A Work Project, presented as part of the requirements for the Award of a Masters Degree in Management from the NOVA – School of Business and Economics.

BUSINESS CONTINUITY MANAGEMENT AT BANIF: DEFINING AND SELECTING RECOVERY STRATEGIES

FRANCISCO TOMÁS VAZ LANCEIRO ABIUL MENANO #1417

A project carried out under the supervision of:

Professor Filipe Castro Soeiro

30th of May 2014

Abstract

This project aims to delineate recovery strategies for a Portuguese Bank, as a way to increase its preparedness towards unexpected disruptive events, thus avoiding an operational crisis escalation. For this purpose, Business Continuity material was studied, a risk assessment performed, a business impact analysis executed and new strategic framework for selecting strategies adopted. In the end, a set of recovery strategies were chosen that better represented the Bank's appetite for risk, and recommendations given for future improvements.

Keywords: Business Continuity; Recovery Strategies; Business Impact Analysis; Risk Assessment; Component Business Model

Table of Contents

I. Introduction

Banif[1] is a Portuguese bank that started its operations in 1988, after acquiring Caixa Económica do Funchal that accounted for over ten millions in losses. It first focused its activity within the Portuguese autonomous region of Madeira, but rapidly expanded its operations to the Continent and overseas.[2] In the beginning of 2008, Banif's dynamism was shown through its consolidation strategy followed by a major rebranding. However, the subprime crisis stopped its ambitions from developing, since it highly affected the bank's stability, resulting in: a Government's intervention, an injection of capital[3] of approximately one thousand million euros and, more importantly, an internal restructuring.[4] This lead to the creation and extinction of some departments and alteration of certain employees' roles; the new reformulation created the perfect environment to start implementing a Business Continuity Management Program, already required by the financial authority.

However, it was in 2013 that Banif decided to implement a complete Business Continuity Management Program, not only to comply with the financial authority[5] but also to increase its organizational resilience and build more confidence towards its shareholders. With that mindset, a team was created, within a brand new department – Direcção de Transformação e Performance (DTP).[6]

II. Purpose and Scope

The ultimate goal of this project is to design and implement a Business Continuity Management Program that will increase Banif's response preparedness

[1] Banif is also known as Banco Internacional do Funchal.
[2] In 1993, Banif started its internationalization through the Cayman Islands and an office in Venezuela.
[3] The State capital injection happen in December of 2012.
[4] The restructuring consisted in a major lay-off plan and in an internal department reorganization.
[5] According to the CNFS 2010 recommendations.
[6] The department creation was a result of the Bank's restructuring plan.

towards disruptive events, which will translate in an increase of its level of resilience, thus protecting shareholders' value. This work project will cover the definition and selection of recovery strategies within a BCM program for three of Banif's entities, overall represent its retail and investment banking activities: *Banif S.A.*,[7] *Banif Banco de Investimento* (BBI) and *Banif Gestão de Activos* (BGA).[8]

Also, and due to the time constrains, the researcher decided not to focus on the "Implementation, Validation and Review" part of a Business Continuity program, even though these are considered of great importance.[9] Therefore, the intended study will focus on a more strategic approach regarding Business Continuity, which corresponds to the mandatory recommendations, numbers five to seven from the *Conselho Nacional de Supervisão* (hereafter CNSF).[10]

In the end, a conclusion will be made on Banif's current resilience capacity and recommendations given for future improvements. Additionally, this work could later on be used as a benchmark tool for either future BCM implementations, improvements or reviews, thus hoping to contribute for a subject that is academically underexplored.

III. Literature Review

3.1) Business Continuity Management

It is universally accepted that unexpected events,[11] regardless of their origin or cause, can lead to an operational disruption, disseminating negative impacts to

[7] Banif SA is a retail bank, which includes activities such as: credit concession to enterprises and individuals, deposits, investment products, and factoring.
[8] BBI represents investment management, capital markets and banking advisory services; where BGA is specialized in asset management activities.
[9] More detailed information about the elements of a BCM program can be found on the literature review chapter under "Core Concepts"
[10] Banco de Portugal (BdP) circular letter 75/2010/DSB.
[11] "[...] ranging from physical crises such as accidents, product failures or loss of utilities (gas, power supply, water, telecommunications), personnel crises such as large scale staff illness or death, industrial action or staff criminality, external criminal crises such as terrorism and product tampering, information crises such as cybercrime or information theft, natural disasters such as flood and storms, economic crises such as economic recession, and reputational crises such as internet defacement or malicious rumours" (Mitroff & Alpaslan, 2003).

organizations, thus affecting its shareholders and stakeholders (Randeree, Mahal, & Narwani, 2012). These incidents can be seen as an inevitable risk that must be taken into consideration by managers, even if the probability of them arising is perceived as being reduced.

With that in mind, a set of procedures exists to help organizations in preparing for these disruptive events in order to reduce their impact and guarantee operational continuity, thus avoiding any escalations to more serious crises. Hence, Business Continuity Management (henceforth BCM) appears as a "*holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*" (ISO 22301, 2012).

In order to better understand the recent strategic role of Business Continuity within organizations, which is the central focus of this project, it is important to revise its origins. For this purpose the researcher has made a historical study on the subject. Business Continuity's early appearance takes place before the 70's, a non-regulated period for this matter, as Crisis Management (Gallagher, 2003). At the time, organizations decided how to implement Crisis Management, characterizing the operations as *ad hoc* reactions instead of predetermined management processes. Thus, still lacking a wide and more strategic organizational approach (Herbane, 2010).[12]

The technological revolution, arising from the early 70's, had one of the greatest influences towards the evolution and development of BCM. In this period, the personal computer appeared, but more important was the increased computer

[12] Nowadays Crisis Management is still used in organizations, but as an element of the whole Business Continuity Management System.

technology adoption by enterprises (Broadbent, 1979). On this field, IBM pioneered with the successful introduction of the mainframe computer systems models,[13] which consisted in and provided organizations with a single management information system (Gum, 1983). By adopting these systems, organizations started to focus on the vulnerability of their data process activities, is that to say, on the hardware failure causes and respective reaction procedures (American Bankers Association, 2005) – data backups represented the central emphasis of the recovery plans, also known as Disaster Recovery (hereafter DR). Due to the great amount of sensitive/confidential data managed, the United States' financial services sector led the adoption of the DR plans, which mainly concerned information technologies' (IT) recovery.

