LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Risk Analysis and Business Continuity for a small business

Andersen, Jonas

2016 Laurea Leppäävaara

Laurea University of Applied Sciences
Leppäävaara

Risks Analysis and Business Continuity for a small business

Jonas Andersen
Degree Programme in SM
Bachelor's Thesis
April, 2016

Laurea University of Applied Sciences **Abstract**
Leppäävaaara
Security Management

Jonas Andersen

Risk Analysis and Business Continuity for a small business

Year 2016 Pages 63

This thesis is an attempt to put together a set of methods to aid a small business in managing its The basis of this thesis was the need of one company to manage its risks and plan for potential crises in a cost-efficient way.

The main problem for the company with doing this kind of process on its own was its lack of resources. The goal of the thesis then became to generate a method that would allow the company to have a solid Risk Analysis and Business Continuity program that could be maintained with the resources that the company possesses.

The development process started with the idea that the company needed both continuity and risk management processes. To make it simple and small enough it was decided to integrate Risk Analysis methods and Business Continuity methods to make a whole that could be a tool that would cover all the risk and continuity needs of the company.

When the system had been made, information was gathered from the company to complete a revelation of the process wheel of the system. The methods used for gathering information was both qualitative and quantitative. There were several interviews conducted, inspections of the premises of the company and a workshop to go through the results and validate certain assumptions made in the process.

The process of going through their business has mapped out the different vulnerabilities and risk factors that the company is facing. The next step was to find out how to handle the different vulnerabilities and risk factors in a cost-efficient way and within their capabilities. The process resulted in executable plans to mitigate risks, handle crisis and recover business processes that gives the company clear planning options for its further development.

Keywords: Risk, Risk Management, Business Continuity Management, Small Business, System Development, Analysis, Annual Loss Expectancy, Fault tree analysis,

Table of contents

1 Introduction

1.1 The company in brief

The company is a family owned small business located a village in southwestern Norway. The vision of the company is to make the lives of the people in the region more beautiful. The method for achieving this is the sale of flowers, flower arrangements and interior design articles. Due to the store itself being located along the main road in the area, a portion of the business is from passers-by and the regional reach is wider due to it being easily accessible from most areas.

The company operates a small shop where most of the business happens as regular retail. In addition to the retail sales the company also delivers flower arrangements for various occasions, with most of the volume being weddings and funerals. Due to the current size of the business, the owners do most of the work. However, once the concept of the store proved to be successful the company hired one part time worker in early 2015.

The company has been operating for one and a half years and is making a healthy profit. The company has grown roughly 50% from the opening in 2014 to 2015. This is a solid number and the liquidity of the company, as of the first quarter of 2016, is good.

The future growth of the company has limitations from the fact that the potential customer base in the local area is small and from this, there are serious challenges in achieving further growth in the current environment.

1.2 The objective of the study

The problem of the company that has become the focus of the study is the lack of a way to structure the threats and weaknesses that face the company. This makes it difficult for the owners of the company to plan future investments as they are unsure of the risks of taking different paths. In addition to this there is a need for tools to plan concrete actions to be taken to control or reduce threats. From this basis, the thesis will do two things:

1: Establish a set of methods to enable the company to have functioning risk analysis and business continuity systems that can operate cost effectively within the limits of the company's resources.

2: Do an initial revelation of the system to identify the main problems to get started on in the year of 2016.

Since it is a small company and so it has few resources to do secondary processes such as risk analysis in a structured way. This is not to say that these processes are less needed as the same challenges face a small company as a bigger one, though the scale and complexity is different.

The result of this process will be a company that is more aware of the risks it is facing and therefore is more prepared to handle threats without compromising the ability to take advantage of opportunities. Going through this process will increase their ability to create the desired development of the business.

1.3 Framework of the thesis

The thesis will be built up in four parts:

1. Theoretical background; where the Theory basis of the thesis is presented and discussed.
2. Development; In this part the development of the method that will be used in the study is shown.
3. Study; In this part the method will be given a run through. The information from the company will be collected and analysed and a set of actions will be developed to solve some of the issues that are identified.
4. Conclusions; in this part the process will be summed up and the results and recommendations that have been identified in the process will be presented.

2 Research

2.1 Research questions the study

These are the main questions that are the basis of this study. They aim to point the research toward the goal of producing results that are applicable in the future and that may generate further improvement.

- How can Risk Analysis and Business Continuity be integrated to make a cost-effective platform that can fill the needs of a small company?

2.2 Research methods

Both qualitative and quantitative research methods were used in this study for different purposes where they were deemed appropriate. There is a fundamental difference in qualitative and quantitative approaches to doing research. Quantitative methods rely on a sufficient amount of quantifiable data to be available to be turned into variables in order to be viable.

Qualitative research deals with unquantifiable information or information where there is insufficient amounts of data to make qualitative research viable (Trost 1993, 7).

Quantitative research methods are, when used correctly, the best way of getting accurate answers to a question (Saunders & Turnhill 2008, 416). It is however important to remember that quantitative research with a too small amount of data will not give the desired accuracy. Qualitative research is best applied where individual people's thoughts, actions and reasoning is an important factor in the goal of the study (Trost 1993, 13). The decision to use either qualitative or qualitative methods should ultimately be based on the type of information that can be gathered and the goal of the research.

In the terms of risk management qualitative and quantitative methods are chosen based on what the desired goal of the study is and what type of information is available. In the different processes it is necessary to gather and analyse different types of data and to put these together. A process that deals with the practical application of a system will necessarily contain both quantitative and qualitative elements.

2.2.1 Interview

The interview is a basic qualitative research method. Interviews are used to gain information from a person based on the person's opinions or experience.

Depending on the situation, the interview will have certain levels of standardisation and structuring. Standardisation is to what degree external factors such as the interviewer's tone of voice or environment is the same in different interviews, while structuring is to what degree the interviewee is free to vary their response (Trost 1993, 15). A fully structured question limits the interviewee to a set of predetermined options, also known as multiple choice. On the other end of the scale, the interviewer gives open questions where the interviewee is free to decide how to respond.

When forming an interview it is important to keep in mind what kind of questions are being asked and in what way. The method of interviewing may affect the result of the information gained in the interview (Brinkmann 2013, 85). It is essential to plan and perform an interview in such a way that it produces the correct type of information.

2.2.2 Collection of secondary data

In order to gain an overview of the larger situation and of events that occur at long intervals it is useful to use data or information that has already been collected (Saunders & Turnhill

2008, 257). There are many such sources of information available, such as information collected by government agencies.

The use of statistics based on already collected information is useful where such information is available (Rugg 2008, 47). For the purposes of calculating risk values for hazard events, the use of already collated statistics can be a useful tool.

3 Theoretical background

3.1 Risk management

Risk management is according to Dictionary.com defined as the "technique or profession of assessing, minimizing, and preventing accidental loss to a business, as through the use of insurance, safety measures, etc." Lars G.W. Johnsen (2005, 31) defines it as the method of implementing systematic safeguards for unwanted occurrences in an organization or business.

An organization that does not manage its risks properly will over time have a poorer performance and may indeed fail. The attention to detail in being proactive in response to the different kinds of risks that face the organization will make a significant impact on its ability to perform, compete and survive. When starting a risk management process it is vital to understand the goals of the subject organization.

In order to have good risk management there needs to be established a system for identifying risks, a set of methods for organizing and evaluating them and a decision making process for deciding what level of risk is acceptable (Rittinghouse & Ransome 2005, 27).

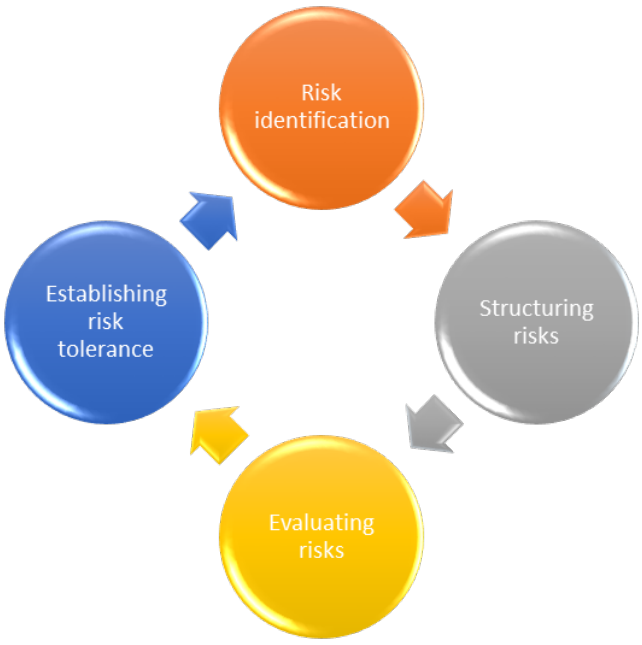


Figure 1 A visual representation of the risk management process as put forward by Rittinghouse & Ransom (2005, 27)

In Corporate risk management, Merna et. Al. (2008, 45) puts forward four main tasks in the risk management process:

- Identification of risks and uncertainties.
- Analysis of implications.
- Response to mitigate risk.
- Allocation of appropriate contingencies.

In order to succeed with a risk management strategy it will need to involve these basic processes in some form. The process of risk management is a continuous process, rather than a linear one (Merna et. Al. 2008, 45). This indicates that there needs to be a risk management system in place that is capable of being continuously updated and revised to stay relevant.

When looking to establish a risk management system there needs to be resources allocated to keep the process running after the initial establishment in order to keep it relevant (Johnsen 2005, 57). If the necessary resources are not available, the system will begin to lose its relevance and will ultimately give false readings to the decision makers and thus lead to an undesirable level of risk exposure and misallocation of resources for risk mitigation.

3.1.1 Risk

Events that have an effect on a subject and that has a probability of occurring attached to it can be called a risk. Risks can be described as either a chance to gain, or a chance to lose. The risk of a negative event occurring or a hazard risk is defined by Dictionary.com as “exposure to the chance of injury or loss; a hazard or dangerous chance.”

In order to organize the risks it is useful to use a system of classification. Paul Hopkin (2010, 29) classifies risks into three categories; hazard risks, control risks, and opportunity risks.

Hazard risks: The risks that only have a possibility for a negative outcome is called a hazard risk (Hopkins 2010, 29). Examples of hazard risks can be fire, flooding or theft. An organization will need to establish a level of how much hazard risk it can tolerate in order to keep losses within a framework that is tolerable.

Control risks: Uncertainty about the outcome of certain events, projects or processes in the company are called control risks. These risks are the factors that decide if a project will have

a positive outcome or not. An organization should seek to eliminate control risks to be able to predict the outcomes of its actions. (Hopkins 2010, 29)

Opportunity risks: Organizations will seek to take risks with an expectation of a positive result. These risks are a called opportunity risks as they are the risks that are taken in order to achieve gain. This is the fundamental reason for business and the quality of the risk analysis in this field may determine to a large degree the profitability of a company. (Hopkin 2010, 30)

Merna, Tony Al-Thani, Faisal F. (2008, 29) offers the view of pure risks and speculative risks as the main types of risks: Pure risks are seen as risks that only deal with a chance of a negative outcome with no upside, such as the risk of a natural disaster damaging the organization. Speculative risks are defined as the risks that are taken with the expectation of a positive return such as an investment in a certain type of merchandise.

Categorizing risks is useful to do a rough sorting of risk factors and the different types of impacts that the different categories imply. The three categories of Paul Hopkin (2010, 29) is a straight forward categorization that will encompass all risks. The more basic sorting of Merna et al. (2008, 29) does not make a clear specification of the middle ground which are the control risks category of Hopkin.

3.1.2 Risk Register

The use of risk registers as a way of structuring the risk management work is a proven way to keep track of the risk management process. The register contains an overview of the whole process, from the identification to the results of the analysis and mitigation actions taken for each individual risk factor.

Risk Identification		Risk Quantification				Risk response		
Risk	Risk category	Probability	Impact	Risk score	Risk ranking	Risk response	Trigger	Risk Owner

Figure 2 An example of a risk register (Piscopo 2015).

The risk register offers an overview of the status of the risk management process and is a way of keeping the risk management work organized. A risk register like the example above con-

tains a section to identify risks, show the calculations done to quantify the risk factors in the risk analysis and how the risks are handled.

3.1.3 Risk identification

The start of the process of managing risks is to identify the factors that affect the organization (Kallman 2007). This is done by investigating the company, its stakeholders and environment. There are several different methods for identifying risks such as interviews or brainstorming. The process of risk identification is dependent on knowing where to look.

In order to identify the risks that affect the company it is necessary to first identify the company's assets (Broder 2006, 4). The assets of a company are the people, material, money or processes that the company possess and/or rely on. The process of asset identification is an essential first step as the assets are what need protection.

After assets have been identified the process can move on to threat identification. James border (2006, 9) asks the question; "what is the company exposed to that could cause or contribute to damage, theft, or loss of property or other company assets, or that could cause or contribute to personal injury of company employees or others?"

The third step of risk identification is the collection of data and information for measuring the impact and probability of risk factors.

James Kallman (2007) puts forward seven approaches to identify threats and to collect information on risk factors:

- Statistical analysis: Where enough relevant data is available on a subject the use of statistics can be a powerful tool. Statistical analysis is useful to give indicators based on past performance. The limitation of using statistics is if the environment is changing then the result of the analysis may not be relevant.
- Contract analysis: A company has many contracts with various stakeholders. These contracts can contain various risks for the company and should be examined to expose these risks.
- Surveys and checklists: The use of risk surveys and insurance checklists can be useful to start building risk register. Risk surveys are surveys aimed at identifying risks. The use of insurance checklists is useful as it will likely include the most common hazards.
- Chart analysis: Charts can be used as a visual aide to identifying risks.

- Expert interviews: An organization has many experts that are both internal and external. These persons have extensive knowledge of their field and may give insight into unimagined risks. The different categories of the companies operations have their experts that can give unique inputs to the process. For example personnel that work on the lower levels on the practical side of the operations should be utilized as they have insight into the processes as they happen on the ground and may help identify risks.
- Financial statement analysis: Financial statements can be very useful in identifying a company's risks. Using financial statements asset groups, critical cash flows and important variable expenses.
- Personal inspections: Personal inspections are a vital part of a risk identification process, to get insight into how the processes function at ground level and to see potential risks. Personal inspection are a way to keep the risk awareness relevant to the development of the company since it enables a direct connection with the operations. Personal inspections can also be a way of validating information from historical sources such as financial statements and statistics.

The result of a risk identification process is a structure such as a register containing all the identified risks as individual factors. This register forms the structure of the further analysis of the risks with the collected data and the risks seen together as a whole.

3.1.4 Risk analysis

When the risk factors have been identified, they need to be collated and analysed. Risk analysis is the process of organizing and valuing the different risk factors based on the information available (Merna et. Al. 2008, 50). The process of risk analysis is done by using available information to make a prediction of the impact and probability of the individual risk factors (Broder 2006, 21). In order to achieve actionable results, the level of uncertainty in the information need to be taken into account as a part of the analysis as well.

3.1.4.1 Annual Loss Expectancy

Risk factors have a certain impact and a certain probability. To make an estimate on the impact of a risk factor over time it is useful to calculate the average impact it will have. A common term for this process is Annual Loss Expectancy. There are many ways of calculating this number, but the basic concept is to take the cost of a certain event and then calculate the interval of the event in years. This produces a number that shows the average yearly impact of the event.

One way of doing this calculation is by simplifying the numbers for impact and probability into scales that are easy to grasp. James Broder (2006, 22) presents a method where, instead of making fractions of years or days, the method instead makes you choose the value that is the closest approximation to the impact of the event and the average interval between them:

If the impact of the event is:	If the estimated frequency of occurrence is:
NOK 10, let i = 1	Once every 300 years, let f = 1
NOK 100, let i = 2	Once every 30 years, let f = 2
NOK 1.000, let i = 3	Once every 3 years, let f = 3
NOK 10.000, let i = 4	Once every 100 days, let f = 4
NOK 100.000, let i = 5	Once every 10 days, let f = 5
NOK 1.000.000, let i = 6	Once per day, let f = 6
NOK 10.000.000, let i = 7	Ten times per day = 7
NOK 100.000.000, let i = 8	One hundred times per day = 8

Table 1 impact and probability scale (Broder 2006,22). The values have been adapted to fit NOK currency.

The formula transmutes three years into 1000 days as a basis for making calculations. When using the impact and frequency values in the table above the values of Annual loss expectancy can be calculated using the following formula (Broder 2006, 22):

$$ALE = 10^{(f+i-3)/3}$$

The use of this kind of method for calculating the relative impact of risk factors can do much to simplify the calculations done in a risk analysis. This approach gives a calculation that is good enough for most purposes of decision-making in a risk management perspective. It is also relatively easy to use with a simple calculation.

The drawback of this method is that it gives a result that approximates the actual value of ALE. The discrepancy between actual values of the variables and the i and f variables creates a difference between the projected ALE and the actual ALE. This difference can make a significant impact on the ALE process. If the ALE process is done for the whole spectrum of a company's risk factors the sum of the companies ALE is likely to be misleading.

Because of this drawback it was decided for this thesis to create a method of calculating ALE that would solve this problem.

3.1.4.2 Fault tree analysis

A risk event has certain causes that can be predicted. When a system is known well enough, the use of a cause analysis can be relevant to identify the root causes of a risk event and thus be a vital aid in calculating its probability (Aven 2008, 40). The method is to use fault trees

for both the events that made the event happen and also the events that allowed the protection measures to fail so that the event could in fact happen.

Another version of a fault tree analysis is the bow tie method. For any event, there are specific causes and consequences and the bow tie method is a way of analysing risks where the starting point of the analysis is the event (Wyllie 2016). In order to understand the risk, the causes and consequences need to be established. The method works by asking two questions: What are the mechanisms that can cause the event and what are the protective measures for them? What are the mechanisms that cause harm as a result of the event, what measures are in place to handle it and what are the final consequences?

