Tuire Siitonen

INFORMATION SECURITY RISK MANAGEMENT
Ensuring the continuity of it in SMEs

Master's thesis

Master of Engineering

Master's Degree Programme in Cybersecurity

XAMK

South-Eastern Finland
University of Applied Sciences

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)	**Degree**	**Time**
Tuire Siitonen	Master of Engineering	May 2020

Thesis title Information security risk management – Ensuring the continuity of it in SMEs	68 pages 4 pages of appendices

Commissioned by
the Union of Professional Engineers in Finland

Supervisor
Marko Oras

Abstract

This thesis studies information security risk management from small and medium-sized organizations' point of view. The purpose was to discover ways to improve the continuity of the implemented information security risk management practices.

The thesis was a practice-based thesis commissioned by the Union of Professional Engineers in Finland, where information security risk management was implemented recently. Very soon, it became obvious that the continuity of the risk management process is at risk of being ignored. This is also the observation of experts involved in information security risk management.

In the theoretical part of the thesis, the risk management process and ISO 31000 standard focused on the benefits they offer for information security management. Also, in one of the chapters, four experts in the field were interviewed, and their answers, observations, and opinions about information security risk management and the importance of continuity were analyzed. The continuity perspective was also studied in the empirical part, where the implementation of information security risk management for the Union of Professional Engineers in Finland, was introduced.

The importance of the role of top management in information security was emphasized by many sources. Because of this, the thesis includes a theoretical chapter focused on the engagement of top management.

In conclusion, there seem to be many ways to improve the continuity of the information security risk management from the top management to the employees. Awareness of the benefits of risk management is the key to improve the process and its outcome.

Keywords risk management, cybersecurity, information security, ISO 31000 standard, information security management, engagement of top management, VAHTI risk management tool

CONTENT

TERMS AND ABBREVIATIONS

Azure AD – Microsoft Active Directory is cloud-based identity and access management service

CIO – Chief Information Officer or information technology director

COSO – The Committee of Sponsoring Organizations of the Treadway Commission is a joint of five American private-sector organizations which provide guidance on e.g. risk management

CRM – Customer Relationship Management is technology for e.g. handlining customer data and service requests

ERM – Enterprise Risk Management is a strategy for enterprises to identify, assess and prepare for hazards

GDPR – General Data Protection Regulation is regulation in EU law which helps to protect individual's privacy and personal identity data

ISO – International Organization for Standardization is international organization providing various standards

ISPE – The International Society for Pharmaceutical Engineering is an association offering to its members guidance for e.g. technical advancement

POA-method – POA is a method for risk identification (In Finnish: Potentiaalisten Ongelmien Analyysi)

SFS - Finnish Standards Association is organization which operates under ISO. It e.g. participates developing standards and provides selected standards in Finnish.

SME – Small and Medium sized Enterprises. In Finland it consists organizations which have 250 employees or less.

VAHTI – The Government Information Security Management Board set up by Finnish The Ministry of Finance

1 INTRODUCTION

The objective of this master's thesis was to study information security risk management. The factors that make information security risk management effective, systematic, and especially an ongoing process is identified among the ways which would ensure sufficient information security risk management.

I work in a small IT department for the Union of Professional Engineers in Finland, whereas in many other organizations, information security and ways to implement it efficiently are continuously discussed. Especially in SME, such as the Union of Professional Engineers in Finland, there are usually not enough resources to cover all possible digital threats and obtain the required knowledge to acquire a very recommended or advertised security solution. In this context, risk management can be the tool for prioritizing security systems and functions and redirecting resources to the acutely most needed operations.

As part of my job in the Union of Professional Engineers in Finland, I have received an opportunity to be engaged in introducing information security risk management as well as overall risk management method leading a risk management coordination team. Information security risk management is led by the IT-department and not assigned by the top management of the Union of Professional Engineers in Finland.

1.1 Scope and background of study

Risk management subject will be studied from Finnish SMEs' point of view, thus including the commissioning organization the Union of Professional Engineers in Finland is included. In Finland, SMEs are defined as organizations that employ no more than 250 people and a turnover that does not exceed 50 million euros (Tilastokeskus n.d.).

Risk management is studied from the IT department and information security point of view. Information security risks comprise various scenarios where sensitive or classified information can be endangered.

Often from my experience, the terms information security and cybersecurity are used interchangeably as synonyms. In this thesis, the term information security is used to emphasize the concept of information and data. In the commissioning organizations, as in many other organizations, the protection of valuable and critical business data is extremely important.

It may be challenging to find solutions for better information security for SMEs as they might not have as many resources as larger enterprises. However, this does not mean that their security level should be any weaker. The implementation of systematic and reliable information security risk management might be a cost-effective method to improve security in any organization.

Information security consists of, for instance, devices, services, programmes, human behaviour, and security management. There are tools and standards helping to discover, manage, and maintain processes related to these security factors. SMEs can benefit from risk management at least as much as larger enterprises, as consequences can be much more severe. If a serious incident occurs, it can run the business down, and SME may not have enough resources to recover.

There are many reasons which can lead to a data breach, and there are, similarly, several actions for preventing breaches. Some of the solutions require economical investments; some do not. It is common that some of the solutions are controlled by the IT department, while some are not. All these factors require systematic management, and as will be demonstrated in this thesis, risk management is one solution. Albeit ensuring total security in the digital world is impossible, it is still possible to minimize the risks and soundly prioritize possible remote resources.

From this study, SMEs which offer digital platforms were excluded, IT or security services to other companies. Furthermore, the focus will be on companies that have their own IT department or at least an IT manager.

1.2 Introducing the commissioning organization

The commissioner of the thesis is the Union of Professional Engineers in Finland. Its main purpose is to act as insurance in case of unemployment and assist in personal development by offering, for example, legal advisory and career coaching. Through various membership organizations, there are approximately 70,000 members in the union. The number of members and the membership data is considered to be the most valuable asset to the union (the Union of Professional Engineers in Finland, n.d.).

Among its approximately 80 employees, the union has its own IT department consisting of an administrator and three other IT professionals. The team is responsible for various tasks, ranging from technical issues to developing systems and information security, including risk management, together with the organization’s IT manager.

According to Kari Malinen (2020), there have been no serious information security incidents been reported in the past ten years. This is due to a good level of know-how among the staff and the fact that it may be very little incentive for anyone to breach the systems of the union.

As the union processes sensitive information, the security of the systems and operation is very important. In the IT department, risk management has proved to be a good tool in anticipating and analyzing potential threats and prioritizing security-related actions and resources. Information security risk management is implemented with the help of a risk management consultant.

Notwithstanding having the information security risk management consultant aiding with implementation is useful, as it has been recognized that the information security risk management process at the Union of Professional Engineers in Finland might be in danger to remain as a single project and responsibility of only the IT manager. Moreover, risk management may be completely forgotten, and all efforts may prove pointless. This challenge with continuity was a strong motivation for focusing on the subject and studying the possible primary causes and solutions for reducing problems and in operation obstacles.

1.3 Methods of research

For this thesis, I will do the research by studying different literary resources such as books and journal articles related to IT risk management. Related standards and available web-resources were studied as well. In addition, four risk management professionals who have several years’ experience in information security risk management were interviewed. In the commissioning organization, I work with developing information security risk management, which offers me practical experience that can be utilized with the study.

2 INFORMATION SECURITY

In this chapter, the starting point of the study, and the reason why the topic is interesting, is introduced.

The thesis was commissioned by the IT manager of the Union of Professional Engineers in Finland. The practice of information security risk management was new to the organization as it has only recently been implemented. First, the possible problem areas in risk management concerning information security had to be determined.

Two professionals of the field, Petri Välkki, and Jan Zilliacus were consulted in this matter, and both stated that in their experience, when working with different kinds of customer organizations, one of the major problems is that even if an SME has implemented some sort of risk management system, it is the often inconsistent process in a continuous state of development and usually is the responsibility of only one person, typically the IT manager.

Often, I learned that the fewer there are people involved in the risk management process, the more likely it will peter out, and all financial and time resources put in the effort may be wasted. As it was deemed highly possible that this challenge might concern the commissioner as well, the continuity point of focus in the thesis was chosen to be examined.

2.1 Information security in general

The main goal of information security is to ensure the confidentiality, integrity, and availability of the information. The term cybersecurity is commonly used to refer to the protection of vital functions, for example, in society (Valtionvarainministeriö n.d.c).

Information security has existed nearly as long as humankind and first related to information on the best hunting areas or the most effective ways to manufacture weapons (Soo Hoo 2000, 2). Today, information security is most commonly associated with the digital world. Security issues concern everyone and are above all political and strategical matters. When making high-level decisions, solutions, and strategical approach, they should be taken into consideration. We have become increasingly dependent on digital platforms, services, and solutions. One of the global megatrends is that better security in the digital environment is consistently needed as economies, societies, businesses, and our lifestyle depend on it. As we are able to benefit from the digital world without geographical and temporal limits, at the same time, we become very vulnerable (Limnéll, Majewski et al. 2014, 8). Because of this, the aspect of vulnerability, security, and usability have a constant fundamental tension between them. Usability requires a free information flow, while security is particularly focused on tightening the control of information and access (Soo Hoo 2000, 3).

It should be observed in the work environment that information security may be jeopardized by various factors in the digital processes, and the consequences can be critical if there are no proper ways to anticipate and tackle the problems. It can be challenging to take concrete actions and make changes without compromising the usability or effectiveness of the systems and services. Information security may be, in most cases, secondary to the business proper.

Information security can be compromised because of several reasons, for instance, system malfunction, negligence, criminal attack, or even natural phenomena.

As it has been frequently stated, the question is no longer if an organization will be breached but rather when. For instance, Rothrock et al. (2018,3) claim that it is inevitable that the organization’s network will be penetrated sooner or later. Because of this, the resilience of the organization has become as important as sufficient security status itself. If there is adequate organizational resilience, and a breach occurs, the organization can respond to the incident more efficiently, and the recovery is more likely to succeed.

The implementation of effective risk procedures can positively affect the level of resilience (Harris & Mitchell, 2012, 4).

2.2 Most common risks

There are a few etymological definitions for the word risk. For example, one of the resources explains that the word “risk” is said to have originated from the ancient Latin word *risiciare*, which can be translated as “dare” or “run into danger” (Online Etymology Dictionary, n.d.).

Today, in colloquial language, the word is used to describe mainly negative deviation, hazard, or uncertainty. More officially, the word means the effect of the uncertainty towards objectives. It can be negative, positive, or both, thus, a risk can create both threats and possibilities (SFS-ISO 31000:2018, 6).

Kuusela and Ollikainen (2005, 16) state that considering the etymology of the word risk and its origin from the word dare, the concept can include choices and alternatives in addition to possible losses. Because of this, it is relevant to notice that assessing the risk can consider being also the question of choosing and daring.

Jordan and Silcock (2005, 1) remind that every business requires taking risks, and it is essential to do so, as being passive and avoiding taking, can be a risk in itself. The risk may not appear immediately frightening, and because of that, its presence may go unobserved.

Nonetheless, the risk is accompanied by uncertainties and the possibility and threat of losses. Due to this, it is only natural that risk is often experienced as frightening. This may be emphasized if the risk itself is uncontrolled, not precise, not sensually detectable or/and it is not taken voluntarily (Kuusela & Ollikainen 2005,17,28).

Järveläinen et al. (2017, 6) claim that an active security culture in the organization that enables the detection of problems, and potential risks at an early stage, can offer mindfulness. Being prepared for the difficult times when risk may be realized is part of mindfulness as well. Mindfulness can be comprehended here as being conscious and present and having a sort of sensory awakening, for instance.

These statuses are something that risk management can provide, and these cannot always be implemented just with technical solutions or technological improvement.

When managing the operation in an organization, it is relevant to consider various information security related detriments because these can result in serious business risks and economical losses. These can also cause negative impacts on organization’s operations, assets, employees or partners (Porvari 2012, 2; U. S. Department of Commerce 2012, 6).

2.3 Risk management and ISO standards in general

The Finnish Standards Association (SFS-ISO 31000:2018, 26) defines risk management as follows: “The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation, and supports the achievement of objectives.”

The nature of risk management implies a systematic and coordinated process that can be used to control and manage the operation. With proper risk management, it is possible to make informed decisions based on analysis and only take risks. A well-targeted risk management system helps to determine strategies and goals (SFS-ISO 31000:2018, 5-6).

Search from the Internet shows that there are numerous tools, frameworks, and methods to manage risks in organizations. Some of the methods are international standards that offer guidelines and specifications, for example, ISO standards, and some of them are provided by commercial companies (Capterra. n.d).

The ISO standards are offered by International Organization for Standardization (ISO) and created by professionals from all over the world to help organizations to operate systematically and effectively (International Organization for Standardization, n.d.a).

In this thesis, the focus is on introducing the ISO 31000 standard. This is because the implement risk management tool implemented in the commissioning organization is based on this standard.

Another option would have been standard ISO 27000, which is more specifically based on information security. Ferreira explains (2018) that ISO 31000 serves as a master standard for all other ISO risk management standards such as ISO 27000, providing general guidelines and focusing mainly on describing the management process.

The commissioner was especially interested in comprehensive means for managing risks, regardless of what the field of risk is. They expressed a desire to use the same standard for managing, for example, financial risks or operational risks. ISO 31000 standard was chosen to proceed with because it does not take a stand on any particular field or industry.

2.4 Information security in Finnish organizations

It is not often enough that only the IT department understands the risks and the proper use of risk management tools. The operation with the processing of risks should be extremely systematic, consistent, and uninterrupted. In this chapter, some of the challenges which are introduced, concern this matter.

According to the Finnish business and security related report by Susi (2018, 3), it is quite challenging to measure financial losses when it comes to security or lack of it in organizations. Although there are no exact numbers, it is still apparent that insecurity and an insecure environment can decrease the trust of customers and investors, for example.

The report by Susi (2018, 2) bases on a survey which was answered by nearly 300 Chief Information officers (CIOs) and decision-makers from Finnish organizations. Most of the respondents worked in supervising positions employing not more than 50 people.

The survey (Susi 2018, 3) reveals that Finnish organizations have strong trust in the existing level of security with 95% of respondents finding Finland to be safe a location of business point of view, and 86% claiming that the operations in their organizations are performed in a secure manner in their organization. However, the overall security status in the future concerns decision-makers, especially with reference to the trade and industrial sectors. The most concerning issues are international security policies (79% of the respondents), immigration and integration of immigrants (58% of the respondents), and cybersecurity (46% of respondents).

The survey respondents are generally concerned about cybersecurity attacks towards society and companies. In addition to this, the respondents are not entirely confident about the capabilities of Finnish authorities to respond to information security threats (Susi 2018, 13).

Porvari (Porvari 2012,2) states that security is an essential part of the organization’s operation in many fields, and it has often been considered a separate aspect of management. According to Porvari, this is not enough as security should be thoroughly implemented and integrated into the business management procedures.

Soo Hoo agrees with Porvari (Soo Hoo 2000, 01) and says that in modern information security, risk management is used to assigned to concern only IT departments and computer security experts. However, as society’s dependence upon information systems has grown and the human factor in security issues is significant, many organizations have started to transfer this responsibility from the IT department to in-house risk management specialists. Alternatively, the information security has been outsourced neatly entirely.

Zilliacus (2019), however, understands why information security is often the responsibility of information management or an IT team. As information tends to be in digital format, the IT teams know and control, for instance, how and where the data or information is stored and what the general architecture is.

In modern ways of processing information, digital surfaces have reached every operation and team in an organization. This is the case in the Union of Professional Engineers in Finland as well. Because of this, information security issues also concern other teams and functions, rather than the IT department alone. The IT team cannot be represented at all meetings, which concerns digital services information security or security risks that have been observed.

One of the challenges is how to get the security issues and risks acknowledged in the organization’s projects, decision making, and daily operation even if experts of system or information security are not available.

3 RISK MANAGEMENT

In this chapter, risk management is studied in-depth, and the standard ISO 31000 risk management is introduced.

