LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Developing a Risk and Security Management System

Ruippo, Joel

2015 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Developing a Risk and Security Management System

Joel Ruippo
Degree Programme in Security Management
Bachelor's thesis
January, 2015

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

Joel Ruippo

Developing a Risk and Security Management System

Year 2014 Pages 34

In the year 2014 the Governing Body of Suomenlinna decided to create a risk and security management system which consists of four different stages. The objective of this study was to create that system. The system consisted of four stages, risk management plan, emergency plan, crisis management plan and a business continuity plan. Action research was chosen to be a research method for this study.

The Governing Body of Suomenlinna requested that the risk management plan and the business continuity management plan would fill the requirements that the International Organization for Standardization (ISO) defines in their standards 31000 and 22301. The rescue plan was meant to fill the requirements of Finnish legislation, rescue act 379/2011. The crisis management plan was created using examples from other Finnish government agencies and earlier documentation from the Governing Body of Suomenlinna.

The project started in spring 2014, and it ended in September. The creation of the plans and the system went according to the timeline which was set in the beginning of the project. One of the key objectives for the system was to make it simple enough that it could be understood by every employee of the Governing Body. Therefore it was decided that the documentation should be thorough and limited. This objective was reached with careful planning. The employees of the Governing Body were active with the project and they provided the information which was needed for the creation of the system.

The first step of creating the system was planning. During the planning stage of the project we created the framework for all of the different plans. After planning the risk management plan was created. Risk management was first because it would give the present status of the organization. For risk assessment and analysis, this stud used three different methods from the ISO 31010 standard, brainstorming, preliminary hazard analysis and business impact analysis. When the risk management plan was finished, the other plans started taking their shape.

Final product of this process was the four plans, and the system which would implement all of the plans. Even though this thesis emphasizes on the creation of the risk management plan, the objective was to present the requirements for all of the other plans as well.

Keywords: Risk and security management system, Risk management, emergency plan, crisis management, business continuity management, ISO 31000, ISO 22301

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Joel Ruippo

Kokonaisturvallisuuden johtamisjärjestelmän rakentaminen

Vuosi 2014 Sivumäärä 34

2014 Suomenlinnan hoitokunta päätti rakentaa kokonaisturvallisuuden johtamisjärjestelmän. Tämä järjestelmä piti sisällään riskienhallintasuunnitelman, pelastussuunnitelman, kriisien hallinta suunnitelman sekä liiketoiminnan jatkuvuussuunnitelman. Tutkimuksen aiheena oli rakentaa tämä järjestelmä, ja tutkimusmenetelmänä käytettiin toiminnallista tutkimusta.

Järjestelmää koskien yksi Suomenlinnan hoitokunnan vaatimuksista oli, että sen pitää, täyttää lakien ja standardien vaatimukset. Riskienhallinta- ja liiketoiminnan jatkuvuussuunnitelman rakentamisessa käytettiin pohjana Kansainvälisen standardointijärjestön laatimia ISO 31000 ja 22301 standardeja. Pelastuslain laatimisen vaatimuksina oli täyttää Suomen pelastuslain 379/2011 vaatimukset. Kriisien hallinta suunnitelman taustalla on muiden valtion organisaatioiden tekemät kriisien hallinta suunnitelmat, sekä Suomenlinnan hoitokunnan aikaisemmat dokumentit aiheesta.

Projektin laatiminen alkoi keväällä 2014, ja järjestelmä valmistui syyskuussa. Järjestelmän laatiminen sujui suunnitellusti ja aikataulussa. Yksi tärkeimmistä tavoitteista Suomenlinnan hoitokunnalla oli, että järjestelmä pystytään toteuttamaan jokaisen työntekijän kohdalla. Näin ollen jokaisen työntekijän tuli ymmärtää järjestelmän sisältö ja tarkoitus. Suomenlinnan hoitokunnan työntekijät ymmärsivät järjestelmän tarpeen, ja kaikki heiltä pyydetyt tiedot olivat helposti saatavissa.

Projekti alkoi suunnittelemalla toimintaympäristö ja puitteet organisaation turvallisuustoiminnalle. Puitteiden tarkoituksena oli osoittaa mitä haluttiin, ja millä tavalla. Kun toimintaympäristö ja puitteet olivat valmistuneet, alkoi riskienhallintasuunnitelman teko. Riskienhallintasuunnitelma rakennettiin ensin, koska sen katsottiin tuovan näkemys organisaation tämän hetkisestä tasosta, turvallisuuden osalta. Tässä opinnäytetyössä käytettiin kolmea eri riskien arviointimenetelmää, jotka ovat löydettävissä ISO 31010 standardista, aivoriihi, alustava vaara-analyysi sekä liiketoiminnan vaikutusten analyysi. Kun riskienhallintasuunnitelma saatiin valmiiksi, oli siitä helppo jatkaa muiden suunnitelmien tekoon, koska suurin osa tarvittavista tiedoista oli jo valmiina.

Tämän opinnäytetyön tarkoituksena oli tuottaa toimiva kokonaisturvallisuuden johtamisjärjestelmä, ja siinä onnistuttiin. Vaikka opinnäytetyö painottuu riskienhallintasuunnitelmaan ja riskien analysointiin, oli tarkoituksena tuoda esille myös mitä muiden suunnitelmien kehittämiseen ja toteuttamiseen vaaditaan.

Avainsanat: Kokonaisturvallisuuden johtamisjärjestelmä, riskienhallinta, pelastussuunnitelma, kriisien hallinta, liiketoiminnan jatkuvuussuunnitelma.

Table of contents

1 Introduction

This thesis was created with Governing Body of Suomenlinna. The Governing Body of Suomenlinna is the government agency which manages the island fortress of Suomenlinna. The island fortress is one of the seven UNESCO world heritage sites in Finland and it is located south from Helsinki. It was built in the middle of the 18th century. The fortress has been under control of three different nations, Finland, Sweden and Russia. Before the thesis process was started the Governing Body of Suomenlinna had realized that their security management was outdated and insufficient. In cooperation with Jyri Paasonen work was begun in order to create a working, and legally sufficient, risk and security management system.

When creating different security documentation during an internship at the Governing Body of Suomenlinna, it was realized that the examples that could be used as a basis for the new security documentation were developed in United States and Canada. This ignited the spark to create an example, made here in Finland, of how these plans are created in this particular context. The objective of this thesis is to describe the process that was used to create a working risk and security management system, while using an action research method. The risk and security management system consists of four different plans: a Risk Management Plan, an Emergency Plan, a Crisis Management Plan, and a Business Continuity Plan, as well as the strategy and policies behind those plans.

The Risk Management Plan and Continuity Plan were created for Suomenlinna using requirements that are presented in the ISO standards numbers 31000, 31010 and 22301. The Rescue Plan was created using the requirements of the Finnish rescue act 379/2011 and the Crisis Management Plan was developed through existing plans that were found in Finland and with the organization's own knowledge of crisis management.

