universität wien

MASTERARBEIT

Titel der Masterarbeit

“The use of Soft System Methodology as a basis for the Analysis of IT-related Risk”

verfasst von

Daniel Nagj

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2014

Studienkennzahl lt. Studienblatt: A 066 926

Studienrichtung lt. Studienblatt: Masterstudium Wirtschaftsinformatik

Betreut von: Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Abstract

In recent years Business Continuity Planning (BCP) has received greater attention within many organizations. It is used to identify internal and external threats to an organization as well as to identify effective prevention and mitigation strategies to the threats discovered. An important part of the BCP process is the conduct of a risk analysis which is based on identifying, assessing and prioritizing the risks/threats to an organization. Soft Systems Methodology (SSM) is a model based on the holistic and systematic characteristics of complex organizations. The purpose of this thesis was to develop a BCP reference model by using SSM for structuring and performing a risk analysis. The reference model developed was then used on the credit card opening process of the Erste Bank in Austria to establish the usefulness of the model.

Following a brief description of terminology, the thesis is structured as six Chapters. Chapters 1 and 2 are based on thorough background research conducted by the author and describe the principles, methodologies and practice of BCP and SSM. Chapter 3 then describes the development of a BCP reference model that uses the seven-stage step-wise SSM methodology as the basis for risk analysis.

In Chapter 4, the applicability of the reference model was tested for both identifying and dealing with risks inherent in the current process or "system" used by the Erste Bank Austria for opening a credit card account. This involved *inter alia*: entering and expressing the "problem situation"; formulating a "root definition" of the system based on both rigorous and comprehensive criteria that ensured inclusion of all tasks involved and therefore likely to be affected by subsequent changes; building a Conceptual Model covering the relevant risks within the overall system (covering tasks/activities that have to be performed within a risk analysis); comparing the model with the real world; formulating changes in structure, procedures and/or attitudes that would be both desirable and feasible; and finally, making recommendations for actions that would improve the real world situation such as increased automation, although because of increased capital and/or operational costs the feasibility of doing this would require detailed analysis prior to presentation to higher management and/or the Board for final approval. These steps are not covered by this thesis.

Chapter 5 then discusses the results obtained using SSM, comparing the advantages and disadvantages of this approach for conducting risk analysis with other available models such as the Object-Process Methodology (OPM) and the Structured Systems Analysis Design Method (SSADM) in terms of quality, clarity, extent of stakeholder involvement etc. While it is acknowledged that SSM has deficiencies for analyzing hard facts, its advantages in terms of dealing with soft systems (i.e. systems highly dependent on human activity and interactions such as opening a credit card account with a bank), arise from the improved understanding it provides of the problem at hand through its inherently iterative processes and use of the rich picture. As exemplified by the bank case study described in this thesis, even in the absence of hard facts, it was possible to use the SSM for both conducting a comprehensive risk analysis and identifying potentially desirable and feasible changes for

improving the current system in operation at the Erste Bank for opening a credit card account.

Based on the study and analyses undertaken, the fundamental conclusions reached by the author in Chapter 6 are firstly, that while SSM can indeed be used to structure and perform a risk analysis for the purpose envisaged in the thesis, it is questionable whether it was worth the effort to go through a seven-stage model to achieve the goal; possibly, similar results could be obtained using the same model with fewer or by combining steps. Secondly, that the use of quantitative data concerning some risks would be advantageous for improving the rigour of the analysis. And finally, it is recommended that a fully-fledged model is created to provide a comprehensive framework for using SSM to perform a risk analysis.

Kurzfassung

In den letzten Jahren tendieren Organisationen vermehrt dazu, dem Business Continuity Management (BCM) eine höhere Aufmerksamkeit zu geben. BCM wird verwendet, um interne und externe Bedrohungen für eine Organisation zu identifizieren und Prävention sowie vorbeugende Gegenmaßnahmen durchzuführen. Ein zentraler Teil des BCM ist die Durchführung einer Risikoanalyse, die auf Identifizierung, Bewertung und Priorisierung der Risiken/Gefahren für eine Organisation basiert. Soft System Methodology (SSM) ist ein Modell, das verwendet wird, um eine Problem Situation ganzheitliche zu betrachten und deren Korrespondenzen ausführlich zu analysieren, um Verbesserungsmöglichkeiten zu finden. Das Ziel dieser Arbeit war es, ein BCM Referenzmodell für die Risikoanalyse zu erstellen das mit der Verwendung von SSM strukturiert und umgesetzt wird. Das entwickelte Referenzmodell wurde anschließend auf den Kreditkarteneröffnungsprozess der Erste Bank Österreich angewendet, um die Brauchbarkeit des Modells zu testen.

Nach einer kurzen Beschreibung der Terminologie ist die Arbeit in sechs Kapiteln gegliedert. In Kapitel 1 und 2 wird eine ausführliche Recherche der Prinzipien und Methoden von BCM und SSM durchgeführt. In Kapitel 3 wird beschrieben wie das BCM Referenzmodell mit Hilfe der siebenstufigen SSM entwickelt wurde.

In Kapitel 4 wurde die Anwendbarkeit des Referenzmodells für die Identifizierung und den Umgang mit Risiken gegen den aktuellen Kreditkarteneröffnungsprozess der Erste Bank Österreich getestet. Dies beinhaltet unter anderem: Die Problem Situation zum Ausdruck zu bringen; Formulierung einer „Root-Definition“ des Systems; den Aufbau eines Konzeptionellen Modelles für die relevanten Risiken im Gesamtsystem (Tätigkeiten, die innerhalb einer Risikoanalyse durchgeführt werden müssen); Vergleich des Modells mit der realen Welt; Formulierung von Veränderungen in der Struktur die wünschenswert wären, sowie abschließend eine Empfehlung, welche Tätigkeiten vorgenommen werden sollen, wie zum Beispiel eine erhöhte Automatisierung im Kreditkarteneröffnungsprozess. Für die Umsetzung der vorgeschlagenen Änderungen wären noch eine detaillierte Kostenschätzung und eine endgültige Genehmigung des Managements erforderlich. Diese Schritte sind aber nicht mehr Teil dieser Arbeit.

Kapitel 5 beschreibt dann die mit SSM erzielten Ergebnisse und vergleicht die Vor- und Nachteile dieses Ansatzes mit anderen Modellen, wie zum Beispiel der „Object – Process Methodology“ (OPM) und der „Structured Systems Analysis Design- Methode“ (SSADM) in Bezug auf Qualität, Klarheit, usw.

Der größte Nachteil von SSM ist ihr Schwachpunkt bei der Analyse von „hard facts“. Trotzdem ist diese Methodologie sehr nützlich für den Umgang mit „Soft-Systems“ (System die stark von menschlichen Aktivitäten abhängig sind). Durch den iterativen Prozess und die Nutzung eines „rich-picture“ kann ein sehr gutes Verständnis des Problems erzielt werden. Ein gutes Beispiel dafür ist die Risikoanalyse die in dieser Arbeit mit Hilfe von SSM gemacht wurde. Obwohl keine „Hard-facts“ bei der Analyse benutzt wurden war es trotzdem

möglich, zahlreiche Risiken im Kreditkarteneröffnungsprozess zu identifizieren, sowie wünschenswerte und machbare Änderungen vorzuschlagen.

Basierend auf der durchgeführten Analyse werden in Kapitel 6 einige Schlüsse gezogen. Die wesentlichste Schlussfolgerung ist, dass obwohl die SSM Struktur verwendet werden kann um eine Risikoanalyse durchzuführen, es fraglich ist, ob es sich auszahlt, ein siebenstufiges Modell zu durchlaufen um das Ziel zu erreichen. Eventuell könnten ähnliche Ergebnisse mit dem gleichen Modell aber mit weniger Ablaufschritten erreicht werden. Außerdem wäre der Einsatz von quantitativen Daten für einige Risiken sicher vorteilhaft gewesen. Darüber hinaus wäre es empfehlungswert, anstatt des Referenz-Modelles ein vollständiges Modell zu entwickeln, um ein umfassendes „Framework“ für die Verwendung von SSM für Risikoanalysen zu haben.

Acknowledgement

Foremost I would like to express my gratitude to my advisor Prof. Gerald Quirchmayr for the valuable guidance, advice, patients and continuous support throughout my thesis research. His guidance was of great help in times when I was unsure of how to continue.

I would also like to thank Erste Group Bank, especially Dr. Michael Berger who provided me with the credit card opening process of Erste Bank Austria. This allowed me to test the developed reference model against a real case scenario.

Table of Contents

Introduction

In recent years, world events have presented challenges for organizations to protect themselves from threats such as terrorist attacks, earthquakes, fires, power failures, cyber-attacks and many more. Therefore it is important that an organization creates an on-going interactive process that serves to assure the continuation of its core activities before, during and after a major crisis event. This process can be described as "Business Continuity Planning". A good Business Continuity Plan (BCP) will keep an organization running through interruptions of any kind that include: IT system crashes, power failures, natural disasters and others. Having a business continuity plan is therefore of great importance for each and every organization. Unfortunately many small and medium sized businesses are often unprepared for disasters. According to the disaster recovery and business continuity survey conducted by Agility Recovery Solutions and the Hughes Marketing Group, most businesses (around 95%) only have a data backup system, and on average less than 50% are able to continue their business processes within a few days in the event of a more serious disaster.

A BCP includes numerous tasks whereby the Risk Analysis (RA) and Business Impact Analysis (BIA) play a crucial role within the BCP. A RA has to be performed to determine what types of threats a business could be facing while a BIA has to be performed in order to analyse what effect(s) those risks/disruptions might have on the business. In other words, RA and BIA are procedures to identify threats and vulnerabilities, analyse them to ascertain exposure, and to highlight how potential impacts can be eliminated or reduced[1].

In order for an organization to implement a BCP certain steps have to be followed. These steps are described in this thesis. Apart from knowing the steps that have to be taken to create a BCP it is also helpful to have a reference model that can be followed in order to achieve the targets. Although the thesis describes the whole process of BCP, the reference model described focuses mainly on the process for RA.

Although for the analysis performed in Chapter 4, the primary knowledge required for its understanding is based on RA, BIA and SSM, a detailed research on BCP is nevertheless performed. This is because RA and BIA are part of the BCP process and research on BCP is required to obtain a better understanding of the dependencies between the different tasks. However, it is possible to perform a RA as well as a BIA without detailed knowledge of the BCP process.

To create the reference model the guidance contained in the Soft Systems Methodology (SSM) developed by Peter Checkland was used. SSM is carried out through a seven-stage process, its primary use being to analyse complex situations where there are divergent views about the definition of the problem.

The thesis is divided into six parts. The first two parts contain a literature survey on Business Continuity Planning and Soft Systems Methodology, while the third part is devoted to the

[1] http://17799.denialinfo.com/risk.htm.

development of the reference model based on the literature survey. In the fourth part, the reference model developed is tested against a real case scenario - namely the process for opening a credit card account in a banking institution. The fifth part is a summary of the results and describes the achievements of the thesis, while the sixth outlines the major conclusions reached and a recommendation for future work.

Terminology

Below are definitions of Business Continuity (BC), Business Continuity Planning (BCP), Business Continuity Management (BCM), Risk Analysis (RA) and Business Impact Analysis (BIA). Although Business Continuity Management is outside the scope of this project some definitions are provided because the author considers that Business Continuity Planning and Business Continuity Management are very similar if not the same, and therefore that it is interesting to compare the two terminologies. In addition the terminology Risk Analysis as well as Business Impact Analysis are included as they play a crucial role within the BCP and BCM processes.

Business Continuity (BC)

"Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions[2]"

"A comprehensive managed effort to prioritize key business processes, identifies significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis[3]"

"Business Continuity is a pro-active process which identifies the key functions of an organization and the likely threats to those functions[4]"

Business Continuity Planning (BCP)

"Business Continuity Planning is the advance planning and preparations that are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organizational services in the event of an emergency or disaster; and to deliver a comprehensive training, testing and maintenance programme[5]"

"Business Continuity Planning is an on-going process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing, and maintenance[6]"

[2] http://en.wikipedia.org/wiki/Business_continuity.
[3] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 9.
[4] http://www.bcmpedia.org/wiki/Business_Continuity.(BC).
[5] Glossary General Business Continuity Management Terms, The Business Continuity Institute, http://www.thebci.org/Glossary.pdf.
[6] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 9.

"Business Continuity Planning is the advance planning and preparations which are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organizational services in the event of an emergency or disaster; and to administer a comprehensive training, testing and maintenance programme[7]"

Business Continuity Management (BCM)

"Business Continuity Management is an holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities[8]"

"Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputations, brand and value creating activities. Also the management of the overall programme through training, rehearsals, and reviews, to ensure the plans stay current and up to date[9]"

"Business continuity management is:

- The on-going management of the business continuity plan to ensure that it is always current and available; and
- the on-going management of operational resilience and process availability within an organization, with the aim of ensuring that the organization experiences the minimum possible day-to-day disruption[10]"

[7] http://www.bcmpedia.org/wiki/Business_Continuity_Planning.(BCP).
[8] Glossary General Business Continuity Management Terms. The Business Continuity Institute. http://www.thebci.org/glossary.pdf.
[9] http://www.bcmpedia.org/wiki/Business_Continuity_Management.(BCM).
[10] http://www.continuitycentral.com/newtobusinesscontinuity.htm.

Risk Analysis (RA)

"The quantification of threats to an organization and the probability of them being realized[11]"

"Risk Analysis is the process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities (likelihood) of a particular event[12]"

"A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences[13]"

Business Impact Analysis (BIA)

"The process of analyzing business functions and the effect that a business disruption might have upon them[14]"

"A management level financial analysis that identifies the impacts of losing an organization's resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide reliable data upon which to base decisions on mitigation, recovery, and business continuity strategies[15]"

Summary

Business Continuity:

- A pro- active process
- Identifies threats to key functions
- A progression of disaster recovery
- The continuation of function during and after a disaster
- Maintains viable recovery strategies

[11] Glossary General Business Continuity Management Terms. The Business Continuity Institute. http://www.thebci.org/glossary.pdf.
[12] http://www.bcmpedia.org/wiki/Risk_Analysis
[13] http://www.nr.no/~abie/RiskAnalysis.htm
[14] Glossary General Business Continuity Management Terms. The Business Continuity Institute. http://www.thebci.org/glossary.pdf.
[15] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 5.

Business Continuity Planning:

- Planning and preparation
- Identify the impact of potential losses
- Formulating and implementing recovery strategies
- Developing continuity and recovery plans
- Training, testing and maintenance

Business Continuity Management:

- A holistic management process
- Identifies potential impacts
- Provides a framework for resilience
- Safeguards stakeholders, reputations, brand and value-added activities
- Retains customers
- Involves training, rehearsals and reviews to keep plans up to date
- Ensures the continued achievement of critical objectives
- Minimizes and manages disruption risks

Conclusions

From the definitions above it can be concluded that BC, BCM and BCP have very similar meanings. For example BC and BCM are processes which identify threats and then responses to these. For this study, many resources were consulted but only British Standards defined both terms, whereas in most other cases either the term Business Continuity or BCM was defined. The author therefore concluded that Business Continuity and BCM have the same or a very similar meaning.

The next aspect to be clarified is the difference between BCP and BCM. Once again, comparison of the definitions of the two terms revealed that there was no or very little difference. BCP may be seen as the physical plan that comes out of the BCM process. However, and as noted above, the author feels that there is very little difference and therefore for the purpose of this thesis, BCP is the term used in further discussion.

Chapter 1: Business Continuity Planning

1.1 Introduction

A BCP is very important for every "business organization". A business organization in this context is any organization that provides services or goods, either to individual customers, to other business organizations, or to the public[16]. This includes manufacturers, distribution companies, sales and transport organizations, utility companies, community services and many more. Not all these organizations exist to make profit, but they all provide some service to somebody, and they are all exposed to risks which can interrupt their business through an unpredictable event such as an earthquake, fire, electricity outage, etc. Therefore every organization should consider having a BCP in place if it is to optimize its chances of successful resumption of business following an interruption.

A BCP addresses actions to be taken before, during, and after a disaster. It should also specify in detail what, who, how, and when[17]. In most cases the interruptions that affect business functions will involve equipment failure, theft, or employee sabotage; however, the organization should also be prepared for the "worst case scenario" meaning that the interruption will occur through major natural disasters such as tornadoes, floods, and fires, or from man-made disasters such as terrorist attacks.

Since one of the main challenges of developing a BCP is to decide on the limits to which resources should be duplicated, it is recommended that as many opinions as possible are taken into consideration when prioritizing the processes. It is unrealistic to expect that the complete business infrastructure can be replaced and duplicated. Therefore it is very challenging to decide on the most critical business activities that can still be executed with limited infrastructure (hot sites) and personnel in case of a disaster. Clearly therefore, no BCP will ever cover all areas and all risks.

Business Continuity Planning requires both immediate and long term resources. Each business unit must be analysed. New equipment may be needed including: a better computer backup process, new security systems, or alternative communications. Organizations may need more insurance coverage, better software, a fire-resistant safe, fences, and much more. The list can be long, suggesting that a BCP may be costly to implement. On the other hand, if disaster strikes the potential damage and cost could be much greater.

[16] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 4.
[17] Texas Department of Information Resources (2004). Business Continuity Planning Guideline, p. 1.

1.2 History of Business Continuity

Business Continuity has its roots in disaster recovery, which emerged in the 1950s and 60s as companies began to store backup copies of their critical data in paper or electronic forms at alternate sites[18]. Initially it was not very popular to have file backup and off-site storage procedures; however, these became more common in the 1970s when a handful of third party storage facilities created an alternative or "hot" site. By the 1980s, alternative sites had become a popular disaster recovery solution for data-dependent financial firms with large, centralized mainframe computers.

The greatest change happened in the early 1990s when computer systems moved from being housed in large centralized data centres to the field. This had a massive impact on the disaster recovery industry. Personal computers (PCs) became ubiquitous, and most companies moved from one centralized mainframe to vast networks of servers and desktop PCs distributed throughout the organization[19]. At this point the term Business Continuity became a popular replacement for the term disaster recovery. This was because computer systems were beginning to have more important roles in organizations, making them more vulnerable to human errors, to network downtime and intrusion, as well as to communication failures. The term disaster recovery therefore came to be used to describe the traditional IT-specific issues involving data backup and recovery, while business continuity became the term to describe the need to maintain continuity across individual enterprises, from facilities to people to communications[20].

[18] http://www.businessresiliency.com/evolution_history.htm.
[19] Ibid.
[20] Ibid.

1.3 Developing the Business Continuity Plan

There are many different approaches for developing a BCP. After detailed research, it was decided to use a five-phase approach because this covers a wide range of specifications: readiness, prevention, response, recovery/resumption and test/maintain. Such an approach is also recommended by ASIS International, which is an organization for security professionals who develop security management standards and guidelines.

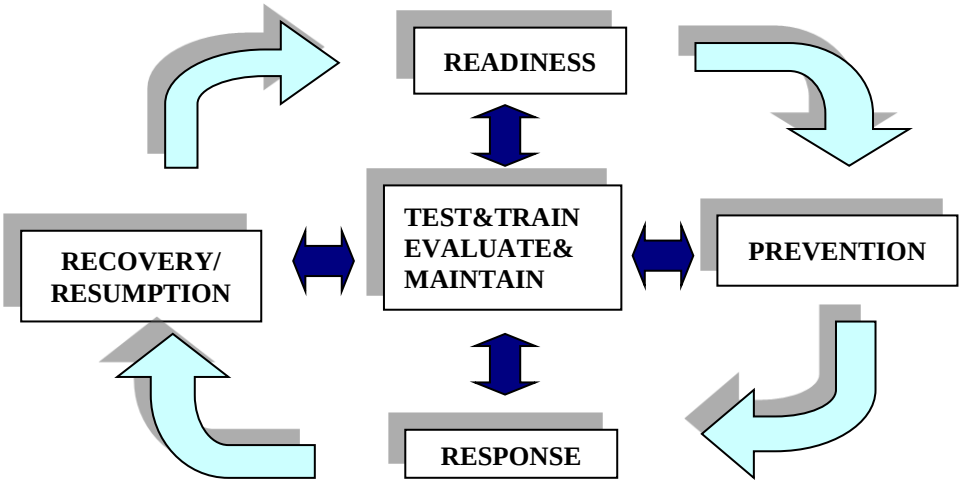

Figure 1: Business Continuity Preparation Process[21]

1.3.1 Readiness

Objective	Address the preparatory steps required to provide a strong foundation on which to build a BCP.[22]
Tasks	Assign accountability, perform risk assessments, conduct business impact analysis, agree on strategic plans, crisis management and response team development.

In order for an organization to be prepared for a disaster it is essential that senior management takes responsibility for creating, maintaining, testing and implementing a comprehensive BCP. A good way to start is with a top-down approach, where a system is broken down to gain insight into its compositional subsystems. In a top-down approach an overview of the system is first formulated which specifies without detailing, any first level subsystems. Each subsystem is then refined in yet greater detail, sometimes at many additional subsystem levels, until the entire specification is reduced to base elements[23].

[21] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p.10.
[22] Ibid.
[23] http://en.wikipedia.org/wiki/Top-down_approach.

When creating the BCP it is essential for senior managers to include\know the following:

- **Corporate Policy –** In the event of a crisis, an organization is committed to undertake all reasonable and appropriate steps to protect people, property and business interests[24].
- **Ownership of Systems, Processes and Resources –** The responsibility for systems and resource availability and key business processes should be clearly identified in advance[25].
- **Planning Team -** A Business Continuity Planning Team with responsibility for BCP development that includes senior leaders from all major organizational functions and support groups should be appointed to ensure widespread acceptance of the BCP[26].
- **Communicates BCP -** The BCP should be communicated throughout the organization to ensure employees are aware of the BCP structure and their roles within the plan.

1.3.1.1 Risk Assessment

The next step is to conduct a risk assessment in order to identify and analyse the types of risks that may impact the organization. A risk in this context is the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities.[27] A risk assessment is the overall process of risk identification, risk analysis and risk evaluation[28]. These risks may range from those with a high probability of occurrence and low impact such as a brief power interruption, to those with a low probability of occurrence and high impact such as natural disasters or terrorist attacks. The most difficult threats to address are those that have a high impact and low probability of occurrence. When doing the risk assessment it is important to use all available information and look at the history of threats that already impacted the organization. The geographical location of all facilities should be considered when identifying and reviewing risks because of natural hazards and facilities nearby that could endanger the organization (e.g. nuclear power station, airports, power plants, etc.). Once all the possible risks have been identified, the likelihood of each happening should be rated. This is a very difficult task because it is hard to quantify potential risks as well as the potential losses and probability of their occurrence. There are high chances of an error occurring when performing this task and it is also very likely that two analysts will have different opinions on certain risks.

[24] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p.10.
[25] Ibid.
[26] Ibid.
[27] http://www.businessdictionary.com/definition/risk.html.
[28] http://www.bcmpedia.org/wiki/Risk_Assessment.

