Julia Boksha

Operational risk assessment exercise and process proposition

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Koulutusohjelman nimi

Insinöörityö

29.5.2017

Tekijä(t) Otsikko Sivumäärä Aika	Julia Boksha Operatiivisten riskien kartoitus ja prosessiehdotus 46 sivua + 4 liitettä 29.05.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tuotantotalous
Suuntautumisvaihtoehto	Kansainvälinen ICT-liiketoiminta
Ohjaaja(t)	ICT-yksikön johtaja, kohdeyritys Ohjaaja Nina Hellman

Kohdeyritys on iso useita tuhansia työntekijöitä työllistävä organisaatio ja työ tehtiin sen ICT-osastolle. ICT-osasto palvelee yhtä konsernin liiketoiminnoista. Osaston liiketoimintahaasteena oli epäsäännöllinen ja puutteellinen operatiivisten riskien riskienhallintaprosessi ja näin ollen puutteellinen tietoisuus sen olemassa olevista riskeistä. Työn tavoite oli suorittaa operatiivisten riskien kartoitus ja arviointi, sekä laatia prosessiehdotus tulevaisuutta varten. Lopputuloksena olivat dokumentoidut riskitaulukot ja teorian sekä tavoitteiden ja kartoituksen pohjalta laadittu riskiarvioinnin prosessi.

Työ toteutettiin tapaustutkimuksena. Se koostuu nykytila-analyysista, tutustumisesta olemassa olevaan tietoon sekä ratkaisusta. Nykytila-analyysi tehtiin usean haastattelun ja sisäisen dokumentaation pohjalta. Haastateltiin sekä ICT-osaston että sen asiakasliiketoiminnan työntekijöitä. Tunnistettiin osaston riskienhallintaan liittyvät vahvuudet ja heikkoudet. Jälkimmäisiin perustuen valittiin tarpeellinen kirjallisuus riskienhallinnan prosessista ja sen implementoinnista. Ratkaisu rakennettiin perustuen kirjallisuudesta opittuun tietoon ja kohdeosaston tarpeisiin. Tämä tehtiin kahdessa iteraatiossa, joissa molemmissa pilotoitiin ehdotettu prosessi suorittamalla riskikartoitus ja –arviointi kohdeosastossa.

Lopputuloksena on syntynyt dokumentaatio olemassa olevista riskeistä ja niiden arvioinneista, joka on arvokas panos kohdeosaston päätöksentekoon, investointipäätöksiin ja kehitystyöhön. Organisaation tavoitteiden mukaisia säännöllisiä riskiarviointeja tukee tässä työssä ehdotettu riskiarviointiprosessi. Tämä auttaa kohdeosastoa saavuttamaan tavoitteensa operatiivisten riskien pienentämisessä.

Työn lopputulos vastaa hyvin kohdeosaston tarpeisiin ja alussa asetettuun tavoitteeseen. Kohdeyritys oli tyytyväinen työhön ja työn lopputulokset otettiin heti käyttöön kehitystyössä.

Avainsanat	Riskienhallinta, riskikartoitus

Author(s) Title Number of Pages Date	Julia Boksha Operational risk assessment exercise and process proposition 46 pages + 4 appendices 29 May 2017
Degree	Bachelor of Engineering
Degree Programme	Industrial Management
Specialisation option	International ICT business
Instructor(s)	Head of the ICT department, case company Nina Hellman, Senior Lecturer

The case company is a large organization with several thousand employees, and thesis study was conducted for its ICT department. The business challenge was to build a proposition of an operational risk assessment process for the case department and carry it out. Therefore, the intended outcome of the thesis study was the risk assessment process proposition and documented risks.

The thesis study was executed as a case study and consists of the current state analysis, review on the existing knowledge and formation of the solution. Interviews with the management of the case department and its customer department and internal documentation were used for the current state analysis. Existing knowledge and best practice were chosen for further study based on the weaknesses identified in the current state analysis. The theory part covers basic concepts of risk management and the risk assessment process. In addition, the best practice on implementing the risk management process was explored in order to design the process easy to adopt. Based on the theory and the needs of the case department, the process proposition was built. This was done in two iterations, simultaneously piloting proposed process by performing the risk assessment in the case department.

The outcome of this thesis study is the process proposition and documentation of the conducted risk assessment. The latter one provides visibility into case department risk environment and a valuable input into the development of decision-making activities. The process proposition enables running regular risk assessment in the future, which is aligned with the strategy of the whole organization and supports achieving goals of the case department.

The outcome of the thesis study meets the needs of the case department and appears as intended. The department was satisfied with the results and utilized them in their development activities immediately.

Keywords	risk management, risk assessment

Sisällys

Liitteet

Lyhenteet

ORM	Operational Risk Management
ERM	Eneterprise Risk management
CSA	Current State Analysis

1 Introduction

This thesis study was carried out for an ICT department in a large company. The purpose of the study was to perform an operational risk assessment exercise and provide guidelines for the risk assessment process for the future use. The need for the study was recognized by the management of the case department, but also dictated by the organizational and industrial regulation requirements. The study provides the case department more knowledge on the current risks, which supports its decision making and communicating the risks to the stakeholders.

The risk tables are only for the company use. The templates with evaluated coded risks can be found in appendixes.

1.1 Background of the case company

The case company is a large concern operating in several countries with several thousand employees. It serves individual customers as well as business and institutional customers.

The organization of the case company in Finland is a complex matrix. Entities forming the concern are quite independent and enjoy cross-concern supporting organizations such as Technology & Development, Legal Services, Procurement and Service Delivery. These functions have the business entities as their customers.

The case department belongs to Technology & Development organization and has a few dozen employees. It serves one of the concern entities. The organization within the department is quite flat consisting of the Head of the Unit, Development Managers, Service Delivery Managers, IT-support team and developers. Service Delivery for most applications is outsourced to the third party vendor and controlled by Service Delivery Managers from the case company side. The main responsibilities of the case department are managing development of the application environment, development of applications according to the business demands and, most importantly, ensuring the continuity of application services for the business needs.

1.2 Business challenge

The need for this thesis came from Development & Technology Department of one of the entities within the concern. According to the concern strategy, operational risks of each business unit should be reviewed and documented annually, following up with mitigation actions. However, ways of doing the exercise are not determined and left to be decided by the units themselves. The process had never been established by the case department and risk identifications and reviews had not been carried out systematically. Therefore, the department was not able to meet its strategic goal of reducing operational risks. Development road maps were not related to the reality and lack of the complete information on the day-to-day risks was affecting decisions of the management.

1.3 Objective and intended outcome

To be able to meet the concern strategy and to secure the availability of the providing services, the case department recognized the need of operational risk identification and evaluation exercise and process proposition for that in the future. The objective of this thesis study was to carry out the operational risk assessment in the case department and provide process proposition for the future assessments. To do this, best practices for doing Risk Management must be researched and adapted for the case department.

Therefore, the intended outcome of this thesis would be a risk assessment process proposition and identified and documented and assessed risks found during the risk assessment.

The case department would benefit from the results of this thesis study gaining more knowledge on the current operational risks and having the guidelines to carry out risk assessments in the future. It would help the case department to review its risks regularly, which will allow having a better control over them. The case department would also get more accurate and complete information for decision-making and a clearer view on the future development needs.

1.4 Scope

This thesis focuses on the operational risk identification and assessment. Only the case department is within the scope of the thesis. Scope includes an operational risk identification and evaluation of most business critical application related risks. This scope was seen most valuable for the case unit as its main responsibility is to ensure functionality of the most business critical applications. The criticality of the applications was determined by the business recently and describes the length of the allowed breakdowns.

There are four criticality classes, CR1 – CR4 with CR1 being the highest. Also, the applications which proved to be risky in the past were included into the study.

Mitigation plans for all the risks are out of scope of this thesis.

Table 1. Objective, outcome and expected benefit of the case study.

Objective	Operational risk assessment and proposition of risk assessment process for the future use.
Outcome	Identified and documented risks and a process proposition.
Expected benefit	Current risks present in the environment of the case department will become acknowledged, commonly understood and explored. The department will get guidelines for the process to do this exercise regularly in the future which will facilitate more informed decision-making and help to achieve strategic goals.

Objective, outcome and expected benefits of the case study are summarized above in Table 1.

2 Method and material

2.1 Research design

Figure 1 describes the flow of this case study.