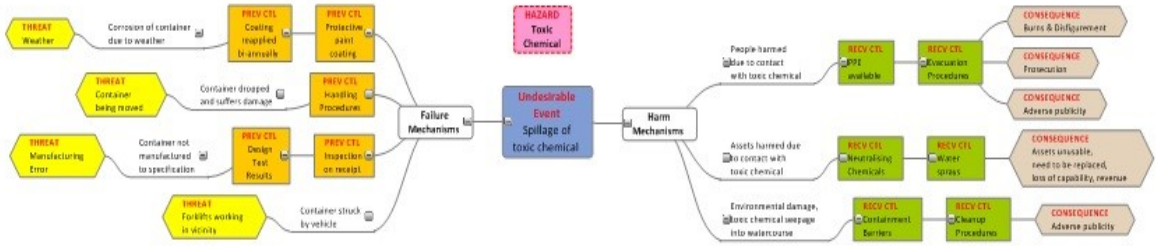


Figure 3 An example of a bow tie analysis with control and mitigation processes. (Wyllie 2016)

In the example above the hazard of a toxic chemical is translated to the undesirable event of a spillage of the toxic chemical. The figure then branches in two directions. These branches describe how the failure and harm mechanisms function. On the far left of the figure are the threats that can cause the undesired event. Between the event and the threat are the safeguards that, if functioning, will stop the event for happening. On the right side of the event are the different consequences of the event. The green boxes are the mitigation mechanisms in place to reduce the impact of the event when it occurs and on the far right are the consequences that may occur due to the event.

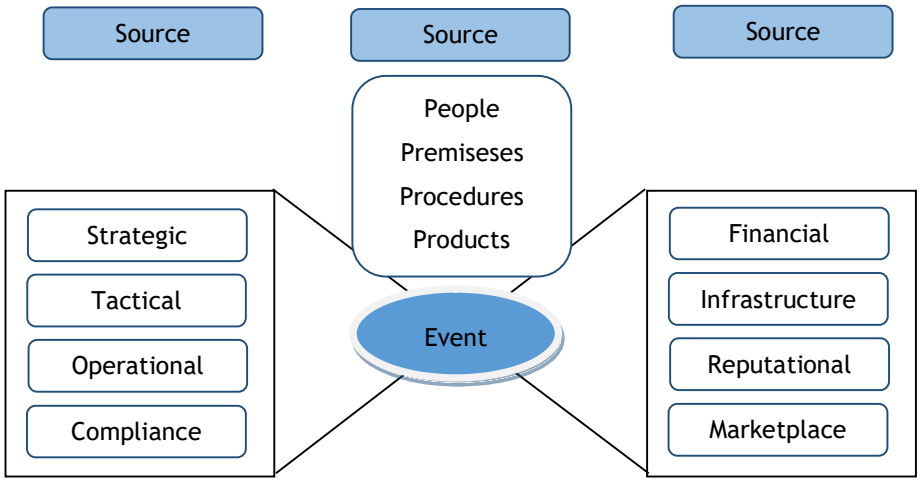


Figure 4 A basic bow tie analysis (Hopkin 2012, 48)

Hopkin (2012, 48) shows in figure 11 a bow tie analysis that takes the assets as the source of events. This method is less complicated than Wyllies (2016) method. The version of a bow tie as shown by Hopkin offers a less comprehensive analysis since the control and mitigation mechanisms are absent. This is however tempered by the way that it is easier to use and offers a simple tool to investigate the underlying causes for an undesirable event as well as the consequences.

3.1.4.3 Risk matrix

A risk matrix is a way of organizing risk factors in order to assess the larger picture. There are many ways to produce such a matrix, but the most common is a simple scaling on the two axis of probability and impact (Aven 2008, 24). There are two main ways to construct a risk matrix. Either using numerical values to define the values on the grid or then terms describing likelihood and impact.

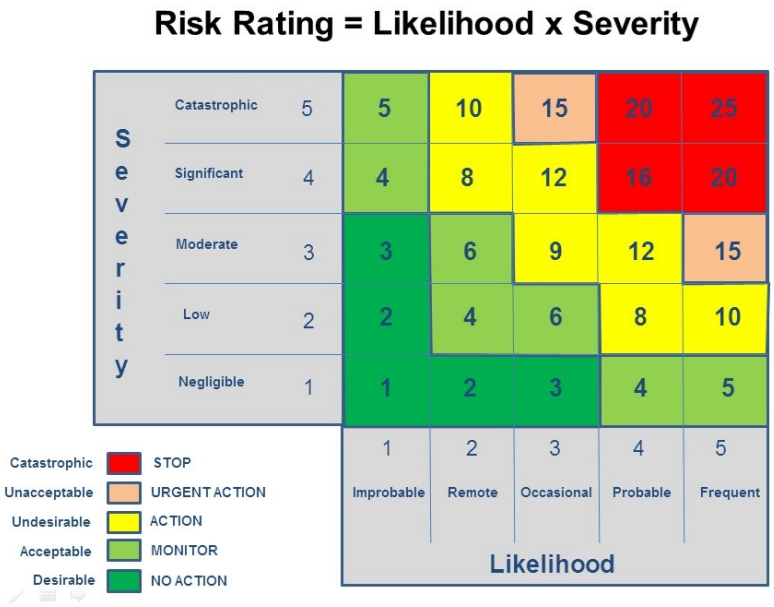


Figure 5 an example of a risk matrix that contains grading for the severity and includes risk tolerance levels (Wyllie 2016).

A risk matrix such as the example in Figure 8 is a useful tool for making a basis for decision-making in the risk management process. The matrix offers a scaling that readily identifies the severity of a risk factor. The drawback of this type of simple matrix is that it is easily misused

and the results can be misleading if the values that are put into the matrix is wrong. This can be offset however by having systems and routines that will ensure the quality in the analysis that leads up to the values to be put into the matrix.

3.1.4.4 Uncertainty

Uncertainty in risk analysis is not the same as risk according to Merna et al. (2008, 14). Merna et al. makes the distinction that "Known unknowns are the risk events whose occurrence is predictable or foreseeable with either their probability of occurrence or likely effect known (…) Unknown unknowns are the events whose probabilities of occurrence and effect are not foreseeable."

Knowledge of the data's strength that underlies the analysis is essential to arrive at a valuable conclusion. Terje Aven (2015, 59) categorizes the relative strength of the information into three ratings: Strong, Medium and weak information.

Weak information:

- The prerequisites for the conclusions represent significant simplifications.
- Data/information is non-existent or very unreliable/irrelevant.
- There is significant disagreements between experts.
- The phenomenon that are involved are poorly understood, models do not exist, or are known to give bad predictions.

Medium information:

A medium rating is represented as achieving a score in between strong and weak.

Strong information:

- The prerequisites for the conclusions are seen as being very reasonable.
- Data/information is available in large quantities.
- There is a broad consensus among the experts in the field.
- The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

This classifying system can be simplified into a scoring system where 1-4 represents the number of strong indicators are achieved. This can then be organized into the following system:

- Strong: 4
- Medium: 2-3
- Weak: 1

When using this type of scoring system the result of the analysis can be visualized in a risk matrix. Figure 2 shows a risk matrix where the confidence levels in the data are represented by green, yellow and red, for strong, medium and weak.

By analysing the risk factors on the basis of the credibility of the information the conclusions may be different than if the presented result of a risk analysis omits any reference to the information's credibility. By including such an analysis the result of the risk analysis process will be more accurate.

3.1.4.5 Risk mitigation

Mitigation is sustained action that reduces or eliminates risks to people or property form hazards or its effects (Broder 2006, 102). According to Begoña Vitoriano, JavierMontero and Da Ruan (2013, vii) "A disaster is understood as the disruption of the normal functioning of a system or community, which causes a strong impact on people, structures and environment, and goes beyond local capacity of response." While Dictionary.com defines disaster as: "a calamitous event, especially one occurring suddenly and causing great loss of life, damage, or hardship, as a flood, airplane crash, or business failure."

When considering hazard risks that may affect an organizations operation or the safety of people in and around the organization, the question of how to deal with disaster events becomes relevant. It is necessary to consider the effects of a disaster event to ensure the safety of people and the survival of the organization. When dealing with hazard events that are occurring a disaster may develop if it is handled incorrectly (Watters 2014, 7). The goal must then be to develop a structure that can handle such events in a way that hazard events, when they occur, will have a limited damage potential.

The mitigation of consequences is the result of the risk management process where the identified threats are removed or have their probability or impact lowered. Risk mitigation is the result of the risk analysis process. The mitigation of consequences is one of the main benefits that can be gleaned from the RM process (Broder 2006, 102). The risk mitigation process takes the results of the analysis work that have already been completed and puts it into practice.

To change the risk levels that the company is facing there needs to be made plans for how to implement the safeguards and other mitigation efforts. This kind of mitigation plan is necessary to achieve the effect of reducing the impact and probability of a risk to an acceptable level. When the risk mitigation efforts are applied, the risk levels are lowered if they are functioning properly. This will need to be examined and the plans that are made to mitigate the risks will need to be evaluated.

3.2 Business Continuity Management

In order to ensure the survival of an organization there needs to be a plan to deal with events that can disrupt the activities of a company. Many such factors can be harmful enough that they can threaten the survival of the company. In order to ensure the survival and effective handling of disasters there needs to be planning and preparation done beforehand to ensure that the company can continue to operate. The term continuity as used in Business Continuity Management (BCM) means that the entity that has continuity will continue to be, despite resistance (Hotchkiss 2010, 1). BCM is a collection of methods that enables a company to endure.

There are two factors that makes BCM a useful tool; the need to mitigate risks that threaten the company and the agility that a company gains from having plans to handle business outages (Hotchkiss 2010, 1). Al Hour (2012, 23) list the benefits of a BCM program as being capable to; Mitigate Disasters, Protect stakeholders interest, Adhere to regulations, Protect reputation, Enhance performance and Reduce losses.

The discipline of Business Continuity Management (BCM) provides a structure to accomplish the desired result of a more effective organization. An organization that is less likely to fail and will be capable of outperforming competitors with quicker and less costly recovery operations.

3.2.1 Establishing a BCM program

A BCM program requires a strong foundation. There needs to be a willingness to see it through and keep it alive. There needs to be a willingness to keep the program working. It will not work if it is not constantly active and a part of the regular workings of the organisation is applied on. According to Al Hour (2012, 29), previous implementations have led to the identification of the following key factors to a successful BCM program:

- Effective top management involvement, commitment and support
- Relevance
- Meeting regulatory requirements and audit guidelines

- Sufficient resources
- Effective communication
- Satisfactory coverage

These key factors are a useful guide when conceiving a BCM program. There needs to be a clear understanding of how the target organisation operates in order to be successful with a BCM program and the whole organization and all of its stakeholders will need to be involved or at the very least taken into consideration.

The approach of Hotchkiss (2010, 23) in this initial phase is to create a continuity strategy based on the companies stated strategy. The approach that Hotchkiss states for making a strategy is however quite similar to that of Al Hours focus on governance systems and policy generation on this basis. The methods of Al Hour as a structure seems to be more in line with the practical implementation. Such a system will therefore be the focus of the further generation of the BCM framework.

3.2.2 Business Continuity Management Governance system

The process of establishing a BCM system into an organization starts with the establishment of a system that lays a foundation for the BCM work. In order to be a document to guide the work in a BCM program the system needs to cover all the necessary allocations that the process will require to function. Al Hour gives a list of the factors that he considers most relevant:

Al Hour (2012, 32) defines the main parts of a governance system as BCM Policy, Roles and responsibility, and reporting and management structure. The model in Figure 11 shows the interaction of these parts.

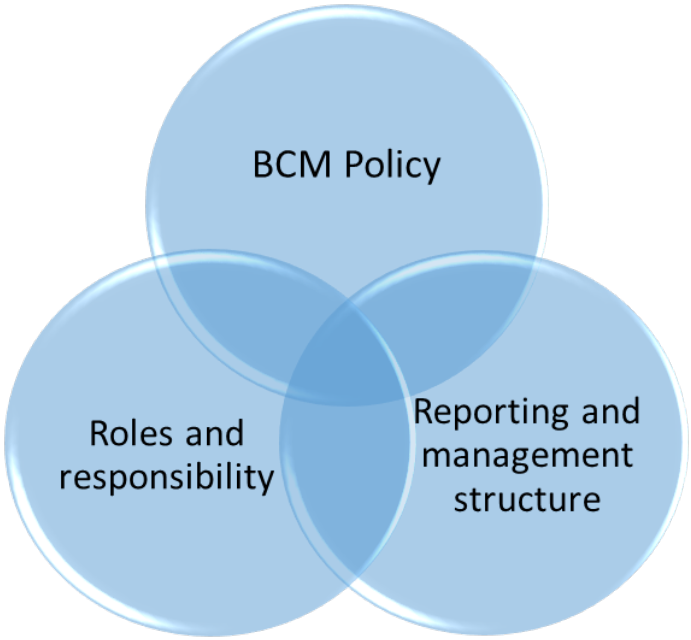


Figure 6 The main parts of the governance system of a BCM program (Al Hour, 33).

3.2.2.1 BCM Policy

At the heart of the BCM process is the BCM Policy. This document is intended to be the source of the processes authority and it will detail who is responsible for what and in what way. The following are four elements of what a good policy should look like (UCDAVIES 2011):

- The policy should be written in a clear, concise and simple language
- The policy statements should address what is the rule rather than how to implement the rule
- The policy should avoid the use of jargon as that can lead to some stakeholders not feeling included in what the policy is doing.
- The statements in the policy document should be readily available to all stakeholders

There can for a BCM policy be included statements for intent, inclusion, seriousness, policy details and compliance (Hotchkiss 2010, 26). There are other factors that may be added to this list such as the objectives of, definitions related to and the scope of the BCM program (Al Hour 2012, 34).

Many things can be included in a policy document. The core of that part of the process is however the statements that clearly state the requirements that the BCM process puts on

each part of the organization. For a Policy to function well it is necessary to include both how the process should be carried out, for what purpose, how the performance is measured and who is responsible for what.

3.2.2.2 Reporting and management structure

In order to get the governance system working it is necessary to have an owner of the BCM process. This needs to be a person with real influence and authority to move things in the company in order to give the BCM program real influence and independence in the organization (Al Hour 2012, 34).

In Al Hours model (2012, 35), the BCM manager who is responsible for the whole BCM program in the company will be subordinate to the owner of the BCM program. This ensures that the BCM manager has the necessary backing to implement the BCM program. The BCM manager, since he has authority from the top can then implement the BCM program and coordinate the BCM work in the different parts of the company. The different parts of the company needs to have assigned coordinators as well to ensure that the BCM work is being done properly in the different parts of the company. There is a need to also get the different BCM related programs into the governance system to be able to effectively coordinate responses to disasters.

3.2.2.3 Roles and responsibilities

In the previous section the different levels of the BCM organisation was laid out; BCM Owner, BCM Manager and coordinators. There needs to be a clear dividing of responsibilities for the different levels of the BCM organisation in order for it to function. Al Hour (2012, 40) presents the following dividing of responsibility; The BCM Owner who is accountable for the performance of the BCM program, The BCM Manager that is the person in charge of keeping the program running and the BCM Coordinators that are the managers of the local departments and branches.

Dividing the responsibilities in the BCM organisation is a vital aspect to consider when constructing a BCM program. The roles of the different levels will need to be designed to support and strengthen one-another so that the program will function properly. When adapting this structure to a smaller organisation the levels of the BCM organisation may be fewer but the roles will need to be fashioned with the same goal in mind.

3.2.3 The BCM Process

In the organisation that is starting to run a BCM process there needs to be certain groundwork to be done before the work on the actual BCM program can begin. The vital parts of this process should be in hand if the organisation has completed the process of making a BCM policy.

There are however many parts in the programs that will need completion before the BCM program is operational.

There may be a need to establish a specific project to create the first edition of the BCM program. According to Al Hour (2012, 53) this project should include a business case, terms of reference, communications plan and risk register.

In order to ensure that the establishment of the BCM program goes smoothly the business case where the reasons for the program is laid out as a series of either historical or potential events that need to be dealt with. The terms of reference of the project would give the boundaries of the project and the scope of the BCM program by showing the different assets, processes and resources that are attached to it.

3.2.3.1 BCM Lifecycle

The BCM process is a continuous loop where once established is will continue to operate and, if it functions properly, improve itself for each turning of the wheel. The process has several steps as shown in Figure 2:

Figure 7 The BCM "Lifecycle" (Al Hour 2012, 51)

The wheel represents the different parts of the process. The sequence shows how they relate to one another. The different parts of the process as represented in Figure 2 need to be done

in sequence in order to achieve the desired results from a BCM process. As the process is established and keeps running the processes will be done in succession throughout the lifetime of the program.

3.2.3.2 Business Impact Analysis

A Business Impact Analysis (BIA) is the first step in a BCM program. The purpose of the BIA process is to go through the processes and assets of the company and identify the threats to these, and the impact of those threats. There are many ways of approaching a BIA process and the process itself can be done in a number of ways.

When considering the threats to a company it is easy to think of all threats as critical. If there is no structured way to force a prioritization of threats this can easily become the case (Hotchkiss 2010, 28). If there is not sufficient prioritization of threats that can be a critical weakness in a BIA process. The threats must also be held up to what processes and assets they affect (Elliott, Swartz, Herbane 2012, 136). The processes and assets themselves may have very different value to the company depending on the timeline. When continuing with the planning of responses the processes that are most vital on a short term basis will need to be given priority (Hotchkiss 2010, 28).

According to Al Hour (2012, 34) the objectives of a BIA process are the following:

- The environment the company is operating in
- The stakeholders requirements
- The regulatory or statutory/legal requirements
- The key core activities in the organization
- The assets or resources, internal and external, support key activities
- The impacts on the organization in the event of key, or core activities over time
- The interdependencies between internal and external resources and assets
- The organizations obligations towards external entities

In order to achieve these objectives, there are certain tasks that need to be done in sequence in order to do the BIA process effectively according to Al Hour (2012, 35). The tasks are to gather information, a process of validating the collected material, analysis of the collected material and lastly to approve and report the results of the BIA.

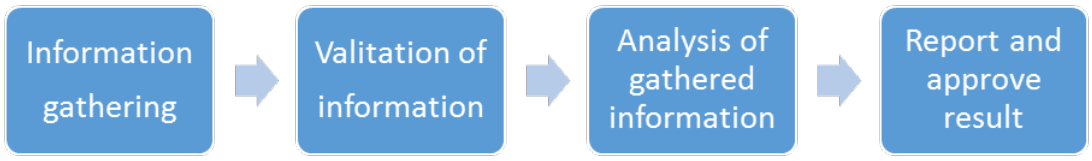


Figure 8 The process of executing a BIA.