In the mid 80's, however, and despite its success, DR started to be questioned because of its limitations, essentially due to its central focus within IT issues. At the time, disaster recovery teams were placed within IT departments (Dugan, 1986). This approach was not fully improving organizations' capabilities in pursuing a higher resilience level, but was constraining planning and testing participation of other areas of great importance such as human resources and management from other business units (Herbane, Elliott, & Swartz, 2004).[14]

Therefore an evolution of DR approach was required, which would incorporate a more strategic vision, beyond IT issues, and included a wider organizational involvement (Herbane et al., 2004). In the 90's, this mentality stemmed the creation and implementation of the early Business Continuity Management plans (Herbane, 2010). This idea was reinforced, and somehow defended, by disruption events that reminded organizations of the necessity of a broader approach,[15] with a value-chain

[13] The IBM mainframe computer system models System/360 and 370 were released in 1965 and 1970 respectively.
[14] Banks, the early adopters of DR, were also stressing the importance of a higher involvement of the information systems' end-user in the process of prioritizing and allocating recovery resources (Burger, 1988).
[15] Examples of these events are the London Stock Exchange in 1990 and World Trade Center in 1993 bombing attacks and the Manhattan power failure in 1990.

view of the organization's critical activities (Vogler & Perkins, 1991). Similarly the criticality of working with outside entities, for example utility providers and insurance companies, in the process of defining recovery strategies and designing communications plans also revealed to sustain the need of Business Continuity as a response to safeguard the continuity and recovery of value-generating activities (Bradford, 1992). The early 90's up to 2001 were characterized by the emergence of independent organizations, such as the Business Continuity Institute (hereafter BCI) in 1994, and the creation of standards regarding BCM (Herbane, 2010).

Subsequently, the 9-11 terrorist attacks were considered to be a milestone for BCM and its development. Such unexpected and mass-destructive events enhanced the criticality of BCM programs among organizations, and spotted some of its most fragile implementations, especially regarding the preparation for a large-scale disaster (Serino & Williams, 2009). Thus resulting in an increase of the number of guidelines and best practices together with the intensification of legislation – the financial service sector was the front-runner in developing BCM in the United States[16] but also overseas[17] (Herbane, 2010).

With an increased number of national standards flourishing from all around the world, which would aim to obtain international recognition and adoption, a new phase was crafted characterized by a competition among BCM standards. In 2006, the British Standard Institution (hereafter BSI) lead this period with the introduction of BS25999 standard, which innate from the UK's Business Continuity Institute (BCI) Good Practice Guideline PAS56. The collaboration between BSI and BCI continued, also influenced by other frameworks around the word, resulting in the creation of the most recent BCM standard to date – ISO22301: 2012 – and an applicable guidance

[16] The Council Business continuity planning booklet, by the Federal Financial Institutions Examination Council in 2003, are an example of the United States BCM developing.
[17] Oversees, BCM guidelines by the Monetary Authority of Singapore in 2003, are just a single example.

issued by BCI – Good Practice Guideline 2013 – which redefines professional practices even further.

3.2) Core Concepts

Prior to defining a working methodology, it was essential to gain a full comprehensive view regarding BCM's core concepts and its fundamental role within the financial service sector. Based on the more recent work on this field,[18] but not exclusively, the researcher dedicated this section to present the different concepts and tools that are part of the complete BCM system implementation, which consists in employing several tools and procedures to increase a company's level of resilience

A BCM system can be divided into a management practice, with the purpose of making sure that the organizations and employees are working towards increasing the organizational resilience level while understanding its critically and importance (Järveläinen, 2013), and a more executional and technical part. The latter, can be further broken down into four practices, 1) Analysis, 2) Design, 3) Implementation and 4) Validation and Review, that together complete a cycle of processes to guarantee a continuous BCM renovation, according to BCI (2013). Although the researcher studied all the components, and acknowledges their criticality to create and adopt a successful BCM system, only the Analysis and Design section will be studied in more depth.[19]

The starting point is done through outlining a formal policy that defines the purpose, the scope and the governance of the Business Continuity Management program within the organization. This will greatly reflect the organization's top managers' willingness towards this subject and the resources allocated to it, thus affecting the changes of a successful implementation. Therefore, international

[18] The most recent BC work is the ISO22301:2012 and the 2013 Good Practice Guideline from Business Continuity Institute.
[19] This is justified by the scope and purpose of this thesis.

practices highly recommend that the program should be directly under the responsibility and overseen by a member of the top managers' team (Labaka, 2013).

3.2.1) Analysis

There are two distinct types of analyses that must be performed. A Risk Assessment analysis, that aims to identify the operational threats that the organization is vulnerable to, and a Business Impact Analysis (henceforth BIA), which underline the effects of an activity interruption.

In order to perform a risk assessment it is necessary to proceed with three steps, a) identification of threats, b) estimation of the risk's probability and c) evaluation the potential impacts through a scoring system (Ferrier & Haque, 2003). Although it is impossible to identify all the threats to which an organization and its operations are subject to, an exercise must be performed in order to identify as many as possible so as to produce a realistic list of possible different scenarios. Moreover, on estimating the probabilities of each event, and in order to overcome what Robert Kates called in 1971 the "Prison of Experience",[20] different sources,[21] based on historical data, must be applied to extrapolate probabilities of such happening. Last but not least important, a scoring system is used to evaluate impacts.[22]

On the other hand, the BIA is a more complex and time-consuming activity that aims to analyze the business' critical activities and identify the resources required to recover from an operational disruption within a desired timescale,[23] thus protecting from a more serious crisis escalation.

