Table of Contents

Figures

Tables

List of Abbreviations

BC	Business Continuity
BCP	Business Continuity Plan
BIA	Business Impact Analysis
COBIT	Control Objectives for Information Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
DPC	Data Processing Center
DR	Disaster Recovery
ERM	Enterprise Risk Management
GC	Grupo Cortefiel
GEIT	Governance of Enterprise IT
IA	Internal Audit
ICT	Information and Communication Technologies
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
IT	Information Technology
RQ1	Research Question 1
RQ2	Research Question 2
SEC	U.S. Securities and Exchange Commission
SOX	Sarbanes–Oxley Act of 2002

1. Introduction

The introductory chapter presents the background of the research study. The chapter introduces the context, problem, purpose, research questions, delimitations and definitions concerning Enterprise Risk Management, Governance, IS/IT Risk and Business Continuity Plan.

1.1. Context

Information systems and information technology are elements present on almost every aspect that pertains the execution of business processes in an organizational context. Both IS/IT are intimately embedded within business enterprise architecture as the enabler of business process performance (Cusack, 2009). With the appearance of emergent technologies, it has become imperative to assess the organizational risks and the impact associated with IT deployment. IS/IT disruption can cause serious repercussions to business areas. Enterprise risk management (ERM) encompasses effective management of organizational risks through a risk assessment process. This leads to preparation for risk treatment, control and mitigation. Governance of Enterprise IT (GEIT) is concerned with both IT value delivery and the mitigation of IS/IT risks (COBIT 5, 2012). Therefore, the risk management function operates in a business/IT hybrid environment in which there is a need for continuous action for the proper identification, evaluation, control and treatment of business and IS/IT risks. In this context, risk assessment is a useful tool that empower organizations towards a secure environment, continuous improvement and provide resource allocation to mitigate potential threats (Nosworthy, 2000). There is a strong belief in the management practice that risk management provides the adequate tools for balancing the conflicts inherent in exploring opportunities and avoiding losses, accidents and/or disasters (Aven, 2011). Thus, corporate executives demand an answer from the IS/IT risk management function: How do we dramatically mitigate the IS/IT risk? Hughes (2006) discuss that the answer relies on treating IS/IT risk within the integrated framework of enterprise risk management. GEIT, together with a holistic risk management approach is required to align business processes with organizational IT capabilities in order to secure enterprise operations.

Enterprises that have a business continuity plan (BCP) implemented can reduce the risk of negative impact due to potential disruption of their business operations. Implementation consist on all the decisions and activities to turn strategic choices into reality (Favaro, 2015). BCP entails the proactive risk assessment approach for business processes and IS/IT key resources that support each process. The risk assessment includes the identification of key resources, vulnerabilities, threats and risks. The risk identification phase is performed during the business impact analysis (BIA) of the BCP to evaluate and implement risk controls. For this reason, business leaders need to take in consideration IS/IT risks during the implementation of a BCP (Cerullo and Cerullo, 2004).

Further exploration on what is facilitating the implementation of a business continuity plan and its benefits and challenges will be pursued utilizing a combined approach on risk management from a governance of enterprise IT perspective.

1.2. Problem

There is a lack of literature in the area of the organizational implementation of the BCP due to the fact that this is a new and emergent theme within IS and IT research. There exists gaps within the theory in the sense that BCP is seen more as an element of contingency planning instead of an opportunity for improvement. In addition, the increasing dependency on IS/IT function and its risk of failure contributes to make the subject complex and difficult to understand from stakeholder perspective. Therefore, the problem relies on identifying the elements that facilitate the business continuity plan, the challenges that organizations confront and benefits that organization perceives when performing this implementation.

1.3. Purpose

The purpose of this exploratory study is to assess how the implementation of a business continuity plan is conducted, together with its challenges and benefits, in an international retail and manufacturing enterprise in order to provide insights on what facilitates its implementation. The study seeks to provide a framework in the aim that enterprises are able to visualize it as a tool to understand the elements that contribute in the BCP implementation.

1.4. Research Questions

The following section includes the research question to be explored during the development of the master thesis:

Research Question 1 (RQ1): What facilitates the implementation of a business continuity plan in a multinational retail and manufacturing enterprise?

Research Question 2 (RQ2): What are the challenges and the benefits of implementing a business continuity plan in a multinational retail and manufacturing enterprise?

1.5. Research Disposition

Chapter 2 – Theoretical Framework: The chapter outlines key terms, such as enterprise risk management, governance of enterprise IT and business continuity. The chapter is divided in four sections. The first section presents the topic of Enterprise Risk Management and presents the frameworks that deal with the risk assessment process. The second section discusses the academic literature related to Governance of Enterprise IT and IS/IT risk assessment process. This section includes discussion on IT Governance, IS/IT risk categories and the construction of IS/IT risk scenarios that visualize the impact of IS/IT on business processes. The third section discusses Business Continuity Plan concepts and traditional approaches. It specifically focuses on the initial phase of the business continuity plan. The section articulates IS/IT risk assessment on the development of a business impact analysis and risk analysis. The chapter is finalized by the establishment of an initial theoretical framework for IS/IT risk assessment on a Business Continuity Plan.

Chapter 3 – Research Methodology: The chapter describes the methodological approach for the study. It explains the philosophical approach of the author, research design and research model followed by the description of the case study design. The chapter presents an argument for the chosen research methodology pertaining to strategy, design, data collection method and data analysis method. The chapter finalizes with aspects associated with the research setting: credibility, validity, ethical aspects and reliability of the study.

Chapter 4 – Group Cortefiel Case Study: The chapter portrays a general description of the selected organization that participated in the study together with the antecedents for the implementation of the business continuity plan and empirical findings.

Chapter 5 – Analysis: The empirical data is analyzed according to the themes covered in the study: Enterprise Risk Management and Risk Assessment, Governance of Enterprise IT and Business Continuity Plan Implementation. According to the empirical findings, each theme has been divided into sub-themes. Based on the analysis performed by matching the empirical findings with the theory, the chapter presents the final framework divided in two parts. The first part present an enhanced integrated view regarding ERM, Risk Assessment and GEIT in the implementation of a BCP. The second part presents a consolidated perspective on BCP Implementation.

Chapter 6 – Conclusions: This chapter aim to answer the research questions of the study.

Chapter 7 – Discussion: This chapter discusses the findings from the study in relation to the contributions been made to the theory and practical domains. Implications for research and practitioners as well as recommendations for further research are outlined in this chapter.

List of References: List the sources used in order to build the theoretical framework

Appendix: Depicts the supporting material derived from the case study interviews.

1.6. Delimitations

The study will not cover the testing and implementation of a business continuity plan. The study is framed utilizing a case study on a company that operates in the manufacturing and retail industry. The study do not seek to perform quantitative analysis on business and IS/IT risk assessment. The study seeks to provide qualitative findings applicable for any company, in disregard of the industry that operates.

1.7. Definitions

The definitions are divided in three separate areas consisting of:

1.7.1. Enterprise Risk Management

Activity

Process or set of processes undertaken by an organization (or on its behalf) that produces or support one or more products or services (ISO, 2012).

Business Risk

Risk that represent threats to the ability of an enterprise to execute business processes effectively and to create customer value in accordance with strategic objectives. (Bell et al cited in O'Donnell, 2005).

Business Impact

The result to the company following the destruction or complete loss of any of its assets, e.g. direct financial loss, embarrassment, loss of confidentiality, etc. (Nosworthy, 2000).

Business Process

Aggregation of activities and behaviors performed by human beings or machines to reach one or more outcomes. Performance is measured by the achievement of enterprise overall objectives in terms of quality, delivery and cost (BPM CBOK cited in Gonçalves C& Misaghi, 2014).

Control Activity

Measure that is modifying risk. Controls include any process, policy, device practice, or other actions which modify risk. Those measures implemented to counteract the impact from occurring. The severity of the impact will depend on the decisions that companies will make whether to accept, transfer, avoid or reduce the associated risk by implementing the relevant controls (Nosworthy, 2000; ISO, 2009b). Risk Control activities are regarded as the application of suitable controls to gain a balance between 'security', 'usability' and 'cost' (Nosworthy, 2000).

Enterprise Risk Management (ERM)

Process, effected by an entity's board of directors, management and other personnel applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO cited in Gordon at al, 2009).

Event

Occurrence or change of a particular set of circumstances. (Aven, 2011).

Information System (IS)

Integrated and cooperating set of software using information technologies to support individual, group, organizational, or societal goals (Boudreau, 2007).

Information Technology (IT)

Transmits, processes, or stores information (Boudreau, 2007).

IS/IT

Acronym that indicates information systems and information technologies across the document.

IS/IT Risk

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise (COBIT 5, 2013).

Probability

Measure of the chance of occurrence expressed as a number between 0 and 1 (ISO, 2009b).

Risk

The effect of uncertainty on objectives. An effect is a deviation from the expected (positive and/or negative). Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. (Aven, 2011).

Risk Analysis

Process to comprehend the nature of risk and to determine the level of risk: identify assets, recognizing the threats, assessing the level of business impact that would be suffered if the threats were to materialize and analyzing the vulnerabilities. The risk analysis results consist of estimated scenario frequency and impact, loss forms, and options to reduce scenario frequency and impact (COBIT 5, 2013; Nosworthy, 2000; ISO, 2009a)

Risk Identification

Process of finding, recognizing and describing risk. The process involves the identification of risk sources, events, their causes and their potential consequences. (ISO, 2009a).

Risk Scenario

Part of risk register that contains a detailed description of an IT-related risk that can lead to a business impact, when it occurs. It includes elements such as actor, threat type, event, assets/resource and time (COBIT 5, 2013).

Uncertainty

State, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequences or likelihood. (Avon, 2011).

1.7.2. Governance

Corporate Governance

The system/process by which the directors and officers of an organization are required to carry out and discharge their legal, moral and regulatory accountabilities and responsibilities (Bird, 2011).

Enterprise

Term used to describe a range of different organizations. It can consist from a commercial business, a public sector organization or a not-for-profit organization (Harmer, 2013).

Governance

Organizational body that ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options. Set direction through prioritization and decision making. Monitors performance, compliance and progress against the agreed upon direction and objectives (COBIT 5, 2012a).

Governance of Enterprise IT (GEIT)

Integral part of governance that addresses the definition and implementation of processes, structures and relational mechanisms in the organizations that enable both business and IT people to execute their responsibilities (COBIT 5, 2012a).

Management

Organizational body that plans, build, runs and monitor activities in alignment with the direction set by the governance body to achieve enterprise objectives (COBIT 5, 2012a).

Organization

Person or group that has its own functions with responsibilities, authorities and relationships to achieve its objectives (ISO, 2012).

Sponsor

The project sponsor is a critical link between the executive and strategic levels of the organization and the effective delivery of the benefits the project/program was created to facilitate. The governance processes that may be delegated to a project sponsor include developing processes to ensure decisions are in alignment with the organization's strategy and overall governance framework. Providing feedback to the strategic decision makers and governing body based on the special knowledge gained through effective sponsorship activities is also a responsibility as well as determining the criteria and methods to be used in the directing and supporting of the projects and programs being sponsored (Too & Weaver, 2014).

1.7.3. Business Continuity

Asset

Of value to an organization or individual that could reduce itself when exposed to a threat. Assets can be tangible, e.g. skilled staff, a computer system and intangible, e.g. company reputation or goodwill of the company and/or individuals (Nosworthy, 2000).

Business continuity (BC)

Holistic management process that identifies potential threats to an organization and, if realized, the impact that threats have on those business operations. Provides a framework for building organizational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, reputation, brand and value creating activities (ISO, 2012).

Business Continuity Plan (BCP)

A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level. (Bird, 2011).

Business Impact Analysis (BIA)

Process of analyzing business functions and the effect that a business disruption might have upon them (Bird, 2011). Develop a common understanding of the business processes that are specific to each business unit, qualify the impact in the event of risk occurrence and critical to the survival of an enterprise (COBIT 5, 2013).

Crisis

Occurrence which threatens the integrity, reputation, or survival of an individual or organization (Tammineedi, 2010).

Disaster

A physical event which interrupts business processes sufficiently to threaten the viability of the organization; unplanned event usually causing denial of access to premises and resulting in human casualties and great damage to property.
(Tammineedi, 2010; Bird, 2011)

Disruption

An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake) (Bird, 2011).

Incident

Occurrence (event) resulting in loss (Tammineedi, 2010).

Internal Audit

Audit conducted by, or on behalf of, the organization itself for management review and other internal purposes and which might form the basis of an organization self-declaration of conformity (ISO, 2012).

Outage

Event which causes a significant disruption to, or loss of, key business processes. The concept of an outage has both time dimension and business process dimension (Tammineedi, 2010).

Threat

A process which, when active, could destroy or damage things of value (Nosworthy, 2000).

Vulnerability

Intrinsic properties resulting in susceptibility to a risk source that can lead to an event with a consequence. A weakness in information controls or a loophole that can be exploited enabling the threat to happen (Nosworthy 2000: ISO, 2009b).

2. Theoretical Framework

The chapter outlines key terms, such as enterprise risk management, governance of enterprise IT and business continuity. The chapter is divided in four sections. The first section presents the topic of Enterprise Risk Management and presents the frameworks that deal with the risk assessment process. The second section discusses the academic literature related to Governance of Enterprise IT and IS/IT risk assessment process. This section includes discussion on IT Governance, IS/IT risk categories and the construction of IS/IT risk scenarios that visualize the impact of IS/IT on business processes. The third section discusses Business Continuity Plan concepts and traditional approaches. It specifically focuses on the initial phase of the business continuity plan. The section articulates IS/IT risk assessment on the development of a business impact analysis and risk analysis. The chapter is finalized by the establishment of an integrated view of IS/IT Risk assessment in the business continuity implementation.

2.1. Enterprise Risk Management perspective on Risk Assessment

Enterprise Risk Management (ERM) is an essential function of corporate governance that addresses the management of risks within an organization. ERM consist on the process for identifying and managing potential events that could affect the entity's ability to manage business risks such that they remain within its risk appetite (COSO cited in O'Donnell, 2005). ERM involves anticipating and managing business risks before problems occur rather than responding and reacting to threats after the fact, when the damage has already been done (Barton et al cited in O'Donnell, 2005). The ERM definition is complemented by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidelines *"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*" (COSO, 2004; Parent & Reich, 2009). This view on ERM position risk management as an important element that assess business risks while also acting as a control system. The goal is to increase stakeholder value by assessing the risks that can prevent the business to achieve its objectives. Furthermore, effective ERM can provide a significant source of competitive advantage for those organization that can demonstrate a strong ERM methodology. While there are organizations that are implementing ERM processes to increase the effectiveness of their risk management activities, Beasley, Clune and Hermanson (2005) perform research on why some organizations embrace ERM and others do not embrace the practice. Their research points out that, in part, ERM deployment is embraced when there is a strong level of leadership and support from corporate boards and senior management. The involvement of this governing bodies is critical to enact the ERM vision since they take accountability on overseeing the portfolio of risks that the organization faces.

Gordon, Loeb and Tseng (2009) depict ERM by addressing how firm performance is improved by acquiring a holistic risk management approach. This view is consistent with trends in corporate governance strategy that views ERM as an integrated approach for determining the business risks that impact an organization's ability to achieve its business objectives and to develop programs for managing the identified risks (Miccolis et al. cited on O'Donnell, 2005). Opposite from viewing risk management from a silo-based perspective, a holistic risk management perspective allows the enterprise to cover business risks associated with their internal and external context. Gordon, Loeb & Tseng (2009), asserts that a holistic ERM approach enables the organization to lower the risk failure, increase performance and create value. The authors argue that the relationship between ERM and firm performance is de-

pendent upon the link that exists between risk management and five critical factors that impact the organization. These factors are (a) environmental uncertainty, which cover the increasing unpredictability of future events affecting the organization; (b) industry competition, that pose a substantial risk to enterprise performance due to substitution of product and services by competitors that prevent the firm to earn sustainable level of profits; (c) firm complexity which increases the need for an appropriate ERM system that can produce integration of information and lessen the difficulties in management control systems within an organization; (d) firm size, which has relevance when considering the design and use of management control systems in the organization and (e) board of directors' monitoring, which active participation and encouragement influences the adoption of an effective ERM system (Gordon, Loeb & Tseng, 2009)

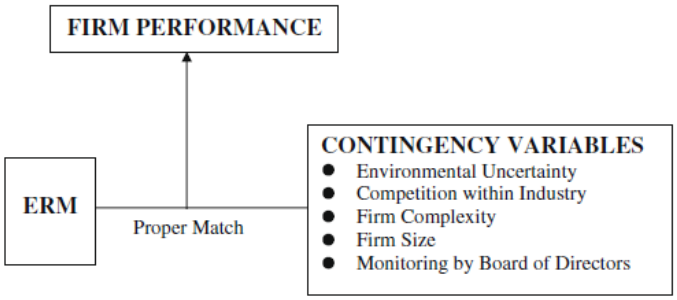


Fig. 1. Impact on firm performance of proper match between ERM and contingency variables.

Figure 2.1 - ERM and Firm Performance. Gordon, Loeb & Tseng (2009)

The authors suggest that there is a positive relation between the degree of the abovementioned five factors confronting a firm and its need for the implementation of an ERM system. O'Donnell (2005), also reinforce this notion by suggesting a holistic approach to risk management based on a systems thinking approach. The author emphasizes the need that enterprises have to assess the interdependence of enterprise components to determine overall performance. Systems thinking provides a comprehensive overview of the enterprise in order that decision makers better understand the behavior of the system and the risks associated with them. The theory implies that the constant iteration and refinement of business processes shapes organizational functions, structure and output. By performing organizational mapping, obtaining a comprehensive view of the relationship among its components and reviewing constantly changes that happen within the business environment, decision makers can manage business risks effectively (O'Donnell, 2005).

Organizations perform risk management activities in the aim to setting and pursuing objectives against an uncertain environment. The uncertainty arises from those internal and external factors that the organization does not completely control but that may lead the organization to not achieve its objectives. Risk therefore is neither positive nor negative but the consequences the organization experiences may vary from loss and detriment to gain and benefit (Purdy, 2010). Organizations that plan, design and implement an ERM system need to count with organizational leadership and direction that can set the tone for responsibility and accountability of enterprise risks. The risk management function must be framed within the decision making processes that governing bodies perform (ISO, 2009a).). Decision making mechanisms steer the direction in which the enterprise moves forward but also can bring on elements of risks that can affect the organization objectives and performance (Purdy, 2010).

The *ERM function in an organization* relies on the main governing body that oversee the risk management function are the board of directors and senior/middle management. The board of directors must have independence from management in order to perform appropriate oversight. The rationale behind this argument relies on the fact that an independent board can perform a more objective assessment of management actions. The independence of the board of directors is central for encouraging the adoption of ERM in the organization (Beasley, Clune & Hermanson, 2005). Since corporate boards often do not have the essential knowledge required to ask substantial questions about IT risk and expense, the Risk Management Committee can facilitate a board in corporate accountability and the risks associated with management, assurance and reporting. The Risk Management Committee responsibility includes disaster recovery risk on business continuity management, technology risk, operational risk and compliance (Posthumus, von Solm & King, 2010).

The appointment of a Chief Risk Officer (CRO) falls within the responsibilities of the risk management committee. The CRO aids in the implementation of risk management initiatives. This role is of relevance when promoting policies and procedures that reinforce risk management notions as part of the key enablers for performing risk management functions (COSO, 2004). Arena, Arnaboldi and Azzone (2010) discuss the organizational roles that participate in the ERM function. On the most detailed level, the authors note that risk uncertainty is addressed by risk management specialists that focus on traditional silos and are primarily concern with assessing quantifiable impact. CROs with internal audit serve as advisors who support managers in taking responsibility for risks assessment process while accountants are been encouraged to take an active approach to risk and link it with the organization performance management. Beasley, Clune and Hermanson (2005) suggest that in order for ERM to be implemented in an organization, the following factors contribute to accelerate the adoption of the practice: auditor type, organization size and industry type. Organizations that conduct their internal and/or external audits with high quality auditors, such as Big Four firms, have a strong commitment to pursue risk management practices. Furthermore, external auditors, who report independently to the higher governance body, review risk management activities and results to ensure that ERM procedures and structures are suitable for the enterprise. Auditors present their independent reviews and communicate them to senior management and the board of directors to take appropriate actions and maintain a consistent ERM framework (Doughtry, 2011). Organization size increases the scope of events that an organization may be exposed. At the same time large organizations can have a better ability to deploy ERM practices because they count with more resources. The industry in which an organization operates also has a great impact on ERM implementation due to the fact that global regulations required a risk management approach to business activities (Beasley, Clune & Hermanson, 2005; Abram, 2009).

The occurrence of risk is associated with the decisions taken while performing business activities. *Business risks* can come from different parts of the organizations or consolidate itself by being an interconnected component of the system, as suggested by O´Donnell (2005). Baker and Filbeck (2014) note the different types of *business risk categories* that exist. The degree of relevance of each category differs considering the type of industry the business thrives. Operational risk remain as one of the traditional risks in organizations. For the development of this study, the focus will be on governance, strategic and compliance risk. Governance risk consist on *"the inability to make the right decisions at the highest levels of organizations"*. Governance risk is structured on four dimensions: people, information architecture, structures and processes, and organizational culture. Strategic risk derives from changes in

society demand/supply or the utilization of new technologies that has an effect on how corporate strategy is addressed in an organization. Technology risk associated with the use of information systems and information technologies are contained within the boundaries of strategic risk. Finally, compliance risk involves the risk of not achieving regulatory and governmental requirements (Baker & Filbeck, 2014). This category covers the risk of noncompliance with applicable laws and regulations, contracts with vendors and customers (Marks, 2010).

Changes in the organization *environmental context* is at the core of ERM. For organizations to be able to keep pace with the emergence of new technologies, critical examination of the environmental context should be assessed (Cornell & Cox, 2014). The authors point out the inability of organizations to challenge their status quo. In fact, assuming that the organization system will not change and remain the same provides failure in monitoring current environmental risks like competitors, market trends and employee performance. Failing to examine and challenge the status quo can have serious implications in a changing environment because it can amplify and materialize the scope of organizational risks. O´Donnell (2005) points out that the impact of changing economic conditions, the level of competition in a particular market space, natural and man-made disasters, and political changes that influence regulatory control can have an effect on the organization environmental context. This effect may impact positively or negatively the organization according to the level of risk associated with business activities.

Organizations design an *internal control framework* to provides internal policies and generate compliance with procedures throughout their business activities. Management support for ERM initiatives is interrelated with the internal audit function. Internal auditors set the tone for laying out the internal control framework and there primary responsibilities within the organization relates to risk identification and assessment. For this reason, they are often engaged with senior management on ERM implementation issues and boost the creation of a risk management culture (Beasley, Clune & Hermanson, 2005). Posthumus, von Solms and King (2010) note that the internal audit committee is responsible for conducting performance reviews of an organization's system of internal control as well as for reviewing internal, legal and regulatory compliance efforts. Internal auditors focus on setting out best practices on internal control by looking deeper into an organization's risk management policies and procedures. Internal audit professional play an important role developing the ERM function as, often, they devote time and resources on the overall risk assessment process (Arena, Arnaboldi & Azzone, 2010).

O'Donnell (2005) discuss risk management from a systems thinking perspective. The author argues that the existence of performance factors within the organization internal control framework that can impulse risk events thus impacting the organizational value chain positively or negatively. This risk events and its performance are associated with the ability to execute procedures by organizational agents. He argues that procedure design, procedure support and procedure externalities can create internal business risks due to failures in internal processes. Procedure design is the ability to accomplish a business process and failure to design it in a satisfactory manner influence management ability to monitor performance effectively. Procedure support, in the form of a supporting infrastructure that connects value chain processes, include tangible resources and services.
The abovementioned procedures are executed by agents that requires skills, motivation and information in order to reduce risks associated with performing procedures. Agent skills re-

lies on document procedures in order to effectively execute supervision and training of internal agents while motivation centers on intrinsic and extrinsic incentives provided by the organization in order to motivate agents to perform well. Agents need information to take decisions while executing procedures. Effective performance is achieved when the agents have the appropriate information to make the correct decisions. Cornell and Cox (2014) note that legal and institutional frameworks are required to further define, clarify and enforce right, duties and procedures by agents in the organization.

Organizations need to define their level of risk appetite and risk tolerance. *Risk appetite* is defined as either the amount and type of risk that an organization is willing to pursue (ISO, 2009a) or as the amount of risk an entity is willing to accept in pursuit of value (COSO, 2004). Van (2009) notes that organizations lose appetite for risk when performance weakens as a result of conducting business activities in a difficult environmental context. Since risks cannot be eliminated, organizations need to define their risk appetite and move within the boundaries of *risk tolerance*, which consist on the maximum amount of risk the organization is willing to take in pursuit of its objectives (Van, 2009). When organizations are confident about their performance in the environmental context, Van (2009) notes that risk tolerance is high and thus decision makers tend to emphasize enterprise growth through acquisition. Aven (2013) examines both perspectives and states that the question is whether an organization possess appetite for risk or an appetite for the value-generating activities that involve risk. As a consequence, the author defines risk appetite as the *willingness to take on risky activities in pursuit of values*.

To perform effective risk management at an organizational level, a *risk culture* model should be instituted in the mindset of business process owners. Ernst and Young (EY) exemplifies a model for managing a risk culture within the organization by describing that risk outcomes are a combination of employee mechanisms and behaviors. Each of them reinforce and feed each other continuously in the form of a loop system. Mechanisms consist on organizational arrangements that collectively influence the way an organization is managed and the behaviors of employees. First of all, leadership is a mechanism that set the tone on how employees look at top leaders to seek for example on how to manage themselves and their activities in the organization. Leadership style develops from top to bottom and is where the perspective that manage risk behaviors is created and communicated throughout the organizations. Secondly, organizations need to provide a structure that effectively governs risk with defined roles and responsibilities. Clear structures underpin good risk behavior because they allow people to be held accountable for their responsibilities and actions concerning risk management. Thirdly, an internal risk framework provides a structure for managing risk appetite, clarifying risk levels and providing risk transparency. Last but not least, as mention in the previous section, incentives help individuals to appreciate managing risks related to their own work and feel rewarded for undertaking the right actions (EY, 2015).

A risk culture that have mechanisms for managing risks in the organization help reinforce employee behaviors by properly leading and influencing employees, analyzing and interpreting information correctly, making feel employees responsible and accountable for risk management, collaborating between departments, operating ethically and in compliance with rules, having an effective communication and managing risks to serve best customers and shareholders interest. Influencing behaviors through well establish organizational mechanisms in the organization signals progress on risk management initiatives, improves the way customers, regulators and external stakeholders view the organization activities and overall

improve the risk culture. Employee risk culture outcomes arise from the interaction of behaviors and mechanisms. Effective communication of the risk strategy needs to be in place to foster change on the organizational culture. Changes in organizational mechanisms offer the most tangible opportunity to achieve and demonstrate progress in regards of creating a risk culture (EY, 2015). An organization that proactively manages opportunities and threats through a consistent risk approach has a high maturity risk organizational culture embedded in the organization (Hillson cited in Cagliano, Grimaldi & Rafele, 2015).

2.1.1. Risk Assessment

ERM adoption of standards, framework and processes have been subject to debate by academic and practitioners in the field. Purdy (2010) notes that there have been several definitions of what constitute risk and the elements contained within the risk management process. Depending on the type of industry where an organization thrives and its characteristics (for profit, nonprofit, regulated or non-regulated), decision makers need to perform confident decisions regarding how to manage risks? Goble and Bier (2013) describe that risk assessments should be viewed as information technologies. The authors discusses that risk assessments are performed to solve a single defined problem and, after the problem has been solved, risk assessment is either put aside or make reference as a model for another risk assessment. When risk assessments are viewed as information technologies they have a much broader potential use in the form of repositories of structured information, medium for communication, allow asynchronous communication and have the ability to address uncertain futures. In providing risk management guidelines, each organization is able to review the risk components of its management system that suits the objectives of the risk management plan (Purdy, 2010). ERM guidelines are intended to provide a voluntary approach to risk management and are not intended as a prescriptive compliance or certification tool. Risk management principles and guidelines can be applied to any organization (either public or private), stakeholders interested in risk management process can use the guidelines as a global reference, risk management scope can be communicated in an organizational context and facilitate education and training programs on risk management in the organization (Dali & Lajtha, 2012).

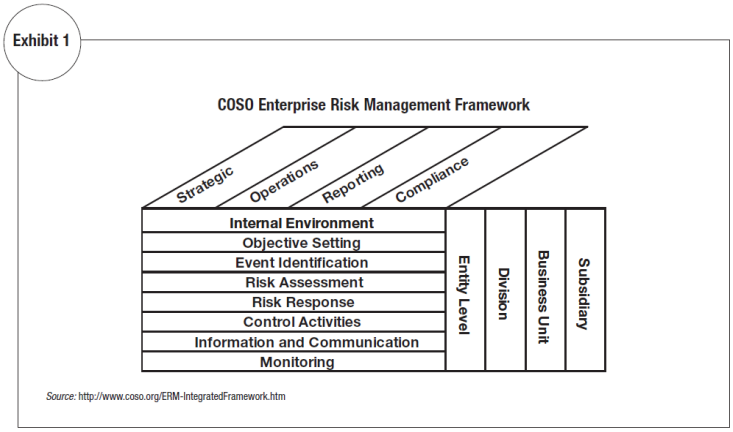


Figure 2.2 - COSO Enterprise Risk Management Framework

The definition of risk management processes establish the foundation for an internal framework. COSO (2004), guidelines state that an internal environment provides the foundation for fostering commitment, discipline and a sound governance structure that boost the risk culture. COSO provides an ERM integrated framework that guides business leaders when assessing enterprise risks (Parent & Reich, 2009). Complementing this view, ISO (2009a), depicts the risk assessment process as a series of steps that involves identification, analysis

and evaluation of risk. The process initiates with establishing the context, which consist on defining the objectives that the organization wants to achieve and analyzing the internal and external environmental factors that may influence objective achievement. Risk are identified, analyzed and evaluated according to the context where the organization operates. Risk treatment is the final deliverable that is produced as a result of conducting the risk assessment process (Baker, 2011). ISO (2009a), guidelines emphasize performance requirements to manage risk. This are embedded in the notion that risk management must create and protect value for stakeholders, be part of organizational business processes and decision making, address uncertainty, structured in a systematic and timely manner, tailored to the organization's needs, take account human and cultural factors and facilitate continual improvement (ISO, 2009a).

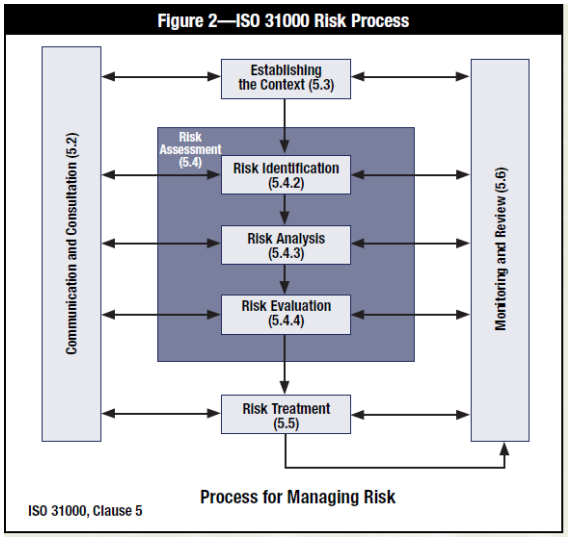


Figure 2.3 - ISO 31000 Risk Assessment Processes

The risk management process structure proposed by ISO will be used as reference throughout the rest of the following sections in order to obtain a systematic knowledge of the phases during the risk assessment process.

2.1.2. Risk Identification

Risk identification is the systematic process of understanding how risk could happen, how, when, and why (Purdy, 2010). COSO (2004) outlines risk identification as events that might threaten enterprise business process performance and this involves the development of a list of events that could affect the ability of the enterprise to meet its strategic and operating objectives. Management has the responsibility for identifying potential events that can have a positive or negative impact on business process performance (COSO, 2004). The two objectives during this phase are to consider a potential range of events and recognize the interrelation among the events. The identification phase starts by performing an analysis on the activities that an organization uses to execute its business processes. The risk identification stage include the collection of background information and the preparation of interview tools such as enterprise objectives, performance measures, audit reports, event summaries, benchmarking, historical data, questionnaires, and surveys (Fraser cited in Kmec, 2011). Risk identification standards that come from the classic ERM philosophy described on ISO and COSO frameworks focus on the property of uncertainty in the form of risk likelihood and risk impact for purposes of event identification. (ISO, 2009a; COSO, 2004).

COSO guidelines approach risk identification using general procedures that serve as a basis for identifying business risks. O'Donnell (2005) suggest a systems thinking approach for risk identification that includes assessment on the organizational value chain, the relationship among its components in the business model and a taxonomy category to analyze those relationships. The author concludes that a risk identification systems thinking approach can aim organization accomplish their objectives by providing a holistic perspective for event identification and by creating a framework for event identification based on a model that emphasize interaction among the components of a value system. On the other hand, Kmec (2011) proposes a temporal hierarchy for risk identification that considers how risk emerges, materializes and evolve as business activities progress over time. A hierarchical view of emerging risk provides a framework for identifying the conditions under secondary risks can evolve. While risk categorization helps decision makers to agree on a common language, the author considers that risk categorization reinforce placing risks on silos thus hindering cooperation between business areas. A hierarchy approach to risk identification breaks down risk causes and risk effects and derives from a general perspective into a more detailed description of identified risks. This method explores risk identification process based on risk relationships, evolution of risk and the movement of risk experienced overtime (Kmec, 2011). The author notes that a hierarchical view of risk is of special relevance when changes in the environmental context occur as a result of major events or decisions that have the potential of becoming a source of risk for the enterprise. Furthermore, the authors suggest that active risk identification of organizational flaws can be performed by testing internally the overall organization system and exploiting vulnerabilities in the aim of identifying weaknesses and strengths.

2.1.3. Risk Analysis and Evaluation

For purpose of presenting the literature review regarding this part of the risk assessment process, risk analysis and evaluation has been clustered in one section as this two components are highly interrelated. Aven and Zio (2014) describe risk analysis as the combination of knowledge about risk-related phenomena, processes, events, etc. and the application of concepts, theories, frameworks, approaches, principles, methods, and models to understand, assess, characterize, communicate, and manage risk. On a global scale, risk analysis gathers data and synthesize information to develop an understanding of each identified risk and the activities associated with them. It involves making a decision about how to assess each risk, how to rank risks and how to promote consensus within the different organizational actors (Purdy, 2010). Risk analysis and risk evaluation can be qualitative, quantitative or a combination of both depending on the enterprise approach to risk management (Purdy, 2010). According to the author, qualitative risk analysis, consist on *"the process of prioritizing risks for further analysis by assessing and combining their probability of occurrence and impact"*. Opposite to this approach, quantitative risk analysis consist on *"the process of numerically analyzing the effect of identified risks on overall project objectives"*.