This thesis emphasizes the Risk Management Plan and the creation of it. The Risk Management Plan gives an understanding of what the current status of the organization is. Once the risks and context of the organization are understood, the other plans can be developed. The thesis presents the requirements that the ISO standards give and how the process was implemented in Suomenlinna. The risk management process consists of five different stages:

1. defining the context
2. risk assessment
3. risk treatment
4. monitoring and review
5. communication and consultation

The risk management process was implemented in Suomenlinna during April, May and June of 2014.

To meet the requirements of the Finnish rescue act (379/2011), an emergency management plan was created. The act requires that if there is a threat of serious consequences an emergency plan must be generated. This plan should consist of a conclusion of the risk assessment, safety arrangements that are in the buildings, guidelines in order to prevent accidents and self-preparedness guidelines.

The crisis management plan was developed in order to minimize the impact of any crisis on the Governing Body. The emergency management plan was created for the purpose of protecting and saving people and property during a crisis. The objective of the crisis management plan is to ensure that the organization survives through a crisis. The plan presents guidelines for communication and actions throughout the crisis and presents the requirements, responsibilities and objectives of the crisis management team to ensure minimal impact on the organization.

The objective of the business continuity plan is to identify the organization's key business operations and the risks and threats against them. The business continuity plan is a collection of plans that when implemented can restore business operations in a specific period of time and to a specific level. The time and level objectives that the organization has to work in must be set in a way that the organization can handle the loss of income. The identification stage of the business continuity plans was implemented using a business impact analysis.

The International Organization for Standardization (ISO) is an independent organization that is the world's largest developer of international standards for different industries. The industries that ISO develops standards varying from technology, to food safety, to agriculture and healthcare. ISO has published more than 19,500 international standards on those industries, and their objective is to ensure quality, safety and efficiency of products, services and systems. (International Organization for Standardization. 2014.) ISO has 164 member countries and Finland's member of the ISO is the Finnish Standards Association (SFS), which controls and coordinates national standardization in Finland. The majority of the standards that the SFS publishes are based on the standards that are published by ISO or the European Committee for Standardization (CEN). (Finnish Standards Association. 2014.)

1.1 Risk and Security Management System

A management system is a combination of organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. The implementation of this combination will provide the organization tools to reach its objectives. (International Electrotechnical Comission 2012, 13)

A management system is a tool which allows an organization to lead their process in a certain way. The management system allows the organization to plan, measure and monitor their processes and actions. The goal of this system is to develop the processes to become more efficient. The management system

- creates a link between the organizations strategy and the processes,
- provides the capability to measure and review the processes,
- contains information how the data should be analyzed, what goals should be set and how, and what actions should be taken,
- helps to anticipate future incidents,
- defines the roles and responsibilities
- creates proper communication channels for sufficient communication.

(Niemelä, Pirker, Westerlund 2008, 117-119)

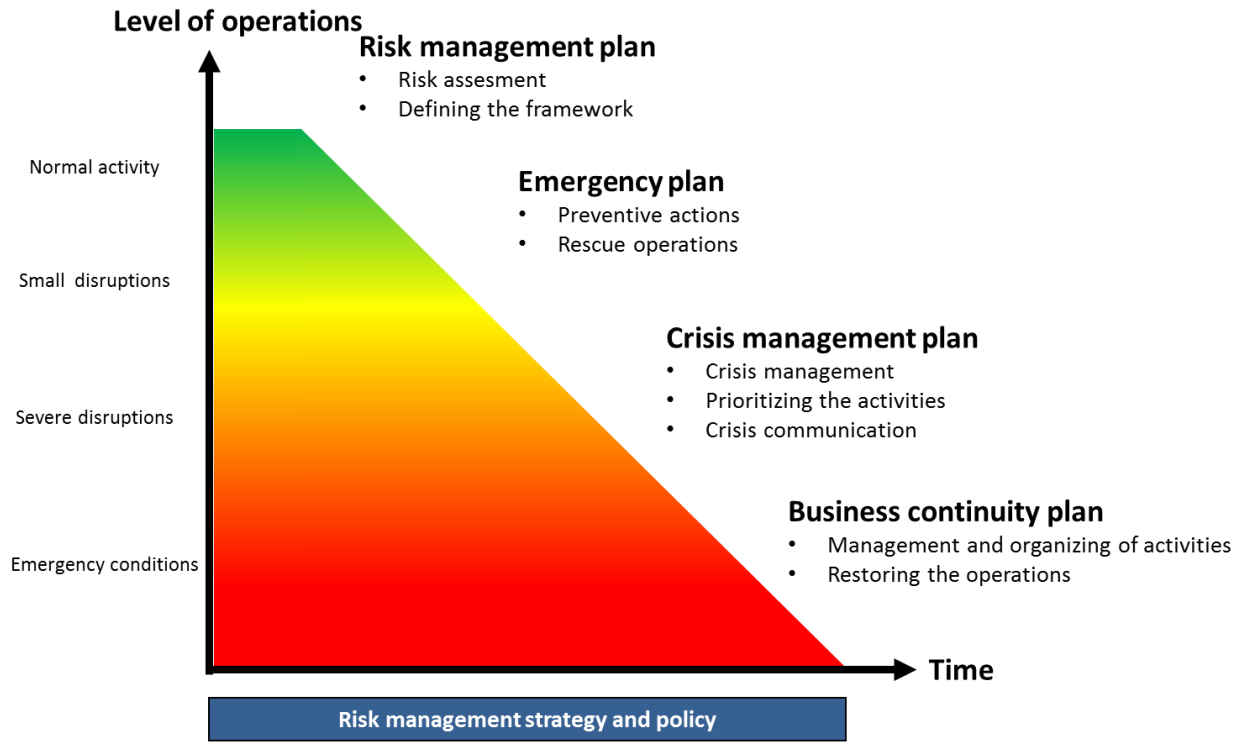

Figure 1 Risk and security management system (created during the project)

Figure 1 represents the Risk and Security Management System that was created for the Governing Body of Suomenlinna. The figure shows that the Risk and Security Management System is based on the organization's risk management strategy and policy. The strategy and policy which were defined for the Governing Body, also gave the framework on how the Risk Management, Emergency, Crisis and Business Continuity Plans should be generated.

After generating the strategy and policy the Risk and Security Management System has a base. The Risk Management Plan contains the current status of the organization. The plan shows what kind of risks the organization faces and what kind of context it works in. During the risk assessment the organization also gets an understanding of how it can work to minimize the effects of the identified risks.

The Emergency Plan is designed to be implemented at the moment when a crisis reveals itself. The emergency plan contains information about how and where the people on the islands are supposed to be evacuated to. The emergency plan assists the organization to minimize the consequences of the events.

The Crisis Management Plan consists of guidelines for crisis management, information on the crisis team and its duties during a crisis, and guidelines and responsibilities of implementing successful crisis communication. The crisis management plan is designed to be implemented after rescue operations have been completed and there is no longer any immediate danger.

The final stage of the Risk and Security Management System, the Business Continuity Plan, consists of information on the key processes of the organization, guidelines for protecting those processes and the different plans in case a disaster threatens those processes. The business continuity plan is implemented after the crisis has passed, in order to get business operations back to a level where the business can operate normally.

