LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

A Step towards Resilience, Creating a Business Continuity Plan for WhiteRock Finland KY

Ibukunoluwa Akinbola

2018 Laurea

Laurea University of Applied Sciences

A Step towards Resilience,
Creating a Business Continuity Plan for WhiteRock Finland KYError! No text of specified style in document.

Ibukunoluwa Akinbola
Degree Programme in Security Management
Bachelor's Thesis
February, 2018**Error! No text of specified style in document.**

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security Management

Error! No text of specified style in document. Ibukunoluwa Akinbola

A Step towards Resilience,
Creating a Business Continuity Plan for WhiteRock Finland KY

Year 20182018 Pages 57

The goal of this thesis and development project is to explore Business Continuity Management and create a Business Continuity Plan as it is the primary objective of the thesis. Also Identifying the possible impacts directed to the company because of a disruption.

Interning at Whiterock Finland KY, was an opportunity to be part of the risk analysis team for the tour and travel business newly established by the company, and this gave an understanding the many risks involved in a tour and travel business from small disruption to critical issues. The need for Business Continuity Plan (BCP) in White Rock KY became necessary. The primary motivators for developing a BCP are to keep the business running, reduce liability, and lower the impact of any market disruption.

Authors have tried to answer the question of what elements makes up the formal BCM system. Ian Storkey gave a six steps framework while Gilbert and Gips saw a BCM system as consisting of four major elements: risk identification, risk assessment, risk ranking risk and management. Business continuity institute(BCI) framework and ISO, all frames that would be discussed in this thesis. These prove the point that there are various ways to divide the different steps in making a Business Continuity Plan. Regardless of which framework a company chooses to work with, it needs to be modified to suit the company's requirements.

Qualitative research methods such as workshop and interviews were used during this thesis and development project which help in the creation of the BCP. Brief orientation was given to the top executive officer after completion of the BCP and as part of the process, the BCP should be updated regularly. Also, an unbiased assessment of the revised BCP and test software should be performed to make sure that both are comprehensive and updated primarily based on the organisation's risk profile and test results.

Keywords: Business continuity plan, Analysis, Risk, Disruption

Table of Contents

1 Introduction 5
1.1 Thesis Information 5
1.2 Company Profile 6
2 Theoretical Framework 6
2.1 Business Continuity Management 7
2.2 Framework for Business Continuity Management 8
2.2.1 ISO 22301:2012 9
2.2.2 ISO 9001:2015 10
2.2.3 ISO 31000 11
2.2.4 Business Continuity Institute Framework 12
2.2.5 Finnish Consumer Safety Act 14
2.2.6 BC planning Process Using Risk Based Approach 15
2.2.7 BCP/DPR Frame by Ian Strokey 17
2.2.8 Gibbs and Buchanon BCP Framework 17
3 Research Methods 17
3.1 Workshop 18
3.2 Interview 19
3.3 Literature Review 19
4 Data Analysis 24
5 Result 39
5.1 Conclusion and Recommendations 40
References 41
Figures 46
Tables 46
Appendices 47

1 Introduction

Business continuity planning and DRP are aspects, that should be of importance in an organisation as the world has been facing a tide turn moment which all public and private institution should be able to adapt to new types of threats. Before companies used to concentrate their operations in a few sites with proximity as an economic strategy, today the policy of two or more mirror sites distantly disperse including the staff seems a much better approach. “Business continuity planning has, as a result, started to adopt a new version that can adapt to both natural and man-made catastrophes.” (Chris Steele, 2002)

According to an article written in 2000 by Felipe Alonso, Risk, and Advisory Services, 40% of companies who suffer a catastrophe go out of commercial enterprise within two years while institute for Business and Home Safety, states that 25% of businesses never reinstate following a significant disruption

‘‘Business survival depends on the assured continuity of core business activities and supporting services” (Gregory Morwood ,1998). And “how businesses prepare, and the plan is critical to their ability to handle an unexpected situation and will determine whether they can prevent an incident from turning into a crisis”. (Clark Graham,2012). Business Continuity (BC) is defined “as the capability of the organisation to continue delivery of products or services at ideal levels following a disruptive incident.” (ISO 22301:2012)

Interning at Whiterock Finland KY, was an opportunity to be part of the risk analysis team for the tour and travel business newly established by the company, and this gave an understanding the many risks involved in a tour and travel business from small disruption to critical issues. The need for Business Continuity Plan (BCP) in White Rock KY became necessary. The primary motivators for developing a BCP are to keep the business running, reduce liability, and lower the impact of any market disruption.

1.1 Thesis Information

The purpose of the thesis is to explore Business Continuity Management and create a Business Continuity Plan as it is the primary objective of the thesis. Also Identifying the possible impacts directed to the company because of a disruption.
This study will give insight on business continuity planning and the procedures to implement a business continuity plan. A BCP is one of the crucial components of any recovery strategy after a disruption. Sadly, not every organisation develops a continuity plan because not all types of body are mandated to have one. This study will create an understanding of the importance of business continuity plan and the effects of not having one, via reviewed literature.

In this thesis, the focus is only on the tour and travel business of White Rock KY, excluding another area of business. This research does have a generalising approach for the business continuity, but it is more focused on the case company, so every company needs to tailor its business continuity plan to suit the risks, and another thing that applies to them while using this research. Moreover, even though, the situation and scenario of the disruptions would be different for each company, the facts were favourable to establish the importance of a business continuity plan within an organisation.

The target group is the case company in which the BCP is created for and other enterprises mainly on management level, background information on the effects of implementing BCM into their organisation is provided. Also, the thesis is targeted undergraduates studying security, risk management or subjects related to those areas.

The Research questions

a. How can a model process be used in developing a business continuity plan?
b. What are the steps in preparing a business continuity plan?

1.2 Company Profile

The core business of the company is educational service consultation and another branch of its business providing tour and travel services. Visit West Africa is an initiative of WHITEROCK FINLAND KY, and this is the section of the company this thesis will focus. They organise group tours to unpopular travel destinations in West Africa. They arrange everything from accommodation, sightseeing to adequate security.

Basic Information:

Name of the Company: WHITEROCK FINLAND KY
Registration Date: 2014
Legal Formation: General partnership
Y-tunnus: 28066589
Annual Turnover: €1,2m.

2 Theoretical Framework

Theoretical framework is, “A group of related ideas that provides guidance to a research project or business endeavour. The appropriateness of a theoretical framework that a marketing department is using to promote its corporate and product image to the consuming public can be an important determinant of its ultimate success.” (Business Dictionary)

2.1 Business Continuity Management

In this chapter Business Continuity and Business Continuity Management is being defined moreover, the different steps to bring a Business Continuity Plan into the company are being studied. There are still no set standards, so terms connected with the BCM are defined differently depending on the source. Several definitions will be brought up in this chapter and then looking at the similarities and secondly set definitions used in this study.

Business continuity

Business continuity is "the process of foreseeing incidents which will affect critical functions and activities of the organisation, and ensuring response to any such incident in a planned and rehearsed manner" (BCI,2008)

Business continuity management

Business continuity management is the whole process that identifies the potential risk that threatens an organisation and provides a structure that helps develop resilience, which also protects key interests of an organisation (BCI 2008). Hiles and Barnes 1999 define Business Continuity Management to mean ensuring the constant provision of products and services. BCM is also a process with several different, but complementary elements that ensure key business practices and output never cease irrespective of circumstances."

Business Continuity Planning

"The planning and preparations which are necessary to identify the impact of potential losses to formulate and implement viable recovery strategies, to develop recovery plan(s) which ensure continuity of business services after an emergency or disaster and to administer a comprehensive training, testing and maintenance programme" (BCI 2008).

The Business Continuity Plan consists of four elements which are Disaster Recovery, Business Recovery, Business Resumption, and Contingency. See figure 1 below

BCP	Disaster Recovery	Business Recovery	Business Resumption	Contingency Planning
Objective	Critical Computer Apps	Critical Business Processes	Process Restoration	Process Workaround
Focus	Data Recovery	Process Recovery	Return to Normal	Make Do
Example Event	Mainframe or server failure	Laboratory Flood	Building Fire	Loss of Application
Solution	Hot Site Recovery	Dry Out & Restart	New Equip. New Bldg.	Use Manual Process

Figure 1: Four BCP Elements (sopinion8ed.wordpress.com)

Contents of the BCP

In addition to the items already recommended above the Business Continuity Plan should contain an action plan or task list with the checklist

1. how to activate the BCP;
2. the person(s) responsible for enabling the BCP;
3. the procedure that person(s) will adopt in taking that decision;
4. the person(s) consulted before such a decision is made;
5. the person(s) who should be informed once a decision has been taken;
6. Address of the Meeting point;
7. Services that are available, also third-party resources;
8. The primary means of communication;
9. There are detailed procedures for manual work and system recovery if necessary.

2.2 Framework for Business Continuity Management

Authors have tried to answer the question of what elements make up the formal BCM system. Ian Storkey gave a six steps framework while Gilbert and Gips saw a BCM system as consisting of four major elements: risk identification, risk assessment, risk ranking risk and management. Six steps BCP/DRP framework by Ian Storkey, Business continuity institute(BCI) and ISO, all frames that would be discussed below. These prove the point that there are various ways to divide the different steps in making a Business Continuity Plan. The Business continuity institute framework is explained below. Regardless of which framework a company chose to work with, it needs to be modified to suit the company's requirements. Gallagher (2005) describes the steps and elements of a BCP.

2.2.1 ISO 22301:2012

“ISO International Organization for Standardization is the world's largest developer and publisher of International Standards. Established in 1947, ISO is a network of the national standards institutes of 159 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.” (ISO International Organization for Standardization)

ISO 22301:2012 is the world's first international business continuity management standard. ISO published it on June 15, 2012 and It cancels the old BS25999 business continuity standard as it was deemed obsolete and replaced by the ISO 22301: 2012. (ISO22301:2012). Cancellation of the BS25999 ensures consistency with all future and revised management system standards and make integrated use more comfortable with, for example, ISO 9001 (quality), ISO 14001 (environmental) and ISO/IEC 27001 (information security). The standard is divided into ten main clauses, starting with scope, normative references, and terms and definitions. Following these are the standard’s requirements. business, taking proactive approach to minimising the impact of incidents, critical functions are kept up and running during times of crises, minimization of downtimes during events and improvement of recovery time, demonstration of resilience to customers, suppliers and for tender requests (ISO 22301)

The following documents are mandatory if an organisation wants to implement ISO 22301:
List of applicable legal, regulatory, and other requirements
Scope of the BCMS
Business Continuity Policy
Business continuity objectives
Evidence of staff competencies
Records of communication with interested parties
Business impact analysis
Risk assessment, including risk appetite
Incident response structure
Business continuity plans
Recovery procedures
Results of preventive actions
Results of monitoring and measurement
Effects of internal audit
Results of management review
Consequences of corrective actions

Other standards that are helpful in the implementation of business continuity are ISO/IEC 27031, PAS 200, PD 25666, PD 25111, ISO/IEC 24762, ISO/PAS 22399 and ISO/IEC 27001.

2.2.2 ISO 9001:2015

ISO 9001 is a standard which helps an organisation to improve its overall operational performance. The potential benefits, stated in the ISO 9001:2015 manual, include:

1. Provided products and services that meet customer, legal and regulatory requirements
2. Enhance customer satisfaction
3. Finding opportunities and indicate risks

The ISO 9001 standard approaches the quality management with Plan-Do-Check-Act cycle, which gives the organisation the opportunity to plan its processes and the interactions between them. The Plan-Do-Check-Act cycle also ensures that the methods and functions have enough resources and are properly managed (ISO 9001:2015).

One of the critical parts of ISO 9001 standard and its implementation is vital risk-based thinking which enables the organisation to map out the factors which could deviate the processes from the wanted results. The ISO 9001 standard gives the organisation the tools and the framework on which it can build the most suitable quality management system for itself.
See figure 2 below for a representation of the Plan-Do-Check-Act cycle.