Hansson and Aven (2014) address this issue of uncertainty by approaching risk analysis and risk evaluation from a scientific approach. This point of view states several kinds of deterministic and probabilistic models contributes to idealize the probability of occurrence for risk related phenomena. This models may include factors like level of occurrence, frequency, magnitude, impact and likelihood when evaluating the impact of risk related activities on business performance. Traditionally, the scientific approach of risk analysis and evaluation aim to provide an estimation for the probabilities and consequences of adverse events. Cornell and Cox (2014) emphasize that the quantification of risk prove useful when assessing the cumulative impact of risk on the organization and its stakeholders because it depicts

avoidable losses and highlight opportunities for improvement in the ERM activities. Quantitative risk analysis can be performed by analyzing the evidence through statistical methodologies like quantitative risk assessment or probabilistic risk analysis. This methodologies were initially developed on the engineering field to assess systems analysis, performance and causes for failure embedded on structural routines (Purdy, 2010). Qualitative risk analysis include adjudicating a risk criteria (low, medium, high), a frequency or likelihood of the event occurrence for each business risk related activity and then quantifying the impact according a consensus base definition from business stakeholders (Cornell and Cox, 2014).

COSO (2004) and ISO (2009a) provide guidelines for conducting risk analysis and evaluation activities yet does not provide a structural process to conduct the end result of this phase. The framework gives freedom to the enterprise to decide on the type of risk analysis and evaluation methodology as long as likelihood and impact are expressed. Furthermore, the analysis should contain the understanding of the current controls in place, reflect confidence on the risk level and be communicated effectively to stakeholders and business decision makers (ISO, 2009a). Developing a risk analysis can clarify the effectiveness and performance of risk management decisions as analyzing the causes of risk and its potential effects on enterprise performance is a valuable tool for reducing risk (Cornell & Cox, 2014). Risk analysis can be executed with a degree of variety that includes assessing the degree, purpose, information and resources available for the analysis. Addressing the interpretation of knowledge from different stakeholder point of views and the uncertainty component of each identified risk has been a subjective issue described in current academic literature (Purdy, 2010; Cox, 2012; Hansson & Aven, 2014). This stage of the process proves judgmental due to the fact that decision making covers a wide range of stakeholders concerns that need to be addressed with risk information from several sources. Finally, the main goal of conducting this activities is to set priorities in order to address risk treatment (Hansson & Aven, 2014).

2.1.4. Risk Treatment

Risk treatment, also known as risk response, constitutes the phase in which identification for risk control and mitigation activities are conducted. According to COSO, two elements are of vital importance: risk response and control activities. During this stage, management select and implement an appropriate risk response and treatment to each identified risk. This is done by the establishment of control activities as a response to each risk (COSO, 2004). Risk response covers the identification of proper actions for responding to risks, and aligning them with the organization's risk appetite. Cagliano, Grimaldi and Rafele (2015) reinforce this notion by placing risk response as the development of actions that increase opportunities and decrease threats. To complement this view, control activities can be seen as policies and procedures for ensuring that risk responses are effectively carried out (COSO cited on Arena, Arnaboldi & Azzone, 2010). Risk treatment involves a systematic approach to new controls or to the assessment of existing controls in the aim of implementing them as a countermeasure to mitigate previous identified risks. The purpose is to modify risk by attempting to reduce the magnitude of risk by determining a valid strategy to mitigate the occurrence of potential risk events. As a result, control activities arise as an outcomes of risk treatment (Purdy, 2010). Traditional risk treatment options include mitigation strategies such as the implementation of controls, accepting risk, sharing risk with partners or not undertake any initiative that induce to risk occurrence (Iliescu, 2010). In this context, management has the responsibility to decide which course of action take to mitigate risk and to ensure that control activities that treat risk are enforced and monitored for compliance with internal controls (Doughty, 2011).

2.1.5. Risk Communication and Consultation

The main objective of this phase is to create risk awareness, provide a framework for share understanding and communication during the ERM program. Dali and Lajtha (2012) discuss that the risk communication and consultation process should be approved at an organizational higher governing and should be instituted as part of policy decision rather than a process done on an "ad hoc" basis among the different levels of the organization. Cornell and Cox (2014) note that in order for the risk communication process to work efficiently, communication filters should work properly. Incentive structure and effective elicitation techniques can aim in the communication process in order to obtain risk information that otherwise will remain hidden from decision makers.

Risk communication is relevant when building up an organizational risk management culture. COSO (2004) states that risk communication needs to be established within the organization to enable employees to carry their responsibilities and to foster feedback mechanism that inform the extent in which the organization is accomplishing its initial objectives. Risk communication and consultation are continually acting as a reinforcing feedback loop together during the risk assessment process (ISO, 2009a). It is imperative that risk is communicated and consulted during the risk identification, analysis, evaluation and treatment process to understand stakeholder objectives, plan their involvement and ensure their views are taken into perspective when defining risk criteria (Purdy, 2010). Organizations that fail to convey risk communication and consultation message to business leaders involved in the decision making hierarchy encourage a culture of detachment from risk responsibility and accountability (Cornell & Cox, 2014). While investments on risk models and compliance structures functions have been heavily promoted at an enterprise level, Doughty (2011) note that few companies have invested on identifying the source in regards of poor risk information, delayed timing and relevance in the quality of information. This has a direct impact on the effective decision making process from the stakeholder standpoint.

2.1.6. Risk Monitor and Review

Risk monitoring is of vital importance since identified risks might change as a result of modifications in either the enterprise objectives or the internal or external environmental context in which the objectives are pursued. Risk monitoring involves a series of activities that engage stakeholders and risk owners on control assurance activities, dissemination of new information and constructing lessons learn from the analysis of the success or failures of control and/or mitigation strategies. To ensure that the organization is effectively governing the risk management framework, monitoring process must be in place to track performance overtime (COSO, 2004). This phase is the final step on the risk management process and continuously iterates with identification, analysis and evaluation phases in the risk assessment. It consist on the continuous management of new risks that become known during the risk assessment process, the procedures for monitoring the status of previously identified risks, the implementation of action plans and responses, risk mitigation status effectiveness, proposal of additional actions to countermeasure risk and the formalization of lessons learned about risk (Project Management Institute cited in Cagliano, Grimaldi, & Rafele, 2015). Finally, deliverables produced as a result of the risk assessment includes a risk heat map, description of key risk issues, status of mitigation actions to reduce risk, accountability and responsibility matrix, key risk and controls indicators and a historical portray of incidents and breakages. This deliverables exemplify the potential impact and likelihood within each risk categories associated with risks generated by business activities risks (Hughes 2006; Doughty, 2011).

2.2. Governance of Enterprise IT perspective on Risk Assessment

Recent corporate scandals and a major financial crisis in 2008 have demonstrated that major risks were either not identified, managed appropriately or ignored. Therefore, corporate governance initiatives have been impulse, in part, by the demands of New York Stock Exchange (NYSE) and London Stock Exchange (LSE) in regards of the companies that operate in the stock market (Nolan & McFarlan, 2005). To be able to be listed as at the stock exchange market, NYSE requires registrants to count with audit committees that assume specific responsibilities with respect to risk assessment and risk management, including assessing risks beyond financial reporting. Furthermore, through the Turnbull Report, the LSE requires companies to adopt a risk-based approach to establishing a system of internal control and reviewing its effectiveness (Emblemsvag, 2010).

New governmental guidelines have linked internal control to ERM and have extended the assessment of internal controls in order to include a wide spectrum of enterprise risks. Since 2002, a holistic approach to ERM has been driven by the enactment of the Sarbanes-Oxley (SOX) regulation in the USA. This regulation have had a worldwide impact on performing risk management on a process oriented based in order to protect shareholder and stakeholder value (Arena, Arnaboldi & Azzone, 2010; Bowena, Cheung & Rohdeb, 2007). SOX regulation set strict standards for internal controls through a risk management approach (Stanton, 2005). In Europe, Basel II Committee on Banking Supervision released a set of recommendation to financial institutions in which the improvement of operational risk management and the management information systems through clearly defined requirements (Mirela, 2010). As a result, ERM has emerged as a new paradigm for managing the portfolio of risks that organizations face and, based on this fact, policy makers continue to focus on mechanisms to improve corporate governance and risk management (Beasley, Clune & Hermanson, 2005). COSO has been a recognized ERM framework endorsed by the SEC as SOX compliant thus its relevance in the industry (Parent & Reich, 2009).

Beyond traditional financial risk reporting, information systems (IS) and information technology (IT) risks have been considered within ERM as fundamental enablers for decision making and for assisting on the development of business operations. There growing importance relies on the fact that stakeholders have a need to drive more value from IT investments. Management of an increasing array of IT-related risk has been essential for business operations and continuity (Cerullo & Cerullo, 2004). Following this line of thought, governance of enterprise IT (GEIT) aligns with the views of corporate governance to set a strategic direction for the business and IT units (Gonçalves & Misaghi, 2014). As a consequence, regulations like Sarbanes Oaxley and Basel II have served as a major catalyst for governing and managing enterprise IT.

ERM manages the assessment of IS and IT risk through a holistic view by exercising a GEIT approach. De Haes and Van Grembergen (2013) notes the underlying difference between IT governance and GEIT. The authors explain that IT Governance focus on the organizational capacity exercised by the board, senior management and IT management to control the formulation and implementation of IT strategy to ensure the fusion of business and IT. GEIT is an integral part of corporate governance that addresses the definition and implementation of processes, structures and relational mechanisms in the organization. The main difference relies on the fact that, IT Governance usually delegates responsibility for implementation initiatives to IT management while GEIT focus on the involvement of board and senior business management in strategic and tactical directions for IT (De Haes, Van Grembergen,

& Debreceny, 2013). The authors discuss that without the business areas involvement, business value from IT investments cannot be realized. It takes the common understanding and collaboration from the business side and IT to achieve business value creation. This enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled investments (De Haes & Van Grembergen, 2013).

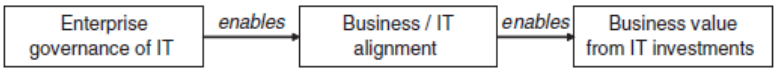


Figure 2.4 - Enterprise Gov. IT, business IT/ alignment and business value

De Haes & Van Grembergen (2013)

Control Objectives for Information Technology (COBIT) version 5 makes a clear distinction between the governance bodies that control the IT enterprise. The higher governing body main responsibility is to ensure that stakeholder's needs, conditions and options are evaluated. This is performed to determine balanced, agreed-on enterprise objectives to be achieved, to set direction through prioritization and decision making and to monitoring performance and compliance against agreed-on direction and objectives (COBIT 5, 2012a). On the other hand, management is in charge of plan, build, run and monitor activities in alignment with the direction set by the governance body to achieve the enterprise objectives (COBIT 5, 2012a). Performance setting, goal achievements and monitoring compliance upon agreed objectives between the governance body and management are all part of a structure ERM program oriented to the technology aspect. This is reinforced in the literature by Gordon, Loeb and Tseng (2009) that suggest there is a positive relation between the monitoring mechanism by a firm's board of directors and the use of a risk management system. For purpose of this study, Governance of Enterprise IT will encompass the topic of IT Governance.

Classic IT governance founders Weill and Ross (2004) explain that an effective IT governance requires a set of mechanisms that encourage behaviors consistent with the organization's mission, strategy and culture. The IT Governance Institute (2005) further discusses that *"Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise"* The domain of risk management within IT Governance exist to prevent IT catastrophes and, if they occur, to minimize and mitigate their consequences to the business. Parent and Reich (2009) denominate this approach as IT Risk Governance and emphasize that this consist on the minimum level of IT Governance that the organization should put in place.

IS/IT risk management consist on *"the process of identifying the vulnerabilities and threats from the framework of an organization as well as designing procedures in order to minimize the impact of them on IT resources"* (Gheorghe, 2010). From a governance on enterprise IT perspective, several authors have pointed out that the process of managing risks associated with the use of technological assets should be an integrated part of the overall governance framework (Iliescu, 2010; Gheorghes, 2010; Marks, 2010). Parent and Reich (2009) analysis on the main IT Governance frameworks propose the existence of three primary objectives of IT risk management: *security of data and information, the integrity of hardware and systems, and the implementation of IT projects.* Each IT objective requires a specific plan and procedure. The authors discuss that frameworks cover key IT resources such as data, application systems, technology, facilities and people. In addition to this resources, COBIT 5 (2012a) identify processes, organizational

structures, culture, ethics and behavior and principle, policies and frameworks as main enablers of the risk function.

Abram (2009) states that IT risk management is one component of the ERM program at an organizational level. The author discusses that within the scope IT risk management tend to focus on "hazard risks", which is the enterprise exposure as a result of the loss of enterprise technological assets. Utilizing an ERM approach, GEIT utilizes procedures to assess IS/IT risk management to minimize the impact that risks may have in the organization. This practices include IS/IT risk analysis, internal control efficiency monitoring, control implementation to reduce IS/IT risk and procedures for creating IS/IT risk transparency. Marks (2010) describes that risk management is a cornerstone of IT Governance by ensuring that the strategic objectives of the business are not jeopardized by IS/IT risk this this risk do not lead to systems failures. In this context, the author emphasize that while some organizations have separate IS/IT and ERM nonintegrated risk assessment, the IT auditor or the internal auditing department can provide added value by helping management to understand the need for a holistic ERM view that includes IS/IT risk across the organization rather than viewing IS/IT risk in a silo perspective. The nature of technology is in nature more complex than other disciplines thus IT is neglected by most governance boards in their strategic and risk management initiatives. Nevertheless, if governance of enterprise IT is ineffective, the governance boards may experience negative outcomes that impact enterprise performance. This negative outcomes may materialize on business losses, damaged reputation, higher costs and lower deliverable quality due to fail IT initiatives, performance decrease in core processes and poor quality of IT deliverables (Gheorghes, 2010).

Overall governance initiatives have been driven by the need for transparency of business risks, the preservation of shareholder value and the pervasive use of technology. Technology has created a significant dependence on technological resources that requires the IT organization to be governed effectively at a board level (Posthumus, von Solms & King, 2010). Nevertheless, integration of new technologies at an organizational level has presented management the challenge to redefine IT components in order to create business value while at the same time minimizing IS/IT risks (Gheorges, 2010). Main IT governance responsibilities include to align IT with the enterprise objectives, enable the use of IT in the enterprise by exploiting opportunities, maximizing benefits and have a responsible use of IT resources across the organization (COBIT 5, 2012a). These aspects are associated with IS/IT components and contain an element of risk that needs to be appropriately managed to ensure that effective IT performance is achieved (Iliescu, 2010). Thus the need to embed IS/IT risk management as not only part of the ERM approach but also as a fundamental component for GEIT. Since IS/IT represents both an opportunity and a source of risk, the organization should ensure that technology related operations, risks, and opportunities are managed to optimize enterprise performance (Marks, 2010).

2.2.1. IS/IT Risk Assessment

COBIT 5 (2012b), outlines the IT risk management process in the domain Align, Plan and Organize (APO). APO process # 12 "Manage Risk" describes the risk process as: *"continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management."* The purpose of this process aims to integrate the management of IT related enterprise risk with the overall ERM framework. The process supports the achievement of a set of primary IT goals included in the framework related to IT compliance, business compliance with external laws and regulations, management of IT business risk, transparency of IT costs,

benefits and risks, security of information, processing infrastructure and applications, delivery of programs benefits (on time and on budget) meeting requirements and quality standards (COBIT 5, 2012b).

ERM and an effective GEIT program should cover the assessment of risks related with the use of IS/IT resources on business activities. IS and IT are intimately embedded within business enterprise architecture as the enabler of business process (Cusack, 2009). The materialization of IS/IT risk can cause detrimental repercussions to the business and lead to a crisis. This may include reputational damage caused by identity theft, financial losses derived from systems failures and regulatory fines from non-compliance issues (Hughes, 2006). Since the materialization IS/IT risk do not happen on a stand-alone basis, it is relevant to obtain a comprehensive view of the relationship between business processes and IS/IT risk. COBIT 5 (2014) defines IT risk as a business risk. Specifically, the framework states that *"IT risk is a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."* The framework points out that risk lies on IT related events that could potentially impact the business. O'Donnell (2005) notes that business risks represent threats to the ability of an enterprise to execute a business process effectively and to create customer value in accordance with strategic objectives. In most enterprises, IT has become a fundamental constituent of the business and its function is of vital importance to reinforce, maintain and grow the business. This makes IS/IT a critical asset for the enterprise and its rapid evolution, at some extent, has changed the way that business processes are designed, maintained and implemented (Cusack, 2009; O'Donnell, 2005; Posthumus, von Solm & King, 2010).

IS/IT risk assessment in an organization can be either performed by the internal audit department as part of the ERM processes or as separate engagement. Often, internal audit perform the examination of IS/IT Risk on business processes. The multidisciplinary nature of the field makes more challenging for internal auditors the task to quantify risk. Hughes (2006) suggest that business leaders should develop an awareness of the nature of different IT risks to the business, quantify the impact to their business resulting from the loss of information or access to applications, understand the range of tools available to manage IT risk, align the cost of IT Risk management to the business value and construct an institutional capability to act and control IT risk with the same level of scrutiny as if it was a financial risk. The difference with the standard risk management guidelines and IS/IT risk assessment is that first of all, internal auditors should perform an inventory of the organization IT assets and recognize which the assets are critical to business processes performance. As a result, risks related to IT processes and activities are managed and assessed in relation their ability to impact the achievement of business objectives (Marks, 2010). IT risk assessments and IT decisions making require that IT risk be outlined in clear business terms. COBIT 5 (2012a) states that effective risk management needs an approach for mutual understanding between IT and the business over the types of risk that need to be addressed and provide justification on which risk needs to be managed and why. Marks (2010) emphasize that the IS/IT risk assessment function will depend on the state of maturity that exist at an enterprise level within the ERM processes and the level of integration between the corporate risk management strategy and IS/IT risk management

Information creates value to the business thus the need to protect this asset from preventing the materialization of risks. IS/IT risk business impact lies in the repercussions that the organization faces when information criteria is not met. COBIT 5 (2012a) describes the business requirements for information that express the condition to which information, as provided through IT, need to be preserved to be beneficial to the enterprise. The following table illustrates the business requirements for information:

Business Information Requirement	Description	Quality Goal
Effectiveness	Information meets the needs of the information consumer who uses the information for a specific task.	Appropriate amount, relevance, understandability, interpretability, objectivity
Efficiency	Relate to the process of obtaining and using information.	Believability, accessibility, ease of operation, reputation
Confidentiality	Restricted access to information	Confidentiality
Integrity	Information is free of error and complete.	Completeness and accuracy
Availability	Information is accessible when required by the user.	Accessibility and security
Compliance	Information conform to specifications covered by any of the information quality goals.	Compliance
Reliability	Information is reliable if it is regarded as true and credible.	Believability, reputation, objectivity

Table 2.1 - Business Requirements for Information. COBIT 5 (2012a)

The IT Governance Institute (2005) emphasize that technology essentially provides the enablement of new business models. IT strategy may even become so deep embedded in business strategy that it changes the way the organization thrives. Additionally, factors such as cost, risk and opportunity not only make IT a strategic asset to an organization's growth, it also causes it to be fundamental for an organization's continued existence (IT Governance Institute, 2005). Hughes (2006) and Marks (2010) provide insights on the effective management of IT related business risks. This authors present a consistent view in which organizations that embed value on their business processes through IS/IT need a structured approach for better managing IS/IT risk. This is done through a risk management program that can address new business risks arising for usage of IS/IT in its business processes. Indeed, there exist a connection between business process performance and the assessment of IS/IT risk. Related to GEIT, effective IS/IT risk management is also influenced by the IT strategy the firm pursue and the degree of dependency that the organization has on IS/IT resources. According to the nature of the products and services that organizations provide, Hérouxa and Fortina (2014) note that not all enterprises have the same degree of dependency on IS/IT resources and this influence the extent in which organizations deploy IT governance mechanisms. Based on research on IT utilization modes by Nolan and McFarlan (2005) the authors discuss the different type of IT dependence modes used in organization and the impact they have on IT governance mechanisms. For instance, firms that operate on support mode do not strategically depend on IT systems and can quickly revert to manual procedures for the bulk of value transactions. Firms that operate in factory mode highly rely on IT systems, as their operations depend on the internet, and business can be lost in the event of a systems failure. This type of firm do not proactively seek IT innovations for competitive advantage. In turnaround mode, firms are in the midst of a strategic transformation involving an important IT project, with the objective of gaining competitive advantages and cutting costs. Firms on turnaround mode are in a transitory stage, and firms subsequently move to a factory or strategic mode. Finally, in strategic mode, firms need reliable systems, but they also aggressively pursue IT solutions to take advantage of process and service opportunities, reduce costs, and develop competitive advantages (Nolan & McFarlan, 2005).

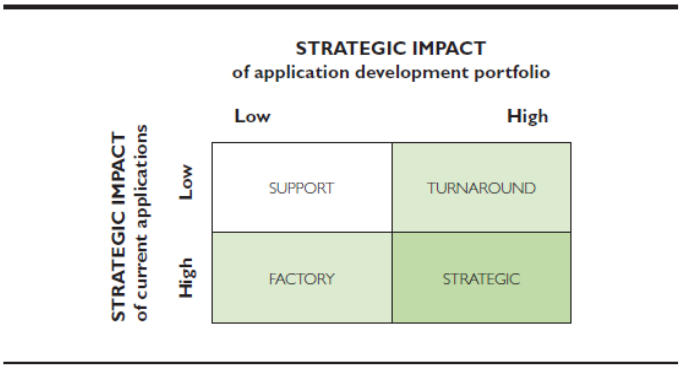


Figure 2.5 - IT Dependency Modes. Nolan and McFarlan (2005)

By drawing an analysis on this scenario modes, Hérouxa and Fortina (2014) conclude that IT governance mechanisms have a greater use in firms that have a strategic and turnaround modes relative to the firms that have a factory and support modes. In strategic and turnaround modes, the level of involvement of board members, senior executives, IT experts, and/or internal auditors involved in governance effort is higher. This level of engagement is important since the board of directors is the ultimately accountable for the organization's success and also responsible for the direction and oversight of the protection of its information. A lack of board-level insight about IT is unsafe because places the organizations at great a risk (Nolan & McFarlan, 2005). To address this responsibility effectively, it is important that the governance board undertake risk management on a continuous basis to ensure that all IS/IT related risks are identified and addressed. Therefore, governance mechanisms used to steer the direction of enterprise IT are influenced by the degree of dependency the organization has on IS/IT resources. The level of dependency on IS/IT has an effect on the level of involvement and commitment to IT initiatives that the higher governance body has towards GEIT. This approach has an impact on the relevance that IS/IT risk assessments have throughout the organization (Parent & Reich, 2009).

2.2.2. IS/IT Risk Categories

As previously noted, IS/IT risks are materialized when executed either by organizational actors together with a business process that brings value to an organization. According to its source, several authors have attempted to categorize IS/IT risk into clusters. This section explores the categorization of IS/IT risk based on the perspective of risk management authors and frameworks. From a governance body perspective, Parent and Reich (2009) address IS/IT risk categories as part of an IT Risk Governance chain. The authors discuss that IT risk management consists of a series of linked actions by actors, internal and external of the organization. The board of directors provide oversight on risk governance activities and value is created when a crisis is prevented and losses are minimized. Business continuity is a business risk that will be discussed in further detail in the section *2.3. Business Continuity Plan*. The following table summarizes the description of each category within the IT Risk Governance chain:

IS/IT Risk Category	Risk Description
IT Competence	From a board of director's perspective, it refers to the lack of IT knowledge and the inability to understand IT risk management impact on the firm's strategy and its risk profile.
IT Infrastructure	Risk of failure or interruption from the digital undercarriage of the organization - computers, networks, operating systems, applications, and databases- that provide the firm with its IT assets.
Business Continuity	Risk that an organization's internal weaknesses, threats, vulnerabilities create susceptibility to external or internal disasters thus causing disruption to enterprise operations. The Board of Directors address this risk by having in place a comprehensive and robust business continuity plan.
Information	Risk of non-compliance with data loss prevention policies, privacy laws, and anti-spamming legislation. Risk of not using data in an authorized manner. Lack of safeguarding data from intrusion, unauthorized use, or inappropriate modification.
IT Project	Risk embedded in the execution of large IT initiatives that has the ability to completely destabilize operations and put enterprise risk operations at risk due to changes in core processes.

Table 2.2 - IS/IT Risk Governance, Parent and Reich (2009)

From an operational perspective, Hughes (2006) divide IS/IT risk into six categories: security, availability, recoverability, performance, scalability and compliance. The following table summarizes the description of each category:

IS/IT Risk Category	Risk Description
Security	Information is altered by non-authorized people. This includes computer crime, internal breach or cyberterrorism.
Availability	Data is not accessible, such as the risk of system failure, due to human error, configuration changes, lack of redundancy in architectures or other causes.
Recoverability	Risk that necessary information cannot be recovered in sufficient time after security or availability incident such as hardware and or software failure, external threats or natural disasters.
Performance	Information is not provided when is needed, thanks to distributed architectures, peak demand and heterogeneity in IT landscape.
Scalability	Business growth, bottlenecks and silo architectures make it impossible to handle major new applications and business cost effectively.
Compliance	Risk that the management or usage of information violates regulatory requirements. This includes government regulations, corporate governance guidelines and internal policies

Table 2.3 - IS/IT Risk Categories. Hughes (2006)

From a business value perspective, COBIT 5 (2014) categorizes IT risk as a specific type of risk related to the delivery of expected benefits associated with business process performance. The framework combines both IS and IT into one category denominated IT risk. The first category is IT benefit/value enablement risk. This category is associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiative. The second category is IT program and project delivery. This category relates to the contribution of IT to new or improved business solutions, usually in the form of projects and programs as part of investment portfolios. The third and final category is IT operations and service delivery risk. This category is associated with all aspects of the business as usual performance of IT systems and services, which can bring destruction or reduction of value to the enterprise (COBIT 5, 2014). Furthermore, there are external factors that can put in risk an enterprise. From an external perspective, factors that are a driver for IS/IT risk rely on risks concerning natural disasters that may affect the technological infrastructure and platform of the enterprise. COBIT 5 (2013) out-

lines this risk under influence of the external context. COBIT 5 (2013) defines external factors that can drive IS/IT risk as those factors who circumstances can increase the frequency or impact of a risk event. This events are not always directly controllable by the enterprise and are compromised by those risk affecting the enterprise geopolitical situation. The external risk that can cause disruption on IS/IT services in the form of fire, flooding, earthquake, tornado, labor disputes and strike, lack of electricity and/or power supply, etc. In the next section, risk scenario construction will be examined in deep in order to visualize how IS/IT risk occurs in an enterprise.

2.2.3. IS/IT Risk Scenario Construction

IS/IT Risk scenarios are used by the enterprise leaders to construct a situation in which risk can materialize by affecting the operations of the enterprise. Risk scenario is a description of a possible event that, when occurring, will have an uncertain impact (negative or positive) on the achievement of the enterprise's objectives (COBIT 5, 2013). An IT risk scenario is a description of an IT related event that can lead to impact in the enterprise (COBIT 5, 2013). Realistic considerations of the risks under multiple scenarios can provide recommendations on how to control, act and mitigate risk under the influence of threats (Nosworthy, 2000). Risk scenarios are defined by business and/or IT leaders and they can follow a top down approach or a bottom up approach. The difference between the approaches relies on the fact that a top down approach perform an analysis of the most relevant and probable IS/IT risks that can affect the enterprise objectives. From this point, the risk scenario is developed in order to reflect alignment with enterprise value drivers. On the other hand, a bottom up approach follow the line of using a generic list of scenarios and customizing them according to the enterprise needs to illustrate risk situations (COBIT 5, 2013; Pareek, 2012). The following table illustrate the approaches for the definition of IS/IT risk scenarios:

Approach focus on	Top Down	Bottom Up
	Business Goals	**Generic Risk Scenarios**
1	Identify business objectives	Identify hypothetical scenarios.
2	Identify scenarios with highest impact on achievement of business objectives	Reduce through high level analysis.

Table 2.4 - Risk Scenarios Approaches, COBIT 5 (2012a)

The framework outlines that risk scenario analysis should consider enterprise past experiences and known events but also plan for future circumstances. The literature points out that risk scenarios must outline and be linked to real business risks in the situational context the enterprise thrives. Risk scenario has a structure and components that need to be considered by the enterprise. COBIT 5 (2013) outlines that the risk scenario construction must include the definition of actors that generate the risk or drive either threats or vulnerabilities. The risk scenario should identify the event and the threat type, which are fundamental to root the causes of the risk. The risk scenario should outline which assets or resources will be impacted. For the enterprise, an asset is any item that generates value to the enterprise and that, if affected, can lead to have a positive or negative impact in the enterprise. In contrast, a resource is an item or individual that helps to achieve IT goals (COBIT 5, 2013). In addition, Pareek (2012) notes that, during the analysis phase, risk scenarios should include the outcomes and its severity, controls in place and the frequency of occurrence.

Goble and Bier (2013), state that while risk assessments present different scenarios, their "what-if" capabilities can serve as an interface for establishing a constructive discussion among stakeholders that hold different values. IS/IT risk scenario analysis bring together technology risk professionals and business leaders together to address technological risk. With the help of business process owners and managers the impact of risk scenarios on the business processes can be identified (Nosworthy, 2000). It aids to establish a picture of what is likely to represent an adverse event or risk in the organization and aids in the establishment and evaluation of controls based on real situations faced by the enterprise (Pareek, 2012). Risk scenario analysis also helps the organization to visualize, within a certain range of probability, how a negative event may impact the enterprise. Performing this task requires an integral view and sponsorship from business and IT leaders and a thorough understanding of the environmental context of the business by the risk management team (Pareek, 2012).

2.2.4. IS/IT Risk and Information Security Risk

Information security is a business risk category that implies the interaction of a series of actors in order for risk to be materialized. Holmquist (2011) points out the specific differences between information technology (IT) risk and information security risk. The author defines IT risk as the *"risk of technology failing to perform in the manner in which it was intended."* IT risk involves the absolute failure of technology assets and the impact of associated with the misuse of this type of technology (hardware, servers, and applications). Concurrent with Hughes (2006), Holmquist (2011) views information security risk is as *"the risk of confidential customer or corporate information being exposed to unauthorized parties."* This is categorized as a business risk since information security risk involves the management of the information systems and is a direct outcome of the interaction between people, processes, technology, and external events. Information security and IS/IT risk management are risks that are interrelated since, in practice, they operate intrinsically. Abram (2009) includes the security aspect in the IT risk management process as he asserts that "*risk management provides the rationale and justification for virtually all information security initiatives."* The author states that information security exists primarily to manage risks to information and IT resources. This complements the efforts for making informed risk decision making from prioritized remediation efforts.

A risk that have shown an increasing prevalence during the last decade is cyber risk. This technological risk can be countermeasure with cybersecurity implementation and controls. The link between information security and IS/IT risk lies on the cybersecurity field of research. Cyber risk is an emerging IS risk that have aroused as a result of development of information and communication technologies (ICT) that have created opportunities for network penetration and malicious attacks. The damage caused by this attacks have a huge economic impact from a societal and economic perspective (Bisogni, Cavallini & Di Trocchio, 2011). Cusack (2009) notes that risk management has been an important aspect of security research though its articulation have had its limits. Cyber risk is an increasing IS/IT risk that is difficult to assess due to the fact that cyberattacks techniques are becoming increasingly sophisticated. A risk management approach to cybersecurity proves useful when mitigating the risk associated with external threats. Because of the sensitivity issue regarding cybersecurity and the negative business impact that this type of incidents have on reputation, confidentiality, and liability against the regulator, ICT companies that suffer from cyberattacks are very reluctant to communicate information about their attacks (Parent & Reich, 2009; Bisogni, Cavallini & Di Trocchio, 2011). Lack of information generates a biased cyber risk assessment and an underestimation of the potential loss. Bisogni, Cavallini and Di Trocchio

(2011) conclude that the improvement of cybersecurity risk information would create openness for obtaining knowledge on the risks that ICT companies are exposed and will support the decision making process related to cybersecurity investments.
Cybersecurity is only one of the many countermeasures derived from the use of IS/IT in the enterprise. The risk of not being cyber secure materializes when a series of system threats or vulnerabilities affects enterprise information systems operations. A threat is a process which, when active, could destroy or damage things of value (Nosworthy, 2000). A threat is a source of external risk to the organization. From a technical perspective on information security risks on business information systems, the following table depicts the main categories of technical threats:

Technical Threats	Description
Hackers	Persons who gain illicit or unauthorized access to computers. This is done by masquerading as an authorized user, exploiting vulnerabilities in passwords and weaknesses in the operating system.
Malicious Software	Includes viruses, macro viruses, logic bombs, worms, Trojan horses, malicious attachments,
Denial of Service	Accidental or malicious. Causes by physical failure (IT components), environmental failures (power loss or flooding) and by logical failures in the system.
Cybercrime and Electronic Fraud	Hacking, intercepting communications and/or manipulating network protocols.

Table 2.5 - Technical threats, Nosworthy 2000

Enterprises can be better prepared to assess and manage this risk scenarios through the implementation of a business continuity plan. The following section outlines the risk management approach on the context of the planning phase of a business continuity plan.

2.3. Business Continuity Plan

Business continuity management is a comprehensive program that aids organizations to design and structure a plan in order to react quickly and effectively when confronting unexpected interruptions. This include anticipating and mitigating the economic loss, reputation and compliance impacts of a crisis, disaster or emergency (Samson, 2013). A business continuity plan (BCP) is implemented in an organization to develop strategies based on the likelihood of the disruption of business process with a negative impact on the enterprise. The main objective of a BCP relies on ensuring the availability of business resources supporting critical business activities and operations in the event of a disruption (Nosworthy, 2000; Tamineedi, 2010). On the other hand, Lavell (2004) approach the implementation of a BCP as a contingency plan for the enterprise that allow operations to continue with minimal interruption. The author notes two different perspectives. From the regulator point of view, BCP focus rely on protecting customers and their assets. From the enterprise point of view, BCP allow the enterprise to survive in case of disruption on its operations. BCP constitute both a response from the enterprise to their stakeholders and regulators in case of a negative event of risk or a disaster that can affect operations. Business continuity focus on risk and governance to provides assurance to stakeholders in the market (Stanton, 2005). BCP contain a business continuity plan (BCP) and it constitutes a collection of procedures and information that have been developed, compiled and maintained in the event of an emergency or a disaster (Arduini and Morabito, 2010).