1.2 Action research

For this thesis it was decided that the method for research would be action research. Action research is a method which allows people involved to understand and change their behavior and practices in certain situations. (Kemmis, 2010 ,421) "Action research aims to explore new ways of doing things, new ways of thinking, and new ways of relating to one another and to the world in the interest of finding those new ways that are more likely to be for the good of each person and for the good of humankind, and more likely to help us live sustainably." (Kemmis, 2010, 425) Therefore it was chosen because it gives a possibility to create an understanding, for anyone reading this thesis, on how the Risk and Security Management System could be created.

Action research starts by generating a question or problem you want to solve. The problem in this thesis is to develop a working security system for the Governing Body of Suomenlinna. In research, the objective is usually to find an answer to a question, in action research the objective is also to measure your findings and make a difference in the field. (Alana, Slater, Buckman 2012. 3)

The first step in action research is to investigate the context of the study and what other researches have done in the similar circumstances. Additionally, other available channels for investigation can be the organization's previous projects or other similar studies which have been conducted and can be found from the internet. In this thesis, older versions of risk assessments that were created in Suomenlinna were used. The second step in action research is measurable action. This means that the researchers who are implementing the action research determine how those could be measured afterwards. The third step is reflection. The researchers reflect on the research in order to find out what is working and what is not. (Alana, Slater, Buckman 2012. 14-19.)

1.3 The Governing Body of Suomenlinna

The Governing Body of Suomenlinna is the government agency that has, through legislation, acquired the responsibility to preserve the landscape and the fortress of Suomenlinna, which is host to a UNESCO world heritage site. The main duties of Suomenlinna consist of preserving the monuments, buildings and equipment that remain in Suomenlinna, providing maintenance and restoration for the monuments and buildings and trying to develop the Suomenlinna world heritage site so it holds a place as a significant monument in Finnish culture. (Finland 1989.)

The Governing Body was founded in 1973 and was made the government agency in 1988. The purpose and mission of the Governing Body comes from the Finnish legislation. The Governing Body is a part of the Finnish Ministry of Education and Culture. The Governing Body gets its financing from the state of Finland and from the real-estate they provide for the people living on the islands of Suomenlinna. The highest policy of Suomenlinna is created by the board of Suomenlinna, which consists of different stakeholder representatives. The stakeholders of Suomenlinna are the Ministry of Education and Culture, the Ministry of Justice, the Ministry of Finance, the city of Helsinki, the National Board of Antiquities, Senate Properties and the residents of Suomenlinna. (Suomenlinna 2014. 23)

The highest decisive branch of the Governing Body is the board. The board consists of representatives from different stakeholders such as the Defence Forces and different Ministries. Representing the board's supervision is the Director of Suomenlinna who manages the daily operations in Suomenlinna. The Governing Body has four units, each with their own specific areas of business. The areas are restoration, governing and legal, world heritage and

maintenance. The restoration and maintenance units work on the buildings and landscape, in cooperation with the inmates of the prison. The world heritage unit takes care of the UNESCO heritage site business and the governing and legal department provides a support unit for the other departments. (Suomenlinna. 2014.)

Suomenlinna is one of the seven UNESCO world heritage sites in Finland. This status has an effect on risk management because according to the UNESCO treaty the landscape and buildings of Suomenlinna must remain authentic. Suomenlinna is also a part of the city of Helsinki, it has over 800 residents who pay rent to Suomenlinna, and this is one of the income streams for the Governing Body of Suomenlinna. The city of Helsinki is responsible for the infrastructure of Suomenlinna and takes care of the bridges and roads. The city of Helsinki also provides a daycare center, summertime emergency services and a library in Suomenlinna. (Management plan of Suomenlinna. 2014.)

On one of the Suomenlinna islands is a prison that works under the supervision of the Finnish Ministry of Justice. The prison inmates take part in the restoration of the fortress. There is also the Finnish Naval Academy that is supervised by the Finnish Defence Forces. Suomenlinna was originally built for the military and it was controlled by the Defence Forces until 1972. Today, the Naval Academy has around 450 students and it is one of the biggest employers in Suomenlinna. (Suomenlinna. 2014.)

2 Theory for the Risk and Security Management System

2.1 Risk management plan

This risk management plan defines the process that was completed according to ISO 31000 standard for risk management. The objective of this risk management plan was to create a working and understandable risk management procedure for the Governing Body of Suomenlinna. The risk management plan contains general information on risk management, for example, what should be in a risk management policy, the defining of an external and internal environment and three risk assessment techniques. It also contains information on risk profiles that were used in during this project, and risk criteria that are used to measure the severity of different risks.

2.1.1 Risk management

According to Paul Hopkin (2010, 42) there are no specific origins to risk management. One way that risk management might have born through the insurance business in the United States. In the 1950s, companies that took out insurance policies realized that there was not enough protection for insurances if there was not enough preventive protection for property and buildings.

The goal of risk management in business is not to exhaust the possibility of the risk entirely. Corporations and other players in the field should accept the risk, but concentrate on preventing the consequences of that risk from getting too great. When working with a risk management system you can calculate what kind of risks you are capable of surviving with. The key is to find a way to accept failure and take risks that will gain the business a competitive advantage against the other companies. (Hopkin, 2010,3-5)

The process of risk management, which is presented in **Virhe. Viitteen lähdettä ei löytynyt.** of this thesis, shows how risk management should be conducted in an organization. Risk management consists of five different stages:

- Defining the context gives the organization an understanding of its objectives, sets the scope and risk criteria for them and creates a framework that should be considered throughout the risk management process.
- Risk assessment consists of risk identification, risk analysis and risk evaluation.
- Risk treatment consists of making the decision implementing it, and deciding how to treat the risks that have been identified and analyzed in the risk assessment stage of the process.
- Monitoring and review of risk management must be done regularly in order to get results and develop the risk management process further.
- Communication and consultation consists of communication between the internal and external stakeholders.