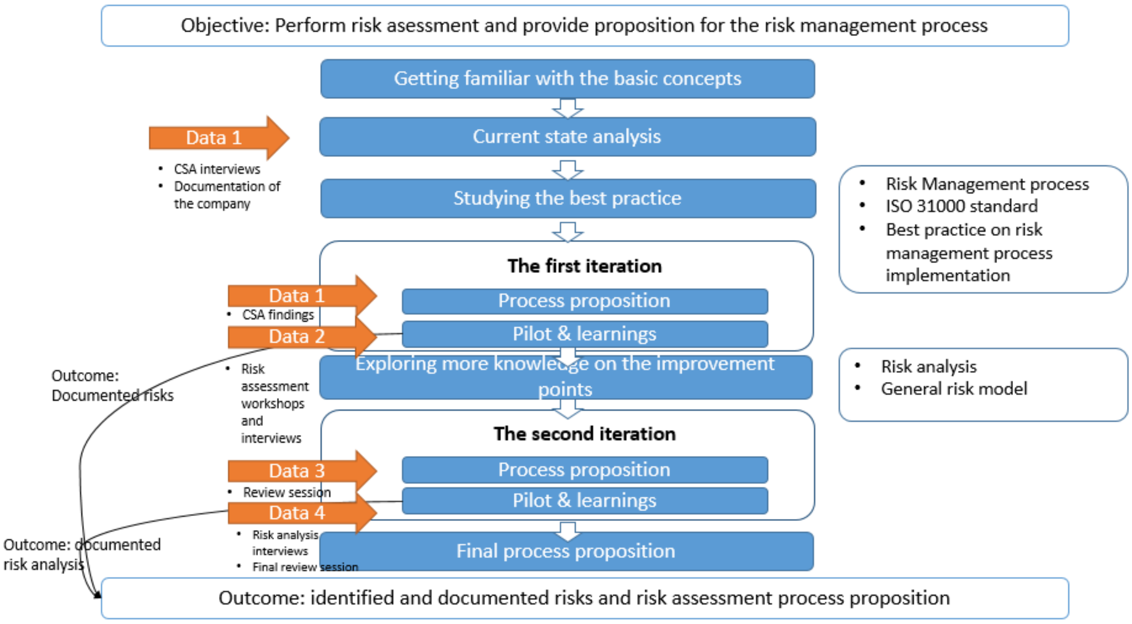

Objective: Perform risk asessment and provide proposition for the risk management process
Getting familiar with the basic concepts
Data 1
• CSA interviews
• Documentation of the company
Current state analysis
Studying the best practice
• Risk Management process
• ISO 31000 standard
• Best practice on risk management process implementation
The first iteration
Data 1
• CSA findings
Process proposition
Data 2
Pilot & learnings
Outcome: Documented risks
• Risk assessment workshops and interviews
Exploring more knowledge on the improvement points
• Risk analysis
• General risk model
The second iteration
Data 3
Process proposition
• Review session
Data 4
Pilot & learnings
Outcome: documented risk analysis
• Risk analysis interviews
• Final review session
Final process proposition
Outcome: identified and documented risks and risk assessment process proposition

Figure 1. Research design of the case study.

As seen in Figure 1, key steps leading from objective to the outcome of the study are listed in the center, used data on the left side and applied theory on the right side.

First step was defining the objective and the outcome of the study, after which the current state analysis was carried out. It was done by exploring internal documentation, the results of the previous risk survey and by interviewing the Head of the case department and the Middle Office Manager of the Customer Business Unit. In Figure 1, this input is marked as Data 1. The purpose was to look into risk managements customs practiced in the company and explore their strengths and weaknesses.

The next step was studying the best practice on the risk management. This knowledge was adjusted to the case company environment according to the findings of the current state analysis and utilized for building the process proposition for the first iteration. Finally, the process proposition was piloted by the risk assessment carried out. It consisted of various workshops and interviews with the stakeholders. In Figure 1, this is shown as Data 2.

Then, the results were reviewed with the Head of the case department. This is Data 3 in Figure 1. Learning points and needs for improvements were identified here and used for improving the process in the next iteration.

After the first iteration, more theory was explored and then applied for drawing an improved process proposition for second iteration. It was then piloted: the risk analysis interviews were carried out and findings were documented (Data 4). The outcomes of the risk assessment exercise were reviewed by the management in the final workshop (Data 4).

2.2 Data collection and analysis Method

In this chapter, it is described how data was collected and analyzed for this thesis study. Data sets from different phases of the thesis study are introduced in Table 2 below.

Table 2. Data gathered in the case study.

Data	Data Source	Purpose:
Data 1	Interview with the Head of the case department Interview with the Risk Manager of the customer (business) department Documentation on the previous risk survey Internal guidelines on the operational risk surveys Strategy documents of the concern Vision documents of the case departments	Current state analysis, Process proposition in the first iteration.
Data 2	Risk identification and scoring/assessment workshops and interviews: • 2 workshops with IT team • Workshop with the developers • Interview with the Service Delivery Manager • Interview with the Development Manager	Identifying and assessing risks Piloting proposed process
Data 3	Review session of the outcomes of the first iteration with the Head of the case department	Analysis of the pilot Identifying additional theory/development needs Process proposition in the second iteration

Data 4	Risk analysis interviews: • Workshop with business owner and end users • Interview with the Head of the customer business unit • Interview with the Service Delivery Manager of the case department • Interview with the Development Manager of the case department • Interview with the vendor representative Documentation on realized risks Final workshop for reviewing the results with the Head of the case department, Service Delivery Manager and Development manager.	Risk Analysis Piloting proposed process Final process proposition

Data 1 is the basis of the current state analysis and consists of interviews with the management of the case department and the customer business department and internal documentation. The Head of the case department was chosen to be interviewed because according to the concern policy, it is his responsibility to report operational risks and he was participating in the previous operation risk survey in the case department. Service Delivery Manager of the vendor and the Risk Manager of the customer department were interviewed to get a better picture on the business environment of the case department. In addition, internal documentation of the case department and the concern guidelines were used in current state analysis and for process proposition.

Data 2 contain performed risk identification workshops and interviews within the case department. It was gathered during the first pilot of the process and provided input for the outcome: documented risks identified.

Data 3 was the review session with the Head of the case department. The outcomes of the first pilot were explored and analyzed and direction of further process development was determined. It was used for the second process proposition.

Data 4 describes more detailed risk analysis conducted in the second iteration. It includes interviews with the end users of the most critical applications and business owners, for the impact assessment. In order to study deeper key risks and analyze their impact, also additional interviews with the Service Delivery Manager and vendor representative were held. For determination of likelihood, also historical data on realized risks was utilized. In addition, Data 4 contains a final review workshop with the Head of the department and Service Delivery and Development Managers to evaluate the results of the risk assessment exercise.

3 Current state analysis

3.1 Operational risk management in the case company

Due to the industry, there are certain requirements to the risk management process the company must meet. The requirements cover the process of recognizing the risks and occurred risk events, registering and reporting them to the authorities. Every deviation affecting the business continuity and all the realized risks are being registered by each business unit and reported to the management once a year. Once a year the report is also provided to the authorities.

There is a centralized risk management department in the organization, whose mission is to provide guidelines for the standard risk management process across the firm. The operational risk part is described in the document titled *Operating model of operational risk management*. The risk department also ensures that the risk management process meets the requirements set for it by authorities. Once a year, all the units should perform the operational risk assessment and fill the gathered information in an organization wide risk management tool. The risk assessment is carried out by each unit itself. There are no detailed directives for the risk assessment process in each unit.

As occurs from the strategy documents, there are specific strategic goals for reducing operational risks at the company level. Specific goals are set for the business functions, not for the supporting functions. However, reducing operational risks is seen important everywhere across the organization.

3.2 Operational risk management in the case department

According to the vision of the case department, its goal is to be the best ICT department in the industry. A meaningful part of this strategy is reducing the number of operational risks. The Head of the ICT department reported in the interview that there was currently, no systematic and adopted approach to the operational risk management process. The tool the concern has chosen to manage operational risks is not used for risk assessments by the case department. It mostly serves the need of reporting high level risks upstream in the organization.

Regularly occurring problems are recognized through every-day operations and quality meetings and being managed and mitigated, if possible, often on ad-hoc basis. This is also an input for the ICT-development process. All the actions are performed with the best effort –principle. All the new applications belonging into the scope of the case unit's application management are being overviewed and the security investigation is carried out. This is also a regulatory requirement. Other than that, risks are not studied.

Last operational risk survey was carried out last year. It was conducted on very high-level, describing the risk areas challenging for the unit. This was made by the management of the unit. Four risk areas were recognized during that survey: programs, tacit knowledge, mistakes in production and vendors.

According to the head of the unit, it is also important to follow-up realized risks. He saw them as a tip of the iceberg, which indicates that there is something bigger below the surface. This means that occurring problems can be visible 'symptoms' of the risks which has not yet happened.

The case department maintains all the applications its customer business unit is using. The customer unit is also the one deciding on the investment and development budget. In his interview, the manager of the customer business unit concluded that providing more stable environment for the application service production would mean fewer interruptions for the business. This statement was supported by historical data on realized risks.

The management recognized the need of improving the way of working within the operational risk management.

3.3 Key findings from the interviews

This section is based on the interviews, which are part of the Data 1 and described in section 2.2.

The case department does not have any risk management processes on its own, so without using the tools and directives of the company the risk management was left to be. There was no clear role responsible for the risk management activities except for reporting the risks to the risk management department of the organization, which was made by the Head of the case department.

The new risk management software was not adopted well. From the demonstration of the software by the head of the unit, it was concluded that the unit did not gain any value from using it, so the motivation for using it was low. There is a reason explaining this- the tool simply does not serve the needs of the case unit. It does not provide any valuable output for the unit itself and is mostly designed for reporting operational risks on a high level further on to the risk department of the whole concern. This is a necessary process according to the risk management policies of the concern. However, the head of the unit recognized the need for more detailed and comprehensive risk documentation, which this tool could not fulfill.

In the case unit, the risks are thought to be recognized, but are not registered and managed. The head of the unit points out a “problem-mindset” within the unit, meaning that problems are mistakenly thought as risks when non-realized risks are not recognized at all. The application management vendor also tends to bend towards problem thinking. The head of the unit explains the key difference between a risk and a problem: “A risk always should have likelihood less than 100%, otherwise it is a problem.”

As occurred from the interview with the customer business unit, quite meaningful percent of business interruptions or losses was due to the application issues. Therefore, reducing operational risks of the case unit means lower operational risks for the business unit as well. This rises the importance of being on top of the risks in the case department even more.