There are three different BIA levels that should be performed by organizations: the strategic, tactical, and operational (BCI, 2013). Depending on the characteristics

[20] Robert Kates states that an individual's past experience can influence the estimation to an extent that may distort the reality
[21] Examples are insurance statistics published and disaster frequency statistics.
[22] Important to note that it is highly recommended by the Business Continuity Institute to use or adapt risk assessments already performed by organizations. (Good Practice Guideline, BCI, 2013)
[23] There is always a tradeoff between recovery speed and cost with recovery resources. This should be balanced according to the organization resources availability and its willingness to take risk.

of the organization it is possible to combine them.[24] All BIA levels assess impacts of an operational outage, identify internal and external organizational interdependencies, estimate the maximum tolerable time of disruption (also known as MTDP) and recognize the recovery resources needed. With the help of this information, the organization outlines its recovery priorities.[25]

3.2.2) Design

The purpose of the design stage is to implement mitigation measures, deploy an effective incident response structure and select recovery strategies that would be aligned with the recovery priorities previously defined, intending to increase the organizational resilience.

Mitigation measures are used for two reasons, decrease a disaster's likelihood and/or to reduce its impact towards the organization. There are a great number of mitigation measures that are already implemented within organizations due to the by-law requirements, such as fire detectors and security procedures. However, a further analysis should not be disregarded.[26]

The incident response structure is a documented set of procedures that should be performed upon a disruptive event. This document should include well-defined recovery teams, their responsibilities and the interaction that must exist between them. It is responsible for, but not limited to: activating recovery plans, invoking resources and coordinating communication. One of the critical successful factors is the two-way communication needed so that decisions and feedback are flawlessly diffused. Important to note that, depending on the organization's needs, the incident's response structure may include external recovery teams, such as the IT recovery provider.

[24] For example, for small size or even less complex organizations it is possible to conglomerate, into a single BIA, the tactical and operational level.
[25] BIA should include but not be limited to the information mentioned.
[26] After performing the already mentioned risk assessment and acknowledging the need to reduce threats, especially if they jeopardize the continuity of critical activities, more mitigation measures should be created and implemented.

Additionally, recovery strategies are a reaction solution to the threats identified;[27] they must be analyzed and selected in order to meet the desired critical activities' recovery timescale whilst simultaneously not exceeding the dedicated budget.

With that in mind, there are a variety of strategies that organizations could select for each loss assumed. Some examples are: replication, post-incident acquisition, subcontracting, displacement and remote workplace. When selecting strategies, it is essential that organizations keep in mind their own structure's characteristics, their recovery prioritization as well the internal resources available.

3.2.3) Implementation

After selecting the recovery strategies, organizations should outline detailed action plans that would be used to respond to a disruptive event. These plans are known as Business Continuity Plans[28] (BCP) and include procedures, in a more operational level, that must be aligned with the recovery prioritization and with the selected strategies. Besides BCP, the implementation phase should also contemplate the creation of a comprehensive internal and external communication plan. In order to guarantee its success, the plans must be produced with the active participation of all its members, including external entities such as critical suppliers, emergency entities and third party IT providers.

3.2.4) Validation and Review

Business Continuity Management must not be seen or treated as a one-time project implementation but as a continuous management system. More than ever, business environments are extremely dynamic and, if organizations are to continue competing, they need to quickly adapt and transform their *modus operandi*. As a

[27] It is important to note that recovery strategies can be treated individually, but should also be considered in multiple-loss-scenarios where, for example, a building damage will result in the loss of people and physical workplace.
[28] Specialized forms of Business Continuity Plans are also known as: Contingency Plan; Pandemic Plan; Disaster Recovery for IT; Media Response Plan. (BCI, 2013)

result, it seems natural that Business Continuity practices should also reflect this and, therefore, require continuous practice and revision.

For this purpose, test and reviews must be performed within organizations at least once a year or upon any major internal or external change (ISO22301: 2012). Tests are part of an overall review that must be practiced regularly and not exclusively on BCP, but to every element within the BCM system. Therefore, BCM systems must be perceived as a continuous effort that organizations must perform to guarantee and increase their level of resilience.

3.3) Business Continuity and the Financial Services

Even though many industries make no effort to implement a BCM program, BC could and should be implemented to all types of organizations and industries. Despite the increase in adoption of such management activity, there is still some hesitance regarding it due to its perceived added value (Continuity Insights & KPGM, 2012).

Financial Service organizations are considered to be one of the utmost important within societies. Their roles are central in facilitating and promoting economic progress towards individuals and organizations, through services such as borrowing and lending, raising capital, promoting investment and insuring risk. These particular characteristics and the enormous societies' dependency, strengthens the need of this sector to be protected and prepared for any disruptive event as a way to avoid an undesired proliferation effect that could be catastrophic.

Terrorism attacks, health epidemics, natural disasters, and computer malware are just some recent examples that have demonstrated that this sector is also vulnerable to an operational disruption risk.[29] This becomes even more severe if it endures overtime, which can lead, for instance, to a lack of confidence, thus resulting in a

[29] Examples of operational disruptive events: Royal Bank of Canada firebombing (2010); Avian Flu (also known as H5N1); Hurricane Sandy (2012); Heartbleed security bug (2014)

frenetic withdrawal of capital from the financial system. Without further explanation, it seems natural that an operational disruption could become a more serious financial crisis. Besides, the complex interdependency between financial institutions indicates that an operational crisis from one could potentially affect others.