Early in the development of the field, Menkus (1994) note that IS and IT had a crucial role in the survival of most organizations thus business continuity should take measures to ensure that the organization fundamental activities are able to resume after a damage had occurred. This activities are to be restored at an acceptable level as quickly as possible. The author

assert that the telecommunications and computing processes used to carry out these activities should be considered in the plan. Arduino and Morabito (2010) describe a disaster as *"an incident that leads to the formal invocation of contingency / continuity plans or any incident which leads to a loss of revenue to the enterprise"*. Based on the standard BS 25999 on BCM from British Standard Institution, Tamineedi (2010) outline three major phases on BCM: pre-event preparation, event management and post event continuity management. The following figure outline the components of the phases:

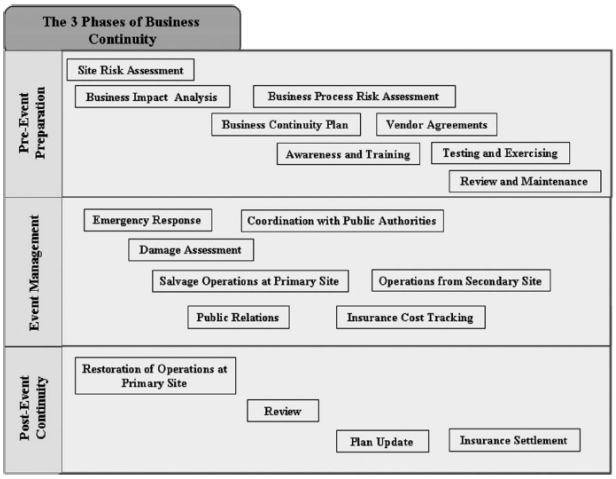


Figure 2.6 - The three phases of business continuity, Tammineedi (2010).

Pre-event preparation consist on the initial phase of identification of vulnerabilities and threats to the enterprise. This phase is fundamental in designing the response to negative events that arise from the risks the enterprise is exposed. Event Management and Post Event Continuity focus on the execution of the BCP and the activities that need to be conducted in an emergency (Tamineedi, 2010). BCP has gain increasing awareness in the industry due to the fact that corporate governance standards have given attention to safeguarding operations and enterprise value to stakeholders, shareholders and customers (Stanton, 2005). The prevailing focus have rested on the risk management approach organizations take when assessing their potential threats and vulnerabilities and implementing the BCP. In the digital networked business world, the nature of impact and the risk demands a BC approach because the growing dependency that exist on IS and IT can severely impact the enterprise (Stanton, 2005; Arduino & Morabito, 2010). Sources of risk and potential threats include natural disaster, malicious attack, user error, power failure, industrial espionage and geopolitical issues (Stanton, 2005).

Karakisidis (1997) presents a series of components for the realization of a BCP in the planning phase: obtain formal approval, establish a business continuity planning committee, perform business impact analysis, evaluate critical needs and prioritize business requirements, determine the business continuity strategy and associated recovery process, prepare business continuity strategy and its implementation plan. For purpose of the theoretical framework, the study will only cover the risk management aspects included in the pre-event preparation part of a BCP.

2.3.1. IT Disaster Recovery Plan

Research by the Guardian IT has pointed out that two thirds of the enterprises view business continuity management as an IT issue rather than a business issue (Gibb and Buchanan, 2006). In the past, the goal was to safeguard only the computer operations and the physical and virtual resources associated with them (Menkus, 1994). Often, disaster recovery (DR) efforts applied mainly to IS/IT systems and infrastructure. DR consist on the processes

that took place during and after an organizational crisis (Stanton, 2005). Business continuity planning, on the other hand, is the process of ensuring that an organization can survive an event which causes interruption (Stanton, 2005). Therefore, while IT disaster recovery (DR) addresses the restoration of business system software, IT infrastructure, services and data, business continuity focus on the recovery and continuity of critical business functions required to maintain an acceptable level of the enterprise operations during an incident (Menkus 1994; Samson, 2013). Restoring the operations in a central computing facility is the focus of an IT disaster recovery plan or IT contingency plan. However, the recovery process requires to handle the impact on the organizational key functions through a business continuity approach (Menkus, 1994).

Arduini and Morabito (2010) asserts that IT DR strategies must treat issues of IT and IS security within a wider internal-external, hardware-software framework. A BCP incorporates disaster recovery approaches but does not adhere exclusively to enterprise facilities. An integrated IS/IT approach to an IT DR strategy is to be included in a BC framework since the field does not focus uniquely upon IT problems but rather utilizes an enterprise holistic approach. To solely focus on the recovery of IS/IT activities is not enough to obtain a holistic view of the enterprise from the business continuity perspective. Therefore, input from all areas of the business, together with IS/IT, is needed to achieve this objective (Stanton, 2005). In the light of a BCP, DR plans are seen from a business wide perspective to enable advantages in the organization (Arduini & Morabito, 2010). Gibb and Buchanan (2006) emphasize that contingency plans, besides the plans made for the loss of technological assets, should be in place in the organization. Throughout the years, the approach from an IT DR plan have had an evolution to a BC approach through an understanding of the interdependencies of business processes and technology that creates value to the enterprise. Among all the activities contemplated in a BCP, BCP integrates IT and IS security with the business processes in the organization. BCP merges the function of management and technology to achieve a holistic view on technology and the business function it supports (Arduini & Morabito, 2010). The next section highlight the organizational actors present in the implementation of the BCP.

2.3.2. BCP Organizational Actors

During the implementation of the BCP, Arduini and Morabito (2010) discuss three essential components that deal with each other systematically: technology, people and processes. The authors discuss that technology focuses on the recovery data and applications within a disaster recovery plan. The emphasis on technology is on a more technical side that will allow to recover against incidents and protect information in a worst case scenario through IT emergency procedures. People refer to the recovery of the employees and physical locations while process refers to activities related to the implementation of the plan (Arduini & Morabito, 2010).

Since the origins of the field, several authors have remarked the importance of counting with sponsorship in the organization from the higher level of the enterprise (Menkus, 1994; Karakisidis, 1997; Samson, 2013). Menkus (1994) assert the existence of the difficulties that senior executives and the board of directors had on separating the organization IS and IT activities from the enterprise functions that this resources support. For this reason, senior management and the board need to understand the meaning of risk and the nature of the dependency on there IS/IT capabilities. To obtain management approval and support is a key issue in the implementation of BCP processes. This is influenced by the fact that enterprise leaders need to recognize as an enterprise problem the disruptive impact caused by threats in the organization (Karakisidis, 1997). Organizations must seek to acquire, first, the

support from the corporate level and, secondly, obtain senior management commitment to the business continuity operations (Samson, 2013). Funding and investment of time and resources for BCP supporting activities related to the development, implementation, testing and maintenance from the plan are needed to make a BCP a reality (Karakisidis, 1997).

As in a governance and program management structure, effective planning for business continuity defines role and responsibilities for decision making and communication structures within the organization (Samson, 2013). Within the organization, there are two essential groups that contributes in the development and implementation of the BCP: program management and internal audit. During the planning phase of the BCP, program management act as a logistic actor that manages the effort of conducting BCP activities. Internal audit brings an enterprise view to the BCP and ensure validation and monitoring of organizational resources (Samson, 2013). Furthermore, an important factor in the implementation of a BCM initiative is the CIO. Gibb and Buchanan (2006) state that the CIO has a fundamental role in promoting the adoption of a business continuity plan, ensuring that the rapid and effective recovery of core business systems can be accomplished and guaranteeing the protection of enterprise information assets through plans, procedures and policies. Melton and Trahan (2009) address the interrelationship of the actors in the coordination of the BCP. The authors state that when operations and risk management areas understand and discuss the risks to the organization, they can collectively determine what measures are needed to mitigate the risks against threats in the BCP. This highlights the importance of coordination between operations and risk management in the drafting and execution of the business continuity plan. Therefore, to achieve consensus among business areas in regards of the technology, people and processes in the organization that are to be included in the BCP, priorities need to be set based on the critical assets and activities that the enterprise need to protect (Stanton, 2005). To achieve this consensus is an underlying issue since organizations should recognize that incidents that have a potential impact or disruption in the organization could be largely driven by external causes. However, the impact of those incidents, at a great degree of extent, are determined by internal factors that remain within the control of the organization (Arduini & Morabito, 2010).

2.3.3. Risk Management through a Business Impact Analysis

During the early stage of the planning phase of the BCP, several authors have noted that business continuity efforts should center on performing identification and assessment of the assets that need to be protected before looking at the possible causes of disruption (Karakasidis, 1997; Stanton, 2005, Tamineedi, 2010; Samson, 2013). This is based on the fact that, to compute the underlying causes of disruption or loss of key enterprise activities, is very uncertain. An approach to both of this issues is performed through risk management (Karakasidis, 1997; Stanton, 2005). Nosworthy (2000) propose a structured approach on risk management and BCP. Business continuity strategies are based on the risk analysis of the enterprise functions, resources and assets.

When assessing the risks that the enterprise faces, security and risk management support the business continuity strategy by reasonably managing risk and maintaining them at an acceptable level (Stanton, 2005). In this context, risk management plays a significant role in the identification of threats, minimizing damage and the implementing measures aimed at reducing the likelihood of the occurrence of those threats (Nosworthy, 2000). BCP adopts a holistic view to the enterprise by focusing on the concept of continuity of the key processes (Tamineedi, 2010; Samson, 2013). This is supported by the fact that to focus on an individual business functions or process, will result on the detriment to the overall BCP efforts in the

enterprise (Tamineedi, 2010). Similar to an ERM approach, a holistic view to the enterprise is driven by an interplay between technology, people and processes in the convergence of a BCP implementation. It begins by a phase of identification that includes the critical aspects and components that enable key operations, the resources needed for enterprise functions, the stakeholders affected by a disruption and a list of internal and external threats that may harm the enterprise negatively.

Business continuity planning foundation rely on a planning phase that includes the realization of a risk analysis through a business impact analysis (BIA) (Tamineedi, 2010). The BIA constitutes a component of risk analysis and assist on the identification and prioritization of enterprise functions and processes. The purpose of the BIA is to *"identify the company's critical business processes and the damage, disruption or loss that may be caused to the organization should there be any degree of disruption in service*" (Nosworthy, 2000). Business wise, Menkus (1994) provides a practical approach in conducting this task. The author states that an organization should classify its essential business activities and then assess the value of the business transactions if they are to be lost due to an event of disruption. Technology wise, a BIA guides the enterprise leaders in determining the level of IS/IT necessary to achieve a minimum level of service and have operations running in an accepted time frame (Wagner, 2007). Activities during the BIA include the evaluation of enterprise functional areas and business processes in order to measure the probable impacts from the unavailability of the operations. This is accompanied by the identification of each of the business processes performed in the units or departments. A rating on the level of relevance of each business process based upon the impact of its unavailability and its priority for recovery is assigned. An important consideration on the BIA is to assess the time sensitivity of each business process to obtain insights on how and when is the worst time for a disaster to occur (Tamineedi, 2010). The BIA also sets the recovery times for the critical areas and business processes identified. The ultimate objective of conducting a BIA is to analyze all the alternatives and strategies that are available to resume core business and associated IT functions and services in the enterprise (Karakasidis, 1997). Afterwards, determining minimum and maximum period of disruption for identified critical functions is performed (Samson, 2013).

Karakasidis (1997) emphasize a risk reduction program throughout the BCP planning process to identify and assess potential threats. Risk analysis support the decision making process on what type of control is needed based on a risk categorization (Nosworthy, 2000). After performing a BIA, risk analysis is in charge of identifying the risks that could impact the key enterprise functions and processes previously outlined, assign the probability of those risks and their likelihood of damage, perform an assessment of the vulnerabilities of enterprise assets to those risks and evaluate the controls that needs to be put in place to reduce the impacts (Nosworthy, 2000; Samson 2013). During the risk analysis phase on BCP, management is able to identify where in the enterprise resources should be allocated. If threats were to be materialized, risk analysis provide assessment on the threats, level of business impact, BC controls, and degree of the vulnerability of the impacted asset (Nosworthy, 2000). After obtaining a clear understanding of all the business operations through the BIA, risk management identifies risks within business operations. This risks can be materialized either in the form of external catastrophic events or in contingent impacts (Melton & Trahan, 2009). Business process risk analysis is broken in two parts: effect and impact of the risk event. The effect of the risk event pertains to the damage or loss adjudicated to a process or service and the impact of the risk pertain to the business consequences that could either result on economic, regulatory and reputational repercussions. (Nosworthy, 2000; Gibb & Buchanan, 2006). As part of the BIA, the risk analysis should include the description of the risk, source

of the risk, severity of the risk, controls being applied to the risks, risk owners, mitigation strategies for reducing risk exposure and the time frame (Nosworthy, 2000). The following figure depicts the risk management approach through a business impact analysis and a risk analysis on BCM:

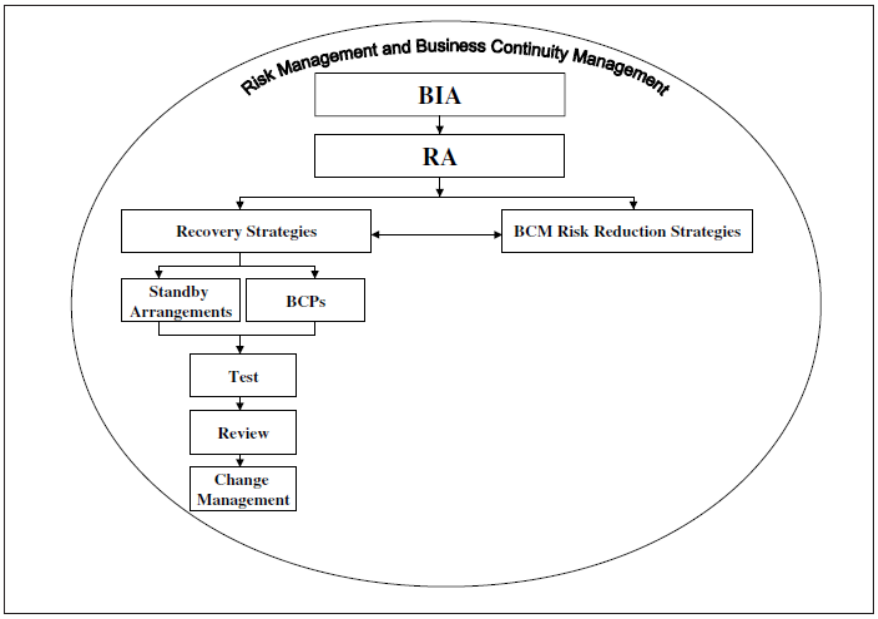


Figure 3: RM and BCM

Figure 2.7 - Risk Management and BCM, Nosworthy (2000)

Organizations creates loss impact scenarios to develop a sound image of the threats exposure and examine the organizational view on this issues (Stanton, 2005). During the development of the BIA, a "worst case scenario" approach is conducted to estimate the effect of disruption on business functions at a critical business location (Tamineedi, 2010). Results of the risk analysis are utilized to create impact scenarios that depict how, in the events of risk, the enterprise is affected (Samson, 2013). Operational business risks, under the light of risk scenarios, includes business risks associated with delay and service interruptions.

The impact in the scenarios is rated using a higher level qualitative risk analysis approach. Nosworthy (2000) justifies this approach by stating that, because the majority of threats to information systems defy probability analysis, risk analysis should be carried on the basis of business impact. Qualitative risk analysis is done by assigning a low, medium or high rate to the threat based on the judgement of those performing the task, which often are business process owners. The purpose of conducting a BIA and risk analysis in the organization during the implementation of the BCP is to establish the exposures to threats that the organization faces in order that business and IT leaders can have the necessary information to perform decision making on the enterprise critical functions and areas in regards of risks (Nosworthy, 2000). As a result of the analysis phase, the organization can elaborate a map in which prioritization of vulnerabilities against risks are visualized. Moreover, the enterprise will count with a view of which business process risk can be escalated and grouped to identify priorities for business continuity investment (Gibb & Buchanan, 2006).

2.4. Initial Framework

The preceding sections have outlined a comprehensive view of the components of enterprise risk management, governance of enterprise IT and business continuity planning. This section integrates the interrelations and characteristics of the three topics into a holistic view of the enterprise to provide an initial framework on the enterprise organization in regards of the implementation of a BCP. The developed framework aids to establish the relationship between the topics and provides a visualization of the enterprise system. Guenther (2012) outlines four framing aspects that can be used by the researcher to guide conceptual modelling direction: business, people, function and structure. This four framing aspects are linked to the components of the design minded enterprise: holistic understanding, systemic modeling and enterprise vision (Guenther, 2012). Based on the design minded enterprise, the four framing aspects together with the development of the direction for establishment of a conceptual modelling, aims to depict the relationship between the concepts in a process of iterative inquiry and adaptation of the model. The complexity embedded by the utilization of technology in the enterprise encourages the creation of a model in a systematic manner. The following figure represents the integrated view of IS/IT risk assessment in the implementation of a business continuity plan:

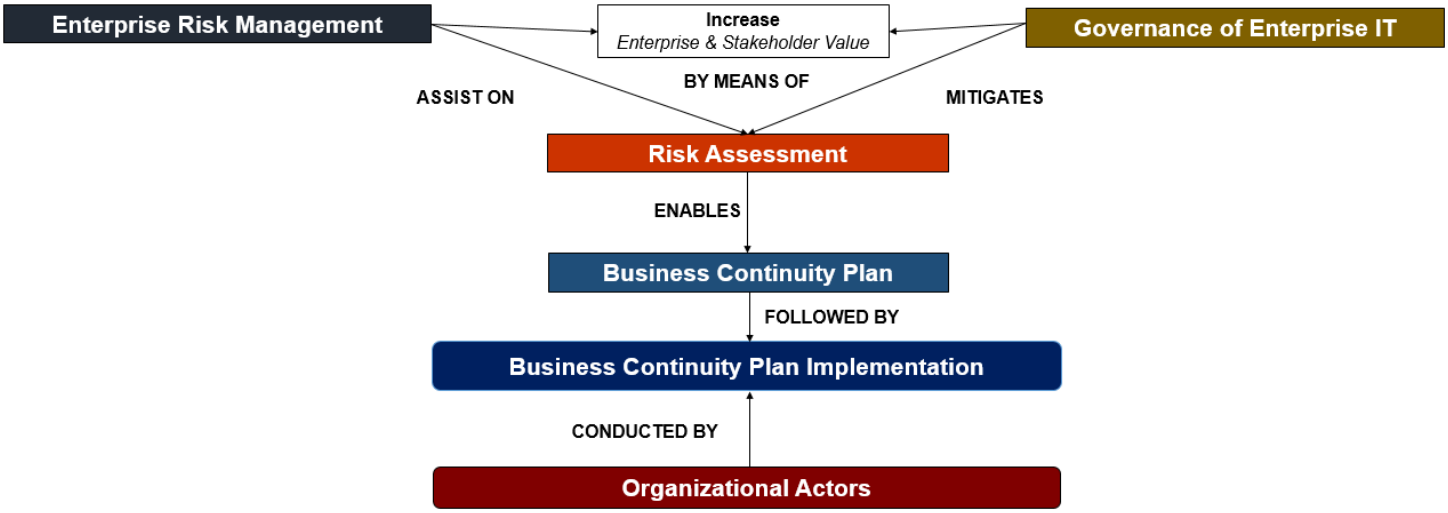


Figure 2.8 - Integrated View of IS/IT Risk assessment in the BCP implementation

2.4.1. Risk Assessment: Enterprise Risk Management and Governance of Enterprise IT

Enterprise Risk Management **assist on** conducting risk assessments in the organization. Information from risk assessments influences how and why the Board of Directors and Senior Management take decisions at an enterprise level. ERM function is supported by strong leadership from an independent organizational body that allows the creation on an internal control framework aided by organizational agents and the establishment of procedures. ERM aids the organization in setting their risk appetite and risk tolerance levels. A mature risk culture with leadership, risk governance structures and an internal risk framework set standards to deal with ERM factors regarding environmental uncertainty. Firm complexity, size, industry type and the exercise of monitoring from the Board of Directors also play an important role in the implementation of the ERM function. Organizations that have the presence of an external auditor tend to strengthen their risk management function. Often, this function is exercised by the Chief Risk Officer together with Internal Audit department

and covers a holistic integrated approach view of the enterprise risks from an operational, governance, strategic and compliance perspectives.

Governance of Enterprise IT **mitigates** IS/IT risk by focusing on providing enterprise benefits realization. The bodies that enable GEIT are separated between governance and management. Enterprise objectives in regards of the utilization of IS/IT are to be ensured due to the fact that business processes have a strong dependency on IS/IT resources and capabilities. An IS/IT risk analysis is to be conducted in order to achieve internal and external regulatory compliance to reinforce the internal control framework of the organization. To perform a risk analysis, IS/IT Risk scenarios are to be developed taking in consideration how given situations related with the use of technology have an effect on business processes. IS/IT risk analysis take into consideration the key IT resources that the organization possess to enable business processes. This resources are data, application systems, technology, facilities and people. This resources are embedded into processes, organizational structures and culture, ethics and behavior of employees. Enterprise policies, principles and procedures direct how the organization utilizes key IT resources. GEIT aims to provide assurance on the utilization of information for business purposes based on the criteria of information effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability. This provide assurance in the organization against the materialization of IS/IT risks that can have an impact on security, availability, recoverability, performance, scalability, governance and compliance of information resources. Increase threats to IS/IT key resources and capabilities include hacker intrusion, malicious software deployment, denial of service and risk associated with cybercrime and electronic fraud. GEIT creates a link between the enterprise and IT in order to make IT a strategic asset to the organization growth and guaranteeing the existence.

2.4.2. Business Continuity Plan

Supported by ERM and GEIT, risk assessment **enables** the enterprise to mitigate IS/IT risk embedded on the realization of business processes through a business continuity plan. IS/IT risk is assessed by performing identification, analysis, evaluation, response and treatment, communication and consultation and monitor and review of the risks faced by the enterprise. During the planning phase of the BCP, risks need to be assessed in order to identify weaknesses, threats and vulnerabilities of the enterprise. BCP aims to safeguard enterprise operations and value and takes two distinct approaches. Governmental regulations aim to protect enterprise customers from any business disruption that can affect its assets. The enterprise view BCP as a method that can enable them to survive in case of a business process disruption that negatively affect the enterprise. BCP conducts risk assessment through a business impact analysis (BIA) and through qualitative risk analysis. The first method identify the critical aspects and the components that enable key operations while the latter identify risk that can impact key enterprise functions and process through the development of risk scenarios. An IT disaster recovery plan serve as a platform for identifying how IS/IT key resources interact during the execution of a business process and serve as a document that is an antecessor for the realization of the BCP.

As part of the BIA, ERM can assist on the risk analysis to consolidate risk management in the organization. Risk management identifies the description of the risk, source of the risk, severity of the risk, controls being applied to the risks, risk owners, mitigation strategies for reducing risk exposure and the time frame. During this risk assessment, both business and IT functions are examined to assign probability and likelihood of damage on identified vul-

nerabilities and threats. Risk Management function evaluate and implement controls to reduce the impact and effect of disruption on enterprise operations. Disruption on business processes supported by technology have an effect in the enterprise due to damage loss adjudicated to a process or service. The effects of the impact in the enterprise are observed through the consequences of that the enterprise experience in terms of economic, regulatory or reputational repercussions.

The **business continuity plan implementation is conducted by** organizational actors in the enterprise. A holistic approach to BCP integrates the functions of ERM, GEIT and risk assessment. During the implementation of the BCP, the higher governance bodies set the tone for identifying critical business areas and processes. Internal Audit and program management support the activities related to the implementation of the BCP. The convergence of this factors is followed by the BCP implementation in the organization.

Refer to be Appendix D to visualize the extended framework components of the integrated view of IS/IT Risk in the implementation of business continuity plan.

3. Research Methodology

The chapter describes the methodological approach for the study. It explains the philosophical approach of the author, research design and research model followed by the description of the case study design.. The chapter presents an argument for the chosen research methodology pertaining to strategy, design, data collection method and data analysis method. The chapter finalizes with aspects associated with the research setting: credibility, validity, ethical aspects and reliability of the study.

3.1. Philosophical Perspective

When initiating a research study, the author needs to embrace a philosophical perspective that aids to steer direction for the research method. Research philosophy is the way researchers develop knowledge in their specific field of interest. By definition, the philosophical perspective contains assumptions on how researchers view the world. Thus this assumptions determine the path that the method will undergo during the development of the study. Interpretivism focus on the necessity of understanding the role of social actors among humans from a researcher point of view (Saunders, Lewin & Thornhill, 2009).The author position the philosophical stance on interpretivism. Because risk occur on a particular set of circumstances with individuals interacting together at a specific time, social actors play an important role on the assessment of IS/IT risk and on the implementation of a BCP. Therefore, the author strongly believe that interpretivism is the most appropriate for conducting the research.

Each philosophy can be classified into the three research paradigms: ontology, epistemology and axiology. The research paradigm concerning ontology refers on how researchers view the reality or world. From an ontological perspective, the researchers can adopt external and multiple views to obtain a complete answer to the research question (Saunders. Lewin & Thornhill, 2009). Epistemology consist on the researchers view on what can be considered as acceptable knowledge. To be able to have a comprehensive view on the matter, the researcher is bounded to adopt a practical position for data interpretation through the observation of phenomena and the analysis of subjective meaning. Axiology takes in consideration the role that the researchers values have on the development of the study thus the relevance on the adoption of subjective and objective stances during research development (Saunders, Lewin & Thornhill, 2009).

A researcher must make a stance on the chosen philosophical perspective. The author position her philosophical perspective on interpretivism from an ontological, epistemological and axiological stance. From an ontological stance, the author believes that business and IT leaders have a difficult interaction when assessing IS/IT risk. This is further complicated by the fact that a business continuity plan needs inputs from stakeholders that, often, cannot communicate using the same business terms. The interpretivism ontological stance, where social phenomena is developed from the perceptions or actions of the social actor (stakeholders) is referred as constructionism (Saunders. Lewin & Thornhill, 2009).

From an epistemological stance, the author accepts as valid the output she has observed during her role as an enterprise risk management consultant on Big4 audit firms. Contact with head of IT departments, external consultants, project managers and the observation of supporting documentation (unit of analysis) during the case study will provide subjective meaning to the information that needs to be analyzed to place the end result into context.

IS/IT risk happens under uncertain conditions though the subjective view of knowledge from each stakeholder is based on its individual's experience.

From an axiological stance, the author finds valuable the topics in the research as she is interested in the interplay between governance structures, enterprise risk management, IS/IT risk and business continuity management in order to properly assess technological related risk. The author appreciate the knowledge acquire and the results of this study as she believes it will actively contribute in her career path as an enterprise risk management professional. Furthermore, the author plans to use the knowledge to enhance her possibilities to pass the examination and obtain the risk information systems and controls certification (CRISC) from ISACA in the future. The author plan to extract this value from the case study. Though the author´s values are bounded with the research.

3.2. Research Approach

The author adopts an interpretivism research philosophy with an abductive approach. The research approach consist on the way the author makes use of the theory during the development of the study. As Saunders, Lewis and Thornhill (2009) states that there can be a combination of methods when designing the research approach. Deductive theory test a proposition or hypothesis from an existing theory, in order to verify or reject the hypothesis (Bryman & Bell, 2001, p.11; Saunders et al., 2009, p.124). Yin (2011) states that, through a deductive approach, the concepts in the theory leads to the researcher to the definition of the relevant data that needs to be collected. The deductive part of this study is represented by the framework created as a result of the development of the literature review. The initial theoretical framework has been developed through the analysis of existing research and theories in the fields of ERM, GEIT, IS/IT risk assessment and BCP. A deductive research helps the researcher with acquiring previous knowledge on the subject and for the exploration of the situation or problem.

The exploratory part of the research is done through an inductive theory. Inductive theory is concerned with the development of emergent concepts or new theory through the acquisition of data. An inductive approach seeks to explore the focus of the research and, through a diverse set of methods, generate theory from the research (Yin, 2011). Though the author do not seek to generate new theory, the aim is to enhance the theory through a set of inductive methods. The inductive part of the study derives from a case study design and semi structured interviews with open ended questions.

The author seeks to use both deductive and inductive approaches to constant move from the empirical to the theoretical dimensions of the analysis. This combination of both deduction and induction in the research approach is denominated abductive. Abduction is defined by Lewis-Beck, Bryman and Liao (2004) as the pragmatic way to construct descriptions and explanations that are grounded in gathered data from activities, discourses, concerns, motivations and meanings used by research participants in a study. In interpretative and case study research, abduction is based on empirical facts and does not dismiss ideas that come from a theoretical background. Abductive theory allows the author to assert conclusions about what is the underlying cause of an observed phenomena without manipulation of the causal factors. Abduction differs from the deductive and the inductive modes of reasoning and implies an *"inference to the best explanation*" (Lukka & Modell, 2010; Dubois & Gadde, 2002).

3.3. Research Strategy

Bryman and Bell (2011) depict four research strategies that provide a framework for data collection and data analysis to the researcher: case study design, experimental design, cross-sectional design and longitudinal design case study. In order to conduct the development of the study, the author is required to choose a research strategy that reflect best the priorities set in the research process. This study focus on examining what is facilitating the implementation of the BCP together with the challenges and benefits that the implementation brings to the organization. In this context, the researcher has chosen a case study research as the research strategy because it will allow to rely on multiple sources of evidence, benefit from prior development of theoretical propositions, attempt to explain links and illustrate the phenomena within a real life context. A case study is defined as *"a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence*" (Robson cited in Saunders, Lewis, & Thornhill, 2009). The case study is considered to be one of the most suitable research strategies to link qualitative data to theory testing (Bryman & Bell, 2011). In addition, Yin (2009) points out that a case study allows to present the boundaries between the phenomenon being studied and the context within which it is being studied. This proves valuable when the boundaries and the context are not clearly evident in the phenomena. The author choose a single case study over a multiple case study because a single case study provides the opportunity to observe and analyze aspects of the phenomena that have not been inspected before. In addition, a single case study provides analysis for a critical aspect or unique case (Saunders, Lewis, & Thornhill, 2009). Yin (2009) states that when using a single case design the author needs to make strong argument in justifying its choice. Therefore, the author find useful to perform a single case study since it reinforces Bryman & Bell (2011) four research dimensions for prioritizing the research focus: presenting interdependencies between variables, generalizing research results, understanding behavior in its specific social context, and having temporal understanding of the phenomena.

An exploratory research study pursue to find out what is currently happening in order to provide new insights to the phenomena. This type of research study is used to make an assessment of the phenomena by asking questions. The researcher clarifies its understanding of the topic through this approach. Interviews with participants in the implementation of the BCP and a literature review of the covered topics are tools that the researcher use to obtain the knowledge of the problem or situation. (Saunders, Lewis & Thornhill, 2009). Complementing exploratory research, an explanatory research is developed to establish the causal relationships between variables. This type of research emphasize a situation or a problem in order to explain the relationships between variables (Saunders, Lewis & Thornhill, 2009). The author seeks to use an exploratory and explanatory research approach to obtain knowledge on the subject of interest in the study.

Yin (2009) distinguish between two types of single case study based on units of analysis: holistic and embedded. A holistic case study is concerned on doing research on organization as a whole while an embedded case study examine sub-units in the organization. The author choose to perform the single case as a holistic case study with one single unit of analysis.

3.3.1. Case Study

The company chosen for the single case study, underwent a period of understanding and consensus among different internal and external organizational actors in order to implement the BCP. Therefore, this unique aspect allows the research to explore what and how was the phenomena perceived by the parties involved in this process. Yin (2009) states that there are several rationales for single case study selection: critical, extreme and unique, representative and typical case, revelatory and longitudinal. Critical cases are used when testing a well formulated theory with a set of propositions and circumstances. Therefore, a single case can confirm, challenge or extend the theory. On the other hand, extreme or unique cases arise when they are rare circumstances that makes the object of the study unique for the phenomena been studied. Typical or representative cases are cases in which the main purpose is to encompass the circumstances or conditions of a phenomena in an everyday situation. Revelatory cases seek to provide the researcher to access to a situation previously inaccessible to observation. Yin (2009) states that to obtain descriptive information will be revelatory to the researcher and the audience. Lastly, a longitudinal study inspect the same single case in two different points in time. The author of this study asserts that the research represents a critical and revelatory single case because it performs examination of the phenomena through the literature in the theoretical framework and links it with the observation of the empirical data in the phenomena. Furthermore, the case possess unique circumstances and is representative of the experience obtained in a large institution.

Guided by Yin (2009) five components of a research design the author will develop the case study. As preconceived propositions in the study, the author asserts that there is a link between the concepts thus seeking an exploratory and explanatory research study. This study consist on a single case study with one single units of analysis: the Business Continuity Plan Implementation. Because the BCP is applied to the organization as a whole, the study seeks to find the interactions between the social actors and the concurrent themes in the BCP implementation. The following illustration depicts the single units of analysis in the study:

Figure 3.1 - Single Case Study Design with One Unit of Analysis

The approach for covering the unit of analysis have been exemplified through the research questions of the author. Research question 1 - *What facilitates the implementation of a business continuity plan in a multinational retail and manufacturing enterprise?* - attempts to link the topics in the thesis into the single unit of analysis. Research question 2 - *What are the challenges and the benefits of implementing a business continuity plan in a multinational retail and manufacturing enterprise?* – covers the challenges and benefits that the BCP implementation brings to the organization.

The company criteria consisted on establishing the foundation for matching the organization with the topics of interest in the research questions. The organization is the entity in which the units of analysis operate. The author considered relevant that both the unit of analysis and that the organization in the case study had implemented a BCP. The literature explores who are the main participants and functions associated in the implementation of the BCP. The research question of the thesis is posed within the organizational context of the enterprise thus the need to focus on a company that have already a BCP in place.

The interviewee criteria consist on establishing the foundation of the characteristics for those interviewed during the case study. The following criteria were used to select the interviewees:

Interviewee Criteria 1: Interviewee had an active and critical participation on the implementation of the BCP. The interviewee must have collaborated actively with organizational stakeholders during the period of the implementation of the BCP. This participation could have been performed by assisting to meetings, giving comments on drafts or acting as an intermediator among the enterprise stakeholders.

Interviewee Criteria 2: Interviewee is continually involved in the enterprise risk management process. Either on business or an IT area, the interviewee is aware of the status of enterprise risk within the organization and proactively contributes to manage and mitigate risks. The interviewees are engaged in the risk management function and is an integral part of their day to day duties.

Interviewee Criteria 3: Interviewee is English and/or Spanish speaking. The interviewee in the study has to be able to communicate in one of the languages that the author commands. The author considered this a factor on the analysis of the interviews in order to accurately interpret the information provided by the correctly the interviewee.

3.4. Research Design

An interpretive paradigm uses a qualitative research method such as discourse analysis and unstructured interview questions to investigate perceptions and constructions of reality by actors in the organization (stakeholders, shareholders, managers, employees). Therefore, the author will use a *multi-method qualitative study research*: a combination of deductive theory through building a theoretical framework and inductive theory through the analysis of the case study to conduct the research through an abductive approach. All this will be done by following a qualitative approach through in depth interviews and employee recalling of the events leading to the implementation of the BCP. This data will be analyzed using a qualitative procedure (Saunders, Lewis, & Thornhill, 2009). Since business and IT actors actively participate by providing input from their specific areas in the development of the BCP, the author believes that in order to obtain the necessary relevant data a qualitative approach is the best suitable approach to the study. The author takes support on her chosen research design method through Yin (2011) features of qualitative research. First, the author seeks to represent the views and perspectives of the persons involved through active participation on the BCP Implementation. Secondly, the author aims to cover the contextual conditions within people live. Through the case study design, the author seeks to explore the organizational context in which the actors thrived. Thirdly, the author aims to contribute with insights into existing or emerging concepts that may help to explain human social behavior in the implementation of the BCP.

