LAUREA

# Building the foundations for information and communications technology continuity management in a merger based company

Lalla, Markus

2009 Leppävaara

Laurea University of Applied Sciences
Espoo Institute

# Building the foundations for information and communications technology continuity management in a merger based company

Markus Lalla
Entrepreneurship and Business Operations
Thesis
May, 2009

**Laurea University of Applied Sciences**
Espoo Institute
Entrepreneurship and Business Operations
Master of Business Administration

**Abstract**

Markus Lalla

**Building the foundations for information and communications technology continuity management in a merger based company**

Year 2009 Pages 54

This thesis case study report describes how a new global company managed to build the foundations for a functional IT continuity management program and a framework for governance and resilience following a business operations merger of two major corporations. This involved creation of an IT continuity management program, whereby the objectives were to analyze industry best practices and the maturity of the current process and to give recommendations on how to move forward in the event of key program personnel not being available. The scope of case study is centered mainly on the beginning of the business continuity management program life cycle as defined in detail in the BS25999-1 standard. Therefore training and exercising are not discussed thoroughly.

This qualitative thesis begins with a description of the relationship between IT and business continuity management as well as the relevant terminology. For a company of any sort, it is important to collect immediate feedback on progress and to understand the reasons behind decision making, especially when two different business cultures are being merged. Data was collected through theme interviews, participant observation, and group discussions with various stakeholders and IT service management team members from IT services defined as business critical. The methods used are also presented along with an assessment of their suitability for this study.

The thesis focuses primarily on general aspects of IT continuity capability design and current global trends in continuity management. The actual program implementation is not reported in detail due to the confidential nature of this work in practice. The thesis is of value mainly to me and the company. It is also a useful benchmarking case for any organization with an obligation to ensure that enough IT recovery response controls are in place or planned to be implemented. Information about supplier chain risks caused by vendors and hosting partners who have a major role in IT continuity is also provided. Furthermore, it was discovered that internal dependencies and single point of failures extending beyond the core scope need to be monitored very carefully.

Keywords: business continuity management, IT continuity management, and disaster recovery

Supervisor: Seppo Leminen

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Laurea Leppävaara
Ylempi ammattikorkeakoulututkinto
Yrittäjyys ja liiketoimintaosaaminen

Markus Lalla

**Tietohallinnon jatkuvuussuunnittelun perustan luominen liiketoimintajärjestelyiden johdosta syntyneelle yritykselle**

Vuosi 2009 Sivumäärä 54

Tämä tapaustutkimusraportti kuvaa kuinka uusi kansainvälinen yritys rakensi toiminnallisen perustan tietohallinnon jatkuvuussuunniteluun kahden kansainvälisen yrityksen yhdistettyä liiketoimintojaan. Itse kehittämishankkeena oli rakentaa kyseinen jatkuvuussuunnittelun ohjelma sekä arvioida parhaita käytäntöjä, nykyprosessin kypsyyttä sekä antaa suosituksia tulevaisuutta varten mikäli keskeiset henkilöt jostain syystä eivät olisi käytettävissä. Aihe on rajattu pääsääntöisesti liiketoiminnan jatkuvuussuunnittelun prosessikaaren alkuun, kuten BS25999 standardissa asia on määritelty, joten kouluttaminen sekä harjoittelu jäävät tässä työssä vähemmälle huomiolle.

Kvalitatiivisen työn alussa kerrotaan tarkemmin liiketoiminnan sekä tietohallinnon jatkuvuussuunnittelun yhtymäkohdista ja kuvaillaan hieman historiallista taustaa tälle ajattelulle. Yritystoiminnan koosta ja toiminnan lajista riippumatta on tärkeää kerätä välitöntä palautetta organisaatiosta sekä ymmärtää päätöksentekoon vaikuttavia syitä, erityisesti kun kaksi erilaista yrityskulttuuria kohtaavat. Tiedonkeruun metodeina käytettiin teemahaastatteluja, osallistuvaa havainnointia sekä ryhmäkeskusteluja erilaisten merkittävien sidosryhmien jäsenten sekä informaatiotekniikan palveluiden vastuuhenkilöiden kanssa. Erityisesti kohderyhmänä oli kriittisiksi luokiteltujen palveluiden henkilöstö. Käytetyt tiedonkeruumenetelmät on kuvattu sekä arvioitu näiden soveltuvuutta tähän tapaustutkimukseen.

Tapaustutkimus käsittelee tietohallinnon jatkuvuussuunnittelun toipumiskykyä ja kansainvälisiä suuntauksia melko yleisellä tasolla. Varsinaisen toteuttamisen raportointi jätetään tarkoituksella vähemmälle aiheen luottamuksellisuudesta johtuen. Työn suurin arvo syntyy tekijälle itselleen sekä toimeksiannon tehneelle yritykselle mutta työ toimii myös hyödyllisenä vertailukohtana organisaatioille, joiden tulee täyttää velvollisuutensa informaatioteknologian palauttamisessa sekä näiden erilaisten ratkaisujen toteuttamisessa. Lisäksi lukijalle selvitetään toimitusketjun riskien merkitystä jossa tavaran- ja palveluntoimittajilla on suuri merkitys. Lopuksi havaittiin myös, että on tärkeää arvioida sisäisiä riippuvuusriskejä ja tunnistaa mahdolliset toiminnan täysin seisauttavat ongelmakohdat.

Asiasanat: liiketoiminnan jatkuvuussuunnittelu, tietohallinnon jatkuvuussuunnittelu sekä palautuminen

Ohjaaja: Seppo Leminen

EXECUTIVE SUMMARY

*“Anything that can go wrong will – at the worst possible moment”.*

*Finagle's Law of Dynamic Negatives*

Company IT Continuity Management program ensuring resilience and supporting business interests in the partnership

In the modern age of complex computing and IT architecture requirements, it is more likely than ever before that something unlikely will happen, and may even happen at the worst possible moment you can imagine. This statement is not influenced merely by the negative aspect of human nature and an agenda to gain executive support, but by genuine concern borne out of realism. It is not just a question of if something will happen, but when, and we can see evidence of this in the news every day all over the world. We should have already learned from history, but for some reason the human memory can be really short. In the case of business dependencies where there are faults in supply chain risk management, the absence of only one key employee may lead to a widespread disaster in mission critical activities affecting business survival. Gaining business approval for well thought out IT continuity plans may save the organization a huge amount of time, which in turn translates into money.

The company IT is taking this change of thinking very seriously and has taken decisions in identifying and evaluating the impact that business has on mission critical applications, platforms, end user services, and data center dependencies hosted mainly by carefully chosen providers. With this foundation and common process risk management, the company is confident that it can help all customers and stakeholders to grow and become successful with us. The company IT continuity management foundation follows global best practice in business continuity management. Together we rise, succeed, and avoid falling. We want to be viewed as a trusted and responsible business partner.

The company IT continuity is organized as a five level maturity cycle, which is managed and monitored by the program management layer. The initial phase involves acquiring an understanding of the business by conducting a business impact analysis with relevant business owners, followed by more detailed risk analyses. The second phase involves identifying and creating possible options for recovery solutions. The third phase is the actual continuity implementation phase, which involves planning and ensuring that the solutions are in place. In the fourth phase, the focus is on ensuring that everybody who has a role to play in the event of a critical incident or disaster knows the correct procedures. Last but not least, the continuity creation phase involves exercising and testing – critical evidence gathering to ensure that all of this preparatory work is actually functional. It also involves following the maintenance and yearly routines after exercising to ensure IT continuity resilience over time.

To manage all of this, an IT continuity manager has been appointed to ensure that the mission critical IT processes are covered by planning, that there are people with the necessary skills in IT units, and that suppliers also know their role in the business risk chain. Continuity is part of IT quality assurance along with IT risk management and IT security management, and together they form a strong alliance in business partnerships.

In a business merger of two leading telecommunication corporations, the company has been given a unique opportunity to improve operational excellence. The company has been successful in gathering the best solutions from both of the parent companies and in implementing only the strongest methods in the new environment. The parent companies have decades of global know-how in incident management between them. The customers are in key focus areas, and this is taken very seriously by the organization.

This case study thesis report describes how company IT continuity manager guides his organization through continuity planning first two steps with mission critical IT services. During this process are gathered best practices, confronted challenges and prepared for the next remaining continuity planning phases. Additionally it is ensured that nothing critical is missed that should need immediate corrective actions. Therefore by doing this is created a broad documentation that by familiarizing oneself with, other companies can avoid unnecessary practical challenges.

EXECUTIVE SUMMARY

*“Kaikki mikä voi mennä vikaan, yleensä menee ja huonoimmalla mahdollisella hetkellä”.*

*Finaglen laki*

Yrityksen tietohallinnon jatkuvuussuunnittelu varmistamassa sekä tukemassa kumppanuutta

Nykyaikaisen monimutkaisen tietohallinnon sekä IT arkkitehtuurin aikana on hyvin todennäköistä, että jotakin epätodennäköistä tapahtuu ja vieläpä pahimpaan mahdolliseen aikaan. Tämä toteamus ei ole saanut vaikutteita ihmisluonnon negatiivisuudesta van se on lähinnä huolestunutta realismia. Kyse ei ole siitä jos jotakin tapahtuu vaan lähinnä koska sillä näemme tästä todistusaineistoa jokapäiväisissä uutisissa ympäri maailman. Luulisi meidän jo oppineen jotakin historiasta, mutta jostakin syystä ihmisen muisti on kovin lyhyt. Yritysten riippuvuuksista ja toimitusketjun haasteista puhuttaessa jopa yhden avainhenkilön poissaolo voi johtaa elintärkeisiin toimintointojen kautta yhä kasvavaan katastrofiin, joka voi jopa uhata koko liiketoiminnan olemassaoloa. Hyvin rakennetut sekä hyväksytyt tietohallinnon jatkuvuussuunnitelmat voivat säästää koko organisaatiolle paljon lisäaikaa jota voi samalla ajatella rahana.

Yrityksen tietohallintoyksikkö ottaa tämän edellä kuvatun ajattelun hyvin vakavasti ja on päättänyt tunnistaa sekä arvioida liiketoiminnan vaikutukset elintärkeissä IT sovelluksissa, alustoissa, loppukäyttäjäpalveluissa sekä konesaleissa, joita osana hoitaa myös huolellisesti valitut palveluntoimittajat. Tätä perustaa vasten sekä yleiseen riskienhallintametodologiaan nojaten yritys on luottavainen, että sen asiakkaat sekä yhteistyökumppanit voivat kasvaa ja menestyä kanssamme. Yrityksen tietohallinnon jatkuvuussuunnittelun perusjalka noudattaa kansainvälisiä parhaita käytänteitä. Yhdessä me nousemme, menestymme sekä vältämme kompuroimista. Yritys haluaa muiden näkevän sen luotettavana sekä vastuullisena liikekumppanina.

Yrityksen tietohallinnon jatkuvuussuunnittelu on organisoitu viisiportaisella kypsyysmallilla, jota johdetaan keskushallinnosta käsin. Ensimmäinen vaihe pitää sisällään liiketoiminnan omistajien yhteistyössä tehtävän vaikutusanalyysin, jota seuraa syvällinen riskien tunnistaminen sekä analysointi. Toisessa vaiheessa tunnistetaan erilaiset palautumiskeinot sekä rakennetaan käytännön järjestelyt. Kolmas vaihe on varsinaisen jatkuvuussuunnitelman rakentaminen, jonka aikana myös varmistetaan ratkaisuiden olemassa olo. Tämän jälkeen neljäntenä vaiheena keskitytään varmistamaan, että jokaisen nimetyn vastuuhenkilön rooli sekä oma toiminta tapahtumasta toipumiselle on kristallinkirkasta. Viimeisenä vaan ei vähäisimpänä, varmistetaan harjoittelemalla, että kaikki valmisteleva työ todellisuudessa toimii suunnitellun mukaisesti. Tämän jälkeen tätä kaikkea ylläpidetään vuosirutiineilla.