The most common way to manage the business is through processes, which tend to include a significant amount of information. The primary purpose of the processes is to manage information flow and utilize it effectively in the actions (Porvari 2012, 86). Recognizing risks and threats and fast response requires a systematic method. Companies are searching consistently for a tool that would be the most efficient (Väisänen 2018).

In the commissioning organization, like in other organizations, information security risk management is commonly the responsibility of the IT manager. One of the challenges of this position is to balance between managing risks and not to impede the spirit of innovation. The current trend creates pressure for CIOs to prefer innovations over risk management, which brings an additional challenge to daily operations (Pervilä, 2018).

In the end, it must be taken into account that it is impossible to gain complete security with risk management or any security system, but it is possible to affect positively single risks with individual security actions (Puolustusministeriö 2015, 9). Sometimes, the risk level must be accepted and weigh it against gained profits and efficiency.

The implementation of risk management in an organization be the result of external motivation. For instance, risk management can be obligatory in order to be granted the ISO-certificate required by authorities or shareholders. In some cases, a merited certificate may be a remarkable business advantage, for instance, compared to competitors. However, it is good to recognize that not every available method, tool, or standard may be suitable for certificate purposes.

If the case is that risk management is implemented in order to acquire a specific certificate, it should be notified in risk management documentation (Puolustusministeriö 2015).

Next, the ISO 31000 standard will be introduced. It is used in the commissioning organization. The introduction presents the expected the must be taken measures if risk management is to be implemented in accordance with the standard.

3.1 ISO 31000 standard

The ISO 31000 standard, Risk management – Guidelines, was developed by ISO (International Organization for Standardization, n.d. b). ISO is an independent and non-governmental international organization whose members, experts in different fields all over the world, develop standards in cooperation. The ISO 31000 standard was published in 2018, and it is applicable to every organization regardless of its size, sector, or activity (SFS-ISO 31000:2018, 23).

The ISO 31000 standard divides risk management to three tiers: principles, framework, and process (SFS-ISO 31000:2018, 24), as presented in Figure 1. In the next chapter, these three tiers will be introduced separately.

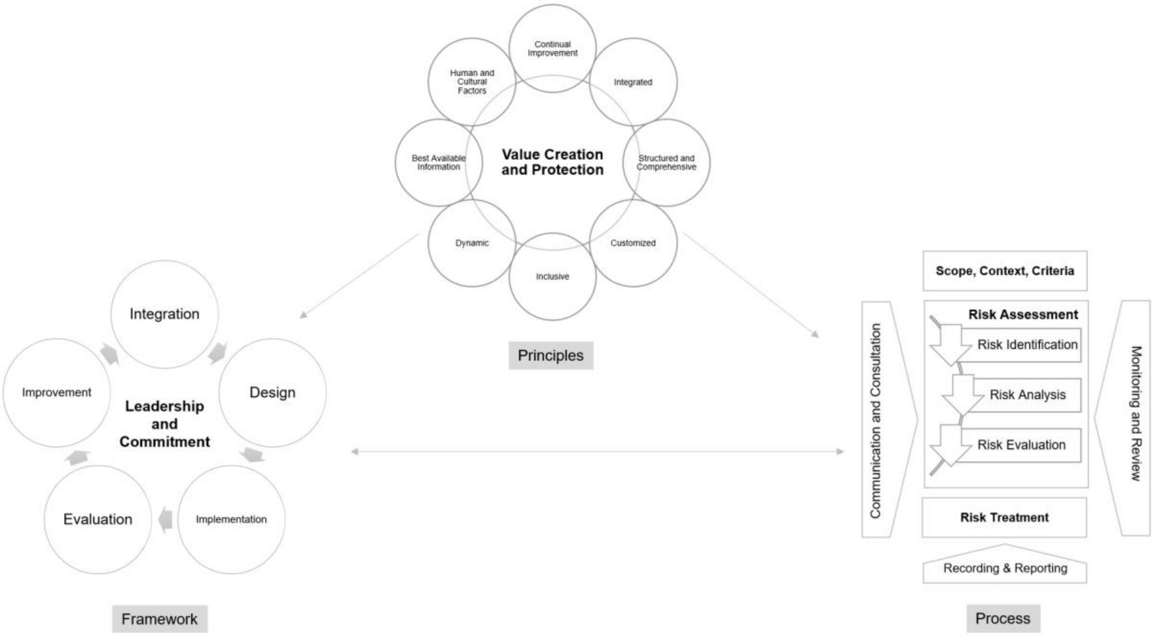


Figure 1. Three tiers in ISO 31000 standard

With these three tiers, the risk management team has a way to outline available recourses, the operational environment, and regularities in which the organization operates.

3.1.1 Principles

Principles, illustrated in Figure 2 (SFS-ISO 31000:2018, 27), create the foundation, consisting of eight elements for the organization’s risk management. As the organization is starting to implement risk management, these matters should be kept in mind and considered in the risk analysis process.

All the elements of the principles are presented in the ISO31000 standard documentation (SFS-ISO 31000:2018, 27-28).

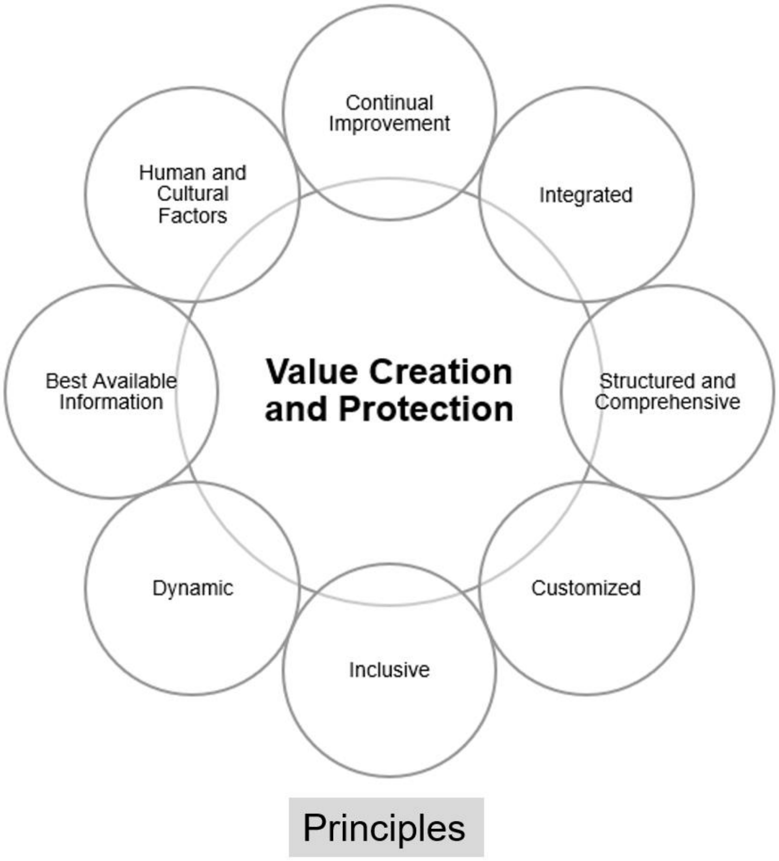

Continual Improvement
Human and Cultural Factors
Integrated
Best Available Information
Value Creation and Protection
Structured and Comprehensive
Dynamic
Customized
Inclusive
Principles

Figure 2. Principles according to ISO 31000 standard

a) Integrated

Risk management should be an integral part of organizations’ daily operations and management systems.

A concrete example could be the regular and systematic reporting of information security-related affairs. The report should reveal the detected threats, required resources, and person responsible. It should also take a stand of schedule, the solved issues, and perhaps most importantly, what is the order of priority of the discovered issues (SFS-ISO 31000:2018, 27-28).

b) Structured and comprehensive

A commonly approved, comprehensive, and structured operations model and approach to risk management ensure consistent and comparable results (SFS-ISO 31000:2018, 27-28).

For instance, in the commissioning organization risk management team has defined conventional processes and operations models based on standards ISO 31000 and ISO 27001. These ground rules apply to information security and risk management processes.

c) Customized

The risk management framework needs to be adapted to the organization's objectives and external and internal operational environment (SFS-ISO 31000:2018, 27-28).

As the commissioning organization, the Union of Professional Engineers in Finland is a union, its operational environment differs slightly from conventional business-oriented companies with respect to, for instance, information security issues and protected value. This needs to be taken into account outlining risk management.

d) Inclusive

All possible knowledge and improved awareness in managing and evaluating risks are useful, so it is vital to take into account the views and perceptions of interest groups and partners in cooperation and their views and perceptions.

For instance, if the organization uses a third party to provide security-related services, it regularly should review threat assessment together with the partner company. Likewise, if some services are outsourced to the third-party partner, this needs to be taken into account when defining responsible persons and response time, etc. (SFS-ISO 31000:2018, 27-28).

e) Dynamic

Risks can emerge, change, or disappear as the organization’s external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.

Especially in the digital world, threats, issues, situations, and environments can change, disappear or emerge in the short term, so is necessary to review risks from the perspective of internal and external environment on a regular basis. Risk management should be able to anticipate, detect, and respond to these changes and issues within a reasonable time (SFS-ISO 31000:2018, 27-28).

In the commissioning organization, the information security risks are reviewed more often than once in a year with the consultant. If there are remarkable changes in systems, or a system is going to be replaced or outsourced, the review will be done on that system as soon as possible after the changes have been made.

f) Best available information

The inputs to risk management are based on historical and current information, as well as on future evaluations or expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders (SFS-ISO 31000:2018, 27-28).

3.1.2 Framework

Successful risk management is integrated into the organization’s decision making and governance. It is based on understanding organizational structure as well as the business environment. The purpose of the framework is to assist the organization in integrating risk management into its activities and functions, and it should be adapted as part of organizational requirements and culture, as presented in this thesis next. This requires the commitment of the top management, which should ensure that risk management is appropriately integrated into significant functions and activities. This can be accomplished, for instance, by implementing all components of the framework, ensuring the required resources (SFS-ISO 31000:2018, 28-29).

Figure 3 (SFS-ISO 31000:2018, 28) introduces the components of the framework: integration, design, implementation, evaluation, and improvement. The core of all the functions is leadership and commitment.

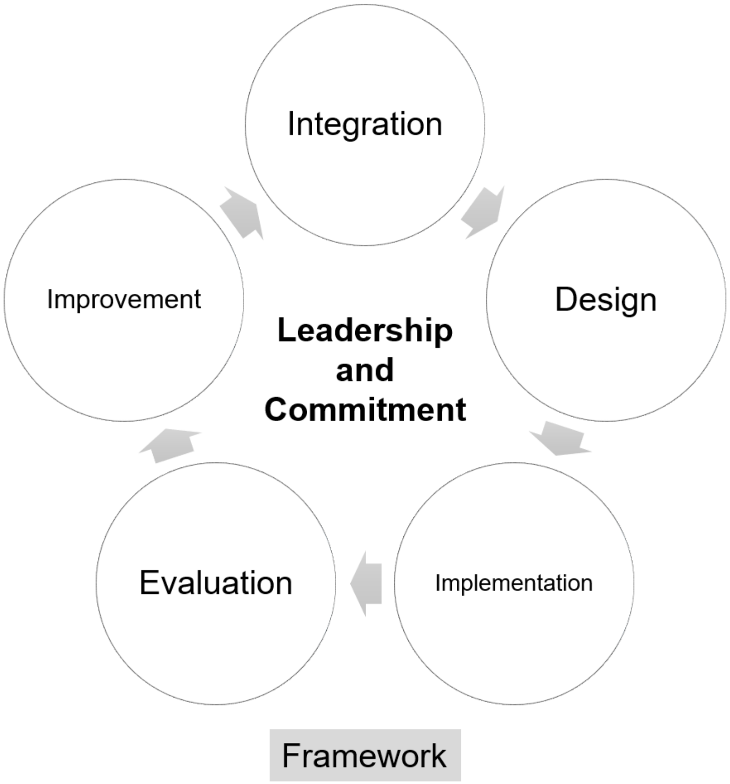


Figure 3. Framework according to ISO 31000 standard

a) Leadership and Commitment

The task of the top management is to ensure that risk management is incorporated to all operations in the organization. It should provide leadership, for instance, to set an example to the rest of the organization. This can be implemented by drawing up a policy document, ensuring the availability of resources and designate employees' responsibilities, for instance. This helps the organization to develop its risk management in accordance with goals, strategy, and culture, communicate the benefits of risk management and advance the systematic monitoring of risk management.

The responsibility of the top management in risk management is to ensure that the risks are acknowledged and managed as planned. The role of the top management is also to supervise the operation and related communication (SFS-ISO 31000:2018, 28-29).

b) Integration

The integration of risk management into the organization’s management system requires an understanding of the operational environment and organizational structure. Risks should be managed in every part of that structure; i.e. every employee has the responsibility of participating risk management process (SFS-ISO 31000:2018, 28-29).

c) Design

When designing risk management to an organization and examining its operational environment, one should recognize internal and external factors, which could be potential risk factors. These can be, for example, international, cultural, financial, or environmental risk factors.

Internal risk factors comprise, for example, the structure of the organization, contractual relations, organizational culture and capabilities, and knowledge (e.g., capital, intellectual property, technologies, and processes).

The design of risk management should show the continuous engagement of the top management. The engagement can be shown by defining the principles of the operation or drawing up a policy document, which includes, for instance, the purpose of risk management, as well as related responsibilities and authorities.

Emphasizing the importance of the integration of risk management into the organization's operations and making the necessary resources available are matters that need to be taken into account in the policy document (ISO 31000:2018, 29-30).

d) Implementation

The framework can be implemented, for instance, by formulating an implementation plan which includes the schedule and list of available resources and ensuring that risk management procedures are clearly understood and implemented in the organization. This requires ongoing communication with different interest groups (ISO 31000:2018, 31).

e) Evaluation

The framework of risk management needs to be evaluated at regular intervals to obtain relevant information on its functionality and suitability (ISO 31000:2018, 32).

The commissioning organization utilizes an external consultant on a regular basis in auditing IT risk management.

f) Improvement

An organization can increase its value by monitoring and adapting risk management framework to address external and internal changes. The ongoing improvement of the suitability, adequacy, and effectiveness ensures up-to-date and high-quality risk management operation (ISO 31000:2018, 32).

3.1.3 Process

Operations are usually managed with or through different processes, which include a significant amount of data. This data is an essential part of the processes and requires careful management (Porvari 2012, 86).

The process of risk management is one of the three tiers in the ISO 31000 standard and perhaps the best known because of its practical nature. The process is based on systematic policies, procedures, and practices, and it includes the activities illustrated in Figure 4 (SFS-ISO 31000:2018, 32).

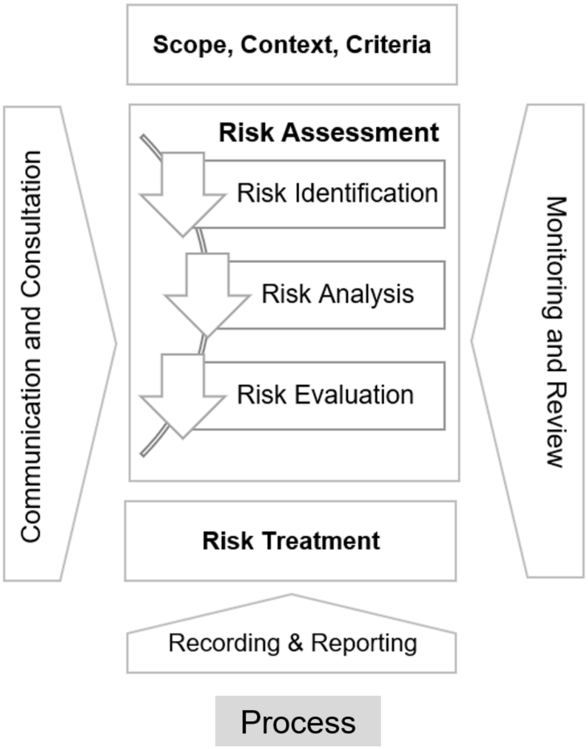


Figure 4. Risk management process according to ISO 31000 standard

a) Scope, context and criteria

The scope of recognition, context, and criteria ensure that the process of risk management for the organization is tailored. This involves, for instance, defining the coverage of risk management, which in turn includes the application of the process on different levels such as strategical, operational, and economic levels.