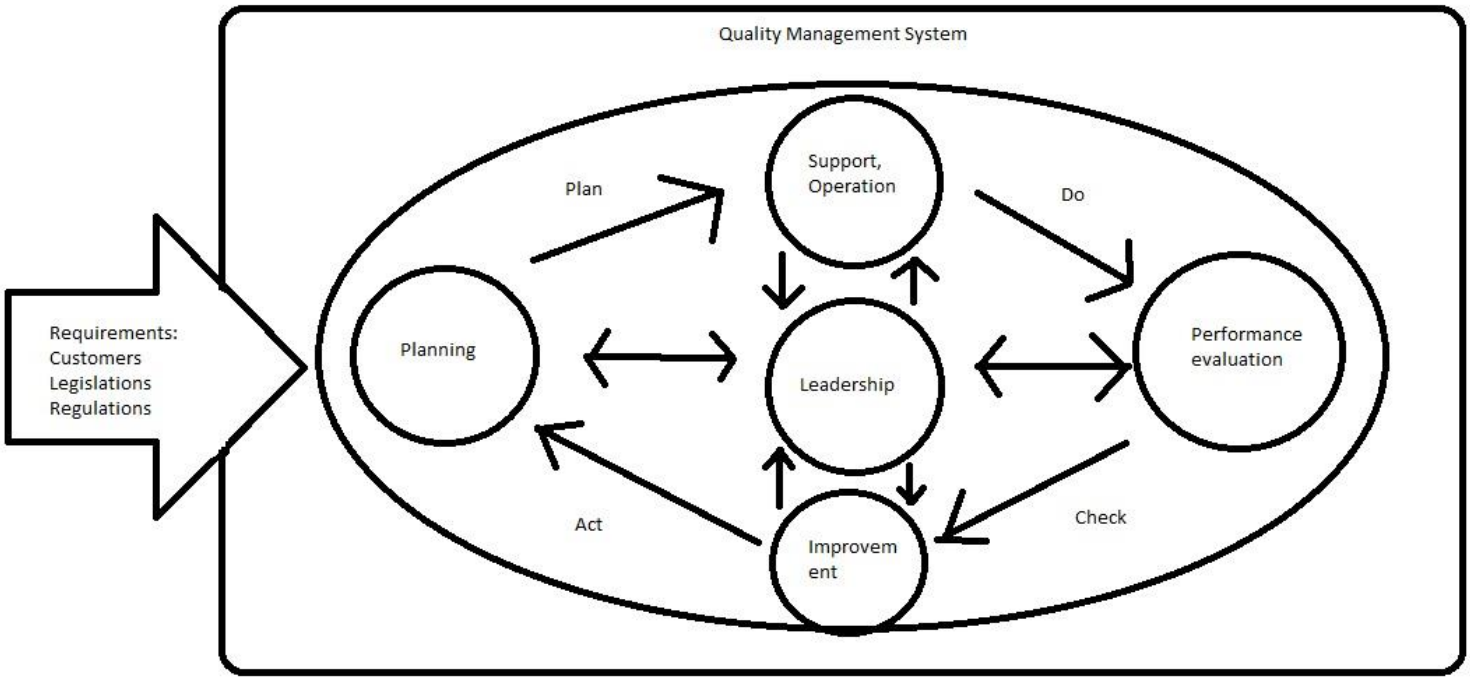

Figure 2: Plan-Do-Check-Act cycle (ISO 9001:2015)

2.2.3 ISO 31000

13th of November 2009 marked the publication of ISO 31000, and it provides a standard for the implementation of risk management. The purpose of ISO 31000:2009 is to be applicable and adaptable for "any public, private or community enterprise, association, group or individual. Accordingly, the general scope of ISO 31000 is as a family of risk management standards and not developed for an industry group, management system or subject matter field in mind, but to give best practice structure and guidance to all operations, concerned with risk management. It uses the generic approach, and it is not specific to any industry or sector it can be applied to any risk (financial, technological, natural, project) and can be applied to any organisation. (Technocratgroup.com, 2017)

"ISO 31000:2009 gives a list in order of preference on how risk can be dealt with:
Risk avoidance by avoiding the activity that gives rise to the threat.
Accepting the risk by engaging in activity that leads to the risk.
Completely removing the risk source
Changing how likely the risk is to occur
Changing the consequences of the risk
Sharing the risk with 3rd party
Retaining the risk by decision" (ISO3100:2009)
The critical elements of the risk management process are shown in figure 3 below.

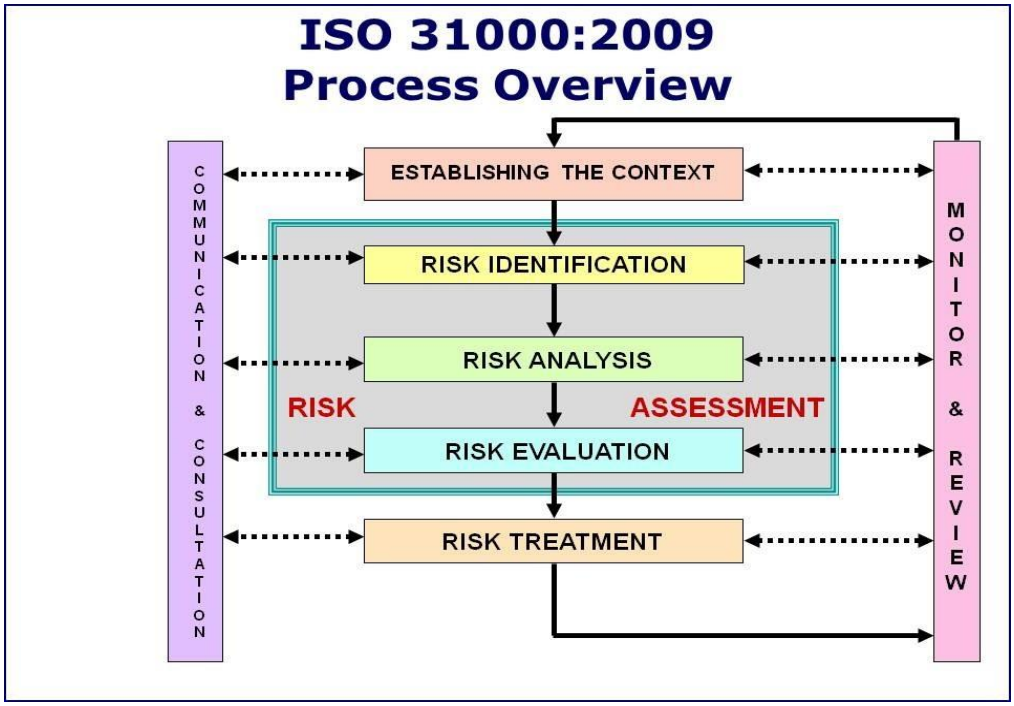

Figure 3: Risk management process (ISO3100:2009)

The activities of identification, analysis and evaluation make up the “risk assessment” part of the risk management process and are the responsibility of the risk owner. The risk owner is specific to the assessment and may be the project manager, chief investigator, organisational unit head, or another staff member with responsibility and accountability for the activities or area being considered.

Many other standards also relate to risk management, which is “ISO Guide 73:2009, ISO 31000, ISO/IEC 31010:2009.

2.2.4 Business Continuity Good Practice Guideline 2008

The framework is divided into six sections (see figure 4):

1. BCM programme management

2. Understanding the organisation

3. Determining business continuity strategy

4. Developing and implementing a BCM response

5. BCM exercising, maintaining, and reviewing BCM Arrangements

6. Embedding BCM in the organisation’s culture (risklogic.com.au)

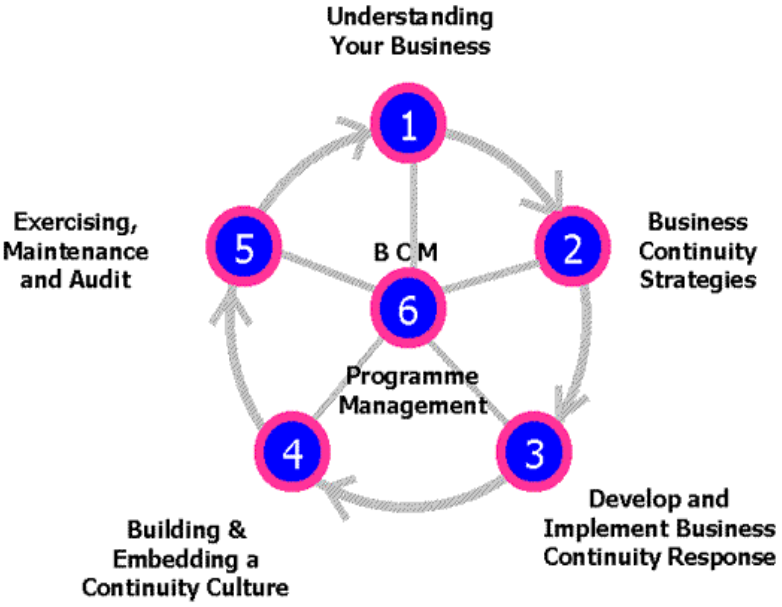

Figure 4: The BCM Lifecycle—BS 25999-1 (The Business Continuity Institute 2007)

1 BCM programme management

Programme management is the centre of the Business Continuity process. The way the organisation approaches the programme depends on the program management. Management's involvement is vital to ensure that the right people are appointed and made accountable for the BCM policy and one or more persons to implement and maintain.

2 Understanding the organisation

This part of the lifecycle identifies the company's essential products and services and the critical activities and resources that support them. This is done with the aim of understanding the organisation. This ensures the BCM programme is in line with the organisation's objectives, vision, obligations, and legal duties. The environment in which the organisation operates, assets and resources, with the inclusion of those outside the organisation, that supports the delivery of these products and services.

A Business Impact Analysis(BIA) is made to "assess the impact and consequences over time of the failure of these activities, assets, and resources" (BCI) It's also in this phase that a risk analysis is made and Selection of risk mitigation strategies.

3 Determining business continuity strategy

This phase is about implementing countermeasures to reduce the likelihood of events happening or decrease the potential impacts of that incidence. It is about ensuring the organisation continues during, and after an incident. The most appropriate strategy depends on the maximum tolerable period of disruption of significant activities, cost of implementation, and consequences of inaction. The right plan needs to be used to maintain the core competence and skills in the organisation. Example of strategy that can be used is the ability for people to work from home in case of problems with premises, use of another supplier, back up information, cold site, and other strategies.

4 Developing and implementing a BCM response

This phase of the BCM lifecycle ensures exercises are performed, also organisations arrangements are kept up to date. The company should structure an incident response that will allow adequate response and quick recovery. To ensure things are done the way it should, a response team should be created, and for example, it can be called crisis management team or Disaster recovery team or whatever just, so people are more responsible and accountable in ensuring a quick recovery. The team should have arrangements for the activation, operation, coordination, and communication of the incident response. Figure 10 illustrates the three major phases over time of an incident, and how incident management and business continuity relates.

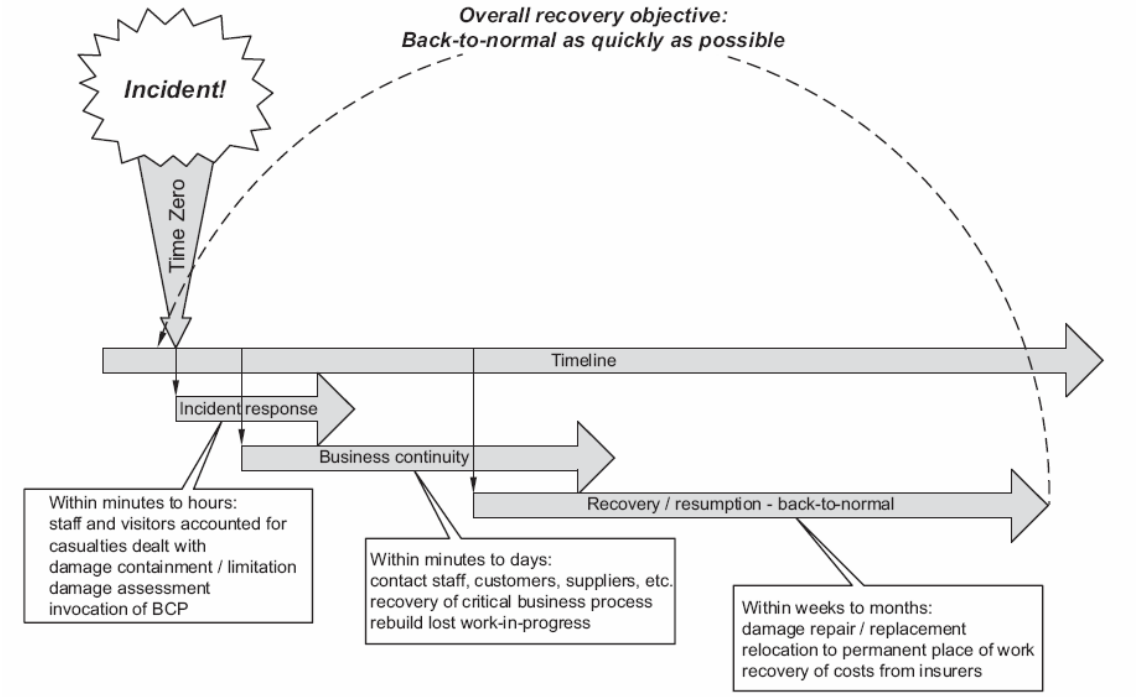

Figure 5: Recovery overview (The Business Continuity Institute 2007)

5 BCM exercising, maintaining, and reviewing BCM arrangements

This phase of the BCM lifecycle ensures the BCP is activated and regularly rehearsed and kept up to date. This gives a guarantee that the plan will work. The technical, administrative, communication, logistical, procedural, and other operating systems of the BCP should be exercised. Also, the infrastructure, relocation of staff, telecommunication and even third-party resources should be tested. The testing and review allow room for improvement and mastering of what to do in case of an incident.