Tämän hallinnoimiseksi yritys on nimennyt tietohallinnon jatkuvuussuunnittelua johtamaan päällikön, jonka tehtävänä on varmistaa, että elintärkeät prosessit on huomioitu, näille löytyy kyvykkäitä ihmisiä sekä yhteistyökumppanit tietävät oman roolinsa liiketoimintariskien ketjussa. Jatkuvuussuunnittelu on osa laadun varmistamista yhdessä riskienhallinnan sekä tietojärjestelmäturvallisuuden kanssa. Yhdessä nämä muodostavat vahvan liiton yrityskumppanuudelle.

Kahden johtavan tietoliikennealan yrityksen yhdistyessä yrityksellä on ainutlaatuinen tilaisuus parantaa operatiivista laadukkuuttaan. Yritys on menestyksekkäästi kerännyt parhaimmat ratkaisut molemmista emoyrityksistä sekä vienyt vahvimmat keinot uuteen toimintaympäristöön. Emoyrityksillä on yhdessä vuosikymmenten kansainvälinen tietotaito ongelmien hallinnoimisessa. Asiakkaat saavat erityisen huomion ja heidän hyvinvointinsa otetaan erittäin vakavasti.

Tässä tapaustutkimuksessa kerrotaan kuinka tietohallinnon jatkuvuussuunnittelun päällikkö johdattaa organisaationsa elintärkeiden tietojärjestelmien vastuuhenkilöt läpi jatkuvuussuunnitteluprosessin ensimmäiset kaksi vaihetta. Prosessin aikana kerätään talteen hyviä opittuja käytäntöjä, koettuja haasteita sekä valmistaudutaan seuraaviin vaiheisiin. Lisäksi työssä varmistetaan, että mitään merkittävää ei ole unohtunut, mikä vaatisi välittömiä toiminnan korjaustoimenpiteitä. Työstä syntyy näin ollen kattavasti dokumentoitu prosessi, johon tutustumalla muut vastaavassa tilanteessa olevat organisaatiot voivat välttyä turhilta käytännön haasteilta.

Table of contents

# Introduction

## 1.1 Background

Business Continuity Management terminology changed remarkably following the terrorist attacks on the World Trade Center in New York on September 11th, 2001. This was also a turning point in IT continuity management, where disaster recovery was the key element. As a result of these terrible acts of terrorism, companies clearly saw the connection between business survival and information technology. 'Disaster recovery' as a term referring to IT related resilience activities was changed by the continuity industry to 'IT continuity management', which more clearly indicates the crucial dependency with mission critical business activities. This was at the same time a huge opportunity for IT organizations not only to better understand business needs, but also to really plan in cooperation with the recovery solution focus areas.

The direct economic effect of the New York attacks was also seen in the London 7/7 bombings. They had a huge impact on the way in which we see IT continuity in supporting business operations. These two aspects really need to work together. IT has a major role in business continuity management, but at the end of the day it is only a support function that does not bring in any money itself. Smith (Edit. Hiles 2007, 206) says that we have progressed from IT-centric disaster recovery, through the process of business continuity planning to the age of information availability, where an organization's key people and critical information must remain connected at all times.

Business and IT continuity management have many largely similar definitions, all trying to clarify same problematic schema. However, it is not only the definitions that are important, but also a real understanding of the activities put in place. I have provided the best definitions I can think of here, which belong to only globally certifiable standard in place at the moment, namely BS25999 from the British Standards Institute. These definitions and requirements are the most important in the western telecommunications industry because they are most often referred to and used with many major suppliers and operators to align and compare resiliency efforts.

BS25999 defines Business Continuity Management (BCM) as a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. IT continuity management is supporting the overall business continuity management process by

ensuring that the required information technology and services can be physically and logically recovered within required and agreed business timescales. The word ‘contingency’ is also often heard and referred to but most of the standards use ‘continuity’, so this is the only term used in this thesis.

The same British institute also has an ICT related standard BS25777. It says that the IT continuity is a capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable predefined level. Disaster recovery is defined as the activities that are invoked in response to a disruption. These are described in more detail in the next chapter.

Myers (1999, 4) looks back at the history of the business world where computer technology has skyrocketed from tabulating historical accounting transactions to the real time assimilation of complex analog and digital data, and the formulation and execution of process control procedures with unheralded quality assurance. Kirvan (Edit. Hiles 2007, 194) sees that companies have become increasingly dependent on information systems not only to conduct business, but also to remain competitive. The stakes involved in a communications system outage have risen. Snedaker (2007, 3) says that business continuity planning came to the forefront in the late 1990’s as businesses tried to assess the likelihood of business systems failure on or after January 1, 2000.

According to Graham (2006, 9), only once an organization has analyzed its business and understood its risks, can it design and implement an effective approach to business continuity management and then construct and implement affective and efficient business continuity plans. Snedaker (2007, 13) says very directly that failing to plan is planning to fail. When we are young, we think nothing bad can ever happen to us. When we are older, we may think we can play the odds. Myers (1999, 48) says that regardless of the size of your company, it has a 40% to 50% chance of going out of business as a result of a natural or a manmade disaster. Unfortunately this is not clear to everybody and knowledge sharing of the urgency is mandatory. For the sake of stakeholders, all organizations need to look somehow into the future and make sure that tomorrow cannot rely only on luck; business continuity is not about luck management. Convincing others and the list of those to whom continuity needs to be sold is impressive: senior management, audit committee members, internal auditors, outside auditors, division managers, department heads, first-line supervisors, and vendors.

IT has a significant role in enabling business proceed efficiently and without too much manual manpower. Smooth and reliable IT operations supporting business demands have been the cornerstone of growth for many companies worldwide. The common objective is to provide customer satisfaction through continuous business operations. Information technology is

supporting companies in business continuity management by ensuring that identified critical IT services and sites can be recovered from disabling failures within agreed timeframes. Unfortunately, modern complexity has led to service availability issues and sooner or later even to critical incidents threatening the whole continuity of business.

There are many external forces driving organizations at every level to provide input in continuity planning. There are, for example, national regulatory requirements, internal controls, requirements relating to insurance coverage, customer demands, and pressure to deal with competitor benchmarking. Furthermore, it is easy to implement business continuity management for some critical functions, but at the beginning of the program it is necessary to define the objectives and the quality aspects of the design. It can be said that IT continuity capability is at a good level when the company can plan and respond to incidents in order to continue IT services at a predefined level.

Requirements in relation to IT continuity capability normally increase along with changing demands over the years of company life cycle management. I had a unique opportunity to start activities for building IT continuity resilience for a new global company merged from two major global corporation business elements. Business mergers are not rare, but this global merger provided an opportunity to begin IT continuity program creation from the ground up by combining the best working methods from both parent corporations.

This thesis will document best practices and common issues with learning aspects for those companies who are starting out in the management of IT continuity capability in business operations of any sort. The approach adopted is not only limited to corporations, but can also be applied to government and community organizations. The lessons learned are not necessarily unique, since continuity management is not considered as a specialist science, but rather practical thinking. This document ultimately aims to show the reader that motivated people with sufficient skills and resources are the key to successful continuity program creation.

It might take only one large scale disaster to shut down the business, but managing these rare effects may also present an opportunity. By monitoring your business environment you can benefit when your competitors are struggling, since you most likely share the same customer pool. One of the main drivers for any business continuity program is the need for reliable corporate governance and infrastructure protection. The reporting obligations under New York Stock Exchange (NYSE) Rule 446 for business continuity are worth mentioning in this context, as it requires organization to establish and maintain BCPs relating to an emergency or significant business disruption. References to standards such as BS25999 and ISO17799 on information security are often seen in global agreements with customers. Customers also

expect network resilience and redundancy with a certain level of service delivery. The most challenging driver is the debate concerning responsibility in case something extraordinary should happen. The dependencies and risk transfer might lead to all partners failing.

Force majeure is also frequently mentioned in commercial agreements, but business continuity goes further. Vendors and suppliers simply can't raise their hands in the event of disasters, but must instead be ready to act as planned beforehand. An incident recovery solution developed in advance may differentiate businesses from their competitors, but planning needs resources. Executives should look towards partnerships that have the competitive edge of being able to manage possible disasters.

## 1.2 Objectives

According to Ellet (2007, 13), a case without a significant issue has no educational value and therefore it can be assumed that every case deals with something important. It is difficult to see anything more valuable for any company than ensuring continuous business operations. Educational value to a company or not, there is a need to understand IT continuity management more deeply.

The objectives for this thesis are to document the current status of IT continuity management after a merger, to gain an understanding as to whether the decisions made so far have been correct and effective, and to accumulate lessons learned along with key focus areas for future activities and development. The thesis document should also strike a balance between being easy to read for those who not experts in business continuity management while at the same time being of value to fellow professionals.

The research element involves finding out and clarifying what should have been done differently in implementing the IT continuity management program, and determining whether any short term action is required in order to ensure proper governance creation in future. The hypothesis is that something that could have been done better, and for that we need to take corrective action.

In the context of a broader continuity concept, my personal objective as a responsible continuity manager is to document my own experiences, since there will always be a need in the future to understand the past, even in a new company that I represent. The secondary objective is to conduct a critical self assessment, as I am doing research into the results of my own actions. Given the somewhat confidential nature of the topic, the written document needs to be kept brief.

# 2 Business continuity management

## 2.1 Business continuity management as a process

Roessing (2002, xi) sums up the challenge in business continuity management: “Businesses should take adequate precautions to ensure that no going concern issues arise from crisis and disasters”. This is also the underlying statement in this thesis based on the defined objectives. He also continues that “In a sense, BCM means reading the future or trying to safeguard an organization against unforeseen events”. Isn’t this a nice confusing starter for a case study? How can we do anything about something we know so little about in the present? Before exploring more deeply under the surface of BCM, I would like to define the approach for this concept and explain how it is used in this document.

The previously mentioned British standard BS25999 establishes the process, principles, and terminology of business continuity management. The purpose of this standard is to provide a basis for understanding, developing, and implementing business continuity within an organization and to provide confidence in the organization's dealings with customers and other organizations. It also enables the organization to measure its BCM capability in a consistent and recognized manner. This standard provides a system based on BCM good practice. This standard is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization; from those with a single site to those with a global presence; from sole traders and small-to-medium enterprises to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation.

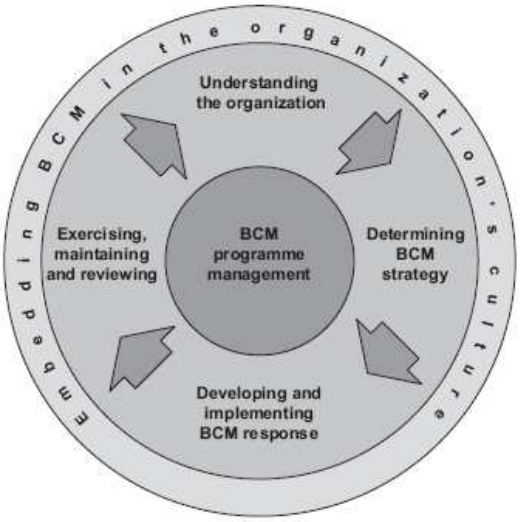


Figure 1: BS25999-1 Business continuity management life cycle.

It is actually not a unique idea to put continuity management into a process model and framework, but this is currently the only actual certifiable BCM standard. The reason for choosing this standard is already presented in the background chapter. At the center of life cycle (Figure 1) lies BCM program management, which is also the starting point for this post merger IT continuity work. Once the basics have been defined, an attempt to gain a better understanding of the organization is made through business impact and risk analysis. This then continues with determination of the most cost effective solutions based on the defined requirements for prioritized mission critical processes and services. Only when the basics are in place can you organize yourself effectively and create an actual continuity plan with adequate resources. However, you need to go even further and make sure that everybody knows and understands their roles, and provide training where necessary. Last but not least, before any maintenance work you should put the plan into practice and test that it works, as without this element there is no evidence that the plan will function should something bad happen.