Risks need also to be communicated across the organization and to the customer unit in order to justify investment budgets. This cannot be done if there is not clear view and sufficient analysis on the existing risks.

The need for the risk survey was now identified as follows: to be able to see also the threats hiding below the surface in order to make informed decisions and to prepare the development road map more solid.

3.4 Strengths and weaknesses of current practices

In this section, the strengths and the weaknesses of the current situation explored previously are summarized.

Table 3. Strengths identified in the Current state analysis.

Strengths
Employees are very competent and have deep knowledge on the environment.
Some bigger risks are recognized and initial steps taken towards the mitigation.
Third party vendor is cooperating and provides monthly reports on realized risks.
Risk evaluation for new applications is always carried out.
Realized risks are documented and managed.

The current state analysis showed that there are certain good things about the current situation. They are shown in Table 3 above. The necessary activities on the risk management, required by the regulators, are performed: risk of the new applications are always explored and historical data on the realized risks exists. There was also good understanding of the need of improving the risk management process and employees' deep knowledge on the environment would allow to do that internally.

However, few weaknesses were recognized as well. They determined the best practices to be explored. They are listed in Table 4 below, followed by the theory addressing them. The theory is described in the next chapter.

Table 4. Weaknesses of the current situation and the theory applied to them.

Weaknesses	**Theory addressing them**
Only realized risks, in other words, problems, are managed	4.1 Definition of risk Source: ISO 31000; *Yrityksen riskienhallinta,* Juvonen et. Al
No risk assessment process in place	4.3 Risk management by ISO 31000 4.4 Risk assessment Source: *Johda riskejä,* Ilmonen et. Al; *Operational Risk Management,* Girling, P.X.
Previous risk assessment was really high-level, not really providing valuable input into decision-making and development	4.4.2 Risk analysis Source: *Johda riskejä,* Ilmonen et. Al; *Operational Risk Management,* Girling, P.X.

No proper tool for documenting risks	4.5 Risk model Source: *Guide for conducting risk assessments,* NIST
Risk assessments are not regular	4.6 The best practice on the implementation of risk management process Source: *Embracing Enterprise Risk Management,* Anderson, R.J., Frigo, M.L.

The biggest weakness was the lack of proper risk assessment process and all the other weaknesses link to it. Since the department's resources are limited, there was no possibility to establish a complex process with the process manager role and tools. It was also delimited by the environment: the department functions in the organization and the processes are 'predefined' to some limit.

In addition, problem-oriented thinking seemed to be in favor in the department. There was control over realized risks, but the Head of the department brought up a necessity of anticipatory thinking and pro-active approach, which required exploring all possible risks. Therefore, was concluded that existing knowledge should be explored on the scalable risk assessment processes and best practice of the implementation of them, thorough risk identification process and methods and operational risk management.

4 Theory

4.1 Definition of risk

There are numerous definitions of risk, as over years, the man has always attempted to manage the risks in some way and risks were approached from different fields. National Institute of Standard and Technology and U.S. Department of Commerce, in its *Guide for Conducting Risk Assessments,* defines risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event". (NIST 2012:6)

ISO 31000 defines risk as an impact of uncertainty on the goals, which can be negative as well as positive. (Lark, J., Nikonov, V. 2015:15) Throughout this study, however, term 'risk' means an uncertainty with negative consequences at least.

Risk event is always associated with three aspects:

- The uncertainty of the event
- The expectations towards the event
- The impact of the event. (Juvonen et al. 2014)

The uncertainty is the main attribute defining the risk. Any event with negative consequences on something falls under definition of risk if its likelihood is less than 100%. In other words, event of any kind certain to happen cannot be considered as risk. (Juvonen et al. 2014). Also in the standard SFS-ISO 31000 defines the risk through uncertainty; according to it, the risk is the effect of uncertainty causes on the goals. The uncertainty is described by its likelihood (lower than 100%).

Another component of a risk is our assumption about what and might happen – our expectations towards the event. Our assumptions also affect the third attribute – the expected impact of the risk in addition to the severity of the risk event itself. Impact can be measured in qualitative or quantitative way (see section 4.3.2.). (Juvonen et al. 2014)

4.2 Definition of operational risk and a regulatory point of view

Financial regulations regarding risk management have developed rapidly over the last years. Some regulations have always been there, but lately, they became more and more detailed and strict, a change driven by globalization and digitalization of the banking industry and central finance crises. In year 1998, there was no common definition for operational risk and no directives what it comes to the operational risk management. (Basel2:3) Papers on the subject published by Basle Committee on Banking Supervision had more of a reporting/exploring point of view. Nowadays, recommendations on the subject are binding and risk management standards in the finance industry are developed significantly.

The focus of this study, the risk identification and assessment is the 6th principle of principles for *The sound management or operational risk* published by the Basel Committee on Banking Supervision in 2011. The book covers fundamental principles of operational risk management, governance and the risk management environment. (Basel :6)

Basel's definition of operational risk can be found in *Operational Risk Management Framework* by Girling, P.X.:

> "… the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk." (Girling 2013:2)

The book introduces 5 tasks that continuously occur in national financial regulations and are the core of the operational risk management:

> "1. Identifying operational risks.
>
> 2. Assessing the size of operational risks.
>
> 3. Monitoring and controlling operational risks.
>
> 4. Mitigating operational risks.
>
> 5. Calculating capital to protect you from operational risk losses." (Girling 2013:4)

First two tasks were the focus of this study.

4.3 Risk management process

4.3.1 Purpose of risk management

The business in any form assumes taking risks. Every organization, regardless of the industry, encounters internal and external risks. (Erola 2000:30) Essentially, the purpose of risk management process is to ensure business continuity by managing them. Risk management has also an important role in meeting set regulations from the outside (e.g. financial authorities). Risk management is not a stand-alone process, but it is closely linked to the strategy and the values of the company. (Ilmonen et al. 2010)

The nature of the company and the industry it is in should form the characteristic of risk management process. The whole risk management process should be integrated into management process across the company. (Ilmonen et al. 2010:49 - 52)

4.3.2 Risk management by ISO

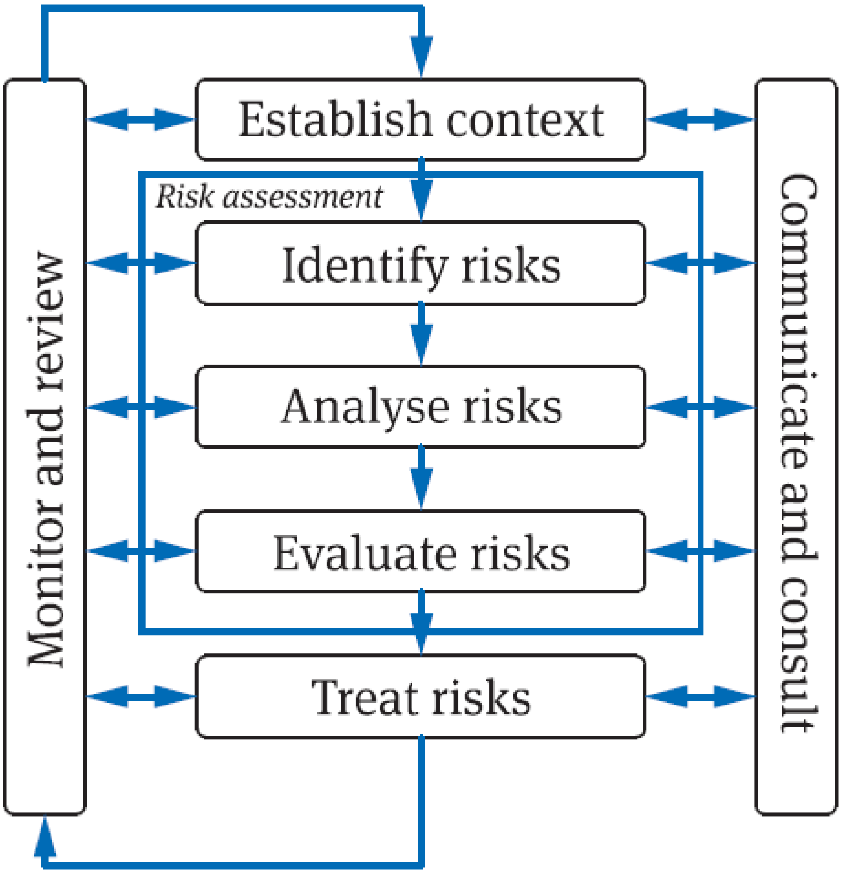
ISO or International Organization of Standardization is an independent non-governmental organization coordinated by a Central Secretariat in Geneva, Switzerland. ISO has published over 20 thousand internationally accepted standards covering almost every industry.

It defines standard as follows:

> "An international standard is a document containing practical information and best practice. It often describes an agreed way of doing something or a solution to a global problem". (ISO in brief)

ISO's standard on risk management is ISO 31000. It is demonstrated in Figure 2 below.