6 Embedding BCM in the organisation's culture

To achieve a successful outcome, business continuity must become part of the company. Embedding BCM in the company's culture ensures BCM becomes part of the organisation's core values.

2.2.5 Finnish Consumer Safety Act

Another theory relevant to this thesis is Finnish Consumer Safety Act by the decision of the Finnish Parliament. This act applies to consumer services that are supplied, performed, marketed, and sold in Finland. Service providers are obliged to make a notification to the supervisory authorities and should also prepare a safety document containing a plan for identifying, controlling risks, and providing warning of said risks.

"In drafting the plan, the service provider must take account of the nature of the service and the scale of the activities in question. The safety document shall be kept up-to-date.
Service providers shall ensure that the persons or parties participating in the provision and performance of the service are familiar with the contents of the safety document. Where necessary, service providers shall organise training for the persons and parties participating in the provision and performance of the service." (Consumer Safety Act - Tukes.fi)
A Government degree may issue further requirements on the contents of the safety document. (Finnish Statute Book (920/2011)

2.2.6 BC planning Process Using Risk Based Approach

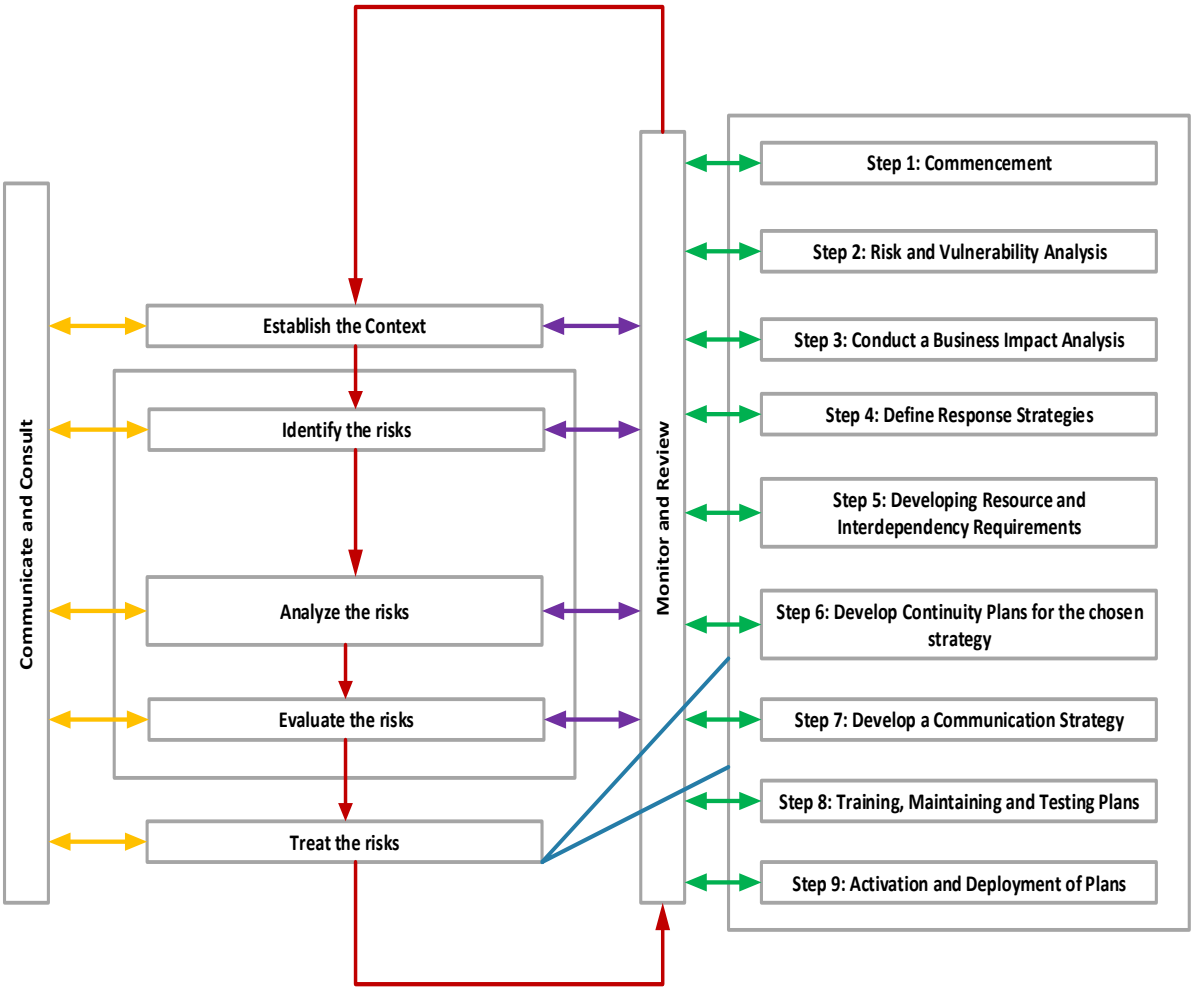

Figure 6: BC Planning Process using Risk-Based Approach. ISO 31000

Step one-The commencement:

The project initiation is the significant part where it was necessary to have all-round support from the organisation's management. Failure to achieve proper project initiation make it more likely for futile resistance towards the BCP project.

Step 2- Risk and Vulnerability Analysis:

The Risk analysis provided an understanding of the organisation's core business functions, its critical processes, Assets, the extent of the contribution of each asset, risk and vulnerability that can cause disruption or loss. Threats to core business function continuity, also threats to the people, information, processes, asset, resources were identified. After identification, these threats were analysed, their likelihood of occurring, a consequence of disruption rated using the consequence ratings in the risk management framework. Potential improvements were identified, and a way to mitigated vulnerability was suggested and in some cases, risk was accepted thereby reducing any residual risk to an acceptable level.

Step 3- Business Impact Analysis:

Business Impact Analysis (BIA), also referred to as Business Consequence Analysis is the process of analysing activities and the impact that a business disruption might have upon them (ISO 22300) The BIA was aimed at building an understanding of disruptive implications or potential problems which require treatment. The business impact analysis was done alongside the cause analysis (RCA)to understand the foundation of the problem.

Step 4- Define Response Strategies:

Determination and selection of strategy were based on outputs from the BIA and RCA and built upon the Maximum Acceptable Outage (MAO) identified for each critical process. Appropriate business continuity strategy to protect the organisation's core functions and essential business processes, stabilise, sustain, re-cover, and restore functions, services, critical methods, their dependencies and supporting resources. In this step Response strategy, Recovery time objective (RTO), Recovery point objective(RPO) were determined.

Step 5- Developing Resource and Interdependency Requirements:

The Business Continuity plan will indicate the resource required to support critical processes and define where resources are shared. The resources considered include, but not be limited to people, information and communication technology, equipment, facilities, third-party arrangements and supplies, transport and coordination, data, and information.

Step 6- Develop Business Continuity Plans:

The BC Plan was then set up defining roles and responsibilities, invoking the process for the response, list of critical suppliers, vital records, details of third-party interdependency relationship provide, contact details of people and teams also the authority to contact during and following the disruption.

Step 7 - Develop a Communication Strategy

A communication strategy was then developed. It was done to ensure availability of the means of communication during an event, facilitate structured communication with emergency responders, vital record information about the fact, actions were taken, and decisions made.

Step 8-Training, Testing, and Maintaining Plans:

A brief orientation is given to the top executive officer, who will then pass knowledge to a member of staff. To avoid the plan ending up a folder on the bookshelf, it is essential that the plan is regularly tested to discover weaknesses, keep employees updated and improve the plan. Tabletop scenario exercise will be used to test the plan.

2.2.7 BCP/DPR Frame by Ian Strokey

1. Documentation of business activities, critical processes, and systems
2. business impact analysis to assess probability and impact
3. Develop BCP/DRP (include third parties)
4. Implementation or update of the BCP/DRP
5. Training
6. Regular testing and updating (Annually)

2.2.8 Gibbs and Buchanon BCP Framework

Gibbs and Buchanon are using nine phases.

1. Program initiation.
2. Project initiation.
3. Risk analysis.
4. Risk mitigation strategies selection.
5. Monitoring and control.
6. Implementation.
7. Testing.
8. Education and training.
9. Review.

3 Research Methods

According to the Business dictionary, research methods are processes used in collecting information and data for decision-making purposes. The methodology may include Interviews, surveys, publication research, interviews and other research techniques, and this information can

be present and historical. Research methodology can be quantitative or qualitative. “Qualitative research methods are looking at the intangibles factors that are not purely numbers driven but can be just as important as looking at the numbers while Quantitative research methods mean looking at actual numbers at different financial metrics, ratios, and statistics that are fundamental to the analysis being looked at.” (Jeffrey Glen, Nov 2013) Qualitative research methods are used for this development project reason being that qualitative research methods are useful in providing rich descriptions of complicated phenomena, qualitative research is systematic and rigorous, and it seeks to reduce error, and to identify evidence that disconfirms initial or emergent hypotheses. (Robert P. Luciano, 1999)

This chapter gives insight into the research design as well as outlining the research methodologies, the collection method of the data, the relevant data processing techniques and process applied in interpreting the collected data. What it aims is to provide an overview of the methods used in conducting the research and obtaining the data required to fulfil the development goal. The means chosen fits the objective of this study and using different methods in collecting and analysing data gives stronger evidence because the approaches complement each other. The most important methods of the study are workshop, theme interviews and literature review.

3.1 Workshop

A risk workshop is a brainstorming session that allows room for Identify each risk that a company is subjected to, determine how significant each risk is, and whether each risk is acceptable or not. A Risk assessment workshop was organised this enabled the company management and some member of staff to both contribute and learn in their natural environment (resolver.com). The workshop lasted about 3-4 hours for two days and two senior managers, and two employees were present at start up sauna at alto university. Beyond the personnel costs, there were also scheduling challenges. The result was not only ranked by a list of critical risks, but also discussion about the control environment, risk, and risk tolerances. During the workshop impact of business, the disruption was discussed which enabled the making of the business impact analysis. The staff members and management walked away from the session with more understanding of the business operations, objectives, and challenges. Management and staff were equipped with the knowledge and the detailed analysis to make improved business decisions. The key benefit from the workshop includes a prioritised list of risks, assigned action plans for each risk, discussion of risks by management and some member of staff, awareness of different viewpoints. Check Risk assessment workshop report in chapter 4 table 5.

3.2 Interview

An interview is a verbal discussion between two or more people with the objective of collecting valuable information for research purpose. McNamara, 1999 states that Interviews are useful for getting the story behind a respondent's experiences. The interviewer can get in-depth information on the topic and Interviews may be helpful as a follow-up to individual respondents. "The main task of interviewing is to understand the meaning of what the interviewees say". (Kvale, 1996) An interview was used in this research to relate to businesses with already existing BCP and get information regarding it.

Nine companies where interview by me with a total of twelve meetings including the case company but only five provided relevant information about to this study. The initial plan was to interview just small and medium enterprises but after the interviews information is gotten were irrelevant because all companies interview was either unaware of BCP or considered having insurance has a BCP. Four more prominent company was then interviewed. Information from Interviewing Four firms was enough for this thesis level according to Eisenhardt (1989), who wrote in her book building theories from a case study that 4 to 10 company cases would be the suitable amount. The interviews can be found in chapter 4 tables 1-4.

3.3 Literature Review

"A literature review is a critical and in-depth study and evaluation of existing research in a particular field of study or related subject." (Martyn Shuttleworth Sep 16, 2009) Much research has been done on business continuity planning and disaster preparedness with many revelations of increase in awareness about the issues in recent times. However, many of the researchers and surveys concluded that the knowledge of business continuity is not translating into disaster preparedness plans. In this chapter, a review of related literature will be exhibited to give a theoretical foundation to create an understanding of the importance and purpose of business continuity management as a business process that aims to neutralise organisational risk, disasters, and crises.

Despite the overwhelming evidence of its influence, many companies do not have well-defined business continuity management protocols in place to minimise the costs and risks that may be engendered by adverse events internally or externally to the company. More generally, many companies do not look at the specific sources of potential risks, e.g., information systems, processing lines, storage facilities, employee accidents, and many others. This poor appreciation of this vital business activity has contributed to significant challenges especially for many travel and tourism companies, hence the need for this project.

The literature review provides a useful source of information about the Business Continuity/Disaster Recovery BC/DR. This report consists of definition disaster recovery, business continuity and how to decide what practise areas are essential for successful recovery. The articles also cover how to plan and implement BC/DR strategies, how business benefits of BC can be measured, factors that avert effective disaster preparedness of businesses and whether previous BC/DR strategies have tested beneficial.

Resilience

Resilience is the ability of an organisation to resist being affected by an event (ISO/PAS 22399) Resilience is also the ability to become healthy and prosperous again after something terrible happens (continuitycentral.com). Resilience has, in the past decades, been a term increasingly employed throughout many filed including business administration, disaster planning, and international development. Dr Linkov and Palma Oliveira's book on "Resilience and Risk is focused emerging field of resilience analysis See figure 7 below. The book starts with a chapter which gives an overview of resilience and explains how resilience driven techniques solutions can be to growing challenges such as loss of biodiversity or cybersecurity in its ability to guard towards the consequences of unknown or unexpected occasions.