In order to begin a process such as a BIA process there needs to be collected a sufficient amount of information to begin creating a foundation for the process. The process of gathering information can be done in several ways such as with questionnaires and interviews. Al Hour (2012, 35) recommends using questionnaires to gather data, conduct interviews based on the data that was gathered and use workshops to filter and structure the gathered information.

Al Hour (2012, 36) goes on to suggest that the following information be gathered initially in the process:

- Processes and activities within the scope
    - What resources are requires to keep them operational
- Internal and external dependencies between the processes and activities
    - Impact over time when the processes are not operating.
- The Maximum Tolerated Outage (MTO) of the processes and activities.
    - The maximum data loss tolerated
- The technology used in the processes and activities
- The key personnel, availability and succession in the organization
- Resources that are required to recover a process in a new location.

When the information on these points has been gathered sufficiently the process can continue. The information that has been gathered will need to be evaluated and further gathering will need to be conducted. These further investigations can be interviews with the owners of certain processes where there is a need for clarification or to gain more depth in a certain critical process.

This stage of the process is a necessary step to ensure the quality of the process as it continues. The data that the process has collected so far will need to be evaluated as a control mechanism to achieve this. When going through the validation process, the experts on each field needs to be consulted (Al Hour 2012, 36). When the process is completed the resulting information should be only information that is reliable and relevant to the process.

When the information has been collected, structured and validated it is ready for the analysis phase of the program. This part is where the actual conclusions of the BIA process are made. The analysis process focuses on defining Recovery Time Objectives (RTO), Recovery Point Ob-

jective (RPO) and the level of criticality for the processes and activities within the scope of the BIA (Al Hour 2012, 34). The result of the analysis should be a structure where the identified processes and activities have their dependencies defined and the RTO, RPO and a ranking on how critical the different processes are.

Another aspect of the report should be how certain processes have a higher impact in certain times of the year and some processes may have a higher importance in crisis times rather than in normal operations.

The results of the analysis needs to be approved by the management and the BCM Owner in order to allocate the appropriate resources to continue the BCM process (Hotchkiss 2010, 57). The following report needs to contain a full view of the analysis results, special concerns that were identified and recommendations for further action (Al Hour 2012, 36). The report should be written in such a way that it is easily accessible for all involved branches, at the same time as it contains enough information for specialists to evaluate the details of the different branches.

When the reported information is approved, the BCM process can continue with a strong foundation based on the BIA that has now established how the company functions, the processes and activities that it relies on. The impacts of what would happen if the different processes were to be taken out is established and with that a rating of criticality and a structure that allows for decision-making on how to proceed with the process.

3.2.3.3 Risk assessment

Risk assessment in a BCM environment is about looking at the risk management process with the priorities already laid out. When the BIA is done the risks to the company processes are already mapped out and so the low impact risks can be safely ignored (Hotchkiss 2010, 42).

There are many parallels between Risk Management (RM) and BCM. The RM process fills out the BCM process by providing the management structure to handle the risks while the BCM process focuses on the company's assets and operations (Al Hour 2012, 26). In order to have a well-functioning BCM program there needs to be a done a thorough groundwork on the management of risks and so a BCM program will be much weaker if the RM processes are not done properly.

The first step of the risk assessment process is to identify the main components of the company. This process will give an idea of where weaknesses may occur further down the line. Next comes the process of identifying threats that may adversely affect these components

and how to organize, analyse and treat them. These threats are what is called risks and the process of handling them is referred to in the section of RM, Risk Analysis.

3.2.3.4 BCM strategy

When the BIA is completed and the risks have been analysed and prioritized, the next step is to find what to do with the information. BCM strategy is where the decisions are made as to how the threats and risks that have been identified should be treated (Al Hour 2012, 38). Risk Treatment Plans (RTP) are the plans for how the risks will be mitigated in practice and form the core of a BCM strategy effort.

There are three factors that should be taken into consideration when evaluating which strategies to pursue. Al Hour (2012, 39) puts forward three points to consider:

- Effectiveness: How effective is the strategy at minimizing probability and impact, protecting critical elements and how well do they align with the continuity requirements?
- Cost-benefit analysis: The strategy will have to be carefully analysed to ensure that the cost of implementing it does not exceed the cost from the risk.
- Applicability: The strategy needs to be made in such a way that it is possible to implement it in a practical way. Ideal scenarios do not exist and a strategy that does not take this into account will have a much lower value.

The scope of the BCM strategy is the parts of the company that are affected by risk. There are many ways to categorize the parts of a company. The main idea is however to partition the different assets in a way so that the processes of the company are made visible and easy to work with when making strategies and RTP's. Al Hour (2012, 39) gives the following categories; Processes, Technology, People, Facilities and premises, Information and Supplies.

Al Hours categorization above is quite detailed. When considering the different parts the organization as a collection of internal and external stakeholders and dependencies, the categories suggested by Sterling (2012, 115) offer a less complex top view; People, Premises, Resources and Suppliers.

Both offer an overview of the same parts of the company but with different categorization and emphasis. For example, the concern for information and technology from Al Hours categories are accounted for in the Premises category of Sterling.

Figure 9 The different parts of a company in terms of asset protection. (Al Hour (2012, 39)

The process of producing mitigation strategies and RTPs are a similar process to that of the RM Risk mitigation as mentioned earlier. The purpose of this part of the process is to make plans and strategies that will lower the overall probability and impact of the threats that are facing the company.

People are the core of any organization. This implies that the people of the company should have the focus of the process. There are different ways to look at strategies for risks involving people. When you have personnel with key competences filling key positions, what do you do to ensure that the processes they were operating will keep functioning (Stirling 2012, 115)? Al Hour (2012, 75) asks a similar question and suggests four main goals for strategies involving the people of the company:

- The safety and well-being of people need to be ensured.
- Minimizing the risks and threats that come from people and staff
- Making sure that there is enough of the right people available to facilitate recovery
- Making sure that people have the right competencies and knowledge throughout the recovery and continuity phases.

These goals show a way of focusing the effort of how the people factor should be handled in a continuity and recovery setting. They then need to be translated into actual plans for how to

make the people in the company ready. Stirling (2012, 116) suggests that there should be made an effort to spread the key personnel out so that a single event can destabilize the continuity plan and make it more difficult and costly to recover.

The premises of a company is all the physical locations that the company uses for its activities. There can be several buildings or areas, or the company may be located all in one room. The main idea of strategies for the premises of a business is to plan for an event where the premises are rendered unusable (Stirling 2012, 117). If such an event occurs then in order to continue operations the company will need to relocate said operations. This means that alternatives need to be found that can be activated when the need arises.

When considering technology what is meant is the technical applications and systems that are used in the companies operations. These can be computers, servers, software or other technological aids that the company needs for its different activities and processes. In the event of these failing there needs to be replacements ready if the processes and activities are to be resumed. The strategies and RTPs for technology generally fall under the category of information security since it deals with the infrastructure of the information flow if the company (Al Hour 2012, 78).

There should be redundant systems for the technical systems in order to facilitate recovery. Having that kind of capability can be crucial to minimizing recovery time. Keeping servers off site, organizing a virtual private network and keeping spares available are some suggestions for enabling recovery (Sterling 2012, 117).

Information security is a vital piece of any business continuity structure. Breaches in this field can have disastrous consequences for the company. The objective of information security is to protect information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction (Vacca 2010, 2). Al Hour (2012, 79) suggests these four requirements for the strategies that are targeted at information:

- Confidentiality: Ensure that information that could harm the company is protected from disclosure.
- Integrity: Ensure that information cannot be tampered with or in other ways be made to give false results.
- Availability: Ensure that information is available to the relevant stakeholders when they need it.
- Currency: Ensure that information is kept up to date as required.

The Confidentiality, Integrity and Availability are standard terms of the different goals of information security. In order to make these goals happen it is necessary to take action to ensure that the strategies and RTPs are within the continuity requirements. Vacca (2010, 11) suggests that in addition to incorporating protection mechanisms, there should be ways to detect and react to attacks in order to facilitate the recovery from such an action.

To ensure confidentiality there needs to be a system for authentication of who can access the information and also a system to prevent external attacks. Integrity is based on the controls of how the information is entered and stored. Availability is ensured by establishing methods and systems that give the relevant stakeholders access to the information they need when they need it.

A company needs supplies to function. Any company will stop functioning if a critical supply will stop coming. This dependency on the supplier means that the whole chain of suppliers, from the producers of raw materials to the suppliers of the material the company needs makes the company vulnerable to disruption at the supplier end (Elliot et al. 2010, 152). In order to avoid or reduce the impact of a supplier having reduced capacity to deliver there should be made arrangements with other suppliers of the same goods to take over if the supplier fails (Stirling 2012, 118).

To prepare for an event where the company's own supplies are damaged or made unavailable it may be a viable option to keep extra stock at a different location or to have arrangements for extra deliveries with suppliers (Al Hour 2012, 81).

3.2.3.5 Planning and implementation

In the BCM process when the strategies for how the different risks should be mitigated then it is time to start making plans for the implementation of the BCM program. There are two main planning tools that regulate the BCM work: The Crisis Management Plan (CMP) and the Business Continuity Plan (BCP) (Al Hour 2012, 42). These plans show in practice what should be done to first, handle the crisis as it happens and then the process towards resuming normal operations.

When shaping these plans it is important to make them as detailed as is practical so that there is little need to think when a crisis occurs. Hotchkiss (2010, 65) suggests a structure as the following for developing procedures, with the following points as columns in a form:

- Process step: An action that is concrete, definable and measurable. A specific action for a specific purpose.

- Who: This would ideally be the name of the person that is to take the action or the position that will take the action.
- Time taken: This is to define how long the step will take. This is useful for planning the crisis management as someone can only do one thing at a time and often actions will have to be done in sequence.
- Resource needed: This means resources of any definition. Whatever is required to fulfil the task, a document, a person or a technical implement, it should be stated exactly what it is that is needed and how to get it.

When using a setup as was suggested by Hotchkiss in the points above the product is a set of plans that give exact instructions in an emergency. In a high pressure situation such as an emergency many people are not capable of making rational decisions (Elliot et al. 2010, 277). Because of this it can useful to have a step by step guide to simplify and make the crisis management and recovery processes effective.

3.2.3.6 Crisis Management Plan

When dealing with a crisis time will be of the essence and having the ability to react swiftly and correctly can have major impacts on the future of the company (Elliot et al. 2010, 225). The crisis management plan is the document that shows how a crisis should be dealt with in detail. From phone numbers to call to mitigation strategies to implement the CMP needs to have all of it taken into consideration. Al Hour (2012, 84) suggests these main objectives of a CMP:

- Enable the correct assessment of the situation.
- Make sure that the communication channels that are required are opened.
- Take control of the situation and limit the impacts.

There are two main approaches to develop a CMP: A scenario based approach or an impact based approach (Al Hour 2012, 85). The scenario based approach is where the focus of development is on the development of scenarios and then developing plans to handle the scenarios. The impact based approach is to develop plans for the different impacts that can affect the company. When evaluating these approaches the organisations capabilities and requirements are important factors.

Coombs (2007) suggests that a CMP is not a step by step plan but a reference tool to guide and aid in the handling of a crisis. This suggests that a CMP should have a limited amount of specific instructions in order to be flexible enough. According to Hotchkiss (2010, 65) a CMP should be very structured with detailed information. In order to fulfil its goal of being a tool

for handling an emergency a CMP should fulfil both these targets of being both structured but flexible where required.

A CMP should however have a structure that allows it function according to its intended purpose. Al Hour (2012, 85) suggests that a CMP should contain the following points:

- Purpose and Scope: The plan should identify which of the company's processes and assets it covers and their continuity specifications.
- Roles and Responsibilities: The roles, responsibilities and authorities for executing the plan.
- Invocation Process: There must be a description of the invocation process functions. This is the process how the crisis situation is identified and the relevant actions to begin dealing with the crisis is implemented.
- Document ownership and maintenance: There should be a defined owner of the CMP that is responsible for keeping it up to date.
- Contact information: The plan needs to contain a list of all the contacts that are needed for the plan to function properly.
- Tasks and actions: The plan should detail the tasks that need to be done and who is responsible for doing them.
- Internal and external communications and responses: The CMP should activate communications channels that are needed for the company to navigate the crisis. Here it is also important to make sure to make allocations for informing the public (Ready.gov 2016). This is to ensure that the company's reputation is protected and that external stakeholders are aware of the developments.
- Command centres and locations: There should be identified alternative locations to manage the crisis in the event that the company's normal locations are unusable.
- Appendices: This part is to put in any other relevant documents, forms and so on that is needed to manage the handling of the crisis.

The CMP should be maintained and tested so that it is up to date and will actually work. When making such a document it is important to keep in mind what is realistic. A plan that assumes too much will not work properly when a crisis does occur.

3.2.3.7 Business Continuity Plan

The CMP is the plan that will try to handle a crisis as it occurs and lessen the impact of it. The BCP comes into effect when the crisis is over and it is time to rebuild and get operations back on track. In order to accomplish this the plan will need to contain all the necessary steps to recover the processes and assets that have been lost in the crisis (Elliot et al. 2010, 163). A

business plan can be written for a business process or may cover all key processes (Rittinghouse & Ransome 2011, 5). The structure of a BCP should be made with the users in mind and with a clear view of the objectives. The following points are a structure for a BCP as suggested by Al Hour (2012, 87):

- Purpose and Scope: The plan should identify which of the company's processes and assets it covers and their continuity specifications.
- Roles and Responsibilities: The roles, responsibilities and authorities for executing the BCP.
- Invocation Process: There must be a description of the invocation process functions. This is the process how the need for the specific continuity plan is identified and the relevant actions to begin activating it is implemented.
- Document ownership and maintenance: There should be a defined owner of the BCP that is responsible for keeping it up to date.
- Contact information: The plan needs to contain a list of all the contacts that are needed for the plan to function properly.
- Tasks and actions: The plan should detail the tasks that need to be done and who is responsible for doing them.
- Assets and resources required for recovery: In this part there should be an overview of the different assets and resources that are required in order to facilitate recovery. It should also be specified on a timeline when the resources are required. The resources can be anything from materials, equipment, people to information or documents.
- Restoration process: The details for how to recover to the point where normal operations are resumed.
- Appendices: This part is to put in any other relevant documents, forms and so on that is needed to manage the handling of the crisis.

A BCP is a document that aims at recovering processes and activities that has been prevented due to an undesirable event. For a BCP to be successful it will need to take the capabilities of the company into consideration. As with other plans it will not work if it does not take the actual capabilities of the company into consideration.

3.2.3.8 Training and awareness

The BCM program's success depends on the ability and willingness of the people of the company to follow through with it. The BCM awareness focuses on building knowledge about how the parts of the process functions, and the BCM training imparts the necessary skills and knowledge to the internal and external stakeholders to execute the BCM processes such as

the CMP and BCPs (Al Hour 2012, 91). Installing a BCM culture in the staff of the company is about retraining the way that the organisation thinks and plans (Sterling 2012, 124). The training and awareness work should focus on creating individuals that are motivated and capable of working together to solve a crisis.

3.2.3.9 Testing

In order to ensure that the BCM system functions as intended it needs to be tested thoroughly. Testing in this context means the actions that are taken to evaluate whether the CMPs and BCPs give the expected results (Elliot et al. 2010, 234). By testing and evaluating the procedures the confidence and capabilities of the workforce can be enhanced (Stirling 2012, 126). Testing and the evaluation of results can give vital inputs for developing the BCM process further.

There are several different types of tests that can be performed to evaluate the BCM processes. The types of tests that are used are dependent on the processes and the resources that are available. Al Hour (2012, 94) suggests the following types of test that can be done; A desk check is a simple test that looks over a part of the program, Walkthroughs is done with the people involved in the steps, a simulation where a disaster is created and the relevant plans are activated. After this is the full test I which the whole system is tested in one operation.

3.2.3.10 Re-Running the Cycle

In order to have a functioning BCM program it needs to be running continuously. There needs to be a continuous readiness and willingness to evaluate and update the plans and procedures that have been developed earlier.

There are two types of triggers to re-run the cycle: Time triggers and Change triggers. Time triggers come from having a plan for re-running the program at a set interval. Change triggers on the other hand are triggers that come from changes in the environment such as staff turnover, new services or products and changes in the infrastructure. There can also be change triggers from internal sources such as a change in the company's goals or strategies. (Al Hour 2012, 96)

When making plans and constructing the crisis and readiness plans there needs to be made a plan for when the structure is to be re-visited. In order for the system to remain relevant there should be a set interval where the system is re-run or audited. In addition the definition of what changes that require the system to be re-visited may be a valuable addition to such a plan.

4 Method and empirical study

4.1 Limitations of the study

The study is divided into two parts; the information that is needed to develop the methods for doing the RM and BCM process for the company and the collection of the information that is needed to run the process.

4.2 Development

4.2.1 Initializing development of a risk and continuity management method

The methods that are shown in the theory part earlier in this paper are for the most part aimed at larger companies with big organizations and a complex set of processes, activities and dependencies. A large company needs similarly complex plan to manage the different threats it is facing. A small company does not have the same complexity, or the same resources, but it is facing many of the same threats and may have an equal or higher risk of failing due to a crisis event.

The company that was the object of this thesis needed a structuring of its risk and continuity management. Risk Management and Business Continuity Management are large complex fields with complicated methods that can seem impossible or unnecessary to a small company. To make a system that would fit for this company the methodology that is applied to large organizations needed to be slimmed down substantially for it to be viable.

During the interview with the owner of the company the requirements for the system was discussed. The following points are the main requirements the company has for the system:

1. There will be only one system, and that will take care of the risk management and business continuity requirements for the company.
2. The company has limited resources to do such a process. The limitations are in both time and money, so the system needs to be cost effective both in terms of the time spent working on it, and money required to establish and maintain it.
3. If it is too large, meaning that it has a too large a scope, it will likely not be maintained and so it will quickly fall out of use.
4. The finished product, once it has been established, needs to be easy to use and easy to update.