## 2.2 Concepts and keywords

Erola (2000, 42) states that risk is a natural part of any business and therefore risk management is the most important aspect of management. When the risk occurs, business operations need to continue. Based on BS25999 (2006, 6), risk management seeks to manage risk in relation to the key products and services that an organization delivers, and business continuity management is complementary to the framework that sets out to understand the risks and the consequences. Erola (2000, 75) also says that overall risk management definitions and practices are part of the company risk management process, and it is precisely this point that makes life challenging, as every company is unique.

Continuity standards and global best practices have many similar definitions and the main ideologies are very closely related. In general, business continuity management is the guiding factor that is supported by IT continuity planning and more detailed disaster recovery planning in order to achieve corporate governance and resilience in relation to different stakeholders. Risk management theories are based on a discussion of probabilities and the simple mathematic understanding that there is no zero. There is a basic need to go beyond luck management, which is not a factor we can rely on.

### 2.2.1 Business continuity management

The British Standards Institute (BS25999-1, 1) defines business continuity management as a holistic management process that identifies potential threats to an organization and the

impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

### 2.2.2 IT continuity management

The British Standards Institute (BS25777, 6) defines ICT continuity as the capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable predefined level.

### 2.2.3 IT disaster recovery

Kirvan (Edit. Hiles 2007, 194) says that IT departments have long recognized the importance of contingency planning and disaster recovery for their computers and related subsystems. According to Snedaker 2007, 4), disaster recovery is part of business continuity, and deals with the immediate impact of an event. She adds (2007, 12) that disaster planning is about recovering after an event, but business continuity planning is not just about recovering from outages of key technical components, it is a way of looking at and managing business.

Gregory (2008, 9) says that the objective of DR planning is the survival of an organization. Closely linked to the IT continuity definition of the British Standards Institute (BS25777, 6), disaster recovery refers to those activities and programs that are invoked in response to a disruption and are intended to restore an organization's ICT services.

## 3 Methodology

### 3.1 IT Continuity management in a case study context

The nature of this thesis is qualitative case study research in which the empirical data collection methods chosen are theme interview, group discussion, and participant observation. I have chosen these methods to fit the objectives set by my organization and due to the fact that quantitative research was not allowed. As the company in question is created from a business merger, there was pressure to use the time allocated wisely and detailed large scale data collection from key personnel was not an option. Furthermore, I believe that given the current state, a quantitative approach would not reveal as many interesting findings in relation to my defined objectives as the chosen method will.

Case study as a methodology has its very own challenge on science and I feel it is necessary to point out from the very outset that I am not trying to be a scientist, but rather a practical specialist in a unique field of expertise. Despite this defense in reasoning, Metsämuuronen (2000, 62) states that a good qualitative thesis includes the same elements as good quantitative research; based on the report a reader must gain an understanding of how the information is gathered and how reliable the information is. Yin (2003, xiii) supports the use of case studies but also understands that the method will be challenged from rational perspectives, and that the insights resulting from case studies may be underappreciated.

I am not trying to spoil the reader experience – research is, after all, not a detective novel – but data collection presents a challenge due to the two year time line in this research. I am also placing the case study into the theoretical framework of business continuity management and empirically testing it against unusual merger based circumstances. I have chosen this approach due to the defined objective to create to create a fit for purpose solution aligning company expectations. Tying into this background, Gerring (2007, 66) says that case studies are more useful when the purpose of the research is hypothesis generating rather that hypothesis testing and when internal validity is given preference over external validity. Metsämuuronen (2000, 14) adds that qualitative approach is especially appropriate when we are interested in individuals and situations that are natural and cannot be tightly tested.

Creating a framework for the actions and decisions taken so far is also a very rewarding experience. I should also at this point explain that the expectations in relation to this MBA level in applied sciences, which is still new in Finland, are based on a bringing together of studies and business to create something new. At the end of the day I am only responsible for myself.

### 3.2 Theme interview

Hirsjärvi (1997, 204) divides interviews into structured, theme, and open interviews. For this case study data collection method, I chose a theme interview where the exact theme was obvious, but without formal questions or any particular order for these. This gave the researcher the freedom to steer the discussion towards the correct context and to evaluate reliability.

Theme interviews were used mainly for gathering stakeholder expectations in relation to a variety of subjects and for obtaining immediate feedback from the service management teams in relation to their commitment and resources for achieving the set targets. The theme was the life cycle management of IT continuity management as described later in more detail in Figure 1. Structured forms were not used, but the interviewer made notes during the

interviews. The method suited the theme of the case study well and each interview was unique. The interviews were not recorded because it was felt that this would jeopardize their openness. The situations were very informal and gave a sense of confidentiality, and all the parties seemed to get something out of the situation.

The reason for choosing this method was to collect the IT continuity planning details needing focus and to understand the associated challenges. Theme interviews were conducted by collecting stakeholder expectations and interviewing the IT service managers responsible for these actions. Yin (2003, 89) says that interviews are essential sources of case study information. Having these two aspects in mind, i.e. stakeholder expectations and IT service manager interviews, the people were chosen simply by doing a stakeholder mapping and by identifying the IT critical services within the company continuity scope.

IT service manager interviews were conducted after training sessions for the setting of objectives, business impact analysis, risk analysis workshops, and follow-up meetings for recovery response solution planning. Stakeholder expectations were mainly gathered during the BCM policy creation process (Appendix 1), but also in the course of the annual process for setting IT continuity specific objectives. Furthermore, as the most meaningful stakeholder had their say after the business impact analysis, the objective was also to gain support, understanding, and commitment for capabilities beyond the SLA.

Method pros

Yin (2003, 86) lists the strengths of interviews as being able to focus directly on the case study topic and to provide perceived causal inferences. Hirsjärvi (1997, 201) mentions that the great advantage compared with other data collection methods is that it is possible to quickly change certain aspects depending on the situation and interviewees. This was proven in practice, with a lot of new ideas created and new ways of thinking proposed. The IT continuity program objectives were also changed several times during the case study and a better understanding of service management teams was gained.

I believe this method was the best choice for this case study and a good way of collecting information. The interviewer was really able to steer the discussion and respond accordingly if the overall atmosphere was negative or positive. The results were appropriate, and with relatively informal questionnaires service managers gave valuable information as to where it necessary to focus in order to best support them in fulfilling their responsibilities. The results and key findings are described in the next chapter, which deals with building an IT continuity management program.

Method cons

Yin (2003, 86) also refers to weaknesses in inaccuracies due to poor recall and reflexivity, meaning that the interviewee gives the answer that the interviewer wants to hear. Hirsjärvi (1997, 202) also says that the interviewee may find the situation threatening or even frightening. Responses were also affected by the workload of service managers and business expectations in relation to actual recovery objectives given the reality of computing capabilities and system changes already identified.

The main challenge was the amount of time needed, as several interviews were needed in order to get a good understanding of the overall situation. In addition, more information was available when there was more than one person present. By this I mean that there were other people from the service management team and not only the service manager. In the absence of any quantitative information, I am not able to make reliable conclusions with regard to the differences between employees with different parent company backgrounds.

Managing theme interviews requires a significant amount of concept knowledge, which is not feasible in short research processes. Furthermore, to have this knowledge in an IT continuity concept, the interviewer must have a relatively long history in IT continuity management related activities. It is also worth mentioning that compared to formal questionnaires, the interviewee may not be completely honest in response to questions being asked by a stranger. This is especially meaningful when the parties do not come from a similar background and there is always a risk of cultural misunderstanding in a global company.

## 3.3 Participant observation

Hirsjärvi (1997, 213) says that it is typical in participant observation that the researcher participates in activities on their terms. Research cases are usually field studies and the researcher often tries to be part of the group in scope. This doesn’t just mean physical participation, but also the fact that the researcher is trying to share knowledge with the group and step into their cultural, symbolic, and language world. In most cases there will be a role for researchers. Participation can vary from total to partial participation.

Based on Hirsjärvi (1997, 211), observation can be very systematic and clearly defined, or it can be totally free and part of the natural behavior and activities. In this kind of research you have to be prepared to be flexible due to changing business environments and strategic focus areas. Due to lack of resources and time, it is not often advisable to use highly systematic and clearly defined models.

Participant observation is one of the most challenging ways of doing research. Bell (2005, 187) states that when researching one's own organization, the familiarity of the personalities, strengths, and weaknesses of colleagues may cause the researcher overlook aspects of behavior which would be immediately apparent to a non-participant observer seeing the situation for the first time. She also says that despite criticism of the method due to a lack of precise, quantifiable data, researchers are able to observe changes over time.

The focus of the participant observation in this case study was on the work of service managers in IT continuity planning. This means observation of the IT service management team members in continuity related training sessions, business impact analysis, risk analysis, and follow-up meetings. The main reason for choosing this method was to closely analyze the behavior of service management team members in order to secure commitment for IT continuity planning. By identifying the persons who tend to be against the program, it is easier to understand the reasoning if something is not proceeding as promised. It also gave more depth because of a history of similar activities conducted in one of the parent companies.

Method pros

Yin (2003, 86) lists the strengths of participant observation as the covering of events in real life and context as well as the gaining of an insight into interpersonal behavior and motives. Hirsjärvi (1997, 209) describes the benefits of the method as being able to gather immediate and direct information on the actions and behavior of individuals, groups, or organizations. An additional benefit is the low cost, as participation takes place during normal activities and analysis is performed later by the researcher.

It was positive to see in practice how service management teams reacted to and managed the defined objectives. Training former company employees who were not familiar with this concept was also a challenge. In my previous organization these IT continuity activities were part of daily business and were self evident. Time was not a factor when this case study took two years.

Method cons

Yin (2003, 86) lists the weaknesses of this data collection method as being time-consuming and biased due to investigators' manipulation of events. Hirsjärvi (1997, 210) also mentions that the observer may cause a distraction and even change the course of the situation. The fact that I am the only full time IT continuity management resource in the company CIO's organization office and the lack of any actual operational responsibilities proved to be

somewhat challenging. This was one of the reasons why I did not enough authority to push things forward in some cases, since task allocation was performed for the respective line functions and IT solution units.

### 3.4 Group discussion

Flick (2006, 191) says that group discussions are used as an explicit alternative to open interviews and unlike the group interview, the group discussion stimulates a discussion and uses its dynamic of developing conversation in the discussion as the central source of information. I also chose this method mainly to save time and money instead of interviewing groups of already very busy people.

This method was used after each separate service management team training session to gain their commitment and understanding in relation to the issues and obstacles concerning actual implementation. This proved to be a really good supporting method for participant observation with instant results. The disadvantage lay in the fact that this was not always possible due to time factors. Additionally, this was not giving as good results in cases where the workshops were held via phone conference. It was noticed that open discussion is only achieved when sitting in the same room with the group being analyzed. It can be concluded that at regional level there is more planning commitment in locations where specialist continuity support is available.

## 4 Building IT continuity management

Snedaker (2007, 11) says that disasters can result in enormous losses with respect to financials, investor confidence, and corporate image. These losses and legal challenges can have a small, short term impact but more often than not, they have a significant, long term impact, and in some cases imperil the existence of the company. So there is simply a need to implement control mechanisms to proactively mitigate the risks and prepare for the worst to survive to some level if something happens, but how can we do this to meet stakeholders' expectations?

Heng (2004, 10) says that there has been a move to take business continuity a step further to become a fully fledged management discipline – to take the business continuity ethos and look at all aspects of the business with the aim of actively managing the continuity of the business so that all its systems and processes operate at a continuously constant level. The company has an approved BCM policy (Appendix 1) where BS25999 is the best practice to be followed and what IT needs to support. A decision has also been made to follow information security standard ISO77999 and the ITIL framework, both of which have requirements in

relation to IT continuity management. The scope of this thesis lies in the early stages of the BCM life cycle described in Figure 1.

## 4.1 Where are we at the moment or where do we believe we are?

This section is structured according to the life cycle described earlier in order to make it easier for the reader to follow. The focus is primarily on the early stages of the life cycle because this is what we can really be sure is being implemented. Following this is merely a dialog on what is in place for the next steps in the IT continuity program, e.g. continuity planning and instructions on managing tabletop exercises and recovery testing.