RESILENS is a task funded by the European Union's Horizon(EUH) 2020 Research Studies and Innovation Programme for the development of gears that support management with the improvement of resilience. One of the tools developed by this project is the European Resilience Management Guidance (ERMG). This device guides several topics like risk management, budget and financial issues, information management systems, business continuity, and risk communication. (resilens.eu)

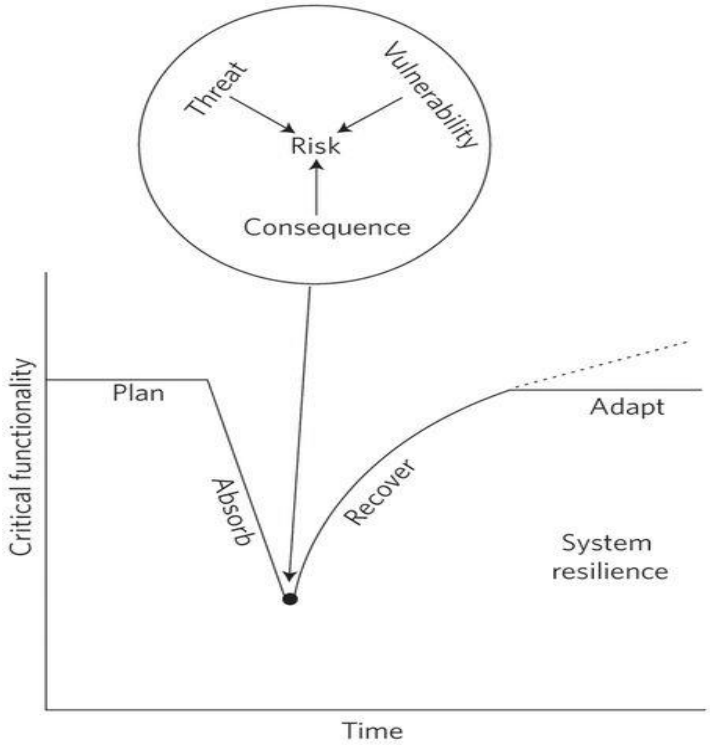

Figure 7: Resilience integration (media.nature.com)

Review of BCP Literature

Swartz (2003) writes about BC/DR plans and which elements are essential to their success. These plans considered as guidelines that ensure a high probability that businesses will outlive a disaster without long-lasting unfavourable effects. Swartz (2003) notes that only about one-fifth of companies in the USA have developed them. Degerfalk and Larsson (2006) confirm that the area of Business Continuity Management has received much attention over the last couple of years as a result sudden disruptions and subsequent losses in big global organisations. Many organisations prioritise business continuity methods that take IT into account, but other elements are essential. Wallace and Webber (2008) explain what should be the basis of prioritising a business continuity plan for more details. Arrangements should be done using input from and think about the needs of, facilities control, human resources, and executive workforce. According to Swartz (2003), overall BC plans ought to include DR as a subcategory, alongside another sort of disruption which causes varying amounts of damage. They need to determine backups, and options for strategies and processes, mainly IT functions, along with functions that cannot be interrupted for the business to continue running. Although Swartz (2003) frequently gives broad recommendations, they could prove beneficial for establishing general BC/DR policies.

Hotchkiss (2010) discusses why we need to have a business continuity plan, what exactly is a continuity plan, how to differentiate between business continuity plan and management, and why management plan fails. Hotchkiss (2010) defined a continuity plan as a collection of things you do when something goes wrong. Hotchkiss (2010) explains that for each potential risk there should be a procedure (or plan) to be executed to get you out of the mess. "A business continuity plan is a document which breaks down into all the little sub-plans (or procedures) to execute when things go wrong" (Hotchkiss, 2010). As previously stated there should be the procedure for every risk retained by a business and no process for those not maintained. The process should work in most cases as long as the threat materialises in the exact form as expected and it is possible that the risk does not emerge in the precise way expected. A new chance could also occur which was unforeseen and for which there are no plan Improvisations, or modifications of a similar procedure should be used in that case. It is essential that, when this happens, the new risk and new process are formalised and included in the plans. This leads to the need for Business Continuity Management (Hotchkiss, 2010).

Hotchkiss (2010) defines BCM as a lifecycle from reviewing risks on a regular basis, updating procedures in the light of the new threat, changed risk or changes in the resources needed to implement a particular method, communicating and training all staff regularly, testing plans periodically and auditing regularly. Failure to undertake all steps means the program exists but no management which will result in eventual collapse of the plan. According to Hotchkiss (2010), the significant effect of the failure of a continuity plan is taking longer than the need to get back to business after an outage. Reasons for failure of failure of continuity management as stated by Hotchkiss (2010) includes: not executing an impact analysis; not understanding the

time commitment required in the initial development of continuity plan and the on-going responsibility to keep the plan up-to-date and test it; Not understanding the advantages. A continuity plan has benefits to a business regarding efficiency and market competitiveness and advantages to customers of the company. If neither of these is fully understood and communicated, the continuity capability will often be seen only as a cost for events which are unlikely or whose consequences is overdramatised. Hotchkiss (2010) gave an excellent introduction and definition to the concept of continuity plan and also differentiates continuity plan from continuity management.

Jones (2011) extensively discusses business continuity management and its goals. According to Jones (2011), Business continuity plans or planning is a comprehensive procedure which determines likely risks, their potential impacts and plans for both risk mitigation and Disaster Recovery strategies". A disaster recovery plan is a plan in writing, for recovering one or more information structure at an alternate site in response to a significant hardware or software failure or destruction of facilities (Swanson, Lynes and Gallup, 2010). This process must consider not only an organisation's stakeholders, from clients to personnel but also its brand and cost producing activities (Jones, 2011). Furthermore, it must be entirely included in the entire organisation to be successful (Jones, 2011). Together with incident response, information security and records control should also be taken into consideration. It includes documenting facts, records and information systems to be protected and recovered, and codifying guidelines for doing so.

Fernandes and Saldanha da Gama (2008) distinguished between two concepts found in the literature that create some ambiguity, namely the Contingency Plans (CP), and Business Continuity Plans (BCP). Fernandes and Saldanha da Gama (2008) illustrates that CP is an operational procedure to restore the operation of a business process or a system, which is facing a situation of contingency. A BCP has a broader scope in the wake of a very critical condition where the survival of the company is at stake according to Fernandes and Saldanha da Gama (2008). Fernandes et al. (2008) mentioned that the BCP typically includes the CP. Fernandes et al. (2008) explain the need for the linkage of contingency planning to supply chain. It is known that Supply Chain dynamics and individual members are more fault-prone than previously assumed. This results from the interaction between the various autonomous members that leads to in numerous states on the local as well as the supply chain level. Hence the existence of possible risks has to be assumed thus resulting in the development of proactive and reactive risk management as a relevant success factor in control (Fernandes and Saldanha da Gama, 2008). Fernandes et al. (2008) identify two broad categories of risks that affect supply chain design and management: (1) risks arising from the problems of coordinating supply and demand, and (2) risks resulting from disruptions to normal activities. This case study demonstrates the importance of contingency planning in Supply Chain Management as well as in traditional business.

Wallace and Webber (2008) describe the strategies for developing a good business continuity plan. Essential steps as mentioned by Wallace and Webber (2008) are to ensure the scope of the project is well defined, careful selection of right team members, Identification of activities required, their durations and who should do the work, to communicate with the entire organisation and lastly to test the plan. Wallace and Webber (2008) also define Business Impact Analysis (BIA) which according to Wallace and Weber (2008) is an exploratory review of the essential functions that are essential for the operation of the business. Active and vocal support from senior management, a capable project leader, complete and honest answers from each department, a well-crafted questionnaire are the requirements for a successful BIA (Wallace and Webber, 2008). Also, Wallace and Webber (2008) defined risk as the potential of a disaster occurring, and propose that risks should be prioritised based on the severity of the damage, the probability of the risk happening and the difficulty of possible avoidance and mitigation options.

Graham (2012), describes that unpredictable factors can have impact on the work environment of any organisation, and illustrates the tsunami in Japan, the repercussions of which were felt throughout supply chains in South-East Asia and beyond, the eruption of Eyjafjallajökull, the civil unrest in the UK in the summer of 2011 as factors that have caused not only physical damage but also reputational damage. According to Graham (2012), 85% of respondents had experienced at least one supply chain disruption in 2011. Graham (2012) study shows that that of those companies affected by supply chain incidents, these reduced productivity levels for almost 50%, and also led to an increased cost of working by 38% and loss of revenue by 32%. Graham (2012) study revealed that the challenges of DHL supply chain implementation of a consistent and straightforward BCM process across all of its operational sites were threefold due to its global nature, the number of services the business provides and lastly, the number of customers the company provides service. Graham (2012, p.19) outlines the Ten-Point Programme adopted by DHL to enable them to implement and maintain a consistent BCM programme across their diverse sites. Graham (2012, p.19) concludes that a BCM strategy that includes a dynamic supply chain able to react to potential problems easily is crucial for businesses to enable them to remain as operational as possible in the event of a disruption.According to ("Business continuity plans: a position for recovery", n.d.), Aviva Survey recorded that companies that don't have disaster recovery and business continuity plans (BCPs) are more likely to close down in the first two years of trading.

Half of SME owners who participated In the Aviva survey revealed they had no BCP in place, and a further 16% said they did not see a need to have one. About 36% of participants were aware of BCP and its importance, while 28% of business owners said they had a functioning BCP in place. The remaining 6% did not know if they had a BCP or not. The study found out that 33% of SMEs believe it would take them only a week and 31% think a month would be sufficient to return to regular trading following severe incident or interruption. However, Aviva says a return to full trading can regularly take a business more than 12 months. Information backed up by the Federation of Small Businesses, which means "80% of SMEs suffering from a major disruption

closes in 18 months, while 90% of SMEs that encounter a data loss from a cyber-attack or another disaster close within two years. That is the main fear considering 99% of businesses in the United Kingdom have less than 50 employees". In a record of major incidents and small business, the FSB states: "Small organisations, by their nature, are more liable to the impact of major incidents and disasters and the impact all too regularly is terminal. This has a severe effect on the entire supply chain in which they were involved and their community ".

4 Data Analysis

Data Analysis

This chapter will show the result of the workshop, interview analysis, risk analysis, business impact analysis and cause analysis, and further discuss their outcomes.

Interview Analysis

Nine companies were interviewed with a total of twelve interviews including the case company but only five provided relevant information about to this study. The initial plan was to interview only small and medium enterprises but after the interviews information is gotten were irrelevant because all companies interview was either unaware of BCP or considered having insurance has a BCP. Four more prominent company was then interview using phone interview after scheduling a time via email because was difficult getting to interview bigger companies in Finland due to the language barrier. Information from Interviewing these Four companies are analysed below.

Company A

This company provides legal, taxation, investment, fiduciary, and financial administration services to private, corporate, and institutional clients. The firm currently employs over 300 employees with ten offices across Africa, the Europe and America. It has over €120 billion worth of international assets under its administration.

Questions	Company A	Analysis of answers
Does the Organisation have a written business continuity plan?	Yes	
Where is the company's BCP kept and who can access this document?	It is kept on share point, so every employee can view it	employers and employees need to be familiar with the content of the plan and their role in the response and recovery.

Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, Location for staff to operate from but we all know it will be from their homes.	
Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP	
Do business continuity and disaster recovery readiness have the support of top management in your organisation? Moreover, if not why?	Yes	Get senior management involved and keep them committed.
What happens if key personnel are not available during a disaster	3rd party is readily available	For a plan to succeed, there must be multiple agency cooperation moreover, involvement.
How frequentlyis the BCP reviewed and updated? How are business critical applications identified?	Our testing is done bi-annually	Keep the plan current – Update the plan as applications get updated
Are back-ups done faithfully and does it include every server and hard disk?	Yes, daily due to the nature of our business.	
How often do you perform a BCP test?	Every six months.	Test the business recovery process and evaluate test results
Does the company BCP highlight what are acceptable downtimes after specific disasters	Yes	Identify recovery point objective (RPO) and recovery time objective(RTO), making sure data protection solutions can meet these requirements.
Has the company experienced major disruption/disaster	Yes	
What was the impact of the Disruption/disaster on business?	Our reputation.	

Table 1:Interview A

Company B

Company B is a tour operator firm with excellent reputation in service rendering to her client as a tour operator the company, also plan tour events and organise regarding transport, accommodation and feeding. The company has 150 employee all full working time.