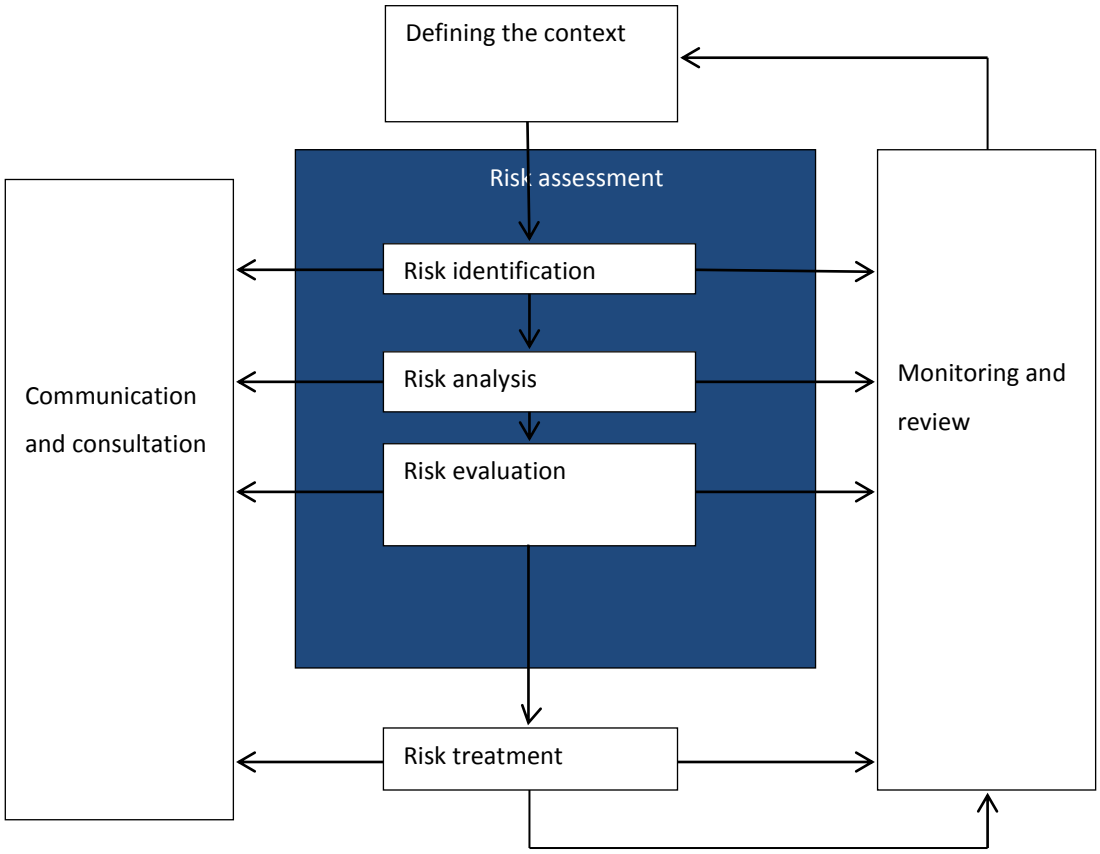

Figure 2 ISO 31000 risk management process
(International Organization for Standardization, 14)

This thesis emphasizes the risk management standard made by ISO. When looking at different risk management standards it can be seen that they are all similar. For example Institute of Risk management (IRM) has their own risk management standard. Their process starts with determining organization's strategic objectives. Then comes the risk assessment and evaluation stage, which continues into risk reporting. After making the decision the standard continues into risk treatment, which is followed with reporting and monitoring stages. (Institute of Risk Management, 2002, 4)

According to ISO 31000 (7-8), if a company wants risk management to work properly, the procedure must follow 11 principles. These principles are:

- risk management creates and protects value
- risk management is an integral part of all organizational processes
- risk management is a part of decision making
- risk management explicitly addresses uncertainty
- risk management is systematic, structured and timely
- risk management is passed on the best available information
- risk management is tailored

- risk management takes human and cultural factors into account
- risk management is transparent and inclusive
- risk management is dynamic, iterative and responsive to change
- risk management facilitates continual improvement of the organization

Risk management creates and protects value, means risk management provides solutions and assists with reaching goals in different areas of the business. (International Organization for Standardization 2009, 7-8)

Risk management is an integral part of all organizations' processes means that every process which is conducted in an organization is part of risk management, as well as risk management is part of every process. This principle guarantees that the group working with the risk management process gets the best and most recent information that exists in the organization. (International Organization for Standardization 2009, 7-8)

Risk management is part of the decision making, means that risk management is supposed to give the decision makers a possibility to make well-informed choices that affect the organization. (International Organization for Standardization 2009, 7-8)

Risk management explicitly addresses uncertainty means that the purpose of risk management is to understand the uncertainties of the information provided and how these uncertainties can be solved. (International Organization for Standardization 2009, 7-8)

Risk management is systematic, structured and timely means that risk management is based on the idea that the management gets more efficient and the organization gets more reliable and comparable results. (International Organization for Standardization 2009, 7-8)

As mentioned before, the risk management should be based on the best available information. The information can be taken from such channels as the organization's own history, stakeholder feedback or expert judgment. However, the top management should understand that there might be differences between internal and external data.
Risk management is tailored means that it is specific to each organization. When implementing this project the business environment that the organization had was like no others in Finland. This meant that there were new risks that other organizations did not have and gave some risks new adjustments that had to be taken into consideration while doing the risk analysis. (International Organization for Standardization 2009, 7-8)

Risk management takes human and cultural factors into account means that it is also a tool that can clarify the different human and cultural factors that organizations might have. The

human or cultural differences in people can have a positive, as well as a negative effect on an organization's activities. (International Organization for Standardization 2009, 7-8)

Risk management is transparent and inclusive means that it should be open and thorough. When the time is right, the appropriate involvement of different stakeholders in the organization should be included in the risk management. This ensures that the information that concerns them stays relevant. The involvement of stakeholders also ensures that their views have been taken into account when defining the risk management plan. (International Organization for Standardization 2009, 7-8)

Risk management is dynamic, iterative and responsive to change means that it is continuously assessed and updated. After any incident there should be an investigation through the risk management plan, in case there was something that was overlooked which led to the incident that occurred. There might also be some changes in the risks that the organization has, some might disappear and other new risks might occur. (International Organization for Standardization 2009, 7-8)

Risk management facilitates continual improvement of the organization means that when risk management is part of daily operations in an organization, it should also be in the organization's strategy that the risk management would be updated at the same pace as every other part in the organization. ((International Organization for Standardization 2009, 7-8)

2.1.2 Risk management policy

The risk management policy is a document that defines the organization's attitude, commitment and objectives towards risk management. It usually contains information on the organization's overall risk management assessment, including the commonalities between the organization's whole policy and objectives. It includes the risk management's policies and responsibilities, the resource commitment that will be given to the risk management, and information about who or what unit is responsible for the resources. The risk management policy also provides information and scales for the measuring the risk management and how it will be reported to the decision-making branch of the organization, as well as commitment and information on how and when the risk management policy and framework is checked regularly or after an unusual situation. (International Organization for Standardization 2009, 10-11)

2.1.3 Defining the Context

Defining of context, or environments, allows the organization to define its internal and external framework, which should be taken into consideration while doing risk management procedures. The structure that the internal and external framework gives helps to define the risk criteria and gives a scope for the risk management process. When developing the environment, it should be taken into account what parts of the environment have an effect on risk management. (International Organization for Standardization 2009, 15-16)

The internal environment takes into account everything that has an internal influence on the way that the risk management is conducted in an organization. The internal environment is designed using the same strategy and framework that the whole organization and its actions are based on. The internal environment can include, for example, the organization's structure, objectives, policies, strategies, resources, internal stakeholders, culture and any contracts or legal agreements that have been signed. (International Organization for Standardization 2009, 15-16)

The external environment includes external influences that the organization has to cope with while achieving their goals. The external environment consists of cultural, legal, economic, natural, political and competitive environment, the stakeholders' opinions on risk management and trends that have influence on the organization's objectives. (International Organization for Standardization 2009, 15-16)

The context for this thesis can be found in chapter 1.3. In the chapter there is an example of what the context could look like. The chapter contains both the internal and external context for the organization.