3.4.1. Process Framework

The author of the study have chosen an abductive approach to perform analysis on the collected data. Richardson and Kramer (2006) states that abduction, in its simplest form, is the process of associating data with ideas that could be checked through further research. The author engages in a methodology for data analysis based on Dubois and Gadde (2002) systematic combining research process. Theory cannot be understood without empirical observation, systematic combining is the redirection of the theoretical framework through the expansion or change of the theoretical model. Systematic combining consist on the combination of theoretical framework, empirical data and case study analysis. This three aspects

evolve simultaneously. The following figure illustrates the data analysis methodology that stems from the abductive approach of the author:

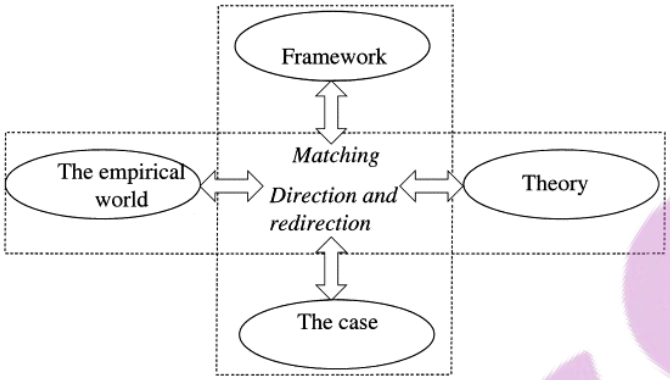


Figure 3.2 - Systematic combining, Dubois & Gadde (2002)

The authors of the framework discuss that the main objective of any research is to confront theory with the empirical world. Therefore, this confrontation is continuous during the research process. There are four components of the research process and two processes in the framework of analysis. The four components are the empirical world, the case study design, the theory and the framework. The two processes related to the framework are matching and redirection and positioning. In the empirical world, the boundaries are set by the author in the definition of what empirical sources need to be addressed in the case. The theory helps defining this boundaries. The expansion of these boundaries provides potential discoveries of new interdependencies within the structure. Therefore, is possible that new insights may bring up new or additional interpretations (Dubois & Gadde, 2002).

The theoretical framework aids the author to find unidentified issues, present important variables, suggests relationships among them, and directs interpretation of findings. In systematic combining, the researcher objective is to discover new variables and relationships and the researcher should consider the observed phenomena into the light of the theoretical framework. This is supported by Yin (2009) that states that theory development has to be dealt with early in the design of the case study. The author engage in the case study and adopt the boundaries of the real world by focusing on relevant theory. The framework aids the author to link theory with evidence. Dubois and Gadde (2002) suggest to use a tight and evolving framework that reflects the degree to which the researcher has articulated preconceptions based on theory. The framework evolves during the study due to the fact that empirical observations bring changes in the view of theory.

Matching between theory and reality is done through a series of going back and forth between framework, empirical findings and analysis. The author of this study develops an n integrated framework based on the theory and goes back to it to explain new findings by developing an enhanced framework. The author focus on direction and redirection to discover new dimensions of the research problem. Direction and redirection of the study play an essential part in achieving matching. The direction of this study is influenced the theoretical framework and exploratory and explanatory case study. The result of the analysis will be a new theory through the iterative dialogue between data and a mixture of existing and new conceptualizations (Timmermans and Tavory, 2012). The author believes that the research ought to confront theory with empirical findings in the real world where the phenomena is observed. Therefore, through a systematic combining approach the confrontation between theory and empirical findings span in a continuous manner throughout the study (Dubois and Gadde, 2002).

In abductive theory, the researcher engage in an ongoing process of moving back and forth from theory to empirical data in order to find explanations about the phenomena. In the aim to provide insights on the BCP implementation, the empirical data of the study is based on the experience of the interviewees that participated in the implementation. Following the design minded enterprise holistic approach, the author created the framework that identify the relationships with the concepts in the theoretical framework. The study identified three major themes and its components. The model is used for exploration, synthesis, and concept development in order to depict the elements that facilitate the implementation of the BCP.

3.5. Data Collection

Data collection for this study is based on the research approach, strategy and design outlined the abovementioned sections. The interpretative research approach to this study allows the author to acquire insights and analyze the information from the interviewees and supporting documentation in the study with a qualitative strategy for data collection. Bryman and Bell (2011) states that qualitative strategy can be done by means of three methods: ethnography and participant observation, focus groups and interviewing. The author will not follow a qualitative strategy on ethnography, participant observation and focus group simply because this methods do not fit in the environmental context of the organization. Since the single unit of analysis in the study, the business continuity plan implementation, has already been performed in the organization, it is not possible to conduct the qualitative strategy using those methods.

The author have chosen the interviewing method because it allows to acquire data using semi structured questions that allow for flexibility from the interviewee perspective. This is supported by Bryman and Bell (2011), who states that the interview method allows *"generality in the formulation of research ideas and on the interviewee's perspective"*. The author asserts that the chosen method will allow to obtain a better perspective on the interviewee' point of view in the implementation of the BCP. Because of the exploratory and explanatory nature of the study, semi structured interviews will be conducted using a specific question design methodology approach. Semi-structured interviews will allow the author to obtain a wide array of rich and detailed responses leading to a deep exploration of the topic (Bryman & Bell, 2011). Saunders, Lewis and Thornhill (2009) describe three types of semi structured interview questions: open, probing and specific and closed ended questions. The author will conduct the interviews using open ended questions. In this context, open questions will give the opportunity to elaborate or describe a specific situation. Open ended questions require a response with more depth and length from the interviewee thus being helpful to answer the research questions of the study. The author summarizes the data collection strategy on the following table:

Data Collection Strategy			
Single Case study with one unit of analysis	**From an individual**	**From an organization**	**Study Conclusion**
	How the organization work	Semi structured interviews with open questions	Derived from the interviews with the organizational actors and refining the framework.
	Why the organization work		
	What organizational functions work		

Table 3.1 - Data Collection Strategy

3.5.1. Primary Data Collection

In order to conduct the case study, the author needed to perform research with a company that possess characteristics suitable for the study. The author search of the company was made possible through ISACA Young Professional Committee, a group within the international information systems organization dedicated to facilitate the development of a community to meet the needs of young professionals. After conducting the search, Grupo Cortefiel, a Spanish retail and manufacturing company that operates internationally, was selected as the company for the case study. This was mainly done because the company already had implemented a BCP. This made it a reliable candidate to perform an examination of the subject. The next step of the process was to inquire which departments have participated in the implementation of the BCP and how this task was conducted. The author found out that the main departments involved in this task were Internal Audit, Group IT and the company steering committee guided by an external consultant that designed the BCP. There were two respondents from the organization and one respondent from the external consultancy. The data was collected through interviews.

In total, three interviews were conducted with each designated expert. A semi-structured list of questions were designed according to the expertise of each interviewee by theme. This approach was used due to the fact that the company selected for the case study is geographically distant from the location were the author is located. A through explanation of the criteria used for selecting the company, the interview questions and the interviewee is outlined in the following sections. The interviews with the project leaders and with the external consultant were performed in Spanish. The author of the study native language is Spanish and translation to English was performed for purpose of the study.
The selected interviewees meet the criteria outlined in section 3.3.3. Interviewee Criteria. From the internal organization, two participants were selected. From the external organization, one participant was selected as he belongs to the consultancy firm that aid the company to develop the BCP.

The qualitative semi-structured interview method allow the author to obtain in depth insights from the participants in the case study. The interview guide consists on a set of questions that the author have divided by theme. Each theme contain questions of interest for the study. The themes cover a number of topics in which the interviewees contribute by providing in depth answers. For each interview, it has been considered the level of expertise and the role that the participant play in the organization, especially in the implementation of the BCP. An interview guide has been developed for each interviewee according to their area of work within the company. The questions asked vary depending on the context of each interview. For ERM and IS/IT risk assessment, the head of Internal Audit was interviewed and he had a design set of questions that allow the author to explore the topic. For GEIT and IS/IT risk assessment, the head of IT Security and Systems also had a set of questions design for the research. Moreover, the external consultant that aid the company in the development of the BCP have also a customized set of questions. The interview questions are outlined in Appendix A – Interview Guide. The interview guide is divided in these key themes: Enterprise Risk Management and Risk Assessment, Governance of Enterprise IT and Business Continuity Plan Implementation.

The interviews were conducted in a one to one basis via skype calls. Every interview was performed personally, meaning that the communication was between the interviewee and the author of the study. The interview guide was sent, in cooperation with the project sponsor, via email to the interviewees. Each participant indicated their preferences regarding time,

date, and medium that best suited their schedule. For purpose of obtaining empirical findings, analysis and categorizing information, with the interviewee's permission, the interviews were recorded using a voice recorder device. Only one participant did not allowed for the interview to be recorded and transcribed. The interview details can be found in Appendix B – Interview Details.

3.5.2. Secondary Data Collection

The secondary data collection consisted on the development of the framework for IS/IT risk assessment in the implementation of a BCP. The author main source of secondary data relies on building the theoretical framework in order to obtain insights from the academic world in regards of the studied phenomena.

Literature Acquisition:

The literature review is structured based on a concept centric approach (Webster & Watson, 2002). The literature included in this study has been clustered upon four distinct topics: enterprise risk management, governance of enterprise IT (includes IT governance), information systems and information technology risk and business continuity. The selected sources come from renowned information systems journals in the form of information technology peer reviewed articles, conference proceedings and scientific research. After the selection of the academic resources was performed, an analysis of the underlying concepts for each cluster was conducted. Literature on ERM, IS/IT risk and BCP have drawn for a wide array of authors and derives mainly on peer reviewed journal article. Literature resources concerning with GEIT has been drawn from peer reviewed journal articles. COBIT 5 publications and recognized academic authors in the field such as De Haes and Van Grembergen have been used to frame the abovementioned topic.

The study explored the literature conceived in the selected topics during the period 1994 - 2015. In addition, material authored by the Information Systems Audit and Control Association (ISACA) was utilized as complement to academic articles to include a practical approach to IS/IT risk and BCP from practitioners. This material includes sources from frameworks on IT Governance, COBIT 5 General Framework, and COBIT 5 for Risk and ISACA trade journals. International Standard Organization (ISO) 22301/02 for business continuity management, ISO 31000 for risk management and Committee of Sponsoring Organizations of the Treadway Commission (COSO) were also reviewed during the development of the study. Frameworks for reference during the development of the thesis by cluster cover COSO, ISO 31000 – Risk Management Guideline and Principles, ISO Guide 73:2009 – Risk Management Vocabulary for enterprise risk management; IT Governance general frameworks, COBIT 5 for Risk, Risk Scenarios Using COBIT 5, ISO 27000 – Information Security for governance of enterprise IT and IS/IT Risk and ISO 22301 for business continuity management.

Eligibility Criteria

The primary method for identifying, locating and extracting resources involved the use of the Jönköping University Library online system "Primo", which has access to several online databases. "Primo" was used to select articles, journals and conference proceedings to conduct a thorough literature review on the clustered topics. ISACA library was also used in order to get resources associated with the topics of interest.

Descriptive Keywords

For enterprise risk management, the following keywords were used: COSO, ISO 31000, ISO Guide 73:2009, risk management, risk identification, risk analysis, risk evaluation, risk mitigation, risk strategies. For IS/IT risk, the following keywords were used: IT risk, IS risk, information systems risk, information technology risk, IT project risk, IT risk management, IT security. For Governance of Enterprise IT, the following keywords were used: IT Governance, governance of enterprise IT, governance of information technology, governance of information systems, COBIT, corporate governance and IT. For business continuity, the following keywords were used: business continuity planning, business continuity management and business impact analysis.

Selection of Resources

The search for relevant academic resources was divided in four parts. Each part consisted on browsing resources related to each specific topic. The credibility and relevance of the academic resources were considered in the selection of the literature review. An advanced search in Primo included specific parameters for the search. For instance, the search was limited to select under the "Subject" or "Title" category items that "contains" or "is (exact)" to the descriptive keywords. Furthermore, the search of available academic resources was limited to filter categories within English language articles, peer-reviewed journals and conference proceedings. Few books were used during the literature review. Physical items within the university library were not reviewed. Peer-reviewed journals, articles and conference proceedings were preferred sources and the most encountered academic resources in the university library. During the descriptive keywords online search, resources from databases ProQuest, ACM Digital Library, EBSCO, SAGE Journals, Science Direct, Springer Link, and Taylor & Francis were used to extract scholarly articles.

The academic articles were divided by topic. The following table portrays the academic journals were the articles were found and utilized by the author during the development of the theoretical framework:

Academic Journals by Topic	ERM	GEIT	IS/IT Risk	BCP
	Accounting, Organizations and Society,	International Journal of Accounting Information Systems	Communications and Strategies	Communications of the ACM
	Risk Analysis	Journal of Information Technology Teaching Cases	Risk Analysis	Information Systems Management
	Reliability Engineering and System Safety	The Journal of Information Systems	Information Systems Management	International Journal of Information Manage-ment
	Internal Auditor	ISACA Journal	The RMA Journal	Industrial Management + Data Systems
	Journal of Accounting and Public Policy	Informatica Economică	California Management Review	Risk Management
	Journal of Risk Research	Internal Auditor		Journal of Investment Compliance
	The EDP Audit, Control, and Security Newsletter	Industrial Management & Data Systems		Computer & Security
	Management Decision	Harvard Business Review		Financial Executive
	J. Account. Public Policy	South Africa Journal of Business Management		Computer, Fraud & Se-curity
	The International Journal of Project & Business	Financial Management		
	Risk Management			
	International Journal of Ac-counting Information Sys-tems.			

Table 3.2 - Academic Journals for Theoretical Framework

For ERM literature review, the most recurrent journal were Risk Analysis, with 6 out of 29 articles reviewed from the journal. Multiple sources from ERM also contributed to the literature review on IS/IT risk assessment. Moreover, GEIT academic articles covered the topic of IT Governance. The literature review also include academic articles within conference proceedings. Few conferences proceedings were used and they mainly reside on the topics of IS/IT risk and governance of enterprise IT.

Evaluation of Resources

The online search provided a large collection of academic resources. Therefore, a review of each resource was performed to determine its relevance with the topic. The criteria selection was based on the proximity of the relation of the abstract content with the selected topic. Once a resource was labeled as useful by the author, the resource reference list was reviewed to verify if additional academic resources could be selected in order to conduct the literature review. If relevant references were found, an online search through Primo was performed again to obtain the academic resources. Due to the events that lead to development of ERM, GEIT and BCM, the cited references in the literature review date have an 18 year range (2000 -2015).

3.6. Data Analysis

Data analysis is performed following Dubois and Gadde (2012) systematically combining abductive research. This involves the combination of the analysis of the empirical findings and the framework model. The researcher is able to expand the BCP implementation insights by performing alternative analysis between this two subjects. In the study, the author develops a framework through an abductive approach to allow the findings in the empirical world to modify the theory and vice versa. Through the process of matching and direction/redirection the author redefines the framework. In this context, direction and redirection guides the author to triangulate the data sources and reach to conclusions. Triangulation relies on using two or more independent sources of data in order to converge the research findings within a study (Saunders, Lewis & Thornhill, 2009). Triangulation of data sources relies on combining of sources of evidence in the aim of obtaining accurate conclusions. The author have used principles of data collection to acquire multiple sources of evidence. This include interviews and building up the initial theoretical framework. Triangulation is used to further develop converging lines of inquiry and strengthen the basis to construct validity in the study. In this study the sources of collecting and analyzing data were the three interviews performed together with the initial theoretical framework for IS/IT Risk Assessment in the implementation of the BCP.

The data analysis process of the study will be conducted by following the case study description. According to Yin (2014), a case description consist *on "organizing the case study according to some descriptive framework"*. Based on the theoretical framework the author have organized the topics covered in the section in the form of themes. The information obtained for each theme is broken down into categories. The information for each category is analyzed from the topics covered through open ended questions in the semi-structure interviews. Chapter 4 – Grupo Cortefiel Case Study present the empirical findings concerning the data collected while Chapter 5 – Analysis presents a thorough analysis of content that emerged from the empirical findings. The outcome of the analysis is presented in section 5.4. Final Framework.

Interview Analysis

The author aims to discover pattern across the interviews performed to develop the case. To be able to analyze the data collected through the semi structured interviews with open ended questions, coding data analysis was used to analyze the interviewee responses. Miles, Huberman and Saldana (2014) defines codes as labels that assign symbolic meanings to the descriptive or inferential information compiled during the study. Coding is deep interpretation and analysis of data meaning. The author will use pattern codes to detect reoccurring patterns in the data and clustered them together to create categories. Pattern codes represent categories or themes, causes or explanations, relationships among people or theoretical constructs. Yin (2009) states that pattern matching approach deals with identifying patterns in the data collected through the study of the phenomenon. Each theme is divided in sub-themes to further conduct the data analysis. The statements of the respondents were contrasted between each other in order that the author can identify pattern matching and perform explanatory building. Interviewee responses were divided into three primary pattern codes or themes:

Theme 1 - Enterprise Risk Management and Risk Assessment

This theme covers how the organization manage business and IS/IT risk in the implementation of the BCP. The main purpose was to inquire how risk is identified, managed, prioritized, and approached at the organizational level for matters of the BCP implementation. The section concludes by inquiring the perspective of risk obtained with the implementation of the business continuity plan regarding the work field of the interviewee.

Theme 2 – Governance of Enterprise IT
This theme covers the role that technology plays in regards of the business processes and operations performed within the organization. It covers IT initiatives before and after the implementation of the business continuity plan and the development of IT risk scenarios from a governance of enterprise IT perspective. The section also covers how the organization mapped the IS/IT resources associated with the execution of business processes in the organization

Theme 3 – Business Continuity Plan Implementation
This theme covers extensively the implementation of the BCP. It outlines the factors that acted as drivers for the implementation of the BCP, who were the key actors and which role they played, the implementation at an organizational level, identification of critical process and business areas, the organizational elements within each department that assisted in the implementation of the BCP and the methodology or guidelines used. Furthermore, this section explores the perception from the enterprise leaders concerning the implementation of the BCP, the decision to whether or not develop the BCP in-house or outsource it to an external service provider, who and what role organizational agents played when performing the process of mapping information systems and technology infrastructure with business processes and how project leaders considered the participation of the external service provider in relation to the implementation of the BCP. The final section contains concluding remarks regarding the challenges and benefits of the implementation of the business continuity plan.

3.7. Research Setting

Saunders, Lewis and Thornhill (2009) describe a cross sectional study as the study of a particular phenomenon at a particular time. This study is a cross sectional due to the fact that the examination of the BCP implementation took place in a specific point in time from the perspective of more than one person that collaborated in the organization.

3.7.1. Validity

Miles, Huberman and Saldana (2014) assert the issue of adequate validity as a major criticism for qualitative studies. The subjective nature of using qualitative data and its unique origin in a single context makes difficult to apply internal validity to the study. Thus the author of this study attempts to construct validity by identifying accurate and applicable concepts in the study. Construct validity means that the researcher derives hypotheses from theories. This hypothesis need to have fundament on the theoretical framework. Miles, Huberman and Saldana (2014) explains the different archetype of analytic bias that may harm or invalidate the study findings. The holistic fallacy implies that the researcher interpret events as more patterned and congruent as they really are. Elite bias means to overweight data from articulate, well informed high status participants while underrepresenting data from lower status participants. A personal bias is incurred when the researcher's personal agenda skew the ability to present fieldwork and data analysis in a trustworthy manner. Going native bias relies on the researcher losing perspective by being immerse on the perceptions of the participants (Miles, Huberman & Saldana, 2014). The theoretical framework was constructed using previous research from valid concepts and models. Therefore, the author base its research on the theoretical framework and avoids bias in order to achieve validity in the study. Based on Miles, Huberman and Saldana (2014), the following guidelines were used in the study in order to ensure internal validity:

- Descriptions are context rich, meaningful and thick.
- Triangulation, data analysis and complementary methods for data sources produce generally converging conclusions.
- Findings are clear, coherent and systematically related.
- Data presented are well linked to the categories of prior emerging theory through the theoretical framework.
- The conclusions were considered to be accurate by the original participants.

External validity discusses if the sample is representative or not of the study sample (Saunders, Lewis, & Thornhill, 2009). External validity is often use in studies that are connected with quantitative studies and possess a large population sample. The empirical findings and the samples are unique and do not represent the whole population or industry. However, organizations can take lessons learned and applied them on their own context.

3.7.2. Reliability

Reliability is the process that asserts that the study is consistent and reasonable over time. (Miles, Huberman & Saldana, 2014). Reliability refers to the consistency of findings, which means that the operations can be repeated with the same results if the study was repeated (Saunders, Lewis, & Thornhill, 2009). Data collection is done through interviews and data analysis is done by coding the empirical findings. Reliability of this study is performed by the author considering the following guidelines (Miles, Huberman & Saldana, 2014):

- The research questions are clear and features of the study design are congruent with them.
- The researcher's role and status within the site have been explicitly described.
- Connected to theory, basic paradigms and analytics have been clearly specified.
- As suggested by the research questions, data were collected across a range of appropriate settings, times and respondents.
- The findings shows meaningful parallelism across data sources (participants, context, and times).

3.7.3. Ethical Aspects

The author of this study adheres to perform an ethical study in all aspects of the research. As stated by Miles, Huberman and Saldana (2014), privacy concerns control over other access to oneself information or preservation of boundaries against giving protected information or receiving unwanted information. Confidentiality relies on the agreement with a person or an organization about what will be done and may not be done with their data (Miles, Huberman & Saldana, 2014). The author has provided full information about the study to the participants and consent has given freely and unforced. The author has agreed on maintaining privacy and confidentiality in the study. The author guarantee to safeguard the information that the organization has provided for the development of this study.

4. Grupo Cortefiel Case Study

The chapter portrays a general description of the selected organization for the case study together with the antecedents for the implementation of the business continuity plan and the empirical findings.

4.1. General Outlook

Grupo Cortefiel is a leading international Spanish clothing retailer headquartered in Madrid, Spain. The company is the second largest apparel retailer in the Spanish market. The company early foundation dates from 1880. The company first brand was launched in 1945. The company is present outside the Iberia peninsula through international retail formats and franchise operations. The company serves the Portuguese market and have a small presence in Austria, Belgium, France and the Netherlands. According to the company website, Grupo Cortefiel counts with overall 2040 points of sale worldwide in 77 countries, has 1455 direct operate stores and 585 franchises. (Grupo Cortefiel, 2015a). With 9904 employees in the group division, the company operates on an international scale. Grupo Cortefiel owns its European stores and franchises locations in Asia, the Americas, and the Middle East.
The company mission is to become a leading international group specialized in fashion chains, aimed at meeting the needs of our clients, provide career growth to our employees and to contribute with society´s development (Grupo Cortefiel, 2013). The company vision to offer the best fashion, consistent with the lifestyle of our customers, achieving the differentiation and greater diversity of products with full international expansion (Grupo Cortefiel, 2013).

Grupo Cortefiel manages four clothing subsidiaries/brands: Cortefiel, Springfield, Women´s Secret and Pedro Del Hierro. Each clothing subsidiary has a different market target: young men, older men, young women, cost-conscious women that seek to acquire high-end clothing. Cortefiel focus on more traditional clothing and it was the first brand created in 1945 by the group. The target market consist of men and women between 35 and 45 years old (Grupo Cortefiel, 2015a). Springfield was founded in 1988 and provides a contemporary and fresh cosmopolitan outlook. The initial target market was directed to men as a mean to provide an alternative to men clothing. The brand has enjoyed sustained growth and in 2006 Springfield launched the women's collection. Since then, the brand target has been men and woman aged between 20 and 30 that are looking for a relaxed outlook on life and fashion (Grupo Cortefiel, 2015b). Women´s Secret was a brand founded in 1993 and specializes on women underwear and lingerie. This brand is under continuous expansion strategy (Grupo Cortefiel, 2015c). Pedro Del Hierro is a brand acquired by Grupo Cortefiel in 1989 and their line of clothing is dedicated to men and women that enjoy dressing with an haute couture or urban style. As Women Secret, the brand has experimented international expansion thanks to the company strategy since 2007(Grupo Cortefiel, 2015d).

Grupo Cortefiel has evolved through a series of mergers and acquisitions in the retail and manufacturing sector. The company has expanded internationally and its ownership have changed in composition throughout the years. The following timeline outlines the progress of the company (Grupo Cortefiel, 2013):

Retail Sector

- 1880: Start of business by Quiros family.
- 1945: Creation of the Cortefiel brand
- 1988: Creation of the Springfield brands
- 1992: Acquisition of Pedro del Hierro brand

- 1992: Creation of the Women´s Secret brand
- 2006: Launch of SPF Woman
- 2010: Launch of Pdh Sport
- 2012: Grupo Cortefiel operates 100% online
- 2013: Launch of Pdh Madrid

Manufacturing Sector

- 1933: Opening of the 1st shirt factory
- 1945: Opening of the 1st suit factory
- 2006: 100% Retail end of own manufacturing

International Presence

- 1960: USA Exports with Cortefiel brand Macy´s – Saks
- 1991-1995: Expansion to France and Portugal
- 2000: European direct expansion and global franchise expansion
- 2014: Grupo Cortefiel is present in 70 countries

Ownership

- 1880: Family owned Garcia Quiros and Hinojosa
- 2005: 30% CVC, 30% Permira, 30% PAI Partners, 10% Management and other minority shareholders.

4.1.1. Organization

The brands within the group operate with its own design team and sales and management structure. They share the administration, finance, technology, expansion and sourcing and human resource divisions, as well as other corporate functions, based at the central offices. The Group has a network of international buying offices in Spain, Hong Kong and India. Distribution is centralized at the Madrid logistics platform, backed up by an additional center in Hong Kong, supplying both the Group's own stores and franchises. The multiband growth strategy has been further reinforced through international expansion and the development of the online channel. Regarding financial regulatory standards, Grupo Cortefiel is compliant with the Payment Card Industry Data Security Standard. The following is the organizational chart of Grupo Cortefiel:

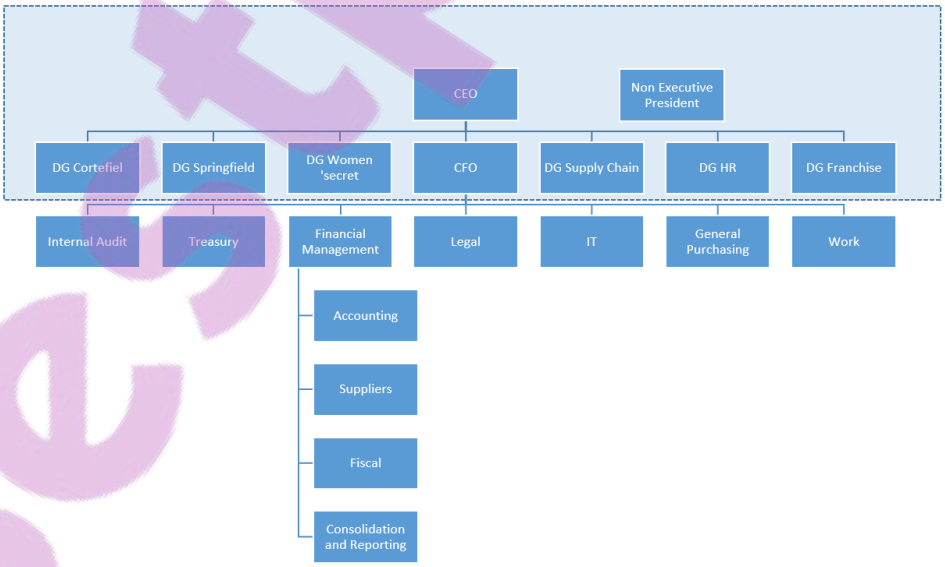


Figure 4.1 - Grupo Cortefiel Organizational Chart

4.2. BCP Implementation Antecedents

The night of February 12-13, 2005 the city of Madrid, Spain experimented a dense grey cloud of ashes caused by a chaotic set of flames in one of its most iconic buildings: Torre Windsor skyscraper. Torre Windsor skyscraper was built in 1979 and had 32 floors. The 106-meter-high building, located in Spain capital business district Paseo de la Castellana north-south Boulevard, took 26 hours to put out the blaze by the city firefighter department (Aunion, 2015). In total, 80 officers were involved over the course of the fire and it was so intense that the risk the building collapse was imminent. Firefighters heard a bang that was caused by the collapse of an exterior emergency stairway and the fire continue to consume the structure. Large pieces of the tower plunged to the ground and the blaze destroyed its top floors and sending columns of black smoke into the night. Madrid Mayor Alberto Ruiz Gallardon said the fire was believed to have been caused by a short circuit on the 21st floor, though the official investigation never established the real cause of the fire (BBC News Europe, 2005; Aunion, 2015). The fire, by far, has been the biggest fire that the city of Madrid had experienced. The prime minister at the time, José Luis Rodríguez Zapatero, visited the site, and the government announced plans to improve security in Spain capital's skyscrapers. Fortunately, the fire resulted in no deaths or serious injuries though it reminded to business operating in the city the magnitude and impact that such event had on their business operations. During the following days after the fire, local businesses and offices around the area remained closed and transport system was diverted (BBC News Europe, 2005). One of the technical experts brought by the insurance company analyzing the underlying causes of the fire stated that "the building was pretty much a paper storage warehouse," making reference to the huge amounts of paper documents kept there (Aunion, 2015). This cause repercussions not only to the companies that were based at Torre Windsor but also to those companies located in the surrounding areas.

Most floors were occupied by company offices, being the Big 4 Audit consulting firm Deloitte the company that occupied more than half of the floors in the building. Even though Deloitte was the main company affected in the Torre Windsor fire by losing their main headquarter and all the paper information they could have possessed, the consultancy firm managed to resume their business operations in three days. The consultancy firm managed to continue offering their services to clients by rapidly putting in execution a plan that allow their employees (partner, managers, consultants and administrative personnel) to work from different locations. Despite Deloitte Spain losing the physical location where they operated, the effectiveness and efficiency of their business activities deployment through business continuity efforts put into perspective the fact that enterprises can suffer a loss from such magnitude in a matter of seconds.

Grupo Cortefiel took the Torre Windsor fire into consideration when outlining the necessity of counting with a BCP that can enable the company to resume operations in an event of disaster. Grupo Cortefiel Internal Audit mapped in their risk map the fact that the risk of not having a BCP in place in case of a disaster or emergency can cause further damage because the company would not know how to act in a negative event. This could further enhance the possibility that the enterprise experience negative effects by lacking the coordination and resources to resume their business operations. Internal Audit perform a risk assessment and communicated their findings to the steering committee. Internal Audit also outline the potential benefits of having a BCP and include the BCP project on their budget for the upcoming year. After careful consideration, the steering committee approved the project and Internal Audit teamed up with the IT Department to conduct the BCP. Given the experience acquired in the implementation and execution of their own BCP, Grupo Cortefiel selected

Deloitte Spain as their external consultant to conduct the BCP implementation. The development of the BCP started during the first months of 2012 and finished mid-2013. Overall, the development of the BCP lasted 8 months. The resources needed for the completion of the project were obtained through the two key sponsors: IT and Internal Audit. A team leader and three external consultants from Deloitte Spain were deployed in order to conduct the BCP implementation.

4.3. BCP Implementation Development

The results chapter provides the empirical findings related to the interviews performed. The following table outlines the participants in the interviews:

Case Study Organization: Grupo Cortefiel					
#	**Name**	**Department**	**Position**	**Business Continuity Plan Implementation Role**	**Interview Description**
1	David Moreno del Cerro	IT	Head of Systems and Security	Sponsors and main leader the project during the implementation of the BCP. He is responsible for IT systems and the security of the technological infrastructure that the company possess in Spain and in the rest of the countries were Grupo Cortefiel operates. He is also responsible for the IT services the company offers internally.	Business Continuity efforts and IS/IT Risk Management
2	Luis Mesa	Internal Audit	Head of Internal Audit	Responsible for internal audit and financial audit reports and he have worked at Grupo Cortefiel for several years. His area is responsible for handling high-level risks. During the implementation of the BCP, the risk that IA reported were taken into consideration. Based on their risk map, the department promoted the implementation of BCM in the organization together with IT department.	Overview of the participation of the department in the implementation of the BCP.
External Consultant: Deloitte					
3	Pablo Rodriguez Cabellos	Manager	IT Enterprise Risk Services	Team leader for the external consultancy Deloitte Spain working in the implementation of the BCP at Grupo Cortefiel. During the implementation of the BCP, he assisted in preparing the implementation of business continuity plan by aiding the organization in identifying the critical areas and by tracing the methodology of the project. Currently, he is a manager in Deloitte Spain IT Risk Services. His work at Grupo Cortefiel as an external consultant begun in October 2012 and finalized in the middle of 2013.	Methodological and practical support to Grupo Cortefiel in the BCP implementation.

Table 4.1 - Case Study Participants

The empirical findings, derived from the conducted interviews, have been summarized in the following sections. The views expressed by the interviewees are based solely on their personal experience during the BCP implementation. The transcript of each interview can be found in Appendix C – Interview Transcript.

4.3.1. Enterprise Risk Management and Risk Assessment

Regarding risk management of the IS/IT key resources, technology plays a fundamental role in the development of the operations of the company. David notes:

"The technology department is essential as all business processes operates based on the technology services that the department offers. The company, without the support of technology may not work. No company in the world can do without technology."

At Grupo Cortefiel, David comments that the main technology risks identified during the implementation of the business continuity plan were based on a previous company assessment: the IT Disaster Recovery Plan (IT DRP). Since the company already counted with an IT Disaster Recovery Plan that is tested and adjusted annually, most IT risks were already identified and corrected.

Technological risk was approached in the organization based on the ability that the IT department had to provide technological services that the company needed in different situations. The risks were lower because the company already had an IT DRP. The IT department assured that the risks included within the IT DRP were consistent with the BCP. In this regard, David asserts:

"The initial risks reflected in the IT DRP had to be adjusted because there were only two or three risk scenarios when, for instance, in the BCP there are many more risk scenarios"

The technological risk reside over the business process of logistics and operations. David notes that a countermeasure against disaster can be:

"To have sufficient computer equipment to service a number of users at a particular time that may need a computer, printer, mobile phone to execute their operations was a risk. The company, in this case, should have a secured stock of computers for users contemplated within the business continuity plan or have an agreement with a company that could provide the technological equipment that Grupo Cortefiel requested."

Since the company is a leading retail and manufacturing clothing company, David states the element of risks were located in the supply chain process and in the financial processes the company execute to continue with their operations.