Nobody can be absolutely sure if everything is taken care of, but by following the process we have clearer visibility that can be reported as maturity and capability. IT is not a blind organism and a large number of required elements are already in place; the key message is that we need to gather those bits and pieces together to gain the trust given to us by the stakeholders. Documentation is necessary and this is also one of the objectives of this thesis. Beyond this thesis time line, most of these systems were already tested in real life prior to the merger and it is especially beneficial to see how they work in the new environment when building IT continuity awareness and capability from the ground up.

One of the key goals in the company after the merger was to find the best solution, adapt it, and simply to make things happen. This made IT continuity program creation really challenging since there was very limited expertise available. I was the only full time employee in the area of IT continuity and the legacy was a heavy burden. The best solution was to adapt the already known and proven IT continuity management system from the past. It also made the decision making process easier knowing that most of the other company employees in this field were not available. There wasn't enough time for learning and developing new ways of working, but instead just for making things happen.

The main things inherited from the parent companies were the recovery solutions already in place, since these were a long time running outside of the company's own network segment. There were also many disaster recovery processes in place and many continuity plans needing only immediate action and updating upon ensuring people with deputies were in place. There was therefore a lot of continuity related activity to be consolidated and organized.

### 4.1.1 Development of an IT continuity program

IT leadership support and organization

Kerko (2001, 27) gives a clear guideline that the change starts with management through active participation. He (2001, 26) also specifies what is actually meant by management commitment:

- Visible and strong commitment
- Informing and participating
- Open communication
- Clear organization
- Setting of demanding objectives
- Definition of roles and responsibilities
- Acting as a role model
- Management that aims on changing attitudes
- Visibility in workplace

IT continuity organization is defined in an operating model, which describes the roles, responsibilities, and principles of IT continuity management in the company. The document is owned by the CIO and is updated and maintained in the organization in which I operate. The operating model rules, as well as the guidelines derived from them, are mandatory throughout the company as minimum requirements. The purpose of this document is to ensure a sufficient level of continuity management to meet Service Level Agreement, customer, and regulatory requirements, to support the achievement of IT objectives by minimizing direct or indirect damage, and to accelerate the recovery from a possible disaster and set minimum requirements for IT continuity management.

The objective of IT continuity management in the company is to provide customer satisfaction through continuous business operations. IT continuity management is a combination of proactive risk identification and control and reactive response capabilities. It puts into place processes and procedures to effectively respond to events that cause interruption in the business processes.

In the event of a disaster, company critical IT services and sites must be recovered in accordance with the Service Level Agreements between the company Business Units (BU) and IT. Each Data Center (DC) hosting services for the company must have adequate continuity plans, covering all critical functions for the service provision of the center. Each service, application, or platform classified in criticality as ‘very high’ or ‘high’ must have an IT continuity plan. These continuity plans must be reviewed and exercised at least twice a year and updated after changes affecting the restoration functionalities.

Senior IT management is responsible for understanding the critical business processes. The board fulfills its business continuity planning responsibilities by setting policy, approving and

reviewing the prioritized applications list, allocating sufficient resources and personnel, approving the IT continuity planning methodology, reviewing exercise key findings, and ensuring maintenance of regularly exercised IT continuity plans.

IT operations management provide across the board support for continuity planning activities in company IT. It ensures that necessary resources are allocated in creating, maintaining, and exercising continuity plans and that the suppliers meet the agreed continuity requirements.

IT supplier and vendor management provides the high level continuity requirements to suppliers and vendors and facilitates communication. All prioritized services hosted in supplier data centers will have recovery response solutions in place that meet the SLA signed by the business unit. Suppliers and vendors will provide the company with evidence of their business continuity plans and reports from recent exercises together with any deviations.

IT service managers are responsible for the continuity of their services and for ensuring that application and platform level continuity plans are developed, maintained, and exercised at least twice a year, and for ensuring that supplier hosted data centers will have a continuity plan in place that meets the signed SLA. One of the exercises needs to be a functional tabletop exercise and the other a technical test, e.g. restoring backups in the testing environment or verifying the crisis communications flow for disaster declaration.

Human resources are responsible for participating in IT continuity planning and exercises and for ensuring that HR policies are followed in the IT continuity plans. Facility management is responsible for being knowledgeable of IT continuity plans at site and data center level. At locations that house a data center, they utilize a change management process to communicate any changes to the data center environment and to coordinate all activities related to the physical site with IT to ensure uninterrupted service is provided. Corporate security has the actual BCM process ownership and is responsible for being aware of IT continuity plans for critical services and for participating in exercises at site level and for the deployment of supporting crisis management teams. All of these parties need to participate in the company IT continuity exercises at site level.

Business Continuity Management policy

Business Continuity Management policy is crucial for success and this was also understood in the company. The Business Continuity Institute (BCI 2007 chapter 1, 13) says that without BCM policy, an organization cannot establish a formal business continuity management system. The BCM policy is a key document, which sets out the scope and governance of the

BCM program. The policy provides the context in which the BCM team implements the required capabilities.

In terms of the parent companies' legacy, the challenge was agreeing on the usage and length of the policy concept. This concept has been implemented in many ways – ranging from a clear one-page statement to a dozen pages of practical instructions. The end result of this effort is seen in Appendix 1, but it was commonly agreed that this provides the framework around which BCM capability is designed and built. The role of IT lies mainly in supporting the company wide BCM approach designed to fully follow BS25999 standard.

The security council is the highest decision making body and ensures that IT continuity management meets business needs and contributes through the chosen BCM methodology in initiating, proposing, reviewing, approving and monitoring the development of a continuity management governance model and continuity management activities, including company IT, and reports on progress to senior management and the executive board.

Maturity reporting

One very important aspect of any continuity program is reliable reporting about the current maturity status over time. Without continuous planning life cycle monitoring, nobody in the decision making bodies can make sound decisions. The company's IT continuity maturity reporting has its roots in one of the parent companies.

Maturity reporting is delivered monthly following the approved cycle of overall IT management reporting of key activities and objectives. I was involved in the IT leadership team where it was proposed that a single-sheet overall view be used for reporting, but it was not seen as appropriate at the time because status collection was only starting and reliable reference points were missing. By following the cycle and reporting at a lower level, it can easily be incorporated into top-level reporting at any time on request.

The maturity report is presented in Microsoft PowerPoint layout but has an embedded Excel spreadsheet for the graphs and detailed status information. The critical IT applications, platforms, and end user services in the continuity scope are listed and the continuity planning status is monitored on a scale ranging from one to five. Status collection is ongoing and monthly status meetings are arranged with most of the IT unit nominated continuity contacts. Service managers and their continuity deliverables are validated immediately and status upgrades are marked when approved.

The maturity and service level key continuity information, i.e. recovery objectives, critical timeframes and resiliency evaluation, are also reported in a separate metadata tool, which is the main live database for any IT related information on IT components, infrastructure, and architectural data. Resiliency evaluation is a service manager's statement on a scale of 1 to 5 as to how well in practice the recovery time target set by the business owner can be met with recovery solution currently in place.

Even if you create good maturity measurements, the continuity objectives should reflect the objectives of the organization and the scorecard is a good place to measure continuity activities. Perhaps the easiest way to measure continuity achievements is by the simple linear fulfillment of continuity steps. In the company we have both of these methods in place for IT continuity management, but there is not enough historical data available at this stage to accurately evaluate the results. This is also where the confidentiality of work completed comes in. With these reporting elements we will obtain greater management commitment to continuity planning if the results will be separate since this will affect the overall incentives. From one of the parent companies we learned that the best way of getting fast continuity planning results was to link the intended end results to individual objectives. Even if money is not a significant factor, the setting of objectives has a huge impact on end result delivery. Furthermore, the individual IT continuity planning objectives are much easier to achieve than many other strict business demands.

Intranet pages and document management

Intranet was from the beginning one of the top priorities for publishing information in new merger based company. The IT continuity management intranet pages include training material, current objectives, roadmaps, operating model with responsibilities, planning related templates and organizational setup with key contacts. However, having a single main source of information is not enough, and the content of this site is kept up to date through meetings held with service management teams.

### 4.1.2 Understanding the organization

In BS25999-1, an understanding of the organization comes from:

- identifying the organization's objectives, stakeholder obligations, statutory duties, and the environment in which the organization operates;
- identifying the activities, assets, and resources, including those outside the organization, that support the delivery of these products and services;
- assessing the impact and consequences over time of the failure of these activities, assets and resources;

- identifying and evaluating the perceived threats that could disrupt the organization's key products and services and the critical activities, assets, and resources that support them.

Fernandez (2003, 57) says that while no one can predict a crisis, every organization can and should identify its vulnerabilities. Heng (2004, 24) states that the first step in creating business continuity is understanding what management expects and assembling the knowledge needed to meet their expectations. As the company supports the BCM policy and is therefore obliged to support the mission critical processes, the IT business owners are in this context the closest partner when it comes to saying what the recovery baseline should be to support business operations.

Snedaker (2007, 73) comments that things can get very political when a discussion of mission critical areas of the business begins, as everyone wants to think of their part of the business as being critical to the company. Overall, I am not that concerned about false expectations at the very beginning due to the fact that the continuity planning process is long, and the money aspect eventually adds a dose of reality to management expectations. Recovery solution implementation needs a cost-benefit analysis in which the criticality discussion will be on the table again.

Understanding of the company critical IT services

Like in any business continuity process, the company began this step of understanding the business by identifying the critical applications, platforms, and end user services in the IT continuity scope. Even if there was understanding of the criticalities from the parent companies, the number of services in the scope still had to be reviewed more closely. Understandably, there was no management support for including everything in scope, so I proposed to pick the most important elements and start ensuring continuity in this new environment for these first, and only later then perhaps broadening the scope.

The identification of critical IT services in the continuity scope was arranged in all IT units, which were organized according to the business processes of management and support, product, customer, delivery and supported by infrastructure operations. Service collection for further analysis and scope definition was performed in all of the units by nominated IT continuity contacts supported by the unit service cluster managers and business liaison managers, who are the main contacts for the business owners.

In this initial scoping, a number of services in each unit were proposed for prioritization. The list was sorted according to the typical characteristics that were already familiar from the parent companies:

1) Defined as business critical by the business owner and service management team
2) In case of any downtime, considerable losses arise for company
3) Where no downtime or loss of data can be tolerated or recovery in 1 to 3 days
4) Definition in service and system classification is very high
5) Other features:
    - Defined in SLA as 24*7 service
    - Use cost for the application is at least one million euro per half year in short term planning
    - Major effects on financial reporting.

Scoping then moved on to the respective unit leadership teams who made decisions based on resources available and used their knowledge to put services into a more detailed business impact analysis process (BIA). The result was a list of critical IT services at a very high level. It might be criticized that there was no real identification of mission critical processes, but there needs to be some kind of starting point based on the given resources, and then when moving on new ones can be added if these are identified as critical dependencies or single point of failures. This approach is also supported by the fact that in the beginning of a new company, the total number of independent IT components can be counted in thousands. The actual BIA process aiming to create service prioritizations is described in more detail in the next chapter.

Business impact analysis - BIA

Business impact analysis is the foundation on which the BCM process is built. Heng (2002, 3) says that in a BIA you define and quantify reasons why you need a business continuity plan and establish and prioritize key processes and business functions, providing and influencing the financial commitment to the BCP process. Snedaker (2007, 211) says that the fundamental task in business impact analysis is understanding which processes in the business are vital to ongoing operations and to understand the impact that the disruption of these processes would have on the business. BIA seeks to identify, quantify, and qualify the business impacts of a loss, interruption, or disruption of business processes so that management can determine at what point in time these become intolerable. The purpose of the IT BIA was to determine the possible impact that an organization could experience as a result of a critical IT related incident.