Questions	Company B	Analysis of answers
Does the Organisation have a written business continuity plan?	Yes	
Where is the company's BCP kept and who can access to this document?	Kept on SharePoint for the whole company to see	employers and employees need to be familiar with the content of the plan and their role in the response and recovery.
Are there any exclusions to your BCP such as personnel, natural disasters, and why?	No	
Does the DRP form part of the BCP or is it a separate plan altogether?	Yes, it is part	
Do business continuity and disaster recovery readiness have the support of top management in your organization? Moreover, if not why?	Of course,	Get senior management involved and keep them committed.
What happens if key personnel are not available during a disaster	3rd party supplies are on standby	For a plan to succeed, there must be multiple agency cooperation moreover, involvement.
How frequently is the BCP reviewed and updated? How are business critical applications identified?	Every six months	Keep the plan current – Update the plan as applications get updated
Are back-ups faithfully and does it include every server and hard disk?	All business-critical servers are backed up daily.	
How often do you perform a BCP test?	Every six months.	Test the business recovery process and evaluate test results
Does the company BCP highlight what are acceptable downtimes after specific disasters	Yes, up to 99%	Identify recovery point objective (RPO) and recovery time objective(RTO), making sure data protection solutions can meet these requirements.
Has the company experienced significant disruption/disaster	Yes	
What was the impact of the Disruption/disaster on business?	Goodwill loss	

Table 2: Interview B

Company C

Company C is a massive cultivation and poultry farm that cultivates, produces and exports agricultural and livestock produce such as cassava, eggs, snail, livestock, fish, and animal feed. Other services include export such as agricultural produce and livestock produce and Hatchery services

Questions	Company C	Analysis of answers
Does the Organisation have a written business continuity plan?	Yes	
Where is the company's BCP kept and who can access this document?	It is kept on SharePoint, and all office staff can assess it	employers and employees need to be familiar with the content of the plan and their role in the response and recovery.
Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, not enough farm staff in the plan only office staff	
Does the DRP form part of the BCP or is it a separate plan altogether?	Yes	
Do business continuity and disaster recovery readiness have the support of top management in your organization? Moreover, if not why?	Yes	Getting senior management involved and keeping them committed is always important.
What happens if key personnel are not available during a disaster	There is an agreement with third party suppliers for support in the event of a disaster.	For a plan to succeed, there must be multiple agency cooperation moreover, involvement.
How frequently is the BCP reviewed and updated?	Annually at least after our 2014 bird flu disastrous event that killed almost all our chickens and turkey	Keep the plan current – Update the plan as applications get updated
Are back-ups done faithfully and does it include every server and hard disk?	All important business servers are backed up daily.	
How often do you perform a BCP test?	Every six months. A user test is done once a year to ensure that all applications restored are fully operational.	Test the business recovery process and evaluate test results
Does the company BCP highlight what are acceptable downtimes after specific disasters	Yes, form part of the BIA.	Identify recovery point objective (RPO) and recovery time objective(RTO), ensure data protection solutions can meet these requirements.
Has the company experienced significant disruption/disaster	Yes. Bird flu event in Dec 2014	

What was the impact of the Disruption/disaster on business?	Financial Impact we had to dispose of the infected birds in their thousands.	

Table 3: Interview c

Company D

Company D is one of Nigeria's most prominent outdoor retail stores, with more than one hundred branches in Nigeria as well as in Ghana and Cameroon. The company has about 1500 permanent staff nationally, and 700 of them working at the Head Office alone. All branches have the latest computer technology for internal communications between staff, management and reaching out to customers. This means the company must be steps ahead when it comes to BCP because any disaster or disruption event could have a significant impact on the company.

Questions	Company D	Analysis of answers
Does the Organisation have a written business continuity plan?	Yes	
Where is the company's BCP kept and who can access this document?	It is kept on share point, so every employee can view it and be on the same page.	Employers and employees need to be familiar with the content of the plan and their role in the response and recovery.
Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, lack additional personnel. We have excluded events such as floods, tornadoes and so on. Non-critical business applications due to budget constraints. Power failures as the company are on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. Not sufficient business and technical staff involve in the plan	
Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP	
Do business continuity and disaster recovery readiness have the support of top management in your organization? Moreover, if not why?	Yes, there is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP	Get senior management involved and keep them committed.
What happens if key personnel are not available during a disaster	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not available	For a plan to succeed, there must be multiple agency cooperation moreover, involvement.
How frequently is the BCP reviewed and updated?	We do our testing every six months, and generally, this	Keep the plan current – Update the plan as

	is when we update our plan, as we test our application changes in the test as well.	applications get updated
Are back-ups done faithfully and does it include every server and hard disk?	No, budget constraints due to the size of data that will be saved to disk. Disks are expensive. Test servers.	
How often do you perform a BCP test?	Every six months. No, not all the time, but then again that it the purpose of a BCP test to identify our short-comings.	Test the business recovery process and evaluate test results
Does the company BCP high-light what are acceptable downtimes after specific disas-ters	It was agreed by auditing committee that there is a recovery window for BC purpose	Identify your recovery point objective (RPO) and re-covery time objec-tive(RTO), making sure your data protection solutions can meet these requirements.
Has the company experienced significant disruption/disaster?	Yes	
What was the impact of the Disruption/disaster on busi-ness?	Stocks could not be updated; our stores had to trade manually accepting only cash transaction. Fi-nancial aspect, we lost money	

Table 4:Interview D

Interview Analysis

All companies interviewed ascribes their longevity and resilience to having a BCP, and com-mon attributes between all companies are regular testing of the plan, BCP accessible to all management and staff and most important still standing after major disasters.
The interview came in handy by acting as a checklist and providing a certain proof that com-panies are going to face disruption at a certain time and only companies prepared for such might get back on their feet.

Workshop Findings

The discussion during the workshop led to the identification of some significant risk and critical findings. As mentioned in 3.1 above, the risk assessment workshop was organised, and this enabled the company management and some member of staff to both contribute and learn in their natural environment. The workshop lasted about 3-4 hours for two days and two senior managers, and two employees were present at startup sauna at alto university. The key benefit from the workshop includes a prioritised list of risks, assigned action plans for each risk, dis-cussion of risks by management and some member of staff, awareness of different viewpoints.

Area	Risk	Control/Actions
STRATEGIC		
Economic	Economic pressure reduces money available to be spent on service	Risk will be accepted. Too high mitigation costs
	Pricing does not match value perceived by customers	Risk will be avoided. Ensuring tours are planned to the satisfaction of customers
	Business stability loss	Risk will be avoided. By employing suitable management accountants to sort out financial aspect of the business.
Competitive	Competitor enters market	Risk will be mitigated. Company uses unique planning and strategies that are implemented into its operations also ensure customer loyalty by maintaining service quality
	Market size shrinks	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time
	Substitute service becomes available	
Employee	Departure of a key employee	Risk will be avoided Don't take anyone for granted. Invest in listening to and improving things for everyone on the team.
	Lack of training	Risk will be avoided. On job training will be done
FINANCIAL		
Credit	Increased bank charges,interest rates, credit card fees	Risk will be mitigated. Careful agreements will be made with the creditors, which are checked and signed in the presence of the legal team. Also, all the margins and interest rates are not tied to the same origin such as six months Euribor. Which does not let one origin effect significantly the credit. Financial department is responsible.
	Slow response of bank (e.g. loan proceeds)	Risk will be accepted. Too high mitigation costs
	Unable to pay loans, run business and go bankrupt	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time.
Inflation	Increased utility rates	Risk will be accepted. Too high mitigation costs
	costs increase	Risk will be accepted. Too high mitigation costs
profitability	Low or no profit	The risk will be mitigated. The profitability risk's impact will be aimed to keep low by planning and cooperation. Avoiding

		risk massive financial plans in the future will be avoided.
OPERATIONAL	Cyber attack	The risk is mitigated by assuring there is up to date cyber security technology in place.
	Poor customer service	Risk will be avoided. Training staff to provide service in accordance with the business objective.
	Poor/unattractive tour packaging	Risk will be avoided. Training staff to plan tours in accordance with the business objective.
	Unfavourable terms from suppliers (e.g. hotels and airlines)	The risk is accepted. Too costly to mitigate and control.
	Dependency on branches abroad	The risk is accepted. Because of the operations of company and the location of the tours, it is impossible to do anything about the risk.
	Technical malfunction	The risk is avoided. All the technical appliances will be maintained regularly and adequately. Backups of the most crucial technical appliances are available.
HAZARD		
Natural hazard	Bad weather n receiving country	Risk will be avoided. Proper planning on time and season of tours will be done
	Natural disasters in receiving country	Risk will be transferred. Insurance company will step in case of injuries or death
technological hazard	Plane crash on the way to Africa or back	Risk will be transferred. Insurance company will step in case of injuries or death
	Car accident during trip	Risk will be transferred. Insurance company will step in case of injuries or death
civil or political hazards.	Violence and threatening behaviour toward tourist in receiving country (e.g. verbal abuse, robbery)	Risk will be mitigated. Cooperation with legal authorities in receiving country will be implemented. This is included in the BCP and emergency plan documents.
	Political unrest in receiving country	Risk will be mitigated. Cooperation with legal authorities in receiving country will be implemented. This is included in the BCP and emergency plan documents.

Table 5: Workshop Analysis

BIA, RCA and Risk analysis, BIA, and RCA

Root Cause Analysis

RCA is a principle-based, systems approach for the identification of underlying causes associated with a set of risks ("Managing Information," 2011) The RCA was done using the five whys technique to give a deep understanding of the problem. The Proper establishment of the cause or causes and contributing factors lead to sufficient corrective actions. Effective corrective actions lead to reduced repeat findings and incidents. Reduced repeat findings and incidents lead to increased safety and reduced costs.

Cause analysis

Problem	Why 1	Why 2	Why3	Why4	Cause/why 5
Economic pressure	Business brings in Less money	Consumer spends less	Increased unemployment	People lose their jobs	Recession
Pricing does not match value perceived by customers	Perceived benefit is low	Perceived price is high	Negative Customer value	Value not defined properly	Bad marketing
Business stability loss	unable to pay for cost incurred	Insolvency	Excessive borrowing to fuel business growth	poor long-term cash management	Lack of proper long-term cash flow planning
Competitor enters market	Nature of business	Economies of scale	Small economies of scale	Capital requirement	Access to capital
Market size shrinks	Disengaged customer	Customers buy elsewhere	Competitor enters market	Nature of business	Economies of scale
Departure of a key employee	Got a new job	Applied for a new job	Employee was demotivated	No job satisfaction	Lack of management care for employees
Lack of training	Employees expected just to know	Company do not train employee	Company cannot afford it	It is expensive For company	Its takes time and money
Increased bank charges	Hidden bank fees	Bank pays for costly restriction	Interest rates are low	Regulatory burden	FG regulations impact bank fees
Slow response of bank	Long queue	Not enough staff to process loan applications	Fewer bank staff this days	Most transactions are done online	Technological advancement
Unable to pay loans	Insolvency	More money spent than gained	Increase in cost	inflation	Economic recession
costs increase	Inflation	Money surplus in economy	More demand in material	Exchange rate advantage	Service is abroad

Cyber attack	System corrupted	Opened malicious file	Received filed via email	No good detection software	Good software is expensive
Poor customer service	Lack of training	Company do not train employee	Company cannot afford it	It is expensive For company	It takes time and money
Poor/unattractive tour packaging	Bad combination of activities	Lack of proper tour planning	Lack of creative employee in tour committee	Cannot afford to employ best tourism expert	It is expensive to employ tourism expert
Unfavourable terms from suppliers (e.g. hotels and airlines)	Price Movements through Business Cycles	Different Market Conditions	No competition	The manufacturers operate under monopolistic conditions in the service market	Nature of supplies business
Dependency on branches abroad	Nature of service provided	Involves home and receiving country	Tours are abroad	Involves two separate branches	Nature of company formation
Bad weather in receiving country	Bad African weather	Increased rain and sun	Rising temperatures	Increased moisture in the atmosphere	Human-induced global warming
Natural disasters in receiving country	Africa nature	Climate change	Rising temperatures	Increased moisture in the atmosphere	Human-induced global warming
Plane crash on the way to Africa or back	Engine failure	Over use of plane	No maintenance	bureaucracy	Organizational culture
Car accident during trip	Engine failure	No maintenance	Driver waiting for repair approval	bureaucracy	Organizational culture
Political unrest in receiving country	Poverty and economic inequalities	Group inequality	Group motivation	Private incentive	Failure of the social contract

Table 6: Root Cause Analysis

Business Impact Analysis

The Business Impact Analysis (BIA)was done using the risk identified during the workshop and recovery time objective was decided alongside the management. The business impact analysis was done after the cause analysis (RCA)to understand the foundation of the problem. The BIA can be found in table 10 as a combined analysis with the risk assessment table and separately in the appendix 5.

What is a Risk Assessment?

A risk assessment is a process of identifying and quantifying the probability of a harmful effect on an item or an individual. An objective evaluation of the risks is considered and ranked by

using a basic formula of rating the potential loss and the probability of occurrence to assess risks.