Luis, from Internal Audit, comments on the role of his department in Enterprise Risk Management. Internal Audit performs audits in operational matters internally in the organization: implements control activities and provides solutions for continuous improvement in the processes of the organization. The functions within the department focus on risk assessments and controls.

Luis notes that at first the BCP only contemplated the operations from headquarters and did not included the logistics part. Luis remarks that due to the nature of the company business, logistics department elaborated its own continuity plan. The determinant factor in the realization of BCP was based on a risk map that the organization already had. The risk scenarios regarding technology were raised by the IT organization. The priority given to risk was based on the process recovery times. The dependencies of each department were analyzed and if the functions were more critical than other functions within the organization. Dependencies and response time were evaluated and how they fit into critical areas. Luis also notes that they assessed how long Grupo Cortefiel can survive without some particular function in the organization. This is done in order to know when a point or no return has been reached.

Regarding technological risk, Luis asserts that IT risks are based on the level of responsiveness in which business critical process feature in relation to the use of technology. On the other hand, business risks relied in the impossibility of the business to sell merchandise and pay to their suppliers. The risk assessment was done based on the criticality of the business process and scenarios. Luis comments that it was very important to have clear when the process have reached a point of no return. For instance, if the company cannot visualize through the system the amount of merchandise that has been sold, this pose a risk that takes the company to a point of no return.

Regarding the risk management of the IS/IT key resources, Pablo, Deloitte BCP External Consultant and BCP implementation team leader, explains how the business and technological risks were identified:

"Depending on the information obtained in interviews about what each area and each functions were performed by each process owner, we identify dependencies in the process. We count with a risk catalog to do so. We performed a match of the business process together with the IS/IT resources (information systems, applications, data, infrastructure). Risks associated with each dependency are linked to the active use of a technological asset within the business process. This information is obtained through the interviews with business process owners with support of the technology department."

Pablo describes that in the planning phase of the BCP, physical risks are taken into consideration. This includes risk concerning fire, flood or environmental disasters that can trigger the activation of the BCP. Cyber risks is an increasing risk that companies should also consider in the implementation of the BCP. In order to perform an IS/IT risk assessment, Pablo notes:

"Technology risks are analyzed, usually qualitatively. The more you try to have a mathematical formula, it becomes more complex and more time will be taken to perform the risk assessment. The method of quantitative risk is more likely to be used in a highly mature organization with a control system of quantified risks."

Pablo explains that a rating of the qualitative risk is later used to give priorities to the risks. To visualize this prioritization, a risk map is performed. The main risk relies on physical risks due to inclement conditions, risk of failure of electricity, human related risks (food poisoning in the organization or labor strikes) and technology risk related activities. Pablo points out that the risks in the organization are translated into what is known as a "threat scenario":

"It is very complex to handle 80 risks (for example) within an organization, but these risks can be reduced to simple scenarios. For instance they can be translated to the inability to access the building, electric power failure, total or partial loss of the building. Instead of posing all 80 risks, 10 risk are summarized by categorizing threat scenarios."

Together with the threat scenarios and the business impact analysis, the external consultant can aid the organization in plotting recovery strategies. Action plans are developed as a result of the review made for the implementation of BCP. Action plans reduce the risk of materialization of an incident that results in the activation of the plan and, on the other hand, aid on preparing alternatives. Pablo explains:

"In a BCP, depending on the impact or damage, incident or disaster, the impacts are measured by business impact and recovery capacity."

To map the business processes together with the IS/IT resources, the consulting team worked in conjunction with the project sponsors and the information obtained during the interviews with each business process owner to depict an accurate map. Pablo notes that the

IT DRP at Grupo Cortefiel was previously prepared by the external technology provider of the organization. The technology provider gives support to IT DRP with in an alternative site and technical support in technology regarding servers.

4.3.2. Governance of Enterprise IT

Regarding the interaction of business processes with IS/IT key resources, David comments that the process of mapping this two functions lies on developing a map of a very high standard. This maps is an inventory of services that specifies which technological assets (data, applications, and infrastructure) matches with the execution of a business processes. He comments:

"This process consist on the link between business processes with the various services provided from the area of IT. Each specific process is placed with its "first and last name" (technological resources that support the function is specifically identified)."

In regards of the time frame of the implementation of the IT DRP and the BCP, David comments that there was an approximate 4 year gap in between:

"This period was marked by an economic moment lived in Spain, where there was a crisis, and companies had to make adjustments at all levels. Budgets were focused on continuing the operation with minimal investment. As the company already had an IT DRP, the company determined that it could survive in the event of an incident without a business continuity plan"

The company counted with a basic plan for IT disaster recovery that was not a purely IT vision as it also mapped some business processes. In this sense, there was enough information so that the company could decide to postpone the development and implementation of BCP. The perspective of risk obtained with the implementation of the business continuity plan for the technology area was fundamental, in part, in the previous work performed within the DRP were technology risks were identified and known in the company. David notes:

"The business continuity plan only came to reinforce our views in regards of technology risk".

In regards of the utilization of technology in the company, Luis remarks:

"The company is dependent on technology as our business thrives from the information that is supplied via our information systems. It is important to have a stock of technological equipment that we can count in case of an emergency or disaster so that people can work from anywhere in the event of an incident."

Luis said that this could be acquired by counting with an outside vendor that can provide the service in order to have the technological support. In order to map business processes with the IS/IT resources, Luis comments that first an understanding of the process was performed through interviews with the business owners. This was obtained through inquiry with the process owners in regards on how they work and what was the optimal response time against a situation of disaster.

Pablo comments that before the implementation of the BCP, Grupo Cortefiel already counted with an IT Disaster Recovery Plan. The IT DRP is a contingency plan that involves the recovery of the technological infrastructure, servers and data processing center. He points out the relationship between this two elements:

"The BCP is a management plan. The BCP functions to restore business critical functions of the organization. The IT DRP seeks to recover the technological infrastructure in the event of a failure in the IT infrastructure. The relationship is that within your BCP, in case is needed, an organization may enable the IT DRP."

The organization already counted with a starting point to implement the BCP, however not all should be seen from the technology side. Pablo further describes the degree of dependency of technology that the enterprise has within its business processes:

"I think virtually all business processes, from the critical processes to the less critical processes have a direct dependence on technology. So you always need technology for executing business activities and for daily access to information contained in the system"

The perspective of risk obtained with the implementation of the business continuity plan for the technology area have aided the organization in improving the support to the risk function. Pablo explains that the implementation of a BCP enriches risk management function:

"A technological layer of risk that the organization considers as part of its business process is added and reinforced with the implementation of the BCP".

Pablo notes the security aspect in the implementation of the BCP:

"Technological threats are linked to the dependency of the enterprise with technology functions. Conventionally, a physical risk (catastrophe, fire, flood, environmental) associated to the enterprise can trigger the activation of the BCP. The reality is that increasingly the map of risk and threat landscape will continue to be maintained and the most common risks are fire, flood and environmental disasters. However, it is more likely that we will be adding cyber risks due to the dependency that exists with IT. If technologies are damaged by any (deliberate or accidental) threat, the impact affects the logistics chain and may triggers impact on other processes."

Pablo discusses that the importance of a BCP does not only rely on the technological side. The technological side is only one aspect and, in case of Grupo Cortefiel, this was already covered with the IT DRP. Nevertheless, the rest of the activities included in the BCP, are not covered in IT DRP such as the ones that involve providing users for technological equipment (mobile phone, computer), or if you lose electricity or communications.

4.3.3. Business Continuity Plan

David remarks that the initiative of counting with a BCP came from the areas of IT, and internal audit. Also he noted that the various annual financial audits performed by its external auditor also prompted the initiative because the company did not have a business continuity plan well founded and developed that went according to the structure of the company. David explains that this view was supported by the governance body:

"The suggestion came primarily from the steering committee. The strongest pressure was from the steering committee and the governing bodies together with IT and Internal Audit department. Every year in the annual report, the external consultant conducting the financial audit, marked as one the areas of improvements the fact that the company needed to strengthen the area of business continuity management. This facts came to support the implementation of a business continuity plan."

Moreover, the fact that the organization launched a process of response to incidents involving the company data processing center (DPC) in the form of an IT DRP helped to establish the necessity for counting with a plan that can also include the restoration of the business processes and enterprise operations. After a few years and motivated by a number of external circumstances that have been happening in Spain, the steering committee and the board of directors set a goal to achieve in a relatively short time the implementation of a business continuity plan.

David comments that there were two pillars that enable the implementation of the BCP: board of directors, CEO, CFO and management support together with the decision of how and with whom to develop the BCM.

"Without the support and the leadership of management it would have been virtually impossible to do this project because there are many business units within the organization and it is difficult to coordinate any action on a transversal level among the units. Without the sponsorship from the board of directors and management, it would have been very complicated to implement the BCP.

David noted that a determinant factor that acted as driver was the awareness that came from the company management to be able to cope with any incident or threat scenario that may directly affect the day to day operations. As a company that operates internationally, the vast majority of the technological services offered by the company's own stores or franchise operations are centralized in one location. David remarks:

"This make that any incident affecting the location has a rather catastrophic effect with respect to the headquarters and shops. There is no sense having a contingency plan for the area of technology without a business continuity plan. In the event of a disaster in the department, there is no sense that the IT department knew what to do or to be capable of serving in a short period of time the operations, but that other departments (business units) did not know what to do"

David outlines the main challenges that the organization confronted in regards of performing the implementation of the BCP were:

"Challenge 1: Decide which processes within the organization fell within the business continuity plan and which did not. To make this choice, the person who took the decision regarding what business processes were to be included was the CFO (Chief Financial Officer). This person has been in the company for 24 years and has a global view of all business processes (from the simplest to the most complex).

Challenge 2: Organizational challenge. The company has 80 departments of which 25 to 30 departments entered into the business continuity plan. To coordinate interviews with each of those responsible in order that the external consultant understood how the internal process fit with the rest of processes was a complex organizational issue.

Challenge 3: Motivate and communicate to the business units the importance of completing the business continuity plan. It is important to have the leadership to boost the plan but it is also important to have the support and understanding of the owners of the business processes."

In coordinating the activities, David asserts:

"To close agendas and getting updated information from each department were challenges in coordinating activities. One must know how to manage this information (about personnel contact information) very carefully due to Spanish data privacy laws."

To identify the business critical processes and areas, the CFO of the company was consulted. He took the decision regarding what business processes were to be included as his tenure in the company provided him with a global view of all business processes. He is also part of the company Steering Committee.

The key actors in the BCP implementation were the IT department, Internal Audit, the Steering Committee, Business Areas and the External Consultant. IT brought expertise in the technological field and coordinate activities in the organization while Internal Audit provide overview of the map of risk linked to the company. Beyond the risks of technology that manages the technology department, Internal Audit offered a view of the business risks. The

steering committee promoted the implementation of the BCP and approve it. The business areas provided the experience and knowledge of how each area works and which information systems used, how they operate and what resources were essential for implementation of the business process. Finally, the external consultant gather information from different areas of the organization and organized this information in an orderly and manageable way. In addition, they provided expertise in developing the BCP. The external consultant conducted the interview with each business area. In regards of the support provided by the external consultant, David comments:

"The role of the external consultant was very important, mostly in developing the business impact analysis. This development requires having a fairly comprehensive knowledge of all business processes, how the company works and also required the development of documentation. To count with resources and experience from the external consultant turned out to be an advantage for Grupo Cortefiel in regards of the implementation of the BCP"

The criteria for selecting the external consultant was relied upon the fact that the organization external financial auditor, Deloitte Spain, offered the organization a more concrete vision of their business. In part this was because the firm have confronted a situation of disaster were the company had to activate its own BCP. The building in which the firm was headquartered caught fire and was declare a total lost. For transparency and objectivity, the company decided to have an external agent which would bring the knowledge and experience of customers from the same industry at the time of preparing the BCM. The methodology was brought by the external consultant, based on the best practices in the industry. David notes:

"The experience that the firm suffered showed us that they were able to restore operations after a disaster situation".

To conduct the mapping of IS/IT resources with business processes, David discusses the participation of the external consultant:

"The external consultant helped bring order to this documentation. With 80 departments and a large infrastructure at Grupo Cortefiel, the task to put order in regards of this documentation was a complicated process. The external consultant brought documentation template and the methodology to document the map clearly and simply way.

Within the IT department, the organizational elements that assisted in the implementation of the BCP relied on the advantage of counting with an IT disaster recovery plan. David comments on this topic:

"Internally, within the IT department, we have been driving initiatives related to risk management and security scenarios that make us feel comfortable with the preparation of this plan and the business continuity activities. I collaborated closely with the consultant and other areas of the company. The technology department was the department who led the coordination of interviews, preparation of business impact analysis and contribute to map information systems linked to business processes"

To formulate the IS/IT risk scenarios on business processes, David asserts that first the IT department verified that the critical business process were included in the IT DRP. If the critical business process were not included within the contingency plan, there was an analysis to whether it made sense to include the business process in the contingency plan, as this represent a cost for the organization. After this process, risk scenarios were formulated according to each critical business process. David states the collaboration with the external consultant:

"The external consultant presented a generic map of physical, logical, organizational threats to technology. Based on a list of 20 or 25 threat landscape in the generic risk map, the technology department chose the scenarios that posed a condition of threat to the enterprise operations. IS/IT risk included sabotage or theft and this were more internal risks. The vast majority of identified risks were exemplified through external risk scenarios (fire, flood, disaster)".

At an organizational level, the perception of stakeholders in regard of the implementation of the BCP was very positive. David discusses that managers from business area managers fully understood the how and why of the project. However, they also have to deal with some negativity from some business process owners as not all the business process were considered critical within the organization. This is best described in the following comment:

"The cost to include all the business processes as critical is not acceptable in the implementation of a BCP. It was very costly to explain to the business owner that the business continuity plan was only able to act in case of a contingency, but the business area do not have to give 100% of their service. When the business owners were told that in case of a contingency, the company could operate with 8 people instead of 20 people in their department, could be a cause of suspicion in the organization. It is possible that business process owners think that will take away resources or funds, when this was not clearly the case"

During the interviews with the business process owners and the external consultant, David noted that the interview questions were directed on acquiring the knowledge of the business process peak moment. Also known as seasonality, each process is greatly influenced on the fact that, at a certain time, how business disruption affects the company. David comments:

"This was a key part in interviews. Each department gave a calendar of seasonality of its process and labeled the incidents that, at a specific time of year, affect in great percentage the operations of the company. We had to ask, by interviewing business leaders, about what these moments were and the time they happened to be clear about the days in which if an incident occurs, could be greater impact on the enterprise operations".

In pointing out the benefits of implementing the BCP in the organization, David notes that:

"The main benefit was that the company was able to obtain a big picture of the organization. Having a clear picture of what the critical business processes were, which processes were required for the company to run and how to react in the event of a contingency were benefits we acquired with the implementation of this initiative. The value that has brought us this plan is very high because of the level of internal knowledge we acquired."

Luis comments that the implementation of the BCM was an initiative that developed internally and was not very public in an open manner. The plan helped to identify supply chains and processes related to this supply chains.

Luis comments about the organizational actors present in the implementation of a BCP:

"The technology department acted as lead actor to boost realization of BCP. The role that internal audit played in the implementation of the BCP was to be a good supporting actor."

Luis remarks that who really led the project was the technology area. Luis also comments that there were designated committee members giving support to the implementation of the plan: crisis, legal and purchasing. Luis comments that there were no formal criteria for selecting the external service provider. The company decided that the service would be provided by a Big4 auditor. Since the company already have an established a client relation with their current auditor (Deloitte Spain), they proposed to offer the service and Grupo Cortefiel decided to implement the BCP with them.

Luis asserts that the seasonal time of each business process was identified and it was also emphasized in the critical moments of each business process. The risk scenarios were drawn through interviews with business owners and the seasonality of each business process was considered. In this context, Luis comment:

"Depending on the activity level, we had to adapt each department seasonal time within the BCP"

Regarding the challenges faced in the organization, Luis remarks:

"Departments have transversal processes that are interrelated with the supply chain of the company. For example, planning or purchase department has its own supply chain internally. Each supply chain has its way of operating. Therefore, not all supply chains within the organization operate in the same way."

This was a challenge when performing the identification of critical processes and business areas. An excel matrix with the specification of the transversal function was elaborated.

Another challenge was the evaluation of the alternatives presented in the implementation of BCM. This was an issue of integration within the enterprise systems. When analyzing this issue, it was suggested to standardize the ways of working with IS/IT applications to make the work homogeneous.

At the organizational level, Luis comments that the implementation of BCM was not valued as a critical project, as is the case of some themes within corporate governance. He notes:

"These topics are presented as common in the work place and usually take time."

Luis remarks that the methodology or guidelines on the implementation of BCM were closely linked to critical areas and response times of business processes. He asserts that several matrix were created and they depicted response time for recovery of the process. This information was obtained through interviews with business process owners.

Luis consider that the involvement of external consultant in the project was very helpful:

"The external consultant gave us the methodology, aid with conducting staff training and with monitoring and reviewing the plan if changes in the organizational structures happen. Employees change as your contact information. Therefore it is necessary to have an update on the methodology and to follow up the plan according to charts, changes have been made in the organization. It is easier to do this work with a service provider that we have previously worked."

During the implementation of the BCP, most of the communication was conducted through interviews. Luis comments that there was pedagogical element in this as the project sponsors had to explain to those who had not participated in the implementation of the plan because why it was done and how.

Luis comments that the implementation of this type of initiative brought benefits to the organization:

"The implementation of BCM allowed us to provide better practices within the organization. For example, it was suggested to digitalize all paper information from the departments. Such things are not included in the IT DRP and to have the information in digital format guarantee that all it is available for departments that needs it."

Furthermore, Luis asserts that the BCP implementation brought a better understanding of the flow of information, help in the detection of gaps in information management and help

IA to propose plans for improvements in business processes in the long and short term. Thus Luis comments that this tasks are not always straightforward:

"It is not easy to manage resources or reach agreements within the organization to perform this task. There are initiatives that have emerged from the implementation in the departments. There are some initiatives that have been made and others will be performed."

Finally, he comments that the implementation of BCP allowed the organization to detect the areas where homogenization of processes were needed.

Regarding the role of the external consultancy firm in the implementation of the BCP at Grupo Cortefiel, Pablo remarks:

"We have had much contact with the staff responsible for information security and technology. We have several projects with them and have works managing security issues by providing advice on specific projects, strategy and IT security consulting."

Pablo comments that the initiative to implement a BCP in the organization was promoted due to one of the requirements within the best practices in the industry. In regards of sponsorship, Pablo remarks:

"Internal Audit and IT acted as one of the facilitators of the project by making recommendations in regards to this topic. They were sponsors of the project by creating awareness regarding the need to establish a business continuity plan for Grupo Cortefiel. This is also driven directly from the financial management of the company to address the more technical part of computer and information systems used in the company.

Pablo comments that the first stage of the implementation of the BCP consists of acquiring sponsors when the project is launched, learning about the organization, address operational issues and have support from technology.

Furthermore, Pablo provides insights on how the firm where he works with activated its own business continuity plan:

"Old Windsor Tower, located in Madrid business district, caught fire in 2005. There was no loss of life but the entire building was consumed by fire. Deloitte had its main offices there and proceed to activate its own BCP. The following Monday, after the fire, the firm had its critical processes running and all resources in the company employees knew what to do. The experience served to demonstrate that a well being activated plan gives good results."

Pablo comments on the fact that, in his experience, organizations often rely on external consultants to implement the business continuity plan. He asserts that companies who are publicly traded (SEC) tend to count with expert consultant advice because they need professional support with business knowledge and experience from other organizations. He states that depending on internal resources or ability to maintain budgetary plan many companies tend to take an outsourced service to implement and maintain the BCP.

At Grupo Cortefiel, Pablo identifies the key actors that assisted the external consultants in their tasks. He comments that Head of IT Systems and Security led the BCP implementation project while the Head of Group Internal Audit acted as sponsor and collaborated in the project. The consulting team also with support of the financial management of Grupo Cortefiel. Pablo remarks:

"When you have as sponsor the Chief Financial Officer (CFO), this gives a degree of importance and awareness of the project in organizing the activities needed for the implementation of this type of plan."

The methodology used by the external consultants relied on standards and best practices from the Business Continuity Institute (BCI), the British standard BS 25999 and the ISO 22301. Pablo comments on the use of this standards:

"At the end this are just guidelines or best practices on how to perform business continuity. We rely on our own experience and from resources that the organization of information systems ISACA within the area of BCM in the area of good practice provides."

Pablo says that the end result is a phase of continuous improvement in the enterprise in the form of action plans that is enriched with new business processes that arise. At the end is the practical methodology that relies on the ISO methodology on PLAN-DO-CHECK-ACT. Pablo describes the purpose of conducting a business impact analysis:

"The initial objective within the business continuity plan is getting to assemble the business impact analysis (BIA). To perform this first step is to know what recovery capabilities the organization currently has: DRP, alternative sites, external sites, etc. With the organizational business process identified, you can identify the critical process. This task is very important as the external consultant carry out this work of inquiry together with the top management of the organization (higher governance body). At the level of Board of Directors, these are the stakeholders that count with the ability to identify critical processes, less critical processes, the essential business functions and the ideal time when the company needs certain functions and processes to work. With the help of management then the process are organized based on their order of criticality."

Pablo states that to acquire this information, interviews are planned with all leaders and managers responsible for processes. In formulating the IS/IT risk scenarios, Pablo comments that the process involves the identification of which information systems each business process utilize to perform its functions. This can be done with support from the IT department. Pablo notes:

"Already knowing the extent of a technological failure against its business processes, provides light on whether or not to activate the BCP. This is the route by which the technological side is connected with the non-technical side of the business."

To identify critical processes and critical business areas, Pablo comments that this was done according to the vision of the company:

"Within the business impact analysis, business processes related to strategy and corporate governance, business growth and management of the company processes were described. Also risk concerning business processes related to the part of design, logistics and management of stores and franchises. Administrative support activities related to the operations of the company in general were also examined."

Regarding the challenges faced in the organization, Pablo comments:

"The main challenge is to ensure that in a very short time, the external consultant can get a photo (big picture) that depicts what the department or business unit does on a daily basis. The second challenge is that the external consultant is able to use language that business unit can understand. Everything should be made easy for the business process owner to understand. Therefore, the external consultant need to the business language and adequately express what is transmitted correctly"

Pablo considers essential to work with the client in implementing the BCP in conjunction with the sponsor of the project within the organization:

"The sponsor or project manager at the client serves as the interface with the external consultant. If the consultant does not completely knows the organization or if some data or period that can be expressed seasonality of business processes is needed, the sponsor can aid in this function."

While working as an external agent in the organization, Pablo comments on the perception of the implementation in the organization:

"The perception is that today you if you lack the technology needed to perform operations it can cause repercussions. Companies have a high dependence on technology, whether for business necessity or not. In the case of Grupo Cortefiel, the company has a chain of large suppliers and needs to access information for the fleet management for all logistics. Therefore, is technology is critical for all business areas."

The seasonality of each business process was taken into consideration when implementing the BCP. Pablo notes that for Grupo Cortefiel industry, seasonality is very strong in the business processes. He comments that the person who knows very well this information is the sponsor of the project.

"The project is successful is because counting with a sponsor as an ally helps to validate and contextualize the work been done."

Pablo comments that the BCP is a plan that contains a collection set of documentation consist in the BIA, risk maps and a threat landscape map that serves as supporting documents for the organization to assess and manage the implementation of business continuity plan.

"Within the methodology there exist a tree of documents that make up a list of everything the company needs to take the business continuity plan. This are details of how a critical role or function recovers with the help of administrative support. The document explains step by step everything that should be done. The document is not only for a business continuity manager, the document is for a business area. It can be used by a principal or a subordinate who has to perform a business function in case of an incident or disaster."

As a final remark, Pablo comments on the benefits of implementing a BCP:

"A project of this type raises an internal reflection to many business areas that perhaps had not been raised before. Everyone has in mind what to do in case of a fire, but at the time of the fire what a person really do is to act, with no time to think about other things. The time to plan is forgotten."

Pablo sees the contribution of the BCP in the following way:

"The contribution of BCP is seen on each business area: a list, simple steps and guidelines of how to act in case of a crisis. It is a benefit that provides peace of mind to the business. The lifting of such information and formal documentation makes an internal reflection within the organization in a form of an internal continuous improvement in business processes. A more mature an organization is, then the organization is going to have a procedure that can be measured or improved"

Regarding the importance of the BCP, Pablo remarks:

"As director or business manager, it is necessary to know which activities have to recover quickly. The question that arise is which resource in the form of staff you need in order together with a place or space to work or with which technological resources you need in the event of a disaster. This is in case employees cannot work in a normal way, such as when access to a building is prevented due to fire or disaster.

5. Analysis

The empirical data is analyzed according to the themes covered in the study: Enterprise Risk Management and Risk Assessment, Governance of Enterprise IT and Business Continuity. Each theme has been divided into sub themes. The chapter presents the final framework divided in two parts. The first part present an enhanced integrated view regarding Enterprise Risk Management, Risk Assessment and Governance of Enterprise IT in the implementation of a Business Continuity Plan. The second part presents a consolidated perspective on Business Continuity Plan Implementation.

This chapter builds on the empirical findings of Grupo Cortefiel Case Study. The perspective of the study participants were evaluated based on the input obtained from the interviews. A cluster of sub themes have been performed following a triangulation of the perspectives of the study participants. The analysis part is framed by outlining the relationship implied in the integrated view of IS/IT Risk assessment in the implementation of a BCP. According to the empirical findings, each topic has been clustered by sub-theme:

	Theme		
	Enterprise Risk Management & Risk Assessment	Governance of Enterprise IT	Business Continuity Plan Implementation
Sub-Themes	Organizational Functions IS/IT Risk Assessment: Risk ID IS/IT Risk Assessment: Methodology Business Risk and IT Risk on Business Process Risk Consistency on BCP & IT DRP IT Risk Mitigation	Map IS/IT Resources with Business Processes IT DRP & BCP IT Dependency IT Risk Perspective IS/IT & Information Security	Initiative Sponsorship and Leadership Organizational Actors External Consultant BCP Methodology Business Critical Areas and Processes IT Risk Scenario Perception Challenges Benefits

Table 5.1 - Theme Analysis clustered by Sub theme

The final sections cover the relationship between the topics and present the final frameworks:

1. Enhanced Integrated View of IS/IT Risk assessment in the implementation of a Business Continuity Plan.
2. Business Continuity Plan Implementation.

The following sections outline the analysis of each topic per theme and cover in a systematical manner each sub-theme following a triangulation of the interviewees perspectives combined with the theory from the literature review. The triangulation of views is combined with the initial theoretical framework to form an analysis of the implementation of the BCP at the organization.

5.1. Enterprise Risk Management and Risk Assessment

5.1.1. Organizational Functions

Internal Audit provides support for the risk management functions through the performance of audits in the organization. Due to the organization size (multinational company with operating franchises) and industry type of Grupo Cortefiel (manufacturing, retailing and distribution), the IT Department plays an essential role in providing the enablement for business processes. Without the technological platform that is provided by IT, the company would not be able to operate. In the BCP implementation, the external consultant plays an important role when supporting both the IT and Internal Audit functions in order to develop the business continuity plan. As Beasley, Clune and Hermanson (2005) suggest in the literature, an enterprise risk management system is embraced when there is a strong level of leadership and support from corporate boards and senior management. The literature points out that the involvement of this governing bodies is critical to enact an ERM vision since they take accountability on overseeing the portfolio of risks that the organization faces. If not addressed properly, business continuity pose a risk to an organization's operations as internal weaknesses, threats and vulnerabilities create susceptibility to external or internal disasters. This can cause disruption to enterprise operations (Parent & Reich, 2009). Risk management in the organization proved to be effective in providing a significant source of competitive advantage for organizations by enabling a business continuity plan as part of the risk management mitigation strategies.

5.1.2. IS/IT Risk Assessment: Risk Identification

COSO (2004) outlines the risk identification phase as the stage were a set of activities that identify the events that might threaten enterprise business process performance are conducted. This activities may include the collection of background information and the preparation of interviews (Fraser cited in Kmec, 2011). Risk identification, during the IS/IT risk assessment at Grupo Cortefiel, is based on how the IT department is able to provide technological services to the business areas. The prior development of the IT Disaster Recovery Plan (IT DRP), with its core in the data processing center (DPC), already covered and outlined most of the IS/IT risks that Grupo Cortefiel faced. To count with a prior plan for IT recovery aided the company in identifying the dependency of technology in the business processes.

A holistic approach to IT risk identification at the enterprise level involves the assessment on the organizational value chain, the relationship among its components in the business model and a taxonomy to category and analyze those relationships. The notions of technology risk management at Grupo Cortefiel is reinforced by the views that O'Donnell (2005) presents in the systems thinking approach to risk identification. This approach aid the organization in objectives accomplishment by creating a framework for event identification based on a model that emphasize interaction among the components of a value system (O'Donnell, 2005). The literature also points out that an organization that is aware of their risk appetite and tolerance put forward initiatives of IT risk identification in order to secure enterprise operations (Aven, 2013). By enacting risk identification through the IT DRP, Grupo Cortefiel enforced risk management approach to their business operations.

Furthermore, the prior identification of risk through the development of the IT DRP, strengthen the risk identification phase. As Kmec (2011) notes, active risk identification of organizational flaws can be performed by testing internally the overall organization system and exploiting vulnerabilities in the aim of identifying weaknesses and strengths. Even when

Grupo Cortefiel did not tested internally the IT DRP, the company is prepared to face the recovery of the data processing center and their IT infrastructure as part of their risk management initiatives.

5.1.3. IT Risk Assessment: Methodology

Environmental uncertainty, firm complexity, firm size and the monitoring function are factors that have a great influence in conducting the implementation of an ERM program (Gordon, Loeb & Tseng, 2009). Cornell and Cox (2014) discuss that risk analysis can clarify the effectiveness and performance of risk management decisions, their importance in affecting outcomes and as a tool for risk reduction. Due to its uncertainty, probability and impact, the empirical findings show that IS/IT risk is to be measured in a qualitative manner. Quantitative risk analysis on technology can be done if the enterprise counts with a good base, rich information and comparable data. Nosworthy (2000) justifies a qualitative risk approach in technology by stating that, because the majority of threats to information systems defy probability analysis, risk analysis should be carried on the basis of business impact. This is done qualitatively by assigning by assessing and combining probability of occurrence and impact (Purdy, 2010). The literature notes that qualitative risk analysis include adjudicating a risk criteria (low, medium, high), a frequency or likelihood of the event occurrence for each business risk related activity and then quantifying the impact according a consensus base definition from business stakeholders (Cornell and Cox, 2014). During the IS/IT risk identification phase, aided by the external consultant, Grupo Cortefiel applied a qualitative risk assessment when assessing enterprise risks in the BCP implementation pre-event phase.

5.1.4. Business Risk and IT Risk on Business Process

Grupo Cortefiel stated that their main business risk relied primarily on the logistics (supply chain) and financial operations processes. Due to the industry nature, the company main business activities are concentrated in this two areas. IT Dependency in this areas is strong since this operations relies in data and information provided by the company information systems. As the theory indicates, in the digital networked business world, the nature of impact and the risk demands a business continuity approach due to the growing dependency that exist on IS and IT since this risks can severely impact the enterprise (Stanton, 2005; Arduino & Morabito, 2010). Therefore, Grupo Cortefiel adopted a business continuity approach to IT risk embedded in business process as a measure to counteract IT Dependency. This approach is exemplified by the implementation of both the IT DRP and BCP and the empirical findings are aligned with the risk and business continuity theory.

5.1.5. IT DRP & BCP Risk Consistency and IT Risk Mitigation

Stanton (2005) noted that disaster recovery efforts applied mainly to IS/IT systems and infrastructure that took place during and after an organizational crisis. While the IT DRP only covers the restoration of IS/IT critical infrastructure, business continuity focuses on the recovery and continuity of critical business functions required to maintain an acceptable level of operation during an incident (Menkus 1994; Samson, 2013).

In this context, Grupo Cortefiel took a proactive, opposite to a reactive, approach in securing continuity of the business operations through the examination of the past and current business and IT risks. This proactive approach is done before a negative event, crisis or incident materializes in the organization. Grupo Cortefiel adopted a business wide perspective on operations continuity by integrating a business and IS/IT risk approach within the existent IT DRP strategy. Prior to the implementation of the BCP, Grupo Cortefiel had already in place an IT DRP. However, management noted that the outlined IT risks in the BCP needed

to be consistent with the IT risks in the IT DRP. To include and cover for the risks not included in the IT DRP had a financial cost for Grupo Cortefiel since the company needed to acquire a services from an external provider (technological provider). Therefore, Grupo Cortefiel considered carefully the emerging type of risks to include in the IT DRP. Grupo Cortefiel do not solely focused on the recovery of IS/IT activities. Instead the company adopted a holistic view of the enterprise and sought to acquire input from all areas of the business, together with IS/IT. In order to mitigate risks as a result of the dependency in technology, Grupo Cortefiel explore an agreement with an external vendor in order to acquire a service for providing technological equipment for the company employees as well as obtaining access to information systems through a secure virtual private network. Both are actions plans that can enable the company employees to count with the equipment to work remotely in case of an event that activates the BCP.

5.2. Governance of Enterprise IT

5.2.1. Map IS/IT Resources with Business Processes

The literature emphasize that business leaders should develop an awareness of the nature of different IT risks to the business, quantify the impact to their business activities resulting from the loss of information or access to applications, understand the range of tools available to manage IT risk, align the cost of IT Risk management to the business value and construct an institutional capability to act and control IT risk (Hughes, 2006). In order to identify the IS/IT key resources (data, application systems, technologies, facilities and people) that enable business processes, an inventory of services needs to be performed. The service inventory specifies which IS/IT resources participate in the execution of a business processes and is done by acquiring understanding of the business process through interviews. Through interview inquiry, the process is denominated in the practice as "mapping IS/IT resources with business processes".

Prior and during the implementation of the BCP, Grupo Cortefiel had, at an initial level, performed the mapping of business processes together with the IS/IT resources that supported each process. This was done between the IT Department (in the IT DRP), Internal Audit (risk map) and with the collaboration of business areas. The theory aligns with the empirical findings since the difference with the standard risk management guidelines and IS/IT risk assessment is that internal auditors perform an inventory of the organization IT assets and recognize which the assets are critical to business process performance. After completing the inventory (map), risk within IT processes and activities can be managed and assessed in relation their ability to impact the achievement of business objectives (Marks, 2010). This is relevant because in order to conduct the business impact analysis, IS/ IT risk needs to be outlined in clear business terms. In this sense, COBIT 5 (2012a) states that effective risk management requires a mutual understanding between IT and the business over the types of risk that need to be addressed and provide justification on which risk needs to be managed and why. Articulating a map that matches the IS/IT resources that enable business process allows enterprise leaders to assess the extent of a technological failure against business processes and prepare action plans to mitigate business and IT risk.