The company parents are both members of the Information Security Forum, which is the world's leading authority on information risk management. The ISF has launched several tools and guidelines, including IT continuity. It has over 300 members from the world's leading organizations. The BIA method used in the company is based on the Information Security Forum Information Risk Analysis Methodology (IRAM) BIA Assistant Version 1.0. There is also a new Version 2.0, but it was launched only after the majority of the company IT BIAs were already conducted. Despite this, the modifications that were made to Version 1.0 are quite close to the Version 2.0 updates, for example adding the risk reference matrix and more details in summary sheet.

Based on the IRAM (2009, 2), the BIA Assistant is an easy-to-use tool designed to help ISF members automate the business impact assessment phase of the IRAM methodology. The BIA Assistant supports the risk analyst in assessing the possible business impact that could arise for a system. It covers all stages in the business impact assessment process. In particular it allows the risk analyst and the organization to determine the:

- possible business impact that could arise as a result of an incident that compromises information in a system,
- business security requirements of the system being assessed, and
- next steps that should to be taken to protect information in the system.

The company IT BIA was used for prioritizing and identifying the business critical functions and the results also served as a starting point for risk, continuity, and security activities in the company IT. The additional summary sheet information gathered was to define the actual Recovery Time Objective (RTO) and Recovery Point Objective (RPO), critical business timeframes, and major end-to-end system dependencies. Carrol (Edit Hiles 2007, 238) defines recovery point objective as how much data you are willing to lose and recovery time objective as how much downtime an organization is willing to tolerate.

According to these statements, we were looking for the business impacts in situations where confidentiality, integrity, or availability is endangered. Confidentiality was described being the assurance that information is protected from unauthorized disclosure, integrity as the assurance that modifications are not made by unauthorized users and authorized users do not make unauthorized modifications. Availability being the main scope in continuity was defined as the assurance that authorized subjects are granted timely and uninterrupted access to objects. On an additional note, the main IT suppliers are also using this methodology and are therefore aligned in putting the understanding in place.

Continuity risk analysis (CRA) focusing on availability

Based on the company risk and opportunity management policy inherent to strategy, the company takes risks to achieve growth, gain competitive advantage, and deliver superior shareholder returns like any other competitor or business in economics. Managing those risks is an important part of fact based management. The company has adopted a common and systematic approach to the management of risks and opportunities across all of our businesses, platforms, and processes, while maintaining business flexibility.

This approach enables the comparison of material risks across the company, the identification of opportunities to the financial benefit of the company and ensures that appropriate strategies are implemented for the management of material risks and opportunities. It is the responsibility of everyone in company to identify, bring to the attention of others, and manage any risks they foresee. Risk management is not a separate process or action but a normal business and management daily practice.

This also applies to company IT, but here the challenge lies in adapting the traditional BCM related risk analysis to this concept. Despite these previous facts, Berg (1996, 151) says that probability formulae are useless for discussing disasters since no calculation is able to say if it will happen tomorrow, the next day, or during the next hundred years. In the IT continuity process, the company has taken this further and is mainly focusing on decision making as to whether or not there should be action to deal with catastrophic risks. The result so far has been that nobody has had the courage or authority to decide not to do anything.

Like in the business impact analysis approach, risk analysis focuses on availability. In this case the dominant feature is the impact on availability should all of the threats be realized. The decision was made to focus on availability, but also to evaluate whether there was a chance that the BIA based major impact on confidentiality and integrity could also cause availability issues. I created training material with templates for continuity risk analysis and gave it the name CRA so that it is more easily distinguished from financial risk and opportunity management, which focuses on the risks threatening short and long term business plans.

According to the company risk and opportunity management policy, a risk is defined as an uncertain event or condition that, if it occurs, has a negative impact on at least one organizational or strategic objective. This is absolutely true, but due to the high-flying nature of service management teams, I highlighted the separation at operational level when we were focusing on understanding the costs and benefits for a recovery response solution relating to recovery objectives set by the business owners (RTO & RPO) and this capability implementation.

With the continuity risk analysis, we identified business continuity and IT availability risks that might endanger the planned business actions, analyzed the root causes, consequences, and magnitude for the identified risks, and agreed on the mitigation actions and risk owners. By this we were more ready to move on in understanding the costs and benefits for a recovery response solution and shift to recovery capability implementation. We also decided not to use a company Web based risk analysis tool, but to concentrate on the manual Excel documentation that was embedded in the service SLA framework. The other reason for choosing this approach was that there was no time allocated to go through the intensive training that the Web tool would have needed.

The continuity risk analysis is summarized in a Word document to be added to SLA as a continuity appendix. It begins with basic information about roles and responsibilities with supplier contacts and an overall service description. This is followed by a list of all the applications and platforms running the service as well as the data center location(s). It also includes information about the hardware, software, and technical solutions that are required to support these applications. The business impact analysis result is also included in this document together with the actual risk analysis Excel sheet describing the risk event chain (Figure 2).

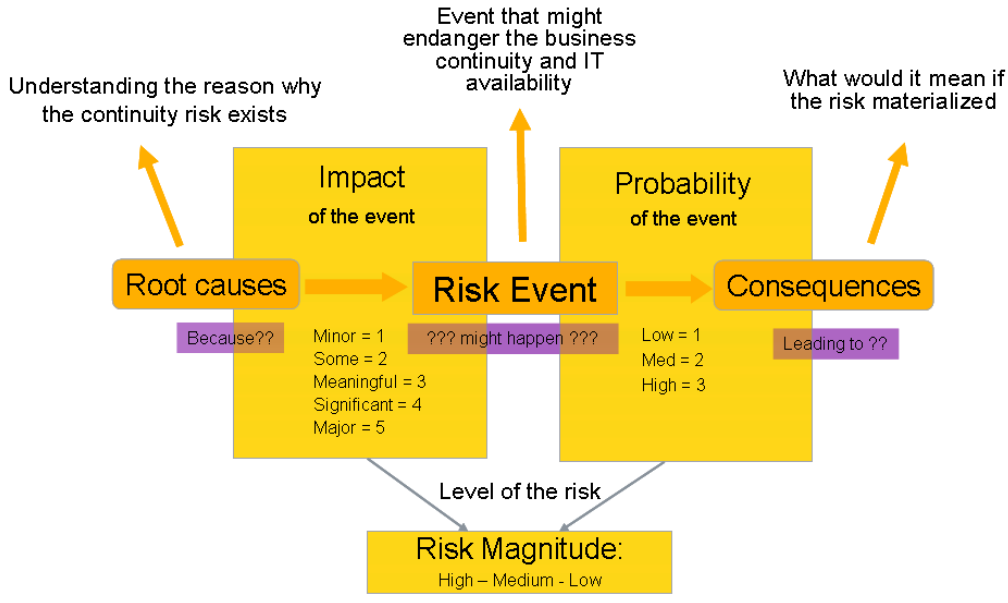


Figure 2: The IT continuity risk analysis event chain

As the risk analysis is focused on the availability related risks and knowing that service management team members are not risk management specialists, the ‘threat universe’ was

given as a baseline on how to focus on different aspects of risks (Figure 3). There was also a decision to be made as to whether any background material should be given at all, but after the theme interviews it was quite clear that without additional material the brainstorming just would not have worked very well.


Figure 3: Company IT continuity threat universe

In addition, the recovery objectives already set were included in this risk analysis document so that everybody reading it would have a clear understanding as to the reasoning behind business impact versus risk. Furthermore, it was necessary to describe whether there was a way to manually perform some elements of the IT process and describe the current solution that was already implemented by the parent companies. The already finalized system and operating guidelines were a helpful source of information, and we saw no problem in adding these as links to documentation due to the fact that only the actual continuity plan should be available if there is a wide network outage. This also helps in the maintenance of continuity risk analysis. Also helpful was the understanding of IT component dependencies that were sourced mainly in the system guides but supported by the enterprise architecture metadata work done in another project.

### 4.1.3 Determining IT recovery response solutions

Myers (1999, 10) say that business contingency strategies are documented as guidelines because they only represent options. Department managers will determine precisely how they will proceed based on the nature of a specific incident combined with an assessment of

damage. This might be relevant to simple facilities recovery, but is not an entirely correct approach to IT because it needs more specified and clear instructions and possibly even pre-approval to any actions needing quick response. As Fay (2006, 378) says, continuity planning is a continuous process and not a one time effort; there is once in a while need to re-evaluate the chosen recovery solutions.

Kirvan (Edit. Hiles 2007, 197) says that while a technology thrust for contingency planning is assumed, one cannot forget simple common sense as a key strategy. Continuity management is not a rocket science, but a willingness to think beyond a comfort zone. According to John Myers (1999, 5), an educational process and the exploration of viable alternatives with the right people are the key to cost-effective contingency planning.

Business continuity standards and best practices commonly use the term ‘strategy’ in the context of creating suitable business recovery solutions in case incidents occur. In the company IT we had a detailed discussion and decided that we should not use term ‘strategy’, as in IT vocabulary this term was only meant to be used in the context of aligning IT strategy to company level. Based on this decision, the company chose to use a recovery solution instead of IT continuity or BCM strategy. This proved to be the correct decision and fit for purpose because based on my own observations, all IT employees immediately understood the reasoning for a recovery solution as they were still familiar with term ‘disaster recovery’. It could be recommended to those in the same position of creating an IT continuity program that they consider this usage and avoiding confusing real life with corporate governance jargon.

There are perhaps as many different recovery options as there are services, with each component uniquely supporting business processes. In this thesis I am not concentrating too much on the different options because the details in IT depend heavily on the architecture and chosen systems. Heng (2005, 17) provides a useful list of the basic range, including

- do nothing,
- mirrored systems,
- multiple processing sites,
- use of alternate sites,
- drawing up quick re-supply contracts,
- providing additional capacity,
- designing and developing resiliency,
- implementing skill backup or cross training program,
- transferring risk via insurance arrangement or contractual agreement and
- applying a combination of the above strategies.

I am therefore not going to go into recovery solutions in more detail, but will instead move on to the important element here, namely the supplier frameworks. The standard recovery options ranging from e-vaulting and e-journaling to shadowing, mirroring, hot standby arrangements and load-balancing are beyond the scope of this thesis. Furthermore, the details of the chosen recovery solutions and locations are confidential information within the company.

Supplier framework in continuity management

According to Erola (2000, 123), the majority of the risks are external and exist outside of the internal organization causing huge dependencies. Graham (2006, 169) says that using suppliers or outsourcing providers is one way of transferring risk away from an organization, but it is not a way of eliminating risk or transferring responsibility for managing risk to others. She continues (2006, 180) that the outsourced plans implemented should form an integral part of the retained organization's business continuity management plans with integrated communication, notification, escalation, invocation, and reporting processes. The company IT has chosen a path of outsourcing as much as possible but retaining the key knowledge in organization itself.

A computing partnership in a supplier framework is a commonly used method in modern business environments, which allows companies to focus on their core business and relieves them of the effort involved in handling complex IT environments in house. In IT continuity and supplier chain risk management, these agreements are vital. The company also saw this as a very important topic and added continuity as a mandatory aspect to all major IT agreements.

The company uses multiple partners and the main idea is to trust partners in actual continuity planning and to ensure the capabilities through joint exercising and testing. The company's own effort is concentrated mainly at the beginning of BCM life cycle in specifying the guidelines for recovery objectives by identifying the scope of critical IT services and reviewing the requirements with the supplier. This is a very confidential area in this thesis which I am not going to discuss in detail. The real challenge lies in service recovery solution creation due to complex technology alternatives. Despite this, the overall responsibility naturally is on the company to ensure that the right decisions are made and the solutions chosen are appropriate and cost effective while taking into account the results of BIA and critical service prioritization.

### 4.1.4 Developing and implementing the response

According to Myers (1999, 45), the two benefits of the continuity plan development process are that it produces a business solution rather than a technical one, and that it encourages function managers to accept responsibility for contingency planning. Miettinen (1999, 272) highlights the fact that each business has a unique continuity plan, as one universal framework doesn't fit all. Of course the plans can't be the same, but from the group discussions the real difference comes from the recovery solution response planning. Furthermore, there are continuity plans in many layers of business; in this thesis I have only focused on the business and IT plans, but project management should also be taken into account.