As an information security risk assessment was made in the Union of Professional Engineers in Finland, it was observed that a system evaluated could encounter various risks from several different levels.

It is significant to understand the external and internal operational environment of risk management because risk management is defined by the objectives and operation of the organization. In some cases, it can even be the source of the risk itself.

Documentation is useful to identify the influential factors that are valuable at the beginning of the implementation of risk management, during the process of assessing risks and in audits. This will help to maintain a comprehensive perspective.

Finally, the criteria of the risks should be defined among the risk types and amount that the organization will consciously take. The defined criteria should consistently reflect the values, objectives, and resources of the organization. Although criteria are relevant to the process at the beginning of risk management implementation, one has to keep it dynamic and make changes when needed (SFS-ISO 31000:2018, 33).

b) Risk assessment

Risk assessment should not be a one-off project but provide permanent and definitive information for making decisions. It is necessary to understand that the assessment needs to be done on a regular basis (U. S. Department of Commerce 2012, 5).

Risk assessment is the second component in the risk management process, including the identification, analysis, and evaluation of risks (SFS-ISO 31000:2018, 35-36).

First, the organization should identify potential threats and internal and external vulnerabilities irrespective of whether the source of the risk is under the control of the organization.

After identifying potential risks, they need to be analyzed. In risk analysis, one can examine various uncertainties, consequences, likelihoods, incidents, scenarios, efficiencies, and controls. As the analysis is done by humans and individuals, the findings can always be subjective. It is good to recognize several factors that can influence the analysis, for instance, dissenting opinions, prejudices, quality of available information, and assumptions.

In order to ensure that the results are sufficiently reliable, it is recommended to assess risks systematically, iteratively, and in cooperation with professionals as well as with stakeholders (SFS-ISO 31000:2018, 35).

This is the reason why the operational environment and risks towards it must be defined at the beginning of the assessment process, and the person who is responsible for risk management arrangements, should in proportion, adjust security arrangements to the operational environment and organizational requirements. The individual who performs risk assessment may have a different perception of the risk from what is defined by the organization, which may negatively affect the process of risk management (Puolustusministeriö 2015, 9).

Finally, the risk needs to be evaluated based on which the organization decides, for instance, not to take any measures, make procedures to mitigate the risk, or maintain existing controls (SFS-ISO 31000:2018, 36).

c) Risk treatment

The purpose of risk treatment is to select and implement the procedures to process the assessed risk. When selecting the correct way to, for example, mitigate the assessed risk, a comparison must be made between the cost or disadvantages of the procedures and the benefits and possibilities. This then needs to be taken into consideration in the risk treatment plan, which introduces, for instance, the selection of the possible treatment options, the person responsible, proposed actions, and required resources (SFS-ISO 31000:2018, 36).

d) Communication and consultation

Communication is a necessary part of risk management. Its purpose is to ensure the exchange of information, reasons, and arguments concerning why specific procedures and actions are needed. The purpose of the consultation is, for example, to utilize the expertise in different fields to receive reliable information and feedback (SFS-ISO 31000:2018, 37).

e) Monitoring and review

Planned, monitored, systematic and ongoing with consideration of all interest groups assure the quality and effectiveness of the process, implementation, and outcome of the risk management process (SFS-ISO 31000:2018, 38).

f) Recording and reporting

All risk management plans, processes, and outcomes should be documented and reported to the top management and interest groups (SFS-ISO 31000:2018, 38).

According my own experience, for instance, all employees in the organization should be aware of the activities at some level, for instance. Well, prepared documentation will further communication and comprehension towards risks, offering information for decision making, and improving risk management activities.

In the commissioning organization, there will be several different risk management processes. For instance, in information security risk management, there are separate processes for different IT-systems, functions, and projects. There will be separate but consistent processes in risk management of occupational health and safety, media and communication, and economy, for instance.

4 EXPERT INTERVIEWS

In this chapter, the views of the four experts working with Finnish SMEs and information security risk management are presented. The interviews revealed how these experts see the current situation with the SMEs concerning information security and risk management.

Because of these interviews, it was possible to gain valuable and current information and outlooks, for instance, how to keep risk management ongoing after the implementation project.

In chapter 4.3., the questions from four to seven are walked through one by one.

The purpose of the questions from one to three was to find out background information about the interviewees and their work on risk management. These will be presented in the next chapter, where the interviewees are introduced.

4.1 Introduction of interviewees

Interviews are done by using a qualitative interview model. The interviewees are four experts outside the commissioning organization. Interviews were conducted as individual discussions using email or phone.

For me, two of the interviewees were known through their work. The other two interviewees were found by information security-related networks. All followed interviewees convinced me of their professionalism and knowledge of the subject in question.

Next, interviewees Jan Zilliacus, Mika Susi, Jani Räty, and Jarkko Puistovirta are introduced.

Zilliacus is the consultant with whom the commissioning organization has worked with on the information security risk management implementation project. Zilliacus (2019) mainly works with different sized customer organizations on information security management and, for instance, information security policy. He has as customers, both listed companies as well as SMEs, so he can utilize the point of view from both sides in his work. Zilliacus’s specialty is data handlining and its risk and security management.

Susi (2019) finds his main job to be disseminating information to companies about information security and the advantages of risk management. He conveys data about cybersecurity information and organizations’ standpoints from companies to authorities and represents the business world in legislation projects concerning risk management and information security. Susi’s client base consists of many different sized organizations, but the focus is on small and medium-sized businesses.

Companies with whom Puistovirta works are security orientated and have got certification against ISO/IEC 27001:2013 standard, which requires having a position on information security risk management. Handling clients' confidential and classified security information requires up-to-date knowledge about cybersecurity risks and management processes and procedures related to them (Puistovirta 2019).

Räty works for an SME being there the person responsible for overall risk management as well as information security risk management. His previous projects have related, for instance, into reviewing products and dealing with information security risks. Räty works with SME clients with risk management as well, although the company does not offer direct risk management services (Räty 2019)

4.2 Interview questions categories

There were drafted seven questions beforehand around the risk management theme. The goal was to keep the questions as few numbered as possible to ensure the availability of the chosen interviewees. The purpose of the first three questions was to elucidate the background of the interviewees in the outline. These following questions were gone through in the previous chapter.

1. How is information security risk management part of your profession or otherwise daily work?
2. Do you have SMEs as your customer or interest groups?
3. Describe what kind of information security projects you have been part of lately?

The purpose of the rest of the questions was to find out what are the main problem areas, what challenges organizations may face, and what are the reasons if (information security) risk management does not meet the required continuity. The answers will be gone through in the following chapters.

4. What are the standards, methods, or tools that you have discovered organizations using in information security risk management?

5. According to your knowledge, have the information security risk management processes met the continuity in organizations after the implementation project?
6. According to your knowledge, have you noticed challenges or obstacles that risk management may face? And what are the reasons that the information security risk management do not meet the continuity?
7. Do you have any other outlooks or comments to offer concerning the subject in question?

All questions were presented in Finnish as all the interviewees were Finnish speaking. One interviewee gave answers in English to ease the translation.

4.3 Question 4: Standards, methods and tools

One has discovered that there are several tools, methods, and standards to follow (information security) risk management for example ISO standards (27000 and 31000) and the related tools like VAHTI risk management tool (introduced in chapter 5.4), commercial services and other models like COSO’s (The Committee of Sponsoring Organizations of the Treadway Commission) Guidance for Applying Enterprise Risk Management (ERM). Because of the various options available, it was interesting to know what tools my interviewees use with their clients or in their own work.

Susi and Puistovirta both have noticed that ISO 31000 tends to be used tool among larger organizations as well as the COSOs ERM model. They have not noticed any particular trend among SMEs. Räty says he works typically with ISO 27001, which is the most required among his clients (Puistovirta 2019; Räty 2019; Susi 2019).

Susi (2018) tells likewise that on a case-by-case basis, SMEs utilize IT or risk management consulting services or independently apply basic tools available like POA-method, (which is a method of analyzing and identifying potential issues). Commercial tools will be used more and more as the availability has got better in the markets.

Zilliacus (2019) prefers the ISO 31000 standard in which many of the tools are based on according to his notes. ISO 31000 standard is easy-to-follow and straightforward with understandable terms. Likewise, when the ISO 31000 standard is known regardless of industry or nationality, it is easier to explain in which the used risk management is based on when needed.

4.4 Question 5: The continuity of risk management after implementation project

This question can be found to be the most interesting one, not just because it is the primary standpoint of the thesis. According to my personal experience, the risk management implementation project, among many other new operation modes, requires much work. It is possible that soon after the implementation project has ended and the consultant has stepped back, it may be challenging to keep risk management ongoing by giving the required time and attention. This is especially the case if risk management is more or less voluntary, and for instance, the top management does not demand to report on a regular basis.

According to Zilliacus (2019), listed companies tend to have risk management in use as the law requires being part of the financial obligations. However, what it comes to, for instance, information security risk management in SMEs, there may reveal shortages. Susi (2019) agrees and tells that in the bigger organizations, the systematic process and being part of the everyday operation is at least an aimed goal. In SMEs, if risk management is implemented, in many cases, it applies to only a financial risk point of view rather than security-related risks. Likewise, the lack of breadth and depth of risk management is common.

Among other interviewed professionals, Zilliacus (2019) has noted that continuity depends mainly on the commitment of the top management and the fact what kind of culture is in the organization in general: Are there all employees in the organization, including top management, used to work with accuracy and conscientiousness? Does the top management understand the benefits of risk management in information security?

Puistovirta (2019) as well, has observed that gaining on a strong risk management process throughout the organization is when effective when the implementation is made carefully, and the top management commitment is stout.

Räty (2019) has noticed that many times SMEs may evaluate risk only from an economic point of view. Risk management may also remain only in a single project level.

4.5 Question 6: Challenges and obstacles in risk management

The purpose of the 6th question was to find out what are the challenges and obstacles experts might be see impeding continuous and systematic risk management.

Räty (2019) noted that the common problem in the field is the reconciliation of management and practical implementation. Often risk management tends to be far too robust and formal, so the actions and observations may not be recorded, and the other hand, high-level risk, tends to be forgotten. All this may be because of a lack of compatible knowhow, conjointly used risk management system and centralized administration, and/or high turnover of workers. Recording risk observations can be forgotten to do if it is not demanded by top management. Puistovirta (2019) points out that such as many other development processes, effective risk management needs to be well planned, described and implemented. If the top management does not see the benefit of risk management, then it does not offer support for decision making.

Susi (2019) reminds us that the certifications and expensive tools are not always required. However, often the commitment of the superiors proved by having risk meetings can bring good results. In SMEs, he thinks the continuity problem is common because of on non-existence of knowhow or commitment. Risk management should not be trivial and forced. Susi, among the other interviewees, has observed that the commitment of the top management seems to be the key to successful risk management.

Zilliacus has noticed that one of the main obstacles may be that organizations do not prioritize risks, systems, and actions. Due to this, it is possible that risk management is too heavy and complicated for the needs of the company. The offset of risk management should always base the actual need of the organization, not the supply of the solutions available. This way, it is possible to gain systematic and cost-saving measures.

According to Zilliacus, the problem might also be that the IT department believes technology to be a silver bullet that offers a solution and a fix for every security issue. The real challenge can be that the IT department does not know how to communicate to the top management and concretize needs or results, for instance. The ability to express strongly one’s opinion concerning, for instance, important security issues is required. At first, it is relevant to inform why the matter is essential and secondly, what are the required measures (Zilliacus 2019).

4.6 Question 7: Other matters to consider

Finally, the interviewees had an opportunity to give a piece of advice or remind something that has not been discussed yet or highlight what they experienced to be essential to remember.

Susi (2019) reminds us that information security risk management should be considered from all organization operation’s framework point of view. Many times, professionals from a secure field consider risk management as a tool only. He also reminds us that the business usually requires taking risks. One must though, understand what kind of risks will be taken and accept that some of the taken risks require a more significant amount of analyzing, decisions, and commitment.

Puistovirta (2019) recommends getting the education of information security risks by familiarizing them with different nationals and annuals assessments and documentation, such as the report by The Finnish Transport and Communications Agency, Traficom.

Räty (2019) advises organizations to decide how often the risk status should be assessed as some of the risks are permanent, and others can hold only for a specific time. Albeit the real-time view might be possible, practical advantages may be questionable if the identification of the risk is not effortless and systematic in every field of the organization. He also reminds that thought organization has implemented risk management for decades, every new generation approaches it differently, which should take into consideration in choosing tools and methods, for example. Räty has found ISPE's (The International Society for Pharmaceutical Engineering) GAMP® 5 to be a useful method as it highlights, for instance, vulnerability issues. It is practical guidance for using digital systems efficiently and effectively.

Zilliacus (2019) finds that all together, it is many times enough if the fundamentals of IT and information security are on track, such as basic users do not have administrator privileges in systems. Changes in some basic settings can make a huge difference. These things need to be noticed. One advantage of risk management is that it will take points of view into account from several perspectives.

5 INFORMATION SECURITY RISK MANAGEMENT IN THE UNION OF PROFESSIONAL ENGINEERS IN FINLAND

Next, I will present my approximately two years' experience of information security risk management based on related work in the Union of Professional Engineers in Finland. As I showed interest in information security and in risk management, I got a chance to participate in an information security risk management project. The project started one year before this master's degree programme.

After I started to gather information for this thesis and information risk management implementation, I found out that the Union of Professional Engineers in Finland did not have comprehensive risk management in use. After a discussion with a representative of the top management team, I involved in implementing the groundwork of one. This way, I could receive a better and in-depth understanding of the entity, in which information risk management will be integrated. I will reveal the implementation project later in chapter 5.3.

Working for the union and not, for example, in a conventional sales organization, I have noticed some differences. However, from the IT team's point of view, one might think the operation to be quite similar; there are networks, information processing programmes, servers, computers, printers, which all should be running as required. Likewise, there is crucial data that needs to be protected from outsiders.

Reflecting on my experience in previous jobs and conversations with colleagues working in other kinds of SMEs can be said that the behaviour of users’ and challenges with the IT-systems are very much alike regardless of the company or industry.

One of the differences comparing to, for example, commercial companies, is that the union handles more sensitive personal data, such as social security numbers. This is the reason that the GDPR must take into consideration more often.

5.1 The reason of introducing information security risk management in the commissioning organization

When introducing a new management technique, working method, or system, there is a reason or a need that has appeared. By interviewing the IT manager of The Union of Professional Engineers in Finland, Malinen (2020), one was able to find out how performing information security risk management in the union got started and why.

Malinen (2012) had some experience of risk management but no recent knowledge of it. The risk management implementation project got started in 2017 while improving the information security of the commissioning organization. Working cooperation with different security service providers, risk management came up. Risk management was also included in an information security policy document that was drawn up together with the consultant for the union.

One of the biggest challenges concerning risk management is the lack of time. Risk management requires much work, especially at the beginning. Working with risk management tends to be the task that will be completed at the point when there are not that many other challenges or duties to be handled (Malinen, 2012).

Malinen states that, at the moment, the top management of the commissioning organization does not regularly take a stand on information security risk management. However, top management in The Union of Professional Engineers in Finland has adopted a risk management policy and staff guidelines concerning information security. The budget for information security is decided by the IT manager (Malinen, himself).

Malinen (2012) thinks risk management is an excellent tool to have a dialog of the state of information security with different parties. It can bring up actual risks and concrete observations from different points of view. Among IT team, the one way of ensuring the continuity of risk management is by using an annual planning cycle wherein risk management is placed, for instance.

In the next chapter, the information security risk management policy document will be introduced shortly. The document was one of the catalysts for implementing risk management in the union. It can also be considered to be an essential part of biding the top management into information security.

5.2 Information security risk management implementation project

The implementation project consisted of five workshops where, at first, me, Malinen, and the consultant draw up the risk management policy document for the union.

The purpose of risk management policy is to commit top management to support the decisions improving information security and its risk management for the organization by defining the main objectives, principles, the person responsible, and procedures to the process. The policy document is beneficial to compile together with a representative of the top management (Valtionvarainministeriö, n.d.a).