2.1.4 Risk assessment

As shown in Figure 2 ISO 31000 risk management process, there are five different steps in a risk management process. This chapter concentrates on the risk assessment part of the process, which includes risk identification, risk analysis and risk evaluation. During the thesis process we implemented three different risk analysis methods. Brainstorming, preliminary hazard analysis and business impact analysis, these methods are explained during this chapter. The implementation of the methods was conducted in cooperation with the units and the head of security of the Governing Body.

Risk identification tries to identify sources of different risks, areas of impacts, events and their causes and consequences. The target is to make a list of different risks that could have an impact on the Governing Body's strategic objectives. The identification part of the process is critical because if the risks are not identified in this part of the process, they might be

excluded from the other parts completely. Risk identification also considers the consequences and causes from which the risks might have. All of the risks that have consequences to business should be included, even if the risk cause is not in the Governing Body's control. (International Organization for Standardization 2009, 17)

The objective of risk analysis is to create an understanding of the risk and to give an evaluation on the need to treat that risk. The outcome of a risk analysis, when it is finished, is to have the probability and consequences of a particular risk. The risk criteria, which are defined in chapter 3, point out how the probability and consequences give each risk their own specific value. (International Organization for Standardization 2009, 18)

The objective of risk evaluation is to assist the decisive-branch of the organization in deciding which risks should be treated and what is the priority of that treatment. The risk evaluation takes into consideration the risk criteria that were defined to meet the context of the organization. Some of the decisions made during a risk evaluation can lead to further analysis of the risk, but some part of the risks can also be left untreated. This decision is based on the influence of the organization's risk attitude and the risk criteria that have been established. (International Organization for Standardization 2009, 18)

2.1.4.1 Brainstorming

Brainstorming is a method that can generate new ideas. The method is based on free conversation between people that have knowledge about the business and its possible risks. It can be a part of multiple risk assessment techniques, or it can be used alone as a trigger for creativity. Brainstorming can be implemented on every level of the organization. The key element of brainstorming is imagination. Therefore, it can be used in situations where there is no existing data about the organization's risks and problems. (International Electrotechnical Comission 2009, 27-28)

Brainstorming can be implemented both formally and informally. When comparing the informal and formal implementation, the difference is that the formal way is structured and participants have prepared themselves in advance. In the formal process, the facilitator of the brainstorming session prepares the areas for discussion beforehand, the objectives and rules of the session are explained to the participants, the facilitator starts the discussion with a thought and the participants explore different ideas about risks and problems. The facilitator guides the participants towards a new thought or discussion area if the prior discussion has exhausted all its possibilities. The other form of brainstorming is informal brainstorming, which is not structured. (International Electrotechnical Comission 2009, 27-28)

Brainstorming results vary depending on what stage of the risk assessment brainstorming is implemented on. At the risk identification stage, on which it was implemented for this thesis, brainstorming could result in a list of current risks and controls. The strengths of brainstorming include encouraging imagination in order to identify new risks, and solutions that would minimize those risks. Brainstorming is quick and easy to set up and it takes into consideration the views of stakeholders, thus promoting communication with the stakeholders. The limitations of brainstorming include the risk of the participants lacking in skills and understanding of the process. It is hard to demonstrate that brainstorming has been thorough due to brainstorming being unstructured, so it might lack the identification of critical risks or the participants might lack group dynamics, which can lead to the point where some people have trouble stating their opinions. The group dynamic problem can be solved with computerizing the process in a way that the ideas could be given to the moderator anonymously and afterwards discussed in a forum. (International Electrotechnical Comission 2009, 27-28)

2.1.4.2 Preliminary Hazard Analysis

The objective of primary hazard analysis (PHA) is to identify hazardous situations and risks that can have consequences to the organization's business. PHA is usually implemented at an early stage of the project. PHA is useful in prioritizing the existing risks and hazards when performing further analysis or determining when there should be an alternative technique used in the analysis of specific risks. (International Electrotechnical Comission 2009, 31)

When conducting a Preliminary Hazard Analysis the organization has to consider materials that the organization is using in its process and the materials that are produced during that process. The reactivity of materials, and equipment that are used during that process and the operating environment of the process must also be considered. The PHA should be updated during each step of the process, in designing, constructing and testing, in order to make adjustments if any new hazards or risks are identified. (International Electrotechnical Comission 2009, 31)

The results of the PHA include a list of hazards and risks, and recommendations for controlling those risks. The strengths of PHA are that it can be conducted while there is a lack of information and it can detect risks early in the lifecycle of the system. The PHA's limitation is that it is not comprehensive and it does not provide information concerning the prevention of the identified risks. (International Electrotechnical Comission 2009, 32)

2.1.4.3 Business Impact Analysis

The Business impact analysis (BIA) analyses how key disruptions can affect the organization's processes, and it identifies and quantifies the capability that is needed to manage the risks.

The BIA identifies the key processes of the organization, what kind of effect disruptions would have on key processes and how disruptions would affect the organization's business objectives. The BIA identifies the capacity and capability that is needed in order to manage the impact. It also determines how the organization can recover its processes to a previously determined level. (International Organization for Standardization 2009, 42)

The BIA determines the criticality and recovery timeframes of processes and other resources, such as people, equipment, and information technology, in order to ensure the achievement of the organization's business objectives. The BIA can be conducted through questionnaires, interviews, structured workshops or a combination of all previous methods. The objective of the BIA is to create an understanding of the critical processes and the effects of losing key processes, and the required recovery timeframe and support resources. (International Organization for Standardization 2009, 42-43)

The key steps of the BIA are

- confirmation of the key processes
- identification of the consequences of a disruption
- identification of the cooperation between internal and external stakeholders
- determination of the available resources and the resources which are needed to keep the organization operable on a acceptable level after a disruption

For each process there must be a maximum acceptable outage time that represents the maximum time a process can be inoperable and the organization can tolerate it.

The organization must determine the recovery time objective (RTO) for any process. The RTO represents the time during which the critical processes and equipment are to be recovered. The last key step of the BIA is to confirm the current level of preparedness for each key process in case of a disruption. (International Electrotechnical Comission 2009, 43)

The results of the BIA show:

- critical processes and their interdependencies
- documented financial and operational effects from losing critical processes
- resources that the critical processes require,
- outage timeframe for the processes,
- recovery times for key information technology and other elements of the process (International Electrotechnical Comission 2009, 43)

The BIA has the capability to provide an understanding of the critical processes that help an organization to achieve their business objectives. It can offer an understanding of the

required resources for the processes and it gives an opportunity to redefine the operational processes of an organization to create resilience in the organization. The BIA can contain misleading data if the participants in the questionnaires and tests are unqualified for the process, or the group dynamics can affect the final analysis As a result, recovery expectations can be unrealistic or unacceptable and the level of understanding the organization's operations and activities can be difficult. (International Electrotechnical Comission 2009, 43-44)