I believe that Myers (1999, 45) hits the nail on the head by saying that if and when a disaster does occur, people are certainly not going to take time to read and follow detailed instructions. Individuals responsible for making decisions following a disaster need only a checklist of tasks that should not be overlooked. Additionally, Snedaker (2007, 15) says that it is virtually impossible and a waste of time to attempt to anticipate every combination of disasters that might occur and to specify exactly what steps should be taken in each instance. A bad or incomplete plan is often worse than no plan at all. This is true teamwork when Fernandez ( 2003, 89) comments that through the initial, continuing, diminishing, and resolution phases of the crisis, many procedures need to be implemented simultaneously to maximize efficiency and respond to multiple demands. Myers (1999, 47) adds that the continuity plans should be flexible, consisting of strategies rather than detailed links to specific disaster situations, so that line managers have the latitude to exercise judgment when the time comes to implement any portion of the plan. In the company IT we see planning as a natural consequence of emerging from the parent companies. We are moving towards hosting our own network and being totally individual.

In the IT context, Bowman (2008, 59) says that the reduced number of data centers and company's willingness to invest in multiple footprints have resulted in fewer and more meaningful data centers. He adds (2008, 60) that another compelling reason to go to the large or main data center scenario is the use of virtualization to improve asset utilization and virtual capacity planning. This presents a significant challenge for IT continuity planning, where systems are getting more and more centralized; the risks for large scale incidents are at the same time getting bigger and bigger. There is always a risk that we have missed something because the speed of change is so high, the systems are becoming more and more complex, and there are fewer internal people handling the operations.

It could be said that world is full of continuity planning templates and tools. It is relatively easy to create any sort of check lists where you can map what is completed and what is next on the agenda to be done. The challenge lies in the fact that the majority of the tools on the market will only provide an answer as to what should be done, and give very little information on how. This is particularly true of standards and best practices. Of course it is up to the organization to make the final decision as to how to make things operational, but this is an interesting topic where there is a very limited amount of literature available. This also ties in with my thinking that BCM is such a common way of working that it is really hard to invent anything new, but these new innovations only come from practical case studies. This discussion probably belongs elsewhere in this thesis, but it applies in particular when discussing templates and tools, the guidelines for making BCM happen.

The company is not using any commercial continuity management tools at the moment but has done some studies about those available. The tools and templates used are created by the specialist and managers working closely together to ensure business and IT continuity. Commercial tools have some key common disadvantages compared to proprietary tailored solutions. Firstly, they are usually expensive, costing even more when there are many company interfaces. Secondly, it is major challenge to find a tool that can be managed entirely by organization itself, and maintaining data in vendor systems might have an information security risk. The third issue is that these really do little to tailor different business operations together and keep continuity planning at a high and broad level. Perhaps the biggest problem is that these tend to be managed over the network, posing a real threat if this is not available during a disaster.

Myers (1999, 47) lists the characteristics of a good continuity plan:

1) Workable – developed by first line supervisors
2) Cost effective – in relation to low probability
3) Flexible – same plan can be used for any disasters
4) Easy to maintain – keep it simple
5) Deals in strategies – not detailed procedures.

The company IT continuity planning is based on business impact assessments and risk analysis. IT continuity plans give exact and detailed guidance and information with regard to the following:

1) What is a disaster with respect to the IT service/application/platform/data center, and what are the defining criteria for disaster declaration?
2) How does the IT service crisis management team operate?
3) How is damage minimized and the immediate cause of the disaster removed?
4) What are the alternative ways of working during the recovery?

5) How does the disaster affect other entities?
6) How does IT or parts thereof recover from a disaster?

Data center continuity management requirements are typically inherited from individual service specific IT continuity plans and requirements, but the following are required as a minimum:

1) All identified continuity risks need to be analyzed regularly.
2) IT continuity management responsibilities and procedures for continuous development need to be created, agreed, taught, and deployed.
3) The person responsible for data center continuity planning plans and organizes a regular evaluation and independent auditor, e.g. a BCM professional performs the evaluation including continuity plan effectiveness, efficiency, and residual risks.
4) All of the above are to be documented in the risk analysis and business impact analysis, IT continuity plan, and the exercise and test documentation.

One result worth mentioning from the theme interviews is that we are not going to produce paper copies of continuity plans. Think about the challenges of keeping continuity plan documentation up to date. Some BCM educational bodies still tend to recommend keeping spare copies with employees at all times, even in the trunk of a car. In Nordic countries, nature would make the plans very hard to read due to the high moisture levels all year round. This is also a real information security risk. We recommend having electronically maintained copies delivered to each individual with responsibility. By electronic, the company means having the plans on encrypted CD-ROMs, memory sticks, and on backup laptops. The main data source is in a shared folder with limited access rights and the suppliers and vendors will be also included in the scope. It is also worth remembering that the key to successful recovery lies in employees knowing the roles and responsibilities off the top of their head.

### 4.1.5 Embedding continuity in the IT organization's culture

Halibozek (2005, 201) describes culture as a common social understanding that leads to commonly agreed assumptions. Lundgren (2004, 123) says that we always make assumptions about the target group and we should therefore know more detail about who are we dealing with. According to Graham (2006, 224), a relatively small number of large organizations have managed to implement a business continuity culture with great success, giving their workforce the knowledge, awareness, and authority to manage risk and continuity effectively. An organization is a blend of attitudes and approaches to risk taking.

O'Hehir (Edit. Hiles 2007, 43) says that training is not the same as testing and this is often the most overlooked component of business continuity planning. Much effort is put into

developing, testing, and maintaining the plan but often personnel are not adequately trained in all aspects of plan activation. Myers' (1999, 120) recommendation is to ensure that a plan is workable; individuals need to be aware of their responsibilities and prepared to implement them in the event of a disaster.

### 4.1.6 Exercising, testing, and maintenance

Bowman (2008, 47) says that companies morph or reinvent themselves every three years; the risk management view should also change. It is a good question to ask how often the plans should be updated and exercised. Wold (Edit. Rothstein 2007, 143) says that recovery plans should be tested at least on an annual basis and for an organization with a relatively new plan, a quarterly or semiannual test may be prudent the first year.

Snedaker (2007, 35) says that if a continuity plan is not maintained, updated, and revalidated from time to time, you will find that the plan may be rendered useless if a disaster does strike. Gregory (2008, 24) goes even further by saying "The time spent on the original DR plan will be a waste if you don't update that plan". Wold (Edit. Rothstein 2007, 141) lists reasons for time eroding a disaster recovery plan's effectiveness:

1) Environmental changes occur as organizations change, new services are introduced, and new policies and procedures are developed.
2) Hardware, software, and other critical equipment change.
3) The organization may experience personnel turnover.
4) Personnel may lose interest or forget critical parts of the plan.

According to Myers (1999, 115), complicated business continuity strategies force unnecessarily complex testing programs where the results are usually frustrating and depressing. Based on Salminen's (2003, 40) statement, the objective for testing is to receive reliable information that the plan actually works and to identify possible deficiencies. She adds (2003, 39) that the tests should be conducted based on management approved principles. Paavilainen (1998, 226) gives a good baseline that the testing should also be conducted as close to real life as possible and ensure one element at a time before going to a whole system of real live testing. Miettinen (1999, 279) agrees by saying that there is a need to go beyond tabletop exercising.

Main objectives for future exercises in the company are:

- To evaluate the organization's current competence on recovery
- To identify areas for improvement or missing information
- To comply with the company BCM policy, governmental and financial regulations, and to meet customer and stakeholder requirements
- To provide information and instill confidence in exercise participants

- To evaluate teamwork during the exercise
- To test the effectiveness and timeliness of restoration procedures
- To correct wrong assumptions which need to be corrected: assuming you know something and you don't, assuming that something is straightforward but it's complicated, and assuming that someone else is doing something and they are not.

The company is not collectively at this continuity maturity stage to the extent that the functionality could be evaluated at company level. Corporate governance in relation to testing and exercising is ready, but the organization as a whole is not ready for a program point of view, only the single most critical instances are close. Of course the testing of technical elements, for example backup restoration, is part of daily work and belongs to the IT continuity scope of testing. Furthermore, totally inherited systems have capabilities in place, especially those still hosted before carve-out by the parent companies.

I have already created an exercising and testing process in a guideline format. It has its origins in one of the parent companies where it was proven to work. Furthermore, the theme interviews showed that many service managers are already familiar with this topic and they also say that testing is part of their normal data center activities. So this capability is in place to an extent, but no action has yet being taken with regard to joint testing with multiple services, data centers, and live testing. We are still waiting for some continuity plans to be implemented due to the network changes and changing IT setups. In summary, by exercising manual and legacy knowledge we will be ready to start exercising when planning maturity is at the required level.

Exercising is an activity that is performed for the purposes of training and conditioning team members, improving their performance, and validating the IT continuity plan. Though several exercise types exist, tabletop exercise represents a good model, especially when the exercise is conducted for the first time. When it is necessary to demonstrate a more profound way of exercising continuity plans, functional exercise should also be considered. The tabletop exercise is a method in which the participating team review and discuss the actions they would take according to their plans, but do not perform any of these actions. The exercise can be conducted with a single team or multiple teams, typically under the guidance of exercise facilitators. Usually this is a scenario-based event where decision making and communication abilities are being examined. The functional exercise method means exercising where teams perform some or all of the actions they would take in the event of plan activation. Functional exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery

configuration and resources. Like tabletop exercises, functional exercises should rely on a planned scenario.

The term ‘test’ is usually used when the reliability and effectiveness of recovery and restoration procedures or availability of key resources are evaluated against specified objectives or measurement criteria, e.g. the recovery time objective and/or recovery point objective defined in the continuity plan. Depending on scope and objective, a test may include:

- Testing of the call tree by calling all the named persons
- Testing of availability of documentation by requesting document owners to deliver these using the method described in the IT continuity plan
- Testing of personnel moving from primary site to the alternate workaround
- Testing of application recovery and resumption process by restoring backups into the test environment
- Testing of availability of logistical support, services, and infrastructure systems at alternate facilities, e.g. water, electrical power, heating, and air conditioning.

## 4.2 Challenges to consider in the continuity life cycle

The main purpose of this section is to fulfill the objectives in collecting lessons learned for future activities and, based on these lessons, evaluate any gaps that might exist in order to proceed. Myers (1999, 11) says that when the economic climate is favorable, contingency planning is last on the list of things to do; when profits are down, contingency planning is the first item to be cut from the budget. While writing this document, the global economy has been hit by a crisis similar to the 1930’s depression, which puts this thesis in a unique position with respect to time and the business life cycle. There is widespread agreement that the good times have come to an end and that things are getting harder.

The data is collected using the methods described and delivered using the continuity stages ideology already described in the previous section. This list does not include the IT continuity capabilities and it should not be assumed that these topics are missing. The point here is that these are simply lists of things to be considered carefully in order to succeed in IT level continuity planning efforts. Most of these are common sense and are supported by the variety of publications on the subject of business continuity management. Despite this, the one key element involved in transforming learning into knowledge is simply doing. Of course the volumes are massive in a global company, but the ideology is the same.

Development of an IT continuity program

As stated in the theory and implementation aspects, this is the most important building block to managing continuity effectively. Like in house building, the foundation needs to solid. In a big merger in particular, the executive support needs to be in place. Business continuity management is somewhat peculiar in that you just can't live without it. In a public company there is nobody authorized to decide that it should not be done. A good tool involves managing the BCM policy creation process from which the end result should be an executive layer signature. Without this documentation, it is hard to get any support from the lower organizational layers. As BS25999-1 says, with IT being a support function, it needs IT level operating procedures. The most effective way of achieving this is to link it to strategic planning and objectives. Clear roles are needed for management, IT services, and to ensure that supplier agreements include statements with regard to risk transfer and continuity recovery solution hosting.