The most common way of performing this task is by creating a risk assessment matrix which sets out to identify risks and prioritize planning strategies. When creating this matrix it should include - but not be limited to - the following major categories of risk[29]:

- Human resource loss
- Technological system loss
- Supply chain interruption
- Physical site loss
- Market access loss
- Cash flow disruption
- Risk related to business partner loss or severe disruption in their business

The matrix itself should contain but not be limited to the following variables: *Threat*, *Likelihood (Rate)*, *Impact (Rate)*, and their *Relative Weight*. Likelihood and impact are the two most important variables. However, additional variables such as onset speed (slow, fast), forewarning (sufficient, insufficient), duration (short, long) and intensity (low, high) can be added as additional columns and entered into the formula[30].

Below is a sample illustrative matrix:

Threat	Likelihood (1-5 (1 = very low, 5 = very high)	*(	Intensity (1 = low, 2 = high)	+	Duration (1 = short, 2 = long)	)*	Impact (1 = low, 5 = very high)	=	Relative Weight

1.3.1.2 Business Impact Analysis

Once the risks have been identified, any organizational impact that could result from an interruption of normal operations should be examined through a Business Impact Analysis (BIA). In other words, after the various threats have been identified in the risk assessment, BIA looks at the critical business functions and the impact of not having those functions within the organization for a set period of time. The two assessments (i.e. RA and BIA) look at the company from two different angles[31]. The risk assessment starts from the threat side,

[29] http://www.tbicentral.com/our-white-papers/business-continuity-planning-framework.
[30] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 12.
[31] Snedaker Susan (2010), Business Continuity and Disaster Recovery Planning for IT Professionals, p. 210.

and the business impact analysis starts from the business process side[32]. In the business process, the processes in the organization which are vital for ongoing operations should be determined and the impact that disruption of these processes would have to the organization should be understood. Therefore it is possible to start with the risk assessment and map the risks and threats discovered to the processes that it might affect, or it is possible to start with the BIA and perform a risk assessment on the processes defined as crucial. Both methods are valid and used within organizations.

The key activities within a BIA include the following[33]:

- **Identify key business process and functions**

  This very important step involves identifying the critical processes and functions within an organization, followed by their categorization. A common categorization system for assessing critical business functions would be as follows:

  - Critical functions
  - Essential functions
  - Necessary functions
  - Desirable functions

  The functions and processes determined as critical and essential should be handled first.

- **Establish requirements for business recovery**

  Establishing requirements for recovery of the business refers to the resources to recover the business functions under analysis. These include human resources (i.e. skilled people) as well as technical resources such as phones, computers, desks, etc.

- **Recovery time requirements**

  Once the critical business functions are identified it is necessary to establish timeframes for recovering the critical functions identified. The most common terms used for recovery time requirements are:

  - Maximum Tolerable Downtime (MTD) – The maximum time a business can tolerate the absence of a particular business function.
  - Recovery Time Objective (RTO) – RTO is part of the overall MTD. RTO is the time available for the organization to recover the disrupted process.
  - Work Recovery Time (WRT) – WRT is also part of the overall MTD. WRT is the time it takes the business to run normally again.
  - Recovery Point Objective (RPO) – RPO usually only applies to IT critical systems because it indicates the amount of data loss that can be tolerated by the critical business system.

[32] Ibd.
[33] Ibid

From the above one can conclude the MTD = RTO + WRT. The difference between RTO and WRT can be exemplified by the following: In case a system is down the RTO would be the amount of days it takes to restore the system (e.g. 1 day) and WRT is the time it takes for the critical business function to be up and running again (e.g. 2 days). In this example the MTD would be 3 days.

One can therefore conclude that MTD and maximum allowable downtime have the same meaning.

- **Determine interdependencies**

  For this task the interdependencies between the business functions have to be established. With the interdependency analysis it should be determined which other process and functions could be affected should a disruption occur to the business function or business process under analysis.

- **Determine impact on operations**

  The aim with this task is to find out how the operation of the organization would be impacted in case the business function under analysis is not available for a period of time.

- **Develop priorities and classifications of business processes and functions**

  Once the critical business functions and process have been identified and the impact of their absence on operations has been determined it will be necessary to prioritize the business processes and their functions. Those processes and functions considered being critical and having a high impact on operations should be handled first.

- **Determine financial impact of disruption**

  Possible costs arising from an unforeseen event or disaster are[34]:

  - **Human Cost -** physical and emotional harm to employees, customers, suppliers, other stakeholders, etc.
  - **Financial Cost -** equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales, regulatory fines, etc.
  - **Corporate image cost -** reputation, standing in the community, negative press, loss of customers, etc.

Another important function of the BIA is to determine the maximum allowable downtime for critical business functions and processes and the acceptable level of losses (data, operations, financial, reputation, etc.) associated with the estimated downtime. These recovery objectives require management to determine which essential personnel, technologies, facilities, communications systems, vital records and data must be recovered, and what processing sequence should be followed so that activities that fall directly on the critical path receive the

[34] Ibid.

highest priority[35]. From the definition it can be concluded that the maximum allowable downtime is a combination of "identification of key business process and functions and its categorization" with "recovery time requirements referencing MTD".

The development of an initial BIA goes through a various phases and should be approached as a project that involves the following steps:

- Project Planning

  The first aim in the creation of a BIA is to gain commitment from management, and objectives have to be established which set priorities and enable sign-off of project deliverables. Because the BIA requires input across the organization, management needs to ensure that the entire organization accepts the process and is responsive to the responsible project team.

- Data gathering

  In this phase the critical business functions and the tools and expertise required to perform each are identified. Data are gathered primarily through workshops, questionnaires, telephone conferences and emails. Process flows should be demonstrated. It is up to the business unit manager(s) to ensure that the employees within the unit(s) concerned support the BIA project team by gathering the data required.

- Data analysis

  The data analysis phase involves quantitative analysis of the data collected; this allows the organization to determine the amount of time it can tolerate an extended outage. After key data is gathered, criticality levels should be introduced for the business and IT functions.

- Documentation of the findings

  The findings have to be documented. The BIA report should include but not be limited to the following: recovery time objectives, recovery point objectives, potential financial (i.e. revenue and, market share losses, etc.) and non-financial (i.e. reputation) losses and human and physical resources required to support business units.

- Management review and sign off

  The management is responsible for reviewing the document and making decisions about which process prevention or mitigation strategies should be developed.

[35] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 9.

From the above, it can be concluded that risk assessment and BIA provide the foundation upon which an organization's BCP rests, since strategies will be formulated and plans developed to meet the needs identified therein[36]. Since they allow management to identify the organisation's most critical business processes, they should be repeated regularly and particularly in response to significant changes in the organization's operating environment.

1.3.1.3 Strategic Planning

Once the key activities and resources have been identified together with the associated risks, the risks need to be managed.

The risks identified are important throughout strategic planning because developing a strategic plan for their management could be very costly; on the other hand, deciding to accept the risk could be even more costly. One can therefore conclude that accepting an increased risk can be rewarding but it can also mean complete disaster. Below are the three most common strategies for management decision-making:

- **Accept the risk and change nothing**

  The organization accepts the risk and waits until a disaster happens and hopes to acquire equipment and facility at the time. This may be appropriate only in cases where an organization can afford a longer restoration period.

- **Attempt to reduce the risk**

  Reduce the risk with some mitigation and prevention strategies. These are discussed later under mitigation and prevention strategies.

- **Attempt to reduce the risk and make plans to restore key activities as soon as possible**

[36] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p.13.

Strategic planning applies to point 3, and the aim of a strategic plan is to implement plans and procedures to respond to any crisis that might occur and to identify methods to mitigate the risks and exposures identified in the BIA and risk assessment. Options that can be considered by an organization to restore key activities quickly after a disaster include:

- **Offsite Storage**

  Offsite storage is a valuable mitigation strategy allowing rapid crisis response and business recovery/resumption[37]. The offsite storage location should be a sufficient distance from the primary facility so that it is not likely to be similarly affected by the same event[38]. Items to be considered for offsite storage include critical and vital records such as documents, tools, computer tapes and discs. Computer data can be transmitted to online backup to tapes stored in tape libraries or silos to disc arrays[39].

  Offsite storage backup should aim to supply secure storage, with contents retrievable 24 hours a day, 365 days a year.

- **Continuous Processing**

  Continuous processing will provide continuous "mirroring" of the production operation at an alternative site with adequate capacity and communications links to permit the production operation to be switched to the alternative site at minimal notice[40].

- **Distributed Processing**

  Distributed processing will carry out processing in more locations and therefore spread the risk around different locations so that in the event of a disaster the whole organization will not be affected.

- **Quick Resupply**

  This approach depends on acquiring equipment, software and communications facilities when the disaster occurs[41]. Equipment vendors or disaster recovery service suppliers may guarantee resupply within a specified timescale in return for a retainer[42].

[37] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 22.
[38] Ibid.
[39] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 5 197.
[40] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 5 196.
[41] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 5 197.
[42] Ibid.

These are just some of the possible strategies, but these and many others can be considered to reduce the risks, mitigate impacts, recover systems and data and resume the business. Strategies therefore address a variety of probable situations, including the duration of the business interruption, the period over which it occurs and the extent of the interruption[43].

It is, however, important that the strategies selected are[44]:

- Attainable
- Have a high probability of success
- Verifiable through tests and exercises
- Cost effective
- Appropriate for the size and scope of the organization

This aspect is discussed further in the Prevention and Response section of the thesis.

1.3.1.4 Developing a Crisis Management Team

One of the most critical steps in a BCP is to form an appropriate crisis management team. Its membership must include the right balance of technical skills, business process knowledge, leadership, and the attitudes to successfully develop an effective continuity plan for the organization. It should therefore be comprised of such skills as human resources, information technology, facilities, security, legal, communications relations, warehousing, and other business critical supporting functions. Another important aspect is that management structure, authority for decision, and responsibility for implementation should be clearly defined. The crisis management team may be supported by as many response teams as appropriate taking into account such factors as organization size and type, number of employees and their locations, etc.[45] Response teams should develop response plans to address specific aspects of potential crisis, such as damage assessment, site restoration, payroll, human resources, information technology, and administrative support. Research has shown that a crisis management team should include at least the following four types of team members:

- **Team leader**

  The team leader should be an individual with sufficient time to spend on the effort and who is also familiar with the organization's technical and business process environments.

[43] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 14.
[44] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 14.
[45] Ibid.

- **Technical team members**

  Technology is a significant concern when planning for business continuity. Most modern organizations nowadays depend on data for everything, and therefore it is important that the technical team consists of a variety of specialists.

  Depending on the business requirements the technical team should consist, but not be limited to:

  - System administrator
  - Database administrator
  - Storage engineer
  - Security professional
  - Application specialist
  - Backup technician

- **Business process team members**

  Since it is important that the team selected has a thorough understanding of each business process, it will be necessary to select a team that is broad enough to represent each of the major business units or processes involved in the organization.

- **Supporting team members**

  During the planning phase, the BCP team leader and business process and technological members will need assistance from others within the organization. Those who may be considered for inclusion in the BCP support team include[46]:

  - **General counsel**

    This individual plays an invaluable role in navigating the legal and regulatory issues surrounding business continuity and disaster recovery.

  - **Public affairs representatives**

    These people serve as the public face of the organization in the event of a disaster; they may have to deal with specific issues and/or issues that are local, national, or global in scope. There will be a demand for information, and management should work with the public affairs group to ensure that it is prepared for that eventuality.

[46] Hewlett-Packard Development Company, LP (2007). Assembling a Business Continuity Planning Team, p. 3.

- **Administrative assistants**

  These individuals can help with the documentation and administration of the BCP. They, too, play an important role in coordinating the company's response in the face of an emergency.

- **Procurement specialists**

  These people can bring important supply-chain knowledge to the BCP table. They know who to contact and what to expect in terms of costs and lead times when planning BCP purchases. For example, procurement specialists can determine how quickly and at what cost replacement servers can be on-site in the event of an emergency.

As with the other teams, the exact composition of the BCP team depends on the organization's specific needs, and therefore some time should be invested in developing a good team.

1.3.2 Prevention

Objective	Address those areas where good planning will allow an organization to avoid, prevent, or limit the impact of a crisis occurring.[47]
Tasks	Compliance with corporate policy and prevention and mitigation strategies.

1.3.2.1 Compliance with Corporate Policy

A BCP has its own policy statements. Usually it is the responsibility of the Board and senior management of an organization to establish policies that define how identified risks will be managed and controlled. This policy is a document written to convey management expectations, in this case regarding long term, life cycle-oriented business continuity programme performance[48]. The policy statements should provide a high level overview of the objectives and expectations, and should rarely change. A well written policy will describe the key players and their responsibilities and will provide clear expectations for business continuity personnel, senior management, key planning contributors and all other employees. It is up to the management to decide whether the format is one with each sentence being numbered or merely a simple checklist, as long as the users of the procedures are comfortable with it.

In order to determine if the formats of the procedures are effective, employees who are newly trained on that function should be tested. If it takes many hours of training to be able to understand and follow the procedures then they are probably too complicated or confusing[49].

When writing the BCP policy statement it is important to remember that compliance with the corporate policy has to be conducted to enforce BCP policies and procedures. Policy and procedural violations should be highlighted and accountability for corrective action assigned in accordance with organizational governance regimes[50].

[47] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 15.
[48] http://www.continuitycentral.com/feature0607.html.
[49] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 185.
[50] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 15.

1.3.2.2 Prevention and Mitigation Strategies

The difference between a prevention strategy and a mitigation strategy is that the former aims to prevent damage from occurring whereas the latter attempts to reduce the impact of damage that occurs in a disaster. It is important to use both prevention and mitigation strategies in tandem in a BCP since they are complementary and thereby increase the overall benefit to the organization. An example of what the differences might look like in a real life situation is given below[51].

Mitigation strategies are developed to resolve potential problems that may arise from internal and external interdependencies. They will depend upon the outcome of the BIA and risk assessment, but should always ensure that processing priorities can be implemented adequately and that the business operations can be resumed in a timely manner[52]. Therefore the strategy should provide detailed information that covers what should happen before, during and after an event. The tables below illustrate how prevention and mitigation strategies can be provided to cover actions that occur before, during and after an event. This example shows how to cover the critical function of providing electrical power for a facility[53].

Before	**During**	**After**
Obtain an emergency diesel driver engine.	Verify the generator is running.	Perform maintenance to repair any malfunctions that occurred during or as a result of continuous operation.
Test the generator monthly.	Verify the fuel tank is full.	Refill fuel tank.

Prevention	**Mitigation**
Install high temperature cut offs to prevent overheating of oven.	Sprinkler system to control fire in an oven.
Install emergency generators that provide immediate power in event of a power loss.	Contract service provider to provide generators within 24 hours of a power loss.

The three most common mitigation strategies are: a device mitigation strategy, a resources-needed mitigation strategy, and a monitoring system and resource strategy. Device mitigation strategies are employed to prevent or lessen the impact of a potential crisis. For example, securing equipment to walls or desks with strapping can mitigate damage from an

[51] Ibid.
[52] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 15.
[53] The St. Paul Travelers Companies (2006). Strategy Guide for Business Continuity Planning, p. 15.

earthquake; sprinkler systems can lessen the risk of fire; a strong records management and disaster recovery programme can mitigate the loss of key documents and data[54]. In the "resources needed mitigation strategy" the various resources required for the mitigation process are identified. The "monitoring system and resource strategy" is used, as the title suggests, for the continuous monitoring of systems and resources. This is very important, because in case of a crisis the organization should be able to rely on the resources and systems which are introduced. Examples of such systems and resources include, but are not limited to[55]:

- Emergency equipment
- Fire alarms
- Local resources and vendors
- Alternate worksites
- Maps and floor plans updated due to constructions and internal moves
- System backups and offsite storage

[54] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 15.
[55] Ibid.

1.3.3 Response

Objective	Develop the steps required to respond effectively, appropriately, and in a timely manner should a crisis occur. [56]
Tasks	Potential crisis recognition, notify the team, assess the situation, declare a crisis, execute the plan, communications, resource management.

The first element in a response programme is to determine if a potential crisis exists. There are four elements that indicate the presence of a crisis situation[57]:

1. Missing or uncertain information
2. Little time to respond
3. A threat to people or resources valuable to people
4. The resources required to resolve the situation exceed the resources available.

These four factors illustrate differences in the level of crisis. The first element can be considered as a problem situation rather than a crisis if there is significant time to respond. However, if there is little or minimal time to respond to missing or uncertain information or there is a possible threat to people or resources valuable to people then that could be considered as a critical problem. A real-crisis situation, however, has a fourth factor added - the situation seems likely to overwhelm those involved. Put specifically, a crisis is a critical problem that has a demand for resources that exceeds the resources available[58].

In many cases there is a signal or indication that a crisis might occur in the near future. If these signals can be picked up and acted upon, then many crises can be prevented before they ever happen. For this reason every organization has to ask itself: "What would count as a signal for an impending or near occurrence of a particular type of crisis?[59]" For example, even an increasing amount of graffiti scribbled on the walls of toilets or an increase in the number of bad jokes that are passed around the organization may be signals of impending employee unrest and sabotage[60].

[56] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[57] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 47.
[58] Ibid.
[59] Ian I. Mitroff (2001). Managing Crisis before they Happen: What every Executive and Manager Needs to Know about Crisis Management, p. 107.
[60] Ibid.

There are four common types of signals that apply to every organization[61]:

- Internal technical signals
- Internal people signals
- External technical signals
- External people signals

It is advisable that an organization has trained personnel assigned to observe warning signs. Nevertheless, the responsibility to report a potential crisis should be communicated to all employees. Achieving this goal is often difficult as employees might not feel responsible or might not take a signal seriously. One possibility for tackling this is to introduce a documented reporting structure, where attention is paid to what the employees report.

When a potential signal for a crisis is recognized the right people should be contacted. It is important that every employee knows how to reach the crisis management team and that the signal reported is in the right form, so that the team can respond quickly and effectively. Once the team is contacted it should know how to respond to the signal. This in turn requires that it has a well-defined reporting and procedure sequence. Even if a signal relates to a known problem in an organization, there must still be a clear reporting sequence[62]. The qualified personnel should have ready access to updated, confidential listings of persons and organizations to be contacted when certain conditions or parameters of a potential crisis are met[63]. It is also important to have redundancies built into the notification system and several different ways to contact the listed individuals and organizations since some types of crises or disasters could impact the notification system directly[64]. Once the team has decided that the situation might escalate into a crisis, an assessment of the reported situation should be made immediately. This is usually done by means of a problem assessment and a severity assessment. A problem assessment is an evaluative process of decision making that determines the nature of the issue to be addressed, while the severity assessment is the process of determining the severity of the crisis and what any associated costs may be in the long run[65]. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation[66].

When a crisis situation emerges, the individuals trying to resolve or contain it before significant damage occurs are likely to be different from those handling the impact damage. In practice, this may mean that on-site organization personnel give way to off-site personnel

[61] Ibid.
[62] Ian I. Mitroff (2001). Managing Crises before they Happen: What every Executive and Manager Needs to Know about Crisis Management, p. 110.
[63] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[64] Ibid.
[65] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[66] Ibid.

from police, fire fighters, and paramedic organizations[67]. In other situations on-site personnel may try to contain the crisis until more specialized trouble-shooters arrive and take over[68].

The following are some of the activities that should be included if a crisis situation occurs[69]:

- Additional call notification
- Evacuation, shelter, or relocation
- Safety protocol
- Response site and alternate site activation
- Team deployment
- Personal assignments accessibilities
- Emergency contract activation
- Operational changes

1.3.3.1 Execute Plan

It is essential to have an updated BCP in order for it to be successfully executed. Updates should be made regularly to ensure that any changes to the organization are reflected accurately and promptly. One way of making sure that the plan is updated is to schedule regular updates to distributed copies and at the same time to have on-site and off-site copies (both in hard and soft copy form) that incorporate all changes as they are made[70].

When developing a BCP a wide range of disaster and crisis scenarios should be considered. It is recommended that the plan is developed around a "worst case scenario" with the understanding that the response can be scaled appropriately to match the actual crisis[71]. This will provide management with the basis upon which to assess the risks and their likely impacts should an incident or disaster occur[72].

[67] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 46.
[68] Ibid.
[69] [69] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[70] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 38.
[71] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[72] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 36.

Also, when initiating a response it is important to ensure that the goals protect the following interests listed in order of priority:[73]

- Save lives and reduce chances of further injuries/deaths
- Protect assets
- Restore critical business processes and systems
- Reduce the length of the interruption of business
- Limit reputation damage
- Control media coverage
- Maintain customer relations

These prioritized classifications can be used as indicators of the magnitude of the crisis or disaster[74]:

Level 1	**Level 2**	**Level 3**	**Level 4**
Routine emergency incidents	Minor business interruption • No casualties • Minimal damage • Limited impact on customer service • No community impact • Local media only	Moderate business interruption • Several injuries or deaths • Moderate damage • Some impact on customer service • Moderate community impact • National media	Major business interruption • Major impact on all areas

Determining the initial level of the crisis and its progression from one level to the next will normally be the responsibility of the crisis management team[75].

[73] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 17.
[74] Ibid.
[75] Ibid.

1.3.3.2 Communications

Once a disaster occurs, effective communication is one of the most important factors in crisis management. Therefore, pre-planning for communications is critical[76]. Drafts of message templates, scripts, and statements can be developed in advance for threats identified in the risk assessment.

Employees who are directly involved in the disaster should be contacted immediately and management has to make sure that each employee is trained and is able to follow the evacuation instructions. Employees not directly involved as well as external groups should be contacted as soon as the conditions of the disaster make it possible. In order to provide the best communications and suitable messages for various groups, it is often appropriate to segment the audiences[77].

Internal	**External**
• Employees and their families • Business Owners/Partners • Boards of Directors • Contractors/Vendors	• Customer/Clients • Contractors/Vendors • Media • Government and Regulatory Agencies • Local law enforcement bodies • Emergency responders • Investors/Shareholders • Surrounding Communities

One of the major concerns for any business is the perceived impact of the disaster on customers and suppliers. This is initially addressed during the emergency when decisions are made about the content of press releases, and what customer services are going to communicate to external audiences. This is not to imply that the organization should give false statements and mislead customers about the seriousness of the emergency, or about the impact of the emergency on customers[78]. Rather, it should be used as an opportunity to inform customers and suppliers about how their requirements are going to be met. In most cases large organizations will have a trained official spokesperson who will manage crisis communications to the media and others. In that case it should be stressed that personnel are

[76] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 20.
[77] Ibid.
[78] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 186.

informed quickly regarding where to refer calls from the media and that only authorized spokespeople should deal with the media[79].

The following factors should be considered when contacting internal and external audiences[80]:

- Communication should be timely and honest.
- To the extent possible, an audience should hear news from the organization first.
- Communications should provide objective and subjective assessments.
- All employees should be informed at approximately the same time.
- All bad news should be given at once.
- If possible, an opportunity should be provided for the audience to ask questions. Regular updates should be provided, and the audience should know when the next update will be issued.
- The communication should be done in a manner appropriate to the circumstance. This could be face-to-face meetings, news conferences, telephone calls, and/or through e-mail, internet sites and local/national media.