The goal of the development of the system was to find a way that the company could have a sufficient readiness and ability to identify, treat and prepare for threats and other risks that may affect the company. After consulting with the owner of the company, the new method

will be referred to as Business Continuity & Risk Management (BCRM) to avoid confusion with its parent methodologies.

4.2.2 Combining Risk Analysis and Business Continuity methods

In the processes contained in the Risk Analysis and Business Continuity Methods Described above there is significant overlap although the methods do not make one another irrelevant. Risk analysis is as described a way to structure risks and set up a way to mitigate them while Business Continuity focuses more on the methods on how to develop the recovery and survival structures of an organization.

When considering what is relevant for the company the practical focus that is more readily available through the shown in Al Hours (2012) Business Continuity Management process is a more viable option. The focus on planning control and mitigation strategies also makes this a more viable option.

Much of the Risk Analysis process is contained in the risk assessment part of the Business Continuity Management process. The main parts that are missing are the control risks and opportunity risks. To make the process contain the Risk Analysis parts that are needed for the company they will need to be contained in the process. Considering that opportunity risks do not fit into the same grading structure as control and hazard risks the opportunity risks will need to have their own space. Other risks that is facing the company in the realm of hazard and control risks will be dealt with in the BIA → risk assessment → mitigation strategies of the Business Continuity Management model.

4.2.3 Business Continuity and Risk Management

Based on this the structure of the system for the company will be referred to as Business Continuity and Risk Management (BCRM). The BCRM system takes its structure for the Business Continuity Management process from Al Hours (2012) with the added focus on managing a wider range of risk types than what is given in that structure.

The BCRM system in its current state of development takes the form of a compressed version of the BCM and RM systems that have been explained in the theory section of this thesis. The full description of the construction of the method can be found in the Appendix BCRM Method.

5 BCRM for the company

The next step for the company is to go through the process of BCRM. The information needed to do the process was collected through a series of interviews, a workshop and an inspection.

5.1 Information gathering

5.1.1 Inspection

The first step of the process of gathering information was to do an inspection of the premises. This inspection gave information that was used for identifying elements for the BIA and risk analysis and for going forward in the information gathering process.

5.1.2 Interviews

The interviews were done in several rounds. The first interview was with the owner and the manager to map out the governance structure and to do the BIA. The second interview was to validate the BIA results, do the risk analysis and to start the work on strategies and RTP generation.

5.1.3 Workshop

While the inspection and the interviews gathered information the workshop was done to validate the preliminary work on the BIA and risk assessment and to work out the scope and direction for the planning process.
The workshop was organized the way that the owner, manager and employees of the company came together and was presented the results of the process up to the point where the strategies had started to take form. The participants were then encouraged to make comments and adjustments to this. The next step was to lay down the scope for the strategies and CMP/BCP work.

5.2 Execution and scope

The scope for the first round of the BCRM process was limited to a selection of processes that were decided to be most relevant. The process was conducted the way that the information was gathered in the ways that are listed in the previous section and the processes that have been laid out in the BCRM section were done.

The processes were done in cooperation with the owner of the company and the results were validated as is laid out in the description of the process.

5.2.1 Business Impact Analysis

To begin the process the scope of the Business Impact Analysis (BIA) needs to be set. The scope is the parts of the company that will be included in the process.

#	Description

1	Flower decoration Prodution and sales
2	Sale of fresh flowers
3	Interior design articles
4	Transportation
5	Billing

Table 2: Business Impact Analysis scope

#	**Process/Activity** that is evaluated	**Resources required** to run the process/activity	**Internal Dependencies** are the internal processes that the process/activity relies on	**External Dependencies** are the external processes that the process/activity relies on	**MTO:** Maximum Tolerated Outage	**MTD:** Maximum Tolerated Data loss	**RTO:** Recovery Time Objective	**RPO:** Recovery Point Objectve	**Technology used** is the techincal instruments or appliances required	**Key personnel required** are the people that the process relies on to function	**Availability of Key personnel** how can they be made availible in a crisis?	**Succession** is who's in charge when comms break down?
1	Booking flower delivery and decorations for events	-Computer -Phone -Booking Book	-Availibility of worker -Booking Book	-Internet connection -Working phonelines	1 hour	2 days	1 hour	1 hour	-Computer -Phone	-The person currently on duty will complete the process	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
2	Making flower decorations for events	-Non perishable materials -Fresh flowers -Qualified worker to make it	-Availibility of Trained worker -Instructions from the Booking Book	-Decoration material supplier is able to deliver -Flowers are delivered as needed	1 day	-	1 day	1 day	-	-Specifically trained worker that can make the decorations of the appropriate quality.	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
3	Delivering flowers and decorations to customers	-Delivery vehicle -Tools for making decorations -Worker with drivers license	-Making flower decorations -Storage of fresh flowers -Delivery of flowers from supplier	-Open roads to the delivery location	30 minutes	-	2 hours	-	-Delivery vehicle -GPS	-	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
4	Billing for flower decorations and deliveries	-Computer -Billing software -Booking Book	-Booking flower decorations -Making flower decorations -Delivering flower decorations	-Power -Internet connection -Accountant oversees and executes billing	1 week	2 days	2 days	1 day	-Computer -Billing software	-The owner does the billing	-Crisis mobilisation sceme	-Owner -Manager
5	Selling fresh flowers	-Fresh flowers -Packaging material for flowers -Cooler to keep the flowers fresh -Cash register -Change -Payment terminal -Worker to expedite customers	-Storage of fresh flowers -Recieving shipments of fresh flowers	-Delivery of flowers from supplier -Delivery of packing material from supplier -Payment terminal service provider	30 minutes	-	30 minutes	.	-Cooler -Cash register -Payment terminal	-A worker able to package the flowers and use the payment systems	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
6	Storage of fresh flowers	-Cooler -Pots	-Recieving delivery of flowers from supplies	-Power	2 hours	-	1 hour	-	-Cooler	-	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
7	Recieving shipments off fresh flowers	-Cooler -Pots	-Stroage of fresh flowers	-Suppliers ability to deliver -Open roads between supplier and the store to allow the shipment to take place.	1 day	-	5 hours	.	-Cooler	-A responible worker or manager will need to be present to take the delivery and handle it properly	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
8	Recieving shipments of interior design items	-Dry storage space	-Storage of interior design articles	-Suppliers ability to deliver -Open roads between supplier and the store to allow the shipment to take place.	1 day	-	5 Hours	-	-	-A responible worker or manager will need to be present to take the delivery and handle it properly	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
9	Storage of interior design articles	-Dry storage space	-Recieving shipments of interior design articles	-	-	-	2 hours	.	-	-	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
10	Selling interior design articles	-Store space -Tables and shelves for showing the aritcles. -Cash register -Change -Payment terminal .Worker to expedite customers	-Storage of interior design articles -Recieving shipments of interior design artices	-Delivery of interior design articles from supplier -Payment terminal service provider	30 minutes	.	30 Minutes	-	-Cash register -Payment terminal	-A worker able to use the payment systems	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
11	Card payment in the store	-Payment terminal -Trained worker	-	-Power -Internet connection	10 Minutes	-	30 minutes	-	-Payment terminal	-A worker able to use the payment systems	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store
12	Cash payment in the store	-Cash register -Change -Trained Worker	-	-Power	10 Minutes	-	10 Minutes	-	-Cash register	-A worker able to use the payment systems	-Crisis mobilisation sceme	-Owner -Manager -Person on duty at the store

Table 3: Business Impact Analysis

5.2.2 Risk Analysis

The risk analysis was performed with the basis on much of the same information that formed the basis for the BIA. The identification of risks was done together with the owner of the business. There were also addtioins made based on the results of the BIA.

The Risk Register here represents a compressed result of the full risk analysis that is shown in Appendix 1: Risk Analysis.

5.2.2.1 Risk Register

Risk #	Risk Name	Risk Type	Threats	Probability safeguards	Impact safeguards	Risk score	ALE	Certainty Level	Notes	Last updated
1	Flooding hazard	Hazard	-Weather patterns create flooding	-Re-locate the store to an area with a lower flooding risk.	-Timely identification of the event and evacuation of the store. -Insurance policy for damages to the store -insurance policy for lost revenue	4	2500	4		01.04.2016
2	Fire hazard	Hazard	-Open fire -Electrical faults -Arson	-Limit the use of candles or fire in or around the store. -Train workers to use electrical equipment properly to prevent the equipment from bein used in potentially hazardous ways. -Maintain electrical equipment to prevent equipment failure -Check electrical equipment regularly and replace them when it is nessecary in order to avoid faults due to outdated equipment.	-Fire alarm with external signaling to reduce the reaction time of firefighters and others to put out a fire as early as possible. -Foam cans readlily available to put out fires before they have time to catch on. Foam cans also do not damage the interior with corrosive material and so the cost of deployment is much lower than powder based extinguishers. -Powder based extinguisher to deal with blazes that cannot be contained with foam. -The personnel that work in the store must be trained in the use of the firefighting equipment. -There must be a plan for evacuating the store in case of a fire to avoid personnel injuries.	5	1000	4		01.04.2016
3	Extreme Weather Hazard	Hazard	-Stormy winds -Heavy Rain -Heavy snowfall	-	-Move materials and vehicles inside to protect them from the weather -Keep backup systems at secondary location to keep the information to stakeholders going	9	17700	3		02.04.2016
4	Weather conditions	Control	-Off Average weather	-	-Reducing or increasing purchases of fresh flowers according to weather projections in a more dynamic purchasing strategy may be an option.	10	208000	4		02.04.2016
5	Theft	Hazard	-Theft by customers -Theft by employees -Theft by break-in	-Reduce the amount of "dark" space in the store by installing mirrors or cameras where applicable. -Screening potential employees in order to weed out	'-Do not store any cash in the store after closing.	5	9600	2		02.04.2016

				potential unfaithful workers. -Regularly checking hte daily report fro anomailes both to show that it is being done and to see if the transactions add up to what has been sold. -Do not display and high values items in the store and do not let the cash register or otherwise be visible when the store is closed.						
6	Violence to staff or customers	Hazard	-Aggressive customer -Aggressive staff member -Third party wants to harm cstomer or staff member	-Traing staff to have a non confrontaitonal attitude when dealing with unhappy customers. -Training and selecting staff on ability to have self control and restraint in the face of a confrontaitonal customer.	-Training staff to procedures to handle violent persons -Debriefings, psychiatrist sessions to handle trauma. -Information to the public to communicate control and show that it is safe.	8	-	4		03.04.2016
7	Car accident while doing transport	Hazard	-Poor weather conditions -Poor road conditions -Other drivers -Irresponsible driver	-Monitor conditions and halt transports when conditions are too bad. -Drive more carefully in areas with poorer road conditions -Own drivers must drive carefully to make up for errors from others -Select workers that are responsible drivers and make it a condition of employent.	-Use safety equipment in vehicle, stow cargo properly. -Have first aid kit available and the training to use it. -Insurance with vehicle replacement clause. -Refund on failed delivery along with an apology. -Inform the public in order to reduce loss to reputation.	10	11900	4		03.04.2016
8	Losses from unused flowers	Control	-Types of flowers -Amount of flowers being purchased -Seasonal changes	-Stay active with the predicitons on how much product will be needed to avoid losses.	-Use flowers that are about to go bad in decorations and for other uses where the longevity of the flowers is not hte issue.	10	52000	3		03.04.2016
9	Losses from improper storage of flowers	Control	-Cooler breaking down -Flowers being kept	-Strict routines on the refridgerations of the flowers and how long they can	-Use flowers that are about to go bad in decorations and for other uses where the longevity of the flowers is not hte	5	10500	4		04.04.2016

			outside cooler -Improper water or nutrition	be outside the cooler.	issue.					
10	Stocking up on interior design items that do not sell well enough	Control	-Misjudging the local market -Buying too large quantities	-Taking care to evaluate moving trends and coosing the ones that are likely to work in the region. -Have routines in place to estimate a maximum saturation for a certain product and not purchasing products past that point.	-Set up an internet store to market items that are attractive in the general market but is not selling well enough locally.	6	30800	4		04.04.2016
11	Breakage of materials and goods	Control	-Staff drop or otherwise break items -Customers break items	-organise the store so that there are no obvious places where someone would bump into goods. -Have proper work routines in place to avoid breaking goods during handling, packaging and wrapping.	-	5	6000	4		04.04.2016
12	Returned goods/delivery of wrong items	Control	-Wrong items delivered on an order -Customer unhappy with product -Product is broken	-Have QA routines in place to ensure that deliveries are the correct type and quality. -Make sure that customer buys the right product for their need. -Remove broken items from the store	-Give customers that return a product credit at the store if they are willing to take it or a similar value item. -Train staff to handle unahppy customers so that they will be made to feel well and so will improve the company's reputation.	4	5000	4		04.04.2016
13	Supplier fails to deliver when required	Control	-Supplier does not have items in stock -Communications break down preventing delivery	-Have a good relationship with the supplier so that if they have to make a priority call the company is morely to get the priority.	-Have arrangements with a secondary supplier to take over if the regular supplier fails. -Keep stock to be able to absorb a late delivery due to weather conditions	5	7000	4		04.04.2016
14	Improper storage of materials	Control	-Items stored in a way that their lifespan is shortened	-Have routines that ensure that all items in storage are stored appropriately.	-Check storage that the goods are stored properly to avoid damage. -Damaged goods may be sold at a discount depending on their condition	6	8000	4		04.04.2016

Table 4: Risk Register

5.2.3 Mitigation strategies and RTPs

The following are the plans for treating the threats and risk factors that have been identified and analysed in the BIA and Risk Analysis processes.

#:1	Process/Asset/Risk factor: Flooding hazard
Mitigation/Treatment plan: The person that is responsible for the readiness of the store will monitor the situation and when the flooding alert shows that flooding is imminent, the material in the store will be evacuated to the emergency storage location. When the flood water recedes the responsible person will organise the clean-up by mobilising the volunteers.	
Projected probability/impact reduction: This will reduce the impact of a flooding event by half the current impact.	Projected cost of implementation: It is estimated that the cost of these actions, will be about 5000 NOK in labour costs per time that it is activated.
Summary: This plan will not cost anything to have implemented outside the times that the events do happen. The cost of 5000 NOK is a small investment compared to the total cost of 100000 of an unmitigated event. The method will be cost effective as it will save an estimated 50000 NOK per time it is properly activated.	Date and sign: 07.04.2016 Jonas Andersen

Table 5: Mitigation Strategy 1 – Flooding hazard

#:2	Process/Asset/Risk factor: Key personnel
Mitigation/Treatment plan: There are very few people trained to operate the various processes of the company. For that reason there needs to be a way to spread out the risk of one person being out of action for some time. This will be done in two ways: 1: Cross training on all vital processes. This means that all the personnel will be able to perform all the tasks that need to be done. There will be a structured program to train and check the qualifications of each member of the organization. 2: Training a replacement that can step in to keep the basic processes going. There needs to be a person that can step in if the normal staff is unable to perform some or all the duties of the company. This person will be the currently inactive second owner that has agreed to be trained as a replacement worker.	

Projected probability/impact reduction: Making all the personnel capable of doing all the tasks will reduce the impact of any event that deprives the company of a person for a period. Training a replacement will reduce the impact further by making the company able to continue operating normally when normally it would have to close	Projected cost of implementation: The cross training is estimated to take roughly five hours and is estimated to cost approximately 2000 NOK. The training of the second owner as a replacement will come at no extra cost. The training will have to be repeated annually.
Summary: Training the staff and the second owner will make the company able to absorb the permanent or temporary loss of a key person more easily.	Date and sign: 07.04.2016 Jonas Andersen

Table 6: Mitigation Strategy 2 – Key Personnel

#:3	Process/Asset/Risk factor: Fire hazard
Mitigation/Treatment plan: In order to be in compliance with fire safety regulation there needs to be done an inspection yearly that the equipment and training of staff is good enough. The training program will be a one day training program in fire safety and first aid that is done by the local fire department. The program will be done yearly to keep the competence fresh. There will be a regular inspection of the electrical system in the store and electrical equipment will be maintained and replaced when needed. The update in equipment that will be done in 2016 is to set up a connected fire alarm that gives a signal to the apartment above the store. This will ensure that any fire outside opening hours will have a short reaction time. There will also be a purchase of foam cans to put out smaller fires. This in addition to the already provided extinguishers.	
Projected probability/impact reduction: The addition of foam cans will reduce the probability of a serious fire by having a handy tool to take out a starting small fire. The connected fire alarms will reduce the impact of a fire by increasing the probability of it being put out before it is allowed to flare up. The training along with the upgraded materials will reduce the probability and impact of fires greatly.	Projected cost of implementation: The training program will have an annual cost of 5000 NOK and the annual renewals of extinguishers will be an additional 500 NOK. The inspections of electrical systems will be an annual cost of 1000 NOK.
Summary: In direct cost benefit these measures will not be cost effective. However the benefits of the reputational boost and avoidance of negative reputational impacts from the better handling of events makes these measures economically viable. The concern with safety also dictates that fire safety measures need to be taken seriously to protect the staff and customers of the	Date and sign: 08.04.2016 Jonas Andersen

company.	

Table 7: Mitigation Strategy 3 – Fire hazard

#:4	Process/Asset/Risk factor: Weather conditions
Mitigation/Treatment plan: The shifting weather conditions are one of the main sources of lost revenue. There is not much to be done about the weather, but there are ways to change ones behaviour in reaction to it. In order to mitigate the losses from the days with off average weather the costs of these days will need to be reduced. When it comes to the general opening times of the store not much can be done since the opening times need to be followed to have predictability. How the time is spent on these days can however be changed and so the work tasks like organizing the storage and budgeting should be saved to these days to make the use of worktime more efficient. One of the main sources of losses from these days are the fresh flowers that reach their expiry time before being sold due to off average weather keeping people from shopping. In order to avoid this the amount of flowers being purchased will be somewhat adjusted for the weather projections. If the next two days show reported off average days then the purchase of flowers will be reduced by 30 %. This will reduce losses and also keep the store properly stocked if the weather turns out otherwise than reported.	
Projected probability/impact reduction: The flexible flower purchasing will reduce the rate of losses by a projected 20 percent.	Projected cost of implementation: The cost of reprioritizing the work load and purchasing will come at no extra cost.
Summary: The adjustment of workloads and purchasing will be cost effectinve measures that will improve the profitability of the days with off average weather.	Date and sign: 08.04.2016 Jonas Andersen

Table 8: Mitigation Strategy 4 – Weather conditions

#:5	Process/Asset/Risk factor: Violence to staff or customers
Mitigation/Treatment plan: In order to avoid violent incidents it is important to be able to handle incidents in a way that minimizes the risk of a violent outcome. In order to do this the workers will be given training in dealing with aggressive persons.	
Projected probability/impact reduction: The probability of an incident with an aggressive person escalates into a violent event will be greatly reduced.	Projected cost of implementation: The course will cost approximately 6000 NOK for all staff to complete it.
Summary: The course will not give a direct cost benefit win but will significantly reduce the vulnerability of the company. The added benefit is to make the workers more confident in dealing with aggressive persons	Date and sign: 08.04.2016

and potential losses from aggravated customers will be reduced.	