Risk management policy document can introduce, for instance, the following elements, as in the ministry of finance’s template document shows (Valtionvarainministeriö, n.d.b).

The scope of application should reveal to whom the document is intended and what the scope of it is. For example, in The Union of Professional Engineers in Finland, the policy document is compiled for information security risk management.

The policy document should include the statement of legal obligations, additional regulations, or instructions concerning the operation and risk management if there is any. It is also relevant to define the main concepts in one of the chapters. The policy document should be understandable to every reader despite the lack of expertise in risk management.

Perhaps the most critical part of the policy is to define **the goals and principles** of risk management: what are the achievements if the policy is adhered to. In the union, these matters are, for instance, supporting proactive management and establishing proper management and governance.

The persons responsible and their roles are essential to define in risk management documents. Responsibilities and roles should be recorded, at least in the job designation level.

It is essential to remember to go through responsibilities with the persons in question, what do the responsibilities mean and require in practice. Add to that, it is relevant to clarify what are the consequences if the responsibilities are not taken care of.

The risk management process can be introduced with the policy document as an attachment, and it imitates the process in ISO 31000 standard (Figure 4).

The assessment and development of a risk management policy document should be implemented regularly. The document should express how implementation will be gained and if internal audit is the tool, for instance.

Finally, the document should be signed by a member of top management and set a valid date (Valtionvarainministeriö, n.d.b).

After the compiled policy document and a launch meeting, the practical work got started. At first, the risk levels were identified by recognizing the commissioning organization’s most valuable asset and the systems which require the most protection. For the members of the project or risk team, it is vital to understand why risk management is brought in to play and what are the protected assets. These matters can be regarded as truism at first, but exchanging ideas and thoughts might help to commit to risk management. Raising enthusiasm among the team members is very useful at the beginning and for the future.

The commissioning organization’s most valuable asset is the personal and case processing data of over 70,000 members. One can also talk about information property. Besides, it was essential to identify the most secured asset, it was nearly as significant to realize the consequences of failing to protect it. In the commissioning organization, the systems that are mainly destined to handle personal data are membership register system and Customer Relationship Management (CRM).

In The Union of Professional Engineers in Finland, there is only one available-for-sale product, and it is the membership of the union. The membership fees are mainly the only source of income and enablers of the operation. Thus, if, for some reason, the quantity of members decreases, and source of income peters out, it can result in significant erosion of operation and job cuts. Long-term membership development can be affected by strategic decisions, for instance. The unforeseen, precipitous, and negative development of member quantity can be disastrous for the operation. From an information security point of view, the reason for this kind of sudden member loss can be due to wide negative publicity or loss of all member data, for instance.

As appeared in interview with Malinen in chapter 5.2, the union has had no systematic information security risk management before, for which the development and implementation of risk management started by identifying risk levels and prioritizing systems to be assessed at the first opportunity. With the help of the consultant, the risk levels were defined and prioritized.

5.3 Introduction of VAHTI risk management tool

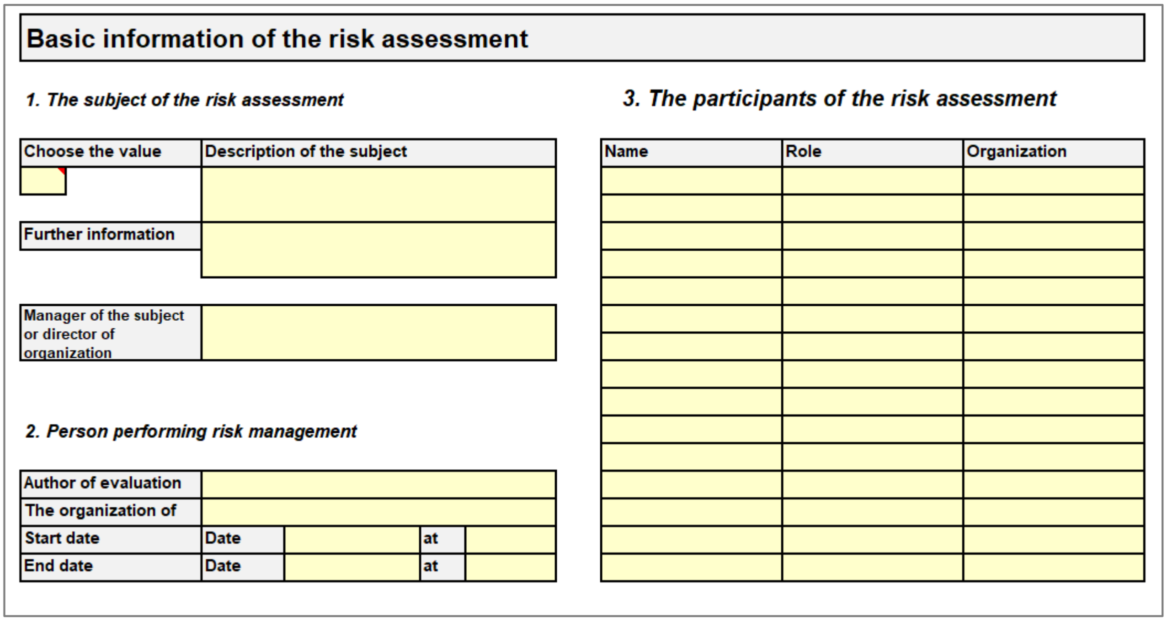
VAHTI risk management tool is a method for risk management created by The Government Information Security Management Board set up by the Finnish Ministry of Finance (Valtionvarainministeriö, 2017). It is designed for the use of public administration but can be utilized by companies and other organizations as well. VAHTI risk management tool is in Microsoft Excel format, and it is available now only in Finnish but in free of charge (I have done the translation for this thesis). It can be received from the ministry of finance’s web site https://vm.fi/vahti. The management tool itself consists of Excel spreadsheets. It is noteworthy that there are several Excel functions in the table, so it is important that the spreadsheet will stay unformatted so that compiler does not add or delete any columns, etc. and only fill out empty fields.

Going through the Excel spreadsheet gives a good example of what a good risk management process can be like. The VAHTI risk management tool is based on the ISO 31000 standard, with some adjusts for the use of public administration (Rousku, 2017, 9).

5.3.1 The function of the basic information

The first sheet (Valtionvarainministeriö, 2017) presented in Figures 5, 6, and 7, has a form which includes empty fields of basic information of the subject to be evaluated. An assessor should fill out the following information:

1. Information about the subject/system/process/product being evaluated
2. The person who will have the principal responsibility of risk management in question
3. All persons who have been part of the evaluation process in question



Basic information of the risk assessment

1. The subject of the risk assessment

Choose the value	Description of the subject
Further information	
Manager of the subject or director of organization	

2. Person performing risk management

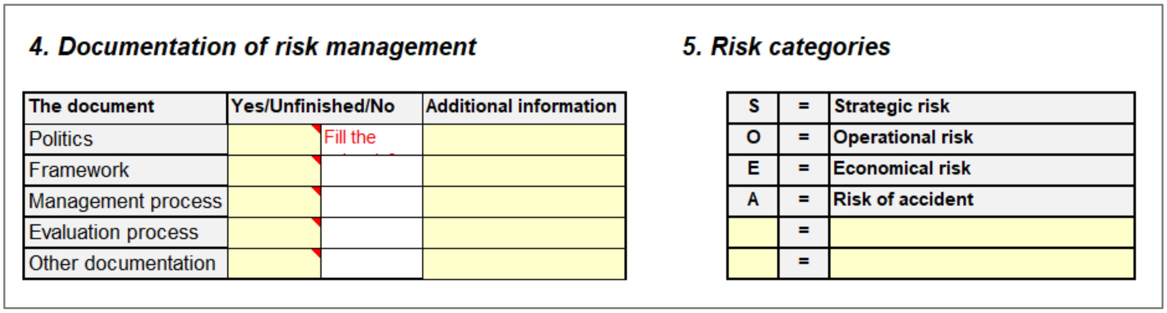
Author of evaluation				
The organization of				
Start date	Date		at	
End date	Date		at	

3. The participants of the risk assessment

Name	Role	Organization

Figure 5. Subject and participants in VAHTI risk management tool

4. All the documentation related to this subject
5. The risk categories in use. The basic categories are strategic, operational, economic risk, or risk of an accident.



4. Documentation of risk management

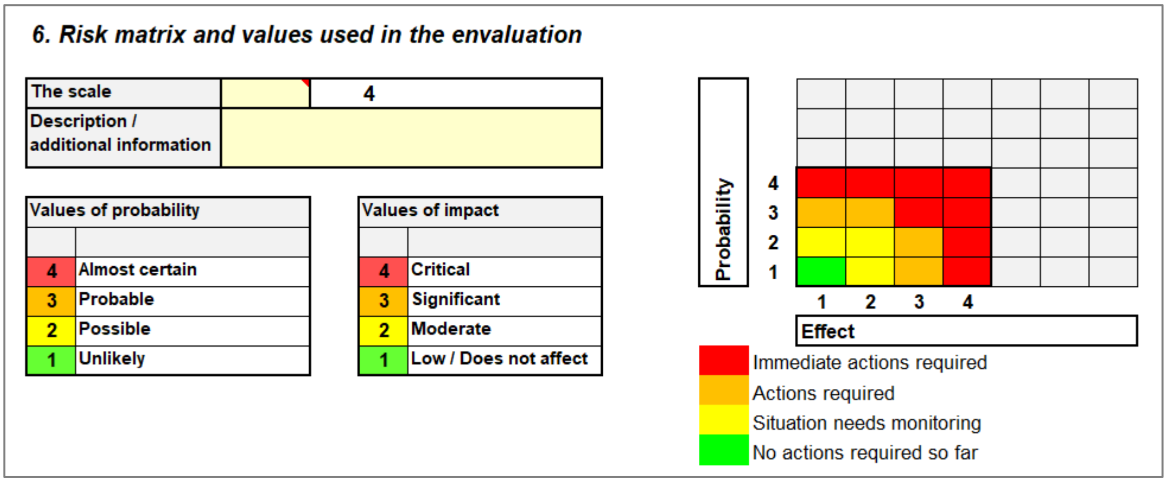
The document	Yes/Unfinished/No		Additional information
Politics		Fill the	
Framework			
Management process			
Evaluation process			
Other documentation			

5. Risk categories

S	=	Strategic risk
O	=	Operational risk
E	=	Economical risk
A	=	Risk of accident
	=	
	=	

Figure 6. Documentation and Risk categories in VAHTI risk management tool

6. Risk matrix and values of evaluations: probability and effect. The basic matrix is given, but for instance, in a hospital environment, the matrix can be compiled differently as for example, consequences may be fatal, and the tolerance for those situations is presumably extremely low.



6. Risk matrix and values used in the envaluation

The scale		4
Description / additional information		

Values of probability	
4	Almost certain
3	Probable
2	Possible
1	Unlikely

Values of impact	
4	Critical
3	Significant
2	Moderate
1	Low / Does not affect

Probability				
4	🟥	🟥	🟥	🟥
3	🟧	🟧	🟥	🟥
2	🟨	🟨	🟧	🟥
1	🟩	🟨	🟧	🟥
	1	2	3	4
	Effect			

🟥 Immediate actions required
🟧 Actions required
🟨 Situation needs monitoring
🟩 No actions required so far

Figure 7. Risk matrix and values used in evaluation in VAHTI risk management tool

5.3.2 The function of the risk assessment template

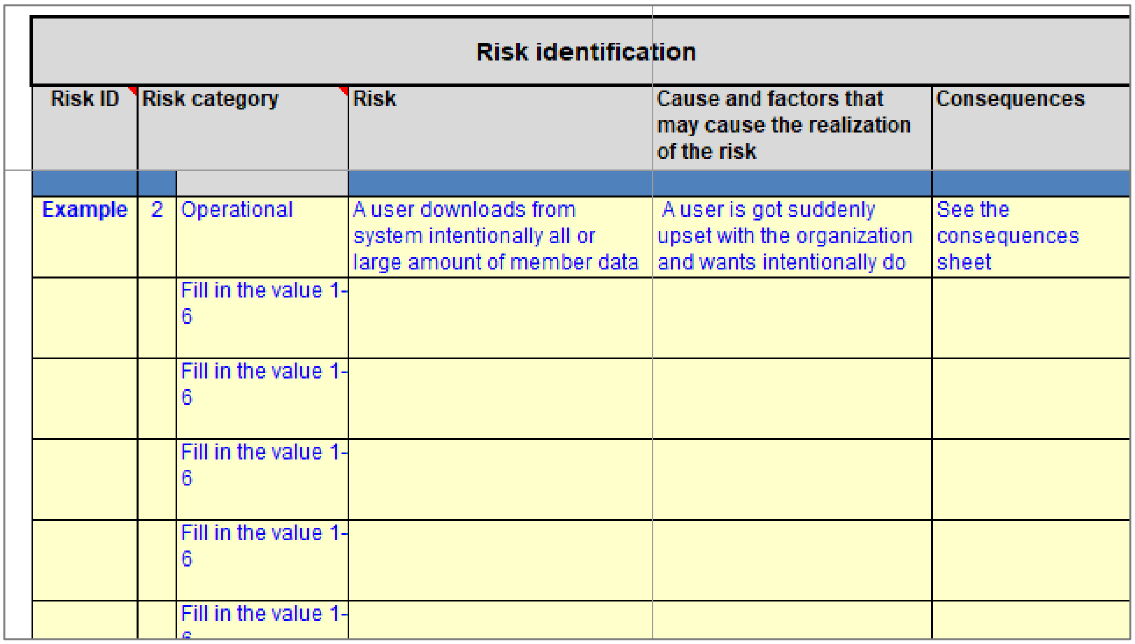
The second sheet (Valtionvarainministeriö, 2017) has a template of risk assessment in which the risks are identified and evaluated. In the first column, as presented in Figure 8, it is possible to give a risk ID (Identifier) to the risk. This easies referring to individual risks in other documentation if needed. In the commissioning organization, risk management coordination group had prepared a document in which all the systems and topics were given an ID numerical scale.

In the second column, one can select a proper risk category. This phase can be done later if the risk category is not yet certain. The chosen category does not have a direct effect on the risk management process at this point.

The completed risk column should present the name of the risk, for example: “A user downloads from system intentionally a large amount of member data into his/her personal computer (and afterward leaks it outside of the organization intentionally or unintentionally).”

The next column should reveal the advanced information about cause/ causes or factors which could lead to situations where risk is realized. This can be such as: “A user is got suddenly upset with the organization and wants intentionally do harm for the company by leaking sensitive or confidential information.”

The followed column contains information about the consequences of the realized risk. In the workshops came up that usually there can be several consequences for one part of the organization at the same time. I ended up adding an extra sheet to Excel, which is named Consequences. Consequences can also be the same in spite of the risk. It can require different perspective and actions, for instance, if occurs personal data leak of a few members vs. 20,000 members. This should be taken noticed when assessing the risks. In this case, the consequences should be considered the point of view of daily operation, individual members, and organization.



Risk identification

Risk ID	Risk category		Risk	Cause and factors that may cause the realization of the risk	Consequences
Example	2	Operational	A user downloads from system intentionally all or large amount of member data	A user is got suddenly upset with the organization and wants intentionally do	See the consequences sheet
		Fill in the value 1-6			
		Fill in the value 1-6			
		Fill in the value 1-6			
		Fill in the value 1-6			
		Fill in the value 1-			

Figure 8. Risk identification in VAHTI risk management tool

If there appears a data leak incident, the consequence for the operational point of view requires the IT team to be caught in an investigation and helping authorities. At that time, other duties might be on hold. For individual members, the data leak brings not only an inconvenience but a risk of getting a victim of identity theft, which can increase the seriousness of the situation. For the organization, this can easily be a major, destructive issue and can lead to a large number of resigning members, which cause immediate financial challenges.

Next columns, in the second sheet and presented in Figure 9, are about evaluating the probability and effect of risk realizing.