1.3.3.3 Resource Management

Staff members and other stakeholders who could include customers, creditors, suppliers, product users, shareholders, owners, and government regulatory agencies[81]; that in one way or the other are involved in generating business and wealth for the organization can be considered crucial to the organization and are therefore a very important part of any BCP. If an organization wishes to have positive and effective crisis management[82] each of these groups needs careful management during response and recovery periods. Therefore it is essential to put stakeholders up front and to make sure they are aware of the crisis/disaster situation that the organization is facing. An important part of BCP is also to maintain a functional payroll system throughout the crisis. In most cases this will ensure that most stakeholders stay with the organization.

In the event of injuries and fatalities, arrangements should be made for quick notification of the next-of-kin. If possible this should be done by a member of senior management and financial support should be offered to the families of victims. It is also very advisable that in cases of severe injury or death, the organization implements a family representative programme. These representatives should have comprehensive training that provides the knowledge appropriate for dealing with people who will be receiving bad news, and may

[79] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 20.
[80] Ibid.
[81] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 52.
[82] Ibid.

therefore act in all kinds of ways from breakdowns to panic attacks. Such representatives should also act as the primary point of contact between the family and the organization.

The organization should also offer crisis counselling for its stakeholders. This should help those directly involved to recover from the shock and also improve the organization's image.

1.3.3.4 Logistics

Logistics is a very important part of the BCP, and is also a part of strategic planning since logistical decisions made in advance will have a considerable bearing on how successful the BCP will be. Some logistical issues worth considering include:

- **Alternative sites**

  Alternative worksites should be identified and selected early in the BCP process for business resumption and recovery. It is possible to select a commercial disaster recovery service supplier or spare in-company accommodation. Alternative worksites should provide adequate access to the resources required for business resumption identified in the BIA[83]. Depending on the required recovery timeframe, the alternative site may be:

  - **A Cold site**

    Cold sites are locations that are part of a long term recovery strategy as they provide an environment in which a new facility can be built from scratch. In most cases this means that the site will provide a backup location without equipment but with the most important assets such as electricity, heating, and network and telephone wiring. While cold sites represent a low cost solution, they typically can take up to several weeks to activate[84]. Therefore, this type of facility is usually not considered an adequate primary recovery option because of the time it takes to start production and resume operations.

  - **A Hot site**

    A hot site is fully configured with compatible equipment; typically it can be operational within several hours as it will be necessary to install systems, applications and data. This means that it provides a duplicate facility in another location, with capacity to absorb the additional workload before its absence becomes critical to business survival[85].

[83] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 22.
[84] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. G-10.
[85] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 5 197.

- **A Warm site**

  Warm sites are somewhere between hot and cold sites. They will provide the basic infrastructure to enable the facility to be reinstated before its absence becomes critical to business survival[86]. This means that they will be fully equipped apart from items that can be supplied quickly from stocks. This recovery option is less costly and requires fewer resources to maintain than a hot site. This alternative is very acceptable if critical transaction processes are not required.

In case of a disaster, an organization will most probably have a hot or warm site so that it can continue operating the main processes shortly or instantly depending on its needs. If the operation centre takes long to be rebuilt the cold site can be activated and equipped so that the resumption of operations can take place at the site.

Another logistical factor to be considered is transportation. Transportation at a time of crisis can be challenging and therefore provision should be arranged ahead of time, if possible. Areas where transportation is critical include, but are not limited to[87]:

- Evacuation of personnel (e.g. from a demolished worksite or from a satellite facility in another country)
- Transportation to an alternate worksite
- Supplies into the site or an alternate site
- Transportation of critical data to worksite
- Transportation for staff with special needs

1.3.3.5 Insurance

Having insurance is an important component of the business continuity process. This should not be seen as a substitute for a BCP, although it may allow management to recover losses that cannot be completely prevented and expenses related to recovery from a disaster. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet represent a potential for financial loss or other disastrous consequences[88]. While the decision to obtain insurance is based on several factors, one consideration should be the probability and degree of loss identified during the BIA[89].

One problem about insurance is that the funds are not necessarily paid out immediately; in some cases costs may take years to be refunded. It will also only pay for what is covered under the policy, and therefore it is very important to establish policy parameters in advance

[86] Ibid.
[87] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 23.
[88] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 33.
[89] Ibid.

which have been approved by the insurance provider. Insurance companies will also only pay for the lost profit and extra costs that arise for a specific time period, typically 6 – 12 months after the disaster[90]. Another problem is that in order to make an effective claim the organization has to prove loss. This usually involves producing records and inventories of equipment, stock, software, and data[91]. However, if a disaster happens while a new product or service is being launched it may be difficult or impossible to prove what the profit from it would have been.

Although appropriate insurance of assets, working costs and profits does provide a lifeline and should be a part of a BCP, an organization should always keep in mind that insurance by itself will not supply customers, nor will it guarantee recovery of market shares.

[90] Andrew Hiles & Peter Barnes (2001). The Definitive Handbook of Business Continuity Management, p. 5 199.
[91] Ibid.

1.3.4 Recovery/Resumption

Objective	Develop policies, procedures and plans to bring the organization out of the crisis, recover/resume critical processes, and finally return to normal operations[92].
Tasks	Damage and impact assessment, resumption of critical and remaining processes, return to normal operations.

1.3.4.1 Damage and Impact Assessment

The two types of damage an organization needs to assess after a disaster are physical and non-physical. The damage will be assessed either by the crisis management team or by a designated damage assessment team. In most cases where the company's property has been damaged the crisis management team will gain permission to enter the facility as soon as it is declared safe by the relevant public safety authority. The team will interact with other physical plant operations groups, the police, and those having information systems and operational functions including vendor and insurance representatives, to keep abreast of new equipment, physical structures and other factors essential for recovery[93]. The team then reports directly to the business continuity management team, evaluates the initial status of the damaged functional area, and estimates the time to reoccupy the facility and the ability to salvage the remaining equipment.

Non-physical damages are those that do not involve immediate physical damage to a company's worksite or facility. They include the business, human, information technology, and societal types of crises[94]. These types of crises will likely impact the organization in the long term. For example, if customer data are lost and there is no backup the organization might lose clients because it does not fulfil its commitments. Another example would be if there is a terrorist attack in the country and the staff members were exposed to the danger, they might be traumatized and not perform as well as they should.

Once the extent of damage is known, the critical processes identified and prioritized in the BIA should be used to guide scheduling of the resumption of processes. If damage occurred which had not been identified in the BIA it should be prioritized, documented and included in the schedule. Decisions regarding prioritization of processes should also be documented and recorded, including the date, time and justification for the decision[95].

Once it has been decided which critical processes are to be restored first, the resumption of work can begin according to the prioritized schedule, and depending on the circumstances of

[92] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 24.
[93] http://web.mit.edu/security/www/pubplan.htm [Accessed 21.10.2009].
[94] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 24.
[95] Ibid.

the crisis, the processes may be restarted either at the current worksite or at an alternative site. After the critical processes have resumed the organization should start to carry on the remaining processes.

When all processes have resumed, the organization should bring the company “back to normal”. If that is not possible a new “normal” state should be defined, whereby the productive work of the organization is set back to “normality” although restructuring may still be occurring in the workplace.

1.3.5 Testing, Training and Maintenance

Objective	Train and educate team members, validate and enhance the BCP.[96] Keep the BCP relevant to the organization using a rigorous maintenance and evaluation programme.[97]
Tasks	Educate and train personnel, test the BCP, conduct BCP review, develop BCP maintenance schedule.

Testing, training and maintenance are the final steps of a cyclical BCP process. In order to be able to execute a BCP as efficiently as possible in different crisis situations, it is necessary to train the crisis management team, the response team, as well as the general employee population. Managers responsible for the BCP have to be aware that a plan is only as good as the performance of the participants. Although it is not very common for the general employee population to be trained, it is very important to do so because if a crisis occurs employees will respond better and panic less if they know how to respond. Therefore it is important that trainers (first line level of management) brief all personnel on the key components of a BCP as well as the response plans that affect them directly. In most cases such training should include procedures for evacuation, information about shelters in place, check-in processes to account for employees, arrangements and alternative worksites, and the handling of media inquiries by the company[98].

The crisis management response teams will require a higher degree of training which will also include educating them about their responsibilities and duties. One way of making sure that the team knows how to respond is by developing a check list of critical actions that have to be undertaken.

1.3.5.1 Testing

The main advantages of testing are that it keeps teams and employees effective in their duties, clarifies their roles, and reveals weaknesses in the BCP that should be corrected[99].

The key challenge for management is therefore to develop a testing programme that provides a high degree of assurance for the continuity of critical business processes, including supporting infrastructure, systems and applications, without compromising production environments[100]. A good testing programme will have a testing policy that includes test strategies and test planning. This testing policy should be established by the Board and senior

[96] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 26.
[97] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 31.
[98] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 26.
[99] Ibid.
[100] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 18.

management and should set expectations, goals and responsibilities for business lines and support functions that have to be followed when implementing testing strategies and test plans[101]. An obvious goal is to determine whether a certain risk response works and how it can be improved. Other less obvious goals can be to test capacity (as in the case of a call in or call out phone system), to reduce the time necessary to accomplish a process (e.g. by using repeated drills to shorten response times, and to bring awareness and knowledge to the general employee population about the BCP).

The policy should also establish a testing cycle that increases in scope and complexity over time. This means that the tests should start out simple (checklists, simple exercises and small components of the BCP), and become increasingly complex (up to full scale activation of the entire BCP, including involvement of external participants involved in public safety and emergency response) as the process evolves.

Once the organization has developed its testing policy, it will typically be implemented by developing testing strategies and test planning.

Test strategies should include the scope and objectives of testing, defining clearly what functions, systems, or processes are going to be tested and what constitutes a successful test[102]. Strategies should also include the following:[103]

- Expectations from business lines (these include all internal and external supporting functions, such as IT and facility management) and support functions to demonstrate the achievement of business continuity test objectives consistent with the BIA and risk assessment.
- A description of the depth and breadth of testing to be accomplished.
- The involvement of staff, technology, and facilities.
- Expectations for testing internal and external interdependencies. An evaluation of the reasonableness of assumptions used in developing the testing strategies.

Once the test strategies are defined, a test plan should be developed based on the predefined testing scope and objectives established as part of management's testing strategy. It is important that the plan contains different types of testing scenarios as well as different methods of testing. Scenarios should include a variety of threats, event types, and crisis management situations which have been identified in the risk assessment.

Testing methods can vary from simple to complex and should include both business and disaster recovery exercises. Business recovery exercises focus on testing business line operations while disaster recovery focuses on testing the continuity of technological components, including systems, networks, applications, and data. It is recommended that business functions that are more vulnerable and more likely to be exposed to some kind of

[101] Ibid.
[102] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 20.
[103] Ibid.

disaster/event undergo a comprehensive testing method where greater frequency of testing is used. While comprehensive tests do require greater investments of time, resources, and coordination to implement, these will more accurately depict a true disaster and thereby better assist management in assessing the actual responsiveness of the individuals involved in the recovery process[104]. Some of the possible testing methods which can be used are:

- **Tabletop Exercise/Structured Walk Through Test**

  This type of exercise is designed to test the ability of a group to respond in an emergency situation, its primary objective being to ensure that the personnel know how to act in certain crisis situations. A walk through of a crisis scenario will identify whether the personnel and all managers with roles in the plan understand their responsibilities as well as what is expected of them. Once the walk through is complete, any findings should be presented in a report and the plan amended if necessary.

- **Functional Drill/ Parallel Test**

  This test involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set out in the BCP[105]. The goal is to determine whether critical systems can be recovered at the alternate processing site and if employees can actually implement the procedures defined in the BCP[106].

- **Full Interruption/Full Scale Test**

  This involves simulating a real-life emergency as closely as possible, the aim being to try to activate and thoroughly test all components of the disaster recovery plan at the same time. This includes: hardware, software, staff, communications, utilities, and alternate site. The exercise should involve the business line end users and the IT group to ensure that each business line tests its key applications and is prepared to recover and resume its business operations in the event of an emergency[107]. The full test verifies that systems and staff can recover and resume business within established recovery time objectives.

After completion, the tests should be evaluated to ensure that their objectives are achieved and that the business continuity successes, failures, and lessons learned are thoroughly analysed. If the test objectives are not achieved, management should undertake the necessary corrective measures and determine whether it is necessary to modify the BCP or conduct another test before the next regularly scheduled exercise.

[104] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 23.
[105] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program/testing-policy.aspx [Accessed 16.12.2009].
[106] Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook, p. 24.
[107] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program/testing-policy.aspx [Accessed 16.12.2009].

1.3.5.2 Maintenance

The plans and strategies that are implemented reflect the requirements of the business at the time. However, in any dynamic organization these requirements may change over time and accordingly plans and strategies must evolve. Therefore the main function of maintenance is to reflect changes in the operation which include procedures, systems or processes of the organization that will affect the BCP. Examples of changes which may affect the plan include[108]:

- System and application software changes
- Changes to the organization and its business processes
- Personnel changes (employee and contractors)
- Supplier changes
- Critical lessons learned from testing
- Issues discovered during actual implementation of the plan in crisis
- Changes to external environment (new business in area, new roads or changes to traffic patterns)
- Other items noted during review of the plan and identified during the risk assessment

Another important function of maintenance is to have a regular BCP review which should take place according to a pre-determined schedule. However, if changes such as those listed above occur, the BCP should be modified immediately.

[108] ASIS (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, p. 32.

Chapter 2: Soft Systems Methodology

2.1 Systems Thinking and Models

Systems thinking has its foundation in the field of system dynamics, founded in 1956 by Professor Jay Forrester of the Massachusetts Institute of Technology. Professor Forrester recognized the need for a better way of testing new ideas about social systems, in the same way as we can test ideas in engineering[109].

Systems thinking is any process for estimating or inferring how local policies, actions, or changes influence the state of the neighbouring universe[110]. It is an approach to problem solving that views "problems" as parts of an overall system, rather than reacting to present outcomes or events and potentially contributing to further development of the undesired issue or problem[111]. Systems thinking is a framework that is based on the belief that the component parts of a system can best be understood in the context of relationships with each other and with other systems, rather than in isolation. The only way to understand fully why a problem or element occurs and persists is to understand the part in relation to the whole, and to realize that the system is only as good as its parts. For example, a motorcycle can be seen as a system and that it is only as good as the parts of which it is made. If, for example, the motorcycle would be missing a tyre, this would have a great impact on the person trying to ride the motorcycle.[112]

Another good example would be the braking system of a car. If we were to try to improve the braking abilities of the car by only looking into great detail at the brake pads such as their size, material composition etc., many things which affect the system and thereby affect how quickly the car will stop would be missed. By expanding our boundaries and looking at braking as a system it becomes clear that braking involves the interaction between brake discs/drums, brake pedal sensors, hydraulics, tyres, driver reaction time, road conditions, weather conditions and possibly others[113].

[109] http://www.oppapers.com/essays/System-Thinking-Example/151847.
[110] http://en.wikipedia.org/wiki/Systems_thinking.
[111] O'Connor, J. & McDermott, I. (1997). The Art of Systems Thinking: Essential Skills for Creativity and Problem-Solving, p. 11. Thorsons Publishing.
[112] Capra, F. (1996). The Web of Life: A New Scientific Understanding of Living Systems, p. 30. Anchor Books.
[113] http://en.wikipedia.org/wiki/Systems_thinking.

2.1.1 Types of Systems Thinking

To obtain a broader understanding of the field, exactly what is meant by the word "system" has to be understood.

A "system" is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs and which together, accomplish the overall desired goal for the system[114]. So a system is usually made up of many smaller systems, or subsystems. For example, an organization is made up of many administrative and management functions, products, services, groups and individuals. If one part of the system is changed, the nature of the overall system is often changed[115].

Systems thinking on the other hand, is a way of helping a person to view systems from a broad perspective that includes seeing overall structures, patterns and cycles, rather than seeing only specific events[116]. Taking this broad view can help to identify the real causes of issues in organizations and know just where to work to address them. In other words, systems thinking differs from traditional forms of analysis because it focuses on how the pieces studied interact with the other constituents of the system rather than, as is the case with traditional forms of analysis, by separating the individual pieces that are studied. The result is often very different from that obtained through traditional forms of analysis, especially when studying dynamically complex issues or when what is studied involves much feedback from internal and external sources.

By focusing on the entire system, one can attempt to identify solutions that address as many problems as possible in the system. The positive effect of those solutions leverages improvement throughout the system. Thus, they are called "leverage points" in the system. Putting priority on the entire system and its leverage points is called whole systems thinking[117].

In general, systems and the application of systems thinking can be grouped into three categories based on the techniques used to tackle a system[118]:

Hard systems: These involve simulations often with computers and the technique of operations research. This approach is very useful for dealing with problems that can be quantified but has great problems in taking into account unquantifiable variables such as opinions, culture and politics and does not take into account the fact that people can be influenced by rather complex motivation factors[119].

[114] http://managementhelp.org/systems/systems.htm.
[115] http://managementhelp.org/systems/systems.htm.
[116] http://www.managementhelp.org/misc/defn-systemsthinking.pdf.
[117] http://www.managementhelp.org/misc/defn-systemsthinking.pdf.
[118] http://en.wikipedia.org/wiki/Systems_thinking.
[119] http://www.business.mmu.ac.uk/mascla/resources/systemsthinking.php.

Soft Systems: These were developed to deal with problems which could not be tackled easily with hard systems, i.e. problems that cannot easily be quantified. Soft systems are useful for understanding motivations, viewpoints and interactions and for addressing both qualitative and quantitative dimensions of a situation[120].

Evolutionary Systems: These were developed for designing complex social systems. Similar to dynamic systems, evolutionary systems are open, complex systems but with the capacity to evolve over time[121].

2.1.2 System Models

When making system models it is important to be aware that they are always constructed from a world view, they all express one way of looking at and/or thinking about a specific situation, and there will always be multiple possibilities for doing so.[122]

Since it is impossible to construct a view which includes everybody, the models should be seen as intellectual devices that can be used as the basis to ask questions about a real situation and thus for exploring that situation[123]. For example, one question could be how the activity in the real world differs from the modelled, and if we would like the real world to be more like the one in the model or *vice versa*. This type of question is an incubator for further structured questions and discussions about the real situation and thus for enabling different views to surface and be explored through discussions for trying to improve the situation at hand. Such discussions will help to find a version of the situation with which people with different views can live.[124] This situation must meet two criteria[125]:

1. It has to be arguably desirable given the outcome of the models used.
2. It must be culturally feasible with the unique situation, unique people, unique history and unique narrative that the participants have constructed over time to make use of their experiences.

[120] http://www.business.mmu.ac.uk/mascla/resources/approaches.php.
[121] http://www.isss.org/primer/evolve2.htm.
[122] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 10-11.
[123] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 11.
[124] Ibid.
[125] Ibid.

2.2 Summary

Systems thinking is extremely effective for solving the most difficult problems surrounding complex issues, i.e. those that depend a great deal on the past or on the actions of others, and those stemming from ineffective coordination among those involved. Some of the main characteristics of systems thinking include[126]:

1. Changing individual perspectives on an issue or problem. This leads to changes in attitude and approach, making it easier to identify the social components required to "solve" complex situations.
2. Holistic thinking. This avoids losing the issues which are intimately associated with the inter-connections of the situation.
3. Simplifying by making more abstract. Some simplification is essential to make a problem tractable, but the simplification must not reduce the connectedness. By becoming more abstract, the connectedness is maintained and the problem simplified.
4. Using standard systems and diagrams. These are "tools of the trade", rather than "characteristics of systems thinking". They allow the other characteristics to be realized.

[126] http://openlearn.open.ac.uk/mod/resource/view.php?id=183684.

2.3 Soft Systems Methodology

Soft Systems Methodology (SSM) was developed by Peter Checkland. It is a qualitative technique used for applying systems thinking to non-systematic situations. SSM tries to contribute to finding solutions for practical problems in real world situations. These problems can be referred to as "soft problems" where the situation to be analysed is complex and where there are divergent views about the definition of the problem[127]. Checkland would probably object to the language used above since he does not agree with using words such as "solution" and "problem" when working with SSM. This is because the word "problem" suggests that there is one clearly defined problem, which there isn't, and also the word "solution" implies that SSM will fix the problem, which is impossible when referring to human systems and organizations.

Checkland refers to problems in the real world as "problematical" rather than a "problem situation". This is because, as mentioned above, in a problem situation there is a clearly defined problem to be solved whereas in a "problematical" situation there is not[128]. One example of a problematical situation is where a government is trying to define legislation to increase security on the streets for its citizens at a time of terrorist threats without diminishing civil liberties[129]. This could be solved by either coming up with random ideas, using emotions and previous experiences, or by using SSM.

2.3.1 Describing Problematic Situations

When interacting with real world situations people make their own judgments. To make these judgments different criteria are used to match the situation against[130]. These criteria differ from person to person. Therefore, any account of the problematic situation should be based on a specific perception (Weltanschauung or world view). For example, an environmentalist could judge a decision to act upon a given situation "good" if it is an environmentally friendly decision[131]. The same situation could be seen as "bad" from the standpoint of a capitalist because the decision would not be economically profitable[132]. There are many reasons for the environmentalist and the capitalist to have completely different views on this matter. One possibility is that they grew up in completely different environments and had different lifestyles. Obviously many other factors could be included such us the culture one was brought up in, genetic inheritance, experiences from the world so far, etc. These factors and the result they produce build up to a personal world view over time. These world views cause people to become what they are. Therefore one person for example would see Che

[127] http://en.wikipedia.org/wiki/Soft_systems_methodology.
[128] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 3.
[129] Olle L. Bjerke (2008). University of Gothenburg; Soft Systems Methodology in Action: A Case Study at a Purchasing Department, p. 22.
[130] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 5-6.
[131] Olle L. Bjerke (2008). University of Gothenburg; Soft Systems Methodology in Action: A Case Study at a Purchasing Department, p. 22.
[132] Ibid.

Guevara as a freedom fighter while someone else might see him as a terrorist[133]. These views can also change over time, for example an emotionally cold person could be more compassionate after experiencing love[134].

A flexible approach is necessary to deal with these kinds of situations because every situation involving humans is unique. To meet this reality it is better to use a methodology than a method since the former uses a set of principles that can be adapted for use in ways that best suit the nature of the situation at hand.[135]. SSM is a flexible and therefore a possible approach for dealing with the situations described above.

[133] http://en.wikipedia.org/wiki/Che_Guevara.
[134] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 6.
[135] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students, p. 6.

2.4 The SSM Process

Although Peter Checkland objects to the use of terms like problem situation, this term is used here because he did, in fact use it previously and in this thesis a problem will have to be solved at a later stage.

The classical SSM consists of seven stages and contains two kinds of activity. Real world activities involve people directly facing the problem situation whereas "systems thinking" activities may or may not involve those encountering the problem situation depending upon the individual circumstances of the study[136].