This explains the BCM work that has been developed within the financial sector, which goes from private initiatives to financial authorities' work to pressure participants to implement a BCM program, collaborate with its peers and apply a continuous attitude towards improvement to ensure a more resilient financial sector.[30] Therefore, and with the goal of increasing the said resilience level through a more regulated financial sector, The Joint Forum[31] issued the *High Level Principles for Business Continuity* in August 2006: "*Financial authorities should incorporate business continuity management reviews into their frameworks for the ongoing assessment of the financial industry participants for which they are responsible*".

Portugal's most recent BCM regulation, concerning the financial service sector, was released in 2010 by Concelho Nacional de Supervisão (CNSF), and gathered eleven recommendations on the implementation and maintenance of a BCM program,[32] which reflects the *High Level Principles*. This occurred under the *Better Regulation* initiative that unifies and stimulates the collaboration of different financial authorities.[33]

IV. Methodology

Having acknowledged the BCM core concepts and its criticality within the financial sector – including the Portuguese legislation towards it – the researcher was

[30] Securities Industry Business Continuity Management Group (www.sia.com); ChicagoFIRST (www.chicagofirst.com).
[31] The Joint Forum is an international group of financial regulatory representatives that was established in 1996. It is composed by Basel Committee on Banking Supervision (BCBS), International organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS).
[32] Banco de Portugal, Carta-Circular nº 75/2010/DSB, 2010
[33] Portuguese financial authorities are composed by Banco de Portugal (BdP), Instituto de Seguros de Portugal (ISP) and Comissão do Mercado de Valores Mobiliários (CMVM).

then able to define a clear methodology to help in answering the project's main research question: **How to define and select recovery strategies for Banif?**

With that goal in mind, a framework was developed consisting in sub-research questions, methodology used and the corresponding expected outcomes.

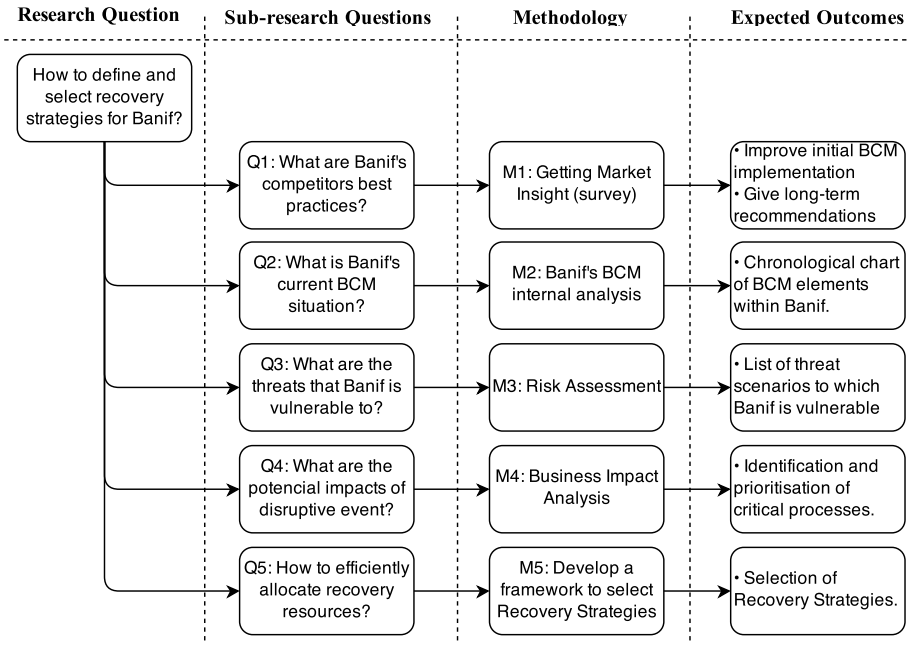

Figure I - Schematic illustration of the methodology used by the researcher, 2014

The market survey will give the researcher useful information to improve Banif's implementation, while the internal analysis will give a holistic view of what was still missing to establish a BCM. Furthermore, the risk assessment and the BIA were essential in identifying threats and critical processes within Banif, and in defining a recovery prioritization. Finally, a framework was developed to manage complexity and support the selection of recovery strategies.

4.1) Market insight

Gathering market insight information was important for Banif to understand some of the practices that its competitors were developing, giving it a trustworthy benchmark that would be helpful in making the BCM decision. The market

information was obtained via a survey and informal conversations about difficulties experienced, shared by each bank's BCM responsible.

Despite the lack of cooperation between banks to share information regarding their BCM,[34] three of the eight biggest banks operating in Portugal,[35] already experienced with BCM, were able to share some of their knowledge. The survey was completed within the presence of the researcher, so as to avoid any misunderstandings. In the end, the expected result was a set of more mature practices that will be used to improve Banif´s initial implementation and provide long-term recommendations (Appendix II).

4.2) Banif's BCM Internal Analysis

In order to understand the work already developed by Banif, the researcher analyzed a set of documents, provided by the bank, from different departments. With this analysis, the researcher came to the conclusion that since its early days Banif has been implementing different elements, much in line with the evolution of BCM before discussed. These implementations can, in part, be explained by the thoroughly regulated sector where Banif operates.[36]

All the plans already applied and related to BCM can be considered part of the "Implementation" phase, so these plans will be treated as specific BCP. Therefore, there exists no need to replicate them but simply to guarantee that they flawlessly fit within the overall BCM umbrella and are aligned with the goal of protecting and recovering Banif's critical activities. Additionally, at the end of 2013, starting elements of the desired BCM Program were defined by DTP: BCM policy and governance, both being part of the required management practice. This internal

[34] Even though it is suggested that an active participation between financial institutions, regarding BCM, should exist, in Portugal there is still some unwillingness in sharing information on these matters. This explains the low participation ratio that was verified upon the researcher's survey request.
[35] For disclosed reasons, the name of the banks will not be reviled.
[36] Financial Service Sector, Banking, which is regulated by Banco de Portugal.

analysis has given the researcher an understanding of what was missing and needed to be implemented. The complete timeline can be found in Appendix III.