Figure 2. ISO 31000:2009 risk management process (Lark, J., Nikonov, V. 2015:14)



Juvonen et al. describe ISO 31000 standard risk management process. It is very clear and straightforward. In a nutshell, it consists of three phases. Firstly, the context of the process is established. This includes aspects such the culture, processes, hierarchy and strategy of the organization and resources available to the risk management process. The purpose of this phase is to define the desired state of the risk management process. If done well, it ensures leading the risks through all the dimensions of the organization in the same consistent way. (Juvonen et al. 2014)

The next stage is risk assessment which includes risk identification, analyzing risks found and risk evaluation. It is important that all these steps are made consulting the stakeholders. In the evaluation phase, risk perceptions pointed out in the identification phase are evaluated against the context. This is the most important part of whole process. It is a meaningful tool for understanding upcoming threats and increasing awareness and visibility. (Juvonen et al. 2014) The outcome of this phase should be a documented risk analysis including list of categorized risks, their descriptions, impact and likelihood assessments, cause analysis and mitigation plan proposals. This phase is the focus of the case study, excluding mitigation plan proposals from the scope.

The last step is the actual technical managing of the risks: for example, carrying out mitigation plans. This is made prioritizing possible life threatening risks over others, then key risks in the order of their business impact. (Juvonen et al. 2014)

4.4 Risk assessment

This is the most time- and resources-consuming phase of the risk management process. The risk assessment consists of risk identification, risk analysis and risk evaluation. In this part of the process risks are being measured and documented and become more concrete and understood.

The purpose of risk assessment is to identify and analyze risks that are present for the organization. Risk assessment can provide valuable input into wide variety of risk-based decisions and activities, such as development of IT architecture, development of information security strategy, implementation and operation of applications. (NIST 2012:6)

Found risks are being categorized and evaluated. In order to do that, the likelihood and the impact of the risks are measured. In addition, the root causes and possible triggers are explored. The risk assessment report should be documented in a way defined in the very first stage of the risk management process – context establishment. All the evaluations should be made against the criteria and goals defined in the beginning.

Regarding operational risks, the report can consist of the following information:

- Description of the risk
- Category of the risk (for example, people or process related)
- Impact of the risk (direct and indirect loss or immaterial impact)
- Root cause of the risk (the cause and possible triggers)
- Control actions in place (reducing likelihood or impact of the risk)

- Probability of the risk
- Value of the risk (calculated from the probability and the impact). (Ilmonen et al. 2010)

If already planned, mitigation plans can be added to the report, together with the reassessment of the value of the risk after implementing mitigation actions.

Risk assessment should be made on regular basis, most commonly, annually to keep the risk management process up to date. Documenting the principles of this phase and adopting them by the employees is necessary to carry out regular consistent risk assessments. (Ilmonen et al. 2010)

4.4.1 Risk identification

Ilmonen et al. 2010 describes risk identification according to ISO 31000 in their book *Johda riskejä*. The identification of risks consists of identifying factors and events possibly affecting the appearance of the risks and the cause and the impact of the risks. Coverage and success of the risk identification plays crucial role in the risk management process. Even comprehensively defined context or meticulously performed risk evaluations will not compensate inadequate risk identification.

Ilmonen et al. 2010 quotes the definition of risk identification phase from ISO 31000:

> “The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.”

To perform the risk identification well, it needs to be well prepared. Philippa X. Girling (2013) lists few sources that might help in preparation and can support the outcomes of the risk survey for more complete picture. Firstly, review available background data from other functions. These can be, for example, recent audit reports or possible SWOT analysis carried out. They might provide insight into existing or arising risks.

Extremely essential is to review previous risk assessments if there are any, possibly also from other related departments or branches. There might be risks related to the departments’ risks on its own or to the services or functions the department is carrying out. Risk indicators can also be found in loss data or realized risks reports. The information gathered from all these sources will help to choose the right risk identification method and to gather data from interviews or workshops comprehensively. (Girling 2013)

Numerous methods were developed to ensure thorough and comprehensive risk identification. One of the most common methods of risk identification is a checklist method. Many risk management and audit authorities use publically available checklists on their own. If the company is facing a need to meet some obligatory standard set by industry or decided by the management, using the check-list (if provided) used by the authority of the standard would be beneficial. (Ilmonen et al. 2010)

Similar to the checklist, there is a questionnaire approach Philippa X. Girling describes in her book, *Operational Risk Management*. It is a template with standard risk questions distributed to the participants. A risk management team designs the question list after analyzing risk categories and/or business processes. This method can also be used for risk scoring (see section 4.7.). The strong side of this method is a standard approach and same terminology providing a consolidated view on the risks across the firm. On another hand, it also requires departments or processes to be standardized in order to be applicable. In addition, if the original question list misses something, it can be left outside of the identification process, as participants might not be willing or able to add new items. (Girling 2013)

Workshops can also be used for risk identification. Especially cross-functional workshops are beneficial bringing to the table insights from different perspectives. This method allows contemplating risks in a broader, more interactive way increasing communication in the organization. (Ilmonen et al. 2010) The down side of the workshop method is that it is time consuming and burdensome. Consolidating the results of different workshops might be challenging due to e.g. different terminology used by different participators. (Girling 2013)

Workshops should be properly designed beforehand and the same template should be used to all the risk identification workshops (if many) them to be consistent. Some kind of checklist, question list or a template can be used to build them up. Facilitator’s responsibility is to check that all the findings are properly documented. (Ilmonen et al. 2010)

Another identification method based on existing statistics of realized risks. Such material is a good way to start and it can be useful aid in interviews or workshops. It is not recommended to use this method alone, as it does not support mapping possible unrealized threats. (Ilmonen et al. 2010)

Identification methods should evolve according to the maturity of risk management and possible changes in the organization and its goals. A firm might use a workshop method in the beginning of risk management process, and a questionnaire designed based on the outputs of these workshops later on. (Girling 2013)

4.4.2 Risk analysis

In the risk analysis phase, the impact and the likelihood of the identified risks are being quantified. This can be done in different ways, depending on the nature of the risk. It can be done in a qualitative or quantitative ways, or combination of both. According to Ilmonen et al. (2010), qualitative impact review consists of the description of the impact but also of an impact estimation using agreed scale (for example, scale from 1 to 5, 1 standing for the smallest impact). The scale does not have to be numerical, the estimations can also be described in words: 1 = does not affect business, 2 = affects business in minor way; 3 = clearly affects business; 4 = significantly affects business, but does not stop it; 5 = stops the business). The estimations do not have to be exact. The goal of this exercise is to arrange the risks into a risk matrix where they can be shown accordingly to their impact and likelihood. This is the simplest categorization tool for risk analysis and evaluation.

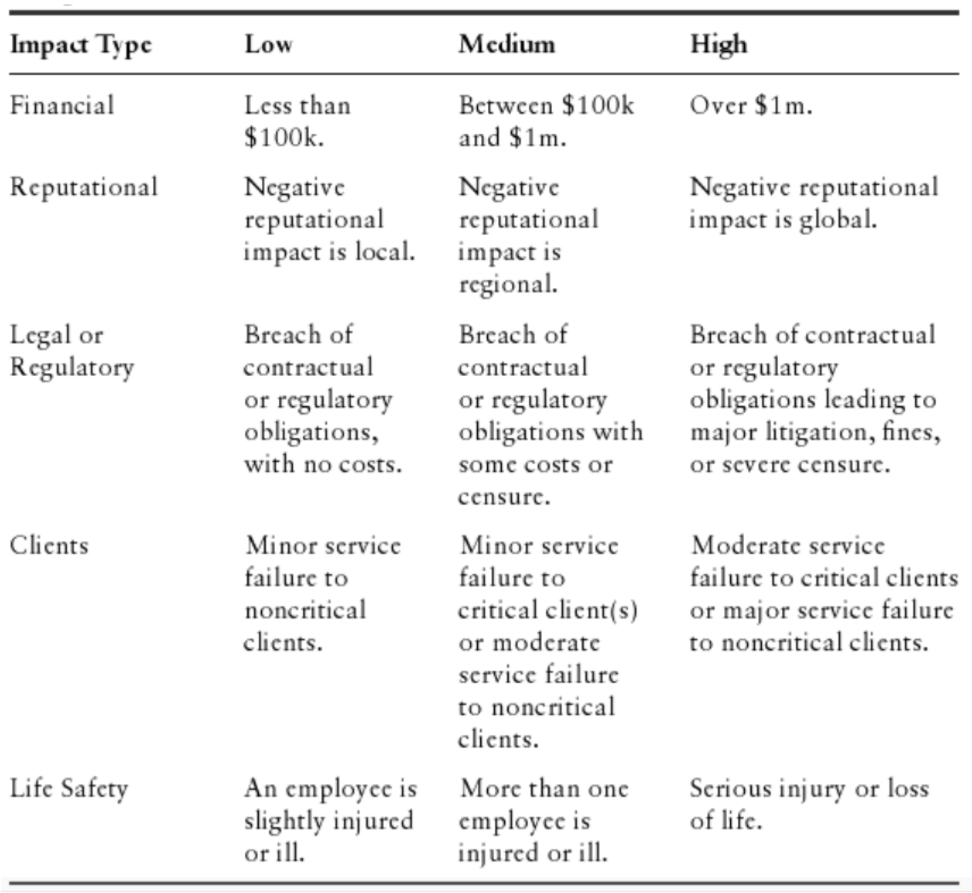
Ilmonen et al. point out that the estimation of the risk impact can be affected by many factors. The qualitative method is not exact and the human factor must be taken into account.

Quantitative method is based on calculating values of impact or likelihood. One way of risk impact scoring is calculating the cost the organization will have to carry in case the risk will realize. It is called quantification. However, when it comes to operational and strategic risks, quantification is not the best practice due to the nature to the risks. Operational and strategic risks and their consequences are very hard to estimate beforehand and the variety is very broad. (Ilmonen et al. 2010)

The impact of a risk can be scored either after all the control actions are in place, on a residual scale; or before the controls, calculating the inherent impact. The latter one can be helpful in understanding the relative value of the controls. (Girling 2013)

The impact can also be scored combining qualitative and quantitative methods. An example of such approach is demonstrated in Table 5 below.