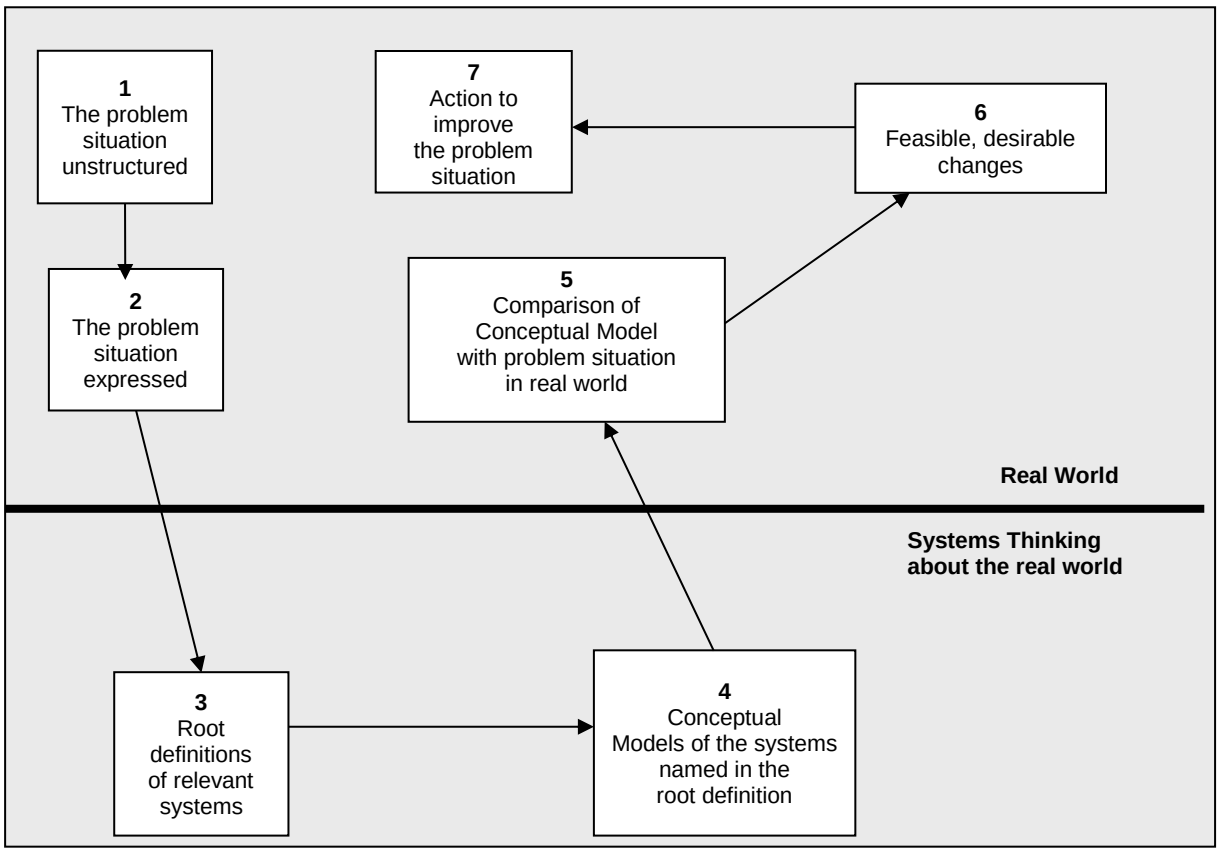

Figure 2: Summary of the Methodology (after Checkland, 1975)

Figure 2: Summary of the Methodology (after Checkland)

Figure 2 represents the chronological sequence and should be read from 1 to 7; this logical sequence is most suitable for describing the methodology but this does not have to be followed when applying[137]. According to Checkland, backtracking and iteration are essential when using the methodology which has proven to be most effective when used as a framework into which to place purposeful activity during a system study.

[136] Peter Checkland (1999). Soft System Methodology, a 30 year retrospective, p. 163.
[137] Peter Checkland (1999). Soft System Methodology, a 30 year retrospective, p. 162.

2.4.1 Stage 1. Explore the problem situation

The first two stages of the SSM model deal with problem expression in which an understanding of the problem situation should be developed. These stages will therefore be a mixture of textual description and high level models expressed in the form of rich pictures and mind maps.

A problem situation can be described broadly as "a situation in which there is perceived to be a mismatch between what might be, could be, or should be[138]. In order to analyse this as effectively as possible, a considerable amount of information should be gathered. Information such as: organizational history, culture, structure, number of stakeholders, their perspectives and assumptions, and questions such as[139]: "Is there a problem?" "What does the system do?" "How does it work?" "What are the processes involved?" should be used.

The purpose of this analysis is to collect as many perceptions of the problem as possible from a wide range of people with roles in the problem situation, and by a determination not to present the analysis in systems terms at all[140]. This means that the main purpose is not to come to a definition of the problem but to get an idea of the parameters and structure of the problem situation so that a range of possible and relevant choices can be suggested.

2.4.2 Stage 2. Express the problem situation

In this stage the problem situation needs to be expressed, ideally with the active participation of the stakeholders where a rich picture is developed to construct a diagrammatic representation of the problem domain. This picture should depict the structure and processes of the organization and the environment in which it operates, as well as soft information (i.e. subjective interpretations of situations, including aspects of conflict and emotions).[141] By structure is meant the physical layout, hierarchy, reporting structure, and the patterns of both formal and informal communication. By process is meant the organization's basic activities (i.e. resource allocation, deployment, monitoring, and control). The relation between structure and process should illustrate the problems, tasks, and elements of the environment in ways that are easy to understand.

In order to make rich pictures that work towards developing an improved problem situation, the practitioner needs to gather as much information as possible through situation interviews while at the same time having a mind-set that "prompts" to ensure that a wide range of aspects are taken into account[142]. Also, Checkland (1981) emphasizes the importance of bearing in mind that however rich the picture is, it could be richer and that rich pictures are

[138] Peter Checkland (1981). System Thinking, System Practice.
[139] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 295.
[140] Peter Checkland (1981). Soft System Methodology, a 30 year retrospective, p. 165.
[141] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 296.
[142] Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems. Methodology and its use for Practitioners, Teachers and Students, p. 24.

snapshots of a situation that will not remain static for very long. Wise practitioners therefore use rich pictures to capture impressions and insights continually and thereby as an aid to thinking[143].

2.4.3 Stage 3. Root definition of relevant systems in the problem situation

Stage three moves out of the "real" world and into the world of systems. Generally, this is considered to be the most difficult part of the process where the idea is to figure out what the system does rather than how it does it.

Initially, the following questions should be answered in order to be able to write a root definition statement:

1. How?
2. What?
3. Why?

These three questions can be used for every root definition made. This is known as the PQR formula in SSM, namely, do P (How?), by Q (What?), in order to achieve R (Why?).

To ensure that the root definitions are completed, Checkland developed the acronym "CATWOE"[144] to assist the memory.

Customers	Those who benefit in some form from the system.
Actors	The people involved, the ones who do the activities.
Transformation	The development from inputs to outputs.
Weltanschauung	The "world view", a holistic overview of both the transformation processes and the problem situation.
Owner	The person in control.
Environmental Constraints	Physical boundaries, political, economic, ethical, or legal issues.

A root definition is a statement defining what is relevant to the system and who is either affected by it or could affect it[145], and it describes the core transformation activities and processes of the system – the conversion of inputs to outputs[146]. Inputs can be concrete or

[143]Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems. Methodology and its use for Practitioners, Teachers and Students, p. 27.
[144] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 296.
[145] Milton E. Lopez (2001). Soft Systems Methodology an Application to a Community based Association, Proceedings Fielding Graduate Institute Action Research Symposium, p. 3.
[146] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 296.

abstract, logical or physical but they cannot be a mixture of expressions. Hence, a concrete input must yield a concrete output, an abstract input must yield an abstract output.

When defining the root definitions it is possible that more than one root definition is formulated as each individual expresses a different perspective of the organization's purpose. It therefore serves to acknowledge that there are conflicts and problems between (for instance) actors, owners and clients of a system.

2.4.4 Stage 4. Making and Testing Conceptual Models

Once the root definitions have been constructed, compared with the rich picture and checked against CATWOE, conceptual models can be developed[147]. Conceptual models are formed from the actions stated or implied in the root definition[148]. Any root definition may be looked at as a description of a set of purposeful human activities conceived as a transformation process. The definition is an account of what the system is; the conceptual model is an account of the activities which the system must do in order to be the system named in the definition[149]. It should be noted that when completed, the resulting model is in no sense a description of any part of the real world; it is simply the structured set of activities which are required to potentially achieve the goal stated in the root definition. When the conceptual model is being constructed one should try to avoid it becoming a description of the real world because that would negate the whole purpose of the approach – namely, to generate radical thought by selecting some views of a problem situation that are possibly relevant to improving it, working out the implications of those views in conceptual models and comparing those models with what exists in the real world situation[150].

The step of moving from root definition to conceptual model is the most rigorous in the whole methodology, the nearest to being a "technique". However it is not quite a technique, in the sense that a technique is a procedure which, when applied properly, will produce a guaranteed result. This is shown by the fact there are always arguable issues about whether one person's model is as adequate a representation of a root definition as another's.

There are many ways to begin constructing a conceptual model; however Checkland recommends the following process:

1. Start by writing down no more than about half a dozen verbs which cover the main activities implied in the root definition.

2. Select activities that are not dependent on each other.

3. Place these activities in a line, and then those that are dependent on these first activities in another line; continue the process until all are accounted for.

[147] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing information and communication systems, p. 298.
[148] Ibid.
[149] Peter Checkland (1981). Soft Systems Methodology, a 30 year retrospective, p. 169.
[150] Peter Checkland (1981). Soft Systems Methodology, a 30 year retrospective, p. 170.

4. Indicate the independencies between the activities.

6. Finally check whether the model demonstrates the following systems properties:

    - An on-going purpose (that may be determined in advance or assigned through observation)
    - A means of assessing performance
    - A decision making process
    - Components that are also systems (i.e. the notion of sub systems)
    - Components that interact
    - An environment (with which the system may or may not interact)
    - A boundary between the system and the environment (that may be closed or open)
    - Resources
    - Continuity

2.4.5 Stage 5. Comparing Conceptual Models with Reality

The Conceptual Model(s) constructed in stage 4 provides structure for a meaningful and coherent debate about the problem situation. It brings a wide range of questions to the surface, and also highlights the differences between the actual situation and perceived reality. It is also a matter of judgment as to when to stop conceptual model building and move on to a real world comparison between what exists and what is in, or is suggested by, the models of systems thought to be relevant to the problem[151].

The reason for it being called the comparison stage is because the conceptual model(s) are checked against both the root definition(s) and the rich picture[152]. Checkland suggests four possible ways of doing the comparison between conceptual model(s) and reality:

1. Informal discussion.
2. Structured questioning of the model(s) using a matrix approach.
3. Scenario writing based on operating the model. This means reconstructing a sequence of events in the past and comparing what had happened in producing it with what would have happened if the relevant conceptual model(s) had actually been implemented.
4. Trying to model the real world using the same structure as the conceptual model(s).

[151] Peter Checkland (1981). Soft Systems Methodology, a 30 year retrospective, p.176.
[152] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 298.

All four methods help to ensure that the comparison stage is conscious, coherent and defensible. In any particular study it may be useful to adopt any one of them or to carry out several comparisons using different methods[153]. However, the second method is the most common – often using a matrix that looks at the component of the model and asks:

- Does it exist in the real world?
- How does it behave?
- How is its performance identified and measured?
- Who does it?
- Why do it that way?
- Is this process any good?

It is very important to imagine that the conceptual model is actually operating in the real world. In this process a real process can then be identified from the rich picture, its sequence followed in the conceptual model and how the sequence would operate in reality compared.[154]

2.4.6 Stage 6. Determining desirable and feasible changes

At this point the methodology tends to stop being sequential and starts swinging back and forth through all seven stages in order to achieve the best results. On the basis of this analysis, possible changes are explored which are not only culturally and organizationally desirable but also economically and technologically feasible[155]. The discussion should be with people in the problem situation who care about the perceived problem and want to do something about it[156].

Checkland[157] describes three kinds of change: changes in structure, in procedures, and in attitudes. Structural changes refer to organizational groupings, reporting structures, or structures of functional responsibilities. Procedural changes include all the activities that go on within the organization, such as operational processes and reporting conventions. Changes in both these kinds are easy to specify and relatively easy to implement, at least by those having authority and influence. Once made, of course, such changes may bring about other effects which were not anticipated, but at least the act of implementation itself is a defined one and can be designed. This is not the case when referring to "attitude". Changes in attitude refer to changes in the expectations that people have of the behaviour of other actors as well as changes in their readiness to rate certain kinds of behaviour as bad or good relative to others. Such changes will occur steadily as a result of the shared experiences lived through by

[153] Peter Checkland (1981). Soft Systems Methodology, a 30 year retrospective, p. 179.
[154] Ibid.
[155] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 298.
[156] Peter Checkland (1981). Soft Systems Methodology, a 30 year retrospective, p. 180.
[157] Ibid.

people in human groups, and they will also be affected by deliberate changes made to structure and procedures[158]. In principle, it is possible to try to bring about changes of this third kind deliberately, although it is difficult in practice to achieve exactly the result desired.

2.4.7 Stage 7. Making changes to improve the situation

This is the implementation step, where the output from stage 6 is applied to the problem situation and may result in changes to procedures, policy, attitude, and technology[159]. In this last step decisions have to be made concerning:

- Who is to take action?
- What kinds of action should be taken?
- Where the action should be made?
- When the action should be made?

Therefore planning, timetables, resources and scope are very important in order to complete the last step successfully.

[158] Ibid.
[159] Steven M. Furnell, Sokratis Katsikas, Javier Lopez & Ahmed Patel (2008). Securing Information and Communication Systems, p. 298.

2.5 Conclusions

Soft systems methodology is only a recommendation for the process and the researcher needs not to hold to it rigorously. It offers backtracking and iteration processes when improvements are needed to the outputs from some of the stages. The work can be done simultaneously at variously detailed levels and points in time.

The following are some advantages and disadvantages of using SSM[160]:

Advantages

- It is a useful process when trying to determine a strategy for improving business processes.
- SSM stages can be used in any order that is appropriate.
- SSM is more useful in solving unstructured and poorly delineated systems where goals are not properly defined or are debatable.
- The methodology can be tailored to fit a particular situation.
- Customer values are not overshadowed by greater emphasis on technical, financial and other values.
- It aims at finding the best possible solution to benefit all those who are involved.

Disadvantages

- SSM does not actually inform about how to build a system.
- Problems are not structured but fuzzy and subject to change because people are involved; requirements emerge from discussion and bargaining processes.
- There is no way of telling whether an SSM project is a success or failure.
- SSM ignores issues of power; it is very unlikely that managers and workers will discuss their ideas openly.
- It includes non-technical issues (which can add complexity).
- It requires time, money and expertise.

[160] http://www.cs.stir.ac.uk/~jco/CSC9T4/special/CSC9T4_SSM_2006.pdf.

Chapter 3: Development of a Reference Model

3.1 Using SSM as a Basis for Risk Analysis

Risk analysis involves identifying the most probable threats to an organization and analysing the related vulnerabilities of the organization to these threats.[161] Risk assessment and business impact analysis (BIA) can be seen as part of the risk analysis process. Once the threats to an organization have been identified they will be assessed in risk assessment for the purposes of identifying their probability and severity. Once the organization is aware of the possible threats and their probability and severity it is possible for it to do a BIA. BIA involves identifying the critical business functions within the organization and determining the maximum acceptable downtime of crucial and other business functions.

Risk analysis can be either quantitative or qualitative. Quantitative risk analysis attempts to numerically determine the probability of a disastrous event happening and the likely extent of loss from that event. Qualitative risk analysis on the other hand, does not involve numerical probabilities or predictions of loss. Instead, it attempts to identify various threats, determine the extent of vulnerabilities to them and develop appropriate countermeasures. As mentioned in Chapter 2, SSM is a qualitative technique, and therefore the reference model employed for this thesis is based mainly on qualitative analysis.

3.2 Reference model development using SSM

This part of the thesis focuses on developing a reference model for BCP using SSM based mainly on risk analysis; however, other BCP topics are also covered and discussed. As every organization is unique and will have different demands and face different risks, the reference model developed should be used as a guideline and adapted to the needs of the individual organization. In other words, the questions, thoughts and descriptions made in the model described here should be considered with caution and adapted to the specific organization. The manner in which the reference model should be used will also depend on whether an organization has a BCP plan. If so, then the reference model can be used to revise the organization's current risk analysis. On the other hand, if the organization is planning to do a new risk analysis the reference model can be used as a guideline for such an analysis.

[161] http://www.drj.com/new2dr/w3_030.htm.

3.2.1 Explore problem situation

Each organization is exposed to certain types of risks which can be viewed as "problem situations". To identify these risks an organization should do a risk analysis. To discover if the organization has a problem the following questions should be asked:

1. Is the organization ready in case of an event that could jeopardize its success?
2. Does the organization have the necessary prevention strategies?
3. How will the organization respond in the case of such an event happening?
4. Will the organization be able to recover?
5. Is the organization's BCP up to date and are employees trained to implement it?

If any of these questions cannot be answered positively, then the organization is exposed to higher risk than necessary. Each of the five categories above can be viewed as a problem situation if answered negatively; however, focusing on all of them is outside the scope of this thesis, the main focus of which is on:

1. Is the organization ready in case of an event that could jeopardize its success?
2. Does the organization have the necessary prevention strategies?

Knowing the focus, it is possible to describe the problem situation that will be analysed:

"Is the organisation protected against the threats it might encounter?"

> ➔ *"Does the organization implement the necessary strategies in order to protect it against the most probable threats?"*
>
> ➔ *"Are all of the most probable threats covered?"*

For an organization to conduct an efficient risk analysis it will be necessary to look at the problem from a wide perspective. The first step is to know how many employees it has, how many stakeholders are involved and how much property it owns. The next step is to find out which departments and which processes are the most crucial, and what the maximum allowable downtime for these processes would be. The third step is to determine which parts of the organization are most vulnerable to what risk. For example, a branch of a bank will be most vulnerable to robbery, and therefore higher security measures against theft have to be considered in that sector. In other words, it is essential that management knows and understands the organisation in order for the necessary countermeasures to be developed against unwanted events. Knowing the history of an organization and unwanted events that jeopardized or disabled certain processes is very advantageous as these events can be analysed and mitigated or prevented in the future. The steps listed above should give management an indication of what exactly has to be protected.

In the event that an organization has already carried out a risk analysis, the description of the problem situation will stay the same but the focus will be more on reviewing the current risk analysis and identifying potential shortfalls.

The mind map in Figure 3 can be used as a guide to what an organization needs as input factors in order to do a risk analysis. The diagram also shows the common tools and techniques that are used to conduct the analysis and the outputs expected.

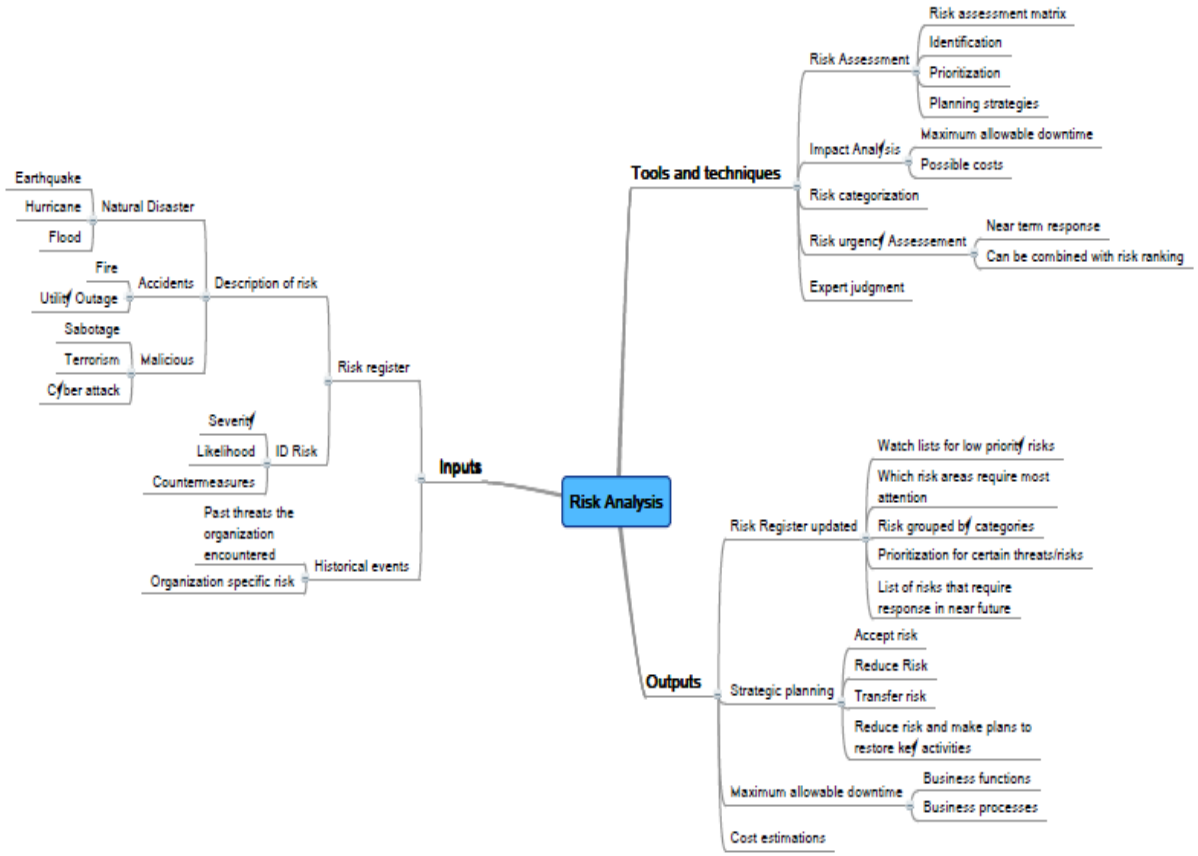

Figure 3: Mind Map for Risk Analysis

3.2.2 Problem situation expressed

Figure 4 illustrates a rich picture which not only involves the risk analysis but also points to many other considerations relevant to developing the BCP. When developing the mind map in Figure 3 the focus was strictly on risk analysis. The rich picture on the other hand ensures that a wider range of aspects are considered and therefore it also shows the stakeholders, structure, communication patterns, etc.

Figure 4 also provides a highly holistic insight into the stakeholders involved in an organization. While the main focus is on the organization itself, the perception of the outside world also has to be considered as it influences the business. The rich picture therefore also shows a common structure of an organization and the thoughts and issues that employees and other stakeholders might be facing when thinking about BCP.

