk was made by the risk department. This information is not handle by the Business Continuity Area.*

Does the organization have an Incident Management Structure?

Answer: *Yes, it does.*

Does the organization have the following documents?

Plan	Organization
Incident Management Plan	☑
Crisis Communication Plan	☑
Business Continuity Plan	☑

Plan	Organization
Disaster Recovery Plan	☑

Which exercises does the organization perform and how frequently?

Answer: *Drill exercises are performed for the critical process once per year.*

How does the organization perform in relation to the following key factors?

Resources		Organization Comments
People	Training	*It is necessary make real exercise to ensure that the people know what they have to do and how are they going to act*
	Documentation	*All the processes and procedures are documented. The organization is working in develop an electronic repository of all these documentation*
	Succession Planning	*It exists. Everybody has a backup this information is detailed in the Incident and Crisis Manual*
	Specialists Third parties	*The organization has a third party in charge of the organization's communication during a crisis*

Resources		Organization Comments
Premises	Secondary Location	*The organization has a another location to continue with the critical process in case of a crisis*
Information	Backup and Recovery Methods	*The organization stores their backups in an external facility*
Technologies	Power	*The organization has UPS*
	Network and Equipment	*There is redundancy of the critical assets*
	Backup Storage	*The organization has backup of their information in an outside location*

Clause 10: Performance Evaluation

Does the organization have a performance assessment process in place?

Answer: *Yes, it does.*

If your answer is yes please answer the following:

- Which factors does the organization have identified as key to the effectiveness of the BCMS?

  Answer: *Communication, response analysis, times, the domain of the information, strategies to follow.*

- How are these key factors assessed?

  Answer: *exercises and management assessments*

- What is included in the audit scope?

Answer: *the internal audits scope include the review of the results of the tests performed and the continuity plan. The audit scope does not include assess the policy framework, review of skills and capabilities of staff.*

Clause 11: Improvement

Is there any BCMS control system in place?

Answer: *Yes, it is.*

If your answer is yes, please answer the following:

- Which assessment criteria is the organization using?

  Answer: *Performance Criteria*

- Which methods of assessment is the organization using?

  Answer: *Internal/External Audits, Self-Assessments*

- How frequently does the business continuity manager review the adequacy of the control system?

  Answer: *quarterly and annual. The control system is based on indicators. The frequency of review depends on the indicators.*

- Which monitor controls does the organization have in place?

  Answer: Exercises, performance evaluations, audits, self-assessments

Has the team found any nonconformities in the last review?

Answer: *Yes, regarding the continuity strategy. The organization does not have an alternate data center or a strategy to continue operating if the primary center is gone.*

Does the organization document the nonconformities found?

Answer: *Yes, it does.*

How does the organization eliminate/remediate the non-conformities and follow it up?

***Answer:** Once the non-conformities have been identified, they have to be reported to the Vice president with possible eliminate/remediate actions. The Vice president assess the viability of these actions and approve or reject them and propose it to the Risk Committee of the organization which approves or denies the actions.*

Which are the areas where continual improvement focus?

***Answer:** people (training and awareness), process and procedures (testing and exercises). In addition, if any nonconformity is detected the area work in fix it and follow it up in order to completely remediate it.*

APPENDIX D

LIST OF RECOMMENDED ACTIVITIES TO BE PERFORMED FOR THE PRE IMPLEMENTATION AND IMPLEMENTATION OF THE BCM

PRE IMPLEMENTATION OF BCM	
RECOMMENDED ACTIVITIES	**TIME TO PERFORM IT**
Definition of BCM Structure	Prior an Event
Evaluation of the BCM current state	Prior an Event

IMPLEMENTATION OF BCM		
ISO 22301 CLAUSES	**RECOMMENDED ACTIVITIES**	**TIME TO PERFORM IT**
Context of the Organization	Perform Corporate Analysis	Prior an Event
	Perform Threat & Resilience Analysis	Prior an Event
	Perform Stakeholder & Regulatory Analysis	Prior an Event
	Define Scope (Alignment of BCM with Business Strategy)	Prior an Event
Leadership	Determine the Resources for BCMS	Prior an Event
	Document the BC policy	Prior an Event

IMPLEMENTATION OF BCM		
ISO 22301 CLAUSES	**RECOMMENDED ACTIVITIES**	**TIME TO PERFORM IT**
	Define Roles & Responsibilities	Prior an Event
Planning	Define the BCM objectives	Prior an Event
Support	Perform a Training Needs Analysis	Prior & After an Event
	Define the Training & Awareness Program	Prior & After an Event
	Document a Communication Plan	Prior an Event
	State a Document Management Policy	Prior an Event
Operation	Perform BIA	Prior an Event
	Perform RA	Prior an Event
	Define BC Strategies (DRP)	Prior an Event
	Define the BC Procedures (IR)	Prior an Event
	Document the Exercise & Testing Plan	Prior an Event

IMPLEMENTATION OF BCM		
ISO 22301 CLAUSES	**RECOMMENDED ACTIVITIES**	**TIME TO PERFORM IT**
	Implement the Exercise & Testing Plan	Prior & After an Event
	Implementation of the Plan, Procedures and Strategies	During an Event
Performance Evaluation	Establish Measures	Prior an Event
	Perform Management Reviews	Prior an Event
	Implement Internal Audit	Prior an Event
Improvement	Develop a Plan for Remediation of Nonconformities	Prior an Event
	Implementation of the Plan	Prior an Event

APPENDIX E

ADDITIONAL RESOURCES FOR THE RECOMMENDED ACTIVITIES

ACTIVITIES	ADDITIONAL RESOURCES
Define the Training & Awareness Program	Information Technology Security Training Requirements: A Role- and Performance-Based Model NIST 800 - 16
Perform BIA	Contingency Planning Guide for Federal Information Systems NIST 800 - 34
Perform RA	Guide for Conducting Risk Assessment NIST 800 - 30
Define BC Strategies (DRP)	Contingency Planning Guide for Federal Information Systems NIST 800 - 34
Define the BC Procedures (IR)	Contingency Planning Guide for Federal Information Systems NIST 800 - 34 Computer Security Incident Handling Guide NIST 800 - 61

ACTIVITIES	ADDITIONAL RESOURCES
Implement the Exercise & Testing Plan	Guide to test, training, and exercise programs for IT Plans and Capabilities NIST 800 - 84
Implementation of the Plan, Procedures and Strategies	Contingency Planning Guide for Federal Information Systems NIST 800 - 34