Table 9: Mitigation Strategy 5 – Violence to staff or customers

#:6	Process/Asset/Risk factor: Storage of materials
Mitigation/Treatment plan: Improper storage of materials can greatly reduce their expected lifespan and may result in goods having to be thrown away or that they are returned with the added impact of an unhappy customer. The following routines will be implemented to ensure that these losses are reduced to an absolute minimum: 1. The person closing the shop will check that the flowers are in the cooler and that the cooler is operating properly. 2. The person responsible for the readiness of the shop will inspect and organize as needed the external storage space.	
Projected probability/impact reduction: These routines will reduce the impact of improper storage by an estimated 50% which is an annual of 4000 NOK.	Projected cost of implementation: There will be no extra cost for implementing these routines.
Summary: The implementation of stricter routines on storage will reduce the amount of materials that are lost during the year.	Date and sign: 08.04.2016

Table 10: Mitigation Strategy 6 – Storage of materials

#:7	Process/Asset/Risk factor: Designate a person to be responsible for readiness
Mitigation/Treatment plan: In order for there to be a real ability for the company to react to incidents there needs to be a designated person to be responsible for reacting to incidents outside of opening hours. Since the owners or manager may be away at some times this responsibility will need to be delegated to a trusted member of staff. This person will be given authority to invocate crisis plans and recovery plans. The manager is responsible for there always being a responsible person that is located in the vicinity of the store and is available to react to incidents.	
Projected probability/impact reduction: Having a person available that can react to incidents as they occur will reduce the reaction time greatly in any hazard event.	Projected cost of implementation: In order to operate this service there will be a cost of 500 to 3000 per incident depending on the duration and timing.
Summary: Having this kind of readiness will make the crisis management much more effective as there will always be someone ready to react if something was to happen.	Date and sign: 08.04.2016

Table 11: Mitigation Strategy 7 – Designate a person to be responsible for readiness

#:8	Process/Asset/Risk factor: Readymade messages

Mitigation/Treatment plan: In order to make the communications to the public more efficient during a crisis there will need to be made a set of ready made messages that can be taken out and sent with some editing as an initial message related to a crisis. These messages will need to be simple statements that let the person handling the crisis be able to quickly make a statement about what is going on so that the company takes control of the communications immediately.	
Projected probability/impact reduction: This will reduce the reputation impact of crisis events by some degree as the company can communicate earlier what is going on.	Projected cost of implementation: No additional cost
Summary: The implementation of a set of readymade messages will help the company communicate more easily when a crisis is underway. More careful communications will need to be following such a message but as long as the company takes initiative the time bought will give time to find the facts before a more comprehensive message is sent.	Date and sign: 09.04.2016

Table 12: Mitigation Strategy 8 – Readymade messages

#:9	Process/Asset/Risk factor: Water supply
Mitigation/Treatment plan: In order to be able to continue operations when the water supply is cut off there needs to be a way to get water to do the washing and other tasks that are needed to maintain and sell the fresh flowers and decorations. This will be done by having a mobile water tank that can be filled and moved to the store.	
Projected probability/impact reduction: The addition of a tank will make the store capable of operating even though the water supply is cut off.	Projected cost of implementation: A tank will cost 50 NOK
Summary: This is a small investment that can potentially save thousands if the water is cut off on a busy day.	Date and sign: 11.04.2016

Table 13: Mitigation Strategy 9 – Water supply

5.3 Results of the process

After going through the process there was conducted a last interview with the owner and manager of the company in order to sum up the process. The feedback from the company was positive with some reservations. The main positive result of the process was to improve the companies awareness of how the different processes work and create interdependencies that in turn create vulnerabilities. In addition to this the identifications of vulnerabilities and fac-

tors that were not in compliance with regulations has allowed the company to take action to improve this.

The negative feedback was that the system still was complicated and that it would require regular follow ups to continue the process. This feedback is understandable and the system will either need to be scaled down, or the management will need to be trained further if the company is to maintain it on their own without any support. Scaling the system down further may not be a useful route however since the main quality in the system is the analyses that underpin the different steps in the process. This part is still a work in progress and the plan is to re-do the process during the first quarter of 2017.

The conclusion from this is then that while the system needs further development an added effort into training the users in utilising the different aspects of it is probably the most cost effective solution.

6 Conclusions

In the introduction to this thesis, it was written that the company is in a vulnerable state. As the company gave guidelines with the needs and limitations that were identified in the interviewing process, the need for a severely compressed system was identified. The requirement would have to be that for the process to be cost effective it would have to be streamlined with as few components as possible. At the same time there was the need for a comprehensive system that would meet both the risk management and business continuity management needs of the company. This process became Business Continuity Risk Management.

To get a relevant result from the process it was important to get the owner and manager involved in working through the system. The actual effect of running the process created in addition to awareness and knowledge, a measurable effect in the projected profitability of the company. The mitigation actions that are taken to improve the losses in the operations of the company include such things as improving the routines for storing goods, and also the possibility of a flexible purchasing policy that can reduce losses due to observed fluctuations in customer behaviour.

The planned mitigation actions that are not directly profitable are still assessed as being an improvement and a necessary cost. The benefits of these are more for the sake of safety, reputation and continuity. Fire safety is such an example where the probability of occurrence is so low that even though the impact can be devastating the cost of fire safety equipment and training is not cost effective in a strictly financial way. There is still a need for this though, for the sake of both compliance with official standards and the credibility of the

company, as well as for the safety of the employees, customers and members of the community.

Another result of doing this process is the development of another method to calculate ALE. The Annual Loss Expectancy Calculator was created to enable this small company to calculate ALE in a simple and precise way. The advantage over formula based methods is that it is easy to use and does not require a lot of knowledge of the theory behind it to be useful and it is at the same time more precise.

After going through this process the company is more aware of its risks and vulnerabilities, and it has now enabled the company to prioritize how to work on mitigating risks and vulnerabilities. The result is that the company is aware of its business environment and knows how to handle risk and opportunities. This increases the company's resilience and achieve the desired development, and minimizes the effect of coincidence.

The system that was made filled the needs of the company. There is however, a need to make tools that simplify the spreadsheets and documents that now form the database structure as well as continue the development of the processes themselves. The process is ongoing and the second revelation of the process wheel is set to be done during the first quarter of 2017. The resuts of the strategies that will be collected then will give a firmer indication to the actual effect the process has had for the company.

References

Al Hour, Abdullah. 2012. Business Continuity Management: Choosing to Survive. <https://laurea.finna.fi/Record/laurus.82565> Accessed 28.02.2016

Aven, Terje. 2015. Risikostyring. 2. edition, Universitetsforlaget, Oslo.

Aven, Terje. 2006. Risk Analysis : Assessing Uncertainties Beyond Expected Values and Probabilities. Wiley. <http://site.ebrary.com.nelli.laurea.fi/lib/laurea/reader.action?docID=10297957#> Accessed 20.12.2015

Brinkmann, Svend. 2013. Qualitative interviewing. Oxford university press. <https://laurea.finna.fi/Record/laurus.82592>

Broder, James. 2006. Risk Analysis and the Security Survey. Butterworth-Heinemann. <http://site.ebrary.com.nelli.laurea.fi/lib/laurea/reader.action?docID=10186101> Accessed 22.01.2016

Elliott, Dominic; Swartz, Ethné; Herbane, Brahim. 2010. Business Continuity Management, Second Edition : A Crisis Management Approach. <https://laurea.finna.fi/Record/laurus.79437> Accessed 01.03.2016

Johnsen, Lars G. W. 2005. Balansert Risikostyring: Praktisk metodebok for virksomheter. 1. edition, Gyldendal Norsk Forlag, Oslo.

Hopkin, Paul. 2010. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page. <http://lib.myilibrary.com.nelli.laurea.fi/Open.aspx?id=293893> Accessed 20.12.2015

Hopkin, Paul. 2012. Fundamentals of risk management: understanding, evaluating and implementing effective risk management. London, Kogan Page

Merna, Tony, Al-Thani, Faisal F. 2008. Corporate Risk Management (2nd Edition). Wiley. <http://site.ebrary.com.nelli.laurea.fi/lib/laurea/detail.action?docID=10300854>

Trost, Jan. 1993. Kvalitativa intervjuer. Studentlitteratur, Lund.

Rittinghouse J. W., Ransome J. F. 2005. Business continuity and Disaster Recovery for infosec managers. Elsevier. <https://laurea.finna.fi/Record/laurus.82566>

Rugg, Gordon. 2008. Using Statistics : A Gentle Introduction. Open University Press. <https://laurea.finna.fi/Record/laurus.78889> Accessed 10.01.2016

Saunders, Mark N.K., Thornhill, Adrian. 2008., Research Methods for Business Students. Pearson Education Limited. <https://laurea.finna.fi/Record/laurus.71906> 01.01.2016

Sterling, Stuart. 2012. Business Continuity For Dummies. Chichester : Wiley, 2012 <https://laurea.finna.fi/Record/laurus.80486> Accessed 10.03.2016

Vacca, John R. 2010. Managing Information Security. Elsevier Science. <https://laurea.finna.fi/Record/laurus.86400> Accessed 10.03.2016

Watters, J. 2014. Disaster Recovery, Crisis Response, and Business Continuity : A Management Desk Reference. Apress. <https://laurea.finna.fi/Record/laurus.86372 >

Hotchkiss, Stuart. 2010. Business Continuity Management: In Practice. <https://laurea.finna.fi/Record/laurus.81654> Accessed 01.03.2016

Journals:

Kallman, James. Identifying Risk. Risk Management 54.9 (Sep 2007): 58-59 <http://search.proquest.com.nelli.laurea.fi/docview/227006224?accountid=12003> Accessed 20.01.2016

Online resources:

Coombs, Timothy W. 2007. Crisis Management and Communications. <http://www.instituteforpr.org/crisis-management-and-communications/> Accessed 12.03.2016

Dictionary.com <http://dictionary.reference.com> Accessed 18.12.2015

Piscopo, Mark. 2015. Risk register. <http://www.projectmanagementdocs.com/project-planning-templates/risk-register.html#axzz3y45iAd1k> Accessed 15.01.2015

Ready.gov. 2016. Crisis Communications Plan. <https://www.ready.gov/business/implementation/crisis> Accessed 12.03.2015

Wyllie, Gordon. 2016. Risk management with Gordon Wyllie. <http://www.mindgenius.com/Resources/Documents/Process-Improvement/Risk-Management-2.aspx> Accessed 24.01.2016

UCDAVIES. 2011. Guide to Writing and Maintaining Campuswide Administrative Policy <http://manuals.ucdavis.edu/resources/GuidetoWritingPolicy.pdf> Accessed 02.03.2016

Mastering VBA for office 2010. 2010. <http://site.ebrary.com.nelli.laurea.fi/lib/laurea/detail.action?docID=10412498&p00=visual+basic+2010> Accessed 10.01.2016

Directorate for Civil Protection and Emergency Preparedness (DSB). 2011. Kjennetegn og utviklingstrekk ved næringsbranner 1986–2009. <http://dsb.no/Global/Brannvern/Dokumenter/Rapport%20naeringsbranner.pdf> Accessed 20.12.2015

Figures

Tables

Appendixes

Appendix 1: Risk Analysis

Analysis of #1: Flooding hazard

The area where the store is located is a low-lying area next to a lake that has tributaries from three different valleys. This makes it especially vulnerable to flooding as the area that drains into the lake is large and stretches up to the mountains.

The picture on the right is a cut out of the flood map for the village where the store is located. with buildings that are exposed in orange. The teal areas are normal waterways and the blue areas show different flood risk levels. The blue shades represent the levels of flooding at annual, 10 year, 50 year and 200 year floods. The location of the store is shown in the red circle.

In December 2015 during the extreme weather system “synne” the conditions were met to create a 200 year flood (VG 2015). In the weeks before the flood there had been heavy snowfall higher up in the mountains, and when “synne” brought warm temperatures and heavy rainfall into the mountains the snow melted.

The owners of the company were aware of the high flooding risk, but the attitude among the people of the village was that the water would not go that high. Unfortunately, the owners chose not to heed the warning signs soon enough. The result of this was that the evacuation of material from the store began too late and much of the stock was damaged by the floodwater.

The challenge with phenomenon that only happen at large intervals is that it is difficult to be prepared for it when it happens. This is shown clearly in the attitude of the people in the village. In retrospect, the signs were clear that a serious flood was coming, but the previous flood was far enough in the past that the people making the decisions did not react appropriately.

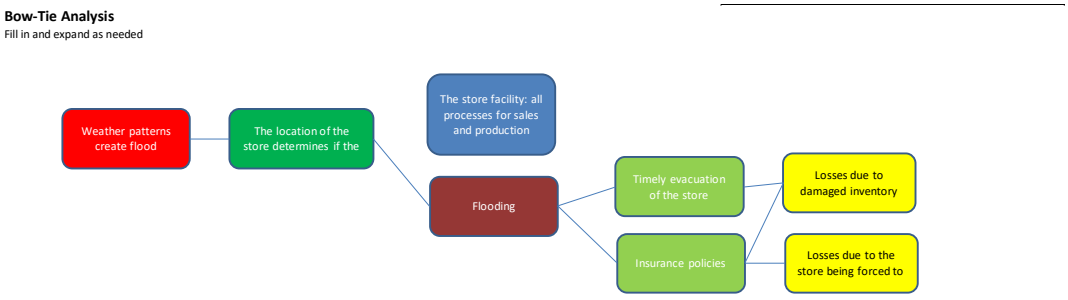
The flood of 2015 was a 200-year flood. That means that the probability that the conditions that need to come into place to achieve a certain water level equates to a 200-year average interval between the events. In the particular case of the company’s location, a 200-year flood put the water level high enough to do significant damage to the building and its interior.

200-year floods are by nature quite rare, but the slightly less severe 50-year floods also have the potential to do significant damage to the store. This implies that the risk of flooding is and will continue to be a significant threat to the company in the future.

When the flood happened, the company had insurance for losses but not for lost revenue from the store being forced to close. This has caused losses in addition to the actual damages. The table on the right sums up the losses incurred as a result of the flood.

A 200-year flood as it happened in 2015 is likely to have a similar impact the next time it occurs. Flooding such as was experienced in 2015 is rare, and the consequences are manageable with the appropriate safeguards. A large part of the losses from this flood was due to the delayed reaction in evacuating the shop. If the evacuation had started when the flood warning was issued the losses due to damaged stock would be far less. The other factor that played a large part in increasing the losses was the lack of an insurance to cover losses from lost revenue the time when the shop was forced to close.

Factor	Cost
The shop closed for three days during the busiest time of the year. This caused losses due to lost revenue.	Kr 20000
Some of the stock was only slightly affected by the water. Ceramics and similar robust items for the most part only had their labels damaged but they could not be sold at the regular price and was sold at a 70% discount.	Kr 20000
Another part of the stock was damaged to the point where it had to be thrown away. This was mitigated by insurance and the cost values is the losses including the insurance payments.	Kr 20000
In the aftermath of the flood the shop has had to be closed for some periods in order to do renovation work. This has caused further lost revenue.	Kr 40000
Total losses:	Kr 100000



What threats cause this risk event?

-Weather patterns

What Safeguards can reduce the probability of ocurrence?

-Relocating the store to an area less affected by flooding

What safeguards can reduce the impact of the risk?

-A timely evacuation of the store where the majority of the stock is preserved. -Insurance policy for damages. -Insurance policy for lost revenue.

Analysis:

The event of a flood is a natural hazard and so it is not possible to prevent it from occurring. It is however important to be able and ready to handle the consequences of the event. It is possible to use barriers to keep floodwater out of small areas, but this is costly and not within the means of the company. Due to the area being as open as it is it is not likely that the municipality will spend resources on flood barriers. This means that the way to prevent a flooding event is to re-locate to an area that the floodwater will not reach.

In order to mitigate the consequences of a flooding event there are ways to lessen the impact of the event. The main mitigation action is insurance policies that reduce the losses from direct damage and lost revenue from the store being forced to close. The relevant action to reduce the level of damages is a timely identification that a flooding event is happening and a strong reaction to evacuate the store.

ALE analysis:

The numbers for a flooding event can be calculated with a fair amount of accuracy due to the wealth of fresh information from the flood of December 2015.

The impact calculation is done on the basis of the numbers from the 2015 flood. This number will then represent a course of action similar to the one that was taken at the last incident. The 2015 event, which was a 200-year flood, will have a higher water table than a 50-year flood. The costs of a 50-year flood will be somewhat lower since the consequences are more manageable.

When calculating the ALE for the flooding hazard, the 200-year has a known impact of 100000, while the 50-year flood is likely to be somewhat lower. The impact of a 50-year flood is calculated with a lower amount of damage to stock. The time that the store would need to be closed is likely to be similar. On the basis of this the impact value is set to 75000 NOK. Using the Annual Loss Expectancy Calculator the ALE value for a 200-year flood is 500 NOK

while a 50-year flood is 1500. The Annual loss expectancy from the flooding hazard is 2000 NOK.

Risk score:

impact	Probability	Score
4	1	4

Annual Loss Expectancy:
What factors have what ALE? (Using the ALE Calculator)

200 year flood:	ALE =	500	NOK
50 year flood:	ALE =	1500	NOK
	ALE sum =	2000	NOK

Certainty level:
The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

1	The prerequisites for the conclusions are seen as being very reasonable.
1	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 4

Conclusion:

A flooding event can be disastrous and is a very high impact event. The frequency of seri-ousfloods are however low. This gives the flooding hazard a relatively low risk score and ALE rating.