2.1.5 Communication and consultation

According to the ISO 31000 standard, communication is a part of the whole risk management process. Effective communication ensures that the stakeholders have a clear understanding of the decisions that are taken and the basis on which those decisions are made. The stakeholders also need to be informed why the required actions have to be implemented. The understanding of risks can vary from one stakeholder to another. The stakeholder understands risks based on how risks can be seen in their own business. The perception of the risk that a stakeholder has can have an impact on the decision-making process. (International Organization for Standardization 2009, 14)

2.1.6 Monitoring and review

Monitoring and reviewing is the final stage of the risk management process. During this stage the organization's objective is to confirm that the risk management process is working as intended. The organization must be able to ensure that the controls, which are set out for risk treatment, have an effect, the organization should acquire information for the improvement of their risk assessment. Through analyzing the organization should learn from the events, changes and trends that the organization faces in the future, the organization should detect changes in the contexts and this stage should provide information on possible new risks. The results of this stage should be reported to both internal and external stakeholders, and the results should be used when reviewing the risk management framework. (International Organization for Standardization 2009, 20)

2.2 Emergency plan

The emergency plan is mandatory through legislation in Finland. This chapter of the thesis gives an understanding of what emergency management is as a whole and what the Rescue Act of Finnish legislation requires the emergency plan to consist of.

2.2.1 Emergency Management

There is no organization, or community, that can be immune to the effects of an impact. Organizations can prepare and plan against disasters in order to minimize their effects. Emergency management is the professional way to address the management of disasters. The

most important stage in both risk management and emergency management is identification of the risks or hazards. Through identification of risks or hazard the likelihood and measure of consequences can be set. Emergency management focuses on the risks or hazards that need the help of emergency services to be taken resolved. Those hazards can be fire, flood or severe weather conditions. The emergency services that help organizations during a disaster are the police department, fire department and rescue services. (Haddow 2014, 31)

2.2.2 Rescue Act

The purpose of the rescue act (379/2011) is to improve the safety of people and to reduce the number of accidents. The Rescue Act ensures that if there is a threat of accident or after an accident, people will be rescued, important equipment or facilities salvaged, and the consequences of those accidents are reduced. For organizations, the Rescue Act mandates that organizations, individuals, enterprises and other legal persons must prevent fires and other accidents, prepare for accidents and operations in case of or during an accident, limit the consequences of accidents, construct and maintain civil defense shelters and they must participate in rescue operations. (Finland 2011)

According to the Rescue Act there must be an emergency plan drawn up in case the consequences of risks can be serious, or if the evacuation or safety operations are exceptionally demanding. The occupant of the building is responsible for drawing up the emergency plan. The emergency plan consists of conclusions on the assessment of risks, safety arrangements for the buildings that the operations are conducted in, instructions on preventing accidents and guidelines for actions during dangerous situations and accidents and any measures that relate to self-preparedness when operating in the sites or buildings. (Finland 2011)

2.3 Crisis management plan

The crisis management plan consists of crisis management guidelines, the purpose of a crisis team and its guidelines, crisis communication guidelines and channels for it, and a list of important stakeholders that the Governing Body has. The crisis management plan was developed using earlier plans that had been generated and plans that organizations with similar contexts had created. Crisis is a short chain of events that have an impact on a condition of a system and its effectiveness. Crisis is an event that can occur anywhere and in any form. The crisis might have developed over a long period of time or it erupts rapidly through some accident. It can be process-oriented, which has developed through years, or a sudden rupture, which rapidly bursts out in days, hours or even minutes. Specific types of crises can be economic, political, environmental, organizational, moral or emergency management. (Farazmand 2014, 3-6)

Crisis management is the ability to make choices. It is a way of implementing activities, which have been planned beforehand, in an emergency situation. The objective of crisis management is to minimize the impact of a particular situation on the organization. Crisis management can be divided in to two different sections, the crisis management itself and crisis communication, which is the cooperation with different organizations during a crisis. (Huhtala 2007, 13)

2.4 Business continuity plan

Business continuity planning (BCP) is planning for the future events that could have an impact on the organization's operations. These impacts, depending on the country, are related to extreme weather, terrorism, civil emergencies, fires and different pandemics. The process of the BCP identifies possible threats that could have an impact on the organization's business operations, and what those impacts affect, if realized. (Hopkin 2011)

The business continuity plan is actually a document containing a collection of plans that are designed for specific events which could interrupt the organization's business operations. The objective of business continuity is to identify the threats against the organization's different operations, and to mitigate the effects of those threats. (Hotchkiss 2010, 1-2)

2.4.1 Business continuity management system

As mentioned before, the business continuity plan is a set of different plans that are designed to respond against incidents which might interrupt the business operations of an organization. The business continuity management system is a collection of everything that has something to do with business continuity. It consists of arrangements to ensure roles, responsibilities, capabilities, a collection of data and different analyses, which when combined give the organization the capability to respond to an incident in the manner that has been designed in the BCP. (Drewitt 2012, 43)

As an example nowadays, certain businesses, like companies listed in the London Stock Exchange in the United Kingdom, are required to maintain a business continuity management system. Business continuity management provides the organization with an opportunity to think about the threats and risks which can face the organization's business operations. During the thinking stage, the organization can work on the risks and try to minimize their impact. Some organizations today, also request information about business continuity from their suppliers. Therefore, a business continuity management system provides an organization with a viable edge on its competitors. (Drewitt 2012, 18-25)

2.4.2 ISO 22301

ISO 22301 is the international standard on requirements for the business continuity management system. As previously mentioned, both the risk management plan and the business continuity plan were created to match the requirements and structure of the ISO standards. The objective of ISO 22301 is to generate and develop a business continuity management system in order to protect an organization against the impact and consequences of specific risks. ISO has an objective that all of the standards could be implemented by any organization. (International Organization for Standardization 2012, v)

The ISO 22301 requires the business continuity management system (BCMS) to consist of a policy containing people with specific responsibilities, documentation of evidence that can be audited, and any other material that is related to the business continuity management process and a process that consists of policy, planning, implementation, evaluation, review and improvement. (International Organization for Standardization 2012, v)

The ISO 22301 standard uses the Plan-Do-Check-Act (PDCA) model for developing and implementing business continuity management.

The Plan-phase of the model establishes the framework for business continuity. It provides the organization's continuity policy, objectives, targets, procedures and processes, which when operating normally, produce a system that is aligned with the organization's overall strategy. (International Organization for Standardization 2012, vi)

The Do-phase, implements all of the procedures of Plan phase. (International Organization for Standardization 2012, vi)

The Check-phase ensures that the organization monitors and reviews the business continuity process and reports to the higher level management of the organization, which decides the appropriate actions to improve the system. (International Organization for Standardization 2012, vi)

The Act-phase of business continuity means that the organization maintains and improves the business continuity management system by implementing the actions that were decided during the management review, and by readjusting the scope and objectives of the business continuity management system. (International Organization for Standardization 2012, vi)

3 Process

This chapter gives an understanding how all of the methodology was implemented for the security management system of Suomenlinna. The project was started, as shown in Table 1, in March 2014. During March the framework for the security system was created and the Governing Body's existing work on the plans was analyzed. In April the creation of the risk management plan started. During April and May the risk assessment was implemented with different units of the Governing Body, and the results were analyzed. The risk management plan was finished in June, but guidelines how the risk assessment could be implemented in the future were created in September. During summer of 2014, June, July and August, the emergency plan, crisis management plan and the business continuity plan were created and added to the security management plan. After the risk assessment guidelines were finished, in September, the risk management system was given to the board of the Governing Body for analysis and approval.