Table 5. A risk impact scoring scale that includes nonfinancial impact categories. (Girling 2013)



Impact Type	Low	Medium	High
Financial	Less than $100k.	Between $100k and $1m.	Over $1m.
Reputational	Negative reputational impact is local.	Negative reputational impact is regional.	Negative reputational impact is global.
Legal or Regulatory	Breach of contractual or regulatory obligations, with no costs.	Breach of contractual or regulatory obligations with some costs or censure.	Breach of contractual or regulatory obligations leading to major litigation, fines, or severe censure.
Clients	Minor service failure to noncritical clients.	Minor service failure to critical client(s) or moderate service failure to noncritical clients.	Moderate service failure to critical clients or major service failure to noncritical clients.
Life Safety	An employee is slightly injured or ill.	More than one employee is injured or ill.	Serious injury or loss of life.

This is a scale to score a risk impact from different perspectives.

Likelihood can also be scored on a scale (from 1 to 5 or from unlikely to extremely likely) or it can be calculated using mathematical probability models on historical data. In this case, it is important to be careful about the risk factors – if they continue affecting in the same way as they had have. Adjusting them, if possible, give likelihood estimation more credibility. (Ilmonen et al. 2010)

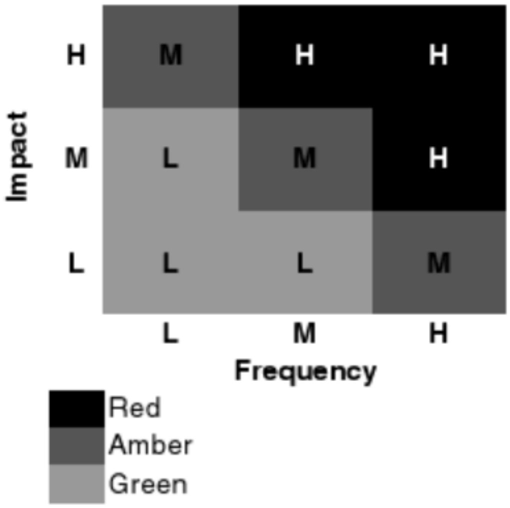
Ilmonen et al. outline that perfect objective scoring of risks should not be the goal. Even then using mathematical models, the outcome would still be subjective, as assumptions made in the process of creating and applying the models can affect the results significantly.

The bottom line of risk analysis can be expressed as this formula:

Impact * Likelihood = Severity

Risk severity score is calculated from the impact and likelihood of the risk. This can be calculated either using numbers, in a quantitative way, or using a RAG matrix for qualitative scale. This is demonstrated in Figure 3 below:

Figure 3. Risk severity scoring matrix. (Girling 2013)



Impact \ Frequency	L	M	H
H	M	H	H
M	L	M	H
L	L	L	M

Philippa X. Girling describes this method in her book: a score of low (L) for impact and high (H) for frequency would give an overall risk severity of medium (M). Scoring scales should be meaningful for the firm. (Girling 2013)

Ilmonen et al. anticipate that this same method (multiplying impact by likelihood) does not necessarily serve best when numerical scale is used for scoring. The assumption the method makes is, that the impact and likelihood have equal priority. It can be described through an example: a risk with likelihood of 5 and impact of 1 will have the same severity as the risk with likelihood of 1 and impact of 5. The latter one will be crucial to the firm when the first one might even leave unnoticed in the big picture. Still, the method prioritizes them as equal, which is misleading. Ilmonen et al.'s advice is to anticipate the impact more. (Ilmonen et al. 2010)

Regardless of whichever method is chosen, Ilmonen et al. outline that the scoring method should be either picked up in collaboration with the management or approved by the management before the actual evaluation. That way, when reviewing the results, all the parties can be sure they ‘speak the same language’. (Ilmonen et al. 2010)

4.4.3 Risk evaluation

In this part of the risk assessment process, the risk analysis is being evaluated against the goals set in the beginning. The purpose of the evaluation is to ensure that gathered information is consistent and sufficient for the purpose. This can be done also by an independent party which has no operational responsibility over inspected business. (Ilmonen et al. 2010)

4.5 Risk model

Risk model is describe in the *Guide for Conducting Risk Assessments* by National Institute of Standard and Technology and U.S. Department of Commerce. It is a part of the second component in four components of risk management:

1) establishing risk context
2) assessing risks
3) responding to risks
4) monitoring risks. (NIST 2012:5)

This approach is very aligned with ISO 31000 standard. Establishing a risk context, which means describing the environment in which risk-based decisions are made. The purpose is to make explicit and transparent risk perceptions for the company's use. (NIST 2012:5).

Risk assessment component identifies threat to organizations, vulnerabilities internal and external to organizations, the harm (i.e. adverse impact) that will occur when the threat exposures vulnerability and the likelihood the harm will occur. The end result is determination of a risk and its expected value.

The third component addressing how the organization addresses determined risks aims at providing consistent and organizational-wide response to risk in accordance with organizational risk frame. The fourth component determines effectiveness of risk responses, identifies risk-impacting changes and verifies that planned risk responses are implemented. (NIST 2012:5)

The focus of this thesis is risk assessment, so let’s have a closer look on the second component. According to *Guide for Conducting Risk Assessments,* a risk assessment methodology typically consists of risk assessment process; risk model; assessment approach and analysis approach. (NIST 2012:7)

In her book on operational risk management, Girling, P.X. stresses that to achieve successful operational risk management, it has to be managed in quantitative as well as qualitative approach. Both are important in order to measure and manage risks. (Girling 2013:9)

Complexity or a number of risk assessment methodology will depend on various factors, such as the complexity and/or maturity of the organization and/or its business processes, the time frame for planning policy and so on.(NIST 2012:7)

Defining the risk factors to be assessed and the relationships between these factors is essential purpose of a risk model. Threat, vulnerability, impact, likelihood and predisposing condition are typical risk factors. More in-depth look into risk factors can be taken by decomposing them into more detailed characteristics, for example, threat could be decomposed into threat sources and threat events. Definitions of risk factors should be documented prior to conducting risk assessment so that risk assessment could rely upon them. Risk factors are used in the risk model as inputs for determination of risk levels in risk assessment. (NIST 2012:8)

Generic risk model with key risk factors discussed above is represented in Figure 4.

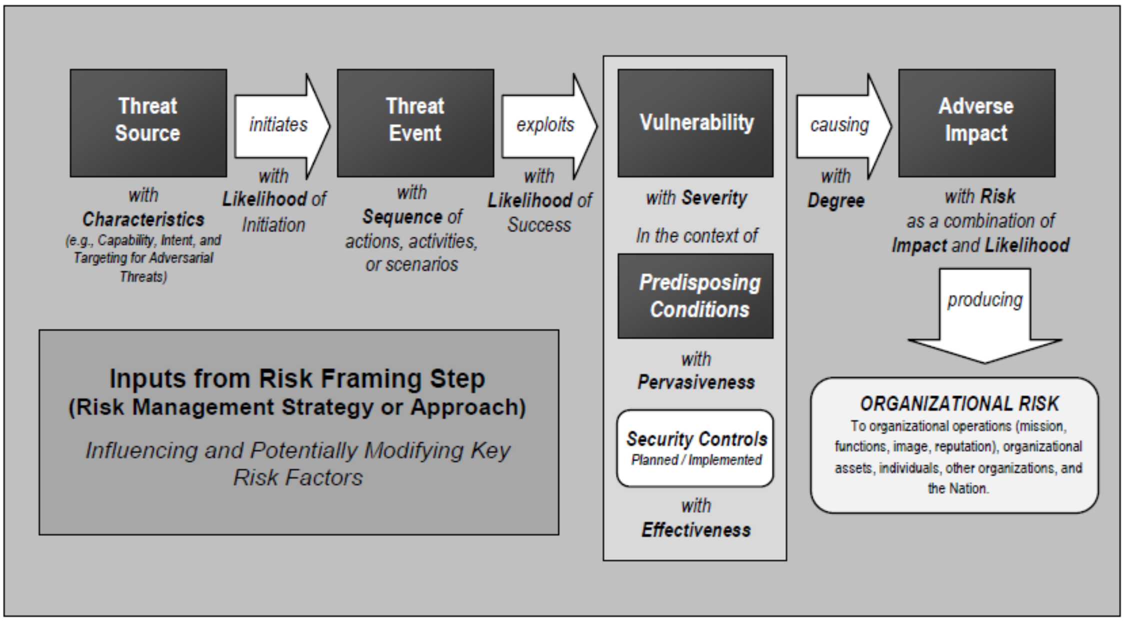

Threat Source
initiates
with Likelihood of Initiation
Threat Event
exploits
with Likelihood of Success
Vulnerability
causing
with Degree
Adverse Impact
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Sequence of actions, activities, or scenarios
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step
(Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

Figure 4. Generic risk model (NIST 2012:12)

In Figure 4, origin and impact of the risk are depicted. A threat source is an intended or accidental situation exploiting a vulnerability by causing a threat event. Multiple threat sources can trigger the same threat event, for example, a server can be taken offline by human mistake, electricity outage or dos attack. A vulnerability is a weakness, facilitating a risk, making it possible. In other words, threat event (or a series of them) takes advantage of one or more vulnerability and creates a risk with a certain likelihood of occurrence and adverse impact. (NIST 2012:8 – 11)

For assessing likelihood and impact of the risks, organizations can use different assessment scales depending on circumstances and purposes. For example, qualitative assessment scale can be used for low-impact applications or risks and more specific, semi-qualitative scale can be used for the key risks. (NIST 2012:28).