5.2.2. IT DRP and BCP

The literature points out that, while the IT DRP cover only the risk associated with the loss of physical technological assets (data processing center), the BCP cover the business processes and their associated risk. Menkus (1994) notes that, decades ago, the goal was to safeguard only the computer operations and the physical and virtual resources associated

with them. However, early in the development of the business continuity field, Menkus (1994) asserted that the recovery of business process requires to handle the impact on the organizational key functions through a business continuity approach. Therefore, is not enough to only focus on the IT operations but to adopt an integrated view to risk management within IT and business functions. Arduini and Morabito (2010) asserts that IT DR strategies must treat issues of IT and IS security within a wider internal-external, hardware-software framework. From a GEIT perspective, companies that count with an IT DRP that enables business processes and functions through IT Deployment have a substantial advantage when implementing the BCP because they can count with a solid base to assess dependencies and damages to business processes that are enabled by IT.

5.2.3. IT Dependency

It is a proven fact that enterprises require the assistance of IS/IT key resources to execute from the less to the most critical business processes. In case of a contingency, IT enables remote work through employee personal equipment and virtual private networks as employees need access to information in a daily basis. The theory depicts that firms that operate in turnaround mode are in the midst of a strategic transformation involving IT projects. Firms do so with the objective of gaining competitive advantages and cutting costs. Complementing this view, firms that operate in strategic mode need reliable systems to pursue IT solutions to take advantage of process and service opportunities, reduce costs, and develop competitive advantages (Nolan & McFarlan, 2005). In the study performed by Hérouxa and Fortina (2014), the authors conclude that IT governance mechanisms have a greater use in firms that have a strategic and turnaround modes and the level of involvement of board members, senior executives, IT experts and internal auditors involved in governance effort is higher.

At Grupo Cortefiel, the interviewees asserted that the dependency on technology that the company has on the execution of business processes is very high. The awareness of this dependency prompted the initiative of securing enterprise operations through the implementation of a BCP. The IT Dependency degree in the execution of business processes influence the level of involvement and commitment to IT initiatives and IT risk efforts from the higher governance body (Parent & Reich, 2009; Hérouxa & Fortina, 2014). The steering committee together with the IT Department and Internal Audit, push forward the initiative in the organization and were highly involved in coordinating the activities for the BCP implementation. Therefore, the empirical findings complement the theory by reinforcing the notion that governance mechanisms and IT decision making is influenced by the degree of dependency the organization has on IS/IT resources. The level of dependency on IS/IT resources has an effect on the level of involvement and commitment to IT initiatives that the higher governance body has towards Governance of Enterprise IT. This approach has an impact on the relevance that IS/IT risk assessments have throughout the organization.

5.2.4. IT Risk Perspective

The implementation of a business continuity plan reinforce the views in IT risk management. The interviewees asserted that this type of initiative pose an internal reflection to technological risk as it adds a new risk layer of that needs to be considered in the management of business processes. From a governance on enterprise IT perspective, this is in line with the view of several authors that have pointed out that the process of managing risks associated with the use of technological assets should be an integrated part of the overall governance framework (Iliescu, 2010; Gheorghes, 2010; Marks, 2010).

5.2.5. IS/IT Risk and Information Security Risk

Information security, IS/IT security and IS/IT risk management are fields, that in the practice, operate intrinsically. Abram (2009) asserts that information security exists primarily to manage risks to information and IT resources. Furthermore, the main IT Governance Frameworks propose the existence of three primary objectives from the perspective of IT risk management: security of data and information, the integrity of hardware and systems, and the implementation of IT projects (Parent & Reich, 2009; COBIT 5, 2012a). The deployment of IS/IT brings into perspective a security issues. For this reason, to count with a proper level of engagement in security initiatives from the management and the board is important since the higher governance bodies in the organization are responsible for promoting initiatives that provide oversight of the protection of the enterprise information. As Nolan and McFarlan (2005) note, a lack of board-level IT insight is unsafe because places the organizations at great a level of risk. In order to secure enterprise operations effectively, it is important that the governance board undertake risk management on a continuous basis to ensure that all IS/IT related risks are identified and addressed. Grupo Cortefiel adopted the implementation of a business continuity plan as a security initiative. The company treated the BCP implement as an integral component of the ERM program. The project enriches risk management through identifying and assessing the continuity of business risks related to information security.

The external consultant noted that companies must be aware of implementing cybersecurity to countermeasure cyber risk. Enterprises must add cyber risks to their risk map due to increasing IT dependency that organization possess on IS/IT resources. Bisogni, Cavallini and Di Trocchio (2011) notes that the damage caused by cyber-attacks have a huge economic impact from a societal and economic perspective due to threats that include network penetration and malicious attacks. Therefore, cyber risks are difficult to assess due to the fact that cyberattacks techniques are becoming increasingly sophisticated (Cusack, 2009). The theory merges with practice by asserting that a risk management approach to cybersecurity is a powerful tool to mitigate risk associated with external threats.

5.3. Business Continuity Plan Implementation

5.3.1. Initiative

At Grupo Cortefiel, the BCP implementation initiative sought to align IT recovery disaster capabilities with a strategy to restore business functions. In part, the BCP implementation was promoted by the opportunities for improvement that the external auditor highlighted as a recommendation to secure business operations in case of a negative even that can affect the company. The initiative was driven by the steering committee, IT and Internal Audit department. The IT DRP supported the implementation of the BCP but along itself the tool was not enough to recover business functions and operations in a threat scenario. The literature asserts that the BCP implementation has gain increasing awareness in the industry due to the fact that corporate governance standards have given attention to safeguarding operations and enterprise value to stakeholders, shareholders and customers (Stanton, 2005). However, regulatory compliance is not always the main reason why enterprises implement a BCP. Grupo Cortefiel did not implement the BCP as a regulatory compliance measure but as a preventive control in order to manage people, processes, technology and structures in case of negative event. The initiative was driven as both risk and security measure. Majorly, it concentrated on identifying what external factors could be the drivers for materialization of risk. External factors that can drive IS/IT risk as those factors who circumstances

can increase the frequency or impact of a risk event. This events are not always directly controllable by the enterprise and are compromised by those risk affecting the enterprise geopolitical situation (COBIT 5, 2013). From an external perspective, the fire that consumed Windsor Tower in Madrid, Spain (2005) prompt the Grupo Cortefiel to realize that no business is exempt of the magnitude of such event. Grupo Cortefiel initiative to implement the BCP also come from the realization of the needs to safeguard the enterprise assets through a comprehensive program that aids organizations to design and structure a plan in order to react quickly and effectively when confronting unexpected interruptions, mitigating economic loss and reputational and compliance issues in a crisis, emergency or situations of disaster (Nosworthy, 2000; Samson, 2013).

5.3.2. Sponsorship and Leadership

During the BCP implementation, sponsorship was driven from the awareness from the Steering Committee to count with a system that can ensure the continuity of business operations. The IT Department, supported by Internal Audit, took a leadership role to ensure that this activities were planned and conducted properly. The theory depicts that organizations must seek to acquire, first, the support from the corporate level and, secondly, obtain senior management commitment to the business continuity operations (Samson, 2013). Karakisidis (1997) states that to obtain management approval and support is a key issue in the implementation of BCP processes. Grupo Cortefiel sponsorship from the Steering Committee and management support from the business areas involved in the implementation of the BCP reinforce the literature notions. Moreover, Karakisidis (1997) notes that funding and investment of time and resources for BCP activities related to the development, implementation, testing and maintenance from the plan are needed to make business continuity a reality. Grupo Cortefiel acquired the services of an external consultant that aid the organization in implementing the BCP. To hire this services, the company needed to invest significant amount of financial resources thus the need to make the initiative a reality. The external consultant required organizational sponsorship to acquire information resources to conduct the BCP implementation. This was obtained thanks to the involvement of the IT and Internal Audit department. Early in the development of the business continuity field, Menkus (1994) assert the existence of the difficulties that senior executives and the board of directors had on separating the organization IS and IT activities from the enterprise functions that this resources support. However, this view have changed overtime as technology pervasiveness expands in the execution of business operations. The literature emphasize the importance of counting with sponsorship from the higher organization level of the enterprise (Menkus, 1994; Karakisidis, 1997; Samson, 2013). The interviewees noted that the organization size and complexity of the project required that the implementation of the BCP was guided by the support from the board of directors, CEO, CFO, senior management, IT and Internal Audit. Grupo Cortefiel leaders recognized as an enterprise problem the disruptive impact caused by threats in the organization and to understood the meaning of risk and the nature of the dependency on IS/IT resources. The sponsorship and leadership from the organization constituted a key resource in the BCP implementation.

5.3.3. Organizational Actors

During the implementation of the BCP, Arduini and Morabito (2010) discuss three essential components that deal with each other systematically: technology, people and processes the key actors that were involved in the BCP implementation at Grupo Cortefiel were the Steering Committee, CEO, CFO, Head of IT and Internal Audit Department, business & IT senior management and the external consultant. The literature depicts that in order for

ERM program and initiatives to be implemented in an organization, auditor type, organization size and industry type are factors that contribute to accelerate the adoption of risk management efforts (Beasley, Clune & Hermanson, 2005). Regarding the organization size, Grupo Cortefiel is a large organization that counts with overall 2040 points of sale worldwide in 77 countries, has 1455 direct operate stores and 585 franchises (Grupo Cortefiel, 2015a). Indeed, Grupo Cortefiel is a large organization that requires to secure the enterprise operations in a physical and virtual scale. Beasley, Clune and Hermanson (2005) assert that organizations that conduct their internal and/or external audits with high quality auditors, such as Big Four firms, have a strong commitment to pursue risk management practices. Grupo Cortefiel acquired the services from Deloitte Spain (one of the Big Four firms worldwide) in order to conduct the BCP implementation. The nature of Grupo Cortefiel industry, manufacturing and retail, was also a factor that contribute to the risk management adoption of the BCP initiative as the enterprise operations can be subject to internal and external threats.

5.3.4. External Consultant

The academic literature do not provide any information regarding the role that the external consultant plays in the implementation of the BCP. The literature points out the need for funding and investment of time and resources for BCP supporting activities related to the development, implementation, testing and maintenance from the plan (Karakisidis, 1997), but do not assert how or who aid the organization in conducting this activities. Nevertheless, external auditors, who report independently to the higher governance body, review risk management activities and results ensure that ERM procedures and structures are suitable for the enterprise (Beasley, Clune & Hermanson, 2005). Furthermore auditors that present their independent reviews and communicate them to senior management and the board of directors aid the organization in taking appropriate actions and maintain a consistent ERM framework (Doughtry, 2011).

Prior to the BCP implementation, Deloitte Spain served as Grupo Cortefiel external financial auditor. The responses from the interviewees asserted that Deloitte Spain had a deep knowledge on how the organization operated and that it was more practical to conduct the implementation with an already known external service provider. Samson (2013) indicated that, as in any governance and program management structure, effective planning for business continuity defines role and responsibilities for decision making and communication structures within the organization. The role of the external consultant in the development of the BCP was to develop and document the business impact analysis with comprehensive knowledge of Grupo Cortefiel business processes and to bring an advantage to the organization due to expertise in the BCP field.

5.3.5. BCP Methodology

The external consultant provided the experience and methodology to conduct the BCP implementation. The methodology relies from industry standards and best practices that consist on guidelines on how to perform business continuity. The methodology brought by the external consultant arose from experience and resources from industry professional bodies of knowledge and the produced results are a set of documentation tailored to the context and needs of the organization. Tamineedi (2010) outlines three major phases on BCM: pre-event preparation, event management and post event continuity management. This outline is based on the BS 25999 published by the British Standard Institution. This standard has been replaced by ISO 22301:2012 (The British Standards Institution, 2012). The external consultant, for the basis of knowledge, relied on the ISO framework as guidance for

the implementation. The external consultant combined the knowledge with previous practical experience and resources from other bodies of knowledge. During the interview, the external consultant noted that, at the end, frameworks are just guidelines on how to perform business continuity and that the firm relied on its own hands on experience and academic resources from ISACA. Based on its own experience, Deloitte Spain had a BCP implemented that included objective settings, policies aligned with business and security and outlined implementation phases (training testing, maintenance, monitoring).

The methodology used by the external consultant complements, in a practical manner, the methodology suggested by Karakisidis (1997). The author presents a series of components for the realization of a BCP in the planning phase that include to obtain formal approval, establish a business continuity planning committee, perform business impact analysis, evaluate critical needs and prioritize business requirements, determine the business continuity strategy and associated recovery process and prepare business continuity strategy and its implementation plan. The external consultant aid the organization in the development of this activities using a designed methodology, based on the firm own experience and knowledge, tailored to the specific needs of Grupo Cortefiel.

5.3.6. Business Critical Areas & Processes

During the early stage of the planning phase of the BCP, the literature suggest that business continuity efforts should center on performing identification and assessment of the assets that need to be protected before looking at the possible causes of disruption (Karakasidis, 1997; Stanton, 2005, Tamineedi, 2010; Samson, 2013). In line with this process, Nosworthy (2000) notes that the purpose of conducting a BIA and risk analysis in during the implementation of the BCP is to establish the exposures to threats that the organization faces in order that business and IT leaders can have the necessary information to perform decision making on the enterprise critical functions and areas in regards of risks The BIA performs the identification of critical aspects and components that enable key operations.

To identify the business critical areas and processes, Grupo Cortefiel pursue the strategy to identify all organizational business processes and perform selection of critical processes. This was done by the Chief Financial Officer (CFO) of the organization. Since he is a person relevant to the operations of the organization, he is also part of the Steering Committee. Therefore, the critical areas and processes are chosen by an experienced business leader in the financial and operations sector. This is line with the external consultant view on the participation of the higher governance body in regards that the Board of Directors are the stakeholders have the ability to identify critical processes and the essential business. Management aids in this task by assessing how critical for the organization are the business functions they performed and current recovery. A risk analysis is performed to indicate the criticality of the business process (Karakasidis, 1997; Stanton, 2005; Gibb & Buchanan, 2006). This is documented in the business impact analysis though interview inquiry with higher governance body and top management. To conduct a business impact analysis, the organization must count with a prior inventory of business processes and IT services that support business functions. This is the part of the BCP implementation were mapping IS/IT key resources with business processes, performing a business impact analysis and looking to each business process through a risk management approach converge to provide the organization with deep and clear insights in order to design strategies to define the criticality, protect and recover business operations in a situation of disaster or emergency.

5.3.7. Business and IT Risk Scenario

The development of the business and IT risk scenarios in order to determine the strategies for recoverability of the enterprise are based on the risk analysis performed on business processes and supporting technology. The literature depicts that the results of the risk analysis in the BIA phase are utilized to create impact scenarios that depict how, in the events of risk, the enterprise is affected (Samson, 2013). For this reason, Grupo Cortefiel stated that it was very important for the enterprise to find consistency among the risks outlined in the IT DRP and BCP. Stanton (2005) states that organizations creates loss impact scenarios to develop a sound image of the threats exposure and examine the organizational view on this issues. The external consultant presented a generic list of risks to the organization and from this point the organization chose the risks that pose more threats into the organization. As Tamineedi (2010) outlined, the "worst case scenario" approach is conducted to estimate the effect of disruption on business functions at a critical business location. Grupo Cortefiel IT Department chose the IS/IT risk scenarios that posed a condition of threat to the enterprise operations. The theory depicts that this process is a bottom up approach to risk scenario (COBIT 5, 2012a) since generic risk scenarios were presented by the external consultant to Grupo Cortefiel, the organization proceeded to identify hypothetical scenarios that pose threats to business operations and the risk scenarios were reduced through a high level analysis.

The identification and assessment of risk scenarios were done considering the input that the external consultant obtained with the help of the IT department on which information systems each business process used to perform its functions. This input was obtained also by interviewing business process owners on their day to day functions in regards of the IS/IT resources they used to perform their business operations. Thus, the empirical findings align with the theory by depicting that IS/IT risk scenario analysis bring together technology risk and business leaders to address technological risk in order to obtain an integral view of enterprise risk (Nosworthy, 2000; Pareek, 2012). A determinant factor that drove the BCP implementation was the awareness that came from Grupo Cortefiel senior management (IT and Internal Audit) to have the need be able to cope with any incident or threat scenario that may directly affect the day to day operations of the organization. Risk scenario aided Grupo Cortefiel to establish a picture of the adverse event or risks in the organization to establish evaluation of controls based on real situations. This was a very sensitive issues from senior management as they needed to visualize how to respond to this type of threat scenarios. This is in line with the theory presented by Pareek (2012) who states that depicting how a negative event may impact the enterprise aids in analyzing how to react against threats. This practice is reinforced by the literature presented by Gibb and Buchanan (2006) as the authors state that after the risk analysis phase, the organization can elaborate a map in which prioritization of vulnerabilities against risks is visualized. Since the degree of IT Dependency is high at Grupo Cortefiel, the external consultant noted that already knowing the extent of a technological failure against its business processes through a risk scenario provides light on whether or not the organization should activate the business continuity plan.

5.3.8. Perception

The examined literature do not provide any insights regarding the organizational perception of the participants in the implementation of the BCP. Nevertheless, empirical findings show that there was a positive reception of the overall BCP implementation. However, the project leaders had to deal with sensitivity issues from business process owners in terms of explain how devising the BCP will not affect the funding and resources of the department.

The project leaders had to thoroughly explain to business process owners that the main purpose of the BCP implementation was to recover only the critical processes that guarantee enterprise continuous operations. The BCP project leaders asserted that, from the business process owner's perspective, this could hurt susceptibilities in the organization. Since some business processes were not included in the BCP implementation, there was a need to justify the business process was not seen as critical for the development of business operations. In regards of organizational perception of technology resources, the organizational view was that there could be repercussions if the enterprise lack the technology needed to perform business operations.

5.3.9. Challenges

The examined literature do not provide any insights regarding the organizational challenges of the participants in the implementation of the BCP. The literature does examine how is the overall process of conducting this implementation but do not assert how the project leaders cope with the coordination and execution of the BCP activities. Grupo Cortefiel project leaders asserted that, from a process perspective, the identification of interrelated transversal processes and the decision on how to choose the critical business processes to be included in the BCP was a challenge. From the organizational perspective, the BCP project leaders stated that they encountered a certain degree of complexity and timing issues when coordinating stakeholder interviews due to Grupo Cortefiel size. From a motivational perspective, the BCP project leaders found challenging to explain and communicate the purpose of the BCP purpose across business units. The fact that the BCP implementation was treated as a security initiative help to perform this communication throughout the organization. From a technological perspective, the BCP project leaders asserted that the examination of business process made the enterprise realize that there was a need for better integration and homogenization of enterprise information systems in order to standardize the business value chain. This is a challenge that Grupo Cortefiel need to have in consideration for future business and IT alignment initiatives. Finally, the external consultant noted that, in aiding Grupo Cortefiel to perform the BCP implementation activities, the team should use business language terms, not technical terms, to accurately communicate and transmit the correct information to the business process owners involved in the BCP implementation tasks.

5.3.10. Benefits

The literature notes that the main conducting a BIA and risk analysis in the organization is to establish the exposures to threats that the organization faces (Nosworthy, 2000). This enable enterprise leaders with the information needed to perform accurate decisions in regards of the risks that the organization faces. The BCP implementation at Grupo Cortefiel brought a holistic view to the enterprise in the sense that it contribute with the generation of valuable internal knowledge as well as providing peace of mind in securing enterprise operations. Gibb & Buchanan (2006) notes that after the BIA phase is completed the organization can elaborate a map in which prioritization of vulnerabilities against risks are visualized. The implementation of this type of best practices also benefit the organization in providing a better understanding of the information flow and detect gaps in information management. Internal Audit benefit from the BCP implementation by being able to propose improvement plans to business processes in the long and short term. The BCP implementation benefit the organization in homogenizing and detecting areas where there was a need to standardized business processes. The developed set of BCP documentation that guides stakeholders on how to act in a crisis situation brought an internal reflection that produced a continuous improvement in organizational business processes.

5.4. Final Framework

The final framework is divided in two parts. The first part emphasize the components and the relationships among ERM, Risk Assessment, GEIT and BCM. The second part emphasize the components of the BCP Implementation. Each gray box represents the empirical findings that have been added to the initial theoretical framework in order to compose the final framework. Based on the analysis, additions to the final framework for IS/IT risk assessment includes:

Relationship among ERM, Risk Assessment, GEIT and BCP

In line with the literature, an organizational risk management approach within this fields **increase enterprise and stakeholder value** by becoming part of organizational business processes and decision making, addressing uncertainty, being systemic and timely, tailored to the organization needs and facilitating continual improvement in business processes.

Risk Assessment: IS/IT Risk

1. **Organizational Functions**: Linked to the ERM components. Effective ERM can provide a significant source of competitive advantage for organizations that apply a strong ERM methodology in their organizational functions.

2. **IS/IT Risk Assessment - Risk Identification:** A holistic approach to IT risk identification at the enterprise level that includes the assessment on the organizational value chain, the relationship among its components in the business model and a taxonomy category to analyze risk relationships.

3. **IS/IT Risk Assessment – Methodology:** Technology risk is to be measured in a qualitative manner due to its uncertainty, probability and impact. Quantitative risk analysis is used in highly mature organizations with a control system of quantified risks.

4. **Business Risk and IS/IT Risk on Business Process**: A business continuity approach to IT Risk embedded in business process counteract the increasingly IT Dependency that organization face in order to execute business processes.

5. **Risk Consistency on BCP & IT DRP and IT Risk Mitigation:** IS/IT risk management needs a business wide perspective. An integrated IS/IT risk approach to an IT disaster recovery strategy is to be included in a business continuity framework.

Governance of Enterprise IT

1. **Map IS/IT Resources with Business Processes:** Inventory of services that specifies the IS/IT resources that participate in the execution of business processes. Technological risk is to be measured in relation to the achievement of business objectives and its impact.

2. **IT DRP & BCP:** The IT DRP enables the business processes and functions through IT Deployment while the BCP restore the business critical functions and outline the role of people, structures and technology in the recovery process.

3. **IT Dependency**: Influence the level of involvement and commitment to IT initiatives and IS/IT risk efforts that the higher governance body has towards governance of enterprise IT. Since enterprises need IS/IT key resources to execute from the less to the most critical business processes, the IT Dependency plays a crucial role in organizations.

4. **IT Risk Perspective:** BCP reinforce IT Risk Management. The business add a technological risk layer is added to the components of risk managed within business processes.

5. **IS/IT & Information Security:** BCP implementation is seen as a security initiative in the organization. This initiative enriches ERM through the continuity of business risks related to information security. It adds cyber risks to business risks due to increasing IT dependency.

5.4.1. IS/IT Risk Assessment on the BCP implementation

The following figure represents the final framework for IS/IT Risk assessment in the implementation of a BCP:

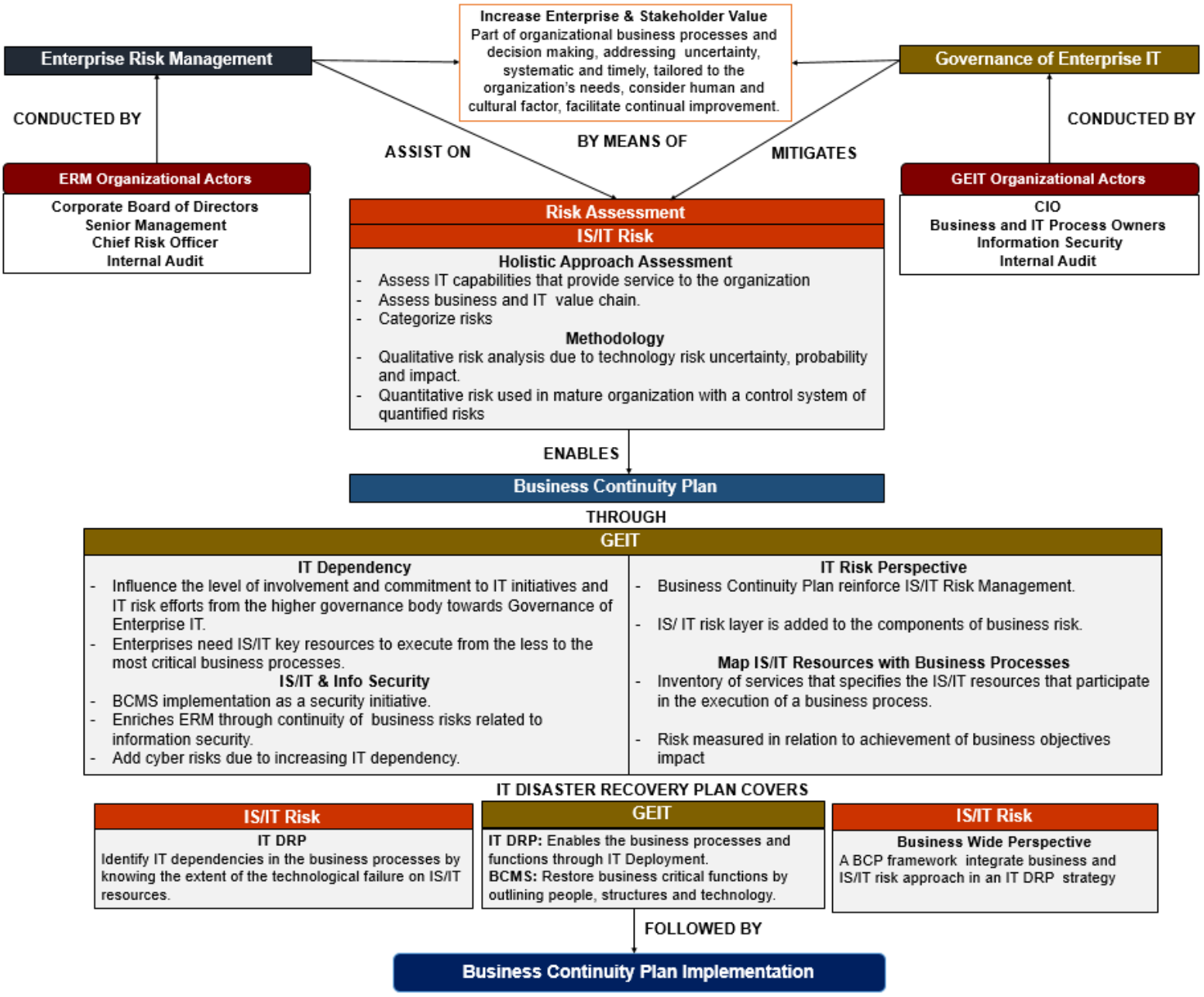


Figure 5.1 - Enhanced Integrated View of IS/IT Risk assessment in the implementation of a BCP

Refer to be Appendix E to visualize the extended framework components of the enhanced integrated view of IS/IT Risk assessment in the implementation of business continuity plan.

5.4.1. Business Continuity Plan Implementation

Based on the analysis, the final framework regarding the BCP implementation includes:

1. **Initiative:** The BCP initiative is **driven by** the need to align IT recovery disaster capabilities with a strategy to restore business functions. The initiative can also derive from the opportunities for improvement outline in the external auditor financial report.

2. **Sponsorship and Leadership:** This factors are **driven by** the awareness from the Steering Committee, IT and Internal Audit has in regards to contribute to secure the enterprise operations. The external consultant requires organizational sponsorship to obtain the resources to conduct the activities related to the BCP implementation.

3. **Organizational Actors:** The sponsorship and leadership for the BCP implementation comes **from** the Steering Committee, CEO and CFO, Head of IT & Internal Audit Department, Business & IT Senior Management and the External Consultant.

4. **External Consultant:** The organization is **aided by** the external consultant expertise in order to develop and document the business impact analysis with comprehensive knowledge of the business processes. To acquire this aid the enterprise need to invest significant amount of financial resources and assign project. The external consultant provides the experience and methodology to conduct the implementation. The external consultant brings an advantage to the organization due to expertise in the BCP field.

5. **BCP Methodology:** The BCP methodology is **supported by** the external consultant. The external consultant provides the guidelines from IS/IT industry standards and best practices. Resources from industry professional bodies of knowledge. Documentation set tailored to the organization context and needs.

6. **Business Critical Areas and Processes:** This task consist in the **identification of** all the organization business processes to perform the selection of the processes that guarantee the enterprise survival against disruption. This decision is based on criticality of the process and is chosen by experienced enterprise leaders in the operations and finance sector. This task also assess current recovery capabilities. The criticality of the business process is depicted in the business impact analysis though interview inquiry with higher governance body, senior management and business IT process owners.

7. **Business and IT Risk Scenario:** The **formulation of** business and IT risk scenarios is based on the risk analysis performed on business and IT processes. The outlines risks should be consistent between the IT DRP and the BCP. Risk simplification can be performed by categorizing threat scenarios. The external consultant presented a generic risk threat map to the organization and the IT Department chose the scenarios that posed a condition of threat to the enterprise operations.

8. **Perception:** The organization **perspective** in regards of the BCP implementation is positive. However, sensitivity issues from business process owners in terms of funding and resources can be encountered. The project leaders had to perform an expla-

nation about the character of the BCP implementation to the business process owners in the fact that the BCP main purpose is to recover only critical processes that guarantee enterprise continuous operations. The perception in regards of technology is that the enterprise lack the technology needed to perform business operations, there could be repercussions in the enterprise level.

The organizational perception in regards of the BCP implementation **covers:**

9. Challenges:

From the BCP project leaders:

- Process: Identify interrelated transversal processes and choose critical business processes to be included in the BCP.

- Organizational: Complexity and timing issues when coordinating stakeholder interviews in a large organization.

- Motivational: Leadership to explain and communicate the BCP purpose across business units.

- Technological: Integration and homogenization of enterprise information systems.

From the external consultant:

- Language: The external consultant relies on business terms, not technical language, in order to communicate and acquire information from the stakeholders involved in the project.

10. Benefits:

The organization benefits from the BCP implementation in several ways:

- Holistic Enterprise View: Internal knowledge value from business processes and IT and peace of mind in securing enterprise operations.

- Best Practices: Provide a better understanding of the information flow, gap detection in information management and aid Internal Audit in proposing improvement plans to business processes in the long and short term.

- Homogenization: Detect areas where there was a need to standardize processes.

- Internal Reflection: Continuous improvement in business processes.

- Documentation: Formal guidelines on how to act in an event of disaster or crisis.

The following figure depicts the business continuity plan implementation at Grupo Cortefiel:

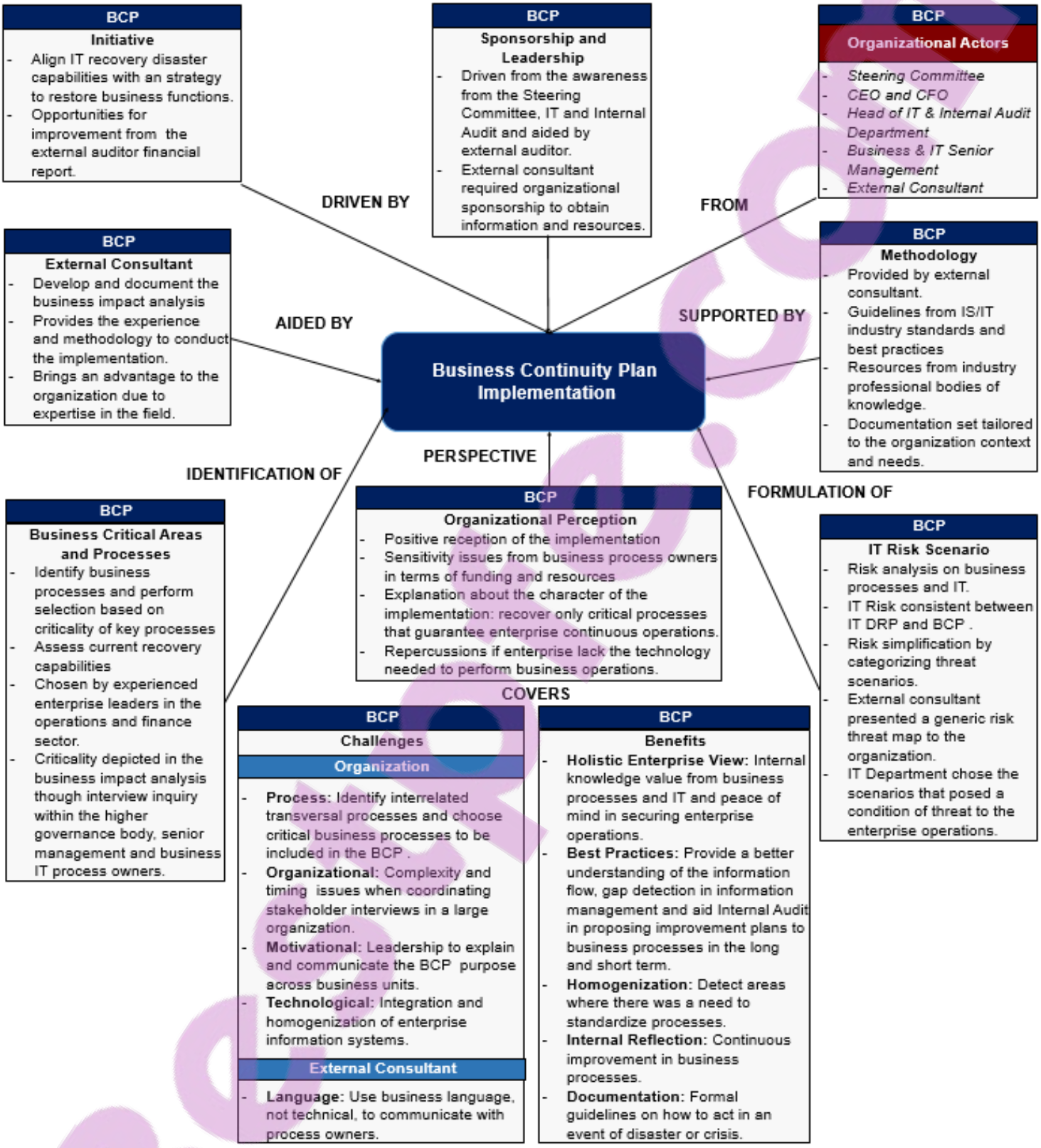


Figure 5.2 - Business Continuity Plan Implementation

6. Conclusion

This chapter aim to answer the research questions of the study.