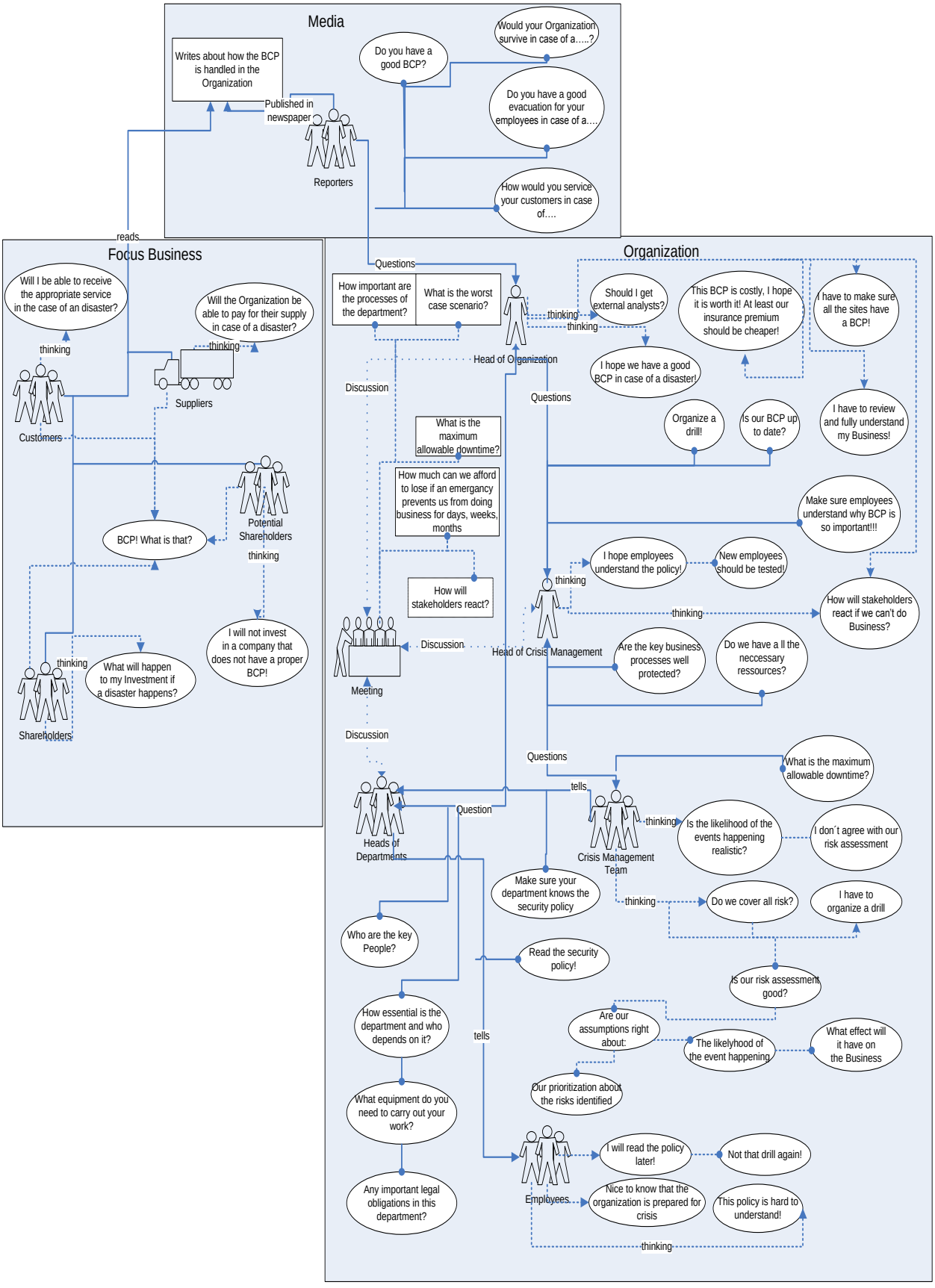

Figure 4: Rich Picture for Risk Analysis Including Elements from BCP Describing Possible Problem Domains

3.2.3 Root definition

The first thing to determine when starting the root definition is the PQR formula. This means that the first question will be:

*"**How** will the organization protect itself from unwanted events?"*

The second question is:

"***What** will the organization try to protect from unwanted events?"*

And the third question is:

"***Why** will the organization try to protect itself against unwanted events?"*

Answers:

How: By doing a risk analysis and identifying the various threats

What: Shareholders, customers, employees and core business

Why: To develop countermeasures against unwanted events, and to be able to continue its business in case of an unwanted event happening.

The next step is to do the CATWOE. As noted earlier, CATWOE is a method devised by Checkland to ensure that nothing is missed when defining the root definition. For this scenario however, the "Weltanschauung" is replaced with "Approach" because the whole methodology is devoted to risk analysis and it is important that this is made clear in the root definition.

Customers	Shareholders, customers, organization, employees
Actors	Employees, especially the crisis management team, Owner
Transformation	From "unprotected business" to protected business
Approach	Risk analysis. With risk analysis it is possible to identify various threats and determine the vulnerability of the organization to these
Owner	Organization head
Environmental Constraints	Budget, time, event estimation, legal issues

After completing the PQR formula and the CATAOE it is easy to formulate a root definition.

Root Definition:

"An organization should protect its shareholders, customers, employees and business by doing a risk analysis in order to both identify various threats and to determine the extent of vulnerability to these that the organization is facing. With the risk analysis completed, the organization will have the possibility to protect the business and its stakeholders by developing countermeasures for the threats identified".

3.2.4 Conceptual Model

Based upon the formulated root definition, a Conceptual Model was developed that represents the system described (Figure 5). This lays out the activities present within such a system as well as showing the logical relationships between these activities. The sentence in the root definition "*An organization should protect its shareholders, customers, employees and business by doing a risk analysis in order to both identify various threats and to determine the extent of vulnerability to these that the organization is facing"* relates directly to risk analysis. The sentence "*With the risk analysis completed the organization will have the possibility to protect the business and its stakeholders by developing countermeasures for the threats identified"* relates more to BCP since it involves more activities than covered by the risk analysis.

The Conceptual Model developed here is based on the BCP research undertaken in Chapter 1. Although some of the activities presented in the model are not connected directly to the root definition, they have logical relationships to the activity and are therefore presented in order for users of the reference model to have a better understanding of which other activities should follow once the risk analysis is completed. Another reason why this approach was chosen is because Checkland considers that the problem should be viewed as part of the system and not individually. In the present scenario the "system" would be BCP, and risk analysis would be only a component where the relationship to the other components has to be shown in order to have a better understanding of the situation.

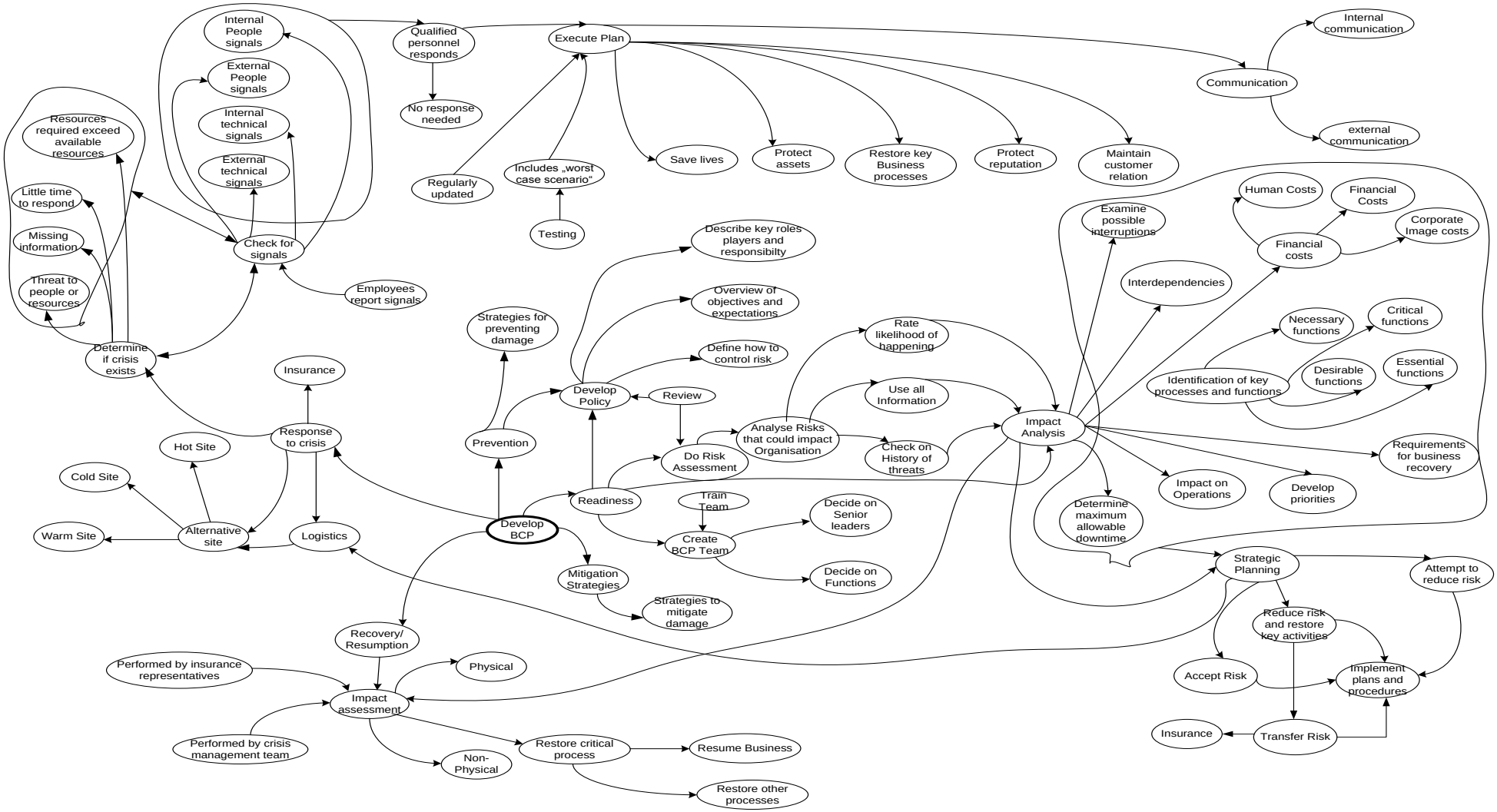

Figure 5: Conceptual Model for Risk Analysis Including Other BCP Components

3.2.5 Comparing Conceptual Model with reality

In this part of the methodology the Conceptual Model is checked against both the root definition and the rich picture. As mentioned in Chapter 2 there are four possible ways of doing this comparison, one of the most common being to develop a matrix model with structured questioning. The questions used were:

- Does it exist in the real world?
- How does it behave?
- How is its performance identified and measured?
- Who does it?
- Why do it that way?
- Is this process any good?

It is very important to imagine that the Conceptual Model is actually operating in the real world.

The Conceptual Model developed was used as a framework to structure the processes in risk analysis. Only those activities required for risk analysis were considered and these are listed below in the vertical boxes of the matrix. Although “Strategic Planning” is not part of risk analysis itself, it is closely related since it is, in essence, one output; it was therefore considered in the matrix. The questions are listed in the horizontal boxes.

	Does it exist in the real world?	How does it work/behave?	How is its performance identified and measured?	Who does it?	Why do it that way?	Is this process any good?	Does it exist in our organization?
Risk Assessment							
Identification of risks							
Rate likelihood of happening							
Use all information							
Check on history of threats							
Prioritization							
Review							
Impact Analysis							
Examine possible interruptions							
Identify key business processes and functions							
Requirements for							

business recovery							
Determine resource interdependencies							
Determine impact on operations							
Develop priorities and classifications of business process and functions							
Financial Impact							
Determine maximum allowable downtime							
Strategic Planning							
Attempt to reduce risk							
Accept risk							
Reduce risk and restore key activities							
Transfer risk							

3.2.6 Determining desirable and feasible changes

After the first five steps are completed it is necessary to review them and look for feasible and desirable changes. In order to determine the feasible and desirable changes the impact analysis can be used as a guide. The risks with the highest probability and highest impact should also have the highest priority for change. In general three main types of changes could occur:

1. **Structural changes**

   Structural changes will involve organizational groupings, reporting structures and functional responsibilities. Examples which could lead to structural changes in an organization include:

   - **Example 1**

     During the risk analysis it was discovered that certain risks were not covered. In order to cover these, some employees will have to be handed new responsibilities or one or a number of new positions will have to be created.

   - **Example 2**

     The Board has decided that it wants to be more involved with the BCP. This will mean that communication/reporting between the head of the crisis management team and the Board members will have to improve.

   - **Example 3**

     A start-up company does not yet have a BCP. It will have to create a new position or new department to develop, monitor and execute the BCP.

2. **Procedural changes**

   Procedural changes mainly involve the operational processes of an organization. Examples of events that could lead to such changes are:

   - **Example 1**

     A manufacturing company operates in a very insecure environment. One solution is to try to find a different manufacturer which works in a secure environment and therefore reduces the risk of staying without stock.

   - **Example 2**

     If not yet present, develop a cold site which can be made functional in a few days in case it is no longer possible to work at the current site.

3. **Attitude changes**

   This is the most difficult change as it refers to changes in the expectations that people have of the behaviour of other actors as well as changes in their readiness to rate certain kinds of behaviour as bad or good relative to others. Each person has a different perception which makes this very difficult.

   An example:

   An organization has a policy which describes what to do if certain events occur. Since the employee cannot be forced to read it, in case of an event he/she might not know how to react which can place him/her and others in danger.

The changes made will depend on the results of the risk analysis. In general, organizations should follow a prioritization process in which the risks with the greatest loss and the greatest probability are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. This may sound simple, but deciding between the importance of high probability/low loss and low probability/high loss can be challenging, depending ultimately on the decision makers themselves as well as the core business of the organization.

3.2.7 Making changes to improve the situation

At this point it will be up to the Board members/organization heads to decide which changes will be carried out. This will depend mainly on the feasibility, budget and prioritization processes conducted during the last stage. In order to successfully complete the changes (structural and procedural) it will require good project management which relies at a minimum on:

- **Defining the Project Scope**

  The project scope will define and describe all the requirements that have to be fulfilled. The project deliverables should be divided into smaller more manageable components. The definition of the project scope can be taken from the root definition. The requirements on the other hand will have to be described in greater detail.

- **Time Management**

  A project plan should be created to complete the project on time. This plan should include a schedule which identifies activities and considers inter-dependencies. The schedule should also show the duration of the activities and the resources required.

- **Cost Management**

  This should ensure that the project is completed within the approved budget.

- **Procurement Management**

  This includes the processes required to acquire goods and services from outside the performing organization.

Chapter 4: Applying the Reference Model to a Real Case Scenario

4.1 Introduction

In this Chapter the developed reference model is checked against a real case scenario to find out whether it could be a useful tool for performing a risk analysis. For this purpose, the reference model is tested against a procedure for opening a Credit Card account. Figure 6 is the official process model for opening a credit card account in the Erste Bank, one of the leading retail banks in Austria. The processes involved in opening such an account are analysed collectively rather than dealing with each process separately. This method is used because as discussed in Chapter 2, SSM is based on analysing the totality of systems rather than individual parts in isolation.

4.2 Process for Opening a Credit Card Account

The process for opening a new credit card is outlined in Figure 6. Further details are as follows:

A customer requests a new credit card account from the account manager in a branch of the Erste Bank. The account manager conducts a legitimization check and then enters the data about the customer into the core system. If the customer is already a client with the bank some data about the customer can be retrieved from the customer database. The customer has to fill out an application form for the credit card and has to agree to the conditions of the bank for opening a new credit card account.

After the contract has been signed the account manager sends the application to the relevant pouvoir [162]holder for approval. After he/she approves the application it is forwarded to sZV[163] where it is checked for completeness and correctness. If no mistakes are found the captured data are sent electronically to sIT Solutions[164] by the pouvoir holder. As soon as this task is completed the account manager or pouvoir holder is informed by e-mail. The original documentation is scanned and saved.

Once the information is received by sIT Solutions all the necessary data (i.e. client and account information) are prepared and transferred electronically in a standardized procedure to MBU[165]. MBU performs the data preparation (for the chip/processor and the magnetic strip) and card personalization (account number, name, expiration date, CCV, etc.) that will

[162] A pouvoir holder is an employee of the bank who has the authority to approve a credit card application.
[163] sZV is a subsidiary of Erste Bank and performs back office tasks related to payments and customer transactions (e.g. internal post service, scanning of documents, document assurance/quality check and other activities related to payments and transactions).
[164] sIT solutions is an IT provider of Erste Group and Erste Bank; it is responsible for the development, implementation and servicing of banking software and its operations.
[165] MBU is a company in Croatia that produces card processors and provides its services to Central and Eastern European countries. (http://www.mbu.hr).

appear on the card for the client. This information is then sent electronically in a standardized way to Austriacard[166].

Austriacard takes the information received and produces the credit card and PIN. The produced credit card will contain the information that was provided by MBU and will be designed (e.g. colour of card, logo, etc.) according to the agreement with Erste Bank. Austriacard delivers the PIN and credit card sealed in an envelope to the Post Office. The Post Office sends the PIN to the client. After two days the credit card is also sent to the client.

In the last step the pouvoir holder provides sZV Market service with all the relevant approved credit card information. sZV then performs another formal inspection before scanning and saving. Once the inspection is concluded the account manager is informed that the business is concluded.

[166] Austriacard is a company that produces different types of cards (e.g. debit cards, Visa Cards, etc.) (http://www.austriacard.at).

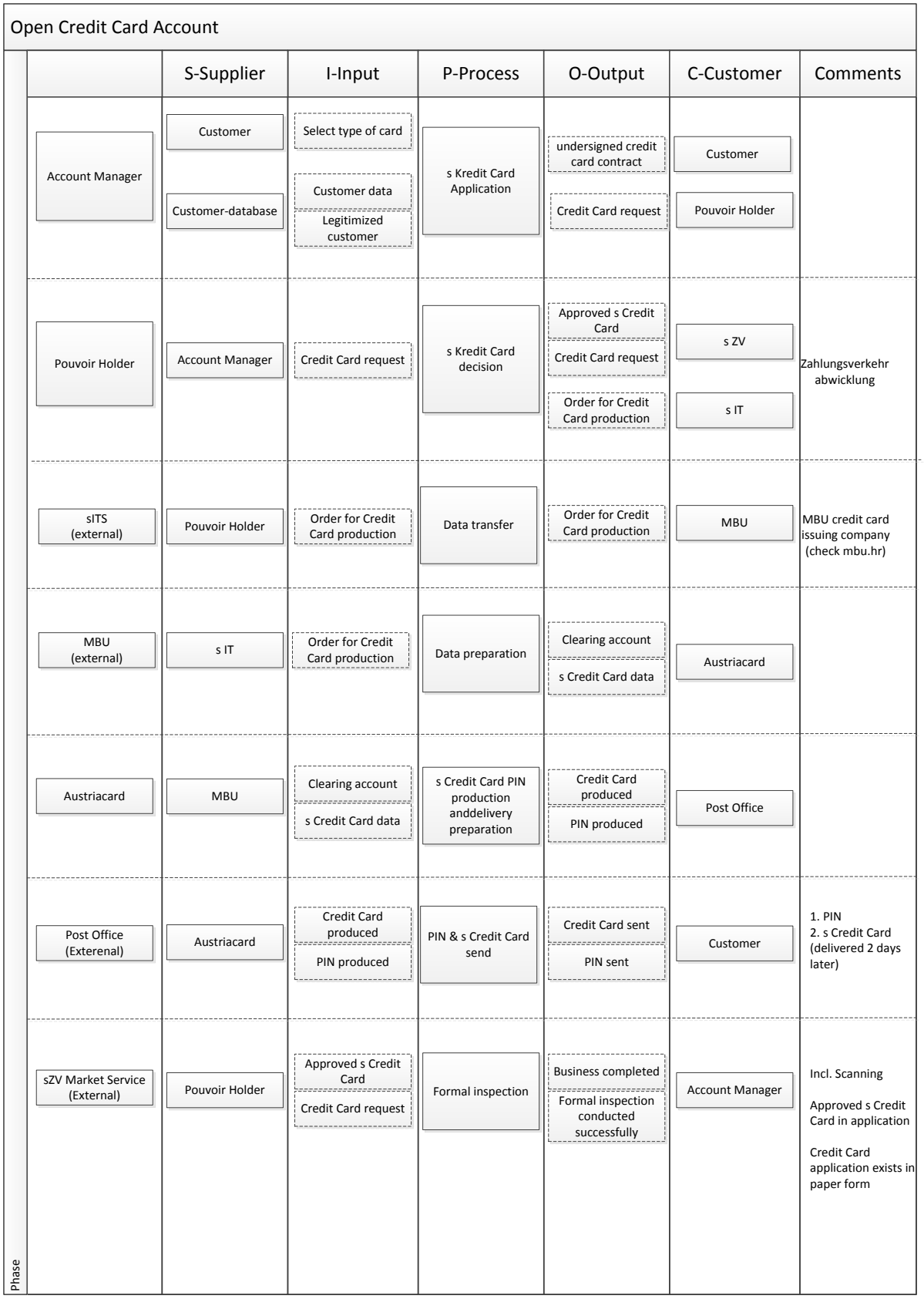

Figure 6: Process for Opening Credit Card Account

4.3 Applying the Reference Model for Opening a Credit Card Account in Erste Bank Austria

Erste Bank is one of the leading retail banks in Austria. It is also active in six other countries and has a total of over 17 million customers. An organization with such an outreach has to have a well-defined business continuity plan. In addition to the risks that other organizations are exposed to, banks also have to consider credit and market risks. According to the banking standards defined by Basel II, credit risk refers to the risk that the borrower will default on any type of debt by not meeting his/her/its obligated payments; market risk refers to the losses arising from movements in market prices. Since it is outside the scope of this thesis to make such an analysis for such an big organization, a small process within the organization that demonstrates the process involved for opening a credit card account is checked against the Reference Model developed in Chapter 3 and used as the basis for analysing the risks that are involved in the process of opening a new credit card account. By applying the reference model to such a scenario it can be determined whether the creation of the model was successful or not.

Since the risk prevention and mitigation strategies involve confidentiality issues a new risk analysis is performed using the Reference Model developed in Chapter 3.

4.3.1 Explore problem situation

In order to determine the risks involved in opening a credit card account the problem situation has to be established and analyzed. To stay within the scope of the thesis the main focus is on the following:

1. Is the organization ready in case of an event that could jeopardize its success?
2. Does the organization have the necessary prevention strategies?

As described in Chapter 3 the Reference Model developed has to be adjusted to the subject being analysed. Therefore the focus description was changed to the following so that it is suitable for the analysis:

1. Is the Erste Bank ready in the event that a part of the credit card opening process fails?
2. Does the Erste Bank have the necessary prevention/mitigation strategy for each part of the process?

Knowing the focus, it is possible to describe the problem situation to be analyzed:

"*Does the Erste Bank have the necessary strategy in case the process or part of the process for opening a credit bank account fails?*

- ➔ Are all the most probable threats that could cause a failure in the credit card opening process considered/covered?
- ➔ Does the Erste Bank Austria implement the strategies needed in case the process or part of the process for opening a credit card account fails?