There is a strong foundation in statistics behind the conclusions in this analysis and the result is a strong confidence in the information that is the basis of the analysis.

Analysis of #2: Fire Hazard

Fire is an ever-present threat that can have potentially fatal consequences. Fire safety is a basic safety and security issue where the probability of occurrence and of significant damage can be reduced significantly by alarm systems and equipment for extinguishing fires.

There was a reduction of commercial fires in Norway during the period 1986-2009 (DSB 2011, 17). The risk of a fire occurring is now reduced. With modern building materials and warning systems the chance of a fire doing crippling damage is reduced as well. Fire is still however a significant risk factor due to the potential to do massive damage to a business.

The graph on the right illustrates the development of commercial fires in Norway during the period of 1986-2009. The graph clearly shows a significant reduction in fires since the start of the measurement in 1986. With the rate of fires peaking in 1997, 12 years later in 2009 saw a clear drop where the rate fell below 700 fires per year.

In the period of 1986 – 2009 there were on average 2,36 fires per year per 1000 companies involved in retail. This is higher than the national average of 1,96 per year per 1000 companies in all sectors. (DSB 2011, 95)

The municipality where the company is located experienced 11 fires in the period of 1986 – 2009. This statistic is presented with the population as the baseline, so the amount of fires in commercial buildings measured per resident in the municipality is 452,1 for every 100.000 residents. The national average is 504,5 per 100.000 residents. (DSB 2011, 97)

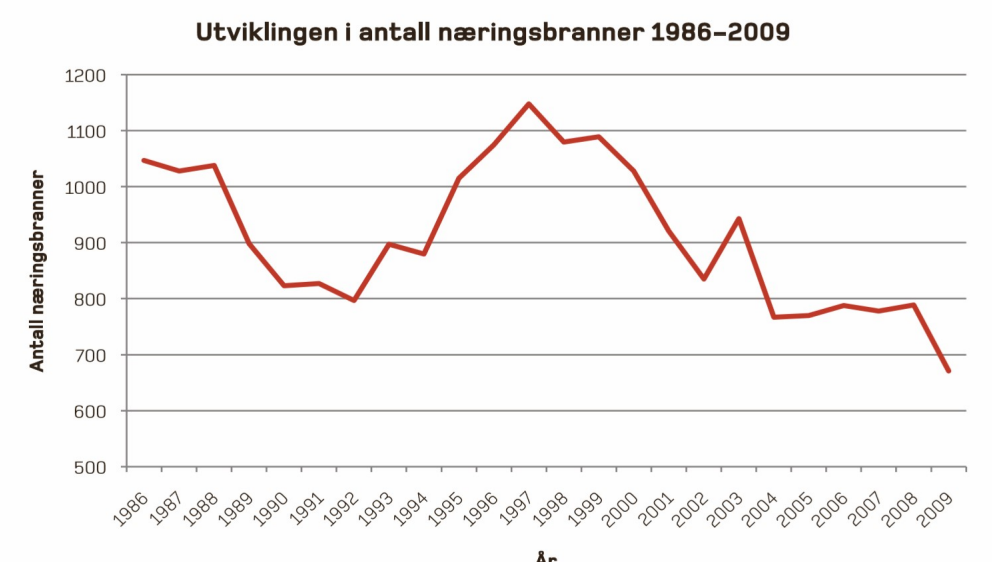
The area where the company is located has a higher rate of commercial fires than the national average. This is possibly due to the high proportion of agriculture operations relative to other businesses. The average for agriculture was 2,15 fires per year per 1000 companies. With this in mind the basis for the data for the municipality is too small to give it any statistical value. The national data does point to an average amount of fires for retail companies that is a significant 20% higher than the national average. This indicates that the risk for the company is higher and that extra care should be taken when addressing fire safety.

According to the Directorate for Civil Protection and Emergency Preparedness (DSB) (2011, 93) investigation into commercial fires the causes of commercial fires had the following distribution:

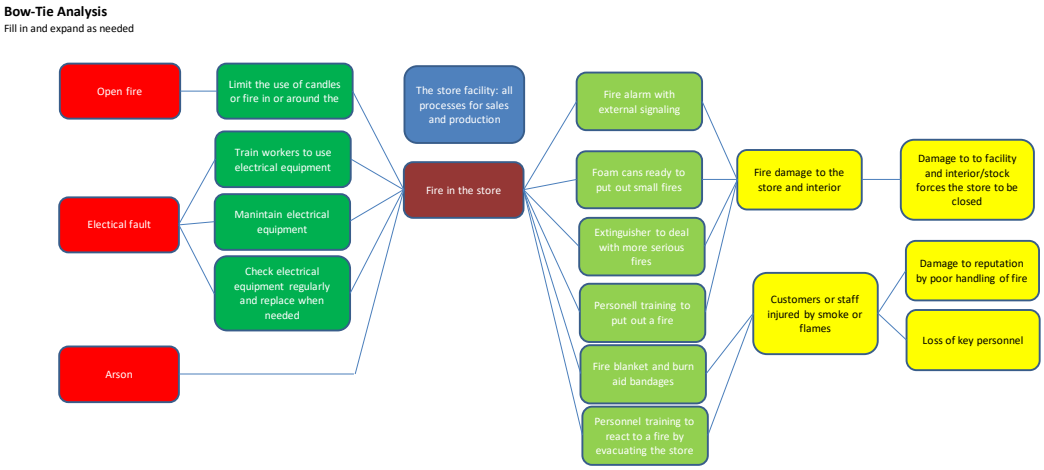
- Unknown 23 %
- Electronics, technical fault 18 %,
- Open fire, Smoking 14 %
- Arson 14 %
- Self-ignited arson 9 %
- Wrong use of electrical equipment 6 %
- Open fire – Welding/soldering 5 %
- Open fire – candles 5 %
- Open fire – embers from a fireplace 5 %.

During the investigation it was found that in one out of ten cases there were missing fire inspections and eight out of ten had below standard fire safety in place before the fire

occurred (DSB 2011, 93). This indicates that a large proportion of commercial fires are preventable and thus a strategy to limit the main causes of fire can be put into place with good effect.



The development in the number of commercial fires in Norway in the period 1986-2009. (DSB 2011, 17)



What threats cause this risk event?

-Open fire
-Electrical faults
-Arson

What Safeguards can reduce the probability of ocurrence?

-Limit the use of candles or fire in or around the store.
-Train workers to use electrical equipment properly to prevent the

equipment from bein used in potentially hazardous ways.
-Maintain electrical equipment to prevent equipment failure
-Check electrical equipment regularly and replace them when it is nessecary in order to avoid faults due to outdated equipment.

What safeguards can reduce the impact of the risk?

-Fire alarm with external signaling to reduce the reaction time of firefighters and others to put out a fire as early as possible.
-Foam cans readlily available to put out fires before they have time to catch on. Foam cans also do not damage the interior with corrosive material and so the cost of deployment is much lower than powder based extinguishers.
-Powder based extinguisher to deal with blazes that cannot be contained with foam.
-The personnel that work in the store must be trained in the use of the firefighting equipment.
-There must be a plan for evacuating the store in case of a fire to avoid personnel injuries.

Analysis:

Fires are one of the most common hazards for a company. The Compnay is no exeption and is at risk of several threat sources that a fire can come from. The probability of a fire can be greatly influenced by the amounts of potential sources of fire that are in the store. The impact of a fire can likewise be mitigated by the rapid alerting of authorities and handling a fire when it starts.

A fire can have large consequences for a company and can lead to the total loss of the companies assets that are located at the store and adjacent storage. such a loss will also mean the cessation of any operations for the forseeable future. This means that even though there is a relatively low probability the impact level is very high.

ALE analysis:

If a fire does occur and gets out of hand the consequences will be severe. At any given time there are goods valued at approximately 200000 NOK in the store. There are also materials and equipment in the store and adjacent storage valued at approximately 100000 NOK. In addition there will be that the facilities will be rendered unusable for an extended period. The cost of relocating and lost revenue is estimated at 200000 NOK. The interval of such a fire is estimated at 500 years from the statistics of commercial fires.

Risk score:

impact	Probability	Score
5	1	5

Annual Loss Expectancy:
What factors have what ALE? (Using the ALE Calculator)
Serious fire: ALE = 1000 NOK

ALE sum = 1000 NOK

Certainty level:
The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

1	The prerequisites for the conclusions are seen as being very reasonable.
1	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 4

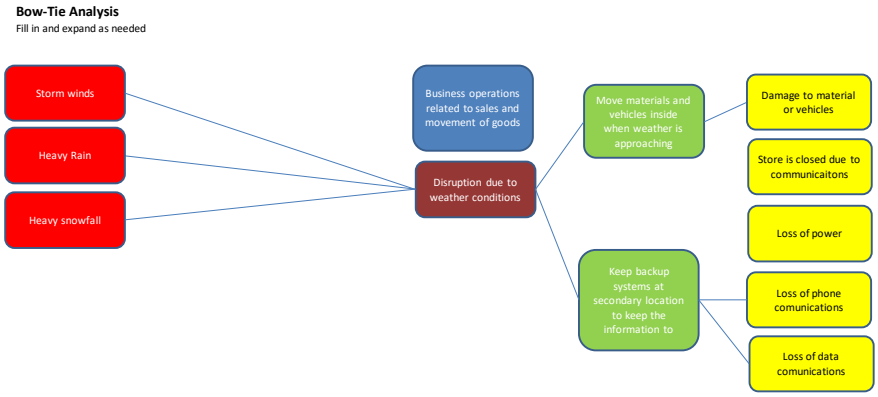
Conclusion:
A fire can destroy the company if its is allowed to take hold. Total loss due to a fire is likely to be the end of a company if the insurance of the company is not good enough. However the actual probability of having a fire is very low so the needs for safeguards should not be overstated.

There needs to be preparations in place to minimize the risk of a fire and to handle it if it occurs. If the company is seen as incompetent in preparing for or handling a fire that may be damaging to the reputation of the company.

Analysis of #3: Extreme Weather hazard
The weather conditions affect the business in two ways: The conditions of the infrastructure that support the business and allow customers to reach it and the way that the weather affects the willingness of customers to og shopping. The Weather Hazard is meant as the way that weather can affect the ability of the company to operate.

The different weather conditions of heavy snowfall, storms and heavy rainfall can disrupt business operations in different ways. the event of flooding that is heavy enough to flood the store is considered a separate event due to its special conditions and rarity. Snowfall that is

heavy enough can cut off communicaitons and thus prevent business opertaions. The same can happen with storms and heavy rainfall. There can also be longer lasting effects from damages to infrastructure.



What threats cause this risk event?

-Stromy winds
-Heavy Rain
-Heavy snowfall

What Safeguards can reduce the probability of ocurrence?

-

What safeguards can reduce the impact of the risk?

-Move materials and vehicles inside to protect them from the weather
-Keep backup systems at secondary location to keep the information to stakeholders going

Analysis:

The threat of disruptions from the weather is a threat in all parts of the year, but is most potent in the fall through spring due to more frequent and more serious storms. There is not much to do to mitigate the impact of the weather on business operations other than to protect the companies assets from exposure and to keep communications lines with stakeholders open as far as possible to inform of the status of the store and when it will re-open. Both the probability and impact of weather hazards is in the medium range area.

ALE analysis:

Weather conditions that force the store to close happen two days per year based on the statisics of the company. The loss of one days revenue is estimated at 7500 NOK. In extreme weather events, sometimes there are damages to the front of the store and there is a risk to vehicles as well. A storm that does damage to the storefront is estimated to be an annual

event with an impact of 2000 NOK. Repairs to vehicles is estimated to have an interval of ten years with an impact of 5000 NOK.

Risk score:

impact	Probability	Score
3	3	9

Annual Loss Expectancy:
What factors have what ALE? (Using the ALE Calculator)

Store is closed:	ALE =	15200	NOK
Damages to storefront:	ALE =	2000	NOK
Damages to vehicles	ALE =	500	NOK
	ALE sum =	17700	NOK

Certainty level:
The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

1	The prerequisites for the conclusions are seen as being very reasonable.
0	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

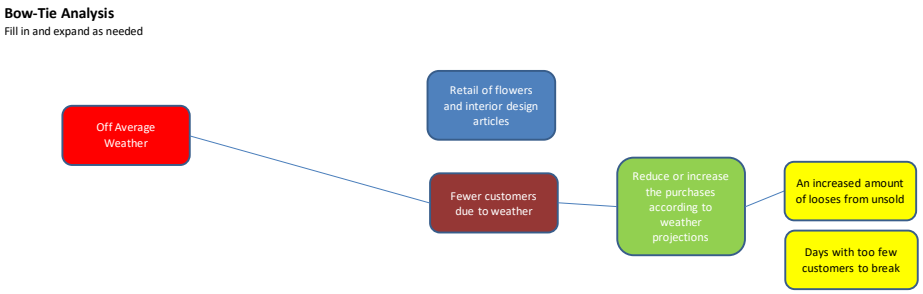
Certainty = 3

Conclusion:
The risk of weather conditions that disrupt business operations are unavoidable. The consequences can however be mitigated somewhat by good communications and a proper reaction to the events when they occur.

Analysis of #4: Weather Conditions
The wather conditions affect the behavious of the customers of the company. The data that has been gathered by the company clearly shows that there is less business when the weather is below or above average. This behaviour is believed to be the result of the climate conditions in the area where the store is operating. The weather in the area is mostly cool and gray with many rainy days and a near constant wind. When there is a sunny day, people want to take advantage of it and when it is too bad they want to stay inside.

This pattern of behaviour affects the retail part of the company where the number of customers drops dramatically in off average weather. The main consequence of this is for the fresh flower that are projected to be sold but will not because of a sudden drop in business.

This can lead to significant losses when the purchasing is not able to take the weather projections into account.



What threats cause this risk event?

-Off Average weather

What Safeguards can reduce the probability of ocurrence?

-

What safeguards can reduce the impact of the risk?

-Reducing or increasing purchases of fresh flowers according to weather projections in a more dynamic purchasing strategy may be an option.

Analysis:

The weather shifts daily and the customers behaviour changes with it. In order to reduce losses and alos increase the odds ofsucceding with certain purchases of fresh flowers the weather needs to be taken into consideration. The impact of each event is small but the probability is very high. This makes weather related losses a medium risk.

ALE analysis:

Days with Off Average weather happen on average once a week. When they do happen the impact of the reduced sales directly impact an estimated 3000 NOK and the losses from un-sold fresh flowers are around 1000 NOK.

Risk score:

impact	Probability	Score
2	5	10

Annual Loss Expectancy:

What factors have what ALE? (Using the ALE Calculator)

Reduced sales D.I.: ALE = 156000 NOK

Unsold flowers wasted: ALE = 52000 NOK

ALE sum = 208000 NOK

Certainty level:
The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

1	The prerequisites for the conclusions are seen as being very reasonable.
1	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 4

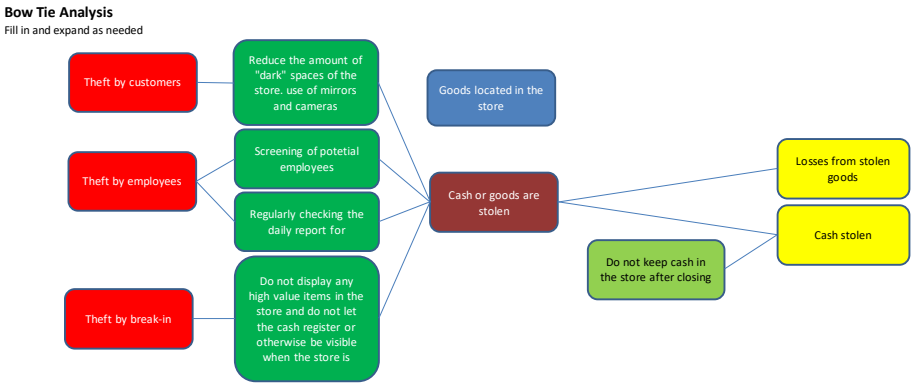
Conclusion:

Weather conditions are one of the major causes of lost revenue and greately contributes to the sum of looses from unused fresh flowers. If arrangements for a more dynamic purchasing strategy can be found then there is the potential for large savings.

Analysis of #5: Theft Analysis

Theft is a common problem for any business and especially so for a company operating in the retail sector. The format of selling where there are goods on display will lead to some amount of it being stolen. Another way that theft can be done is if an employee of the comany is taking goods or money from the company. In a small company with few employees this form of theft is less likely.

Another way that theft can occur is by someone braking into the store outside of opening hours and then stealing goods or money that is found in the store.



What threats cause this risk event?

-Theft by customers
-Theft by employees
-Theft by break-in

What Safeguards can reduce the probability of ocurrence?

-Reduce the amount of "dark" space in the store by installing mirrors or cameras where applicable.
-Screening potential employees in order to weed out potential un-faithful workers.
-Regularly checking hte daily report fro anomailes both to show that it is being done and to see if the transactions add up to what has been sold.
-Do not display and high values items in the store and do not let the cash register or otherwise be visible when the store is closed.

What safeguards can reduce the impact of the risk?

-Do not store any cash in the store after closing.

Analysis:

The risk of theft is a serious threat that shoud be given attention to reduce the probability and impact of it. In the store as is there have been no incidents of someone bieng caught of stealing, but there are strong indications from the number of items that go missing that stealing does occur. The frequancy of this is high but the impact for each event is very low since the smaller items that are more likely to be stolen are also for the most part less valuable. The chance of a break-in occuring is low considering the low value to size and weight ratio of the goods in the store.

ALE analysis:

Theft in the store probably happens about once every other day. The amount stolen will be small and the average is calculated to be about 50 NOK. A break- in will likely lead to very little theft and will probably be more a case of vandalism.