The reason why the plans were created using law requirements and ISO standards came from the Governing Body of Suomenlinna. Because the Governing Body is a governmental agency, they need to fill requirements from the legislation of Finland. The Security Specialist in the Governing Body, Jyri Paasonen, wanted that the Risk Management Plan and the Business Continuity Plan would follow the requirements of ISO standards so they could be reviewed in the future.

Month	March	April	May	June	July	August	September
Beginning of the project	■						
Creating of the framework	■						
Analyzing the existing work	■						
Risk management plan		■	■	■			■
Risk assessment (Brainstorming, PHA, BIA)		■	■				
Emergency plan				■	■		
Crisis management plan					■		
Business continuity plan					■	■	
Boards approval							■

Table 1 Timetable for the project, year 2014

Before this process, of generating the system begun, there were parts of all the plans ready in Suomenlinna. The idea was to generate a clear package of all of those parts, and create a management system for the future.

After generating the idea of the thesis, the process started with generating the risk management policy. The risk management policy was the framework for the rest of the process. The policy was constructed in a way that linked it to the organization's whole

strategy. Then it defined the environment where the organization manages its business. The policy also explained how communications inside the organization and with the stakeholder should be conducted when communicating about risk management. The policy has information on reporting and measuring, risk analysis, and evaluating. It also contains the policies for crisis management, workplace health and safety, and continuity management.

The risk management plan already had the framework in place. All that was needed was the implementation of the risk assessment methods. Brainstorming had been implemented prior to starting the project behind this thesis, but the results had to be analyzed more carefully. After the primary hazard analysis, it was decided that the results would be taken to each of the four units of the Governing Body and they would give their input to the risk management. After all, as mentioned previously, one of the principles for successful risk management is to involve the whole organization in the risk management process. Using a risk assessment form meant it was easy to gather the results from each of the units and insert them into the analysis which was done for Suomenlinna.

Risk	_____				
Risk profile	_____				
Description	_____				
	_____				
	_____				
Likelihood	1	2	3	4	5
Severity	1	2	3	4	5
Reason	_____				
Consequences	_____				
Suggested actions	_____				
Actions taken	_____				
Responsibility	_____				
Unit	_____				

Table 2 Risk assessment form
(Paasonen 2009. 163)

Risk profile is a specific description of a particular set of risks. These risks can be related to the whole organization, part of it or as otherwise defined. (International Organization for Standardization 2009, 5) In Suomenlinna, the risks were divided in four different categories, and all of them are related to the whole organization. The four categories are operational risks, strategic risks, hazard risks and economical risks.

Strategic risks are risks that are linked to strategic objectives, the context of the organization or the location's legislation.

Operational risks are linked to leadership, decision making, communication, processes, employees, equipment or premises.

Hazard risks are associated with property, nature, personnel safety or facility safety. Hazard risks can be seen as workplace health and safety risks, fire hazards, and other accidents or natural disasters.

Economic risks can be liability risks, investment risks, credit risks, market risks, and all other risks that are involved in the organization's business operations.

Risk criteria are the terms of reference, based on the context of the organization that the significance of a risk is evaluated against. The local laws, policies and requirements, as well as international standards, can form the basis of risk criteria. (International Organization for Standardization 2009, 5). For Suomenlinna's risk criteria, this thesis used criteria made by the Finnish State Treasury. From the matrix which had been developed by the Treasury, the consequence level was determined. The consequence stages are insignificant, small, moderate, considerate and catastrophic. The probability of a risk was calculated from events that had happened in the past, and then the probability of the risk was discussed in a brainstorming session until a consensus was reached. There are five different stages of probability: almost certain, likely, possible, unlikely and rare.

After determining both the probability and consequence, the results are fed into a consequence/probability matrix, which can be seen below in Table 3. This matrix is used to give priority listing of the risks. It is usually used after the risk identification stage when many of the risks have been identified in order to determine which risks need treatment first, or which need to be taken for further analysis. (International Electrotechnical Comission 2009, 84)

Consequence					
Probability	**Insignificant (1)**	**Small (2)**	**Moderate (3)**	**Considerate (4)**	**Catastrophic (5)**
Almost certain(5)	Moderate (5)	Great (10)	Serious (15)	Serious (20)	Serious (25)
Likely (4)	Moderate (4)	Great (8)	Great (12)	Serious (16)	Serious (20)
Possible (3)	Low (3)	Moderate (6)	Great (9)	Great (12)	Serious(15)
Unlikely (2)	Low (2)	Moderate (4)	Moderate (6)	Great (8)	Great (10)
Rare (1)	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

Table 3 Consequence/Probability matrix

The emergency plan was created to meet the requirements of the Finnish Rescue Act (379/2011). The law requires that an organization must prepare personnel to protect persons, property and nature, and to perform any rescue operations that they are capable of. The plan, which was created for the Governing Body of Suomenlinna, consisted of the context of the organization, a list of all the properties that the Governing Body has and the requirements, which are based on law and governmental decrees on natural and chemical safety. For every building that the Governing Body owns, a specific emergency plan was created using the original organizational plan and making new editions depending on the building. After this thesis process was completed all of the buildings that Suomenlinna owns on the islands, had their own emergency plan. The emergency plans which were made for specific buildings contained information on what exists in the building, the escape routes and route to the neares evacuation area. The organizational emergency plan contained information from the rescue act and what should be done on the organizational level, in case of an emergency.

The crisis management plan was created after the risk management plan was completed. For the crisis management plan, previous crisis management guidelines that existed in Suomenlinna were used, with minor modification to suit present needs. The crisis communication guidelines were designed from the organization's normal communication guidelines and there was an effort to learn from previous mistakes that were made during crisis communication. From these sources it was possible to create a clear, simple set of guidelines and a plan on what to do after the emergency plans guidelines and action requirements have been completed.

The process of business continuity management is similar to the risk management process. The Business Continuity Plan was the only plan which didn't have any material in the

organization in the beginning. With the guidelines and requirements that were given by the ISO 22301 standard and the objectives given by the framework, the plan was created. The first stage was to identify the crucial processes which can have an effect on the continuity of the organization. After the processes were identified a few risks from the earlier risk analysis was taken into closer analysis in order to protect the crucial processes that the organization has. This analysis is called Business Impact Analysis (BIA). After the BIA was completed the results were given to Mr. Paasonen for approval, and added to the Risk and Security Management System. Suggestions on what to do in order to minimize the effects of the risks, we gathered ideas around the organization to be given to the board for them to make the final decision on the actions for business continuity.

One of the main reasons for Suomenlinna in this project was the need of a management system on overall security. The Governing Body wanted that they would be able to see how these guidelines and plans had been created, in case someone would need to know in the future. When the people who have been along this thesis project from the organization's side, leave the Governing Body, the new employees can go back to the ISO standards, laws and regulations to see how and why the system was made the way that it was made for this thesis process. This is why it was made to be a specific management system based on ISO standards.