The purpose of this exploratory study was to assess how the implementation of a business continuity plan is conducted in an international retail and manufacturing enterprise and provide insights on what facilitates its implementation together with its challenges and benefits. **Research question one** focused on identifying the elements that facilitate the implementation of a business continuity plan. The main objective of the implementation of the BCP is to ensure that the enterprise can operate in a situation of crisis that can affect business process performance. There are factors within the organization that facilitate when and how the BCP implementation is conducted. First of all, the dependency that business processes have on IS/IT resources influence how the higher governance body view the need to implement the initiative. This views are correlated on how the organization values activities related to enterprise risk management, IS/IT risk management, IS/IT security and information security. Secondly, for an optimal BCP implementation, is recommended the expertise from an external provider. For organizations, this service is very costly. Only large organizations that can grant financial resources and add internal sponsorship and leadership to the BCP implementation from the enterprise pool of human resources are able to conduct the project at a global scale. Furthermore, in order to perform a proper business impact analysis that presents an accurate risk analysis and risk scenarios, the BCP implementation requires the coordination and collaboration of the external consultant and business and IT leaders. This efforts in itself requires that the enterprise assign resources in order to make the initiative a reality. Thirdly, the BCP implementation must be linked to the core business activities. This should be done with the same determination in which enterprises implement new business units or information systems. The determinant element that facilitates the BCP implementation is how the organization view the role of risk management in the development of the operations. Organizations can no longer afford to view risk and security management issues in an isolated manner or as a sole responsibility of the IT organization. Risk and security management is not exclusive of the technology department but must be viewed from a global perspective. Decades ago, organizations were implementing a BCP based on being able to remain in compliance with local and international regulations. In fact, this could be used as a reason or as an excuse to raise the BCP implementation initiative to the steering committee. As of today, regulatory compliance is no longer a justification to drive the initiative and the BCP implementation should be embedded into the model of corporate governance. This initiative should be guided by a holistic view of risk management and aligned with security policies of the organization. Furthermore, the BCP implementation must count with the sponsorship and leadership of the organizational actors in order to accurately depict the business critical areas and processes so that risk scenarios can be constructed.

Research question two examined what are the challenges and benefits in the organization when conducting the BCP implementation. A major challenge for the BCP implementation relies on the lack of organizational culture regarding risk management. The consolidation of an established enterprise risk culture depends greatly on the type of industry in which the organization operates. If the enterprise already has a solid culture of risk, the BCP implementation will count with steady support and appeal from the actors involved in the process. However, if the enterprise do not count with an organizational culture that revolves around risk management, there is a need to inculcate the value of addressing and managing risk in order to generate value from the BCP implementation. The greatest benefit of the BCP implementation is that it provides stakeholders with a guarantee that the business can survive

in the event of an incident. To perform an internal reflection of the enterprise activities in order to implement a continuity system contributes to the continuous improvement of the organization processes. Business transformation arise from the ability to visualize the business processes that need to be optimized due to the fact that they are not formally defined or aligned with risk management and security policies. Organizations are able to visualize this needs through the BCP implementation. A risk management approach in the initial phase of the BCP implementation contributes to the identification of risks and threats and aims to provide improvement to processes and control mechanisms for the enterprise in order to be prepared against a situation or emergency, crisis or disaster.

7. Discussion

This chapter discusses the findings from the study in relation to the contributions been made to the theory and practical domains. Implications for research and practitioners as well as recommendations for father research are outlined in this chapter.

7.1. Result discussion

The results of this study were based in the theoretical framework and derived from the analysis performed in the empirical findings. The main purpose of the study relied on identifying the elements shaping the implementation of a business continuity plan together with its challenges and benefits. Aided by the theoretical framework, the initial framework for IS/IT risk in the implementation of a business continuity plan was consolidated by outlining the components of each theme in a systematical manner. The interviewees input contributed to further reinforcing, enhancing and expanding the initial framework in order to present the relationships within the themes in the final framework. The frameworks were created to exemplify in the study a conceptual relationship among the themes in order that enterprise leaders can visualize the importance of considering this functions when implementing a business continuity plan. The final frameworks IS/IT Risk Assessment and BCP implementation depict the elements that are shaping the implementation of the initiative. When analyzing the empirical data, a number of sub-themes were identified per theme and the study findings were analyzed by performing a contrast of empirical data and the literature related to each theme. The identified sub-themes consist on the empirical data interpretation of the elements that are shaping the implementation of the BCP. This served as the principal source in order to answer **research question one**. This elements form a combination of organizational processes together with the deployment of resources and are enabled by the interaction of key organizational actors. This convergence of factors facilitate the BCP implementation. Even when it pertains to both ERM and GEIT, IS/IT risk assessment moves towards the ERM function as it is an integral part of risk assessment in the organization. Risk identification and mitigation within risk assessment initiatives lead to identifying business and IT risk in the execution of business processes. To perform the process of mapping the IS/IT resources that enable the business processes allow the enterprise to identify the dependency on IS/IT and adopt a risk perspective into the technological assets. The BCP implementation initiative is promoted based on the relevance that risk management exerts into the organization. Sponsorship and leadership from the organizational actors lead to conduct the implementation activities and aid the external consultant in applying the methodology to conduct the project. The external consultant aids the organization in documenting the criticality of business areas and process in the aim to constructing the risk scenarios.

Research question two aim to identify what were the challenges and benefits during the BCP implementation. The abovementioned elements lead to identify the challenges and benefits that the organization faced during the BCP implementation. The answer related to the challenges is not bases completely in the theory, but leans towards the practical perspective of the BCP project leaders. The analyzed data acknowledge that the project leaders main challenges faced in the organization were related to process, when identifying the critical/transversal business process; organizational, when dealing with the complexity of the task and timing issues with stakeholders; motivational, when communicating the BCP purpose across business unit and technological, when performing the integration and homogenization of enterprise information systems. The external consultant faced the challenge to communicate on business terms, rather than in technical terms, in order to acquire the input that contribute to develop the BCP. The answer related to the benefits obtained by the organization after the BCP implementation is, in part, based in the theory in the sense that the BCP project leaders acquired a holistic enterprise view thanks to the risk management approach that the project entails and the need to secure enterprise operations. Furthermore, the BCP implementation brought to the establishment of best practices. The benefits identified from are related to the standardization of business processes, the continuous improvement brought by promoting the homogenization of this process and the formal set of documentation generated in order guide the organization in the advent of negative circumstances.

7.2. Methods discussion

A single case study, with one unit of analysis in the form of the BCP implementation, was chosen as the research strategy. The decision on why to perform the study was based on the fact that, in order to explore the BCP implementation, the selected organization already needed to count with the experience of implementing the initiative. The author find justification on the decision to perform a single case study based on the purpose of the study, which relies the in the basis of an exploratory and explanatory research. The criteria for selecting the organization did not seek to select an enterprise that operate in a specific industry. This was not a choice that the author consider when selecting the organization. Moreover, since the selected organization is a multinational corporation with a large size and scope, the interviewee selection criteria aimed to obtain responses only from the personnel that was deeply involved in the BCP implementation activities. Therefore, the interviewees were selected taken into consideration this aspect. A much larger interview sample from personnel in the organization would not have been feasible for the author of this study due to the fact that the business stakeholders were not as involved in the implementation as the project leaders. This is accompanied by the fact that timing an issue that limited the author development of the study. Since big consulting firms thrive in a hectic environment, the main project sponsor in the organization aid the author into contact the BCP team leader external consultant responsible for the activities in the BCP implementation. This prove very useful since the external consultant provided an independent view of the implementation elements.

The study was conducted using a qualitative approach due to the fact that the interviews provided insights into the events leading and taking place during the BCP implementation. A quantitative approach, especially when performing technology and business risk analysis, would have not have provided meaningful insights into the BCP implementation. An abductive approach was utilized in order to, based on the theory, enhance the initial theoretical framework as a result of the analysis of the empirical findings. The end result was the creation of a framework divided in two parts: the components of IS/IT risk assessment on the implementation of a BCP and the activities related to the BCP implementation. The results that arose from the interview summary complement and further enhance the theory in the final

frameworks. Due to the inherent tasks pertaining ERM and risk assessment, IS/IT risk was positioned within the ERM field. The decision to do so relies on the fact that a holistic approach to ERM includes the identification, analysis and mitigation of technological risk. The author asserts internal validity of the study by moving away from being bias as much as possible. The creation of the framework do not leave space for bias resulting on the researcher's own views and opinions. In the light of external validity, the study cannot be generalized as applicable to all industry sectors. This study is performed by doing interviews with a small number of participants that collaborated in the BCP implementation thus generalizations cannot be made. Nevertheless, the results of this study are based on the methodological process that the stakeholders involved in the BCP implementation undergo in the manufacturing industry. Therefore, the results can be generalizable to a certain extent in the fact that they demonstrate how and why the implementation of a BCP is conducted in an organization. Regarding reliability of the study, the author makes the study reliable as the interview questions direct the respondent to answer freely and based on its own experience. Response coding was applied to interviewee responses based on their perspectives and perception of the phenomena. Finally, the interviews were conducted in Spanish, transcribed in Spanish and translated to English. Only one interviewee did not allowed to record and transcribe the interview thus the author made use of the interview notes to develop a summary of empirical findings. Therefore, there is a risk in the unsuitable translation of the interview. For this reason, this factor presents a limitation for the study.

7.3. Implication for research

The study converge the views of ERM, GEIT and BCP into one single study. Traditionally, this fields of research in information systems have not been merged in a consolidated manner in order to depict how the BCP implementation is conducted. The results of this study contribute to the bodies of knowledge in the domains of IT governance, IT risk and IT security. In the future, the frameworks for IS/IT risk assessment and BCP implementation can be used as basic models for further refinement as theory develops in this fields of research. The created frameworks can be of interest for the researchers interested in studying the impact that a BCP implementation have in an organization. Concepts of interest that emerged from the performed research are the risk consistency that should exist between the IT DRP and BCP in order to align and cover business and IT risk in a holistic manner, the role of that the external consultant plays in the BCP implementation, the organizational perception related BCP implementation of the actors involved in this activities, the challenges faced by the organization and the benefits that the BCP implementation brought as a whole to the organization. The end frameworks are based on concepts from academic sources, industry standards and guidelines accepted in the risk management community. It utilizes concepts from COBIT and ISO. Therefore, the study already contains a common vocabulary that allows to further enhance the knowledge in the ERM, GEIT and BCP fields of research thus allowing researchers to embody new theory into this domains of study. Therefore the theoretical contribution of this study relies on the construction of the IS/IT risk assessment in the implementation of a BCP framework and the practical contribution relies on the construction of the BCP implementation framework

7.4. Implication for practice

The findings of the study show that the BCP implementation is conducted in an organization when there exist the initiative from the organization to pursue this task in aims of securing the enterprise operations. This requires a risk management approach that considers the role of sponsorship and leadership from the organizational actors and the expertise

from an external agent in order to aid the organization to identify the business critical areas, processes and risk scenarios. Based on the study findings, the author of this study provide recommendations for practitioners in the enterprise risk management, governance of enterprise IT and business continuity field. Even though the findings cannot be generalized, practitioners can rely on this recommendations by obtaining insights from a previous BCP implementation:

- Evaluate the IT Dependency on business processes: Practitioners should focus on obtaining a deep insight on the dependency that business process has on IS/IT resources in order to promote the BCP implementation.
- Adopt a risk management approach: An active approach to risk assessment and taking in consideration the risks that pose threats or can disrupt the business operations in a major scale. This is fostered by encouraging an organizational risk management culture.
- Promote the BCP implementation as a risk and security measure: To ensure the business operations through properly securing and protecting technological assets and involving the business units in the process will create organizational awareness and ease the BCP implementation. The initiative should be promoted at an enterprise level and not be exclusive only to the IT organization.
- Assign internal resources to the initiative: Promote sponsorship and leadership in the organization by assigning project leaders that are accountable for the BCP implementation.
- Acquire external expertise: When possible, considerate obtaining support from an external agent that can provide a state of the art insights through combination of experience and advanced methodology in order to perform the BCP implementation.
- Incorporate the initiative into the governance model: Rather than a compliance requirement, adopt the initiative as part of the elements of a robust corporate governance model.

7.5. Future Research

The theoretical framework of this study covers the relationship among enterprise risk management, risk assessment and governance of enterprise IT in the business continuity plan implementation. The created frameworks represent an innovative approach to merge the theory and practice presented in real context. At first hand, the study identifies the elements that facilitate the business continuity plan implementation together with its challenges and benefits in the retail and manufacturing industry within a one enterprise. It would be of benefit to the research community to gain insights from a comparison of the facilitating elements in organizations that thrive in different industry sectors. Consequently, a study of organizations that have already implemented a business continuity plan can be performed in order to draw similarities and/or differences among several enterprises to acquire understanding of what and how activities related to business continuity are conducted. The study can serve as a benchmark that frame implementation best practices in organizations. Furthermore, researchers can seek to obtain lessons learned from organizations while conducting this benchmark. Regarding the challenges and benefits of the BCP implementation, recommendations for further research include the investigation on how the perception of organizational actors contribute to enhance the organization business continuity and resilience capabilities. This can cover the study on how the implementation of action plans and the continuous process improvement, that arose from the recommendations made through the business continuity implementation, contribute to the enterprise efforts in enterprise risk management and governance of enterprise IT initiatives.

List of References

Abram, T. (2009). The Hidden Value of IT Risk Management. *ISACA Journal, 2*, 1-5.

Arduini, F. and Morabito, V. (2010). Business Continuity and the Banking Industry. *Communications of the ACM, 53* (3), 121-125.

Arena, M., Arnaboldi, M. and Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society, 35* (7), 659–675.

Aunion, J. (2015). *Return to Madrid's towering inferno*. [ONLINE] Available at: http://elpais.com/elpais/2015/02/16/inenglish/1424091787_862295.html. [Accessed 31 March 15].

Aven T. and Zio E (2014). Foundational issues in risk assessment and risk management. *Risk Analysis, 34* (7), 1164–1172.

Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering and System Safety, 96* (7), 719-726.

Aven, T. (2013). On the Meaning and Use of the Risk Appetite Concept. *Risk Analysis, 33* (3), 462-467.

Baker, K. and Filbeck, G. (2014). New Perspectives on Risk Management. *The European Financial Review*. [online] Available at: http://www.europeanfinancialreview.com/?p=3908 [Accessed 24 Feb. 2015].

Baker, N. (2011). Managing the Complexity of Risk. *Internal Auditor, 68* (2) 35-38.

Barton T, Shenkir W, Walker P. (2002). Making enterprise risk management payoff: how leading companies implement risk management. *New York Financial Times Prentice Hall.*

Beasley, M., Clune, R. and Hermanson, D. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24,* 521-531.

Bird, L. (2011). Dictionary of Business Continuity Management Terms. *Business Continuity Institute.*

Bisogni, F., Cavallini, S. and Di Trocchio, S. (2011). Cybersecurity at European Level: The Role of Information Availability. *Communications and Strategies, 1* (81), 105-123.

Boudreau, M.-C. , Chen, A. J., and Huber, M. (2007). *Green IS: Building Sustainable Business Practices.* In Watson, R. T. (ed.) Information Systems (1–15), Athens, GA: Global Text Project.

Bowena, P., Cheung, M. and Rohdeb, F. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information Systems, 8,* 191–221.

Bryman, A. & Bell, E. (2011). *Business research methods.* 3rd edition. Oxford: Oxford University Press.

Cagliano, A., Grimaldi, S. and Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research, 18* (2), 232-248.

Cerullo, V. and Cerullo, M. (2004). Business Continuity Management: A Comprehensive Approach. *Information Systems Management, 21* (3), 70-78.

COBIT 5 (2012a). A business framework for the Governance of Enterprise IT. ISACA.

COBIT 5 (2012b). Enabling Processes. ISACA.

COBIT 5 (2013). Risk. ISACA

COBIT 5 (2014). Risk Scenarios Using COBIT 5. ISACA.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2004). Enterprise risk management integrated framework. *American Institute of Certified Public Accountants.*

Cornell, E. and Cox, L. (2014). Improving Risk Management: From Lame Excuses to Principled Practice. *Risk Analysis, 34* (7), 1228-1238.

Cusack, B. (2009). Assessing Business Value of IT and IS Risk: Security Issues. *ACIS 2009 Proceedings.* Paper 72.

Dali, A. and Lajtha, C. (2012). ISO 31000 Risk Management— "The Gold Standard". *EDPACS: The EDP Audit, Control, and Security Newsletter, 45* (5), 1-8.

De Haes, S. and Van Grembergen, W. (2013). Improving governance of enterprise IT in a major airline: a teaching case. *Journal of Information Technology Teaching Cases, 3,* 60–69.

De Haes, S., Van Grembergen, W. and Debreceny, R. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building blocks and research opportunities. *The Journal of Information Systems, 27* (1), 307–324.

Doughty, K. (2011). The three lines of defense related to risk governance. *ISACA Journal, 5*, 6-8.

Dubois, A. and Gadde, L. (2002). Systematic combining: an abductive approach

To case research. *Journal of Business Research, 55* (7), 553-560.

Emblemsvag, J. (2010). The augmented subjective risk management process. *Management Decision, 48* (2), 248-259.

EY, (2015). [Podcast] EY Risk Culture Framework. Available at: https://www.youtube.com/watch?v=yyeaSw3dITI [Accessed 7 Mar. 2015].

Favaro, K. (2015). *Defining Strategy, Implementation, and Execution*. [online] Harvard Business Review. Available at: https://hbr.org/2015/03/defining-strategy-implementation-and-execution [Accessed 2 Apr. 2015].

Fraser, J.R.S. (2010), "How to prepare a risk profile", in Fraser, J. and Simkins, B.J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Hoboken, NJ, 171-88.

Gheorghe, M. (2010). Audit Methodology for IT Governance. *Informatica Economică, 14* (1), 32-42.

Gibb, F. and Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26* (2), 128-141.

Goble, R. and Bier, V. (2015). Risk Assessment Can Be a Game-Changing Information Technology—But Too Often It Isn't. *Risk Analysis, 33* (11), 1942-1950.

Gonçalves, M. and Misaghi, M. (2014). Proposal of a Framework of Lean Governance and Management of Enterprise IT. In: *Proceedings of iiWAS2014*. CONFENIS2014 Papers, 554-558.

Gordon, L., Loeb, M. and Tseng, C. (2009). Enterprise risk management and firm performance: A contingency perspective. *J. Account. Public Policy, 28* (4), 301-327.

Grupo Cortefiel. (2013). *Corporate Social Responsibility Report 2013*. [online] Grupocortefiel.com. Available at: http://www.grupocortefiel.com/en/corporate-responsibility [Accessed 25 Mar. 2015].

Grupo Cortefiel. (2015a). *Grupo Cortefiel About Us*. [online] Available at: http://www.grupocortefiel.com/en/about-us. [Accessed 17 Mar. 2015].

Grupo Cortefiel. (2015b). *Grupo Cortefiel Springfield*. [online] Available at: http://www.grupocortefiel.com/en/brands/springfield-2. [Accessed 17 Mar. 2015].

Grupo Cortefiel (2015c). *Grupo Cortefiel Women'secret.*. [online] Available at: http://www.grupocortefiel.com/en/marcas/women-secret. [Accessed 17 Mar. 2015].

Grupo Cortefiel (2015d). *Grupo Cortefiel Pedro del Hierro.*. [online] Available at: http://www.grupocortefiel.com/en/brands/pedro-del-hierro-2. [Accessed 17 Mar. 2015].

Guenther, M. (2012). *Intersection. [S.l.]:* Morgan Kaufmann.

Hansson, S. and Aven, T. (2014). Is Risk Analysis Scientific?. *Risk Analysis, 34* (7), 1173-1183.

Harmer, G. (2013). *Governance of Enterprise IT based on COBIT 5: A Management Guide*. Ely, Cambridgeshire, U.K.: IT Governance.

Hérouxa, S. and Fortina, A. (2014). Exploring IT Dependence and IT Governance concerning risk management. *Information Systems Management, 31,* 143–166.

Hillson, D. (1997). Towards a Risk Maturity Model. *The International Journal of Project & Business Risk Management, 1* (1), 35–45.

Holmquist E. (2011). IS Risk and IT Risk: They're Not the Same Thing. *The RMA Journal, 93* (5), 61-65.

Hughes, G. (2006). Five Steps to IT Risk management Best Practices. *Risk Management, 53* (7), 34-40.

Iliescu, F. (2010). Auditing IT Governance. *Informatica Economică, 14* (1), 93-102.

ISO (2009a). Risk management principles and guidelines. ISO 31000:2009

ISO (2009b). Risk management vocabulary. Guide 73:2009

ISO (2012). Societal Security. Business continuity plans Requirements. ISO 22301:2012.

IT Governance Institute, (2005). IT governance domain practices and competencies: IT alignment - Who is in charge?. [online] Rolling Meadows, IL, USA: IT Governance Institute. Available at: http://www.isaca.org/Knowledge-Center/Research/Documents/IT-Alignment-Who-Is-in-Charge_res_Eng_0105.pdf [Accessed 1 Mar. 2015].

Karakasidis, K. (1997). A project planning process for business continuity. *Industrial Management + Data Systems, 97* (8), 320-326.

Kmec, P. (2011). Temporal hierarchy in enterprise risk identification. *Management Decision, 49* (9), 1489-1509

Lavell, J. (2004). Business Continuity Plans: An Overview. *Journal of Investment Compliance, 5* (2), 62-64.

Lewis-Beck, Bryman, and T. F. Liao (2004). *The Sage Encyclopedia of Social Science Research Methods.* Thousand Oaks, CA. Sage

Lukka, K. and Modell, S. (2010) Validation in interpretive management accounting research. *Accounting, Organizations and Society, 35* (4), 462–477

Marks, N. (2010). The Pulse of IT Governance. *Internal Auditor, 67* (4), 32-37.

Melton, A. & Trahan, J. (2009). "Business Continuity Planning", *Risk Management, 56* (10), 46-48.

Menkus, B. (1994). The New Importance of "Business Continuity" in Data Processing Disaster Recovery Planning. *Computer & Security, 13* (2), 115-118.

Miccolis J., Hively K., and Merkley B. (2001) *Enterprise risk management: trends and emerging practices.* Institute of Internal Auditors Research Foundation.

Miles M., Huberman M. and Saldana J. (2014) *Qualitative data Analysis: A Methods Sourcebook. Thousand Oaks.* Sage Publications.

Nolan, R.. and McFarlan F. (2005). Information technology and the boards of directors. *Harvard Business Review, 83* (10), 96–106.

Nosworthy, J. (2000). A Practical Risk Analysis Approach: Managing BCM Risk. *Computers*

& Security, 19 (7), 596-614.

O'Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. *International Journal of Accounting Information Systems, 6* (3), 177-195.

Olson, D.L. and Wu, D. (2010), *Enterprise Risk Management Models*. Springer-Verlag, Heidelberg.

Pareek, M. (2012). Using Scenario Analysis for Managing Technology Risk. *ISACA Journal, 6,* 1-6

Parent, M. and Reich, B. (2009). Governing Information Technology Risk. *California Management Review, 51* (3), 134-151.

Posthumus, S., von Solms, R. and King, M. (2010). The board and IT governance: The what, who and how. *South Africa Journal of Business Management, 41* (3), 23-32.

Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide*). 4th ed. Newtown Square, PA: PMI.

Purdy, G. (2010). ISO 31000:2009—Setting a New Standard for Risk Management. *Risk Analysis, 30* (6), 881-886.

Richardson, R. and Kramer, E.H. (2006). Abduction as the type of inference that characterizes the development of a grounded theory. *Qualitative Research, 6* (4), 497-513.

Robson, C. (2002) *Real World Research.* Blackwell. 2nd edition.

Samson, P (2013). "Beyond the First 48 Hours: Can Business Continuity Management Go the Distance", *Financial Executive, 29* (5), 54-57.

Saunders, M., Lewis, P. and Thornhill, A. (2009). *Research methods for business students*. 5th edition. Harlow: Financial Times Prentice Hall.

Stanton, R. (2005). Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security, 7,* 18-19.

Tammineedi, R. (2010). Business Continuity Management: A Standards Based Approach. *Information Security Journal: A Global Perspective, 19* (1), 36–50.

The British Standards Institution, (2012). *Moving from BS 25999-2 to ISO 22301: The new international standard for business continuity plans.* London, W4 4AL United Kingdom: The British Standards Institution. REPORT

Timmermans, S. and Tavory I. (2012). Theory Construction In Qualitative Research: From Grounded Theory To Abductive Analysis. *Sociological Theory American Sociological Association, 30* (3), 167– 186.

Too, E. and Weaver, P. (2014). The management of project management: A conceptual framework for project governance. *International Journal of Project Management, 32* (8), 1382–1394.

Van, d.S (2009). Enterprise Governance. *Financial Management,* 38-40.

Wagner, K. (2007). Technical Storm. *Journal of Property Management, 72* (3), 40-45.

Weill, P. and Ross, J.W. (2004*). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.* Harvard Business School Press, Boston, MA.

Yin, R.K. (2009). *Case study research: design and methods*. 4th edition. London: SAGE.

Yin, R. K. (2011). *Qualitative research from start to finish*. New York: Guilford Press.

Zsidisin, G., Melnyk, S. and Ragatz, G. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research, 43* (16), 3401–3420.

Appendix

A. Interview Guide

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
JÖNKÖPING UNIVERSITY

INTERVIEW GUIDE

Acronyms: Enterprise Risk Management **(ERM)** & IS/IT Risk Assessment **(IS/IT Risk)**, Governance of Enterprise IT **(GEIT)**, Business Continuity Plan **(BCP)**
Participants: Grupo Cortefiel Head of IT Systems & Security **(IT)**, Grupo Cortefiel Head of Internal Audit **(IA)** and Deloitte BCMS External Consultant **(EC)**

Participant	Theme	Question
IT, IA & EC	Introduction	Can you tell me about yourself, your role in the organization and the role you played in the implementation of the business continuity plan?
IT & IA	BCP	Can you tell me how the initiative to implement a business continuity plan arosed in the organization?
IT & IA	BCP	What factors acted as drivers for the implementation of the business continuity plan?
IT & IA	BCP	Which role the key actors played in the implementation of the business continuity plan?
IT, IA & EC	BCP	Can you tell me about the methodology or guidelines that were utilized during the implementation of the BCP?
IT, IA & EC	BCP	How was the interview process conducted with each business area?
IT, IA & EC	BCP	How was the business process peak moment (stationary time) taken into consideration during the implementation of the business continuity plan?
IT & IA	BCP	What was the criteria for selecting the external provider for the implementation of the business continuity plan?
EC	BCP	How did the external consultant got the engagement concerning the implementation of the BCP at the client?
EC	BCP	Can you tell me how the initiative to implement a business continuity plan was promoted in the organization?
EC	BCP	Could you please tell me how the firm activated its own business continuity plan when confronted with a situation of disaster?
EC	BCP	How was the activities with the organization managed during the documentation of the business continuity plan?
IT, IA & EC	BCP	What were the benefits that the organization obtained after the implementation of the business continuity plan?
IT & IA	BCP	Who were the key actors in the implementation of the business continuity plan?
IT, IA & EC	BCP	How was the development of the implementation of the BCP at an organizational level?
IT, IA & EC	BCP	Can you mention the challenges that the organization confronted when implementing the BCP?
IT, IA & EC	BCP	How was the identification of critical process and areas performed during the implementation of the business continuity plan?
IT, IA & EC	BCP	What organizational elements within your department assisted in the implementation of the business continuity plan?
IT, IA & EC	BCP	What was the perception of the implementation of the business continuity plan in the organization?
IT, IA & EC	BCP	Who and what role organizational agents conducted within the organization when performing the process of mapping information systems and technology infrastructure with business processes?
IT & IA	BCP	How fo you consider the participation of the external service provider in relation to the implementation of the business continuity plan?
IT & IA	BCP	How was the comunication performed in the organization during the implementation of the business continuity plan?
EC	BCP	How and why an organization decides to implement a business continuity plan?
EC	BCP	How do you see the future of business continuity at the enterprise level?
IT & IA	ERM	How were risks approach in the organization during the implementation of the business continuity plan?
IT, IA & EC	ERM	How and where were the identified risks prioritized during the implementation of the business continuity plan?
IA	ERM	Which role plays your area in the development of operations Grupo Cortefiel?
EC	ERM	Can you explain me which process areas were examined during the implementation of the business continuity plan?
IT, IA & EC	ERM & IS/IT Risk	What were the main business and technology risks identified during the implementation of the business continuity plan?
IT & IA	ERM & IS/IT Risk	What is the perspective of risk obtained with the implementation of the business continuity plan in your area?
IT, IA & EC	GEIT	Can you tell me about the process of mapping business processes with information systems?
IT	GEIT	What was the time frame between the implementation of the IT Disaster Recovery Plan and the implementtaion of the business continuity plan?
IT & EC	GEIT	How were the IS/IT risks scenarios formulated within the business process?
EC	GEIT	What is the relationship between the development of the IT Disaster Recovery Plan and the Business Continuity Plan?
EC	GEIT	Can you tell me how the business continuity plan was implemented, based on the previous existence of an IT Disaster Recovery Plan in the organization?
EC	GEIT	How was the perception of the business leaders/ process ownes in relation with technology components?
EC	GEIT	What is the degree of dependency that the organization have on the technology that they use?
IT	GEIT	What is the perspective of risk obtained with the implementation of the business continuity plan for the technology area?

B. Interview Details

INTERVIEW DETAILS						
#	Name	Position	Company	Interview		
				Date	Channel	Length
1	David Moreno del Cerro	Head of IT Systems and Security	Grupo Cortefiel	4/6/2015	Skype Call	90 MIN
2	Luis Mesa	Head of Internal Audit		4/23/2015		30 MIN
3	Pablo Rodriguez Cabellos	BCMS Implementation Team Leader	Deloitte Spain	4/10/2015		90 MIN

C. Interview Transcripts

C1. Interview 1 - GC Head of IT Systems and Security

David Moreno Del Cerro - Grupo Cortefiel Head of ITS Systems and Security

The interview was conducted with David Moreno del Cerro, Head of Systems and Security Department at Grupo Cortefiel on Monday April 6th, 2015 16:00 – 17:30.

Introduction

1. **Can you tell me about yourself, your role in the organization and the role you played in the implementation of the business continuity plan?**

I am the responsible for the security system, my liability is based on the management of all the technological infrastructure that the company possess both in Spain and in the rest of the world. I am in charge of the technological infrastructure concerning not only the part of computer equipment on servers but also the communication, physical and logical information security assets and procedures. I also have to do with everything related to the various services offered from the Department of Information Technology of Grupo Cortefiel.

ERM and IS/IT Risk

2. **Which role plays your area in the operations development of Grupo Cortefiel?**

This department is essential as all business processes are based on the technology services that the department offers. The company, without the support of technology may not work. No company in the world can do without technology. In a hypothetical case of a complete loss of all IT services, shops are autonomous to some extent. A store may sell autonomously for up to one week. After this time the store would not run commodity prices, cannot update the need for more stock and at the end the store begin to be inoperative. Therefore technology is fundamental for both the development of the operations of the company and in the assessment of the processes that concern business and technology in the implementation of the business continuity plan.

3. **What were the main business and technology risks identified during the implementation of the business continuity plan?**

The following were the main business and technology risks identified:

- There were certain inconsistencies between services that were included in the IT Disaster Recovery Plan and the processes that emerged from the business impact analysis. We had to adjust the IT DRP (contingency plan9 to make it consistent with the BCP.
- There was technological risk over logistics and operation. To have sufficient computer equipment to service a number of users at a particular time that may need a computer, printer, mobile phone to execute their operations was a risk. The company, in this case, should have a secured stock of computers for users contemplated within the business continuity plan or have an agreement with a company that could provide computers when Grupo Cortefiel requested.
- Since the company counted with an IT Disaster Recovery Plan that is tested and adjusted annually, most IT risks were already identified and corrected.

4. How and where were the identified risks prioritized during the implementation of the business continuity plan?

The element of risk were located in the supply chain – to ensure that the goods are distributed correctly and that there exist merchandise in stores to sell - and in the financial processes for paying suppliers. The main risk facing the company was that it can be unable to pay suppliers on time and not being able to meet financial obligations. Failure to provide timely financial information requested can cause the company to go into default and our investment funds could execute the debt that the company previously acquired. It is a problem of reliability.

5. How were risks approached in the organization during the implementation of the business continuity plan?

The approach to risks in the area of technology was based on the ability to provide the services that the company needed in different situations. The risks were lower because the company already had had a previous work in the form of an IT DRP. The department assured that the services included within the IT DRP were consistent with the BCP. The initial risks reflected in the IT DRP had to be adjusted because there were only two or three risk scenarios when, for instance, in the BCP there are many more risk scenarios. Risk of a pandemic or a judicial or police incident that prevent employees to enter the building is a risk for the company operations. One possibility to countermeasure this was to include in the plan that different company employees could work from home. To meet this need, the company enter an arrangement with one of the major telecommunications company in Spain by hiring a service or remote access virtual private network connection so that employees can even resume their work from an external site. This set expectations for the technology resources needed for the business areas when performing the BCP implementation.

6. Can you tell me about the process of mapping business processes with information systems?

It is a map of a very high standard. Consists in linking business processes with the various services provided from the area of IT. Each specific process is placed with its *"first and last name"* (technological resources that support the function are specifically identified). It goes to a very detailed level as it matches the IS/IT resources with the applications it supports. In the event that there is a problem with a company server, which affects IT services and business processes, the company will be able to identify where it resides the technological impact.

We were surprised by the information obtained from users because we realized we had processes that were being external to IT. In other words, there were certain elements that users

had been putting together over time and had sufficient importance in the business unit to incorporate services that are offered from IT.

Governance of Enterprise IT

7. What was the time frame between the implementation of the IT Disaster Recovery Plan and the implementation of the Business Continuity Plan?

After two years of the beginning of the implementation of the IT DRP, the plan was adjusted so that it was 100% functional. It was possible to include in the IT DRP all the services the company at that time established as critical and the recovery time to lift critical services that the company requested. In practice this was done in around four years. This period was marked by an economic moment lived in Spain, where there was a crisis, and companies had to make adjustments at all levels. Budgets were focused on continuing the operation with minimal investment. As the company already had an IT DRP, the company determined that it could survive in the event of an incident without a business continuity plan. When the IT DRP was performed, the processes were included in a map together with an inventory of assets and human resources that were needed to operate IT services. This was documented in the IT DRP. Therefore it was not a complete BCP, but the company counted with a basic plan for disaster recovery that was not a purely IT vision. There was enough information so that the company could decide to postpone the development and implementation of BCP. The completion of the BCP was made when the economic conditions of the company improved. The IT department, the internal audit area and the various annual financial audits prompted the initiative because the company did not have a business continuity plan well founded and developed and that went according to the structure of the company. The suggestion came primarily from the Steering Committee. The strongest pressure was from the Steering Committee and the governing bodies together with IT and Internal Audit department. Every year in the annual report, the external consultant that conducted the financial audit, marked as one the areas of improvements the fact that the company needed to strengthen the area of business continuity. All this facts came to support the implementation of a business continuity plan.

8. How were the IS/IT risks scenarios formulated within the business process?

When the critical business processes were defined, we verified that those same business processes were included in the contingency plan. If the business process is included in the contingency plan, there was already all the necessary information. We review the plan to update it and test it on annual basis. If the critical business process were not included within the contingency plan, there was an analysis to whether it made sense to include the business process in the contingency plan. The IT DRP provides that in a maximum of 48 hours IT services must be established to provide essential operations for the company. This does not mean that there are other services that cannot be reinstated within 48 hours and are equally important. Two levels of urgency: 48 hours critical level and there are other processes that can be expected to be restored within 72 hours. These processes are not treated with the immediacy with which a critical process is. This analysis was done because the process to include inside the contingency plan a critical process (not included previously) has an economic cost since it is done via an outsourced service. Sometimes the cost does not justify include business process within the contingency plan. After this process, risk scenarios were formulated according to each critical business process. There were 3-4 business processes that were not included in the contingency plan and were necessary to include. Renegotiation was performed with the external vendor in charge to host these processes.