Risk score:

impact	Probability	Score
1	5	5

Annual Loss Expectancy:

What factors have what ALE? (Using the ALE Calculator)

Theft while open:	ALE =	9100	NOK
Theft from break-in:	ALE =	500	NOK

ALE sum = 9600 NOK

Certainty level:
The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

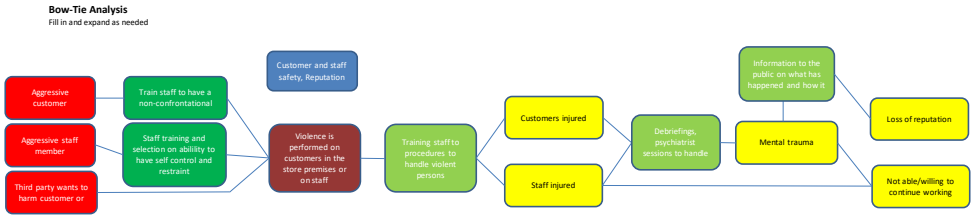
1	The prerequisites for the conclusions are seen as being very reasonable.
0	Data/information is available in large quantities.
0	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 2

Theft will continue to be a problem for any retailer. The probability of theft occurring can however be greately reduced by applying some simple mitigation strategies.

Analysis of #6: Violence to staff or customers

The safety of staff and the customers that come to visit the store is a very important concern for the company. There have not been any threatening incidents at the store as of yet, it cannot however be ruled out that a violent event may happen in the future. It is not unthinkable that something will occur that will end up placing the staff and or customers at risk of being physically hurt, and the mental trauma of such an event can be severe. The reprecussions of such an event can be large, not just for the direct impact of the event, but for the company's reputation.



What threats cause this risk event?

-Aggressive customer
-Aggressive staff member
-Third party wants to harm cstomer or staff member

What Safeguards can reduce the probability of ocurrence?

-Traing staff to have a non confrontaitonal attitude when dealing with unhappy customers.

-Training and selecting staff on ability to have self control and re-straint in the face of a confrontaitonal customer.

What safeguards can reduce the impact of the risk?

-Training staff to procedures to handle violent persons -Debriefings, psychiatrist sessions to handle trauma. -Information to the public to communicate control and show that it is safe.

Analysis:

Since there is no recorded incident and no indication that it will occur the probability of a violent incident is very small. The potential impact is however very high due to the potential injuries to customers and staff and the loss of reputations such an incident would accrue.

ALE analysis:

There is not enough data to make a ALE projection.

Risk score:

impact	Probability	Score
4	2	8

Annual Loss Expectancy:

What factors have what ALE? (Using the ALE Calculator)

factor 1: ALE = xx NOK

factor 2: ALE = xx NOK

ALE sum = xxxx NOK

Certainty level:

The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

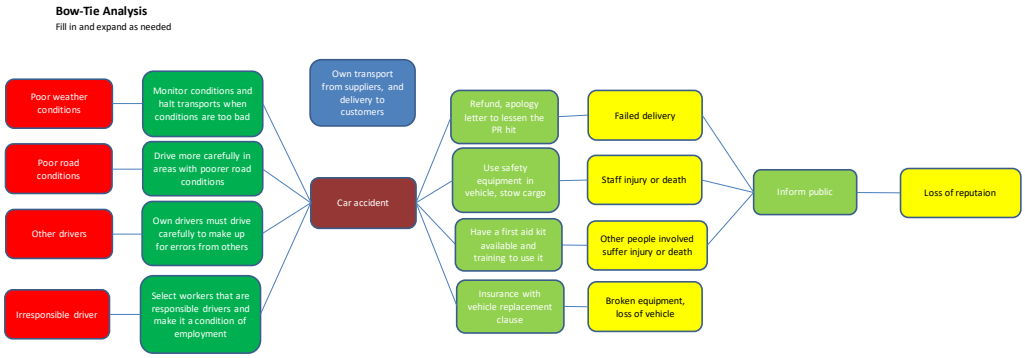
1	The prerequisites for the conclusions are seen as being very reasonable.
1	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 4

Analysis of #7: Car Accident

As a part of the companies operations there is a large amount to driving being done by the company. The driving is done to pick up materials from suppliers and to transport finished products to customers in the region. Many of the roads being used are narrow and in some

places in poor repair. Combined with poor weather conditions this can lead to dangerous situations.



What threats cause this risk event?

-Poor weather conditions
-Poor road conditions
-Other drivers
-Irresponsible driver

What Safeguards can reduce the probability of ocurrence?

-Monitor conditions and halt transports when conditions are too bad.
-Drive more carefully in areas with poorer road conditions
-Own drivers must drive carefully to make up for errors from others
-Select workers that are responsible drivers and make it a condition of employent.

What safeguards can reduce the impact of the risk?

-Use safety equipment in vehicle, stow cargo properly.
-Have first aid kit available and the training to use it.
-Insurance with vehicle replacement clause.
-Refund on failed elivery along iwth an apology.
-Inform the public in order to reduce loss to reputation.

Analysis:

A car ccident can have large consequences for a small business. If the vehicle used for transport for the company is taken out of action it can be costly to replace and the transports that are not done will cause losses. The main danger is however that since the company has so few people available that can do the work. If one of the people working at the company is injured, all the processes of the company is at risk of being put out of action. There is also of course the risk of harming other people in an accident. If such an event is handled poorly the fallout on hte company's reputation can be severe.

ALE analysis:

The impact of a traffic accident can be a wide range, but for this exercise the esti-

mate is made for an acident that will cause the company to be without a vehicle for approximately 2 days since that is the time that a replacement can be reliably expected to be available with the current arrangements. Also the accident in the example will put one staff memeber out of action for two weeks. The probability of such an incident is fairly low and the interval was set at 5 years for that reason. The impact of the incident however was set at 20000 NOK for the vehicle related issues and an estimation that the store would have to close for 5 days during the period which would lead to an estimated loss of 37500 NOK. The fact that additional transports would not be available for two days due to the unavailability of a vehicle the impact of that would be an estimated 2000 NOK

Risk score:

impact	Probability	Score
5	2	10

Annual Loss Expectancy:

What factors have what ALE? (Using the ALE Calculator)

Vehicle unavailable:	ALE =	4000	NOK
Store closed for 5 days:	ALE =	7500	NOK
No transport 2 days:	ALE =	400	NOK
	ALE sum =	11900	NOK

Certainty level:

The following statements each give a certainty rating of 1 each and froms a certainty rating scale of 0 to 4 where 0 is unreliable and 4 is very reliable.

1	The prerequisites for the conclusions are seen as being very reasonable.
1	Data/information is available in large quantities.
1	There is a broad consensus among the experts in the field.
1	The phenomenon that are involved are well understood, and the models that are used are known to produce accurate predictions.

Certainty = 4

Appendix 2: Business Continuity and Crisis Management Plans

Business Continuity Plans

Scenario:	A disaster event has forced the store to be evacuated and in need of repairs
Processes covered:	All processes related to the business operations
Continuity specifications:	RTO 2 days

Roles and responsibilities:

Owner of the plan:	Manager
Authorised to invocate:	Manager

Activation of the plan:

Triggers:	The store has experienced a crisis forcing it be evacuated.

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:
Owner	+4799999999	company@online.no
Manager	+4799999999	company@online.no
Staff member 1	+4799999999	company@online.no
Cleaning company	+4799999999	company@online.no
Volunteer 2	+4799999999	company@online.no

Assets and resources needed to recover:

Type:	Quantity:	Source:
Transportation vehicle	1	Company transport vehicle
Cleaning equipment	2	Cleaning company
Bucket	3	Company stores
Special cleaning materials	1	Cleaning company
Drying machine	1	Nearby company

Tasks to be completed in order to complete the recovery:

Task:	Responsible for task:	Resources needed:	Goal:	Time:
Empty the store for water and damaged goods	Manager	2 People, Vehicle	Empty the store location to be ready for cleaning	1 hour
Sort out the goods that can be sold at a reduced price	Owner	Owner	Sort out the goods that can be sold at dis-	3 hours

			count and goods that are lost	
Clean the store	Manager	2 people	Clean the store so that the cleaning company can come in and finish the job	3 hours
Dry out the store	Manager	Drying machine	Get the store dried out before it can be re-stocked	1 – 5 hours
Functionality check on payment systems	Owner	Owner, (vehicle if replacements need to be picked up)	Check that payment systems have not been damaged and repair and replace where needed	1-5 hours
Re-stock the store	Manager	3 People, vehicle	Get the goods that were evacuated back to the store and arranged.	5 hours

Criteria for ending the BCP:

When is the process(es) running in a satisfactory way?	What other criteria can end the BCP?
When the store is re-established, cleaned out, the payment systems are functioning and the store is ready to open.	If the damage to the facility too great, the store will need to remain closed until it is repaired or until the company re-locates the store.

Comments:

Scenario:	There is no water in the pipes
Processes covered:	Sale of fresh flowers, production of decorations
Continuity specifications:	RTO – 1 hour

Roles and responsibilities:

Owner of the plan:	Manager
Authorised to invocate:	The person working in the store when the water stops

Activation of the plan:

Triggers:	The water stops coming

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:
Public services office	+4799999999	Municipality@gov.no
Manager	+4799999999	company@online.no

Assets and resources needed to recover:

Type:	Quantity:	Source:
Vehicle	1	Company vehicle
Mobile water tank	1	Alternate storage location

Tasks to be completed in order to complete the recovery:

Task:	Responsible for task:	Resources needed:	Goal:	Time:
Fill the water tank with clean water	Manager	Vehicle, water tank	Get the water that is needed	10 minutes
Transport the water tank to the store and mount it	Manager	Vehicle, full water tank	Mount the tank in position so that the water can be used	30 minutes
Call public sevices office	Manager	Phone	Find out when the water will come back on	10 minutes
In needed: set up a regular refill routine until the water is back on	Manager	-	Make sure that the store is supplied with the water it needs to keep operating.	10 minutes

Criteria for ending the BCP:

When is the process(es) running in a satisfactory way?	What other criteria can end the BCP?
When the water comes back on and there is no need for an extra water supply to keep it going.	

Comments:

Crisis Management Plans

Scenario:	Fire
Processes covered:	All processes located at the store location
Continuity specifications:	-

Roles and responsibilities:

Owner of the plan:	Manager
Authorised to invocate:	Designated responsible person

Activation of the plan:

Triggers:	- A fire is spotted in the store - The fire alarm is triggered

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:
Owner	+4799999999	company@online.no
Manager	+4799999999	company@online.no
Fire department	113	-
Nearby company 1	+4799999999	Neighbour@online.no
Nearby company 2	+4799999999	Neighbour@online.no

Tasks to be completed in sequence:

Task:	Responsible for task:	Resources needed:	Goal:	Time:
Attempt to put out fire	Person on duty in the store	Extinguisher	Put out the fire immediately if possible	5 seconds
Evacuate the store	Person on duty in the store	-	Get all persons out of the store	10 seconds

Call Fire department	Person on duty in the store	Phone	Alert the fire dept. to the situation.	2 minutes

Communication plan:

Target:	Message:	Projected effect on target:	Timing:
Alert the companies operating in the adjacent buildings	Inform the companies what the situation is at the moment to give them a chance to react	The companies will avoid losses by being able to implement their own crisis plans.	After fire department has been alerted
Public, Facebook, Twitter	What has happened, what has been done about it, what will happen next.	The people following the store will be informed on what is happening. It is important that the company is seen to handle it in a professional way.	When the situation is clear and the owner or manager has some time to spare the first thing to do will be to send the message.

Alternative locations and succession:

Succession:	Alternative locations:
Manager,Owner,worker	The alternative storage location can act as a command centre if the store location is not operational

Criteria for ending the CMP:

When is the crisis ended?	What other criteria can end the CMP?
When the fire is put out and the public and other stakeholders have been informed.	-

Comments:

Scenario:	Flooding
Processes covered:	All processes related to the running of the shop
Continuity specifications:	RTO – 2 days

Roles and responsibilities:

Owner of the plan:	Manager
Authorised to invocate:	Person designated as the responsible person for the period.

Activation of the plan:

Triggers:	An official flood warning of a 50 – 200 years flooding levels.

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:
Owner	+4799999999	company@online.no
Manager	+4799999999	company@online.no
Volunteer 1	+4799999999	company@online.no

Tasks to be completed in sequence:

Task:	Responsible for task:	Resources needed:	Goal:	Time:
Trigger the process	Designated resp.	Phone	Get the process started	10 min
Evacuate the store	Manager	Company car, owner/Manager/volunteer	Save materials from damage	5 hours
Prevent structural damage to building	Manager	-	Make sure that water pressure doesn't build up	1 hour

Communication plan:

Target:	Message:	Projected effect on target:	Timing:
Public, Facebook, twitter	Inform what has happened and what is being done to help.	Public will know why the store is be closed and will be in the loop on when it	When the evacuation is completed

		will re-open.	

Alternative locations and succession:

Succession:	Alternative locations:
Manager, Owner, Staff	Alternative storage location

Criteria for ending the CMP:

When is the crisis ended?	What other criteria can end the CMP?
When the flood water recedes and the communication lines are open to safely go back and forth between the alternative storage location and the store location.	If the flood is lower than anticipated and the peak flood does not in fact flood the store the crisis is called off.

Comments:

Scenario:	Loss of communications with suppliers
Processes covered:	Sales of interior design articles, decorations and fresh flowers
Continuity specifications:	-

Roles and responsibilities:

Owner of the plan:	Manager
Authorised to invocate:	Person responsible for readieness

Activation of the plan:

Triggers:	When the communications between the suppliers are broken for a long enough time for the projections to show that the store will run out of something.

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:
Owner	+4799999999	company@online.no
Manager	+4799999999	company@online.no
Alternative supplier flowers	+4799999999	company@online.no

Tasks to be completed in sequence:

Task:	Responsible for task:	Resources needed:	Goal:	Time:
Call alternative supplier to arrange delivery	Manager	Phone	Set up the delivery of the materials that the supplier was unable to deliver	1 hour

Communication plan:

Target:	Message:	Projected effect on target:	Timing:

Alternative locations and succession:

Succession:	Alternative locations:

Criteria for ending the CMP:

When is the crisis ended?	What other criteria can end the CMP?
When the supplier is able to deliver again then normal deliveries can be resumed.	If it is decided to change supplier permanently

Comments:

Appendix 3: BCRM Method

The process in the company

Business Continuity Risk Management Policy Document

This document is made to regulate the processes that establish and maintain a BCRM system at The Company. When the policy is established the leadership of The Company will adhere to the instructions that have been agreed on in this document. The following statements are the foundation of the process that will see the BCRM implemented and maintained at a desirable level:

Statement of intent:

The intention of doing a BCRM process is to make the company more robust and profitable. The BCRM process will make the company able to handle crises so that damage to assets and reputation are minimal. Additionally, the BCRM process will identify threats and weaknesses and to reduce their probability and impact in order to make the company less exposed to risk.

Statement of inclusion:

In order for the instructions that are made to be effectively there needs to be a broad awareness of the BCRM work in The Company. In order to achieve this the whole organisation needs to be included in the process if it is to be successful.

Statement of seriousness:

The BCRM process with the plans and instructions that are developed in it need to be followed. Compliance with the regulations are mandatory and failure to maintain ones part of the system can have catastrophic consequences for the future of The Company.

Statement of compliance:

Audits of the BCRM system is done yearly. In this process the performance and compliance of all parts of the system is evaluated.

BCRM organisation

In order for the process to be done properly there needs to be a structure in place that ensures the that the BCRM process will run properly. In The Company the owner of the BCRM process is the owner of the company. The BCRM manager is the manager of the company that oversees the day-to-day operations.

The BCRM manager is responsible for maintaining and developing the structure and reports to the BCRM owner. The owner approves the BCRM processes workings and signs off on the budg-

ets for the actions that need to be taken in the BCRM system. An external advisor will aid the BCRM manager in doing the yearly audits

Reporting

The reporting system of the BCRM program will be simple since the organisation is small. It is however vital to keep track of developments, incidents and progress to enable The Company to continue development of its continuity and risk management programs.

Reporting Schedule:

- Incident reports are filled out immediately after an incident is resolved.
- When a change to the BCRM process is made it is noted in the change log.
- The annual audit of the BCRM system will be done at the end of the fiscal year.

Owner of BCRM: BCRM Manager:

…… …….

Governance

The governance part is where the administrative layout of the process is formed. It contains the space for allocating resources and responsibilities for the BCRM process. The tool to accomplish this is a policy document that includes all the necessary information and statements for the BCRM process to work.

For the policy of the BCRM to be effective it needs to be concise in the way it presents its guidelines. The statements and instructions should be clear and easy to understand. A policy document is not supposed to give instructions or describe procedures, but rather to construct the framework that the procedures will work in. The following points are the different statements that start up the BCRM policy.

- Statement of intent: This is to outline why the BCRM process is being done and what is intended to be accomplished with it.
- Statement of inclusion: States who is involved in the process.
- Statement of seriousness: This states how serious the process is for the company and how compliance with the process is mandatory.
- Statement of compliance: This states how the compliance with the process internally is measured and dealt with.

The policy will also detail who is responsible for what parts of the process. In a small organisation it is likely more relevant for the owner of the company to also be the owner of the BCRM process. If the owner of the company is also the manager then the owner should also take on the role of managing the BCRM process.

The reporting structure will be outlined in the Policy. It is important to keep records and to inform both the owner of the BCRM process how the system is functioning and what could be improved. This does not need to be large documents, especially in a small company where the owner might be reporting to him or herself. The value of keeping a record of changes and performance is however an important part of keeping the system relevant as time goes by.

BCRM process

When the governance framework is put into place the work on the BCRM process can begin. The governance document will give instructions as to who will have what roles in the process. The BCRM process itself is divided into five sections; BIA, Risk Analysis, Mitigation and control, Planning and implementing and testing/evaluating. These together give a process that, when completed will give the company a clear view of its risk exposure and readiness levels concerning crisis events.

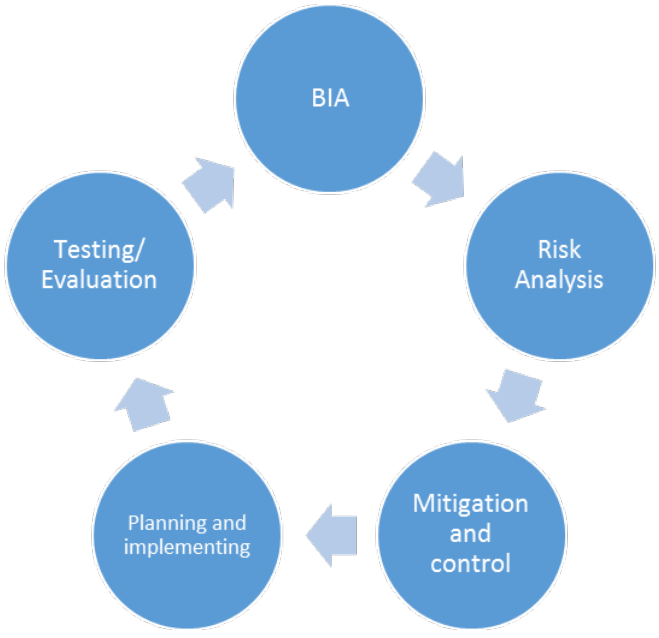


Figure 10 The BCRM process.