In addition to organizational setup, there is a need for steering at both operational and governance level. Maturity monitoring should be arranged and ensure planning cycle status delivery on a regular basis. Maturity reporting should be on the management agenda and actions need to be taken if things are not proceeding as planned. The reporting should also reflect to the capabilities supporting company mission critical processes so that there is also a business visibility to supply chain risk management. I am saying that there is a need to convince customers and other stakeholders. The continuity maturity reporting should also reflect the true capabilities and progress should only be measured with relevant documentation of the life cycle capabilities.

Sometimes there are just far too many projects, as was especially the case after the merger. It might help if there is a clear decision in relation to the scope, focusing initially on the most mission critical components and later when things settle down moving to a more broad scope, also having the interdependencies analyzed and more resources allocated. Last but not least, it is necessary to highlight the importance of knowing your stakeholders and understanding their demands.

Understanding the organization

The most important thing we learned is to be really careful when conducting business impact analyses with business owners. This is where things might get political. It is understandable that people tend to be convinced that their area is the most important. This will get more complicated in the future when there may not be enough resources to implement the recovery solutions but the recovery objective may remain. Sometimes business expectations

are just aimed too high, but it is worth mentioning that without money there is only so much effort that IT can give. The normal SLA frameworks don't usually take disaster recovery into account, focusing solely on the maintenance intervals.

The beginning of the continuity program always takes time and there should be a clear roadmap agreed by management. One should exercise caution when saying that continuity is not a project but a never ending process, as this can be a true killer of motivation. The cake should be eaten in small pieces. Talking about cakes – continuity is a topic in which everybody is interested. If you are responsible for continuity program creation and maintenance, you should be aware that many people like to take a piece of it but only a few will stay enjoying it with you.

The program management foundation is thus the key to success. You need to gain management support, form the roles and responsibilities, and gain organizational acceptance through continuous training and placing governance closer to operations. You should never forget the importance of management leading by example. According to the theme interviews and group discussions, the wider operational audience wants to see action to be reassured that they are not the only ones making an effort and that management is sharing the burden.

Determining IT recovery response solutions

IT recovery response solution creation needs to be aligned with the business impact analyzed and agreed by the business owners. In addition, there must be a re-evaluation of those impact assessments if people should change the role or the operational environment should change. This should not be overlooked in the merger based company.

Knowing what to plan for is also important and there should be decisions made by management as to what qualifies as a disaster and on a high level if it is at all approved to have systems on a single site. These are the baselines also considered in the risk analysis when considering the threats towards availability. This also forms the basis for supplier hosting of data center environments and is taken into account in the IT architectural design of recovery classification. According to the classification there will be a mandatory baseline supporting the continuity capability.

The key statement is that every service mainly focuses on its own environment and recovery solution. One should not forget to map the dependencies, as there is always an information flow in the process. Interdependencies are good to have on the agenda at the very first level of risk analysis. This is also a good way of exerting internal group pressure for service management teams interested in the critical dependencies caused by other systems or

platforms. If company has a metadata approach in place, this is the easiest way to obtain a collective understanding with regard to the single point of failure.

Hosting partners or internal computing should form an approach for handling information about the different recovery options. This also involves the factors of money and resources. The baseline is normally agreed in the global agreements, but the question pretty soon turns to one of what it is actually possible to buy in practice. ‘As early as possible’ would be the main message, but unfortunately in this merger based case study this was not possible. The agreements were built in many layers and the systems were changing very rapidly from one network to another and from the parent companies’ to the company’s own responsibility.

Developing and implementing the response

Continuity planning with document creation was not actually in the scope of this thesis, but there are few points needing attention. From the very beginning there should be an understanding as to who is responsible for the continuity plans, since in an IT environment these are handled at service, platform, end user, and data center level. Responsibilities need to be agreed with suppliers as soon as possible. The company has chosen a path where actual planning responsibility lies within the hosting organization, but there is a clear link with service management team support. There is not so much back office work and communication possible for IT service personnel because most of the physical and availability risks mitigation actions are focused on the computing hosting environments and on where the actual recovery takes place.

Embedding continuity in the IT organization culture

As this continuity life cycle step concentrates on training and awareness, it can simply be said that it is extremely important to ensure that a thorough understanding of the roles and responsibilities exists. The responsibilities need to be shared and understood at computing, operational, and governance level. In modern working environments, people change jobs so often that constant education through a program is mandatory. Intranet pages and resource mailboxes are not enough, somebody needs to go there and have personal meetings. Modern business environments use remote working methods where there is somewhat faceless communication. It might be not a surprise to learn that the best results are gained only by personal communication. It is extremely challenging to be sure that the counterpart understands your message if the response is just silent approval. It also helps if there are known counterparts responsible in the line management for unit level continuity planning. Governance level continuity managers have only a little influence on making actions happen

on their own. People are working in different time zones might also be a factor, but this is a separate topic and relates to business decisions as to how the company operates.

Exercising, testing, and maintenance

As described earlier, the company's basic testing capabilities are in place and the path to true live testing is still not yet possible. From the past we have learned the importance of test scoping and objectives setting. Exercise participants might not be dedicated and motivated if there is a lack of information about the importance of exercises, they are all too busy with other tasks, or even if the wrong people are invited. For functional exercise in particular, cost factors are not recognized and calculated and risks need to be analyzed. Testing fallback plans need to be created, especially for technical tests. The exercise scenarios also need to be realistic and not too complex or trying to cover too many areas at the same time. Exercise logs and memos need to be complete for the reviews and stakeholder reporting.

## 4.3 What have we learned so far as a company?

Due to the fact that the IT continuity capability as a program has existed from the very beginning, there certainly are things we have learned. It could be said that the main lesson learned is that there is no other way of gaining an understanding of continuity capability maturity but to organize the planning through process methodology. Having gone through the analysis and research before this section, it can be concluded that there is a lot of work still to be done. Business continuity management is truly a never ending process. Even when you think something might be at a good level, business decisions may be made at management level that lead to a need for urgent updates, resourcing, and changes to current plans.

The main driver for the decision to have IT continuity in the first place was described briefly in the background chapter of this thesis. All parties of this company are agreed that it is a necessity given that IT has a significant business support role, and we cannot bet our future in luck management. Furthermore, we don't have any crystal balls so we need to make choices and plan for the worst, focusing our efforts on most likely scenarios with the biggest business impacts. Despite a common understanding, there comes the reality of making decisions as to whether we should just make things work and then plan for the difficulties. To some extent this might be appropriate, but at the end of the day it is more cost effective to implement recovery solutions at the beginning than to change something later. These statements can be applied to the building of any IT continuity program. Sometimes it is easy to follow the enterprise life cycle, but there are always some systems built where this dilemma arises.

There is no doubt that the company faces a major challenge in progressing continuity management. Erola (2000, 131) describes a triage model for decision making, which might be worth investigating further. The term ‘triage’ is borrowed from the battlefields of war, where medical staff need to make quick inspections in order to determine who should be treated first. The wounded soldiers are divided into three groups:

1) Those that will die no matter what,
2) those who could survive with minor procedures or can wait, and
3) those requiring immediate action in order to survive.

Combining this with BIA and risk analysis magnitude measurement, people might be subconsciously forced to promote business continuity planning by decision making that is later difficult to refuse.

One justification is that we are benchmarked with others and customers tend to have business continuity as a major possible show stopper. Even in tendering phases, this could be a road block preventing further progress. It is both fortunate and unfortunate that we have an excellent standard BS25999 – this is what BCM specialists need in companies for risk transfer, but at the same time it gives huge expectations with regard to trust that can be lost only once. This is such a fundamental issue, that even the executive board would have their heads on the block if they made a decision to run operations based on a governance mist.

Customer business continuity requirements also exist on several layers; inside company governance, product creation and projects, customer account management, goods delivery, and even in hosting networks. The company BCM therefore affects every single area from the first concept of partnership to auditing of the end results. As Heng (2006, 25) says, full simulation is the ultimate business continuity plan test. This should also be the final IT delivery supporting the company BCM policy where IT continuity capabilities can be ensured.

# 5 Conclusions

## 5.1 Reliability and results

As a thesis author, I have sometimes taken a huge liberty with statements that may not have any reliable evidence from an academic perspective. Given that this thesis and the educational objectives of further studies at Finnish universities of applied sciences are judged mainly on the basis of the support of organizations and the work done, I may be able to justify this on a smaller scale.

Furthermore, the data collected for the results may not be reported with the necessary level of detail, and the process has been long and perhaps too wide in its scope with its multiple interviews and participant observation times. This definitely has an effect on reliability, but reflects the company's expectations and challenges quite well.

When this work is carried out extensively in one organization, these comments may not apply to everybody. Despite this, most of the work completed and the statements are in line with industry recommended standards and best practices for continuity. Successful auditing to BS25999 and BS25777 would naturally evaluate this in more detail, but at this point further details on maturity are company confidential.

## 5.2 Own thesis evaluation

Ellet (2007, 6) says that case study method students need two distinct sets of skills; being able to analyze a case by giving it a meaning in relation to its key issues and being able to communicate thinking effectively. One might say that giving a meaning is easier than putting ideas on paper effectively. As far as I have understood, education is about learning and I have tried my best. If I were to assess my learning, I would say that I have learned a lot, but I am not so sure about the end results for business continuity in terms of society or to the company I represent.

The objectives came mainly from IT management in my organization and the similar program that is ongoing in one of the parent companies. I believe the objectives have been quite adequately met, but as this is not all about science or making history. I know there are many open questions where I have not given enough details and definitions, but continuity management is not a project but more of a never ending process. With regard to this concept I would say that this case study is not an exception, the story continues and program maturity has not yet reached the highest level.

## 5.3 Learning and importance of the thesis

From an organizational perspective, the work done is extremely important since there is an urgent need to document the work done for the IT continuity program. I am also the weak link without a proper substitute in case of any emergencies from an employee point of view. If I were to leave the company, I believe this would result in a short term break in proceeding with the program.

In creating this thesis, I really learned more about the relationship with best practices and industry's way of managing the continuity program. I am also more prepared to debate the reasoning behind many decisions made in organizations in my capacity as an internal consultant. With this document I have also written a legacy for my successors, since I really believe my company has great potential for long-term success. Even if the work done here is not at all in line with the thesis requirements, the time spent on it has been worth it. In a more broad perspective, quantitative elements such as the addition of continuity maturity measurements would have taken it to a new level, but due to the confidential nature of the process this was out of the question.

## 5.4 Further IT continuity management program development

As continuity program management is defined in key standards as a continuous process and not a project, managing resiliency and corporate governance must go on and there are still some gaps to fill in to achieve an excellent level of IT continuity. As the work done so far is only the beginning, monitoring and maturity development is needed before we can say that IT is supporting business at a good level. Focusing and creating effective program foundations are crucial for future development. The first truly internal company measurement milestone is the exercising and testing of effort done. This will still take some time, but is also the most beneficial aspect for continuity specialists if objectives are met. Without exercising results, we don't have any evidence as to whether our efforts have actually worked. This is also necessary for convincing external customers and other stakeholders.

Ultimate capability maturity in this thesis concept can only be ensured by live testing of the shifting of IT operations to another site. My opinion is that before this objective can be achieved, more resources and skills are needed together with more properly identified mission critical processes in business excellence.

This context would need some more research later when the IT continuity program maturity increases. Quantitative data collection methods would also be required in order to really understand the capabilities after recovery solution testing. Having said that, the focus in

future should be shifted from this company scoping the objectives to supplier chain risks and end user expectations.

References

Bell, J 2005. Doing your research project: a guide for first-time researchers in education, health and social science 4th edition. New York: Open University Press.

Berg, K-E. 1994. Yrityksen riskinhallinta. Helsinki: Suomen vakuutusalan koulutus ja kustannus Oy.

British Standards Institute. BS25999-1:2006 Business continuity management – Part 1: Code of practice.

British Standards Institute. BS25999-2:2007 Business continuity management – Part 2: Specification.