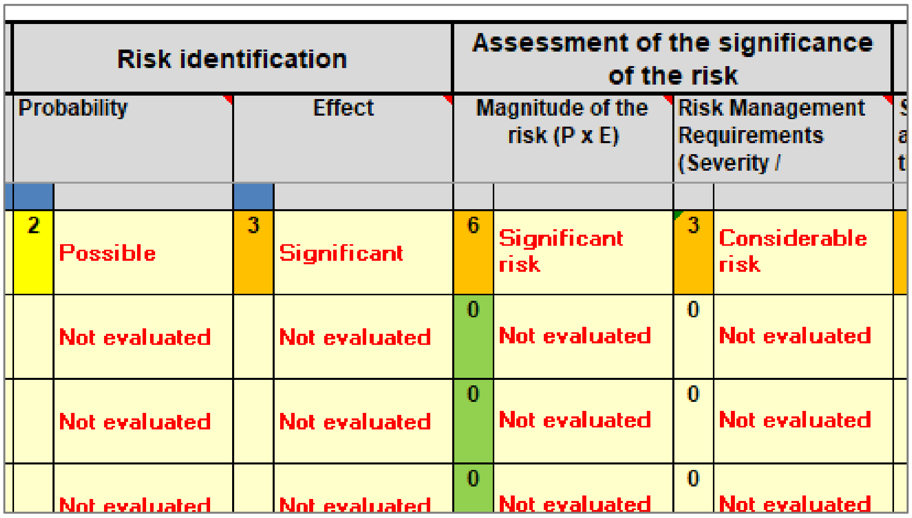
Probability: The compiler gives the value of 1 to 4:

1 = Unlikely
2 = Possible
3 = Probable
4 = Nearly certain

Effect: The compiler gives the value of 1 to 4:

1 = Minor
2 = Moderate
3 = Significant
4 = Critical

The Excel sheet has an automated function that calculates the seriousness of the risk, the need for action, and suggestion on how to proceed.



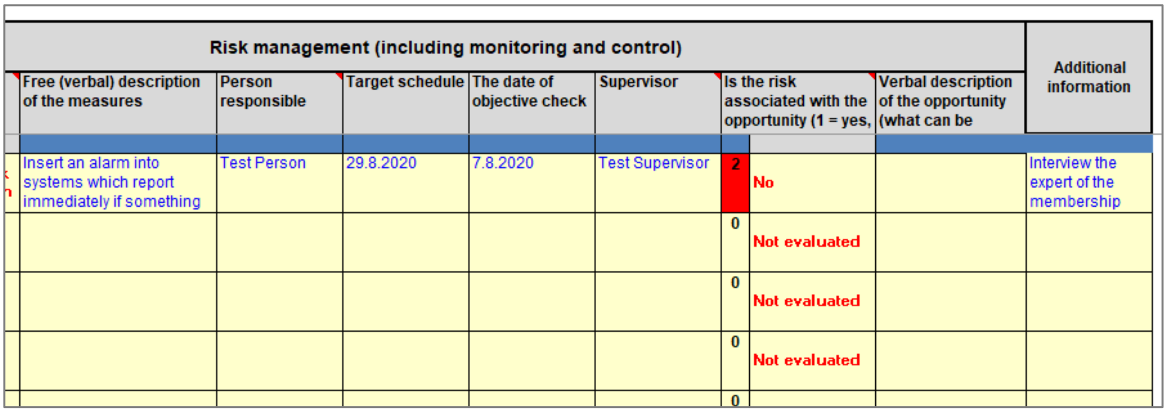
Risk identification				Assessment of the significance of the risk				
Probability		Effect		Magnitude of the risk (P x E)		Risk Management Requirements (Severity /		S a t
2	Possible	3	Significant	6	Significant risk	3	Considerable risk	
	Not evaluated		Not evaluated	0	Not evaluated	0	Not evaluated	
	Not evaluated		Not evaluated	0	Not evaluated	0	Not evaluated	
	Not evaluated		Not evaluated	0	Not evaluated	0	Not evaluated	

Figure 9. Risk identification and assessment of the significance in VAHTI risk management tool

If the result suggests taking action, the next column can be filled out with a verbal description of the concrete measures that are going to be done to avoid, minimize, outsource or accept the risk in question (in Figure 10). The description of taking an intentional risk and taking no action should be recorded as well if that is the case. The suggested measure for this data leak example could be, for instance, inserting an alarm into systems that report immediately if something more massive amount of data is downloaded. Alternatively, the solution restrains basic users from downloading the data, if possible.

If measures' implementation is desired to be done, it is important to direct the compiler, deadline, and author to the operation. These records increase the possibility of implementation.

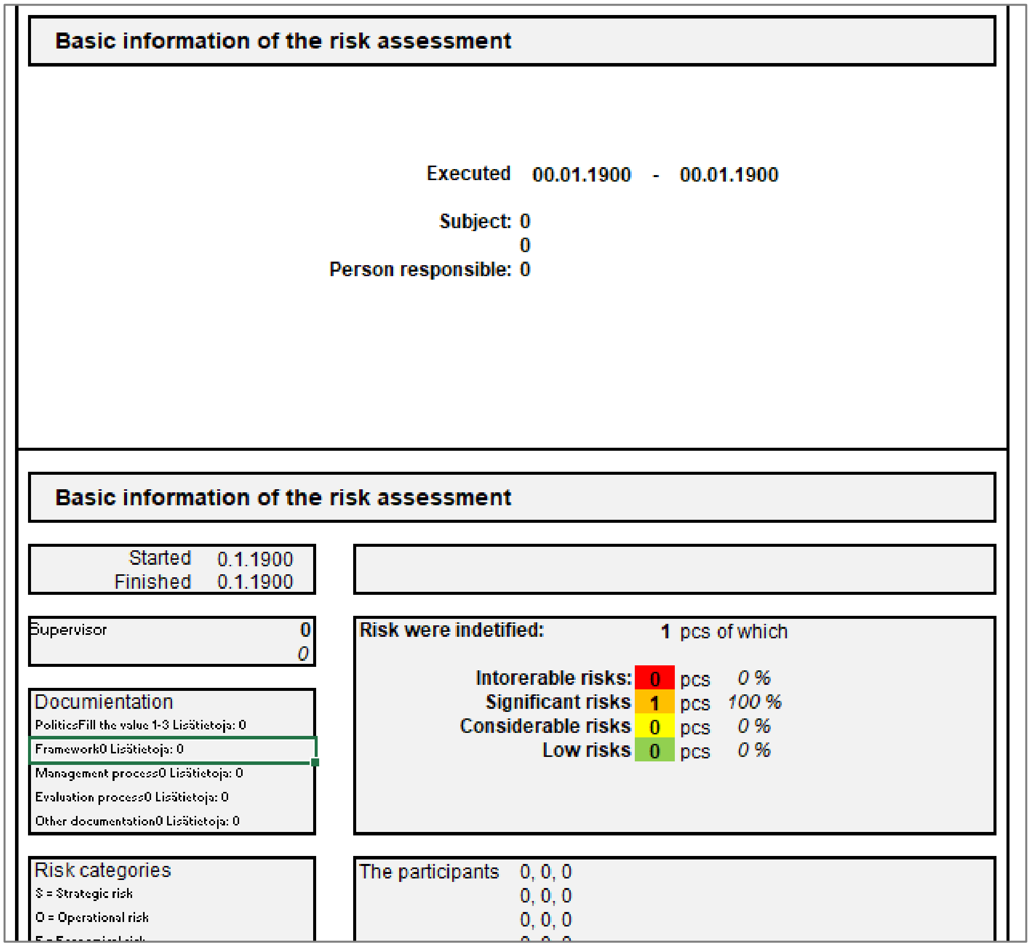
During the risk assessment, it is good to analyze if the risk includes any opportunities to be utilized.



Risk management (including monitoring and control)								Additional information
Free (verbal) description of the measures	Person responsible	Target schedule	The date of objective check	Supervisor	Is the risk associated with the opportunity (1 = yes,		Verbal description of the opportunity (what can be	
Insert an alarm into systems which report immediately if something	Test Person	29.8.2020	7.8.2020	Test Supervisor	2	No		Interview the expert of the membership
					0	Not evaluated		
					0	Not evaluated		
					0	Not evaluated		
					0			

Figure 10. Risk management in VAHTI risk management tool

The last tab, illustrated in Figures 11 and 12, will be automatically filled out with result based on completed information from previous sheets. The summary report displays the amount of identified risks, persons responsible, and list of risks and required actions.



Basic information of the risk assessment

Executed 00.01.1900 - 00.01.1900

Subject: 0
0
Person responsible: 0

Basic information of the risk assessment

Started 0.1.1900
Finished 0.1.1900

Supervisor 0
0

Documientation
PoliticsFill the value 1-3 Lisätietoja: 0
Framework0 Lisätietoja: 0
Management process0 Lisätietoja: 0
Evaluation process0 Lisätietoja: 0
Other documentation0 Lisätietoja: 0

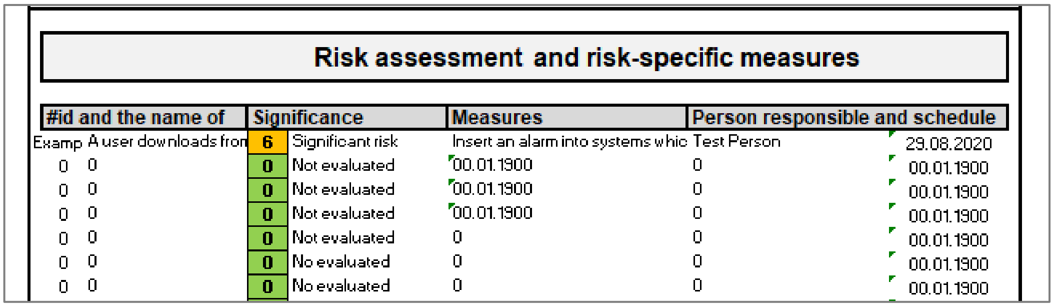
Risk categories
S = Strategic risk
O = Operational risk

Risk were indetified: 1 pcs of which

Intorerable risks:	0	pcs	0 %
Significant risks	1	pcs	100 %
Considerable risks	0	pcs	0 %
Low risks	0	pcs	0 %

The participants 0, 0, 0
0, 0, 0
0, 0, 0

Figure 11. Summary report, Basic Information in VAHTI risk management tool



Risk assessment and risk-specific measures

#id and the name of		Significance		Measures	Person responsible and schedule	
Examp	A user downloads fron	6	Significant risk	Insert an alarm into systems whic	Test Person	29.08.2020
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	0	0	00.01.1900
0	0	0	No evaluated	0	0	00.01.1900
0	0	0	No evaluated	0	0	00.01.1900

Figure 12. Summary report, Risk assessment and measures in VAHTI risk management tool

5.4 Workshops with the consultant

Although the VAHTI risk management tool was available for the commissioning organization and the gain of risk management was realized, using the tool and understanding how it works would be difficult and time-consuming without the help of an expert. With a professional consultant, the project started efficiently.

The consultant helped to comprehend completeness and action sequences that can be applied in operations in the commissioning organization.

He suggested that we would evaluate information security risk a system by system. Due to this, we prioritize the most important functions: Membership register, Microsoft CRM, Microsoft O365, Azure AD, and network infra. As the data is the valuable asset for the commissioning organization, every subject was evaluated with four main levels: Data leaks, data is not available, data is incorrect, and data does not evolve. These originate in three basic information security principles: availability, integrity, and confidentiality (National Institute of Standards and Technology 2020, 3).

Jordan and Silcock (2005, 164) listed for the objective of information asset following requirements:

- Should be available for only quarters with authorities
- Shouldn’t have errors and should be updated, exact and review as needed
- Should be available when needed

Add to this, Jordan and Silcock have added a point that includes compliance with the law and regulations. From the point of view of the GDPR-regulation, this is necessary to be taken into account. Because of the nature of business in the union, which is mainly based on the processing of personal data, the GDPR relates matters should take seriously and evaluate at each system and even separately as well.

During the implementation project, there was a workshop approximately once a week at three hours at the time. It required deep focusing on the subject and cerebration to identify different information security risks. With the help of the consultant, it was able to keep the focus of the subject in question.

After workshops, the independent work in the commission organization started with risk identification cooperation with colleagues. It was observed that the identification and risk analysis is fairly slow and requires focusing and without interruptions. As working with a different project and daily tasks, identifying risks need to keep in mind constantly and document observations which could be useful.

At the moment, working information security risk management continues with evaluating Microsoft Office 365 services and Azure AD. As the CRM system and the membership register will be transferred into the cloud, both systems need to be reanalyzed for risks. Because of the transfer to the cloud system, maintenance and data will be outsourced, which will create new risks and tackle some as well.

5.5 Risk management for the commissioning organization

Implementing risk management requires an organization’s resources and, sometimes, financial investments. If a potential risk is decided to be avoided by protective measures, it usually requires resources as well.

It is common that the mitigation of many information security-related risks requires financial investments, such as upgrading existing devices or systems or purchasing third party auditing services. Those investments need to be rationalized to the IT department, but also to the top management.

For the thesis, seeking information from the commissioning organization was required. The information of already existing risk management or information that had been gathered that could be utilized, was searched. During the information searching there was a discussion with the representative of the top management. There came up a suggestion that I could put together a small team and draw up basics for risk management for the union comprising consistent operation methods, tools, figures, and processes.

Searching for the information about possibly existing risk management in the commissioning organization, it was discovered that one of the co-workers was also processing with risk management about occupational safety and she was starting to implementation.

With her and with The Union of Professional Engineers in Finland’s development manager, we had a meeting where we compared the information and methods each had to experience with. The decision to proceed with an ISO standard.

To get more information on ISO risk management standard, I participated in a seminar about the ISO 31000 standard organized by the Finnish Standards Association. In the seminar, there was discussions of the standard and the VAHTI risk management tool. All the experts in the seminar I had discussions with recommended using tools based on this standard, for example, VAHTI risk management tool. Based on these discussions, I was convinced that the ISO 31000 standard and the VAHTI risk management tool are safe and stable guidelines to work with.

Using known standard have many pros. For instance, if someday is the case that I will no longer be working with these matters in the union, whoever is able to continue the work because of the commonly and internationally known and used standard. The International Organization for Standardization (ISO) also takes care of that the standard will be reviewed regularly with professionals all over the world and will be evolved to serve modern risk management if needed (International Organization for Standardization b).

With the risk management coordination team, we decided to start to gather information and compile the guidelines based on the standard. As we did this besides our main work duties, finding common time was sometimes challenging, and the work progressed slowly. Approximately half a year later, we introduced our plans and findings to the top management. They were pleased and suggested to carry on. Next was asked if it would be possible to draw up a proposition which would present the three subjects that would be the most important operations to the commissioning organization. The implementation of risk management would start with those three systems or function.

After some examining, we ended up suggesting proceeding with these three functions: economy, the membership volume management, and the various media in which the union operates and communicates. The next step is to formulate a plan on how to start the practical implementation work in organization. This implementation project is still going on, as this thesis is finished.

Because of the implementations and working with the top management, I gained out valuable information, for instance, how the management of the union responds to risk management. It was also possible to have a view to more comprehensive risk management in organization. With this approach, I got the opportunity to work with the management, and now there is a dialog concerning risk management.

6 ENGAGING TOP MANAGEMENT

According to my experience, I have noticed that getting a process ongoing in an organization can usually be due to the reason that people find the process to be useful or bring some other benefits they have noticed. Sometimes it can take time to get the process ongoing so the advantages will appear. In these cases, it is relevant that the management sees the gains, leads, and gives pressure to get the process started and ongoing.

Information security, like any other security, tends to be an investment that always does not bring immediate, direct benefits or results. If a security incident occurs and causes financial losses, it can be said that security controls may not have been in place.

According to the ISO 31000 standard, and the interviews for the thesis, the role of the top management is significant. As well, in my opinion, the top management of the organization can be one of the keys to keeping the risk management process ongoing and efficient. Therefore, I decided to raise this issue for further study in my thesis.