HOW THE RISK ASSESSMENT WAS DONE

FIND Risk

List of all hazards and possible situations associated with the event activity that may expose people to injury, illness or disease or the company in danger or business disruptions was made. The list was done with the help of management and employees of client company during the workshop. (City of Greater Geelong)

ASSESS Risk

This step invoves taking a closer look at the risk identified by rating them and understanding the consequeses and likelihood. (City of Greater Geelong)

FIX IT

Identifying what practical measures could be put in place to eliminate or reduce the likelihood of the danger occurring was another critical step in the risk assessment phase. This was where changes were made to the event to reduce the risks. (City of Greater Geelong)

LIKELIHOOD	**RISK RANKING MATRIX**				
HIGH	**5**	**10**	**15**	**20**	**25**
SIGNIFI-CANT	**4**	**8**	**12**	**16**	**20**
MODERATE	**3**	**6**	**6**	**12**	**15**
LOW	**2**	**4**	**6**	**8**	**10**
NEGLIGIBLE	**1**	**2**	**3**	**4**	**5**
CONSE-QUENCE	**NEGLIGI-BLE**	**LOW**	**MODERATE**	**MAJOR**	**CATASTROPHIC**

Table 7: **RISK RANKING MATRIX** (City of Greater Geelong)

LIKELIHOOD DEFINITIONS	
High	It is predicted to occur in most circumstances There is a high likelihood of the event reoccurring
Significant	Comparable disruption has been recorded on a frequently Considered that it is likely that the event could occur
M**oderate**	disruptions have occurred irregularly in the past
L**ow**	only a few known incidents of occurrence Has not happened yet, but it could occur sometime
N**egligible**	No acknowledged or known incidents of occurrence little chance may only occur in an exceptional circumstance

Table 8: **LIKELIHOOD DEFINITIONS**(City of Greater Geelong)

CONSEQUENCE DEFINITIONS	
Catastrophic	Multiple or single death Company goes out of business
Major	Loss in bulk of customer Disruptions in critical business process for days
Moderate	Paid sick leave due to injuries few hours out of services
Low	injuries and Claims repayment
Negligible	slows down business process for few minutes

Table 9: **CONSEQUENCE DEFINITIONS** (City of Greater Geelong)

Risk control is an integral part of risk management. It involves determining what to do with uncontrolled risks. There are four basic strategies for controlling risks: avoidance, transference, mitigation, and acceptance. (City of Greater Geelong)

Risk Control	
Avoidance	This control method involves preventing the exploitation of vulnerability. This can be achived by applying technical security controls and safeguards that eliminate or reduce the uncontrolled risk
Transference	This Control method involves shifting the risk to other areas and most especialy to outside entities.
Mitigation	This control method involves taking an active approach to lessen the severity or impact should an incident successfully exploit a vulnerability.
Acceptance	This control method involves acknowledging the risk understanding the consequences without any attempts at control or mitigation

Table 10: **Risk Control** (City of Greater Geelong)

Area	Risk	Risk rank	RTO	Business Impact	Control/Actions	Responsibility
STRATEGIC						
Economic	Economic pressure	12	2 weeks	Loss of business stability	Risk will be accepted. Too high mitigation costs	Accounting and Finance department
	Pricing does not match value perceived by customers	6	3days	Reduced sales	Risk will be avoided. Ensuring tours are planned to the satisfaction of customers	Tour planning committee
	Business stability loss		1week	Potential struggle for survival	Risk will be avoided. By employing suitable management accountants to sort out financial aspect of the business.	Accounting and Finance department
Competitive	Competitor enters market	12	1 week	Fewer customer	Risk will be mitigated. Company uses unique planning and strategies that are implemented in its operations also ensure customer loyalty by maintaining service quality	Manager
	Market size shrinks	12	3days	Reduced profit	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time	Accounting and Finance department
	Substitute service becomes available	12	5days	Fewer customers	Risk will be accepted. Strategies to gain customer loyalty will be will be enforced	Manager
Employee	Departure of a key employee	12	3days	Reduced workforce and additional recruitment cost	Risk will be avoided Don't take anyone for granted. Invest in listening to and improving things for everyone on the team.	Manager
	Lack of training	10	5days	Slow or total stop in poor service	Risk will be avoided. On job training will be done	Manager
FINANCIAL						
Credit	Increased bank charges, interest rates,	12	1week	Cost Increases	Risk will be mitigated. Careful agreements will be made with the creditors, which are checked and	Accountant

	credit card fees				signed in the presence of the legal team. Also, all the margins and interest rates are not tied to the same origin such as six months Euribor Which does not let one origin effect considerably the credit. Financial department is responsible.	
	Slow response of bank (e.g. loan proceeds)	6	2weeks	Slows down processes	Risk will be accepted. Too high mitigation costs	Accounting and Finance department
	Unable to pay loans, run business and go bankrupt	20	1week	Loss of business stability	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time.	Accounting and Finance department
Inflation	Increased utility rates	6	1week	Reduced profit	Risk will be accepted. Too high mitigation costs	Accounting and Finance department
	costs increase	6	1 week	Reduced profit	Risk will be accepted. Too high mitigation costs	Accounting and Finance department
profitability	Low or no profit		1week	Reduced profit	The risk will be mitigated. The profitability risk's impact will be aimed to keep low by planning and cooperation. Avoiding risk massive financial plans in the future will be avoided.	Accounting and Finance department
OPERATIONAL	Cyber attack	20	4hours	Reputation and loss of information	The risk is mitigated by assuring there is up to date cybersecurity technology in place.	I.T department
	Poor customer service	12	1day	Loss of good reputation and customers	Risk will be avoided. Training staff to provide service by a business objective.	All employee

	Poor/un-attractive tour packaging	8	2hours	Reduced sale and profit	Risk will be avoided. Training staff to plan tours by the business objective.	Tour planning committee
	Unfavourable terms from suppliers (e.g. hotels and airlines)	8	1day	Bureaucracy and increased cost	The risk is accepted. Too costly to mitigate and control.	Tour planning committee
	Dependency on branches abroad	1	1day	Bureaucracy	The risk is accepted. Because of the operations of the company and the location of the tours, it is impossible to do anything about the risk.	Management
	Technical malfunction	20	3days	Overlapping schedule	The risk is avoided. All the mechanical appliances will be maintained regularly and adequately. Back-ups of the most critical technical appliances are available.	I.T department
HAZARD						
Natural hazard	Bad weather n receiving country	8	1day	Overlapping schedules	Risk will be avoided. Proper planning on time and season of tours will be done	Tour planning Committee
	Natural disasters in receiving country	16	1day	Severe injury or Death of staff, customer and reduced workforce	Risk will be transferred. Insurance company will step in case of injuries or death	Tour planning committee
technological hazard	Plane crash on the way to Africa or back	10	1week	Severe injury or Death of staff, customer and reduced workforce	Risk will be transferred. Insurance company will step in case of injuries or death	Tour planning committee
	Car accident during trip	10	1day	Severe injury or Death of staff, customer and reduced workforce	Risk will be transferred. Insurance company will step in case of injuries or death	Tour planning committee
public or political hazards.	Violence and threatening behaviour	12	1day	Lawsuit and reputation loss	Risk will be mitigated. Cooperation with legal authorities in receiving country will be	Tour planning commitee

	toward tourist in receiving country (e.g. verbal abuse, robbery)				implemented. This is included in the BCP and emergency plan documents.	
	Political unrest in receiving country	12	1day	Severe injury or Death of staff,customer and reduced manpower	Risk will be mitigated. Cooperation with legal authorities in receving country will be implemented. This is included in the BCP and emergency plan documents.	Tour planning commitee

Table 11: Risk assessment

5 Result

The BCP process commenced by gaining all-around support from the organisation's management to avoid unnecessary resistance towards the BCP project and get as much information needed. The risk identification and risk analysis were the first part of the actual work as mentioned in chapter 4 above. The risk assessment workshop was organised mainly for the risk identification, and suggestion of mitigation strategy was then developed to reduce the probability that a hazard will have a significant impact, but before then an RCA was performed. Root Cause Analysis is an often-used technique that helps answer the question of why the problem occurred in the first place, as it aims to identify the origin of a problem. Still, in the risk assessment phase, the Business Impact Analysis (BIA) was done using the current risk identified. This method was used because the existing risk approach gives a better impression of which incidents can happen, therefore, allowing room to focus on consequences of those events further.

The Determination and selection of response strategy were based on results from the risk assessment built upon the Maximum Acceptable Outage (MAO) identified for each critical process, which was recognized with the help of the manager. In this step response strategy, recovery time objective (RTO), recovery point objective(RPO) were determined. After which Resource and interdependency requirement alongside communication strategy was developed. Brief orientation was given to the top executive officer after completion of the BCP, who will then pass what was learnt to a member of staff to avoid the plan ending up a folder on the bookshelf. It is also crucial that the plan be regularly tested to discover weaknesses, keep employees updated and improve the plan. Table top scenario exercise will be used to test the plan.

5.1 Conclusion and Recommendations

The reliability of this development project and study is such that the project can be repeated, and similar result is expected as numerous people will have a similar interpretation by using the methods and procedures used. Using more than one methods of data collection in the study and development project, consistency of findings generated by the different data collection methods, and the research measuring to what it was intended to measure, is a prove of the validity of this research. It should be noted that each company is different, disruptions, threats and business model are company unique but following the same methods should give tailored results.

This research aimed to create a BCP for the case company and to determine how a model process can be used in developing the business continuity plan, the steps in preparing a BCP and kinds of risks companies face these days. The extensive literature covered in chapter 3 highlights the different types of disruption events, critical elements of an efficient BCP and the factors that cause BCP failure.

Due to system integrations, most companies have come to understand that their business now relies more on IT than ever before and that greater focus should be placed on BCP to ensure that businesses do not experience prolonged downtime during a disruption. Companies should strengthen their BCP and close any defects that might exist.

As part of BCP process should be updated accordingly. Also, an unbiased assessment of the revised BCP and test software should be performed to make sure that both are comprehensive and updated primarily based on the organisation's risk profile and test results.

References

Business continuity: awareness and training programs
Kingstoncitygroup.co.uk. (2017). Gregory Morwood Business continuity: awareness and training programmes Information Management & Computer Security 6/1 [1998] 28–32 [Accessed 10 0ct. 2017] http://www.kingstoncitygroup.co.uk/includes/docs/library/businesscont/Business%20Continuity%20-%20article%20-%20awareness%20and%20training.pdf

Continuitycentral.com. (2017). Business continuity statistics: where myth meets fact. [Accessed 10 0ct. 2017]. http://www.continuitycentral.com/feature0660.html

Business Impact Analysis (BIA)
Itsm.ucsf.edu. Business Impact Analysis (BIA) | IT Service Management Office. [Accessed 10 0ct. 2017].http://itsm.ucsf.edu/business-impact-analysis-bia-0

Clark, Graham (AMBCI), 'Making BCM a part of your culture' Q2, 2012. [Accessed 28 Nov. 2017]

Consumer Safety Act (Finnish Statute Book (920/2011)
Tukes.fi. (2017). [Accessed 10 0ct. 2017]http://www.tukes.fi/Tiedostot/Kuluttajaturvallisuus/Kuluttajaturvallisuuslaki_EN.pdf

Doughty, K. (2000) Best Practices, Volume 15: Business Continuity Planning: Protecting Your Organization's Life. Boca Raton, FL, USA: Auerbach Publishers, Incorporated, p 6, 8. [Accessed 28 Nov. 2017]http://site.ebrary.com.bibl.proxy.hj.se/lib/jonhh/Doc?id=10074957&ppg=29

Eisenhardt, K. M. 1989. “Building Theories from Case Study Research”, Academy of Management Review, Vol. 14, No. 4, pp. 532-550.EY. EUROAC. [Accessed 28 Nov. 2017] http://euroac.ffri.hr/wp-content/uploads/2010/06/Eisenhardt_1989_Building-Theories-from-Case.pdf.

Felipe Alonso, Risk and Advisory Services, KPMG, ‘Managing Business Continuity Part 1’ http://my.advisor.com... [Accessed 28 Nov. 2017]

Fernandes L.J and Saldanha da Gama, F. (2008). Contingency Planning: A literature review. [Accessed 28 Nov. 2017]Retrieved from https://www.researchgate.net/publication/230807504_Contingency_planning_-_a_literature_review

Hotchkiss, S. (2010). Business Continuity Management: In Practice. Swindon: British Informatics Society Limited. Home Page | BCS - Bookshop. [Accessed 28 Nov. 2017] http://shop.bcs.org/resources/pdf/9781906124724.pdf

King, Mark. "Business Continuity Plans: A Position for Recovery." The Guardian. Last modified February 23, 2011. [Accessed 10 0ct. 2017] https://www.theguardian.com/money/blog/2011/feb/23/business-continuity-plans-smes.

Ian Storkey , Operational Risk Management (ORM) and Business Continuity Plans (BCP), Economic Policy and Debt Department, World Bank Treasury. [Accessed 28 Nov. 2017] http://treasury.worldbank.org/bdm/pdf/operational-risk-management-and-business-continuity-planning-for-modern-state-treasurie.pdf.