4.6 Best practice on the implementation of risk management process

Anderson and Frigo in their publication *Embracing Enterprise Risk Management: Practical Approaches for Getting Started* list few keys to success of implementing enterprise risk management regardless the method or approach chosen:

- Support from the top is a necessity.
- Build ERM using incremental steps¨.
- Focus initially on a small number of top risks
- Leverage existing resources.
- Build on existing risk management activities.
- Embed ERM into the business fabric of the organization.
- Provide ongoing ERM update and continuing education for directors and senior management. (Anderson 2011:1 - 3)

Firstly, it needs to be supported by the top management to demonstrate its importance across the organization and get the ERM resources it needs. (Anderson 2011:1) Ilmonen et al also notice that it is important that risk management is extensively utilized in decision making process of the organization. (Ilmonen et al 2010:61)

Secondly, authors recommend building the risk management process using incremental steps. Especially for small organizations, step-by-step approach has proven beneficial. It allows implementing key practices and achieving immediate, tangible results. Maybe even more important is the possibility to change and tailor the risk management process and for management to request to broaden or deepen the risk management activities, if needed. Step-by-step approach also makes visible the value of each step, making adopting risk management easier. (Anderson 2011:1) Ilmonen et al also support this point of view. According to them, adoption of risk management process always takes time and proceeding slowly in small steps is a healthy approach. (Ilmonen et al 2010:61)

Ilmonen et al advice not to adjust any risk management standards or models as it is, but always adjust to the environment and maturity level of the organization. He emphasizes that if they are any hesitations regarding complexity of chosen risk management practice, just boldly simplify it and build it up only later, when the process is genuinely adopted in the organization. (Ilmonen et al 2010:102)

Third advice given by Anderson et al. is to initially focus on a small number of top risks. It can be either the risks critical to be strategic objectives or few top risks of one business critical unit. The point is to focus on manageable number of risks first, and then apply the lessons learned to assessing additional risks in the organization. (Anderson 2011:2)

To get the risk management on the rails easily, it is smart to exploit existing resources and risk management activities. It lowers the threshold of starting with risk assessments. Most organizations start their ERM effort without any specific technology or tools. New activities should be aligned with already existing guidelines or processes. A company should have common set of risk definitions or risk framework across the organization. (Anderson 2011:2)

ERM process should be linked to core processes and structures of the organization. While the process is evolving, it is important to inform and educate the senior management so they would stay on top of things. This is particularly important in some specific industries, where the focus on ERM is increased by regulators. (Anderson 2011:3)

4.7 Applying theory in forming the solution

The following theory was applied for building the risk assessment process proposition (Table 5):

Table 5. Weaknesses of the current situation and the theory applied to them.

Weaknesses	**Theory addressing them**
Only realized risks, in other words, problems, are managed	4.1 Definition of risk Source: ISO 31000; *Yrityksen riskienhallinta,* Juvonen et. Al
No risk assessment process in place	4.3 Risk management by ISO 31000 4.4 Risk assessment Source: *Johda riskejä,* Ilmonen et. Al; *Operational Risk Management,* Girling, P.X.

Previous risk assessment was really high-level, not really providing valuable input into decision-making and development	4.4.2 Risk analysis Source: *Johda riskejä,* Ilmonen et. Al; *Operational Risk Management,* Girling, P.X.
No proper tool for documenting risks	4.5 Risk model Source: *Guide for conducting risk assessments,* NIST
Risk assessments are not regular	4.6 The best practice on the implementation of risk management process Source: *Embracing Enterprise Risk Management,* Anderson, R.J., Frigo, M.L.

Firstly, I made myself familiar with the basic concepts of risk management and defined risk in the context of this study.

The risk assessment process was built one the basis of ISO 31000 standard, described in official ISO documentation and by Juvonen et. al. ISO 31000 was chosen for its international recognition and easily scalable structure. It was complimented with the best practice of risk assessment from Ilmonen et. al's book *Johda riskejä* and *Operational Risk Management* from Philippa X. Girling.

For the second iteration, the initial process proposition was improved by implementing more in-depth risk analysis. It was conducted based on the general risk model, introduced and explained in *Guide for conducting risk assessments* by NIST.

The process was built taking into account the need of easy adoption and limited resources of the case department introduced in COSO's *Embracing Enterprise Risk Management* publication.

All of these best practices mentioned above were implemented adjusting to the environment and the needs of the case department. They were also piloted during risk assessment exercise in the case department and completed with learning points from two iterations.

5 Building risk assessment process proposition

This section describes how the risk assessment process was designed. It was made combining the knowledge gained from theory (described in section 4.) and CSA analysis (described in section 3.).

5.1 Adjustment for the case department according to the best practice

The whole risk assessment process was decided to keep simple for a number of reasons. Firstly, the study was conducted to the department of the company, which already has risk management department so the process must to stay within given guidelines. Secondly, the case department needed risk assessment method light and easy to adopt, as they could not invest any money or much time into adopting complex process or tool. Thirdly, knowledge on obstacles of risk management gained from theory was considered. It is good practice to start with the light risk assessment process to avoid risk of reduced motivation of the employees and tailor it according to the needs of the organization in the future. (Anderson et al. 2011:1) More sophisticated process can then be developed ‘on top’ of the proposed one, if needed. Too complicated process might sometimes be inconvenient to run, as the case department is limited on resources. According to the vision and goals of the case department, regular risk assessment is important (Data 1), so the process is good to keep simple.

Recommendations on starting with ERM process given by COSO in section 4.6 were found useful and were applied in the design of the process proposition. Both Andersen et al. and Ilmonen et al. advise risk management process to be implemented in incremental steps and developed gradually (see section 4.6). On top of that, giving desired light approach and an eagerness for fast results, building the proposition of risk assessment process was decided to be made iteratively. In the case of this study, it required two iterations to draw a final proposition. They are narrated below.

5.2 First iteration

5.2.1 First proposition of risk assessment pilot process

For the basis of the risk assessment process for the case department ISO 31000 standard was chosen. It is the best practice of the risk management and internationally used and valued standard. The structure of ISO 31000 risk management process supported the need of light scalable approach the case department was pursuing. According to ISO 31 000, there are three phases in risk assessment: risk identification, risk analysis and risk evaluation. All three were seen useful and valuable and could be implemented lightly now and scaled later on, if needed. Therefore, all three were included into risk assessment proposition.

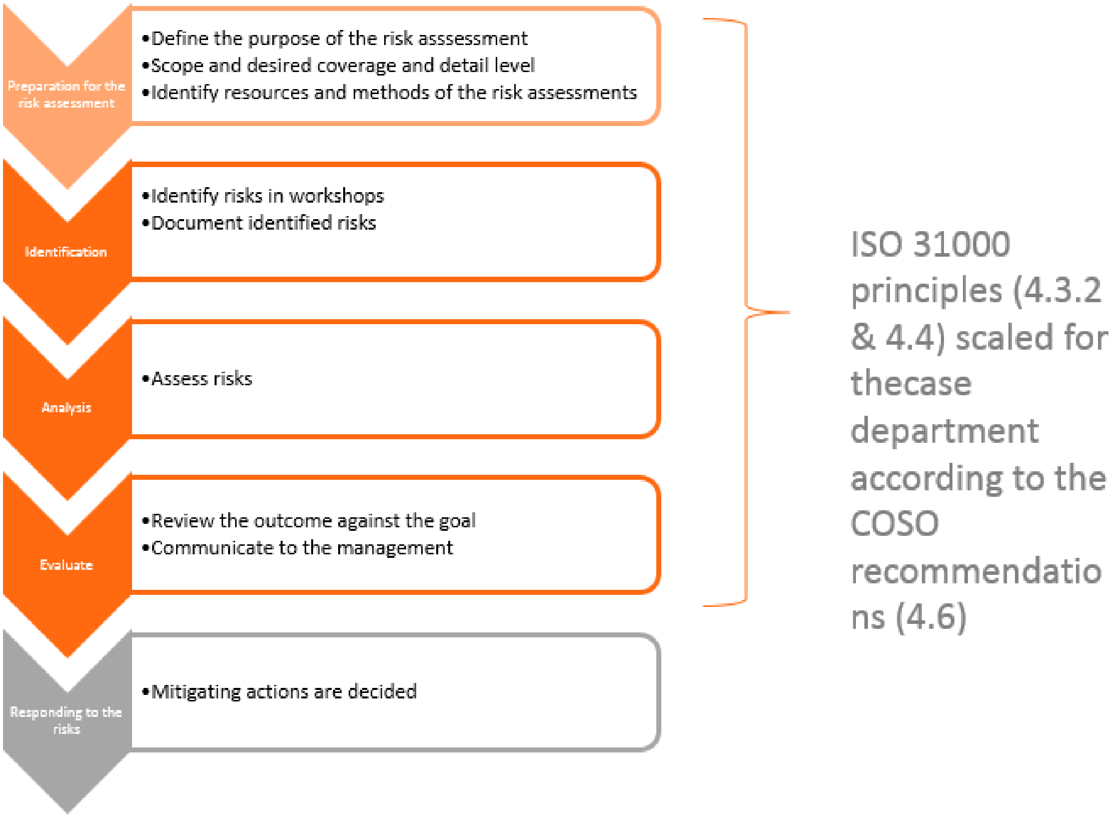

Preparation for the risk assessment
•Define the purpose of the risk asssessment
•Scope and desired coverage and detail level
•Identify resources and methods of the risk assessments
Identification
•Identify risks in workshops
•Document identified risks
Analysis
•Assess risks
Evaluate
•Review the outcome against the goal
•Communicate to the management
Responding to the risks
•Mitigating actions are decided
ISO 31000 principles (4.3.2 & 4.4) scaled for thecase department according to the COSO recommendatio ns (4.6)

Figure 5. The first risk assessment process proposition.