Shortly after commencement, I learned that it is difficult to find the source literature or research about the subject of engaging management into information security in organizations. It would have been valuable to find various researches about concrete ways to impact management’s engagement. Doctor of Philosophy and Staff productivity researcher and developer Ossi Aura (2016) has also made the observation about the lack of researches concerning the engagement of the top management into projects or operation models without, for instance, bonus systems. He writes engagement of top management in his blog and frets over the lack of information found online.

The few mentions it was able to be found from researches, and other literature was highlighting the importance of the engagement of the top management. For instance, Mary Sumner has made this observation in her study about Critical Success Factors in Enterprise Wide Information Management Systems Projects (Sumner 1999, 223-224).

Other found literature mainly referred engagement of the employees or engagement of the managers by using bonuses or other financial support.

6.1 Problem mapping technique

Jesper Simonsen wrote in his article that the support and engagement of the top management are reported to be constantly the most significant challenge to gain within IT projects (Simonsen 2007, 54). Simonsen introduces in the same study a problem-mapping technique and believes it could be the solution to involve top management in IT projects. Although information risk management is not directly IT project but mostly a way of managing, implementation of it can be treated like one.

With the help of a problem-mapping technique, the IT solution can be visualized and structured. This requires the presence and active participation of top management and other parties and can be accomplished by workshops. The technique requires well-done preparation beforehand by gathering current and explicit information about the organization as well as recognize existing assumptions and hypotheses (Simonsen 2007, 54).

Comparing this into risk management and the ISO 31000 standard, the analysis of operational environment and principles is important, as presented in chapter 3 in the thesis. This can be used for analyzing information security risks in an organization as well. For instance, in the commissioning organization risk management team discussed the culture in the commissioning organization concerning information security. If an employee notices a possible security issue, it is crucial how the IT department will react. Do employees feel comfortable informing the IT team if they notice something or they think they have done something terribly wrong? Such as this kind of information can be used in the problem mapping technique.

As mentioned before, it has been noticed that it is relevant to observe, record, and analyze the starting point, operational environment, and issues that are characteristic to the field or organization type when implementing information security risk management into an organization. Add to this, it is essential to review the most valuable assets for the organization and analyze current and possible information security threats. It is also important to document the observations, review those documentations regularly, and report about critical findings to the (top) management.

The problem mapping technique introduced by Simonsen is based on the concept of a mapping technique. This can be done, for instance, with a piece of paper that will be filled with keywords. These keywords have been collected from the preparation material. These notes will be sorted into four columns: ‘need/problem’, ‘causes’, ‘consequences’, and ‘solutions. Simonsen finds this technique to be simple yet effective for top management to understand the need for information security and its risk management, for instance (Simonsen 2007, 56).

In conclusion, this technique might be a good tool in the implementation of the project. If the top management is involved from the beginning, it may give the advantage to keep the project, or in this case, risk management, ongoing. It is still not a comprehensive tool ensuring the continuity and engagement of the top management, for example, if the persons in the management team change. It is essential to keep in mind that as risk management is a long-term mode of operation, the employees and managers may change over time. This can bring challenges if the engagement is taken into consideration only in the implementation project and not later.

6.2 Involving top management in information security management

According to my observations, engaging management into information security can be easier if there has been a severe information security incident in the past of the organization. Engaging is also easier if directors have had personal experience beforehand, or they have knowledge, interest, or comprehension concerning the security issues. The required financial investments in information security can be at risk if there is no engagement, and the security measures are not comprehended to be necessary and worth it.

There are differences between various industries and how the top management sees the benefits of information security risk management, says Zilliacus (2019). He states that if the business is completely based on data, which is in digital format, the value of the data and benefits of risk management is understood more easily.

The situations may exist where the IT department understands the value of data, and the top management does not or does not realize it. The IT department's comprehension of the business and its needs is in a key position in discovering information-based risks. Nevertheless, there has been no previous security incidents, IT managers should have a genuine dialogue connection to the top management, and they should be able to set out convincingly the risks and benefits of preventing or mitigating them. (Zilliacus 2019).

Rothrock et al. (Rothrock, Kaplan et al. 2018, 2) have researched corporate boards of public companies in the United States in the years 2017 to 2018. Rothrock et al. state that it is important to ensure that the members of the top management understand the responsibility of legal actions and possible consequences. For instance, as there was a massive breach towards Target

Corp. in 2013, and even though the board members were not to be guilty by the law, both CEO (Chief Executive Officer) and CIO resigned. Also, for the top management, it is important to understand that over time, the network will be penetrated, or the system will be breached (Rothrock, Kaplan et al. 2018, 02).

Rothrock et al. (2018) suggest the top management team learn to ask the right questions from the IT department and find together with the IT team the language that both sides understand. This can be difficult since Rothrock et al. have found out that many directors cannot ask the right questions because of missing metrics or numeric targets and adequate understanding of cybersecurity terms. Nonetheless, according to Rothrock et al., directors may spend too much time reading technical reports and trying to understand what this all means for the business. There are solutions to address these issues. One is to have basic cybersecurity training for the directors, which will help them to understand the implications of cybersecurity issues, for example. Investing an hour now and then can make a difference in understanding security risks. Using a third-party consultant who has experience in information security and communication with top management, can be helpful.

Rothrock et al. (2018) also suggest to, for instance, regularly provide meaningful information about the state of data security for the management team. It can be such as a report of the organization’s resilience and state of the digital network, and it should be provided more than once in a year. Discussions on the basis of the report can lead to numerical goals in management, which in turn, can lead to monitoring and actions from directors, as Aura wrote (2019, 20).

The company leadership should be educated about cybersecurity terms, risks, and key elements at a basic level. Managers also need to understand the possible legal implications of information security risks and their realization. This requires the IT team an ability to communicate effectively to the top management by presenting assessments, resilience, and budgeting by using unambiguous metrics and non-technical terminology.

6.3 Interview with the director of the commissioning organization

Because of the scope of engaging the top management, I interviewed one of the directors of the commissioning company Mika Leppinen about the subject and how he sees the continuity of risk management.

Leppinen has worked approximately 25 years as a top manager or part of the top management team. He has also practiced as a district prosecutor. In the commissioning organization The Union of Professional Engineers in Finland, Leppinen has worked approximately two years as one of the four directors (Leppinen, 2020).

His experience of risk management in previous positions has been at the general level, such as recognizing the most critical risks and implementing required measures. This has been done with no use of any specific tool or method. In the commissioning organization, Leppinen is part of a risk management implementation project in which the goal is to have a risk management method as part of managing business-critical risks (Leppinen, 2020).

Leppinen (2020) notes that mensurable goals are more accessible and more meaningful to follow than qualitative goals. He finds mensurable goals also more motivating as it is possible to state if the goal is reached or not. If there is only a qualitative goal, one can never be sure if the goal is reached or not. Among mensurable targets, he also mentions that goals that motivate must also be objectively possible to achieve.

What it comes to operating as a director, Leppinen experiences that correctly implemented risk management methods may offer par excellence protection for the person responsible at the individual level, who, in several cases, is part of the top management team. At least, this may be the case with business-critical risks or other legal responsibilities. The continuity of risk management from this point of view is indisputably a benefit for the top management and thereby helps with commitment (Leppinen, 2020).

Leppinen (2020) finds risk management to be a useful tool for managing, for example, information security risks. It can be a prove of goal-oriented daily operation and management. It also can prevent incidents that can affect legally or undermine operation.

What it comes to the continuity issue, according to Leppinen, risk management, or some other operation method, could be kept ongoing among employees by compensations or bonuses rather than demanding reports or having strict control. Recording risk management checkpoints into the annual planning cycle is also an excellent way to create a frequent operating model. Leppinen finds that the overall positive culture, covering colleague's backs and being loyal towards the employer to be in key position handling and observing risks in everyday operation.

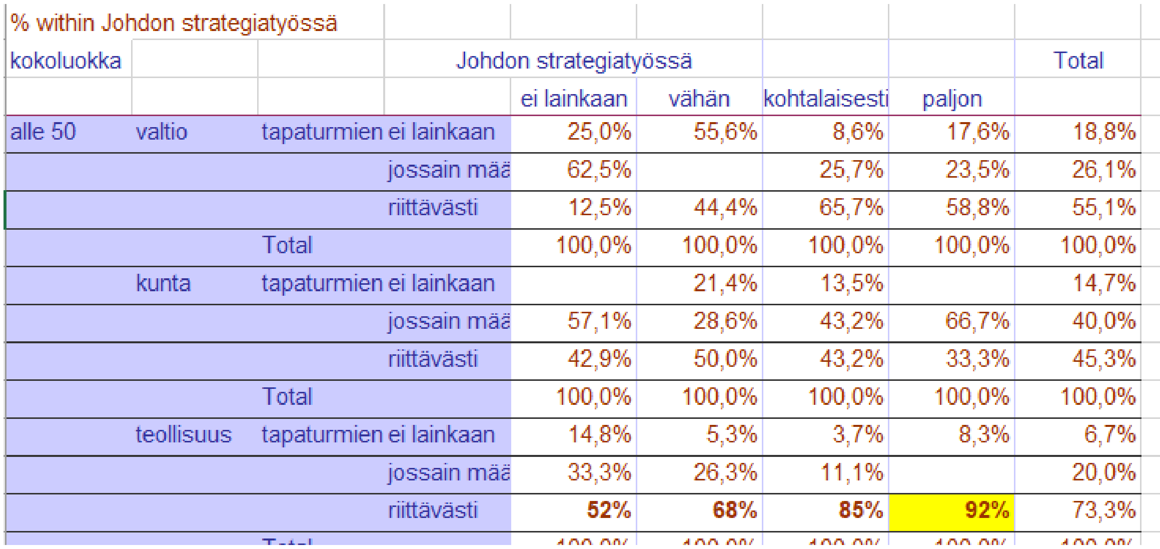
6.4 Importance of clearly defined objectives

As Leppinen mentioned in the previous chapter, concrete goals and intermediate steps can help maintain interest and pace. This is the reason I studied the ways to further the commitment of top management. Although the focus is on top management, one can think of the concrete goals to be useful for motivating the IT team also.

Aura (2019, 20) has studied staff productivity management in the industrial sector, engagement of the management and leaders in it. This information can be useful in security management as well.

Aura (2019) has noticed the lack of numerical objectives among management in staff productivity. He noticed in his research that the level of the concreteness of objectives is rather weak in different aspects of management what it comes to staff productivity. For instance, in industrial safety, only 22% of the respondents' managers had a numerical target, and 35% of respondents had no target in any shape or form. In other fields, the percentages were even weaker.

Aura also noticed in his study (2019) that if the top management has taken a matter into account in the organization’s strategy, the matter, whatever it is, will more likely to be handled more sufficiently. This was the case with analyzing reasons for accidents in industry organizations employing less than 50 people in the years 2009-2018. According to Aura's research (2019), if top management took the analysis into account its strategy work, 92% of the organizations in which this was made, accomplished analyzing reasons for accidents in a sufficient level. This is illustrated with a chart in Figure 13.



% within Johdon strategiatyössä								
kokoluokka				Johdon strategiatyössä				Total
				ei lainkaan	vähän	kohtalaisesti	paljon	
alle 50	valtio	tapaturmien	ei lainkaan	25,0%	55,6%	8,6%	17,6%	18,8%
			jossain mää	62,5%		25,7%	23,5%	26,1%
			riittävästi	12,5%	44,4%	65,7%	58,8%	55,1%
		Total		100,0%	100,0%	100,0%	100,0%	100,0%
	kunta	tapaturmien	ei lainkaan		21,4%	13,5%		14,7%
			jossain mää	57,1%	28,6%	43,2%	66,7%	40,0%
			riittävästi	42,9%	50,0%	43,2%	33,3%	45,3%
		Total		100,0%	100,0%	100,0%	100,0%	100,0%
	teollisuus	tapaturmien	ei lainkaan	14,8%	5,3%	3,7%	8,3%	6,7%
			jossain mää	33,3%	26,3%	11,1%		20,0%
			riittävästi	**52%**	**68%**	**85%**	**92%**	73,3%
		Total		100,0%	100,0%	100,0%	100,0%	100,0%

Figure 13. Percentage of the organization in which the well-being at the work has increased (Aura 2019)

According to Aura’s studies and observations (2019, 20), all in all, successful management and leadership base on numerical targets, which can enable the monitoring of different occurrences and efficiency of procedures.

Zilliacus (2019) suggests dividing the risk, target system, or operational method under development into small pieces and trying to discover numerical objectives, though it might seem to be difficult at first. For instance, if there is a risk that the customer data in the CRM-system does not evolve because the system is not used and the data is not recorded, the solution for discovering numerical values could be monitoring the amount of the records of only a few users. If the starting values indicate the lack of records in the system, one can be done some corrective measures. This can be such as directions from the management. After the corrective actions, the values of records can be calculated again and make a comparison if there has been any (positive percentual) development.

In the commissioning organization, these numerical checkpoints could be added in the IT department’s annual planning cycle as wherein the risk management checkpoints are. This procedure may enable the continuity of monitoring these numerical measurements.

Gaining an interest of the top management towards information security increases if there are numerical arguments to present. This can be done, for instance, reporting the most significant, potential risks or proves of reduction of impacts. If there are not yet meetings together with top management about data and information security, adding meetings in the annual planning cycle could be in place to do (Zilliacus, 2019).

In the following discussion and conclusion chapters, I will summarize my findings and review the actions I could recommend implementing.

7 DISCUSSION

With this thesis, my goal was to find out what could be the most effective ways to ensure that information security risk management will meet the continuity after the implementation project. I studied for Finnish small and medium-sized enterprises in which the commissioning organization is included.

I study from the point of view of Finnish SMEs because I believe that the stakes can be even higher with smaller or medium-sized companies as realized risk may cause more severe impact than in larger organizations with, for instance, more financial capital to recover. Furthermore, in SMEs, risk management is not required by the law but the usually voluntary operation of an organization.

If risk management is not top management-oriented, required by the law, or has some other compelling reason, my initial study before writing the thesis showed it would quickly be forgotten after the implementation. The interviews later provided the same observation. The experienced benefits of risk management, in many cases, will help a particular course of action to meet the continuity. Still, with risk management, the advantages may not appear right after the beginning of the introduction of it. This has been noticed by my interviewed professionals working with information security risk management and SMEs. I found the continuity aspect essential to study and write the thesis about it because in the commissioning organization, The Union of Professional Engineers in Finland, this is the topical challenge. The time, effort, and financial investment that has been made in the implementation should not be wasted.

From a financial point of view, risk management is available for every sized organization. As I have also found out, risk management is not expensive to bring into use, albeit it requires work and commitment.

As I have been able to work with risk management in the target organization, I have discovered it overall to be a competent tool for managing information security and essential tool for the information security manager. If risk management is made carefully with thought, I have learned that it will additionally help to organize the daily operation of the IT department in many other ways. It will ease prioritizing critical risks, which helps to prioritize the need for measures. It can also give guidelines for setting up a budget, for instance.

Information security is not only the IT department's inconvenience, but its tentacles extend in other operations and departments. Primarily information risk management aims to take into consideration risk from every perspective as well as encourages communication between different teams and interest groups inside and outside the organization. The amount of work and commitment is significant, so the continuity will not be carried out effortlessly.

This conclusion I have done according to many literature sources, several interviews and my own hands-on-experience. I find my most important sources to be the interviews of risk management professionals (in chapter 4), the ISO 31000 standard (chapter 3), and my own experience enabled by the possibility to work with risk management in the target organization.

There have been cases I have been argued about why wasting managers' or employees' time on risk management; would it be more efficient to use the time handling the risks as they occur. Alternatively, it has been said that it would be more efficient as the main risks are mainly known, and the actions can be implemented whenever the situation requires.

These objections can do harm to the continuity of risk management if they are coming from the top management, from the IT team, or they are your doubts. Have no tolerance for uncertainties and, in contrast, gather good arguments and current knowledge for yourself and others.

One can agree with the matter that information security is essential. It is especially important in organizations in which any data in digital form is business-critical. Information security must always be managed somehow and entrusted to be operational and efficient. This does not differ from if the security is outsourced at some level. After all, the ultimate responsibility is always in the organization itself and people who work there.