Igor Linkov & Jose Palma, O. (2017). "Resilience and Risk- Addressing the Current State of Resilience Studies." RESLIENS Project. [Accessed 10 0ct. 2017]http://resilens.eu/resilience-and-risk-addressing-the-current-state-of-resilience-studies/.

"ISO 31000 Risk Management." ISO - International Organization for Standardization. [Accessed 28 Nov. 2017]. https://www.iso.org/iso-31000-risk-management.html.

"ISO 22301 Business Continuity Management." Share and Discover Knowledge on LinkedIn SlideShare. Last modified February 7, 2014. [Accessed 28 Nov. 2017] https://www.slideshare.net/RamiroCid/iso-22301-business-continuity-management.

ISO 22301:2012 - Societal security - Business continuity [Accessed 28 Nov. 2017] https://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

ISO 22301:2012 - Societal security - Business continuity [Accessed 28 Nov. 2017] https://www.iso.org/standard/50038.html

IT Continuity Framework | GTA – Enterprise Policies ... [Accessed 28 Nov. 2017] https://gta.georgia.gov/psg/book-page/it-continuity-framework

"RIM Fundamentals: How to Avoid Disaster: RIM's Crucial Role in Business Continuity Planning." ARMA International. [Accessed 28 Nov. 2017]. http://content.arma.org/IMM/November-December2011/rimfundamentalshowtoavoiddisaster.aspx

Valackiene, Asta. 2015. "Significance of Business Continuity in Change Management: Theoretical and Practical Perspective."
Gregory Morwood, (1998) "Business continuity: awareness and training programmes", Information Management & Computer Security, Vol. 6 Issue: 1, pp.28-32, [Accessed 28 Nov. 2017] https://doi.org/10.1108/09685229810207425

Steele, Chris. "Post-9/11 Location Strategies: Rethinking Business Continuity Planning." Site Selection Online Insider. Site Selection Magazine, 21 Oct. 2002. [Accessed 28 Nov. 2017]http://www.siteselection.com/ssinsider/snapshot/sf021021.htm>

Swanson, M., Lynes, D., & Gallup, D. (2010). Contingency Planning Guide for Federal Information Systems. Nist Special Publication 800 –34 Rev 1. NIST Page. Accessed February 6, 2018. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf [Accessed 28 Nov. 2017]

Templeton, Tom, and Tom Lumley. "Statistics from 9/11 and the Aftermath." The Observer - US News. The Guardian, 17 Aug. 2002. [Accessed 10 0ct. 2017]http://www.theguardian.com/world/2002/aug/18/usa.terrorism>
Swartz, N. (2003). Few Organizations Have Effective Continuity Plans. Information Management Journal, 37(3), 7. Templeton, Tom. "Statistics from 9/11 and the Aftermath." The Guardian. Last modified July 14, 2017. [Accessed 10 0ct. 2017] https://www.theguardian.com/world/2002/aug/18/usa.terrorism

Wallace, M. & Webber, L. (2011). The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets (2nd ed.). New York: American Management Association. [Accessed 28 Nov. 2017] http://privat.bahnhof.se/wb578186/pdf/the-disaster-recovery-handbook_a-step-by-step-plan-to-ensure-business.pdf

What is Business Continuity? [Accessed 28 Nov. 2017] http://www.thebci.org/index.php/resources/what-is-business-continuity

What is business impact analysis (BIA)? [Accessed 28 Nov. 2017] http://searchstorage.techtarget.com/definition/business-impact-analysis

Business Continuity: Awareness And Training Programmes, [Accessed 28 Nov. 2017] http://www.kingstoncitygroup.co.uk/includes/docs/library/businesscont/Business%2

Business Continuity Planning - Ffiec It Examination. [Accessed 28 Nov. 2017], https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program/updating

theoretical framework. BusinessDictionary.com. WebFinance, Inc. http://www.businessdictionary.com/definition/theoretical-framework.html
(Accessed: December 26, 2017).

Resilience integration (media.nature.com) https://media.nature.com/m685/nature-assets/nclimate/journal/v4/n6/images/nclimate2227-f1.jpg

Business Continuity Terms - Unit 1 Flashcards | Quizlet, [Accessed 28 Nov. 2017]https://quizlet.com/33974485/business-continuity-terms-unit-1-flash-cards/

Business Continuity and Disaster Recovery Plan Template, [Accessed 28 Nov. 2017]
https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/media/it

Disaster Recovery and Business Continuity | Pef Services, [Accessed 28 Nov. 2017]
https://www.pefservices.com/disaster-recovery-business-continuity/

Best Practices for Creating an Effective Business., [Accessed 28 Nov. 2017]
https://esj.com/articles/2012/11/05/business-continuity-plan.aspx

Snapshot from The Field - Site Selection, [Accessed 24 Oct. 2017]
http://siteselection.com/ssinsider/snapshot/sf021021.htm

Gibb, F. and Buchanan, S. (2006). A Framework for Business Continuity Management. International Journal of Information Management, Vol. 26, Issue 2, pp. 128-141

Resilience and Risk- Addressing the Current State Of., [Accessed 28 Nov. 2017]
http://resilens.eu/resilience-and-risk-addressing-the-current-state-of-resilienc

Business Continuity Plans: A Position for Recovery | Money., [Accessed 28 Nov. 2017]
https://www.theguardian.com/money/blog/2011/feb/23/business-continuity-plans-sme
Business Continuity Management Is A Luxury in Times Of.,
https://studentshare.net/environmental-studies/20899-business-contiunity-managem

Toward Effective Business Continuity Management: A Check., [Accessed 26Oct. 2017]
https://www.boj.or.jp/en/research/brp/ron_2008/data/ron0807a.pdf

Martyn Shuttleworth (Sep 16, 2009). What is a Literature Review? Retrieved Feb 13, 2018 from Explorable.com: https://explorable.com/what-is-a-literature-review

How to Do A Risk Assessment – Refer to Template, [Accessed 20 Oct. 2017]
https://www.australiaday.org.au/storage/13966_AusDay-EventOrganisers-RiskAssessm

Business Continuity Management | Continuity Management For., [Accessed 03 Oct. 2017]http://www.zonecast.com/continuity/bcp.asp

"Post-9/11 Location Strategies: Rethinking Business Continuity Planning, Site Selection Online Insider." Site Selection - The Magazine of Corporate Expansion & Area Economic Development. [Accessed 03 Oct. 2017]. http://siteselection.com/ssinsider/snapshot/sf021021.htm.

Iso-international Organization for Standardization, [Accessed 28 Nov. 2017]
https://global.ihs.com/standards.cfm?publisher=ISO&rid=Z56&mid=ISO

Glossary Of General Business Continuity Management Terms, [Accessed 28 Nov. 2017]http://c.ymcdn.com/sites/www.continuity.net.au/resource/resmgr/imported/BCI_Glos
: Iso 22301 Business Continuity - Plain English Introduction, [Accessed 28 Nov. 2017]

http://praxiom.com/iso-22301-intro.htm
Technocratgroup.com. (2017). ISO 31000:2009 | Risk Management System | Technocrat Consultants | ISO Consultant in United States of America (USA) | Management Consultant in South Africa | Integrated Management System Consultant in Singapore | Information Security ISO 27001:2005 Consultant in United States of America (USA) | ISO Consultant in Gujarat | Integrated Management System Consultant in Mauratitus | ISO 45001. [Accessed 28 Nov. 2017]. [online] Available at: http://www.technocratgroup.com/risk_management_system_ISO_31000.html

Consumer Safety Act - Tukes.fi, [Accessed 28 Nov. 2017].

http://www.risklogic.com.au/site/wp-content/uploads/2009/06/Business-Continuity-Good-Practice-Guidelines-2008.pdf

http://www.tukes.fi/Tiedostot/Kuluttajaturvallisuus/Kuluttajaturvallisuuslaki_EN

: Operational Risk Management (orm) And Business Continuity., [Accessed 28 Nov. 2017]. http://siteresources.worldbank.org/INTDEBTDEPT/Resources/468980-1238442914363/59

Business Continuity Planning - FFIEC It Examination., [Accessed 28 Nov. 2017]. https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program/updating

Why Is Business Continuity Important? | Travelers Insurance, [Accessed 28 Nov. 2017]. https://www.travelers.com/resources/business-continuity/why-is-business-continui

39 Examples of Small Business Risks – Thomas M. Bragg., [Accessed 28 Nov. 2017]. http://www.thomasmbragg.com/2010/01/15/39-examples-of-small-business-risks/

research methodology. BusinessDictionary.com. WebFinance, Inc. [Accessed 28 Nov. 2017]. http://www.businessdictionary.com/definition/research-methodology.html

Qualitative vs quantitative. BusinessDictionary.com. WebFinance, Inc. [Accessed 10 0ct. 2017] http://www.businessdictionary.com/article/968/qualitative-vs-quantitative-d1113/

Qualitative methods: what are they and why use them?
Robert P. Luciano Professor of Health Care Policy, School of Public Affairs, Baruch College, New York, New York 10010, USA. 1999 Dec;34(5 Pt 2):1101-18. [Accessed 28 Nov. 2017]. https://www.ncbi.nlm.nih.gov/pubmed/10591275

BUSINESS CONTINUITY MANAGEMENT FRAMEWORK Griffith University, August 2013 http://policies.griffith.edu.au/pdf/Business%20Continuity%20Management%20Framework.pdf

"BUSINESS CONTINUITY MANAGEMENT FRAMEWORK." 1pdf.net. Last modified January 1, 1970. [Accessed Dec 6. 2017]. https://1pdf.net/business-continuity-management-framework_58537725e12e89c8061cba8d.

Risk assessment template City of Greater Geelong. [Accessed Dec 6. 2017]. http://www.geelongaustralia.com.au/common/Public/Documents/8cbc48484619721-Event%20Risk%20assessment-%20%20Risk%20Assessment%20Example%20and%20Template%20.doc

"Business Continuty.pdf - [PDF Document]." Vdocuments.site. [Accessed Dec 6. 2017]. https://vdocuments.site/business-continutypdf.html.

Etusivu - Tukes. [Accessed Dec 6. 2017]. http://www.tukes.fi/Tiedostot/Kuluttajaturvallisuus/Kuluttajaturvallisuuslaki_EN.pdf.

"Policies and Procedures Library - The University of Queensland, Australia." Policies and Procedures Library - The University of Queensland, Australia. [Accessed Dec 6. 2017]. https://ppl.app.uq.edu.au/content/enterprise-risk-management-procedures.

"BS25999 BCM Standart." PowerShow. [Accessed Dec 6. 2017]. http://www.powershow.com/view/3b6187-YzNmM/BS25999_BCM_Standart_powerpoint_ppt_presentation.

"ISO-International Organization for Standardization." IHS Markit Standards Store | Engineering & Technical Information. [Accessed Dec 6. 2017]. https://global.ihs.com/standards.cfm?publisher=ISO&rid=ASA.
"Countries in International Organization for Standardization." Academic Dictionaries and Encyclopedias. [Accessed Dec 6. 2017]. http://en.academic.ru/dic.nsf/enwiki/4720133.

http://www.overmanassoc.com/quality_iso/iso/

"International Organization for Standardization." Wikipedia, the Free Encyclopedia. [Accessed Dec 6. 2017]. https://en.wikipedia.org/wiki/International_Organization_for_Standardization.

"NETWORKING CONCEPTS. OSI MODEL Established in 1947, the International Standards Organization (ISO) is a Multinational Body Dedicated to Worldwide Agreement. - Ppt Download." Slide Player - Upload and Share Your PowerPoint Presentations. [Accessed Dec 6. 2017]. http://slideplayer.com/slide/6076460/.

"Why is the International Organization for Standardization Important for Social Networking?" E Notes. [Accessed 10 0ct. 2017]https://www.enotes.com/homework-help/can-anyone-expand-why-iso-important-social-449101.

"Free Business Continuity Policy Template." SearchDisasterRecovery [Accessed 10 0ct. 2017]. http://searchdisasterrecovery.techtarget.com/feature/Free-business-continuity-policy-template-for-SMBs.

"7 Steps Toward More Resilient Business Continuity." Continuity Centers. Last modified October 30, 2015. https://continuitycenters.com/7-steps-toward-more-resilient-business-continuity/

"Business Resilience – the Next Step Forwards for Business Continuity." Continuity Central: The International Business Continuity Management Portal. [Accessed 10 0ct. 2017]. http://www.continuitycentral.com/feature083.htm.