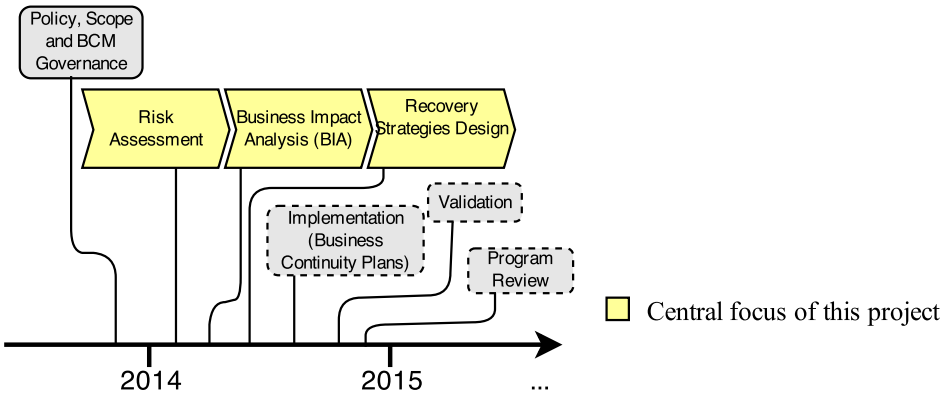

Figure II - Timeline of Banif's BCM Program Implementation, 2014

4.3) Risk Assessment

This assessment was fundamental to filter and prioritize the recovery strategies that the Bank would have to prepare – higher probabilities combined with higher impacts would require a more prompt action than those with lower probability and lower impacts. This becomes even more important, since it was Banif's first time implementing a full BCM program, thus needing to prioritize its response actions in order to allocate the scarce resources as efficiently as possible.[37]

Even though for Business Continuity purposes it is not relevant to analyze where the threats are coming from, it is important to have a perception of their potential lengths and impacts. Thus, from the threats already identified by Banif,[38] a list of eight different disaster scenarios was deduced, considered and included in Banif's risk assessment. Based on a grading system used, there were four levels of impact: being 1 the grade with the least impact and 4 the one with the greatest impact.

[37] According to BCI (2013), no great analytical or precise probability value is needed to measure risk occurrence in BCM program. Since the level of detail require is lower and a more qualitative analysis preferable. This idea is also supported by CNSF (2010).
[38] Banif's Security Office had already developed a document that assessed the risks for each central building: The Security Plan for Central Buildings.

The same scale was also applied in representing the probability of occurrence for each scenario (Appendix IV).

Finally a risk scoring was computed: for each central building the eight different scenarios were considered, and attributed with the respective probability and impact.[39] As a result, the scoring was obtained by simply multiplying the impact's grade with the probability of occurrence (Ferrier & Haque, 2003). This assessment has pointed out the disaster scenarios with higher risk to Banif, thus providing a prioritization of the recovery strategies that needed to be implemented.

4.4) Business Impact Analysis (BIA)

The goal of performing a BIA is to identify the critical activities within the organization – through their impacts to the Bank in case of an event that might lead to an operational disruption –, their support infrastructure, both technological and non-technological, and to detect the internal and external dependencies. In the end, this will result in a prioritization of the critical activities and the minimal resources that must be in placed in order to guarantee a more efficient recovery, thus increasing the organization's overall level of resilience.

At Banif the analysis was conducted through its organizational internal structure, which was then subdivided by the list of the Bank's processes, which is in line with its competitors practices (Appendix II). Also, this choice was made to fit the top management's request and helped with the gathering of information. The analysis involved three different entities (Banif SA, BGA, and BII), thirty-two business units and more than three hundred processes.

Even though the author acknowledges that international best practices consider different levels of BIA – strategic, tactical and operational –, in Banif's case the

[39] In order to avoid impact misrepresentations, an estimated time was considered for every scenario.

decision was to combine them into one due to the organization's urgency in performing the BIA and its relative medium size that permitted this fast implementation. This technique is not totally uncommon and has the BCI's support.

The analysis was divided into three main blocks: normal operations, business impacts and recovery resources. First, all information was gathered by business processes within each business unit, and included: general information about business unit and processes' brief description, so everyone could understand easily even if not directly engaged with that part of the organization function; the physical infrastructures they relied upon (central building); number of employees; technological and non-technological resources; and internal and external dependencies.

Assuming a total activity interruption, the second bulk of information concerned four types of impacts to Banif's business: Financial, Legal, Reputational and Customer Service impacts. While the last one is not mandatory according to CNSF recommendations, it is highly advocated as seen in the survey responses (Appendix II). Similar to the risk assessment, the goal was not to have a precise and analytical BIA, but a reasonable and more qualitative evaluation, thus a high-medium-low impact scale was used.

Additionally, distinctive interruption durations were considered: 4 hours, 1 day, 3 days, 5 days, 10 days, 20 days and 30 days.[40] This information will give an insight on the maximum tolerable period of disruption (henceforth MTDP), also included in the BIA, which will later serve as a criterion to identify Banif's critical processes.

Finally information about recovery resources was considered, such as: alternative sites; resources (e.g. computers and printers); IT application and respective

[40] These times are much in line with the disaster recovery practice solution designed by IBM (Warrick & Sing, 2004)

Recovery Time Objective (RTO) and Recovery Point Objective (RPO); and work-from-home possibility.

After deciding upon the information required to perform the BIA, an excel template file was created. However, before the rollout to each business unit, the variables required testing. Thus, DTP[41] served as an experiment, since the team would be able to quickly tackle any issue that might have appeared. With a successful trial, the template was deployed to every business unit director, is that to say to every BC owner. Additionally, individual meetings were scheduled with the BC owners to help in any details related with the information being requested.