This thesis' research method was action research. As mentioned in the action research chapter, the method has the objective of giving a person an understanding of something that they are doing, or finding a new way of doing something which has been done in the past. From the very beginning the research on this Risk and Security Management System was action research. It was impossible to find existing material on this subject from Finland. So it was decided that the research would be conducted on an international level, and then through own perception it would be changed to fit the context of the Governing Body of Suomenlinna. That is what action research is, through understanding generate a new way of doing something.

The system was completed in September of 2014. The feedback which was given by the Governing Body was positive. The risk and security management system was given to the board of the Governing Body for final approval.

4 Conclusion

The objective of this thesis was to create a working security management system for the Governing Body of Suomenlinna. The Risk and Security Management System consisted of four different stages:

a) A Risk Management Plan for identifying the current state of the organization and what risks are there on each of the processes the organization has,
b) An Emergency Management plan to minimize the casualties and consequences of the realization of risks,
c) A Crisis Management Plan for the management of the organization during a crisis situation and the organization preparations of procedures for what to do when the crisis and its immediate consequences have passed and the organization has to commence e.g. crisis therapy for their employees,
d) A Business Continuity Plan in order to restore the business operations of the organization after a disruption to a previously set level.

One of the most important phases in developing a Risk and Security Management System, is to prepare and plan the process carefully. In the planning phase of this study, it was decided what the plans would be based on. The plans were based on existing standards on the subjects as well as Finnish laws and decrees that regulate for example emergency planning.

During the creation of this study it was identified that the period of time, which is given for the creation of a similar system, must be flexible. There has to be time in process to read through what has been created and make modifications along the way. The Governing body of Suomenlinna insisted that all of the plans could be understood by each employee. During the process it was understood that implementing the plans might be difficult for employees, therefore the Governing Body also wanted to make guidelines for implementation which could be given to every employee.

People working in the security branch of the organization can't create a Risk and Security Management System without support from other parts of the organization, for example the communications branch must be involved in the process when developing the crisis management plan. It is important to involve several members of the organization, from different fields, in to the process, in order to ensure the effectiveness of the system.

The Risk and Security Management System is great for any size of organization. When creating the framework, policy and strategy, properly the organization can decide the requirements and resources for the system depending on the organizations possibilities and requirements.

During the creation of this thesis it was identified that if the project is well planned, the creation of a similar system is not hard. Following the ISO requirements and the laws and regulations which exist here in Finland, the system can be created in any organization. With the help of the Risk and Security Management System an organization can identify what is

threatening them and what can be done to prevent those threats. This will help the organization to survive for years to come.

Using the standards and legal requirements to create the Risk and Security Management System will give the organization framework which has been proven sufficient and it will give the organization also a reference which can be presented to a wider audience. In the future when the employees have changed, new employees can also go back to the material and see how the system has been created and on what foundations.

As mentioned in the text this thesis concentrates on the ISO standards and legal requirements. ISO standards were chosen because they have been developed and are used in multiple countries across the world. During the creation of the Risk and Security Management System, any other standard could have been chosen, but the Security Specialist in the Governing Body decided that the ISO standards should be used.

The Risk and Security Management System is also useful for the future of the organization. When the Risk and Security Management System has been done properly, a timetable for future use and development can be set. The timetable defines when to update the different plans in the coming years. For that reason modifications can be done every year without doing the plans all over again. Building the system this way, it will reduce the amount of resources that would have to be put into the security branch of the organization.

From the thesis' author's point of view the Risk and Security Management System is a great solution for any organization. The framework can be built depending on the organizations own resources. The framework also gives information on what grounds the organization is on, what the risks for the organization are and what should be done in order to reduce the risks that might lead to the organizations bankruptcy or equivalent end of business.

For future development of this study, it could conducted using the objective of trying to compare different standards and legislation, on how to generate this. The objective could be to create a similar system using different standards, and trying to create a system which would answer to any organization's needs in different parts of the world. The implementation which was shown in this thesis had the objective of answering how a Risk and Security Management System can be generated, using ISO standards and Finnish legislation. Therefore it is only comparable here in Finland. Trying to make a general system, which would work around the world, would have difficulties fulfilling all of the law requirements in different countries.

References

Alana, A. Slater, T. Bucknam A. 2012. Action research for business, non-profit and public administration: a tool for complex times. London: Sage.

Drewitt, T. 2012. Everything you want to know about business continuity. Ely: IT Governance.

Farazmand, A. 2014. Crisis and Emergency Management: theory and practice. 2nd edition. Florida: CRC Press.

Finland. 1989. 168/1989 Asetus Suomenlinnan hoitokunnasta. Accessed 19.9.2014. http://finlex.fi/fi/laki/alkup/1989/19890168?search%5Btype%5D=pika&search%5Bpika%5D=suomenlinna

Finland. 2011. 379/2011 Rescue Act. Accessed 15.9.2014. http://finlex.fi/en/laki/kaannokset/2011/en20110379.pdf

Finnish Standards Association. 2014. Accessed 29.9.2014. http://www.sfs.fi/en/sfs_in_brief

Haddow, G. Bullock, J. Coppola, D. 2014. Introduction to emergency management. 5th edition. Burlington, MA: Butterworth Heinemann. (31)

Hopkin, P. 2012. Fundamentals of Risk Management: understanding, evaluating and implementing effective risk management. 2nd edition. London: Kogan Page.

Hotchkiss, S. 2010. Business continuity management: in practice. Swindon: British Informatics Society.

Huhtala, H. Hakala, S. 2007. Kriisi ja viestintä. Helsinki: University Press Finland.

Institute of Risk Management. 2002. A Risk Management Standard. Accessed 18.11.2014. http://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

International Electrotechnical Comission. 2012. ISO 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. 2nd edition. Switzerland.

International Electrotechnical Comission. 2009. IEC/ISO 31010: Risk management – Risk assessment techniques. 1st edition. Geneva: IEC.

International Organization for Standardization. 2014. Accessed 24.9.2014. http://www.iso.org/iso/home/about.htm

International Organization for Standardization. 2009. ISO 31000: risk management – Priciples and guidelines. 1st edition. Switzerland.

International Organization for Standardization. 2012. ISO 22301: Societal security – Business continuity management system – Requirements. 1st edition. Switzerland.

Kemmis, S. 2010. What is to be done? The place for action research, Eduactional Action Research. Australia. Accessed 18.11.2014. http://www.tandfonline.com/doi/pdf/10.1080/09650792.2010.524745

Niemelä, M. Pirker, A. Westerlund, J. 2008. Strategiasta tuloksiin – tehokas johtamisjärjestelmä. Juva: WS Bookwell Oy.

Paasonen, J. 2012. Oppilaitoksen turvallisuusjohtaminen. Helsinki: TIetosanoma.

Suomenlinna. 2014. Management Plan. Finland.

Walker, D. 2012. Mass notification and crisis communications : planning preparedness, and systems. Florida: CRC Press.

Tables

Figures