Managing Information Security Risk. (2011). Retrieved from http://csrc.nist.gov/publications/nistpubs/800- 39/SP800-39-final.pdf

"Business Continuity Plan | Ready.gov." Plan for Disasters | Ready.gov. [Accessed 10 0ct. 2017]. https://www.ready.gov/business/implementation/continuity

Jeffery Glen Nov 2013 Business Dictionary Quantitative vs Qualitative research methods http://www.businessdictionary.com/article/968/qualitative-vs-quantitative-d1113/ . [Accessed 10 0ct. 2017]

"How to Build Your BCP in 6 Steps." InConsult. [Accessed 10 0ct. 2017]. http://www.inconsult.com.au/how-to-build-your-bcp-in-6-steps/

Introduction to business continuity https://sopinion8ed.wordpress.com/2013/01/22/business-continuity-introduction-3/

Figures

Figure 1: Four BCP Elements (sopinion8ed.wordpress.com) 8

Figure 2: Plan-Do-Check-Act cycle (ISO 9001:2015) 10

Figure 3: Risk management process (ISO3100:2009) 11

Figure 4: The BCM Lifecycle—BS 25999-1 (The Business Continuity Institute 2007) 12

Figure 5: Recovery overview 14

Figure 6: BC Planning Process using Risk-Based Approach. ISO 31000 15

Figure 7: Resilience integration (media.nature.com) 20

Tables

Table 1:Interview A 25

Table 2: Interview B 26

Table 3: Interview c 28

Table 4:Interview D 29

Table 5: Workshop Analysis 31

Table 6: Root Cause Analysis 33

Table 7: **RISK RANKING MATRIX** (City of Greater Geelong) 34

Table 8: **LIKELIHOOD DEFINITIONS**(City of Greater Geelong) 34

Table 9: **CONSEQUENCE DEFINITIONS** (City of Greater Geelong) 35

Table 10: **Risk Control** (City of Greater Geelong) 35

Table 11: Risk assessment 39

Appendices

Appendix 1:Business Continuity Plan Summary 47

Appendix 2: Interview Questions 48

Appendix 3: Summary of Interview Questionnaire 49

Appendix 4: Workshop Summary Report 53

Appendix 5:BIA 56

Appendix 1:Business Continuity Plan Summary

This disclosure is provided for this thesis to inform how the company's business continuity plan addresses possible future business disruptions and how the company's plan deals with disruptions of varying scope. The outcome of this thesis was a detailed written business continuity plan. The availability of different elements may affect the execution of the plan. The company's plan provides for redundancy in the backup of records that are important in the operation of the company as well as alternative means of communicating with critical business constituents.

The plan is designed to enable the business continues functioning in the event of a limited disruption, which may make access to some resources difficult, but would allow the company to operate from its central offices here in Finland and abroad. When there is a significant business disruption which renders the office inaccessible or hotels during tours, the plan provides that the business operation or during the trip will continue critical business operations and tourism activities but at an alternative site reserved for the companies use both here in Finland and abroad during trips. This section provides computer, communications, data, and internet connectivity, and in the case of disruptions and planned hotels cannot be used there is an alternate hotel that tourist would be lodged into.

The plan provides for various means by which critical employees may communicate with each other to coordinate the company response to an event. Customers and clients will be able to talk with the company through regular phone contact, which will be rerouted to the alternative business site. In addition to, telephone contact with clients, the company will also post essential announcements regarding its business status on the company's website and people desiring to communicate with their respective family member abroad during the tour will be able to do through means provided by those custodians.

The plan also provides a step by step process of plan activation, the person(s) responsible for activating the BCP, contact details of third-party interdependencies both here in Finland and abroad during tours. Recovery-time objectives were provided to establish goals for business resumption. However different external factors surrounding a disruption, such as time of day and scope of disruption, can affect the actual recovery time.

The BCP is made to prepare the company and its employees for critical business incidents and to ensure operations go back to normal as quickly as possible. The information contained above is only a summary and not intended to provide complete details of the BCP. The BCP, cannot be delivered to external parties because of its confidential nature.

Appendix 2: Interview Questions

Research Interview for bachelor's Degree in Security Management
Interview conducted by Akinbola Deborah Ibukunoluwa
By participating in this interview, you declare that all information provided is true and accurate and can be used for this research.
May I proceed with this interview and do you agree to the above declaration Yes
Name of Company: _____
Name of respondent: _____
Contact Details: _____
Email: _____
Department: _____

1. Does the business have a written business continuity plan?
2. Where is the company's BCP kept and who can access this document?
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?
4. Does the DRP form part of the BCP or is it a separate plan altogether?
5. Does business continuity and disaster recovery readiness have the support of top management in your organization? Moreover, if not why?
6. What happens if key personnel are not available during a disaster?
7. How often is the BCP reviewed and updated?
8. How are business critical applications identified?
9. Who is responsible for identifying these applications?
10. Are back-ups faithfully and does it include every server and hard disk?
11. How frequently do you perform a BCP test?
12. Does the company BCP highlight what acceptable downtimes are after specific disasters?
13. Has the company experienced significant disruption/disaster?
14. What was the impact of the disruption/disaster on business?

Appendix 3: Summary of Interview Questionnaire
In the tables below the companies will be abbreviated as follow:

Company A (A)

Company B (B)

Company C (C)

Company D (D)

Questions	Company A	Company B	Company C	Company D
Does the business have a written business continuity plan?	Yes	Yes	Yes	Yes
Where is the company's BCP kept and who can access this document?	It is kept on share point so that every employee can view it	Kept on SharePoint for the whole company to see	It is kept on SharePoint, and all office staff can assess it	It is kept on share point, so every employee can view it and be on the same page.
Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, Location for staff to operate from but we all know it will be from their homes.	No	Yes, not enough farm staff in the plan only office staff	Yes, lack additional personnel. We have excluded events such as floods, tornadoes and so on. Non-critical business applications due to budget constraints. Power failures as the company are on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. Not sufficient business and technical staff involvement in the plan
Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP	Yes, it is part	Yes	The DRP is part of the BCP

Do business continuity and disaster recovery readiness have the support of top management in your organization? Moreover, if not why?	Yes	Of course,	Yes	Yes, there is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP
What happens if key personnel are not available during a disaster?	3rd party is readily available	3rd party supplies are on standby	There is an agreement with third party suppliers for support in the event of a disaster.	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not available
How frequently is the BCP reviewed and updated?	Our testing is done bi-annually	Every six months	Annually at least after our 2014 bird flu disastrous event that killed almost all our chickens and turkey	We do our testing every six months, and generally, this is when we update our plan, as we test our application changes in the test as well.
Are back-ups faithfully and does it include every server and hard disk?	Yes, daily due to the nature of our business.	All business-critical servers are backed up daily.	All important business servers are backed up daily.	No, budget constraints due to the size of data that will be saved to disk. Disks are expensive
How frequently do you perform a BCP test?	Every six months.	Every six months.	Every six months. A user test is done once a year to ensure that all applications restored are fully operational	Every six months. No, not all the time, but then again that it the purpose of a BCP test to identify our shortcomings.

Does the company BCP highlight what acceptable downtimes after are specific disasters?	Yes	Yes, up to 99%	Yes, form part of the BIA.	It was agreed by auditing committee that there is a re-covery window for BC purpose
Has the company experienced significant disruption/disaster?	Yes	Yes	Yes. Bird flu event in Dec 2014	Yes
What was the im-pact of the disruption/disaster on business?	Our reputation.	Goodwill loss	Financial Im-pact we had to dispose of the infected birds in their thousands.	Stocks could not be updated; our stores had to trade manu-ally accepting only cash trans-action. Finan-cial aspect, we lost money

Appendix 4: Workshop Summary Report

A Risk assessment workshop was organized this enabled the company management and some member of staff to both contribute and learn in their natural environment. The workshop lasted about 4 hours for a day and two senior managers, and two employees, were present at startup sauna at alto university. Beyond the personnel costs, there were also scheduling challenges. List of crucial risks did rank not only the result, but also discussion about the control environment, risk, and risk tolerances. During the workshop impact of business, disruption was discussed which enabled the making of the business impact analysis. The staff members and management walked away from the session with more understanding of the business operations, objectives, and challenges. Management and staff were equipped with the knowledge and the detailed analysis to make improved business decisions. The key benefit from the workshop includes a prioritised list of risks, assigned action plans for each risk, discussion of risks by management and some member of staff, awareness of different viewpoints.

Area	Risk	Control/Actions
STRATEGIC		
Economic	Economic pressure	Risk will be accepted. Too high mitigation costs
	Pricing does not match value perceived by customers	Risk will be avoided. Ensuring tours are planned to the satisfaction of customers
	Business stability loss	Risk will be avoided. By employing suitable management accountants to sort out financial aspect of the business.
Competitive	Competitor enters market	Risk will be mitigated. Company uses unique planning and strategies that are implemented into its operations also ensure customer loyalty by maintaining service quality
	Market size shrinks	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time
	Substitute service becomes available	
Employee	Departure of a key employee	Risk will be avoided Don't take anyone for granted. Invest in listening to and improving things for everyone on the team.
	Lack of training	Risk will be avoided. On job training will be done
FINANCIAL		
Credit	Increased bank charges ,interest rates, credit card fees	Risk will be mitigated. Careful agreements will be made with the creditors, which are checked and signed in the presence of the legal team. Also, all the margins and interest rates are not tied to the same origin such as six months Euribor. Which does not let one origin effect significantly the credit. Financial department is responsible.
	Slow response of bank (e.g. loan proceeds)	Risk will be accepted. Too high mitigation costs
	Unable to pay loans, run business and go bankrupt	Risk will be mitigated. Good Hands in the finance industry will be involved as well as forecast made from time to time.
Inflation	Increased utility rates	Risk will be accepted. Too high mitigation costs
	costs increase	Risk will be accepted. Too high mitigation costs
profitability	Low or no profit	The risk will be mitigated. The profitability risk's impact will be aimed to keep low by planning and cooperation. Avoiding risk heavy financial plans in the future will be avoided.
OPERATIONAL	Cyber attack	The risk is mitigated by assuring there is up to date cyber security technology in place.
	Poor customer service	Risk will be avoided. Training staff to provide service in accordance with business objective.
	Poor/unattractive tour packaging	Risk will be avoided. Training staff to plan tours in accordance with business objective.

	Unfavourable terms from suppliers (e.g. hotels and airlines)	The risk is accepted. Too costly to mitigate and control.
	Dependency on branches abroad	The risk is accepted. Because of the operations of company and the location of the tours, it is impossible to do anything about the risk.
	Technical malfunction	The risk is avoided. All the mechanical appliances will be maintained regularly and adequately. Backups of the most significant technical appliances are available.
HAZARD		
Natural hazard	Bad weather n receiving country	Risk will be avoided. Proper planning on time and season of tours will be done
	Natural disasters in receiving country	Risk will be transferred. Insurance company will step in case of injuries or death
technological hazard	Plane crash on the way to Africa or back	Risk will be transferred. Insurance company will step in case of injuries or death
	Car accident during trip	Risk will be transferred. Insurance company will step in case of injuries or death
public or political hazards.	Violence and threatening behaviour toward tourist in receiving country (e.g. verbal abuse, robbery)	Risk will be mitigated. Cooperation with legal authorities in receiving country will be implemented. This is included in the BCP and emergency plan documents.
	Political unrest in receiving country	Risk will be mitigated. Cooperation with legal authorities in receiving country will be implemented. This is included in the BCP and emergency plan documents.

Appendix 5:BIA

Area	Risk	RT0	Business Impact
STRATEGIC			
Economic	Economic pressure reduces money available to be spent on service	3 weeks	Loss of business stability
	Pricing does not match value perceived by customers	2 days	Reduced sale
	Business stability loss	1 week	
Competitive	Competitor enters market	1 week	Fewer customers
	Market size shrinks	3days	Reduced profit
Employee	Departure of a key employee	5days	Reduced manpower and additional recruitment cost
	Lack of training	3 days	Slow and poor service
FINANCIAL			
Credit	Increased bank charges interest rates, credit card fees	5 days	Increased cost
	Slow response of bank (e.g. loan proceeds)	1 week	Slows down process
	Unable to pay loans, run business and go bankrupt	2 weeks	Loss of business stability
Inflation	Increased utility rates	1 week	Reduced profit
	costs increase	1 week	Reduced profit
profitability	Low sales	1 week	Reduced profit
OPERATIONAL	Cyber attack	4 hours	Reputation and loss of information
	Technical failure	1 day	Slow or total stop in service
	Poor customer service	2 hours	Loss of good reputation and loss of customers
	Poor/unattractive tour packaging	1 day	Reduced sale

	Unfavourable terms from suppliers (e.g. hotels and airlines)	1 day	Bureaucracy, increased cost
	Dependency on branches abroad	3 days	bureaucracy
HAZARD			
Natural hazard	Bad weather in receiving country	1 day	Overlapping schedule
	Natural disasters in receiving country	1 day	Loss of cash and death of staff
technological hazard	Plane crash on the way to Africa or back	1 week	Reduced manpower
	Car accident during trip		Reduced manpower
civil or political hazards.	Violence and threatening behaviour toward tourist in receiving country (e.g. verbal abuse, robbery)	1 day	Lawsuit and reputation
	Political unrest in receiving country	1 day	