In Figure 5, suggested risk assessment process is being introduced. It is preceded by preparation phase and followed by responding to the risks.

As advised by Ilmonen et al.(2010:61), the standard was not implemented as it is, but it was adjusted to the needs of the case department. Some components from the steps were left out at this stage of pilot process proposition in order to implement only the essential steps in the beginning. Likewise, all the steps were kept simple and straightforward. The assessment of the risks was decided to be made before control actions in place, to keep the process simple. Mitigation plans are out of scope of this study, as stated in section 1.4, but a part of risk management process.

Context/preparation phase is a context establishment step, recommended by ISO 31000. For the case department, the scope of this step is much narrower, than suggested by ISO 31000 simply because it is a department functioning in the context of its own organization: a lot is determined ‘externally’ from the department point of view.

Firstly, the context was established in a light manner, defining the guidelines and the goals of the future process. It is naturally delimited by regulation requirements and strategy and risk management guidelines of the organization. Also method for the risk identification and analysis should be determined. This step requires input from the management, to ensure its support and approval for the risk assessment. Nominating responsible person for the risk assessment is required. This addresses the need of gathering and documenting information on the risks, which was not done before. He or she will facilitate the assessment and ensure that it will meet the requirements.

The next step is identifying the risks there are. This is facilitated by the risk assessment responsible and made by with other employees of the department. As learnt from the theory (Ilmonen et al 2014:122), this is most critical step in the risk assessment and should be kept as comprehensive as possible. To ensure that, all the functions within the case department should be included into the identification. Also, discussion enabling techniques should be considered to address the need of identifying unrealized risks (Data 1).

The following step is the risk analysis. Impact and likelihood of the risks should be assessed and scored. Finally, the risk assessment is reviewed and evaluated against the set criteria by the management of the department.

5.2.2 First risk assessment pilot

In the beginning, context was established. The environment of the risk assessment process was determined to be the case department and to include all the operational risks within it. The goal was set to be identifying and assessing all possible operational risks of the case department. The desired state of the risk management process within the case department was defined as follows: regularly performed risk assessment providing valuable insight into the department's operational environment. (Data 1) The responsible person was nominated to be me.

To facilitate the biggest coverage what it comes to risk identification, for the risk identification method it was decided to combine workshops and interviews. Keeping in mind, that no thorough risk assessment were made in the near past, the questionnaire is not the best technique of choice for this purpose. Workshops allowed to have in-depth conversations about the risks and to bring in some creativity in order to identify 'the icebergs' – the unrealized risks the head of the unit was most interested in. In addition, as Ilmonen et al advise, tacit knowledge was important to consider and workshops allowed that as well. Interviews were conducted with the managers due to time saving reasons.

Workshops were designed with an input from the head of the department (Data 1). Participants were chosen in a manner that all the functions would be represented: IT support-team, Development Manager, Service Delivery Manager and Developers. Qualitative method of assessment was chosen to start with, which was seen to be supportive of a light approach and brainstorm-designed workshops.

Three workshops and three interviews were held (Data 2). They are listed in Table 6 below:

Table 6. Risk identification workshops and interviews.

Workshop 1	IT team
Workshop 2	IT team
Workshop 3	Developers
Interview 1	Service Delivery Manager
Interview 2	Development Manager

Interview 3	Vendor representative

It was also decided to document risk triggers: aspects launching the risk event or underlying problems. This would address the need of identifying hiding 'iceberg' the Head of the case department mentioned in this first interview. (Data 1) Scales were also determined in time and money, to keep scoring more objective. The following scales were suggested by the Head of the department:

Likelihood		
Low Less than two times a year	**Medium** 2-5 times a year	**High** Once a month
Impact		
Low Less than 20 000€	**Medium** 20 000€ - 100 000€	**High** Over 100 000€

Table 7. The qualitative scale used in the risk assessment.

All findings were documented in the following manner, introduced in the Table 7:

Table 8. Risk identification table.

Risk description	Risk trigger	Impact	Likelihood
Risk 1	Event 1	Low	High
Risk 2	Event 2	Medium	Medium

All together, 34 risks were identified. The full risk table is accessible in the Appendix 1.

Next, risks were assessed. Redundant risks were aggregated and risks were categorized by categories used in the previous assessment. Risks were color marked by severity using RAG matrix approach. The outcome of this step is documented in Appendix 2 available for the case company use only.

The risks were reviewed against set goal – comprehensive risk identification and valuable input into operational decision making of the case department by the Head of the unit (Data 3). The risks were identified from different perspectives and it could be concluded that the workshop method was well suitable for the purposes of the case department. Risk analysis on the other hand, while providing a solid understanding of risk division by category, did not serve any desired goals. It was insufficient and not deep enough for the decision making. Therefore, it was decided to proceed with the second iteration and develop risk analysis process further.

5.2.3 Learnings

Workshops turned out to be the right identification method for the case department. Risk were identified thoroughly from different categories and on different levels. During preparing and running workshops, it became clear, that the risk assessment is convenient to do in connection with the identification: during the same workshop. Impact and likelihood could be addressed right away because usually the people present were familiar with possible consequences of the risk they just identified.

After the workshops, it occurred that it is meaningful to categorize the risks. This was not thought in the beginning, but for the future is recommended to assign each risk to its category already in the identification phase. Risk category field can be included into the risk identification template which will save from unnecessary work afterwards.

The outcomes of the first iteration of risk assessment was reviewed together with the Head of the unit. Broad coverage being an obvious strength, the depth of the analysis was not seen sufficient. For the purposes of the case department, such as development road map (section 1.2), the RAG matrix did not provide enough information on actual cost of the risks and their impact on the business. Even though, this approach was enough to identify the most challenging category, for example, for the development and investment decisions, as well as for the possible communication of the risks to other parties, it was not enough output.

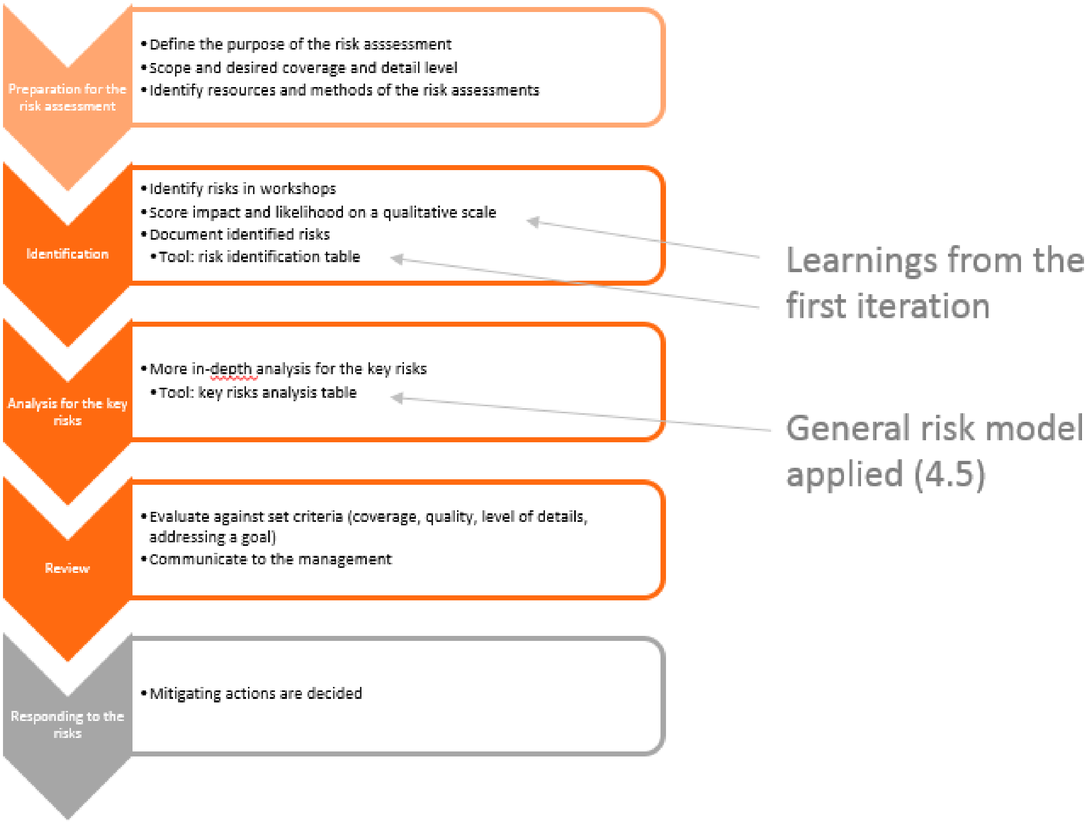
In addition, the origin of the risks being already addressed, it needed to be more consistent and structured, distinguishing the risk triggers from the underlying problems or weaknesses. This would provide valuable input for the mitigation planning.