After all the information was gathered and approved, a consolidation to a single excel file was executed to facilitate any analysis that needed to be performed. Moreover, the criteria to define the critical activities was then selected. By definition, critical activities are the ones more susceptible to jeopardize BC and to create an unwanted impact to the organization in case of their interruption (Horváth, 2013). Thus, it seems logical to measure this criticality through the different impacts that each process has to Banif, and for this purpose, as stated above, the MTDP was used.

Even though international practices suggests that critical activities should be all which have an equal or lower to six days MTDP, in Banif's particular case, it was decided that the model would only consider the ones up to three days of MTDP.[42] The reason behind this choice was simply to decrease complexity and avoid an overinvestment in what was Banif's first year of implementation. However, the researcher has strongly suggested that for the following years this parameter be properly reviewed and justified to improve the overall resilience capacity.[43]

[41] DTP is the department responsible for Business Continuity.
[42] This was decided and included in Banif internal document regarding the scope of its BCM program.
[43] Internal dependencies, only first tier relations, were taken in consideration while assessing the MTDP to each process.

4.5) Framework to Select Recovery Strategies

A challenge ahead is to compile the amount of complex information to be presented to the Board of Directors. For someone not fully involved with the project, it was difficult to understand and strategically discuss all the recovery options within BC Project.

To this end, the researcher decided to use and adapt a Component Business Model (henceforth CBM).[44] This framework, besides having some shared notion with Michael Porter's value-chain approach, offered the desired implementation flexibility without jeopardizing the strategic vision through individual business components (Business Process Trends, 2007).[45] For this purpose, and based on a variety of sources,[46] a more intuitive and easy to read CBM was created (Latimore & Robinson, 2004). The result was a framework with six clusters organized by their value chain contribution to the organization, and a breakdown of individual business components that altogether represent all of the bank's activities/processes.

With a CBM tailored to BC (Appendix V), and after matching the critical processes to components, it was possible to analyze, compare and efficiently select the different recovery strategies options.[47] This holistic approach not only gave an overall recovery panorama but also provided specific component recovery times. Besides, and in order to help the researcher in this process of properly selecting the different strategies for each component, two recovery strategy positioning maps were created: one recovery strategy for facilities and the other for people, both taken in consideration the associated cost, speed of implementation and their reliability (for

[44] The CBM is a strategic framework developed by IBM. It was primarily conceived to define IT strategy solutions. However, due to its flexibility it rapidly expanded to other business areas (Cherbakov et al, 2005).
[45] "Business components are the modular building blocks that make up the specialized enterprise" (IBM, 2005).
[46] The sources are: a CBM example (Pohle, 2006), a Banking Classification Framework (IPQC, 2013), and an BIA from Banif.
[47] Additionally, and similar to a value chain analysis, the organization's costs were distributed by component giving an idea of the opportunity cost of the components in case of a operational interruption.

facilities) and the reorganization adjustment needed (for people).[48] More detailed information on Appendix VI. Last but not least important, and in order to guarantee that all sources of competitive advantage were to be contemplated within recovery strategies, thus reinforcing Banif's continuity resilience, a Barney's VRIO analysis was performed to every non-critical CBM component (Appendix VII).[49]

V. Results and Discussion

5.1) Threat Scenarios

The risk assessment performed has identified eight threat scenarios and the correspondent risk to which Banif was vulnerable. After compiling all the risk scorings, which were organized by central building, the researcher came to the conclusion that Banif should be focusing on developing recovery strategies in order to increase its level of resilience towards the most threatening scenarios: Loss of accessibility to the office, decrease of available human resources and the unavailability of the technological platform.

Threat Scenarios	Central Buildings' avarege risk*
C1 - Loss of accessibility to the office	11,6
C7 - Decrease of available human resources	9,4
C2 - Unavailability of the technological platforms	8,6
C6 - Critical supplier service interruption	6,8
C3 - Lost of communication systems	6,6
C8 - Physical archive damage	6,4
C4 - Electricity outage	6,0
C5 - Interruption of water and basic sanitation supplied	2,0

* the risk scoring goes from low to high risk level (1-16)

Table I - Summary of Banif's Risk Assessment, 2014.[50]

5.2) Critical Activities

Furthermore, a fundamental result from this BCM program project was the identification of Banif's critical processes. Therefore, and according to the

[48] The recovery strategies taken into consideration were the ones tailored to be used as a response to the risk scenarios identified and to which Banif was more vulnerable.
[49] Interesting to note is the proven relationship between level of resilience and the organizational capacity in attaining competitive advantage (Parsons, 2010).
[50] The more complete risk assessment, which was performed by building, can be found in Appendix VIII.

methodology used by the researcher, Banif has identified one hundred and thirty four critical processes, which represents around thirty four percent of the total (Appendix IX).[51] However, in order to analyze and discuss these results, the strategic framework CBM was used to help in managing complexity – instead of dealing with more than one hundred processes, only a few components were examined.[52]

Based on the processes' MTDP, the business components were divided into three levels of criticality (Appendix X). Within the first group, are the components that must recover before a four-hour period of disruption and were related with customer service, legal, external reporting,[53] some support activities, but especially concerning components within the "Processing" CBM cluster. This is easily understandable and explained by the four impacts analyses considered in the BIA: Customer Service, Reputational, Legal and Financial impact.[54]

The second critical group is composed by fifteen components that are now expanded to one more cluster, the "Business Development", but not limited to it. Within this group are the components that must recover in less than a day. Last but not least, the third group, with only eight components, represents the rest of the critical processes. However their recovery requirements are less demanding, with only until three days of outage permitted.