In the digital world, if the goal is to run IT efficiently by making rational and safe decisions and leading the operation in a controlled manner, it involves some operation models and rules to follow. Operating by these rules and procedures, in turn, involves documentation like policy documents. Documentation has several positive features, for instance, if the person responsible changes. It may not be sensible to reinvent the wheel but reciprocally use existing well-tried documentation. As one follows these provided suggestions and instructions, the information security management will be taken care of at a sufficient level, at least. I find that there are several excellent and prepared documentation, best practices, and free tools available for every sized organization, as I have proved in chapters 3 and 5.

In my opinion, if some matter is "under control," it means it is truly controlled. It involves systematic operation, well-performed documentation, and every action has sensible grounds. Nothing depends just on gut feeling. This is, for me, a part of true professional skills and essential value that risk management represents.

The “lost” time in risk management is an investment for a more safe and controlled future.

I interviewed four professionals working with risk management. Albeit, the number of interviewees was small, I got valuable information because the interviewees work with many organizations. My interviews with four risk management professionals gave valuable information on the current situation of risk management in Finnish organizations. They and their customers seem to prefer ISO standards, likewise our organization. For ensuring the continuity of risk management, it is good to lean the practical operation of it on standards and tools that are generally and internationally stated to be valid. The ISO 31000 standard and VAHTI risk management tool are a safe choice even though they are not the only ones available. If the tool like VAHTI risk management tool offers prioritizing, goal-oriented and mensurable operation towards risks, it will undoubtedly help with the continuity challenge.

The interviewees recognized the problem with the continuity of information security risk management, especially in SMEs. The identified common challenge seems to be the lack of commitment of top management. Likewise, the problems may be too heavy implementation, non-existence of knowhow, or prioritizing. These can be reasons which result in forgetting risk management after the implementation project.

Due to these observations, I recommend focusing on engaging the top management and the operation of the IT team by ensuring the risk management process to be as light and as practical as possible. This will secure the continuity of it after the implementation. If the IT and the top management team have an annual cycle plan, risk management or parts of it should be found from those as well.

I would have wanted to do more examination of engaging the top management into information security and its risk management. However, the challenge I met was the shortage of the number of literature references, such as researches. I managed to find the literature on how to engage management with financial bonuses, but in the commissioning organization like in many SMEs, the bonus systems are not possible or otherwise sensible. I find this topic to be relevant to be researched in the future, especially from the information security point of view.

The research by Susi about the state of information security in SMEs in Finland did give a good outlook. However, analysis of SMEs' top management approach towards information risk management would be interesting to have in the future as well. Because of the limited time and resources, I left out the interviews of the SME IT managers besides the IT manager of the commissioning organization. Those interviews would possibly bring some interesting insights and perspectives. Whereas, I utilized the experience of the interviews of professionals who work with SMEs, their IT managers, and top management.

In an IT team or under the leadership of an IT manager, the continuity of information risk management can be ensured in many ways as well. These measures can be implemented with or without the engagement of the top management. However, it is clear that with the strong support of the top management, the effectiveness of risk management is more reliable. Engaging top management may require, for instance, form the IT manager some sales expertise and skills to reason clearly why information risk management is essential, why it improves security and why the top management’s support is required.

The study for the thesis shows that risk management benefits from mensurable targets. The mensurable target helps to comprehend if the goal is reached or not and may offer extra motivation. Numerical or mensurable goals can be given from the top management, or IT manager can make a decision of them. In VAHTI risk management tool, mensurable goals can be the date of an objective check, for instance. Adding numerical values in the column 'Suggestion for action to address the risk' helps to prioritize actions that need to be done to mitigate the risk.

My conclusion is that if the data is business-critical for the organization and the top management is engaged to protect it and monitor related risks, the information security increases. Finding numerical measurements and bringing the protection of data in the strategy of the organization will increase the security as well. The commissioning organization does not yet have the information security in its strategy. From my point of view, this is something that may require consideration. At the moment, the mensurable goals concerning information security are risk management oriented. In information security, the next step in the union is to obtain risk management to be more systematic, lighter, and concrete.

8 CONCLUSIONS

With this thesis, my goal was to find out how to get information on security risk management as an ongoing course of action after the implementation project in small and medium-sized organizations. It is a danger that risk management will be forgotten soon after the implementation. This challenge was recognized in the commissioning organization, The Union of Professional Engineers in Finland as well. In conversations with some people in the trade, I learned that the same challenge was a more general issue, and that led me to choose the main title for this thesis.

As I researched risk management as a method for managing security issues, I learned that it is an excellent tool for managing information security in organizations, notwithstanding the size or industry of it. I noticed that standards such as the ISO 31000 are rational methods to use in risk management because they are international, widely used, pragmatic, and continuously evolving. Furthermore, following the ISO 31000 standard supports a better understanding organization’s operational environment and various points of view in it.

Avoiding potential security risks is part of the proficient operation of the IT department. Especially information security risk in today’s world can cause stress and the feeling of being out of control. Having potential risks listed and measures being decided and scheduled can elevate one’s mindfulness of the state of the organization’s information.

Possible risks need to be rationalized to many parties in organizations and its domain. It is not convincing to simply claim that, for instance, the cloud service is riskier than on-premises solutions or vice versa. One must have reasonable arguments on either solution’s potential consequences and/or effects. Risk management is a useful method justifying and reasoning for specific actions or use of resources. It will also ease the decision making, such as prioritizing measures and planning budgets. All this is ineffective unless risk management is implemented systematically, comprehensively, and continuously.

To meet the continuity with risk management in SME is not easy as it requires resources, mostly time and brainwork. It requires commitment and entrusts to its benefit of existence.

The support of the top management plays a vital role in the continuity of risk management. In optimal conditions, the top management sees the benefits and understands its responsibility, ultimately before the law. If top management shows an interest in information security operation and risk management, it can provide enough resources and motivation for everyday work. This may not be so, if the managers or the organization itself have no experience of security incidents or there have been no severe incidents concerning rival companies, for instance.

If the top managers show no interest in information security and its risk management, I suggest trying to sell the idea to them by presenting benefits in a simplified form and giving some measurable targets if possible. If an issue requires a decision from the top management, in my opinion, the best way is to make a ready, concrete proposition with as few technical terms and descriptions as possible. It is also essential to add reasonable arguments to the proposition so the top management can make more straightforward decisions. Moreover, the interest of the top management will increase if one can deliver clear reports of the risks which need the most attention. This can be arranged, for instance, twice a year. All of these actions will involve top management in information security risk management.

In the IT or risk management team, including information security risk management into an annual cycle plan, is recommended. Reviewing assessable objects, for instance, twice a year, is, in many cases, sufficient. My advice is to avoid making risk management too heavy and all-embracing. At first, it is relevant to focus on the most critical systems and their substantial risks. When risk assessment becomes a routine, adding systems and points of view gets easier. Using an outside consultant and keeping up a dialogue with him/her will help with the continuity issue.

During studying risk management and writing the thesis, I have noticed my comprehension of the state of information security in the commissioning organization has increased. For any IT professional, this is valuable knowledge as well as understanding the operational environment, having a comprehensive outlook for potential threat scenes, and having the ability to process with the most significant risks. All this will give me the motivation to work with information security risk management continuously by assessing risks, systems, and modes of operation.

To conclude, I offer a few positive words for anyone who is working with information security, including myself: Appreciate the benefits that risk management serves. Stop and see the big picture and the advantages it will offer in the long run. Roll up your sleeves and start the job. Be persistent. Enjoy the raffle prizes that come along the way. Get excited, and encourage the rest too! Moreover, finally, share information about successful risk management with others!

REFERENCES

Aura, O. 2019a. Henkilöstötuottavuuden johtaminen 2018, aineiston lisäanalyysit. Not available from a public source.

Aura, O. 2019b. Henkilöstötuottavuuden johtaminen teollisuudessa. Helsinki: Ossi Aura Consulting Oy.

Capterra. No date. Risk management tools. WWW document. Available at: https://www.capterra.com/sem-compare/risk-management-software?gclid=EAIaIQobChMInqXfzaCu6QIVxQ8YCh0efAviEAAYASAAEgL5MfD_BwE [Accessed 28 March 2020]

Ferreira, G. 2018. Comparing ISO 31000 and ISO 27000. WWW document. Available at: https://theriskacademy.org/is0-31000-iso-27005/ [Accessed 3 January 2020].

Harris T. & Mitchell K. 2012. Resilience: A risk management approach. PDF document. London: Overseas Development Institute. Available: https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7552.pdf [Accessed 20 February 2020].

The Union of Professional Engineers in Finland. No date. WWW document. Available: https://www.ilry.fi/yhteystiedot-0/union-professional-engineers-finland [Accessed 16 April 2019].

International Organization for Standardization. No date a. About us. WWW document. Available: https://www.iso.org/about-us.html [Accessed 4 August 2019].

International Organization for Standardization, No date b. Standards in our world. WWW document. Available: https://www.iso.org/sites/ConsumersStandards/1_standards.html [Accessed 4 July 2019].

Jordan E. & Silcock L. 2005. Strateginen IT-riskien hallinta. West Sussex, England: John Wiley & Sons Ltd.

Järveläinen, J., Niemimaa, M.& Zimmer, M. (2017). Mindfulness parantaa jatkuvuutta ja luotettavuutta. Turvallisuus & Riskienhallinta. PDF-document. Available: https://www.researchgate.net/publication/319187538_Mindfulness_parantaa_jatkuvuutta_ja_luotettavuutta [Accessed 24 February 2020].

Leppinen, M. 2020. Director of services. Interview 3 February 2020. The Union of Professional Engineers in Finland.

Malinen, K. 2020. Head of IT services. Interview 17 February 2020. The Union of Professional Engineers in Finland.

Online Etymology Dictionary. No date. WWW Document. Available: https://www.etymonline.com/word/risk [Accessed 20 October 2019].

Pervilä, M. 2018. Näillä keinoilla riskit kuriin ja innovaatiot eloon. Tivi 28 April 2018. https://www.tivi.fi/CIO/nailla-keinoilla-riskit-kuriin-ja-innovaatiot-eloon-6722652 [Accessed 28 October 2019]

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Helsinki. Aalto-yliopisto, sähkötekniikan korkeakoulu, elektroniikan laitos.

Puistovirta, J. 2019. Lead auditor. Email interview 6 March 2019. Kiwa Inspecta.

Puolustusministeriö, 2015. Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille. PDF.document. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf [Available 20 December 2019]

Räty, J. 2019. Director, Information Security and Quality. Email interview 18 November 2019. Aditro AB.

Rothrock, R.A., Kaplan, J., Oord, F.V.D., 2018. The Board's Role in Managing Cybersecurity Risks. MIT Sloan Management Review, 59(2), 12.

Rousku, K. 2017. Ohje riskienhallintaan. PDF-document. Available: http://urn.fi/URN:ISBN:978-952-251-862-0 [Accessed 17 August 2019]

Simonsen, J. 2007. Involving top management in IT projects. Communications of the ACM, 50(8), 52-58.

Soo Hoo, K.J. 2000. How much is enough: A risk management approach to computer security, Stanford University. PDF-document. Available: https://www.files.ethz.ch/isn/20032/How_Much_Is_Enough.pdf [Accessed 16 October 2019]

Sumner, M. 1999. Critical success factors in enterprise wide information management systems projects. PDF-document. Available: https://dl.acm.org/doi/pdf/10.1145/299513.29972 [Accessed 28 November 2019]

SFS-ISO 31000:2018. 2018. Risk Management - Guidelines.

Susi, M. 2019. Risk manager (EQM). Email interview 12 April 2019. Elinkeinoelämän keskusliitto.

Susi, M. 2018. Turvallisuudesta kilpailuetua – Yritysten näkemyksiä ja viestejä turvallisuudesta. Helsinki: Elinkeinoelämän keskusliitto EK.

Tilastokeskus. No date. Käsitteet. WWW document. Available: https://www.stat.fi/meta/kas/pk_yritys.html [Accessed 9 November 2019].

U. S. Department of Commerce. 2012. Guide for Conducting Risk Assessments: Nist Special Publication 800-30, Revision 1. Gaithersburg: Computer Security

Division Information Technology Laboratory National Institute of Standards and Technology

Väisänen, L. 2018. Riskienhallinnan periaatteet - menestyksen avaimet. WWW document. Available: https://www.sfsedu.fi/ajankohtaista/riskienhallinnan_periaatteet_-_menestyksen_avaimet.839.news?439_o=30 [Accessed 15 October 2019]

Valtionvarainministeriö, 2017. Riskienhallintatyökalu. Excel-document. Available: http://vm.fi/documents/10623/1898625/Riskiarviointi+laaja/3980a4f9-d94b-4014-a259-3c46fe1a05ab [Accessed 23 February 2019]

Valtionvarainministeriö. No date a. Riskienhallintapolitiikka. WWW document. Available: https://vm.fi/riskienhallinta/riskienhallintapolitiikka [Accessed 5 February 2019].

Valtionvarinministeriö. No date b. Riskienhallintapolitiikkamalli. Word document. Available: https://vm.fi/documents/10623/307569/Riskienhallintapolitiikkamalli.docx/bd6687cd-c4c4-4e79-87f8-a6db82d138b9 [Accessed 5 February 2019]

Valtionvarainministeriö. No date c. VAHTI-ohje. WWW document. Availabe: https://www.vahtiohje.fi/web/guest/691 [Accessed 27 February 2019]

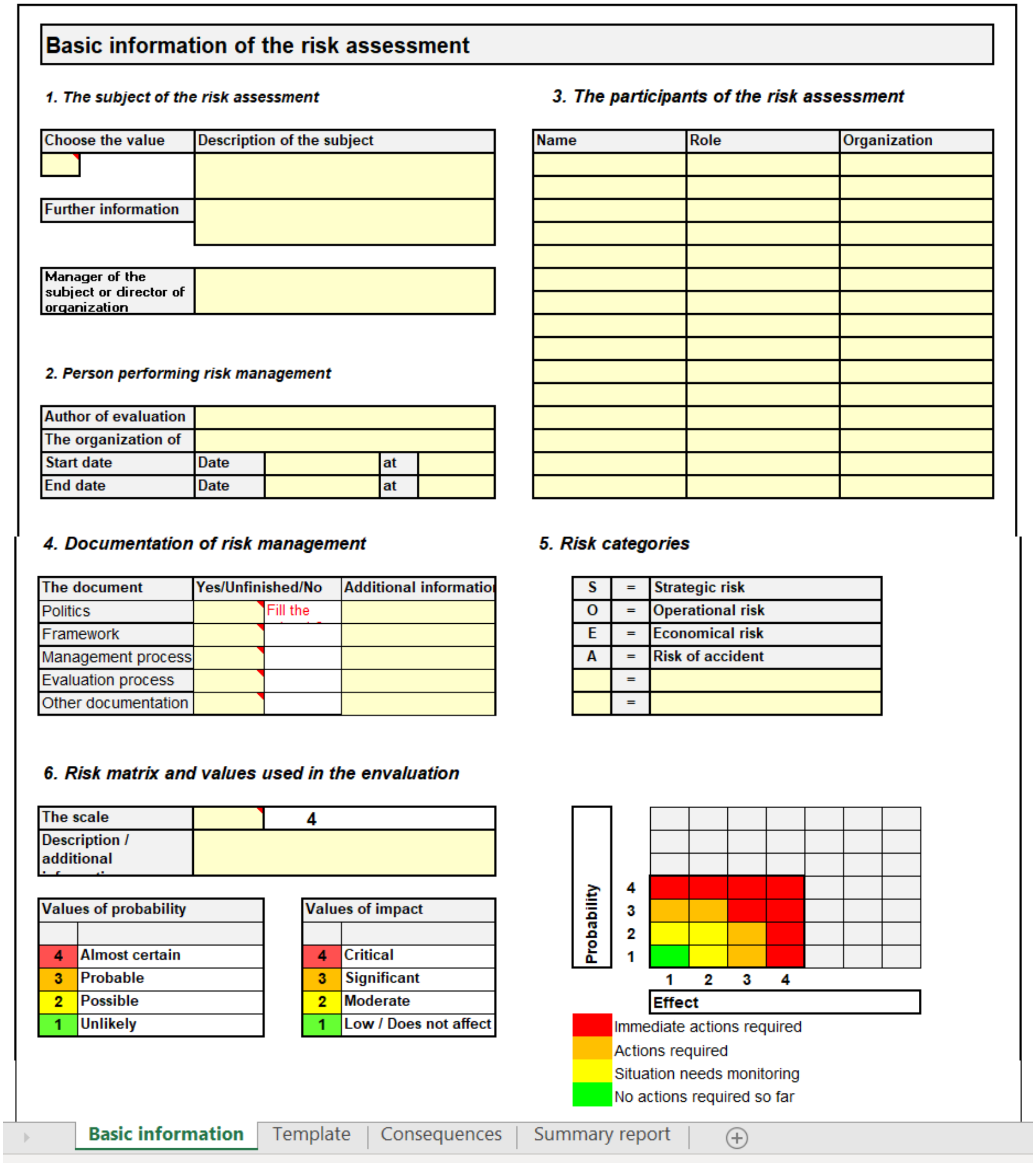
Zilliacus, J. 2019. CIO. Phone interview 8 March 2019. Morral Mobile.