Business Impact Analysis

Business impact analyses is the process where the companies vulnerabilities are uncovered and graded. The parts of the process are to gather information, validating the information,

analysis of the information and reporting and approval of the result. These steps need to be done in sequence in order to be effective.

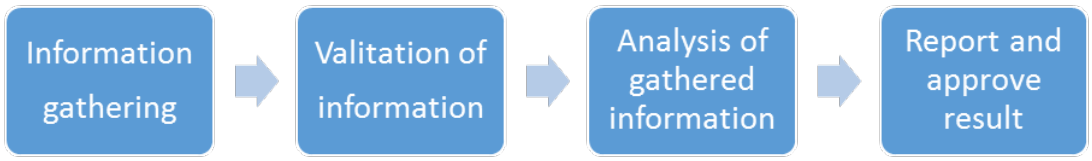


Figure 11 The process of executing a BIA.

The scope of the BIA should be all the processes, activities and assets of the company. The following list should be considered a part of the scope of the BIA:

- The environment the company is operating in
- The stakeholders requirements
- The regulatory or statutory/legal requirements
- The key core activities in the organization
- The assets or resources, internal and external, support key activities
- The impacts on the organization in the event of key, or core activities over time
- The interdependencies between internal and external resources and assets
- The organizations obligations towards external entities

When the scope of the BIA is established the next step is to gather the information that is needed for the process. The information is gathered by first filling out the questionnaire with a standardized set of questions, the information is then assessed and an interview will be conducted to gather further information based on the questionnaire. It is also useful to have a workshop with staff and if relevant stakeholders to gain further depth and new inputs. The information that is vital to gather in the start of the process is the answers to the following questions:

1. What internal and external dependencies are there between the processes and activities?
2. What is the impact over time when the processes are not operating?
3. What is the Maximum Tolerated Outage (MTO) for the processes and activites?
4. What is the Maximum data loss tolerated?
5. What technology is used in the processes and activities?
6. What are the Key personnel of the company?
7. What is their availability?
8. How is the succession within the company?

When information is gathered and collated the owner and manager of the company will have to sign off on it to ensure the quality of the information that has been gathered. Any other experts that are available should be consulted for further quality assurance. After this stage in the process the only information that is left is information that is relevant to the process and within the scope of the process.

The information that has been gathered and validated then needs to be analysed to see what conclusion can be made with it. In this part, the RTO and RPO of the processes and activities will be established along with the level of criticality they have. The finished product will have a list of the different assests, products and activities with their respective values of MTO, RTO, RPO and dependencies.

The information from the process will be put into the template of Annex A: Business Impact Analysis. Annex A gives the necessary structure to build a BIA and to make a report from the process that can then be evaluated. Contained in the template is also the format of a BIA report. Considering the size of the organization the report will be a brief summary of the findings of the BIA process.

Risk Analysis

Risk analysis is the process of identifying and assessing risks. The process takes most of its parts from the realm of RM as it is the treatment of risk factors. The risk analysis part of the BCRM process starts when the BIA is completed. This ensures that the risk analysis is done on a strong foundation. During the BIA the different assets, processes, activities and dependencies are defined.

The risk analysis consists of two main parts; Risk identification and Risk assessment. Risk identification is focused on finding the different risks that affect the company and the necessary information about them. The methods for finding this information is questionnaires, interviews, brainstorming and workshops. Since the vulnerabilities of the company is already established in the BIA the identification work starts with looking at the BIA process and drawing the relevant information from it. The process consists of the following steps:

1. Identify the company’s assets.
2. Identify risks that can have a negative impact on the assets.
3. Fill in the identified risks into the Risk register.
4. Use the Bow tie analysis to describe the risks in terms of causes and consequences.
5. Score the risks on the scale 1-5 x 1-5 for impact and probability in the risk matrix
6. Calculate ALE for the risk factors.

7. The level of confidence in the information that forms the basis of the analysis will be rated on a scale from 1 to 4.
8. Based on the analysis of the different risk factors they will need to be rated on a scale from 1-5 based on how critical it is to treat them.
9.

The Risk analysis process produces a excel document that contains the risk register, risk matrix and the analysis of the risk factors. The template for the document is found in Annex B: Risk Analysis. The finished product is an overview of the risk factors with all relevant information attached.

Mitigation & Control

For the BCRM process to be able to accomplish a betterment of the companies situation, the information from the BIA and risk analyses processes need to be used to enable appropriate responses. These responses take the form of strategies and risk treatment plans allow the company to reduce the probability and impact of risk events and crises. It should not be forgotten to plan for the unforeseeable and have strategies in place that cover basic readiness can be useful.

For every problem, there can be many solutions. In order to choose the correct solution the options need to be carefully evaluated. Three factors need to be considered when evaluating a potential strategy or RTP:

- Effectiveness: How effective is the strategy at minimizing probability and impact, protecting critical elements and how well do they align with the continuity requirements?
- Cost-benefit analysis: The strategy will have to be carefully analysed to ensure that the cost of implementing it does not exceed the cost from the risk.
- Applicability: The strategy needs to be made in such a way that it is possible to implement it in a practical way. Ideal scenarios do not exist and a strategy that does not take this into account will have a much lower value.
-

When thinking of making strategies for the company there are a set of categories that should be covered:

- Processes
- Technology
- People
- Facilities and premises

- Information
- Supplies

The Mitigation and Control part will produce a series of entries where each contains a strategy or RTP for a specific problem. The templates for the strategies and RTPs are found in Annex C: Strategies and RTPs.

Planning and Implementing

The planning phase of the process is where the BIA, Risk Assessment and strategy development come together to create practical procedures. There are two types of plans related to the readiness of the company to combat a crisis. These are the Crisis Management Plan (CMP) and the Business Continuity Plan (BCP). These will be developed on the lines of scenario based planning where a set of scenarios will be created from the information of the previous steps. Annex D: Business Continuity Plan and Annex E: Crisis Management Plan have the templates to make said documents. The plans will be developed on a scenario base where the process starts with the identification of a scenario and the plan aims to solve that scenario. The goals of a CMP is to enable the company to handle a crisis. The plan should therefore enable the person encountering the crisis situation to: assess the situation correctly, open the correct communications channels and from there to take control of the situation and start working to limit the impacts of the crisis.

The BCP takes over when the situation is under control and the recovery work is to begin. The goal of the BCP is to enable the company to resume operations again with a minimum loss of productivity.

Testing/Evaluation

Once the plans are in place and are beginning to be implemented they need to be tested to ensure that they work in a satisfactory manner. Before they are implemented there will be a dry run of the plans where all the personnel that have a part in the plans will take part. There will also be a session where the plan is presented and explained to the staff and relevant stakeholders.

As a minimum there needs to be done a live test of the main parts of each plan that is implemented. Regular tests and evaluation of results will need to be an integrated part of the overall plan. The criteria for re-evaluating the BCRM process is if there are major changes in the market or environment or there is an event that expose weakness. There should also be a plan for regular audits of the system. An annual evaluation is appropriate in most cases.

Appendix 4: Business Impact Analysis – Template

This document is made to regulate the processes that establish and maintain a BCRM system at XXXX. When the policy is established the leadership of XXXX will adhere to the instructions that have been agreed on in this document. The following statements are the foundation of the process that will see the BCRM implemented and maintained at a desirable level:

Statement of intent:

The intention of doing a BCRM process is to make the company more robust and profitable. The BCRM process will make the company able to handle crises so that damage to assets and reputation are minimal. Additionally the BCRM process will identify threats and weaknesses and to reduce their probability and impact in order to make the company less exposed to risk.

Statement of inclusion:

In order for the instructions that are made to be effectively there needs to be a broad awareness of the BCRM work in XXXX. In order to achieve this the whole organisation needs to be included in the process if it is to be successful.

Statement of seriousness:

The BCRM process with the plans and instructions that are developed in it need to be followed. Compliance with the regulations are mandatory and failure to maintain ones part of the system can have catastrophic consequences for the future of XXXX.

Statement of compliance:

Audits of the BCRM system is done yearly. In this process the performance and compliance of all parts of the system is evaluated.

BCRM organisation

In order for the process to be done properly there needs to be a structure in place that ensures the that the BCRM process will run properly. In XXXX the owner of the BCRM process is the owner of the company. The BCRM manager is the manager of the company that oversees the day-to-day operations.

The BCRM manager is responsible for maintaining and developing the structure and reports to the BCRM owner. The owner approves the BCRM processes workings and signs off on the budgets for the actions that need to be taken in the BCRM system.

Reporting

The reporting system of the BCRM program will be simple since the organisation is small. It is however vital to keep track of developments, incidents and progress to enable XXXX to continue development of its continuity and risk management programs.

Reporting Schedule:

Incident reports are filled out immediately after an incident is resolved.
When a change to the BCRM process is made it is noted in the change log.
The annual audit of the BCRM system will be done at the end of the fiscal year.

Appendix 5: Risk Analysis – Template

Risk Identification			Risk Analysis							
Risk #	Risk Name	Risk Type	Threats	Probability safeguards	Impact safeguards	Risk score	ALE	Certainty Level	Notes	Last updated

Appendix 6: Mitigation strategies-RTPs – Template

The following are the plans for treating the threats and risk factors that have been identified and analysed in the BIA and Risk Analysis processes.

#:	Process/asset/Risk factor:
Mitigation/Treatment plan:	
Projected probability/impact reduction:	Projected cost of implementation:
Summary:	Date and sign:

#:	Process/asset/Risk factor:
Mitigation/Treatment plan:	
Projected probability/impact reduction:	Projected cost of implementation:
Summary:	Date and sign:

Appendix 7: Business Continuity Plan – Template

Scenario:	
Processes covered:	
Continuity specifica-tions:	

Roles and responsibilities:

Owner of the plan:	
Authorised to invocate:	

Activation of the plan:

Triggers:	

Execution:

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:

Assets and resources needed to recover:

Type:	Quantity:	Source:

Tasks to be completed in order to complete the recovery:

Task:	Responsible for task:	Resources needed:	Goal:	Time:

Criteria for ending the BCP:

When is the process(es) running in a satisfactory way?	What other criteria can end the BCP?

Comments:

Appendix 8: Crisis Management Plan – Template

Scenario:	
Processes covered:	
Continuity specifications:	

Roles and responsibilities:

Owner of the plan:	
Authorised to invocate:	

Activation of the plan:

Triggers:	

Execution

List of contacts that are needed to execute the plan:

Name:	Phone:	E-Mail:

Tasks to be completed in sequence:

Task:	Responsible for task:	Resources needed:	Goal:	Time:

Communication plan:

Target:	Message:	Projected effect on target:	Timing:

Alternative locations and succession:

Succession:	Alternative locations:

Criteria for ending the CMP:

When is the crisis ended?	What other criteria can end the CMP?

Comments:

Appendix 9: BCRM Policy – Template

This document is made to regulate the processes that establish and maintain a BCRM system at XXXX. When the policy is established the leadership of XXXX will adhere to the instructions that have been agreed on in this document. The following statements are the foundation of the process that will see the BCRM implemented and maintained at a desirable level:

Statement of intent:

The intention of doing a BCRM process is to make the company more robust and profitable. The BCRM process will make the company able to handle crises so that damage to assets and reputation are minimal. Additionally the BCRM process will identify threats and weaknesses and to reduce their probability and impact in order to make the company less exposed to risk.

Statement of inclusion:

In order for the instructions that are made to be effectively there needs to be a broad awareness of the BCRM work in XXXX. In order to achieve this the whole organisation needs to be included in the process if it is to be successful.

Statement of seriousness:

The BCRM process with the plans and instructions that are developed in it need to be followed. Compliance with the regulations are mandatory and failure to maintain ones part of the system can have catastrophic consequences for the future of XXXX.

Statement of compliance:

Audits of the BCRM system is done yearly. In this process the performance and compliance of all parts of the system is evaluated.

7 BCRM organisation

In order for the process to be done properly there needs to be a structure in place that ensures the that the BCRM process will run properly. In XXXX the owner of the BCRM process is the owner of the company. The BCRM manager is the manager of the company that oversees the day-to-day operations.

The BCRM manager is responsible for maintaining and developing the structure and reports to the BCRM owner. The owner approves the BCRM processes workings and signs off on the budgets for the actions that need to be taken in the BCRM system.

8 Reporting

The reporting system of the BCRM program will be simple since the organisation is small. It is however vital to keep track of developments, incidents and progress to enable XXXX to continue development of its continuity and risk management programs.

Reporting Schedule:

Incident reports are filled out immediately after an incident is resolved.

When a change to the BCRM process is made it is noted in the change log.

The annual audit of the BCRM system will be done at the end of the fiscal year.

Appendix 10: BCRM test and change log - template

BCRM test log

Enter the instances where tests have been performed and record the methods and results of the tests.

What part of the BCRM was tested?	What testing method was used?	What result did the test have?

BCRM change log

Enter changes and developments that are made to the BCRM process. This needs to be one to keep track of changes and to log how changes in the environment is taken into the BCRM system.

What BCRM part was changed?	What provoked the change?	What was changed?	Date implemented

Appendix 11: Annual Loss Expectancy Calculator (ALEC)

For this project, there was a need to have a more precise way of calculating ALE in order to give a number that gives a greater level of certainty. The challenge with improving upon such a method as presented by Broder (2006, 22) is the simplicity it offers. If another solution is to be viable, it will need to be operable with the same or even greater ease.

This problem has two sides; the mathematical function that will make the calculation, and a way in which the user of the method can do so without needing to resort to manually calculating fractures. When attempting to improve the method, the first attempt was to create a formula to calculate the fractions of the i and f values. This was found to not be practical as the resulting equation would be too complicated to be usable on its own.

The mathematics of the problem is simple in essence; the value of the impact of an event is divided by the value of time in years. The resulting value will then represent the average losses that can be expected from the event. In order to make this mathematical problem usable it became evident that what was needed was a program to handle the fractional values that would occur along the way in the calculations and still make it usable.

Formula for Annual Loss Expectancy calculator			
Years = y	Months = x	days = a	Hours =b
y = 8760y	x = 720x	a = 24a	b = 1
i = cost of the event			
ALE = $\frac{i}{y+x+a+b}$ 8760			

Figure 12 The mathematical formula for the Annual Loss Expectancy Calculator. The amounts are rounded to simplify calculation.

The equation for ALE in figure 13 shows the way that the average impact is over a certain period of time. For this model the basic unit was made to be in hours so as to avoid unnecessary complications with fractions of higher numbers representing months, days and hours. In this way the values of y, x, a and b are represented in hours. In order to get the result of the equation to represent the annual value the $\frac{i}{y+x+a+b}$ was multiplied by 8760 which is the amount of hours in a year.

The next step was to make a functioning model in Excel to test that the equation would be solved properly and to lay the groundwork for the future programming work. The formula can be seen at work in figure 14 where the event of a flower arrangement being dropped every four months is used as an example to test the method.

Name of Event:	A flower arrangement is dropped to the ground and ruined					
"What is the interval between events?"			8760	720	24	1
Years			0			
Months	4			2880		
Days					0	
Hours						0
"What is the impact value of the event? (NOK)"	1500					
ALE =	4563		0,520833	2880	8760	

Figure 13 The Excel model of the program making an ALE calculation.

The actual program was made with the Visual Basic (VB) programming language. VB was chosen for its compatibility with windows office applications and its relative simplicity. The program was then built from the mathematical model that had been made in Excel.

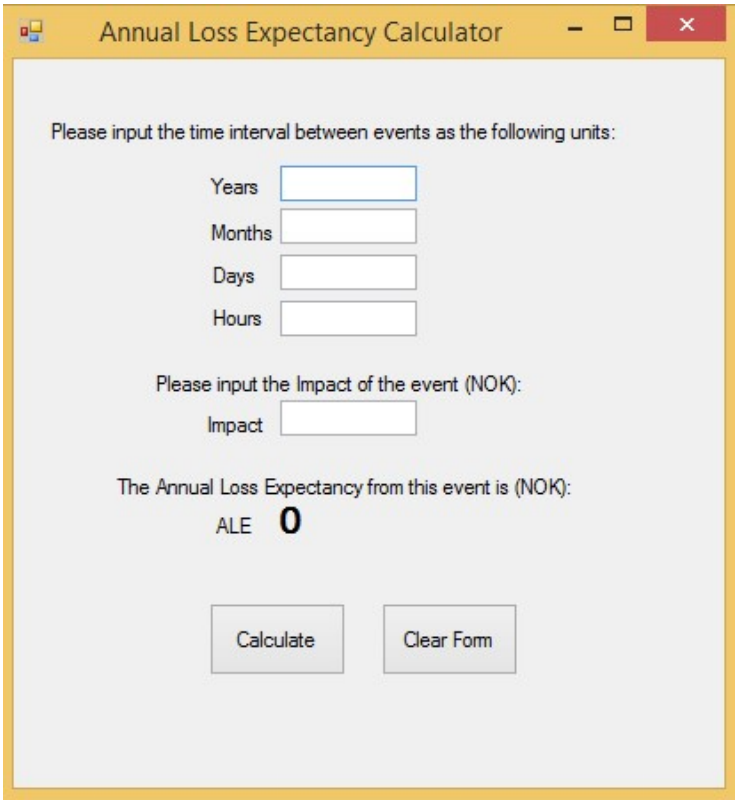


Figure 14 The interface of the ALEC application v1.0.0.2

The functioning Annual Loss Expectancy calculator allows the company to accurately predict the average amount of losses that will be occurred in a year. It will by doing this give the company the ability to calculate the actual impact of recurring events over time, and so give the ability to employ mitigation efforts more accurately to the risks that these represent.