After performing the VRIO analysis to each non-critical component identified in the BIA, the researcher has concluded that none of them are a source of competitive advantage to Banif, therefore, it doesn't seem relevant to include any additional business component within the recovery strategies (Appendix VII).

[51] It is important to note that Banif's branches are not within the scope of this project, but only the central buildings and the organizations: Banif SA, BBI and BGA.
[52] Each process was allocated to a specific component and internally validated by Banif operational risk manager.
[53] This means reporting to external entities such as the regulator, BdP.
[54] Financial impact can be a possible consequence of an interruption of any of the previous impacts.

5.3) Define Recovery Strategies

With the critical components already defined, it was necessary to select recovery strategies that would guarantee their continuity in case of a disruptive event, thus avoiding major negative impacts to Banif. The recovery strategies aimed to work towards a solution for the highest threats previously identified, thus divided into three categories: Facilities, People and IT.[55]

5.3.1) Facilities and People

This exercise required the certification that the components would recover within the MTDP that was defined and an efficient resources allocation. To that end, the created recovery strategies positioning maps was consulted (Appendix VI). In order to help the researcher, the critical components were organized by central building and their level of criticality, allowing for a further understanding of the possible strategy that could be applied. The facility strategy was chosen first, and only then was a people's recovery strategy selected. The reason behind this is the strong relationship between them, which must be faultlessly coordinated.

Since the alternative central building strategy seemed to be the most inexpensive and still delivered a reasonable level of reliability and a short implementation time, it was firstly considered to all components. However, in order to be selected, two conditions needed to be verified: 1) the presence of a central building within the same city and 2) the existence of that component within that building with no fewer number of components associated.[56] If the previous did not meet the minimum conditions, the second cheapest strategy was to be validated – Remote

[55] Facilities and People strategies were treated together due to their close relationship and dependency. Although very important part of the recovery strategies, the researcher decided not to focus on the technical issues of the IT recovery.
[56] The second criteria insure that the alternative central building have the capacity to received the reallocated critical component and have the necessary resources to perform it.

Workplace.[57] Since this information was included in the BIA, it was easy for the researcher to verify its applicability to each component.

The remaining facility strategies would only be applied in case of none of the above resulting in a valid solution. However, the criteria for selecting among them was based on the components' demanded recovery time, which was represented by their level of criticality. Therefore, for the high critical components a hot-site strategy was selected due to its reliability and fast implementation. On the other hand, for the medium critical components the cold-site seemed to be the reasonable option, since it is still reliable and its implementation speed is aligned with the demanding recovery times within that group. Finally, the post-incident acquisition was chosen for all the other low critical components; although the less reliable among all, it is the most cost-efficient for these particular set of components that have more time to recover.

The design strategies for people recovery were then selected. Logically, for every component adopting an alternative central building, the displacement strategy must have been verified due to workplace constraints. On the other hand, the rest of the components will adopt a "no-changes-required" strategy for its employees, since they would not require anyone else to perform their tasks for them. However, it was necessary to bear in mind the possibility of having people unavailable within a disruptive disaster. For this purpose a second strategy shall be used, in any case, which consists in a replacing strategy that is already defined within an internal and confidential Banif document. This information can be found in appendix XI.[58]

[57] It is important to mention that the remote workplace allows a very fast implementation, which is makes it compatible with demanding recovery times.
[58] The subcontracting strategy was taken into consideration, however will not be applied within Banif's since it is the most expensive and would require a great effort of adjustment, which is not recommended to a critical activity.

5.3.2) Information Technologies

The IT recovery strategy does not aim to delve into technical details because that is not the scope of this project. However the researcher acknowledges the ultimate importance of IT as a fundamental tool to almost every process within the bank. Therefore, through the information that was gathered while performing the BIA, a matrix was created with all applications and their requirements for every department within Banif SA, BII and BGA (Appendix XII and XIII).

With that information provided, which includes the RTO and RPO for each IT application, the information system's department could arrange the technical means to implement it. This could be achieved in three different ways: entirely delegate this responsibility to an external IT provider, development of an internal solution or a mixed approach.[59]

5.4) Conclusion

This analysis demonstrates that by selecting recovery strategies for only thirty four percent of the internal processes, Banif can guarantee its continuity even under unexpected disruptive events. Acknowledging that these strategies could differ, the researcher believes that they represent Banif's attitude towards risk, since they are the most cost efficient and still deliver the desired recovery times. Therefore this project helped increase Banif's resilience – avoiding customer service, financial, legal and reputational harmful impacts – and enhanced confidence, by protecting its clients and shareholders interests. Finally, while meeting financial authority's requests, it will also contribute to a more stable financial sector.

[59] Further information about the IT strategy that would be implemented was unknown at the time of this project, since the IT department was undergoing a major reformulation.

VI. Limitations and Future Recommendations

Despite the underlining advantages of the developed framework, such as managing complexity, having a more strategic view and a practical implementation and flexibility, it has some limitations. Since it conglomerates processes into components that are later analyzed independently, some detailed information could be lost. Therefore, Banif should not be limited to it nor disregard a further verification of the selected strategies by process level.

Furthermore, regional disasters may jeopardize the execution of some selected recovery strategies. For example, in Lisbon, where the Bank holds most of its central buildings, this limitation can be stressed, since certain predetermined strategies would become inadequate. Therefore, Banif should have this in considerations and properly arrange alternative solutions, such as establishing additional hot and/or cold-sites. For this purpose a collaborative design with other banks could appear as a way to share the associated costs.

For future implementation, as parts of the BCM strategy, Mitigation Measures and the Response Structure should be further explored. Even though some are already implemented due to mandatory regulations, Banif should not discard a more thorough analysis to additional mitigation measures since they can prevent/avoid disasters, most of the times at a low capital expenditure.[60] On the other hand, the response structure implementation was not mentioned in this project since it had been previously defined at Banif, in the beginning of 2014. However, the researcher suggests a mass notification software implementation; this tool will ensure that notifications are quickly spread to all members of the response structure, providing brief first instructions and thus reducing the responsiveness upon a disaster event.