The BCP external consultant presented a generic map of physical, logical, organizational threats to technology. Based on a list of 20 or 25 threat landscape in the generic risk map, the technology department chose the scenarios that posed a condition of threat to the enterprise operations. Example, an earthquake is unlikely in Madrid and was discarded. Fire, flood, power problems by adjacent works are more likely to happen. These were external scenarios. In regards of internal scenarios, a succession plan in which detailed human resources are replacing a position or role in the event that the employee is unavailable was developed. This was an interesting job because it was not available before the development of this plan. The succession plan existed only at a Steering Committee and senior levels. HR together with the BCP external consultant collaborated to gather a succession plan for those scenarios where for any contingency a business owner could not have the primary responsibility for the business areas he or she was in charge of. IS/IT risk included sabotage or theft and this were more internal risks. The vast majority of identified risks were exemplified through external scenarios.

9. What is the perspective of risk obtained with the implementation of the business continuity plan for the technology area?

Since we already counted with an IT DRP were technology risks were identified and known in the company, the business continuity plan only came to reinforce our view in regards of technology risk.

Business continuity plan

10. Can you tell me how the initiative to implement a business continuity plan arose in the organization?

In 2007/2008, the organization launched a process of response to incidents involving the company data processing center (DPC) located in the company headquarter in Madrid. The company used this plan as a contingency for the technology area. This plan was focused on giving continuity to the IT services of the company in case there was a disaster in the building where the DPC was located. This was done as a preventive measure. In order to counterpart the fact that a disaster can affect wholly or in part to the services offered, the company device an IT Disaster Recovery Plan (IT DRP). The plan was launched in 2008 and it was done with the help of IBM, that assisted in in the whole process data replication and infrastructure in an alternate data center. The IT DRP was very focused on IT processes and did not have a global scope. It was not linked to business processes beyond the infrastructure services. At this point we count with an overall view of the IT stage. After a few years and motivated by a number of external circumstances that have been happening (terrorism attacks, cyber threats), in 2010 the Steering Committee and the Board of Directors set a goal to achieve in a relatively short time the implementation of a business continuity plan, not only from the standpoint of technology but also from the point of view of the business processes of the company. Perhaps this was something that should have been done when the disaster recovery plan was developed, but in practice the business continuity plan was not addressed. This was also partly because the company had no internal resources or expertise to develop a business continuity plan. The implementation of a BCP is more complex because it affects processes beyond the technology and there was a growing concern for counting with this type of plan.

11. What factors acted as drivers for the implementation of the business continuity plan?

A determinant factor was the awareness that came from the company management to have the need be able to cope with any incident or threat scenario that may directly affect the day to day operations. The company has presence in 75 countries with over 2000 outlets. The vast majority of the technological services offered by the company's own stores or franchise operations are centralized in the building that the company has in Madrid. This make that any incident affecting the building has a rather catastrophic effect with respect to the headquarters and shops. There was a sensitivity on the part of management to be able to respond to this type of threat scenarios. Also, in order to support the technological part, a contingency plan had been drawn. However, there is no sense having a contingency plan for the area of technology without a business continuity plan. In the event of a disaster in the department, there is no sense that the IT department knew what to do or to be capable of serving in a short period of time the operations, but that other departments (business units) did not know to do. It is a rather anomalous situation. The contingency plan covered only the critical processes of technology in the data processing center of Grupo Cortefiel in Madrid.

12. Who were the key actors and which role they played in the implementation of the business continuity plan?

- Technology: I was the project manager and acted as coordinator of all work done.
- Internal Audit: Provide overview map of risk linked to the company, the information they manage and report regularly to the risk committee. Beyond the risks of technology that manages the technology department, Internal Audit I offer business risks. These risks have already been agreed with the organization.
- Steering Committee: Promote the plan and approve it.
- Business Areas: Provide the experience and knowledge of how each area works and systems used, how they operate and what resources are essential for implementation of the business process.
- External Consultant: Gather information from different areas of the organization, organize information in an orderly and manageable way. Provide expertise in developing the BCP. Conducting the interview with the business area and obtained information really necessary.

13. What organizational elements within your department assisted in the implementation of the business continuity plan?

The IT department had the advantage that there was a disaster recovery plan already in place. What is certain is that the experience made the business (Grupo Cortefiel) observe the draft of the business continuity plan with a much more open view and without being experts who are knowledgeable of the requirements that are demanded. Internally, within the IT department, we have been driving initiatives related to risk management and security scenarios that make us feel comfortable with the preparation of this plan and the business continuity activities. I collaborated closely with the consultant and other areas of the company. The technology department was the department who led the coordination of interviews, preparation of business impact analysis and mapping information systems linked to business processes.

14. What was the criteria for selecting the external provider for the implementation of the business continuity plan?

Back at that time, the contingency plan / IT disaster recovery plan was carried out with IBM and there were other diverse security initiatives underway with KPMG. Deloitte offered the organization a more concrete vision of our business because they are our financial auditors and because they have confronted themselves a situation of disaster were the company had to activate its own BCP. In 2005, Deloitte Spain had a serious incident in Madrid in which the firm lost all of their physical offices (headquarter) h following a catastrophic fire that destroyed the Torre Windsor skyscraper entirely. The experience Deloitte suffered showed that they were able to restore operations after a disaster situation like that have happened in their organization. Grupo Cortefiel chose Deloitte Spain as the most appropriate external consultancy firm in order to implement the business continuity plan.

15. How was the development of the implementation of the BCP at an organizational level?

The key was to count with management support. Without the support and the leadership of management it would have been virtually impossible to do this project because there are many business units within the organization and it is difficult to coordinate any action on a transversal level among the units. Without the sponsorship from the Board of Directors and management, it would have been very complicated to implement the BCP. The first part in the development of the project was to acquire the commitment of the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO). The second part was to decide whether the continuity plan was done internally or externally. The company decided to have the support of an entity external consultant to conduct the business continuity plan. The industry of the company is manufacturing and scrap. The company is expert in carrying out the development of a business continuity plan. For transparency and objectivity, the company decided to have an external agent which would bring the knowledge and experience of customers from the same industry at the time of preparing the BCP.
There were two pillars that enable the implementation of the BCP: Board of Directors and management support together with the decision of how and with whom to conduct the BCP implementation. We made a tender in order to choose the supplier. The supplier presented a focus of how the project would work, the planning, the definition of the project and those responsible within the company for supporting the external company in making the plan. Moreover also included on how to acquire the know-how knowledge to keep the business continuity plan alive. Grupo Cortefiel chose Deloitte Spain as the service provider in the implementation of BCP.

16. Can you mention the challenges that the organization confronted when implementing the BCP?

Among the areas of business and technology units there existed some challenges:
Challenge 1: Decide which processes within the organization fell within the business continuity plan and which did not. The main challenge was to identify optimally which processes were to be included in the business continuity plan. These processes would later be the ones that were to be included in the BIA.

Challenge 2: Organizational challenge. In the company there are 80 departments of which 25 to 30 departments entered into the business continuity plan. To coordinate interviews with each of those responsible in order that Deloitte, the external consultant, understood how the

internal process fit with the rest of processes was a challenge. This was done to provide insights to create a Grupo Cortefiel process general map. The coordination of interviews and internal resources needed to conduct the BCP implementationpresented a complex organizational issue.

Challenge 3: Motivate and communicate to the business units the importance of completing the business continuity plan. It is important to have the leadership to boost the plan but it is also important to have the support and understanding of the owners of the business processes. Communicate the importance of developing the BCP, communicating the company vision on this plan to ensure the continuity of business operations and what to do if disaster occurs. Also that personnel understood the specific impact and business operations recovery time and availability of the service was a challenge.

17. **What were the challenges in coordinating activities in implementing the plan?**

To close agendas and getting updated information from each department were challenges in coordinating activities. Rotation in the company is not high, but there are internal changes within itself so to keep information current (example: having personal telephone numbers of employees and address where you they can be reached if case of an event) is an issue that is delicate by Spanish data protection law. One must know how to manage this information very carefully. There were organizational and continuous improvement challenges: perform review, simulation and training to mobilize many people in case of a disaster. By role play we did a simulation of a contingency or incident and ensure that everyone knew what to do in case of invocation of the plan.
The IT DRP refers specifically to the data processing center of Madrid, where services are centralized. The logistics center also has a BCP and is consistent with our BCP. A future challenge is to increase the scope of BCP to other geographical areas where the company operates.

18. **How was the identification of critical process and areas performed during the implementation of the business continuity plan?**

To make this choice, the person who took the decision regarding what business processes were to be included was the CFO (Chief Financial Officer). This person has been in the company for 24 years and has a global view of all business processes (from the simplest to the most complex). Not only the CFO has the vision of the financial and economic area but also has contact with other areas of the company because he is a member of the Steering Committee. These processes would later be the ones that were to be included in the BIA.

19. **Can you tell me about the methodology or guidelines that were utilized during the implementation of the BCP?**

The methodology or guidelines were brought by the external consultant. They help us to implement the BCP based on the best practices in the industry.

20. **What was the perception of the implementation of the business continuity plan in the organization?**

The business area managers fully understand the how and why of the implementation of business continuity plan. It is human nature that had to lower expectations a bit since at the end the business area managers thought they were going to develop a plan that, in a case of incident, the company can operate at 100%. This is not the case as the company is to return

to a sufficient level in regards of the most critical processes that can be operational to be able to continue working. The cost including ALL business processes as critical is not acceptable. It was very costly to explain to the business owners that the business continuity plan was only able to react in case of a contingency. Therefore, the business area do not have to give 100% of their service. During the implementation process, some interviewees said that in order to restore their business process in case of an event they needed to count with the same resources or more and this was not certainly the goal of the implementation.

As a remark of Spanish culture: when the business owners were told that in the BCP document, in case of a contingency, the business area could operate with 8 people instead of 20 people was a cause of suspicion in the organization. It is possible that business process owners think that will take away resources or funds. There were business owners who are not comfortable in knowing that their business process would not be included in the BCP. They felt left out as their process was not seen as a critical business process. However, the fact that there are critical process does not mean that other processes are not as important. We had to deal with some negativity in the organization, but overall reception plan implementation was very positive**.**

21. How was the interview process conducted with each business area?

Between the team leaders and the external consultant, each director of department or business unit was explained about the purpose of carrying out the BCP. Each director explained how his department function, how the activities were interrelated with other areas of the company, what resources were essential to operate, what and how many human resources is needed to provide the minimum service from the operations in case of disruption, description of technology and software resources needed for conducting its business process and what their seasonal moments (peak load) were.

22. How was the business process peak moment (stationary time) taken into consideration during the implementation of the business continuity plan?

The moments in time, also known as seasonality, of each process greatly influences how an issue concerning business disruption affects the company. This was a key part in interviews. Each department gave a calendar of seasonality of its process and labeled the incidents that, at a specific time of year, affect in great percentage the operations of the company. It was fundamental. We had to ask, by interviewing business leaders, about what these moments were and the time it happened and be clear about the days in which if an incident occurs, there could be a seasonal effect on the company as it affects business processes (depending on the severity of the incident).

23. Who and what role organizational agents conducted within the organization when performing the process of mapping information systems and technology infrastructure with business processes?

There was a mix of resources to execute this task. The map of processes and information systems and technology infrastructure belonged to the organization. The external consultant helped bring order to this documentation. With 80 departments and a large infrastructure at Grupo Cortefiel, the task to put order in regards of this documentation was a complicated process. The external consultant brought documentation templates in the aim of documenting the map clearly and simply way.

24. How do you consider the participation of the external service provider in relation to the implementation of the business continuity plan?

It was important the role of the external consultant performance, mostly in developing the BIA. This development requires having a fairly comprehensive knowledge of all business processes, how the company works and also required the development of documentation. As this is extensive work, at that time Grupo Cortefiel would not have been able to take on this task. Furthermore, having the most objective view from an outsider to analyze our situation help us because the external consultant was able to approach company issues differently and based on that, to suggest different decisions. There are tasks that are still being conducted with the external consultant regarding initiatives: user training and maintenance of the plan. To count with resources and experience from the external consultant turned out to be an advantage for Grupo Cortefiel in regards of the BCP implementation.

25. How was the communication performed in the organization during the implementation of the business continuity plan?

There was an internal communication plan that was performed by a direct request from our CEO to the various department heads to get involved in developing the plan referring to our corporate security policy explaining it because of the development of the plan and asking the direct collaboration of these people. Through the channels of communication with the employee (email and intranet) stakeholder were informed about the development of the plan, its purpose and the documentation that each department needed to manage individually for completion of the business continuity plan.

Conclusion

26. What were the benefits that the organization obtained after the implementation of the business continuity plan?

The main benefit was that the company was able to obtain a big picture of the organization. There was an agreement of information with all stakeholders: senior management and business process owners. Having a clear picture of what the critical business processes were, which processes were required for a company like Grupo Cortefiel to run and how they react in the event of a contingency were benefits we acquired with the implementation of this initiative. The value that has brought us this plan is very high because of the level of internal knowledge we acquired. We learned a lot from our IT processes that were simple, but had more complexity than it looked at first glance.

C2. Interview 2 - GC Head of Internal Audit

Luis Mesa - Grupo Cortefiel Head of Internal Audit

The interview was conducted with Luis Mesa, Grupo Cortefiel Head of Internal Audit on Thursday April 23th, 2015 17:10– 17:40. At the request of the interviewee, the interview was not recorded neither transcribed. The author of this study use notes taken during the interview to acquire insights into the BCP implementation. The empirical findings section contain Luis Mesa remarks. Therefore, this section do not contain the transcript of the interview.

C3. Interview 3 - Deloitte BCP External Consultant

Pablo Rodriguez Cabellos – Deloitte Spain IT Enterprise Risk Services Manager

The interview was conducted with Pablo Rodríguez Cabellos, IT Enterprise Risk Service at Deloitte Spain on Friday April 10th, 2015 13:30 – 15:00. Pablo Rodríguez Cabellos serve as the team leader for the consultants working in the implementation of the BCP at Grupo Cortefiel.

Introduction

1. **Can you tell me about yourself, your role in the organization and the role you played in the implementation of the business continuity plan?**

At the time of the implementation of the BCP at Grupo Cortefiel, I was the team leader for the consultants who implemented the business continuity plan. We assisted Grupo Cortefiel to identify the critical areas by tracing the entire methodology of the project. At the present moment, I am manager in Deloitte Spain IT Risk Services. The tasks we do in my division are to provide consulting services and review clients from the more technical level without forgetting organizational issues. Our work at Grupo Cortefiel begun in October 2012 and finalized in the middle of 2013.

ERM and IS/IT Risk

2. **Which role plays your organization in the implementation the business continuity plan of Grupo Cortefiel?**

We have had much contact with the staff responsible for information security and technology. We have several projects with them and have collaborated by managing security issues and providing advice on strategy and IT projects. With Grupo Cortefiel we have had a client-customer relationship that dates from the past. The client requests proposals for solutions required to suppliers and at the end is a tender procedure. The provider that offers the best services and project wins and Deloitte Spain was awarded this project.

3. **What were the main business and technology risks identified during the implementation of the business continuity plan?**

Depending on the information obtained in interviews about what area and functions were performed by each process owner, we identify dependencies in the process. We count with a risk catalog to do so. We performed a match of the business process together with the IS/IT resources (information systems, applications, data, infrastructure) that support it. Risks associated with each dependency are linked to the active use of a technological asset within the business process. This information is obtained through the interviews.

Technological threats are linked to the dependence of the enterprise with technology functions. Conventionally, a physical risk (catastrophe, fire, flood, environmental) associated to the enterprise can trigger the activation of the BCP. The reality is that, within the map of risk and threat landscape, the most common risks are fire, flood, and environmental disasters.

However, it is more likely that we will be adding cyber risks due to the dependency that exists with IT. If technologies are damaged by any threat, the impact affects the logistics chain and

may triggers impact on other processes. Ransomware attacks are attacks via encrypted computer virus and if the virus spread throughout the network (which constitutes a security incident) derives in the impact that no one can work with the computing resources of the company. This leads to activate the BCP and the IT DRP can be used to recover from this incident.

Technology risks are analyzed, usually qualitatively. The more you try to have a mathematical formula, it becomes more complex and more time will be taken to perform the risk assessment. The method of quantitative risk is more likely to be used in a highly mature organization with a control system of quantified risks. Usually what you do is make a qualitative assessment to describe how much technological risk impacts the business process. This could be done by expressing a simple mathematical formulation on a scale of 1-5. Later this scale is used to prioritize risks. The technological risk assessment is very complex. It can have absolute values but it is difficult to give a figure valuation more than a qualitative description.

In my experience, if you reach a point where there is no information on risk at all, assessing IS/IT risk is done qualitatively. A risk analysis must need to be simplified to explain and address risk linked to business processes. So you may have identified what your business processes are critical and from there make the dependence down. If you have a good base, rich information and comparable data, it possible to perform the risk assessment in a quantitative manner.

4. **How and where were the identified risks prioritized during the implementation of the business continuity plan?**

   A risk map is performed. The firm has a fairly detailed risk map that outlined what can happen to the organization. The risk relies on:
   - Inclement physical risks: flood, fire.
   - Risk of failure of electricity, human risks as food poisoning that prevent the workforce to resume its functions.
   - Cyber risks: cyber suffer a loss of communications.
   - Labor strike: a scenario of transport in the metropolitan area that impacts employees. This is because you cannot move your workplace and if the strike lasts a long time then there is an impact on the business.

The risks in the organization are translated into what is known as a "threat scenario". It is very complex to handle 80 risks (for example) within an organization, but these risks can be reduced to simple scenarios. For instance they can be translated to the inability to access the building, electric power failure, total or partial loss of the building. Instead of posing all 80 risks, 10 risk are summarized by categorizing threat scenarios.

With the threat scenarios and the BIA, we could can start plotting recovery strategies and plans. To implement a BCP, there are a series of action plans that have to be undertaken. These action plans are developed as a result of the review made for the implementation of BCP. Action plans reduce the risk of materialization of an incident that results in the activation of the plan and, on the other hand, aid on preparing alternatives. This is done by creating an inventory of assets and resources of the organization. These action plans are organized in the short, medium and long term. Within the action plans that work to consolidate recovery strategies, which are similar to IT DRP, the aim to be to think of people and resources. These strategies can be raised from different alternatives according to the possibilities of the organ-

ization. A possibility could be work with external suppliers who can provide the necessary services if the organization cannot operate because of a disaster or incident. This is an example of a recovery strategy. In a BCP, depending on the impact or damage, incident or disaster, the impacts are measured by business impact and recovery capacity.

5. **Can you tell me about the process of mapping business processes with information systems?**

We did this during the business impact analysis together with our project sponsors and the information obtained during the interviews with each business process owner.

Governance of Enterprise IT

6. **What is the relationship between the development of the IT Disaster Recovery Plan and the Business Continuity Plan?**

The BCP is a management plan. The BCP aim is to restore critical business functions of the organization. The IT DRP seeks to recover the technological infrastructure in the event of a failure. The relationship is that within your BCP you are going to enable the IT DRP. Example: If the building is on fire *(as in the case of Deloitte Spain in 2005 after losing the Windsor Tower*), the organization loses the physical offices and data processing center (DCP). The BCP is then activated. Within the BCP, the IT DRP is activated in an alternative site. The DCP is not in the offices since one of the lessons learned in practice is that if the physical location of the offices of the organization is lost, then the DCP which is essential for enterprise operations is not lost. If the headquarters must not be occupied then the DCP is not in the office. In this case, the BCP is triggered, but the IT DRP is not since it still works.

The technology provider gives support to IT DRP in an alternative site and all technical support in technology regarding servers. The rest is not covered in IT DRP such as providing users of technological equipment (mobile phone, computer), or if you lose electricity or communications. These things are not covered by an IT DRP.

7. **Can you tell me how the business continuity plan was implemented, based on the previous existence of an IT Disaster Recovery Plan in the organization?**

The IT DRP is an element that you have but you do not need not see all from the technology side. It is part of what has already been done in the organization. In this case there was already an IT DRP in the logistics center of the organization (external site). This site already had a disaster recovery plan and BCP. You do need to put on the table all the pieces of the puzzle that you already have. The current situation of the organization in terms of trying to identify which processes are critical and non-critical processes is analyzed. The initial objective within the BCP is getting to assemble the business impact analysis (BIA). To perform this first step is to know what recovery capabilities the organization currently has: DRP, alternative sites, external sites, etc. With the organizational business process identified, you identify the critical process. This process is very important as the external consultant carry out this work of inquiry together with the top management of the organization (higher governance body). At the level of Board of Directors, these are the stakeholders that count with the ability to identify critical processes, less critical processes, the essential business functions and the ideal time when you need certain functions and processes to work.

With this input from Board of Directors already you can identify the critical processes. With the help of management then you can proceed to organize the processes based on their order of criticality. The organization of interviews is planned with all leaders and managers responsible for processes. With this information, the BIA is already been capable of being developed and you can calculate the recovery time of each function and the business tolerance to disruption. This provides an inventory of staff and minimum resources necessary to recover each of the processes. In parallel, you already know what you may materialize risk and the activation of the business continuity plan. The BCP must be activated when critical processes are impacted by an incident and the company cannot operate.

8. **How were the IS/IT risks scenarios formulated within the business process?**

Technological risks, which may be failures in technology or inability to exploit the technology. This process is relatively simple. When developing technological risk threat scenarios during the interviews one of the things that are obtained with the help of the IT department is to identify which information systems each business process used to perform its functions. Thus, already knowing the extent of a technological failure against its business processes, provides light on whether or not to activate the BCP. This is the route by which the technological side is connected with the non-technical side of the business.

9. **What is the degree dependence Grupo Cortefiel on their technology?**

It is difficult to quantitatively reach a number. I think virtually all business processes, from the critical processes to the less critical processes have a direct dependence on technology. So you always need technology for executing business activities and for daily access to information contained in the system.

10. **What is the perspective of risk obtained with the implementation of the business continuity plan for the technology area?**

Improving the support to the risk function. BCP enriches risk management based on the continuity of the risks of information security in the business. Business risk are brought to a new layer of risks, such as those of technology that affects business processes. A technological layer of risk that the organization considers as part of its business process is added and reinforced with the implementation of the BCP.

Business continuity plan

11. **Can you tell me how the initiative to implement a business continuity plan was promoted in the organization?**

It was promoted due to one of the requirements within the best practices in the industry. Internal Audit acted as one of the facilitators of the project by making recommendations in regards to the risk management. They were sponsors of the project by creating awareness regarding the need to establish a business continuity plan for Grupo Cortefiel in Madrid. This is also driven directly from the financial management of the company to address the more technical information systems part linked with the business side.

12. **Could you please tell me how the firm activated its own business continuity plan when confronted with a situation of disaster?**

Old Windsor Tower located at Nuevos Ministerios caught fire in 2005. There was a problem of power outages and that caused a large fire in the building. There was no loss of life but

the entire building was consumed by fire. Deloitte activated its own BCP and the following Monday, after the fire, the firm had its critical processes running and all resources in the company employees knew what to do. There were employees who had to stay home because they had no computers or technological equipment, but there were employees who had computers available and could work. There were delays in projects. However, gradually the capacity of all information systems recovered. The experience served to demonstrate that a well being business continuity plan gives good results.

13. How and why an organization decides to implement a business continuity plan?

In my experience, organizations often rely on external consultants. If the organization has sufficient capacity and resources within the area of security strategy or the management area related to technological risk, if there is sufficient equipment and human resources to maintain and create the plan then the plan is typically develop internally. However, those companies who are publicly traded (SEC) tend to have an expert consultant because they need professional support with business knowledge and experience from other organizations. This experience come from having done many other projects in other clients. The theory of the manual concerning the implementation of the BCP tells you how you should do the plan, but is not the same to exemplify this theory without counting with external experience. Depending on internal resources or the ability to maintain budgets many companies tend to obtain an outsourced service.

14. Who were the key actors and which role they played in the implementation of the business continuity plan?

The Head of IT Systems and Security led the BCP implementation at Grupo Cortefiel. He was the person who accompanied us throughout the process. Also the Head of Group Internal Audit acted as sponsor and collaborated with us. The manager provided us with support. We also counted with support of the financial management of Grupo Cortefiel. When you have as sponsor the Chief Financial Officer, this gives a degree of importance and awareness of the project in organizing the need for a plan of this type. This person also works partly as an operations manager.

15. What organizational elements within your department assisted in the implementation of the business continuity plan?

We were a team of external consultants that assisted the organization in implementing the BCP.

16. How was the development of the implementation of the BCP at an organizational level in regards of the methodology used?

The methodology is based on standards and best practices. The most important thing to succeed within an implementation of BCP is to know and understand the organization. The first stage consists of acquiring sponsors when the project is launched, learning about the organization, address operational issues and have support from technology. The importance of a BCP does not only rely on the technological side. The technological side is only one aspect. In case of Grupo Cortefiel, this was already covered with the IT DRP as this took in charge of recovering the computer servers. The IT DRP is a contingency plan that involves the recovery of the technological infrastructure, servers and data processing center).

The methodology is based on standard of business continuity from the Business Continuity Institute (BCI) standard BS 25999 and the ISO 22301. The old BS25999 evolves in ISO 22301. The BS25999 gives origin to the ISO 22301. The ISO gives requirements for preparing business continuity. At the end this are just guidelines or best practices on how to do the BC. We rely on our own experience and academic resources that the organization of information systems ISACA within the area of BCP in the area of good practice provides. Based on experience, the firm has a BCP system implementation: Objectives, policies aligned with the business and security, implementation phases (training testing, maintenance) and monitoring plan. The plan needs to be reviewed and audited. The end result is a phase of continuous improvement that is the plan of action that is enriched with new business processes that arise. At the end is the practical methodology that relies on PLAN-DO-CHECK-ACT.

17. Can you mention the challenges that the organization confronted when implementing the BCP?

Usually, the problem in organizations is that they have little time to meet with the consulting team. You have to acquire information in the hierarchy within the organization and acquire information regarding the process owners: what they do and later explain them the least they need to make their business process to be operable in a threat or incident. The main challenge is to ensure that in a short time the external consultant can get a photo (big picture) that depicts what the department or business unit does on a daily basis.

The second challenge is that the external consultant is able to speak in simple language (as in the field you are used to speaking in technical language), to use language that business unit can understand. From the point of view of providing consulting services in the implementation of BCP or a security strategy, where you talk to senior management or operations, you have to make everything easy for them in that you need to use their language and adequately express what is transmitted from business unit correctly.

It is essential to work with the client in implementing the BCP in conjunction with the sponsor of the project within the organization. The sponsor or project manager at the client serves as the interface with the external consultant. If the consultant does not completely knows the organization or if some data or period that can be expressed seasonality of business processes is needed, the sponsor can aid in this function.

18. How was the identification of critical process and areas performed during the implementation of the business continuity plan?

At the time of our work at Grupo Cortefiel, the identification of critical processes and areas always came from the vision of the company. There were three levels related to critical processes and processes with a lower criticality grade. The key is to not fill the draft with precise and exact mathematical methodologies but try to be as practical as possible. Within the BIA, business processes related to strategy and corporate governance, business growth and management of the company processes are described. Also risk concerning business processes related to the part of design, logistics and management of stores and franchises. Administrative support activities related to the operations of the company in general were also examined.

19. What was the perception of the implementation of the business continuity plan in the organization?

The perception is that today you if you lack the technology needed to perform operations it can cause repercussions to the organization. Companies have a high dependence on technology, whether for business necessity or not. In the case of Grupo Cortefiel, the company has a chain of large suppliers, needs to access information for the fleet management for all logistics. Therefore, technology and information systems are critical for all business areas.

In that sense the technological part was heavily covered with IT DRP so that servers are backed up and always available and can work. It is the awareness from business process owners to know that all of the business operations are based on managing information that resides on technological assets. It is in the implementation of a BCP where the minimal resources are dis-covered. As director or business manager, it is necessary to know which activities have to recover quickly. The question that arise is which resource in the form of staff can count with a place or space to work or with technological resources in the event of a disaster. This is in case employees cannot work in a normal way, such as when access to a building is prevented due to fire or disaster.

20. How was the business process peak moment (stationary time) taken into consideration during the implementation of the business continuity plan?

For this type of industry (manufacturing, retailing and distribution) seasonality is very strong in the business processes. For instance, there could be processes that work very hard for a while because they are responsible for the design of clothing and everything must be ready before launching the product campaign for months in advance. The person who knows very well this information is the sponsor and can help in contextualizing problems in regards of the seasonality of the department: workload at the time. The key to avoid unexpected risks occurring and that the project is successful is because of having to sponsor as an ally helps to validate and contextualize the work been done.

21. How were the activities with the organization managed during the documentation of the business continuity plan?

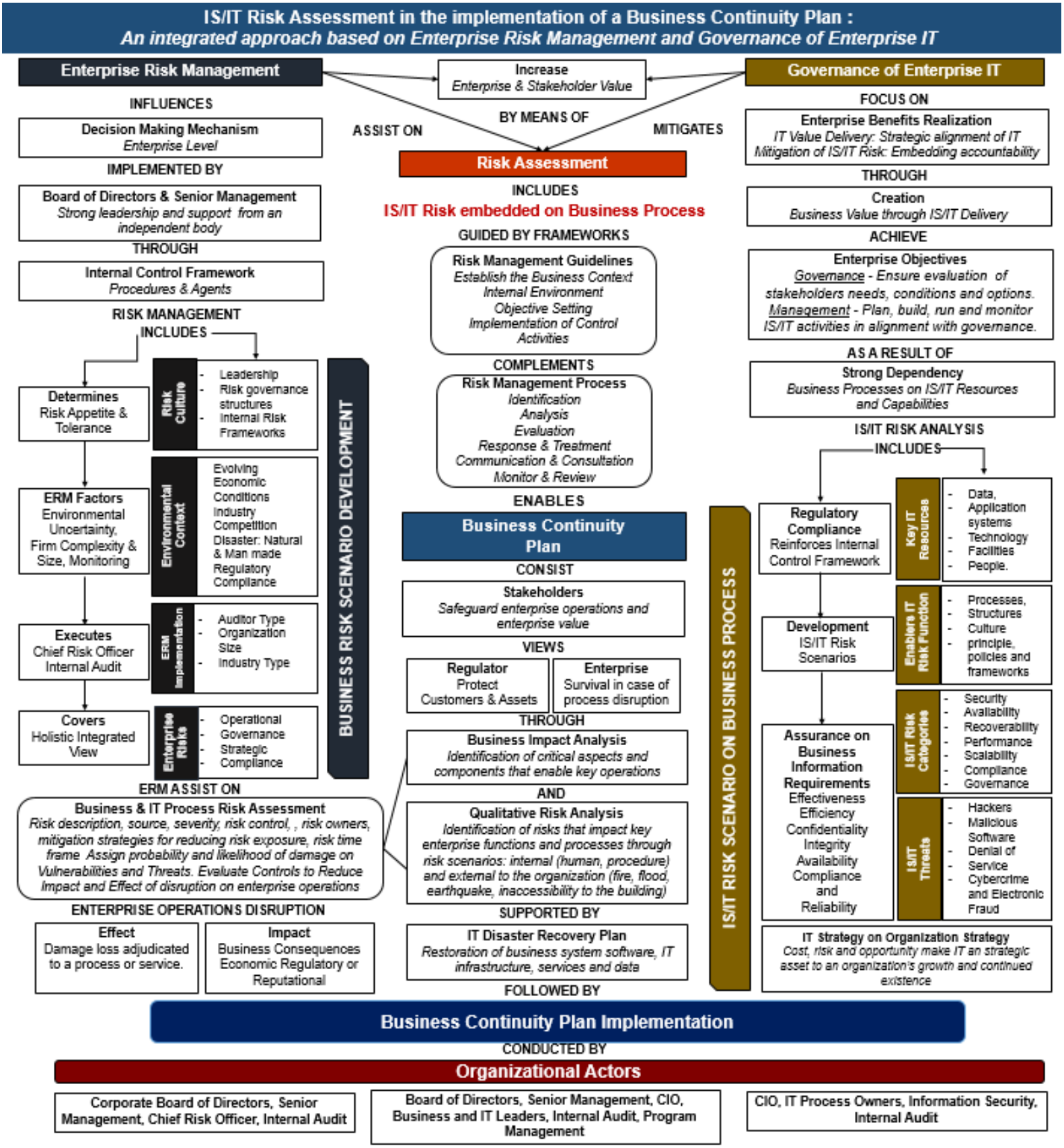
The BCP contains a collection of documentation that are supporting documents for the management of BCP. This consist in the BIA, risk maps, maps threat landscape that serves as supporting documents for the organization to assess and manage the implementation of business continuity plan. For example: test and training plan. This are elements of the management plan. Then there are the executable plans: plan of recovery in the business continuity plan that is broken down into several documents. Within the methodology there exist a tree of documents that make up a list of everything the company needs to take in consideration when conducting the business continuity plan. This are details of how a critical role or function recovers with the help of administrative support. The document is a working document in Excel format. It is an interactive document for a laptop, IPad or any technological equipment that a business manager or the person interested in access can navigate through the document. The document explains step by step everything that should be done. The document is not only for a business continuity manager, the document is for a business area. It can be used by a principal or a subordinate who has to make up a business function.

Conclusion

22. What were the benefits that the organization obtained after the implementation of the business continuity plan?

A project of this type raises an internal reflection to many areas and business issues that perhaps had not been raised before. Everyone has in mind what to do in case of a fire, but at the time of the fire what a person really do is to act, with no time to think about other things. At that moment you act. The time to plan is forgotten. The contribution of BCP is seen on each business area: a list, simple steps and guidelines of how to act in case of a crisis. It is a benefit that provides peace of mind to the business. The lifting of such information and formal documentation makes an internal reflection within the organization in a form of an internal continuous improvement in business processes. A more mature is an organization, then the organization is going to have a procedure that can be measured or improved. In the future I believe that this function will arise. From my personal point of view, what has to happen is that business continuity function must integrate well with crisis management function. In organizations crisis are going to happen and we must learn how to manage them. This is not only internally. It is also externally. Learn to interact with your suppliers, customers, government authorities when a crisis happens, especially in large companies that have a social responsibility or are systemic companies. On the other hand, I think it will happen as part of a very strategic vision within the continuity of business operations. A much more dynamic vision is provided by the technological risk. The collaboration, alignment of the BCP, IT DRP, organizational capabilities and resilience against any threat, particularly in the technology have to work together hand by hand. Separately these functions will not work.

D. Extended Framework: Integrated View of IS/IT Risk assessment in the implementation of a BCP



E. Extended Framework: Enhanced View of IS/IT Risk assessment in the implementation of a BCP