To explore the problem situation further it is necessary to put "opening a credit card account" into a risk category. As mentioned earlier, banks are in general exposed to three main risk categories, namely Credit Risk, Market Risk and Operational Risk. Operational risk is defined by the Basel Committee as: "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition excludes strategic and reputational risk. From this definition it can be concluded that any risks not belonging to the risk category of credit, market, strategic and reputational risk can be categorized as operational risk, which leads to the conclusion that opening a credit card account belongs to the risk category of Operational Risk. This statement can be further evaluated by considering that opening a credit card account is a process and is dependent on people and systems as well as external events. This means that any loss occurring due to a failure of the "opening a credit card account" process will be recorded as operational risk. Therefore, within a bank, operational risk management assists in the elaboration of BCPs based on business impact analysis within Strategic Risk Management.

The Erste Group Policy for managing operational risk states that any loss event has to have a minimum of the following dimensions[167]:

- **Event type**

  Loss events are classified according to their event type. According to Basel II there are seven event types[168]:

  1. **Internal Fraud -** Losses due to act of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, and which involves at least one internal party.
  2. **External Fraud -** Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.

[167] Group Policy for Managing Operational Risk; Group Operational Risk Control, 2012.
[168] http://www.riskglossary.com/link/operational_risk.htm.

3. **Employment Practices and Workplace Safety -** Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events.
4. **Clients, Products & Business Practice -** Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients.
5. **Damage to Physical Assets -** Losses arising from loss or damage to physical assets from natural disaster or other events.
6. **Business Disruption & Systems Failure -** Losses arising from disruption of business or system failures.
7. **Execution, Delivery & Process Management -** Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

- **Organizational unit**

  Loss events are assigned to organizational units.

- **Basel II business line**

  The mapping of losses to Basel II business lines is used for the aggregation of data at group level.

- **Business function**

  A classification of loss events by business functions is carried out since failure on the execution or poor design of processes contribute significantly to the operational risk exposure.

- **Product**

  A classification of loss events by product is carried out since failures in the poor design or launch of products contribute significantly to the operational risk exposure.

In case any part of the "opening a new credit card account" fails, the above dimensions would be the minimum that the bank would use to record if the loss amounted to more than 1 000 EUR. From the author's perspective any of the possible seven event types could be responsible for the failure of the process. Therefore all seven types are considered in the risk analysis. One of the main differences between the risk analysis performed with the Reference Model and that through the banks analysis is that the latter uses both quantitative and qualitative risk analysis to analyze the operational risk whereas the Reference Model is based only on qualitative analysis.

It should be noted that the reason "opening a credit card account" does not belong to the category of credit risk is because credit risk refers to the prospective borrower not being able to meet his/her/its obligations in accordance with the agreed terms. After approval and the customer receiving the credit card, it starts to belong to the risk category of Credit risk; however such an analysis is outside the scope of this thesis.

In the event of failure in the process it is probable that this will have negative quantifiable and/or non-quantifiable consequences/losses. These losses have to be reported to the operational risk unit within the Bank. The operational risk unit then categorizes the loss according to the seven event types and captures further information such as:

- Effect type (e.g. loss, potential loss, provision). An event can have other effect types.
- Effect status (e.g. open, closed, potential)
- Costs. These are split into direct and indirect losses. Direct loss is split into loss, provision and potential loss.

In the model used in Chapter 2, the costs are differentiated into financial costs, human costs and corporate image costs. However, for the purposes of this analysis and in order to match the Basel II requirements the model of Marshall Christopher [2001] is used, in which the costs for calculating operational risk include[169]:

- **Direct Costs,** i.e. costs directly related to financial operations, including reduction in income or loss of the assets and liabilities of a business organisation. A loss event on income is specifically the additional cost expended for resolving an incident and the costs allocated to prevent such incidents from happening.
- **Indirect Costs,** i.e. events leading to indirect losses as a result of harm to an organization's image or reputation, which also affects other loss events or the functions of a business organisation. Indirect costs are the consequences of reputational risk that may lead to significant negative public opinion and thus potentially bring about critical losses of customers or stakeholders
- **Opportunity Costs.** These represent the maximum potential revenues not earned as a result of a loss event. For example, late settlement may result in counterparty withdrawal. Other examples are late penalties, retaliatory penalties, staff overtime and staff opportunity costs.

Figure 3 is used as a guide to describe the factors to be considered when performing the risk analysis.

[169] Bank of Indonesia, Directorate of Accounting and the Payment System (2004). Study of Down Time Risk and Recovery Time Objectives for the Bank of Indonesia Real Time Gross Settlement System.

In order to conduct a thorough risk analysis it is necessary to gather a considerable amount of information as well as to consider the problem from a wide perspective.

This means that while performing the risk analysis the following stakeholders have to be considered:

- Account Manager
- Customer
- Pouvoir Holder
- sITS
- MBU
- Post Office
- Austriacard
- SZV Market service

Having multiple stakeholders involved in a process can have certain risks. Therefore it is important to identify and analyze the stakeholders and their interests. In general it can be assumed that if the benefits are high for the stakeholder the cooperation will be good and if the benefits are not very beneficial then there might be a possibility that the cooperation/service might be on a lower level. In general there are three types of stakeholders: primary, secondary and key stakeholders. These are defined as:[170]:

- **Primary Stakeholder - Beneficiaries or targets of the effort**

  Beneficiaries are those who stand to gain something – services, skills, money, goods, social connection, etc. – as a direct result of the effort. Targets are those who may or may not stand to gain personally, or whose actions represent a benefit to a particular population or to the community as a whole.

- **Secondary Stakeholders - Those directly involved with or responsible for beneficiaries or targets of the effort**

  These might include individuals and organizations that live with, are close to, or care for the people in question, and those that offer services directly to them.

- **Key Stakeholder - Government officials and policy makers**

  These are the people who can devise, pass, and enforce laws and regulations that may either fulfill the goals of any effort or directly cancel them out.

[170] http://ctb.ku.edu/en/tablecontents/chapter7_section8_main.aspx.

According to these definitions only primary and secondary stakeholders are involved in the process. Key stakeholders are not involved in the process. According to the above definition, key stakeholders would be those that can change and influence the process (CRO, CIO, etc.). None of the stakeholders in the process are therefore key stakeholders. In Table 1 below the stakeholders are categorized according to stakeholder type.

Stakeholders	Primary Stakeholder	Secondary Stakeholder
Account Manager		✓
Customer	✓	
Pouvoir Holder		✓
sITS		✓
MBU		✓
Post Office		✓
Austriacard		✓
SZV Market service		✓

Table 1: Stakeholders

All the stakeholders have a benefit from the process and therefore it can be assumed that there should not be any major problems with cooperation. However, the credit card opening process does involve a lot of outsourcing and therefore the risks involved in outsourcing activities have to be considered. In fact, only the first part of the process, namely where the client is applying for the credit card is the bank completely in control. Indirectly, the Erste Bank has control over sZV Market Service as well as sIT Solutions as those are subsidiaries of Erste Bank. Therefore the part of the process performed by those entities can be controlled, influenced and monitored to a greater extent.

Outsourcing can be very effective, but it brings significant risks that must be recognized and managed as the bank is relying on another company to run certain business functions in order to complete the credit card opening process. If those risks are not managed properly, they may negatively affect the bank’s operations and customers.

Here are some of the risks taken by the bank when outsourcing a large part of the credit card opening process:

- Delays can be caused by many factors that are outside the control of the bank.
- Credit card quality may suffer, affecting customer satisfaction.
- Providers might become insolvent, causing an interruption in the process.

In general, before deciding on the company to which an activity should be outsourced the following three analyses are performed (Outsourcing assessments)[171]:

- Material assessment
- Strategic and reputational assessment
- Outsourcing controlling risk assessment
    - counterparty risk and operational risk
    - dependency risk and financial risk
    - legal and compliance risk
    - Other risk

Finally, if it is decided that an activity is going to be outsourced it will be considered within risk management and consist of three elements: provider management, service level agreement (SLA) and billing accuracy[172]. Provider management keeps track of the statistics or historical performance of the outsourcing relationship over time. These statistics are continually leveraged to improve the performance of the relationship for the outsourcer and the outsource provider. The SLA states the requirements of both parties. It should be reviewed and updated periodically as defined clearly in the contract terms. Billing accuracy keeps track of the invoice matching and ensures compliance with the contract terms[173].

The next step is the actual identification of all the risks to which the credit card opening process is exposed. These are described in Table 2. The risk identification was based on the seven event types that are currently used by the Erste Bank. The risks identified were then mapped to one of the event categories. This task was performed to support the rich picture which depicts the whole process.

[171] Group Operational Risk Control; Decentralized Operational Risk Management Guideline, Sep., 2013).
[172] http://www.isaca.org/Journal/Past-Issues/2005/Volume-5/Pages/Outsourcing-A-Risk-Management-Perspective1.aspx.
[173] http://www.isaca.org/Journal/Past-Issues/2005/Volume-5/Pages/Outsourcing-A-Risk-Management-Perspective1.aspx.

Internal Fraud	Unauthorized activity	Internal fraud and theft
External Fraud	External fraud and theft	Credit fraud
Employment Practices	Discrimination Robbery Accidents happening to employees at work	Sexual harassment Unfair dismissal
Business Interruption & System Failures	IT system breakdown Slow operation of system	Infrastructure breakdown Inappropriate functioning of system
Clients Products & Business	Incorrect advice to customer Improper business practice	Breach of bank security
Execution, Delivery and Process Management	Human processing error Incomplete customer data input Incomplete information provided to customer	Human error, wrong information to customer Incomplete customer documents
Damage to Physical Assets	Fire Major snowfall	Flood Natural disaster & accidents

Table 2: Risks identified within the credit card opening process

The next step was to map the risks identified to each stakeholder and to the functions with which the stakeholder is involved as well as rating the function according to its importance according to the opinion of the author. Although only part of the process is within the control of the bank, the identified risks were based on the whole process as is suggested by SSM. Those risks were also mapped to the corresponding function with which the stakeholder is involved.

Account Manager		
Function performed	**Key function identification**	**Risk**
Product offer to customer	Critical	Discrimination towards customer; sexual harassment; unfair dismissal; incorrect advice to customer; (deliberate) wrong information to customer (non-deliberate); breach of bank security; improper business practice; incomplete information provided to customer.
Legitimization check	Essential	Human processing error, incomplete customer documents, unauthorized activity.
Enter customer data	Critical	Internal fraud and theft; IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system; human processing error; incomplete customer documents.

Pouvoir holder		
Function performed	**Key function identification**	**Risk**
Pouvoir holder approval	Essential	Unauthorized activity; improper business practice; unfair dismissal.
Application sent via internal post	Necessary	Human processing error; incomplete customer documents.
Electronic request sent to sIT for card production	Essential	Human processing error; IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system.

sZV		
Function performed	**Key function identification**	**Risk**
Check correctness	Necessary	Unauthorized activity; improper business practice; unfair dismissal.
Send confirmation to Pouvoir holder	Necessary	Human processing error; IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system.

sIT Solutions		
Function performed	**Key function identification**	**Risk**
Send data electronically to MBU	Critical	Human processing error; IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system.

MBU		
Function performed	**Key function identification**	**Risk**
Data preparation (chip/processor and magnetic chip)	Critical	IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system; improper business practice; human processing error.
Card personalization (account number, name, etc.)	Critical	IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system; improper business practice; human processing error; external fraud and theft.
Send data electronically to Austriacard	Critical	IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system; human processing error.

Austriacard		
Function performed	**Key function identification**	**Risk**
Card Design and Production	Critical	IT system breakdown; IT infrastructure breakdown; slow operations system; inappropriate functioning of system, human processing error, improper business practice.
PIN Production	Critical	IT system breakdown, IT infrastructure breakdown, slow operations system, inappropriate functioning of system; human processing error; improper business practice.
Provision of PIN to Post Office	Essential	Human processing error; improper business practice; external fraud and theft; accidents to employees at work/on the way to work; external fraud and theft.
Provision of card to Post Office	Essential	Human processing error; improper business practice; accidents to employees at work/on the way to work; external fraud and theft.

Post Office		
Function performed	**Key function identification**	**Risk**
Provides PIN to customer	Critical	Human processing error; improper business practice; accidents to employees at work/on the way to work; external fraud and theft.
Provides card to customer	Critical	Human processing error; improper business practice; accidents to employees at work/on the way to work; external fraud and theft.

Customer		
Function performed	**Key function identification**	**Risk**
Filling out application	Essential	Credit fraud, robbery.
Providing legitimization	Essential	External fraud and theft.

Apart from the operational risks identified above there are two additional risks that arise from outsourcing, i.e. Dependency Risk and Counterparty Risk.

In Appendix A the risks and processes are consolidated in one table. The risks identified have been graded with a residual risk grade, residual risk being the risk that remains after controls are taken into account (the net risk)[174]. The risk grades for the residual risks are calculated by taking into account the inherent risk and control. Inherent risk is the risk that an activity would pose if no controls or other mitigation factors were in place (risk before control)[175]. The following table from Erste Bank operational risk management was used for determining the correct residual risk grade:

Control						
	No Control	3	5	6	8	9
	Poor	3	4	6	7	8
	Moderate	2	3	4	6	7
	Good	1	2	3	5	6
	N/A	Negligible	Low	Medium	High	Catastrophic
		Inherent Risk				

Mitigation or prevention strategies for high residual risk points should be defined as soon as possible.

[174] http://ishandbook.bsewall.com/risk/Assess/Risk/inherent_risk.html.
[175] Ibid.

4.3.2 Problem situation expressed

The rich picture in Figure 7 depicts the main stakeholders involved with the Erste Bank. Although the rich picture considers and describes a wide range of aspects, its main focus is on the tasks performed within the bank. In order to identify these risks the whole process has been depicted including *inter alia* not only the entire chain of events involved in the credit card opening process but also the thoughts - including both the possible subjective interpretations by and emotions of stakeholders - as well as the actions that each stakeholder has to perform for the process to succeed.

The subjective interpretations and emotions were considered mainly for the functions performed within the bank itself because these might be relevant for the risk analysis. Although other actions involved in the process of opening a credit card account are also depicted in the rich picture these are not subjected to detailed analysis as the tasks performed belong to the category of Dependency Risk.

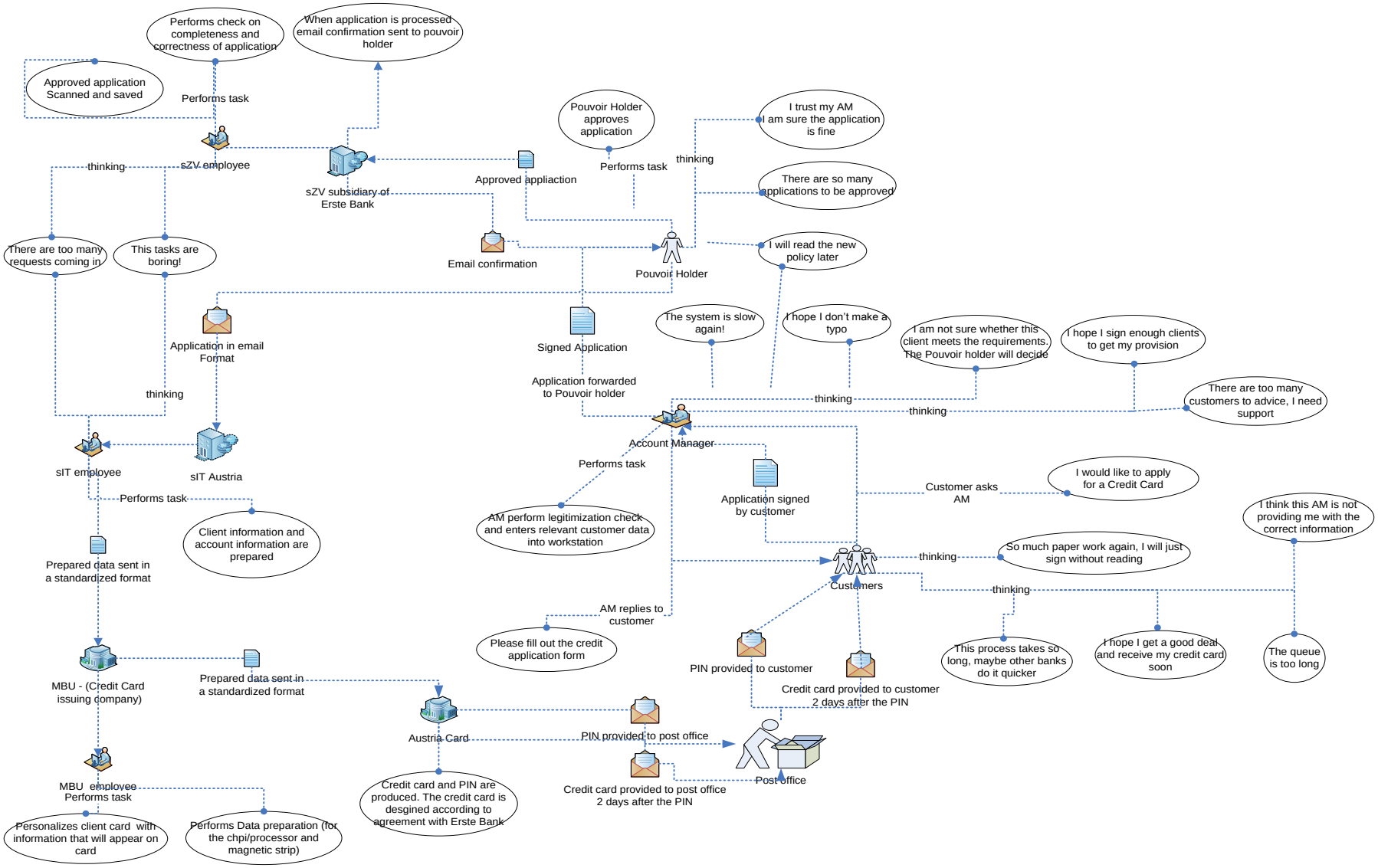

Figure 7: – Rich picture

4.3.3 Root Definition

As described in Chapter 2 (Section 2.4.3) the best way to start the root definition is by applying the PQR formula which involves asking three questions:

First question:

> "How will the possible threats/failures in the processes undertaken by the Erste Bank for opening a credit card account be identified?"

Second question:

> "What will the Erste Bank try to protect by identifying possible threats/failures and having prevention/mitigation strategies for those in the credit card account opening process?"

Third Question:

> "Why will the Erste Bank try to protect itself against a failure in the credit card account opening process?"

Answers:

How: By doing a risk analysis and identifying which parts in the process of opening a credit card account are exposed to risk.

What: The Erste Bank will try to secure the process of opening a credit card account against failure in order to protect part of its core business.

Why: In order to further generate profit and to keep its customers satisfied.

After using the PQR formula, the CATWOE method was applied to ensure that nothing was missed for defining the root definition. Once again "Weltaunschauung" was replaced with "Approach" because it is a more appropriate term to be used for this analysis.

Customers	**Clients**
Actors	Account Manager, Pouvoir Holder, sITA, SZV, MBU, Austriacard, Post Office.
Transformation	Analysing the credit card opening process so that risks and threats within the process can be mitigated/prevented.
Approach	Risk analysis. Through risk analysis it is possible to identify various risks and threats that could cause the credit card opening process to fail. Knowing the threats and risks, appropriate countermeasure can be considered.
Owner	Process management department.
Environmental Constraints	Event estimations, only part of the process can be influenced as there are many dependencies on other counterparties.

After completing the PQR formula and the CATWOE it is possible to form the root definition.

Root Definition:

"Erste Bank should investigate the vulnerabilities within the credit card opening process by doing a risk analysis in order to identify various risks and threats that could jeopardize the process. With the risk analysis completed the bank will have the possibility to prevent/mitigate the risks identified. In addition good customer relationships can be maintained and future revenues and profits can be expected."

4.3.4 Conceptual Model

A Conceptual Model that represents the system was developed based on this root definition. If one compares the root definition of the framework (Section 3.2.3) with that formulated here it is noticeable that the two are very similar, the only difference being that the root definition from the framework is very general while the current one is adapted to the specific situation. Therefore, some of the activities represented in the Conceptual Model from the framework and in this scenario are the same; the former was therefore followed. The main difference between the two conceptual models is that for the purposes of this thesis only the risk analysis activities were considered, i.e. BCP activities were omitted as these were beyond the scope of the thesis.

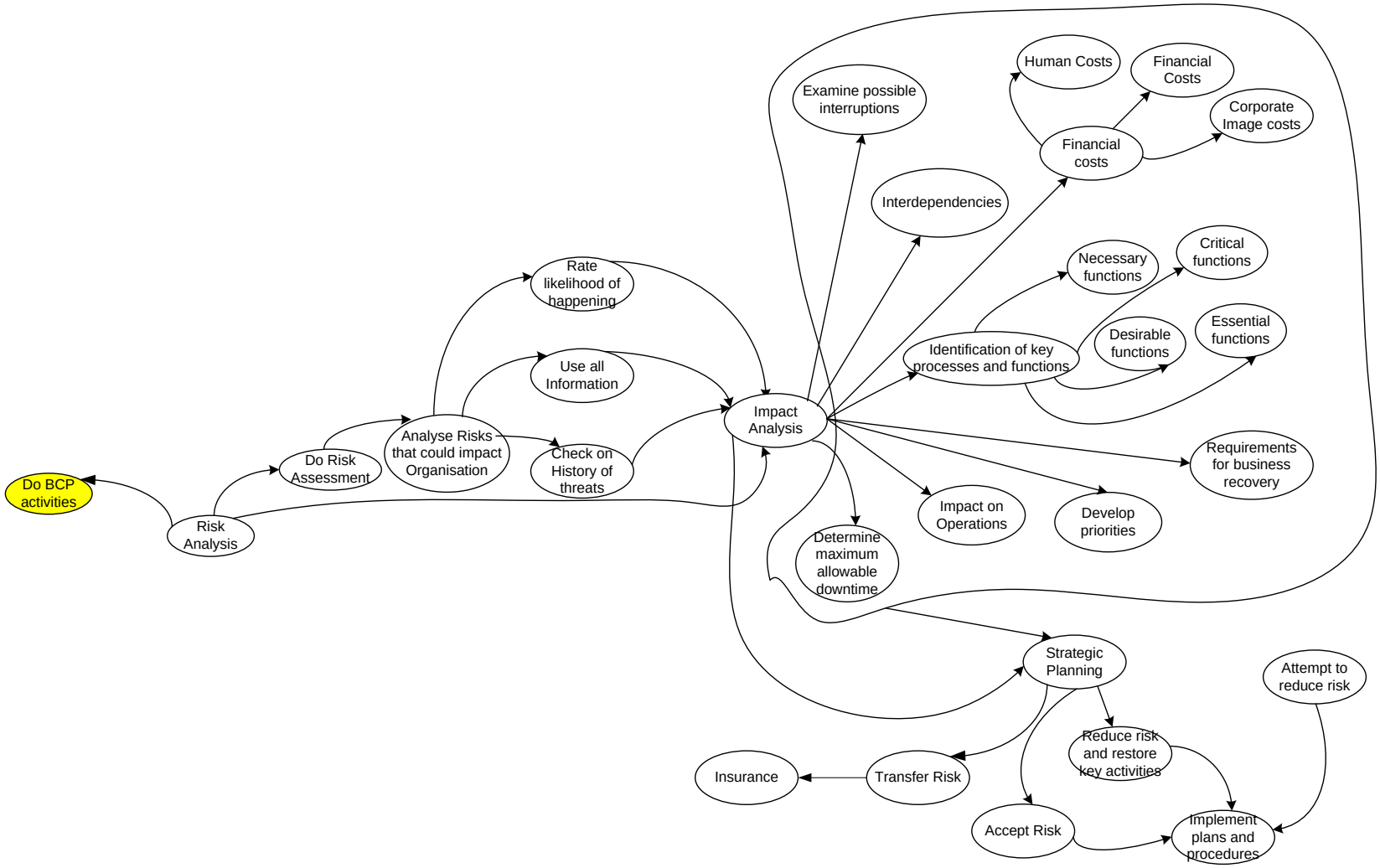

Figure 8: Conceptual Model Considering only Components Relevant to Risk Analysis

4.3.5 Compare Conceptual Model with Reality

In this part of the methodology the Conceptual Model was checked against both the root definition and the rich picture. In Chapter 3 a matrix model was developed to perform this check. As the model developed considers only those activities required for risk analysis, the matrix developed in Chapter 3 was used for comparing the Conceptual Model with reality. For each activity forming part of the risk analysis the following questions were asked:

- Does it exist in the real world?
- How does it behave?
- How is its performance identified and measured?
- Who does it?
- Why is it done that way?
- Is this process any good?