[60] An example of the mitigation measures implemented in Banif, besides the ones required by law, is the alternative electrical power supply installed in all its central buildings.

Moreover, threats with a lower risk scoring, identified during the risk assessment, should be considered for future BC improvements. For example, an organization may fail in its process of recovery due to external dependencies.[61] One way to avoid this is to identify all the critical suppliers, verify if they have a BCM program implemented that is periodically updated and encourage their participation in internal recovery strategies discussions.[62]

As a conclusion, Banif should perceive BCM not as a static implementation but as a continuous process in improving their preparedness towards disruptive events. Therefore, periodic tests and improvements to all BC elements should be taken as a serious commitment, starting from the Board of Directors to all employees within the organization. This commitment and involvement normally occurs while tests and reviews to the program are performed and requires an active participation.[63]

[61] This represents the fourth highest risk scenario identified that is "critical supplier service interruption".
[62] While performing BIA, information concerning external dependencies was collected for future improvements purpose.
[63] This was confirmed by the survey performed by the researcher that can be found in Appendix II. Other tools for engaging employees regarding BCM are highly recommended such as educational sessions, internal discussions and conferences.

VII. Bibliographic References

American Bankers Association. 2005. "Business continuity planning, born in DP, needs human element." *ABA Banking Journal*, (April), 46–48.

APQC, 2013. "Banking Process Classification Framework". *American Productivity & Quality Center.* http://www.apqc.org/process-classification-framework (accessed April, 2014).

Barney, J.B. 1991. "Firm resources and sustained competitive advantage." *Journal of Management*, 19, pp. 99-12.

Bradford, M. 1992. "Banks told to be ready to handle a power loss." *Business Insurance*, 26(9), 10–11.

British Standards Institution. 2007. BS 25999-2 Specification for business continuity management. London: *British Standards Institution*.

Broadbent, D. 1979. "Contingency planning." Manchester: *National Computing Centre*.

Burger, K. 1988. "Beyond DP: Banks expanding scope of disaster recovery." *Bank Systems and Equipment*, 25(3), 43–47.

Business Continuity Institute. 2013. "Good practice guidelines" (1st ed.). London: *Business Continuity Institute*.

Business Continuity Institute. 2010. "The Business Case for BCM". *Business Continuity Institute.*

Cherbakov, L., Galambos, G., Harishankar, R., Kalyana, S., & Rackham, G. 2005. "Impact of service orientation at the business level." *IBM Systems Journal*, 653-668.

Continuity Insights & KPGM LLP. 2012. "Global Business Continuity Management (BCM) Program Benchmarking Study." http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/2012-cin-kpmg-management-study.pdf (accessed April, 2014)

Dugan, E. 1986. "Disaster recovery planning: Crisis doesn't equal catastrophe." *Computer- world*, 20(4), 67–71.

Ferrier, N., & Haque, C. E. 2003. "Hazards risk assessment methodology for emergency managers: A standardized framework for application." *Natural Hazards*, 28(2-3), 271-290.

Gallagher, M. 2003. Business continuity management – how to protect your company from danger. 1st Edition: *Prentice Hall*.

Goh, M. H. 2013. A Manager's Guide to ISO 22301 Standard for Business Continuity Management System: An Organizational Journey to BC Management System. *GMH Continuity Architects*.

Gum, P. H. 1983. "System/370 extended architecture: facilities for virtual machines." *IBM Journal of Research and Development*, 27(6), 530-544.

Harmon, P. 2007 "Value Nets and Value Chains." BPTrends Advisor, Vol. 5, No. 12. http://www.bptrends.com/publicationfiles/advisor200706261.pdf (accessed on April, 2014).

Herbane, Brahim. (2010). "The evolution of business continuity management: A historical review of practices and drivers". *Business History*, 52(6), 978–1002.

Herbane, B., Elliott, D., & Swartz, E. M. 2004. "Business continuity management: time for a strategic role?" *Long Range Planning*, 37(5), 435-457.

Hiles, Andrew. 2010. *The definitive handbook of business continuity management*. Wiley.

Horváth, G. K., & CISM, C. 2013. Information Security Management for SMEs: Implementating and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle. Proceedings of FIKUSZ'13, 133-141.

International Organization for Standardization. 2012. ISO 22301 Societal security – Business continuity management systems – Requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038 (accessed March, 2014).

Labaka, L., Hernantes, J., Rich, E., & Sarriegi, J. M. 2013. "Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery." *Journal of Homeland Security and Emergency Management*, 10(1).

Latimore, D., & Robinson, G. 2004. "Component business modeling: a private banking example". *IBM Institute for Business Value*, 5(6).

Mitroff, I.I., & Alpaslan, M.C. 2003. "Preparing for evil." *Harvard Business Review*, 81(4), 109– 115.

Parsons, D. 2010. "Organisational resilience." *The Australian Journal of Emergency Management*, 25(2), 18-20.

Pohle, G., Korsten, P., & Ramamurthy, S. 2006. "Component business models. Innovative approaches for sustainable growth", 68. *IBM Business Consulting Services.*

Porter, Michael. 2008."The value chain and competitive advantage." *In Competitive Advantage: creating and sustaining superior performance*, ed. Simon and Schuster, 50-66.New York: The Free Press.

Vogler, M., & Perkins, C. 1991. "Disaster plans must focus on more than data." *National Underwriter*, 95(32), 17–19.

Warrick, Cathy & Sing, John. 2004. "A disaster Recovery Solution Selection Methodology". *IBM redbooks.* 1-17. http://www.redbooks.ibm.com (accessed April, 2014)