British Standards Institute. BS25777:2008 Information and communications technology continuity management – Code of practice.

Business Continuity Institute (2007) Good practice guidelines. Chapter 1, BCM Programme management. The Business Continuity Institute.

Ellet, W. 2007. The Case study handbook: how to read, discuss, and write persuasively about cases. Boston: Harvard Business School press.

Erola, E. & Luoto, P. 2000. Riskit voimavaraksi, liiketoimintariskien hallinta yrityksessä. Helsinki: Oy Edita Ab.

Fay, J 2006 Contemporary Security Management – second edition. Elsevier Butterworth-Heinemann.

Fernandez L. & Merzer M. 2003. Crisis communications handbook. Jane's Information Group.

Flick, U. 2006.Introduction to qualitative research 3rd edition. London: Sage Publications.

Gerring, J. 2007. Case study research: principles and practices. New York: Cambridge University Press.

Graham, J. & Kaye, D. 2006. A risk management approach to business continuity. Rothstein Associates Inc.

Gregory, P. 2008. IT disaster recovery planning for dummies. Wiley Publishing Inc.

Halibozek E & Kovacich G. 2005. Mergers and Acquisitions Security. UK: Elsevier Butterworth-Heinemann.

Heng G. M. 2004. Managing your business continuity planning project. Singapore: GMH Continuity Architects.

Heng G. M. 2002. Conducting your business impact analysis. Singapore: Hibis Consulting Singapore Pte Ltd.

Heng G. M. 2005. Managing Developing recovery strategy for your business continuity plan. Singapore: GMH Pte Ltd.

Heng G. M. 2004. Implementing your business continuity plan. Singapore: GMH Continuity Architects.

Heng G. M. 2006. Testing & exercising your business continuity plan 2nd edition. Singapore: GMH Pte Ltd.

Hiles, A. 2007. The definitive handbook of business continuity management 2nd edition. John Wiley & Sons Ltd.

Hirsjärvi, S., Remes, P., Sajavaara, P. 1997. Tutki ja kirjoita. 4th edition. Helsinki: Kirjayhtymä.

IRAM 2009. BIA Assistant User Guide. Information Security Forum.

Kerko P. 2001. Turvallisuusjohtaminen. Jyväskylä. PS-kustannus.

Lundgren, R & McMakin, A 2004. Risk Communication – third edition. Battelle Press.

Metsämuuronen, J (2006). Laadullisen tutkimuksen perusteet. Helsinki: International Methelp Ky.

Metsämuuronen, J. 2006. Tutkimuksen tekemisen perusteet ihmistieteissä. Helsinki: International methelp Ky.

Miettinen, J.E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Jyväskylä: Gummerus Kirjapaino Oy.

Myers, K. 1999. Manager's guide to contingency planning for disasters 2nd edition. John Wiley & Sons Inc.

Paavilainen J. 1998. Tietoturva. Espoo: Suomen Atk-kustannus Oy.

Roessing, R. 2002. Auditing business continuity: global best practices. Rothstein Associates Inc.

Rothstein, P. 2007. Disaster recovery testing: exercising your contingency plan 2007 edition. Brookfield: Rothstein Associates Inc.

Salminen H. 2003. Liiketoiminnan jatkuvuussuunnittelu. Espoo: Teknillinen Korkeakoulu.

Snedaker, S. 2007. Business continuity & disaster recovery for IT professionals. Burlington: Syngress Publishing Inc.

Yin, R (2003) Case study research: design and methods. California: Sage Publications Inc.

Figures

Appendix

Company Business Continuity Management policy (public version)

1. Purpose of the policy

This company Business Continuity Management (BCM) policy sets out the objectives, roles and responsibilities, minimum standards, and best practices for BCM in the company. The minimum standards and implementation guidelines for BCM program management and Business Continuity planning are further detailed in a separate document, the Company BCM Guidelines. The objectives, roles and responsibilities, minimum standards and best practices for crisis management in the company are detailed in separate documents the company crisis management policy and company crisis management guidelines.

2. Vision

Business Continuity Management in the company protects the interests of the company's key stakeholders, reputation, brand, and value creating activities. BCM in the company is a value driven process that aims to establish a world class fit-for-purpose program for business continuity enhancing the company's credibility towards its customers, investors, regulators and other key stakeholders. A value driven BCM program is proactive, preventive and embedded in the corporate culture, thus enabling the company to maintain its competitive edge. BCM in the company is integrated into corporate change management and new business development processes enabling proactive and preventive handling of business risks. Through a holistic approach to BCM that incorporates early and holistic identification of weaknesses and vulnerabilities, BCM contributes to the process of continuous improvement and building business excellence throughout the organization. Finally, the company is committed to being a responsible corporate citizen and protecting the environment under all circumstances, including crises and business disruptions. Being a good corporate citizen means not only caring about business interests but taking responsibility for the society wherever we are, an whatever location and community we live. The company recognizes that a crisis in the environment and societies we operate in has implications to the long-term sustainability of our business and our brand image. Consequently the company aims beyond internal business recovery and seeks to proactively engage in contributing to disaster preparedness and recovery efforts in the societies we operate in.

3. Objectives

The company is committed to the continuation of all critical business functions, identified as a result of a Business Impact Analysis (BIA) process, through an effective and comprehensive fit-for-purpose program of disaster prevention and holistic business continuity. BCM in the company extends beyond recovery by exercising early and holistic identification of potential weaknesses in business processes towards effective prevention, mitigation and management of relevant risks.

4. Key principles

Business Continuity Management in the company adheres to the following foundational principles:

1) BCM is an integral part of corporate governance and is to be integrated into existing business processes and practices. All BCM strategies, plans, and solutions must be business owned and driven.

2) BCM is a business management process that is undertaken because it adds value rather than because of governance or regulatory considerations and BCM activities must match, focus upon, and directly support the business strategy and goals of the company. BCM efforts must address the vulnerabilities and objectives determined by a comprehensive Business Impact Analysis (BIA).

3) BCM must provide fit-for-purpose solutions building resilience throughout the organization to optimize product and service availability.

4) Business continuity plans must be based on a holistic understanding of potential risks and their impact to the company business operations. A holistic understanding of risk is acquired through risk analysis, within the context of a company risk framework, and
Business Impact Analysis that identify, quantify and qualify the Mission Critical Activities in the company. The company does not tolerate risks with regard to the personal safety of people, key assets like the brand and reputation or those which lead to a breach in any law. The required efforts to identify, mitigate and manage such risks are detailed in company crisis management policy.

5) BCM is complementary to a holistic risk management framework that sets out to understand the risks to operations and business, and the consequences of those risks. Industry best practices and standards such as ISO27001:2005 and BS25999-1:2006 form the basis for the company BCM framework. The company BCM process life cycle and its steps define company best practice.

5. Process life cycle

BCM program management in the company is an iterative process that is based on a Plan-Do-Check-Act (PDCA) cycle to establishing, implementing, operating, monitoring, exercising, maintaining, and improving the effectiveness of the program and plans. BCM is a business owned, business driven process that establishes a fit-for-purpose strategic and operational framework that

1) proactively improves the company's resilience against disruptions and enhances the resilience of Mission Critical Activities,

2) provides a rehearsed and tested method of restoring ability to supply key products and services to an agreed level within an agreed time after a disruption, and

3) delivers a proven capability to manage a business disruption and protect the company's reputation and brand.

The BCM life cycle comprises six elements:

a) BCM program management is an ongoing management and governance process owned by Corporate Security and supported by the company executive management. Its goal is to ensure that the necessary steps are taken to identify the potential risks, impact of potential disruptions and that the appropriate business continuity plans are implemented, reviewed and tested in compliance with industry standards, best practices and this company BCM policy.
b) Understanding the organization provides information that enables prioritization of the company products and services and the urgency of the critical activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies.

c) Determining business continuity strategy enables a range of strategies to be evaluated. This allows an appropriate response to be chosen that ensures the company can continue critical activities at an acceptable level and within an acceptable timeframe during and following a disruption.

d) Developing and implementing a BCM response results in the creation of a management framework and a structure of incident management, business continuity,
and disaster recovery plans that detail the steps to be taken during and after an incident to maintain or restore operations.

e) Exercising, maintaining and reviewing BCM arrangements leads to the organization being able to demonstrate the extent to which its strategies and plans are complete, current and accurate and identify opportunities for improvement.

f) Embedding BCM in the organization's culture enables BCM to become part of the company core values and instills confidence in all stakeholders in the ability of the organization to cope with disruptions.

6. Roles and Responsibilities

**Executive Board** will review the progress and respond accordingly to achieve the company business continuity commitments towards all stakeholders and customers.

**Security Council** is the highest BCM program decision making body in the company and shall manage the status and program by reviewing the continuity resilience.

**Business Continuity Management Steering Group** monitors the BCM program and reports continuity resilience status to Security Council. BCM SG also ensures that the company key process areas are covered in planning. BCM SG involves representatives of COO, CMO, CFO, Services, Operations and central functions. Program monitoring and reporting are based on key performance indicators (KPI) set by the BCM SG.

**Corporate Security** is accountable for facilitating and monitoring BCM activities in the company and reporting the program status and progress to the company Security Council. Furthermore, Corporate Security is responsible for facilitation and support for implementation of BCM in Business Units and company key processes by providing training, expert advice, common tools, and methodologies based on industry standards and best practice.

**IT** supports the overall BCM program by ensuring that the information technology and services can be recovered from a disabling failure within required and agreed business timescales.

**Business Units** have the overall ownership for business continuity plans. Business units at all levels; site, country, project, sub-region and region, as well as support functions must have business continuity plans in place. This principle applies regardless of the main function of the site, e.g. manufacturing, research and development, sales or customer care. Management in business units must appoint a nominated plan owner responsible for BCM planning efforts with appropriate capabilities and resources. It is primarily the responsibility of the business units to ensure that the company BCM standards are met and plans are regularly tested and reviewed.

**Corporate Functions** support business continuity planning and management based on requirements determined as a result of business impact, risk and stakeholder analyses carried out by Business Units.

**Human Resources**, for instance, may be required to produce plans to ensure the company's ability to deploy skilled resources in response to a disaster or disruption in the shortest possible timescale and redeploy skilled resources for normal work assignments and work rotations in order to facilitate business recovery. HR may also be required to facilitate training programs and manage Occupational Health and Safety requirements related to business continuity.

**Real Estate** may be required to facilitate arrangements relating to the deployment and use of alternate sites and workplace resources as identified in business continuity plans.

**Corporate Communications** supports business continuity through the creation of communication strategies, guidelines and in order to facilitate accurate and fast factual communications towards internal and external stakeholders to minimize negative outcomes and maintain business confidence. Other support functions, such as **Legal and Compliance**

and **Strategy and Business Development** are also intimately involved in business continuity and may have specific tasks to fulfill in business continuity plans.

Roles and responsibilities for **business and support functions** are described in detail in the **Company BCM Guidelines.**

**Crisis and Continuity Management Teams (CCMT)** are purpose built teams for managing the impacted units out of crisis and towards business recovery. CCMT's are to be formed on local, country, sub-regional, regional, functional level and corporate levels.

**Employees** are an integral part of BCM efforts in the company. Each employee shall seek to identify and report any risks that threaten the continuity of the company's reputation, brand or value creating activities.

7. Reporting

The status of the company's resilience against business disruptions is monitored and benchmarked by Corporate Security based on maturity status information collected from business units in a comprehensive BCM status report.

8. Crisis Management and Emergency Response

Crisis management (CM) and emergency response are vital integrated processes within the overall BCM concept. Crisis is, by definition, a situation or condition that threatens the survivability of the company's business operations, assets and the wellbeing and life of its employees. Crisis situations, such as natural disasters, political and civil unrest and pandemics, must be efficiently managed and mitigated prior to business recovery towards re-establishing normal operations can be resumed. Crisis management and emergency response plans are critical processes to achieve this. The specific requirements, processes, roles and responsibilities for these efforts are specified in the company crisis management policy and guidelines.