LIST OF FIGURES

APPENDIX

VAHTI risk management tool

Basic Information -tab:



Basic information of the risk assessment

1. The subject of the risk assessment

Choose the value	Description of the subject
Further information	
Manager of the subject or director of organization	

3. The participants of the risk assessment

Name	Role	Organization

2. Person performing risk management

Author of evaluation				
The organization of				
Start date	Date		at	
End date	Date		at	

4. Documentation of risk management

The document	Yes/Unfinished/No		Additional informatio
Politics		Fill the	
Framework			
Management process			
Evaluation process			
Other documentation			

5. Risk categories

S	=	Strategic risk
O	=	Operational risk
E	=	Economical risk
A	=	Risk of accident
	=	
	=	

6. Risk matrix and values used in the envaluation

The scale		4
Description / additional		

Values of probability	
4	Almost certain
3	Probable
2	Possible
1	Unlikely

Values of impact	
4	Critical
3	Significant
2	Moderate
1	Low / Does not affect

Probability					
	4	🟥	🟥	🟥	🟥
	3	🟧	🟧	🟥	🟥
	2	🟨	🟨	🟧	🟥
	1	🟩	🟨	🟧	🟥
		1	2	3	4
		Effect			

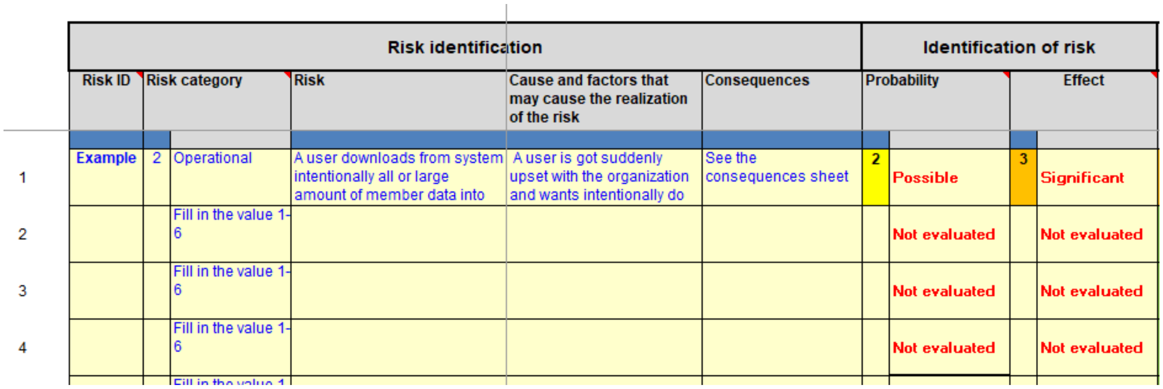
🟥 Immediate actions required

🟧 Actions required

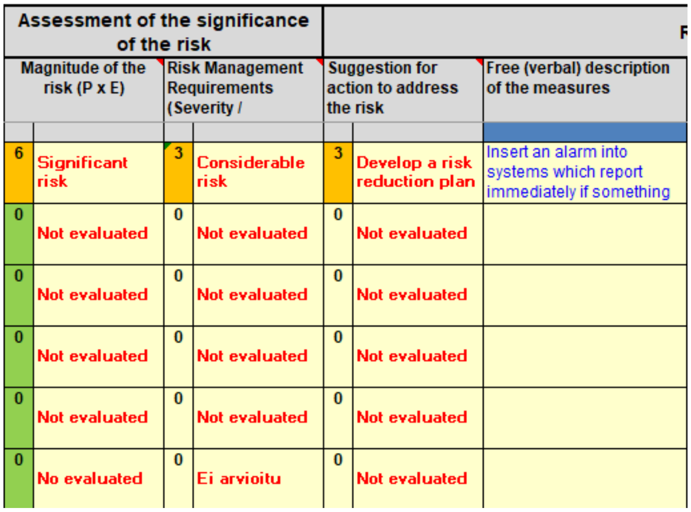
🟨 Situation needs monitoring

🟩 No actions required so far

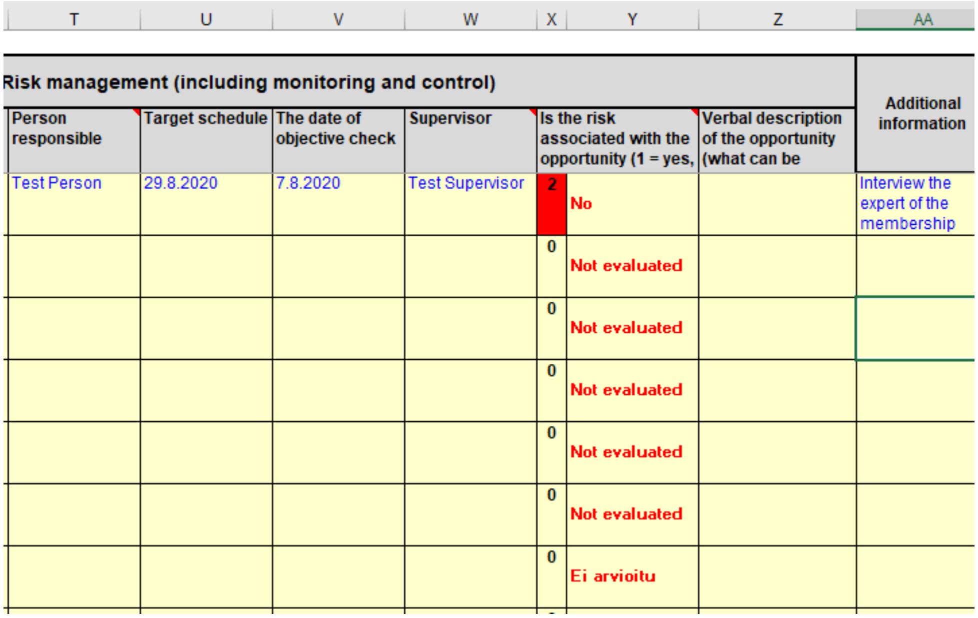
Template -tab:



	Risk identification						Identification of risk			
	Risk ID	Risk category		Risk	Cause and factors that may cause the realization of the risk	Consequences	Probability		Effect	
1	Example	2	Operational	A user downloads from system intentionally all or large amount of member data into	A user is got suddenly upset with the organization and wants intentionally do	See the consequences sheet	2	Possible	3	Significant
2			Fill in the value 1-6					Not evaluated		Not evaluated
3			Fill in the value 1-6					Not evaluated		Not evaluated
4			Fill in the value 1-6					Not evaluated		Not evaluated
			Fill in the value 1							

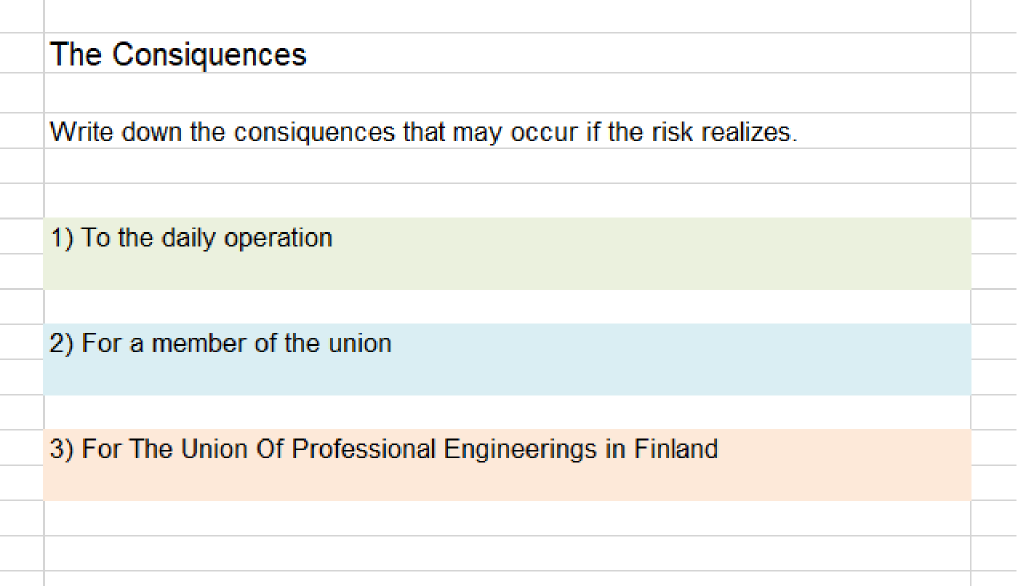


Assessment of the significance of the risk				R		
Magnitude of the risk (P x E)		Risk Management Requirements (Severity /		Suggestion for action to address the risk		Free (verbal) description of the measures
6	Significant risk	3	Considerable risk	3	Develop a risk reduction plan	Insert an alarm into systems which report immediately if something
0	Not evaluated	0	Not evaluated	0	Not evaluated	
0	Not evaluated	0	Not evaluated	0	Not evaluated	
0	Not evaluated	0	Not evaluated	0	Not evaluated	
0	Not evaluated	0	Not evaluated	0	Not evaluated	
0	No evaluated	0	Ei arvioitu	0	Not evaluated	



T	U	V	W	X	Y	Z	AA
Risk management (including monitoring and control)							Additional information
Person responsible	Target schedule	The date of objective check	Supervisor	Is the risk associated with the opportunity (1 = yes,		Verbal description of the opportunity (what can be	
Test Person	29.8.2020	7.8.2020	Test Supervisor	2	No		Interview the expert of the membership
				0	Not evaluated		
				0	Not evaluated		
				0	Not evaluated		
				0	Not evaluated		
				0	Not evaluated		
				0	Ei arvioitu		

Consequences-tab:



The Consiquences

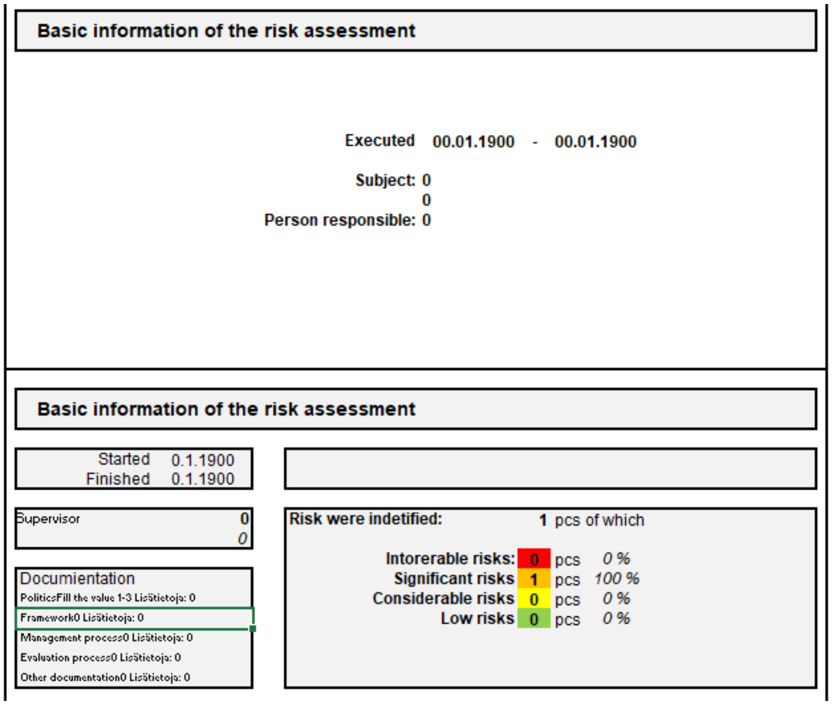
Write down the consiquences that may occur if the risk realizes.

1) To the daily operation

2) For a member of the union

3) For The Union Of Professional Engineerings in Finland

Summary report -tab:



Basic information of the risk assessment

Executed 00.01.1900 - 00.01.1900

Subject: 0
0
Person responsible: 0

Basic information of the risk assessment

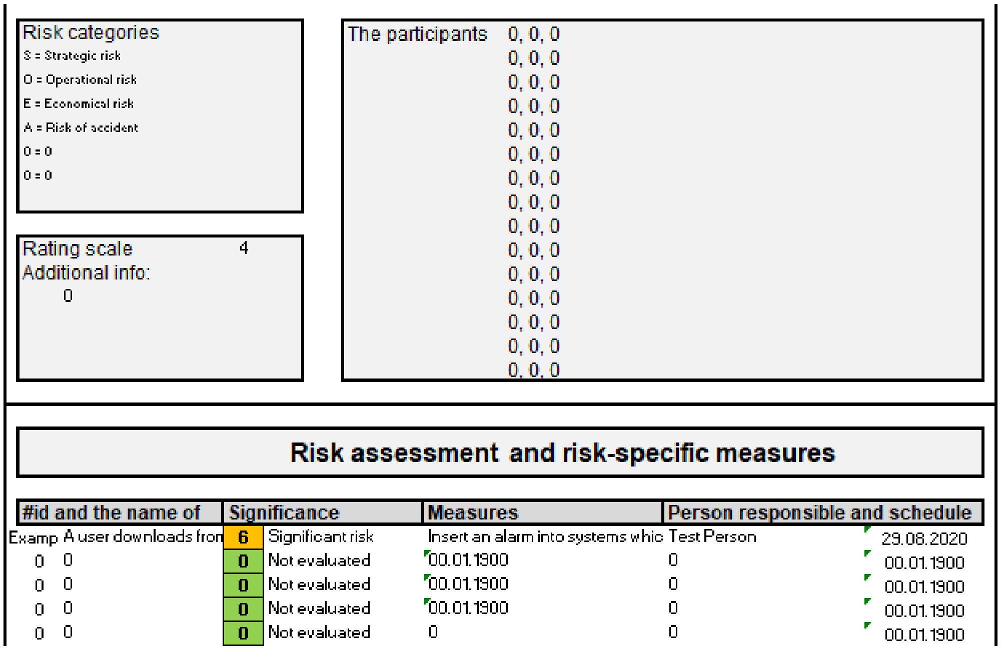
Started 0.1.1900
Finished 0.1.1900

Supervisor 0
0

Documientation
PoliticsFill the value 1-3 Lisätietoja: 0
Framework0 Lisätietoja: 0
Management process0 Lisätietoja: 0
Evaluation process0 Lisätietoja: 0
Other documentation0 Lisätietoja: 0

Risk were indetified: 1 pcs of which

Intorerable risks:	0	pcs	0 %
Significant risks	1	pcs	100 %
Considerable risks	0	pcs	0 %
Low risks	0	pcs	0 %



Risk categories
S = Strategic risk
O = Operational risk
E = Economical risk
A = Risk of accident
0 = 0
0 = 0

Rating scale 4
Additional info:
0

The participants 0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0
0, 0, 0

Risk assessment and risk-specific measures

#id and the name of		Significance		Measures	Person responsible and schedule	
Examp	A user downloads fron	6	Significant risk	Insert an alarm into systems whic	Test Person	29.08.2020
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	00.01.1900	0	00.01.1900
0	0	0	Not evaluated	0	0	00.01.1900