Identification of risks exists in the real world and this can be confirmed by the case of the process within the bank that is being studied. Every risk that could possibly jeopardize the process of opening a credit card account in the Erste Bank is assessed, and in a perfect world all the events that could jeopardize the credit card opening process would be identified by using the SSM in combination with the risk assessment. In a risk assessment the identification of risk is essential since it seeks and appropriately identifies the risks to which the credit card account opening process at the Erste Bank is exposed.

With regards to rating the likelihood of occurrence, the applicability of the Conceptual Model for identifying risks confirms that it can be rated in the real world. Additionally, the Conceptual Model is efficient as it both identifies and rates each risk in accordance with the probability of occurrence. Within the bank the probability of an identified risk occurring is done by the operational risk management and business units involved. In general, rating of risks is often based on the severity of loss and frequency of the risk. There are those risks that occur frequently within an organization but the extent of potential loss is not severe. On the other hand, there are risks that while occurring less frequently, can have very severe consequences. In the process under study both cases are applicable. An example of low occurrence high severity would be that the post office delivers the credit card to the wrong person, and that this person miss-uses the credit card. Not only would the bank incur losses but it would also have dissatisfied customers. An example of a high occurrence and low severity loss within a process would be that the account manager does not provide all the information required to the customer for opening a credit card account. Since the customer signs a contract he is also obliged to read it and all the required information is provided in the document. Therefore failure to provide all information to the customer might occur often but will not in most cases lead to severe losses.

As shown from the risk analysis, the rating of an event is not only based on its probability but also on its control. The reason for rating each risk according to probability and control is because this ensures a more accurate analysis. For example, if an account manager forgets to enter the birth date of the client into the system and a control check within the system is developed that blocks further processing of the application until the birth date is entered, than although the probability of failing to enter the birth date is high, the residual probability would be non-existent as the account manager would be reminded to enter the birth date in order to proceed with the application. For the process under study, it is clear that the highest risks are those where there is little or no control.

In the context of prioritization, the process under study confirms this reality. After the risks were identified and rated, they were prioritized. Those risks with highest severity/loss in combination with probability of occurrence are attended to first, by developing mitigation and prevention strategies where possible.

The main problem with prioritization is that the performance of the prioritization will only be measurable after a certain time period. This is because only after the passage of a certain period and the identification of some risks is it possible to determine whether the prioritization was performed correctly. Prioritization is a fundamental process since it is the only way that risks requiring attention first are handled. Risk prioritization at any organization - also for the Erste Bank - is an essential risk management practice. If absent, it could happen that prevention and mitigation strategies are first developed for risks that are less likely to happen and where the outcome is less severe.

The Conceptual Model also entails conducting an impact analysis which includes an examination of possible interruptions caused by a particular event. Mapping these to the process of opening a credit card account demonstrates that several interruptions could arise due to a failure in a function. For example, in the event that the workstation of the account manager is not working properly, or there is a timeout in the core database, the account manager would stop the current account operations in order to focus on the failure. Besides the account manager, other parties not directly involved in the credit card opening process might be affected. In this situation it is possible that that the branch manager also becomes involved in trying to sort out the problem and by so doing, his/her normal work will have been disrupted, thereby reducing their effectiveness in undertaking higher management responsibilities.

The above example illustrates the point that for each event the possible interruption within the process should be analysed. Under a best case scenario, for each event that happens a specialist within the bank (preferably unit) should be able to match the interruptions previously assumed with the risk analysis.

Another characteristic of the model is to identify the business process and functions. In this case, a business process would be the credit card opening process and a function would be the

tasks that are performed within the process, e.g. account manager talking to customer, account manager inputting data of client into core system, etc. Therefore, only the key business functions within the credit card opening process have to be identified and rated as only one process is being analysed. For example a crucial function within the credit card opening process would be capturing the client data in the core system. If this function was not available the entire process would be compromised and therefore this function can be rated as crucial. Once all key business functions have been identified and rated, they should be prioritized. In general, those functions identified as "crucial" or "essential" for the credit card opening process should be handled first, as they are indispensable for the process to work at all. In addition to prioritizing functions, all requirements essential for securing recovery of the function under consideration have to be established. For example, in order for the account manager to be able to capture data of a client at least the following resources will be required: desk, chair, power supply, workstation and network connection to core system. This indicates that performing an analysis of the resources required for each function is crucial because without the required resources it will not be possible to complete that function.

Another part of the model is to determine the interdependencies. A good illustration of the importance of the interdependencies is a system outage. In case of a system outage, not only will the credit card process itself be affected but a multitude of other processes such as: creating a new account for customer, creating a mortgage or credit for customer, etc. will be affected by the outage.

In the model the impact on operations is also analysed. In the event that the whole credit card process is disrupted, the end result on operations would be revenue loss due the missed customer acquisition. In reality, however, much more likely would be that one function within the overall process experiences a disruption.

The model is also used to examine the possible costs (financial impact) associated with the occurrence of a potentially damaging event. Banks are obliged by Basel II to have capital set aside to buffer against the occurrence of unpredictable events. This capital buffer is called the minimum capital requirement and includes Credit, Market and Operational risk. The possible costs associated with an identified event within a process require specific assessment so that when/if the event happened it would be easy to match the predicted costs against the initial costs. If these costs are similar, it implies that the analysis is not only effective but also appropriate.

Banks use a quantitative approach for calculating how much capital has to be put aside for operational risk management. Within Basel II there are different approaches for capturing the minimal capital requirement. The Erste Bank uses the most advanced approach available, namely the "Advanced Measurement Approach" which is based on the internally developed risk measurement framework. With this in place, it can be concluded that funds are available

to cover the costs of occurrence of an unpredicted event at the process level, such as the credit card opening process.

A further feature of the Conceptual Model is the inclusion of the maximum allowable downtime, the function of which is to assist the Erste Bank to minimize emergent losses. This process is performed through collaboration between operational risk management and the key employees of the unit, which in this case would be the branch managers. In general a workshop would be organized where the branch manager and an employee from operational risk management would meet to discuss the most essential and core procedures within the credit card opening process are discussed. This particular task usually starts with checking the processes that are most essential for a bank. Subsequently, the maximum allowable downtime for each step of the process is determined.

Within the Erste Bank, the maximum allowable downtime is set by a threshold defined for a Key Risk Indicator (KRI). A KRI is a measure that reflects risk level or the quality of risk controls of an organization. By determining qualitative ranges in the corresponding sphere, risk indicators can be derived from actual performance indicators[176]. KRIs show the dynamic changes in dedicated risk points over time. All relevant departments within the organization have to be involved in the collection of these KRIs[177]. For example, the IT systems used within the process of opening a credit card account have to be available 98% of the time. After a quantitative analysis (data covering at least 6 months) it would be determined whether the threshold is attained. In the event that the availability of the IT systems is lower, improvements for the KRI would be required. The suggested improvements are recorded under "corrective measures". Corrective measures describe the possible mitigation and prevention strategies that will be put in place within a given period. After a given period, the unit responsible for implementing the corrective measure is checked for progress.

The next feature is to strategically plan how to reduce the identified risks. This requires developing both mitigation and prevention strategies. Doing so involves capturing the risk(s) in the system through the following process:

1. Record risk (e.g. a critical system outage).
2. Define risk (e.g. a critical system is defined as where system failure can have severe economic consequences for Erste Bank).
3. Select the Unit in the bank affected by the risk.
4. Select KRI's for the risk (e.g. number of outages, normal system availability, etc.).

[176] Group Policy for Managing Operational Risk; Group Operational Risk Control, 2012.
[177] Ibid.

Once the above process is performed the risk is described in greater detail, allowing determination of whether it is currently controlled through a prevention or mitigation strategy. If not, then a corrective measure together with a timeframe for its implementation is entered.

Unfortunately it is not always possible for the bank to create mitigation or prevention strategies for the risks identified. Therefore it is acknowledged that the following strategies are further options:

- Transferring the risk to another party such as an insurance company
- Outsourcing of the activity
- Ceasing the activity
- Accepting risk

Within the credit card opening process the outsourcing of the activity definitely plays a crucial rule. In fact a very high proportion of the process is outsourced. Outsourcing activities and their attendant risks are described in Section 4.3.1.

The least favourable possibility is to simply accept the risk. The reasons the Erste Bank might be inclined to accept certain risks are because the costs of any potential losses incurred are not intensified and/or would not have significant adverse knock-on effects, e.g. on customer relationships. Acceptance of risk is, however, not a preferable course of action and operational risk management specialists believe that risk acceptance should be avoided entirely as it could lead to a situation where bank operations are in some cases severely compromised.

By answering these questions an overview was created describing how each activity is performed and its purpose.

	Does it exist in the real world?	How does it work/behave?	How is its performance identified and measured?	Who does it?	Why do it that way?	Is this process appropriate?	Does it exist in our organization?
Risk Assessment							
Identification of risks	Yes	All the risks that could jeopardize the process for opening a credit card account are looked at.	All events that happen to the organization should have been identified. If all events are in the list and covered then the risk identification was good; otherwise some risks are missing.	Specialist with support of business unit.	There is no alternative.	Yes, because it identifies risk to which the credit opening process is exposed.	Yes
Rate likelihood of happening	Yes	All the identified risks are rated with a probability of happening.	All the risks/events that happened and did some damage or were mitigated/prevented can be compared against the rating of the likelihood. If the rating was correct it will reflect the real life event occurrence.	Specialist with support of business unit.	Because it is the most appropriate way to measure risk.	Yes, because it tries to identify the likelihood of an event happening. This is a difficult process and prone to wrong estimations.	Yes

Prioritization	Yes	All identified risks are prioritized. For the risk with the highest priority a prevention/mitigation strategy should be developed first.	The performance of the prioritization process can be measured only after a certain period y.	Specialist with support of business unit	Only with prioritization is it possible to decide which risks should be attended to first.	Yes, because otherwise it could happen that the prevention/mitigation strategies are described for less important processes.	Yes

Impact Analysis							
Examine possible interruptions arising from an event	Yes	This is performed by analyzing all possible interruptions to the credit card opening process caused by an identified event.	If an event happens it should be possible to associate with the interruptions that were assumed; in such a case the analysis was successful.	Specialist with support of business unit.	This is the only way to examine possible interruptions.	Yes, since the organization will know what type of interruptions can occur after an event.	Yes
Identify key business processes and functions	Yes	All the key business processes and functions performed in the credit card opening process are identified. Each function within the process has to be analyzed and its importance for the process has to be determined.	The key business processes and functions identified have to be rated. In case of an event disabling more business processes and/or functions for a period of time it will be possible to determine whether the categorization was performed correctly.	Specialist with support of business unit.	Only with identification of key business functions is it possible to know which functions are critical for operations.	Yes, the identification of key business process is crucial in order to complete the impact analysis.	Yes

Requirements for business recovery	Yes	For all the key business functions within the credit card opening process that were identified as critical or essential, the required resources for the recovery of the functions have to be identified by checking what resources are required for the function (e.g. computer, personal, office space, etc.).	In case of an event disabling a business function the necessary resources should be available. If the recovery time takes longer due to lack of resources it will mean that the requirements for business recovery where not met fully.	Specialist with support of business unit.	Because it is the most appropriate way to figure out which resources are required for the critical business functions.	Yes, because in case of an event the organization should know which resources are required in order to get the business process or business function active again.	Yes

Determine interdependencies	Yes	The interdependencies of the functions within the credit card opening process have to be identified by checking how an event would affect other processes or functions.	In case an event causes a disruption to a function within the credit card opening process, the bank will be prepared that other process or functions that are interdependent might be affected. In case the interdependencies analysis was performed correctly the affected processes or functions will match the predicted.	Specialist with support of business unit	Because it is the most appropriate way to determine whether a disruption within the credit card process will affect other business functions outside the credit card opening process.	Yes, because in case of an event the organization should be aware what resource interdependencies exist, and which other business processes might be affected in case the credit card opening process cannot be performed.	Yes

Determine impact on operations	Yes	It has to be determined how the organization will function in case the credit card opening process or a function within the process cannot be performed for a period of time.	If an event disables a business function within the credit card opening process and the impact of this function not being available for operations was analyzed correctly, it will be possible to match the predicted against the actual occurrence.	Specialist with support of business unit.	Because it is the most appropriate way to figure out how the organization's operations will continue in case the credit card process is not available for a period of time.	Yes, because the organization needs to be aware how a disruption in the credit card opening process would affect its overall operation.	Yes
Develop priorities for business processes and functions	Yes	The critical business processes and functions have to be prioritized.	After an event that affected an additional business process and functions it will show whether the prioritization was performed correctly.	Specialist with support of business unit.	Only with prioritization of the functions within the credit card process is it possible to determine which function should be recovered first in case of an event	Yes, because by doing a prioritization it will be clear which functions should be recovered first in order to enable the credit card opening process again.	Yes
Determine financial impact	Yes	This is performed by analyzing the possible costs that an identified event could incur to the process.	If an event happens it should be possible to match the predicted and actual costs. If these are similar, the analysis was thorough.	Specialist with support of business unit	This is the only way to examine possible costs.	Yes, as the bank will be able to determine how much damage an event will cost in case the insurance does not cover it. With this approach it is possible to prepare some reserves (e.g. put funds aside to be able to restore key processes).	Yes

Determine maximum allowable downtime	Yes	The most important procedures within the credit card opening process are determined. For those prioritized with high importance the maximum allowable downtime is determined.	It is performed by first checking which processes are the most important for the organization. Once these are identified the maximum allowable downtime for this process should be determined to enable the organization to minimize its loss.	Specialist with support of business unit.	This is the only possible way to examine possible costs.	Yes, as it will make the bank aware of which processes are the most crucial. This will enable the bank to prepare mitigation strategies in order to continue crucial processes on time.	Yes

Strategic Planning							
Attempt to reduce risk	Yes	Identified risks should be reduced by developing prevention and mitigation strategies.	The performance can be identified if the event occurs and the mitigation or prevention strategy helped the bank to minimize damage.	Specialist	If the aim is to reduce a risk, the only way of doing this is by developing either a mitigation or prevention strategy. Another possibility would be to transfer the risk.	Yes, because if prevention or mitigation strategies are in place, the bank could save a lot of money.	Yes
Accept risk	Yes	Although the bank is aware of the risk within the process it accepts it. There is nothing to be done in this case.	There is no performance check if the risk is accepted.	-	The bank will accept the risk because the budget is insufficient and/or experience is missing.	No, accepting risks should be avoided as it could destroy the business.	Yes

Reduce risk and restore key activities	Yes	A strategic plan is implemented to respond to any crisis that might occur and to identify methods to mitigate the risks and exposures identified.	The performance can be assessed if the event occurs and the strategic plan helped in restoring the process and its key activities rapidly.	Specialist	Developing a strategic plan is the most efficient way to reduce risk and restore key activities.	Yes because a good strategic plan will enable the bank to restore key activities quickly and enable it to continue its business.	Yes
Transfer risk	Yes	Insurance for risks identified is agreed with an insurance company. Insurances mainly only cover what has been destroyed.	In case of an event happening that has been insured against by the organization, the organization recovers the value of the property/equipment destroyed.	Organization owner	It is quick and in some cases is the best way to mitigate certain events (e.g. break-ins)	This process is very good if combined with a strategic plan where prevention/ mitigation strategies are also considered. Insurances only cover current business; they do not insure the contingency of the business.	Yes

Table 3: Comparing the Conceptual Model against Reality

4.3.6 Determine desirable and feasible changes

The impact analysis was performed as described in Chapter 1.3.1.2 and the risk categories described in Table 4 were used for the chart. While these operational risk categories were applied to the entire credit account opening process, only the risks actually applicable to the bank were considered for the impact analysis. The operational risks identified for the processes being outsourced were, however, aggregated under the risk category "Dependency Risk".

Risk Category
Internal Fraud - Operational Risk
External Fraud - Operational Risk
Employment practice and workplace safety – Operational Risk
Clients, products and business practices- Operational Risk
Business disruption and system failure
Execution, delivery and process management
Dependency Risk
Counterparty Risk
Financial Risk

Table 4: Risk Categories

The impact analysis (Figure 9) shows that the highest risks within the credit card opening process are within the execution, delivery & process management, business interruptions and system failures within the bank itself as well as counterparty risk and dependency risk. For the counterparty and dependency risks the Erste Bank takes consistent measures to control these by performing outsourcing assessments on a 1-2 year basis. The outsourcing assessment activities are described in Chapter 4.3.1.

In the next step, the structural, procedural and attitude changes that should be considered for the parts of the process performed within the bank are described. The changes that are proposed are a combination of the risks discovered through the risk analysis and the rich picture. Any of the recommended changes that have not already been considered the by Erste Bank, need to be analysed and prioritized. For the proposed changes an example of a more detailed risk analysis was performed which can be found in Appendix B. Only the tasks considered by the author to

be necessary for the risk analysis were performed; in effect, not all representations of the conceptual model were used.

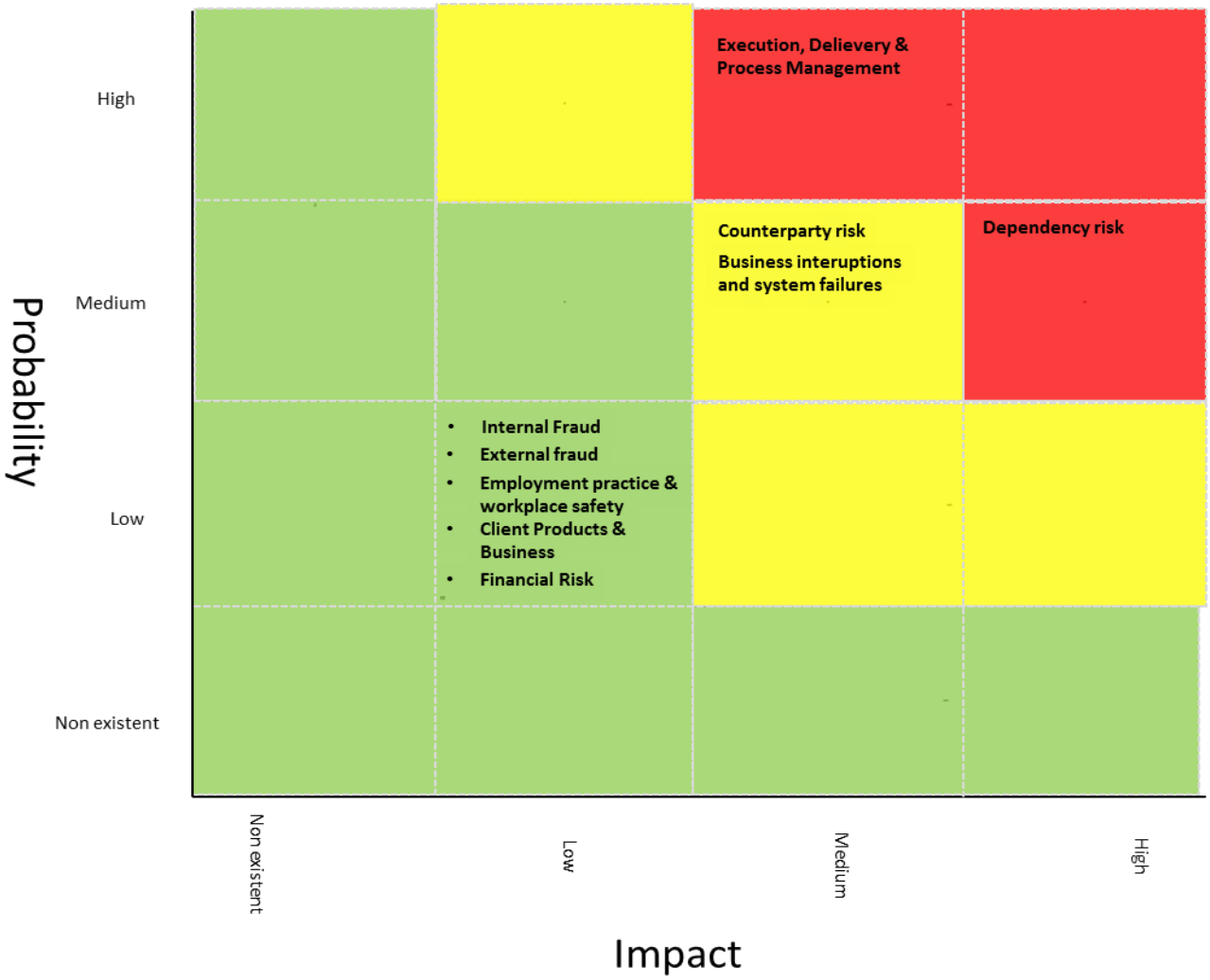

Figure 9: Impact Analysis

Structural changes

In the process of conducting a risk analysis at the bank, several operational risks were identified that might have to be looked at in greater detail, e.g. the risk of an employee not attending to his or her daily duties due to an emergency arising from an accident or sudden illness. Such duties could include conducting the tasks for opening a new credit card account. To cover such risks adequate resources have to be made available within each branch. This type of risk can potentially affect most of the tasks undertaken within the credit card opening process as human actions are a necessity. In case of such an event, the credit card opening process may not be stopped, but could be slowed, which could lead to unhappy customers. As mentioned earlier, the Erste Bank can only strive to cover its part of the process, and has to rely on assurances by the outsourced companies that sufficient resources are made available for all incoming requests. One of the problems with this identified risk is that it cannot be quantified and the

only way for the bank to find out whether it is losing revenue would be through a customer survey.

Procedural changes

Many tasks in the credit card opening procedure are performed manually and therefore, as shown in the risk analysis, there is a high risk of human error. The process requires significant paperwork and any typographical error would mean that the account opened would not be usable since it would have the wrong details. Currently, client information is double checked by the sZV; however this is also prone to human error. In order to determine whether the current procedure meets standards it would be necessary to find out how many credit cards were returned by customers due to typing errors. Then, it would have to be ascertained in which part of the process this happened and whether the error was the bank's responsibility or occurred in one of the outsourced organizations. It is outside the scope of this thesis to analyse this further. While such an analysis should theoretically be undertaken by the Erste Bank, it should be noted that it has already introduced a digital account opening procedure that enables customers to order a credit card online, which makes the customer liable for all the given information. When a client applies for a credit card over an online application the possibility of an account manager making typing error can be excluded.

Another high risk discovered during the risk analysis is that the Erste Bank has a high dependence on outsourcing companies. A further analysis should therefore be performed where outsourcing companies were responsible for delays in the credit card opening process. In the event that such an analysis shows that a credit card is in many cases delivered later than agreed with the client due to the fault of an outsourcing company, further steps should obviously be taken.

Attitude changes

All Erste Bank employees involved in the credit card account opening process are supplied with a booklet and regular training about the products and their conditions of use. It is difficult for the bank to control whether the employees concerned actually read the booklet and understand the updates provided in workshops. If this is not the case, it could happen that a client does not receive all correct and current information about the credit card being applied for, or that the client' application is rejected although he/she is eligible to receive the credit card. Customer service can only be rated by receiving regular customer feedbacks; however, even a customer evaluation of the account manager will not prove whether the information was provided or not. One possibility would be to conduct regular tests on account managers on the products they offer.

4.3.7 Making changes to improve the situation

Following the analysis, the management of the bank has to decide whether it is necessary to make any of the changes suggested above. The implementation of any change will depend greatly on the totality of proposals for projects within the bank and their prioritization, as well as on the overall budget available within the year for capital expenditure CAPEX[178] purposes. If the management decides that changes in the credit card process are necessary and that it has high priority then a feasibility study and an estimation of the costs would be provided to management for decision-making.

Within the overall process it is clear that some improvements could be made. For example, a great deal of manual work has to be performed for a client to receive a credit card and any process that includes significant manual work is prone to errors. In this regard a feasibility study should be performed on how to automate the process to a greater extent. Once conducted - which would involve several units such as business and IT – the feasibility study containing the proposed changes and estimated project cost and the potential operational costs (OPEX[179]) would be presented to management. OPEX costs might increase for example due to a higher demand for resources and/or more maintenance work and training are required due to the changes planned. Such estimations would be provided by IT experts from sITA Solutions which, as mentioned earlier, is a subsidiary of Erste Group Bank. Although this is an independent entity, it is the main solution provider for any entity within the Erste Group Bank, which includes Erste Bank.

The account opening process is an integral bank operation, playing a key role in determining the direction of the company since it is, in effect, a barometer of customer confidence in the bank in delivering its services to them. The more people applying for an account, the higher is the level of confidence with the bank, which in turn implies growing revenues. Therefore changes that would improve the overall credit card opening process should have a good chance of being implemented.

[178] Capital expenditures (CAPEX) are expenditures made available within an organization to create future benefits by either buying assets or adding value to existing assets. Within the bank CAPEX refers to "change the bank".
[179] Operating expenditures (OPEX) are ongoing costs that an organization has to pay to run their business and/or systems. Within the bank OPEX refers to "run the bank".

Chapter 5: Discussion of Results

According to Checkland and Poulter (2006), and in contrast to other models such as OPM (Object- Process Methodology[180]), SSADM (Structured Systems Analysis and Design Method, Version 4), UML (Unified Modeling Language) and Unified Process, the Soft Systems Methodology is both effective and very efficient in dealing with a variety of elements constituting a very complex system[181]. To be precise, the SSM model usually supports both activities and processes whereas the Conceptual Model is used for representing the activities of the root definition[182]. This is a different characteristic to many other models. Wilson (2008) supports the distinctiveness of the Soft Systems Methodology and indicates that the resources can be described or represented in the root definition and at the same time, the activities modeled can be related to the definitions in the conceptual models[183].

A further distinct characteristic of the SSM is that quality is usually validated using or through defining measures for activities depicted in the Conceptual Model of the system that is under analysis. For the SSADM Version 4, quality is usually defined at the outset by a certain level of error rate and constantly seeking to check the system. On the other hand, quality in the context of the OPM is defined through using numerous numerical scores where each risk identified is assigned a numeric score[184].

However, compared with other models, it is acknowledged that SSM has its weakness in the analysis of hard facts. Other models such as SSADM version 4, UML and Unified Process are more suitable when such types of analysis are required. Despite this being a weak part of the system, Checkland and Poulter (2006) consider that the SSM model is capable of dealing with every element of the soft approach – a feature which other models do not possess[185]. In this regard, the SSM is best when used for its efficiency in improving one's understanding of the problem by looking at the whole picture, as demonstrated here in the credit card account opening process.

Another major difference between the SSM and all other models is the use of rich pictures to represent both the complexity of human affairs and the problem situation. As a result, it enables discussion of the problem situation with all stakeholders in an effort to obtain a clear picture of the problem situation. While it is also usually possible to get a good picture with other models, these do not provide the clarity derived from using SSM since there is no usage of the rich picture. This explains why the rich picture is important in understanding the problem situation.

[180] OPM is a modeling language often used as an approach for designing information systems by depicting them using object models and process models.
Peter Checkland & Jarred Poulter, (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers, and Students.
[182] Brian Wilson (2008). Soft Systems Methodology: Conceptual Model Building and Its Contribution.
[183] Ibid.
[184] Ibid.
[185] Peter Checkland & Jarred Poulter (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers, and Students.

In addition, with the SSM model, the stakeholders should be engaged in gathering the information for defining the problem situation through workshops[186]. These mark the distinction of the SSM model in relation to the other models commonly used.

As exemplified by the bank case study described in this thesis, it was possible to use the SSM model to perform a risk analysis although hard facts were not used for the analysis. Also, using the model enabled identification of the potentially desirable and feasible changes.

[186] Brian Wilson (2008). Soft Systems Methodology: Conceptual Model Building and Its Contribution.

Chapter 6: Conclusions

The aim of this thesis was to create a reference model for performing a risk analysis by using the SSM seven- step approach and applying it on a real case scenario to find out whether this approach is practical. Based on information provided within its earlier Chapters describing SSM and its applicability, it is evident that the model is effective inasmuch that it allows the user to determine the root cause for certain risks and the necessary changes that should be initiated in order to mitigate or prevent the risks identified. The great advantage of the model was that during the analysis it was possible to simplify the complexity of the human interactions involved and to derive the possible adverse consequences of those interactions by using the rich picture. As mentioned in Chapter 2, SSM can be used to identify and analyse complex problems where there might not even be a concrete problem description. This was exactly the case with the credit card account opening process, since there was no concrete or obvious problem when initiating the analysis. Instead, a problem situation was created and analysed, which led to the identification of potential risks which, if arising in practice, would result in a failure within the overall process. It was then possible to determine possible and feasible changes that could be made in order to prevent or mitigate the risks.

In the process of using the SSM methodology it became clear that key aspects were unlikely to be overlooked. This is due to the highly iterative nature of the process, particularly during stages one to four. Thus, while performing an analysis during one stage, another activity is discovered that was/is missing in the previous/next stage. For example, while creating a rich picture it was discovered that a further analysis had to be performed at the stage of exploring the problem situation and *vice versa*.

Throughout the thesis, attempts were made to answer various research questions, the most interesting being whether it was possible to use SSM for this specific risk analysis. This led to the conclusion that the SSM can indeed be used efficiently to both structure and to perform the risk analysis, as well as to carry out further planning. In fact, this case study confirms the validity of the statement made by Checkland and Poulter (2006) that SSM is an excellent approach for conducting a soft fact analysis since it was possible to analyze comprehensively both the problem situation and to identify prevention as well as mitigation strategies for the risks that came to light.

Nevertheless, some questions remain unclear. These relate to the seven stages of the model suggested for conducting a comprehensive risk analysis. Is it worth the effort to follow these seven steps to achieve the ultimate goal? On the one hand, being a seven-stage model with many iterations, the likelihood of overlooking any factor that could compromise the rigour of the risk analysis and subsequent actions in terms of prevention and mitigation are small. On the other hand, one could argue that the same results could be achieved by reducing or combining some stages.

Another unresolved question is whether a qualitative analysis is sufficient for this particular case study. While the qualitative analysis which formed the foundation of this thesis provided valuable results concerning risk identification, for certain risks there is no question that having quantitative data would have been highly advantageous. For example, when dealing with "breakdown of IT system", quantitative data would have made it possible to perform a more rigorous impact analysis for certain risks. Consequently, in the author's opinion the current approach used within the bank of performing both quantitative and qualitative analysis is optimal for analyzing processes and both establishing and, where necessary, implementing corrective measures.

Further work would be to create a fully-fledged model. The first step - in the form of a generalized reference model - was tested on the "credit card opening process" of the Erste Bank. The next step would be not only having a reference model, but to have a framework which would demonstrate in more details how the SSM can be used for risk analysis. In addition it would be interesting to compare results obtained here with those using a different methodology.

References

Andrew Hiles & Peter Barnes (2001). *The Definitive Handbook of Business Continuity Management.*

Asgary, A., & Mousavi-Jahrom, Y. (2011). *American Journal of Economics and Business Administration*, **3** (2): 307-315. Power Outage, Business Continuity and Businesses' Choices of Power Outage Mitigation Measures.
[Used as additional reference]

ASIS International (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.

*(*http://www.uschamber.com/sites/default/files/issues/defense/files/guidelinesbc.pdf*).*

Bank of Indonesia; Directorate of Accounting and the Payment System (2004). Study of down time risk and recovery time objectives for the bank Indonesia real rime gross settlement system.

Bjerke, Olle L. (2008). Soft Systems Methodology in Action: A Case Study at a Purchasing Department. University of Gothenburg, Sweden.

(https://gupea.ub.gu.se/bitstream/2077/10551/1/gupea_2077_10551_1.pdf).

Business Continuity Institute (2011). Dictionary of Business Continuity Management Terms. (http://www.thebci.org/glossary.pdf).

Cabinet Office (2006). Expecting the Unexpected. Business Continuity in an uncertain world. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61089/expecting-the-unexpected.pdf).

Capra, F. (1996). The Web of Life: A New Scientific Understanding of Living Systems. Anchor Books.

Casper Fire Department (2005). Developing a Government Continuity Plan to Ensure Survivability. (http://www.usfa.fema.gov/pdf/efop/efo36202.pdf).

Checkland, Peter (1981). System Thinking, System Practice. John Wiley and Sons.

Checkland, Peter (1999). Soft Systems Methodology, a 30 Year Retrospective. John Wiley and Sons.

Checkland, P. & Poulter, J. (2006). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers and Students. John Wiley and Sons.

Checkland, P. & Scholes, J. (1990). Soft Systems Methodology in Action. John Wiley & Sons.
[Used as additional reference]

Chen Peng. (2005). Improve the Method for Requirements Analysis on Commercial Information System. Blekinge Institute of Technology, Sweden.

(http://www.essays.se/essay/5344936589/).

Directorate of Accounting and the Payment System Bank Indonesia (2004). Study of Down Time Risk and Recovery Time Objectives for the Bank of Indonesia Real Time Gross Settlement (BI-RTGS) Systems.

(http://www.bi.go.id/NR/rdonlyres/BFE104F0-AB82-480B-8639 376BA5D2936/13361/kajianOperasionalBIRTGS_Engl.pdf).

Enzinger, Evelyn (2006). Entwicklung einer virtuellen Kommunikationsplattform mit SSM und Rapid Prototyping. Technischen Universität Wien.
[Used as additional reference]

Federal Financial Institutions Examination Council (2004). Business Continuity Planning, IT Examination Handbook.

(http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/GroupDocuments/whole.pdf).

Furnell, Steven, Katsikas, Socrates, Lopez, Javier, & Patel, Ahmed. (2008). Securing Information and Communications Systems: Principles, Technologies, and Applications (Information Security & Privacy*).* Artech House.

Erste Group Policy for Managing Operational Risk. (2012). Erste Group Operational Risk Control.

Hewlett-Packard Development Company, LP (2007). Assembling a Business Continuity Planning Team.

Hiles, A., & Barnes, P. (2001). The Definitive Handbook of Business Continuity Management. John Wiley and Sons.

Kollar, Dezso, & Jankowski, Adam (2013). Erste Group Operational Risk Control; Decentralized Operational Risk Management Guideline.

Lopez, Milton E. (2001). Soft Systems Methodology an Application to a Community based Association. Proceedings Fielding Graduate Institute Action Research Symposium.

(http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.7766&rep=rep1&type=pdf).

Mitroff, I. I. (2001). Managing Crisis before they Happen: What every Executive and Manager Needs to Know about Crisis Management. AMACON.

Monetary Authority of Singapore (2008). Internet Banking and Technology Risk Management Guideline.

(http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Commercial%20Banks/Regulations%20Guidance%20and%20Licensing/Guidelines/IBTRMChecklist.pdf).
[Used as additional reference]

O'Connor, J. & McDermott, I. (1997). The Art of Systems Thinking: Essential Skills for Creativity and Problem-Solving. Thorsons Publishing.

Spruit, Marcel, E. M. & Samwel, Paul H. (1999). *The International Federation for Information Processing,* **26**: 89-101. Risk Analysis on Internet Connection.
[Used as additional reference]

Snedaker Susan (2010), Business Continuity and Disaster Recovery Planning for IT Professionals.

(http://cdn.ttgtmedia.com/searchSecurityChannel/downloads/443_Disaster_04_(2).pdf)

Texas Department of Information Resources (2004). Business Continuity Planning Guideline.

(http://www2.dir.texas.gov/SiteCollectionDocuments/Security/Policies%20and%20Standards/bcpg.pdf).

The St. Paul Travelers Companies (2006). Strategy Guide for Business Continuity Planning. (http://www.aaaabenefits.com/business/forms/PBCSG.pdf).

Wilson, Brian (2008). Soft Systems Methodology: Conceptual Model Building and its Contribution. John Wiley & Sons.

Williams, Bob (2005) The Kellogg Foundation; Soft Systems. (http://www.kapiti.co.nz/bobwill/ssm.pdf).
[Used as additional reference]

Electronic Sources

BCM Media URL:

http://www.bcmpedia.org/wiki/Business_Continuity_(BC) [Accessed: June, 2009]

http://www.bcmpedia.org/wiki/Business_Continuity_Planning.(BCP) [Accessed: June, 2009]

http://www.bcmpedia.org/wiki/Business_Continuity_Management_(BCM) [Accessed: June, 2009]

http://www.bcmpedia.org/wiki/Risk_Analysis [Accessed: February, 2014]

http://www.bcmpedia.org/wiki/Business_Impact_Analysis_(BIA) [Accessed: February, 2009]

http://www.bcmpedia.org/wiki/Risk_Assessment [Accessed: June, 2009]

Business Dictionary

http://www.businessdictionary.com/definition/risk.html [Accessed: June, 2009]

Cisco Security Systems

http://www.cisco.com/ [Accessed: June, 2009]

Community Tool Box, Section 8. Identifying and analyzing stakeholders and their interests

http://ctb.ku.edu/en/tablecontents/chapter7_section8_main.aspx [Accessed: December, 2013]

Continuity Central; The international business continuity information portal URL:

http://www.continuitycentral.com/newtobusinesscontinuity.htm [Accessed: June, 2009]

http://www.continuitycentral.com/feature0607.html [Accessed: June, 2009]

http://www.continuitycentral.com/news04597.html [Accessed: June, 2009]

Disaster recovery journal URL:

http://www.drj.com/new2dr/w3_030.htm [Accessed: August, 2009]

Federal Financial Institutions Examination Council URL:

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program/testing-policy.aspx [Accessed: June, 2009]

Free Management Library URL:

http://managementhelp.org/systems/systems.htm [Accessed: August, 2009]

http://managementhelp.org/misc/defn-systemsthinking.pdf [Accessed: August, 2009]

Information Security Handbook

http://ishandbook.bsewall.com/risk/Assess/Risk/inherent_risk.html [Accessed: December, 2013]

ISACA.ORG

http://www.isaca.org/Journal/Past-Issues/2005/Volume-5/Pages/Outsourcing-A-Risk-Management-Perspective1.aspx [Accessed: December, 2013]

Manchester Metropolitan University URL:

http://www.business.mmu.ac.uk/mascla/resources/systemsthinking.php [Accessed: August, 2009]

http://www.business.mmu.ac.uk/mascla/resources/approaches.php [Accessed: August, 2009]

Oppapmers.com; Research papers and essays for all URLs:

http://www.oppapers.com/essays/System-Thinking-Example/151847 [Accessed: August, 2009]

Other URLs:

http://www.businessresiliency.com/evolution_history.htm [Accessed: June, 2009]

http://www.nr.no/~abie/RiskAnalysis.htm [Accessed: February, 2014]

http://www.ready.gov/risk-assessment [Accessed: June, 2009]

http://web.mit.edu/security/www/pubplan.htm [Accessed: June, 2009]

http://www.isss.org/primer/evolve2.htm [Accessed: August, 2009]

http://openlearn.open.ac.uk/mod/resource/view.php?id=183684 [Accessed: August, 2009]

http://www.cs.stir.ac.uk/~jco/CSC9T4/special/CSC9T4_SSM_2006.pdf [Accessed: August, 2009]

http://www.kernschweiz.ch/de/Anwenderberichte/09_Kern_2600_Kuvertiersystem/Sparkassen%20Zahlungsverkehrsabwicklung%20GmbH%20-%20Linz.pdf [Accessed: November, 2012]

TBI- Technology & Business Integrators

http://www.tbicentral.com/our-white-papers/business-continuity-planning-framework [Accessed: June, 2009]

Risk Glossary

http://www.riskglossary.com/link/operational_risk.htm [Accessed: November, 2012]

Wikipedia URL:

http://en.wikipedia.org/wiki/Business_continuity [Accessed: June, 2009]

http://en.wikipedia.org/wiki/Top-down_approach [Accessed: June, 2009]

http://en.wikipedia.org/wiki/Systems_thinking [Accessed: August, 2009]

http://en.wikipedia.org/wiki/Soft_systems_methodology [Accessed: August, 2009]

http://en.wikipedia.org/wiki/Che_Guevara [Accessed: August, 2009]

http://www.soopertutorials.com/technology/disaster-recovery/1590-risk-assessment-of-e-banking.htm [Accessed: August, 2009]

http://www.wholesalesolar.com/backup/4400-watt-home-battery-backup-system.html [Accessed: June, 2009]

http://17799.denialinfo.com/risk.htm [Accessed: February, 2014]

APPENDIX A – Risk Map

		Internal fraud		External Fraud			Employment Practices & Workplace Safety			Business Interruption & System Failure			
Stakeholder	**Functions performed**	Unauthorized activity	Internal fraud and theft	External fraud and theft	Credit fraud	Robbery	Discrimination	Sexual harassment	Unfair dismissal	IT system breakdown	Infrastructure breakdown	Slow operation of system	Inappropriate functioning of system
Account Manager	Product offer to customer						3	3	3				
	Legitimization check	5											
	Enter customer data		3							4	4	4	4
Pouvoir Holder	Pouvoir holder approval (check data)	4							1				
	Pouvoir holder sends application via internal post												
	Pouvoir holder sends electronic request to sIT for card production									2	2	4	3
sZV	sZV checks correctness of data			3									
	Send e-mail confirmation to Poviour Holder									4	4	4	4

sITs	Data electronically sent to MBU									2	2	2	2
MBU	Data preparation (chip/processor and magnetic strip)									5	5	5	6
	Card personalization (account number, name, etc)			5						5	5	5	5
	Data electronically sent to Austriacard									3	3	3	3
Austriacard	Designs card/produces card									3	3	3	3
	Produces PIN									5	5	5	5
	Provides Post Office with PIN			3									
	Provides Post Office with card			3									
Post Office	Sends PIN to customer			3									
	Sends card to customer			3									
Customer	Customer fills out application				4								
	Provides legitimization			4									

		Clients Products & Business Practices			Execution, Delivery & Process Management					Dependency Risk	Counterparty Risk
Stakeholder	**Process**	Incorrect advice to customer	Breach of bank secrecy	Improper business practice	Human processing error	Human error - wrong information to customer	Incomplete customer data input	Incomplete customer documents	Incomplete information provided to customer		
Account Manager	Product offer to customer	6	5	7		6			5	None	None
	Legitimization check				5			4			
	Enter customer data				7		3				
Pouvoir Holder	Pouvoir holder approval (check data)			3						None	None
	Pouvoir holder sends application via internal post				7			3			
	Pouvoir holder sends electronic request to sIT for card production				5		5				
sZV	sZV checks correctness of data			5	3					Medium	Low
	Send e-mail confirmation to Poviour Holder				5						

sITs	Data electronically sent to MBU				3					Medium	Low
MBU	Data preparation (chip/processor and magnetic strip)			8	6					High	Medium
	Card personalization (account number, name, etc.)			8	6						
	Data electronically sent to Austriacard				5						
Austriacard	Designs card/produces card			8	5					High	Medium
	Produces PIN			3	5						
	Provides Post Office with PIN			3	5						
	Provides Post Office with card			3	5						
Post Office	Sends PIN to customer			3	5					High	Medium
	Sends card to customer			3	5						
Customer	Customer fills out application									None	Low - High
	Provides legitimization										

APPENDIX B – Risk Analysis

Detailed Risk Analysis					
Risk Assessment			**Impact Analysis**		**Strategic planning**
Risk identified	**Rate likelihood of happening**	**Prioritization**	**Examine possible interruptions**	**Determine maximum allowable downtime**	**Reduce risk; Accept risk; Transfer risk**
Account manager not arriving to work	medium	low	Customer waiting in the queue and not being attended to	N/A	Attempt to reduce risk by recruiting additional account managers
Account manager does not know policy or credit card product	medium	medium	Account manager provides customer with wrong information or cannot answer all customer questions	N/A	Attempt to reduce risk by having regular workshops and examinations
Typing error	medium - high	high	The account opened would appear as if belonging to a another customer	N/A	Reduce risk by implementing greater automation
System failure	medium	high	No operation taking place at all	few minutes	Reduce risk by improving the network structure within the Erste Bank

N/A: not applicable

Lebenslauf und wissenschaflicher Werdegang

- Sep 1994 - Jun 2000: Vienna International School; Abschluss: International Baccalaureate Diploma und Österreichische Matura Äquivalents
- Sep 2002 – Jun 2005: BSc in Business Computing an der *Leeds Metropolitan University*; Bachelorarbeit: "Self-charging Robot".
- Sep 2006 – Jan 2009: Wirtschaftsinformatik an der *Universität Wien*
- Sep 2009 – Sep 2010: Zertifikat in „Applied Bank Management" an der Universität Wien
- 2014: Diplomarbeit für Wirtschaftsinformatik Studium: „The use of Soft System Methodology as a basis for the Analysis of IT-related Risk"