5.3 Second iteration

5.3.1 Second risk assessment process proposition

The risk assessment process was now improved based on the learning from the first iteration and risk analysis theory introduced in section 4.5. Improved process is proposed below in Figure 6:

Figure 6. The second risk assessment process proposition


Preparation for the risk assessment
• Define the purpose of the risk asssessment
• Scope and desired coverage and detail level
• Identify resources and methods of the risk assessments
Identification
• Identify risks in workshops
• Score impact and likelihood on a qualitative scale
• Document identified risks
• Tool: risk identification table
Analysis for the key risks
• More in-depth analysis for the key risks
• Tool: key risks analysis table
Review
• Evaluate against set criteria (coverage, quality, level of details, addressing a goal)
• Communicate to the management
Responding to the risks
• Mitigating actions are decided
Learnings from the first iteration
General risk model applied (4.5)

Firstly, the risk identification step was modified. It now includes preliminary assessment of the risks as well. It is made and documented during the identification workshops or interviews using the same qualitative method and scale introduced in the first iteration. Also, a category field was added into the risk identification table (Table 8) providing a modified table shown below:

Table 9. Risk analysis table.

Risk category	Risk description	Vulnerability	Impact	Likelihood
People	Risk 1	Weakness 1	Low	High
Processes	Risk 2	Weakness 2	Medium	Medium

The next step is stated as the risk analysis, which is now suggested to be performed for the key risks. This is driven by the need of the case department to get more detailed information on operational risks in its environment. One of the most meaningful weaknesses identified in current state analysis was regarding the level of analysis of the risks being insufficient for the needs of the case department (Data 1). Due to the limited resources and the best practice advise by COSO (Andersen et al. 2011:2), more in-depth analysis should be made on the key risks only.

For that, more theory on the risk analysis were studied and from the general risk model, which describes risk origin and its consequences, the table above was derived. The table also provides more visibility into the origin of the risks.

The general risk model described in *Guide for conducting risk assessments,* models the genesis of the risk and the factors related to it. The most relevant key factors from the generic risk model were transformed into a table in the following manner:

Table 10. Key risk analysis table.

Threat Event	**Vulnerability**	**Risk**	**Severity**
An event or change of circumstances which has consequences for the business through affecting existing vulnerability	Existing weakness in technology, processes or other areas.	Actual risk – an event with adverse consequences and likelihood less than 100%	Calculated severity and qualitative impact for the key risks

The case department was especially interested to know the underlying problems causing risks, risk origin and total cost or severity (Data 1, Data3). Angling these needs, the table above was concluded.

The impact here is suggested to be assessed in both qualitative and quantitative ways, which is advised by Philippa X. Girling in her book, to achieve the most versatile assessment. (Girling 2013:9) Impact can be assessed by interviewing the business owners, as recommended in the *Guide for conducting risk assessments* by National Institute of Standard and Technology and U.S. Department of Commerce. (NIST 2012:28)

Considering very low maturity of the cade departments risk management, the assessment method were decided to keep as simple as possible, with no complex quantification methods. (NIST 2012:7)

These were the only changes made into the process of the risk assessment proposed in the first iteration. The second Risk Assessment Pilot

Since the risk identification was sufficient and broad enough, it was unnecessary to redo it. Basically, only more extended analysis on the key risks was needed to do.

For the key risks, likelihood and impact were scored in a more detailed manner. Likelihood was calculated based on historical data. Interviews with the business owners were conducted for more thorough assessment of the impact of the biggest risks (Data 4).

They are listed in Table 11 below:

Table 11. Risk analysis interviews and workshops.

	Participants	Purpose
Workshop 1	Business owner, end users	Impact assessment
Interview 1	The Head of the customer business unit	Impact assessment
Interview 2	Service Delivery Manager 1	Impact and likelihood assessment
Interview 3	Development Manager	Impact and likelihood assessment
Interview 4	Vendor representative	Impact and likelihood assessment

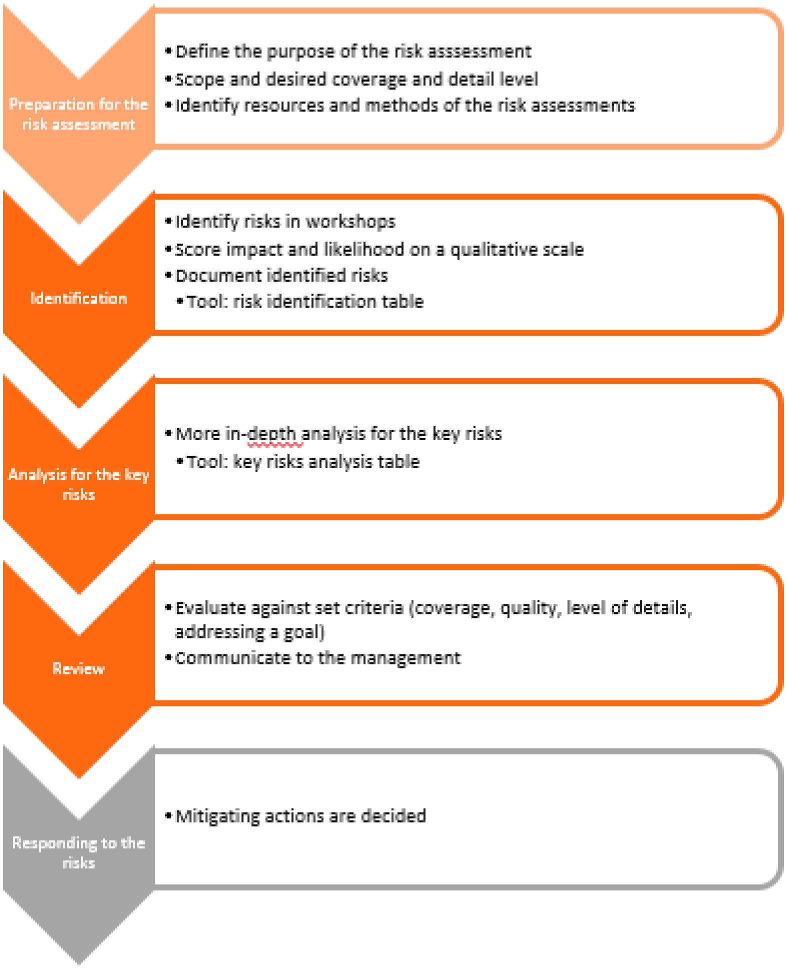
The further analysis was reviewed in a workshop with the Head of the case department, Service Delivery Manager and Development of the case department (Data 4).

It was concluded that now the risk assessment met the goal that was set for it. Impact and severity assessments were detailed enough and were utilized in the road-map development immediately.

5.4 Process proposition

On the basis of goals, theory and the iterations completed, the final process proposition was drawn (Figure 7). As before the pilot, simple and straightforward risk assessment process would fit the needs of the case department the best. The process consists of three steps and does not require any special training or software. This was also pointed out by Ilmonen et al: they emphasized that the risk management process can always be ‘built-up’ when it is already up and running, and it is recommended to keep it the simplest in the beginning (section 4.6).

Figure 7. Final process proposition


Preparation for the risk assessment
•Define the purpose of the risk asssessment
•Scope and desired coverage and detail level
•Identify resources and methods of the risk assessments
Identification
•Identify risks in workshops
•Score impact and likelihood on a qualitative scale
•Document identified risks
•Tool: risk identification table
Analysis for the key risks
•More in-depth analysis for the key risks
•Tool: key risks analysis table
Review
•Evaluate against set criteria (coverage, quality, level of details, addressing a goal)
•Communicate to the management
Responding to the risks
•Mitigating actions are decided

5.4.1 Preparation for the risk assessment

The whole process starts from preparation for the risk management. This is the phase, described as context establishing in ISO 31000 (section 4.3.2). Key activities here are:

- Defining the purpose of the risk assessment to ensure that the assessment will provide appropriate outcome, which will support the intended decisions.
- Identifying scope of the assessment. This includes, defining things such desired coverage and detail level of the assessment. Scope differs depending on the purpose.
- Identifying methods and resources for risk identification and analysis.

It is good to acknowledge these issues, and they should be reviewed on the regularly basis and every time the needs or goals of the case department change or there are some organizational or regulatory changes. If not, normally the preparation made in this case study, as well as determined tools, can be used in future as well.

As this step defines the whole risk assessment process it is good to proceed through it with a common sense, avoiding too sophisticated or bureaucratic approaches. This will reduce risk of insufficient resources or decreased motivation for the risk assessment.

5.4.2 Risk identification

The next step is risk identification, the most important and laborious step of the risk assessment. Key activities suggested here are:

Identify risks. These is recommended to be done in 2 or 3 bigger cross-function workshops within department. It is good to keep an open mind brainstorming risks in the beginning and then to review risks from previous assessment conducted and to complete risk list with reviewed old ones.

Document identified risks. This is the only way to make the risks more visible and manageable. This also addresses a challenge, identified in CSA (section 3.3), standardizes the perception of risk and brings visibility into risks of the case department.

Score impact and likelihood on a qualitative scale. Qualitative scale is to be decided by the management or workshop facilitator. The one used during this case study can also be used, it was experienced convenient during pilot.

Risks are suggested to be documented using the following table. This table was derived from a generic risk model, described by National Institute of Standards and Technology and U.S. Department of Commerce (section 4.5) and from its modification used in the second iteration (section 5.3.1).

Risk Category	Vulnerability	Risk	Likelihood	Impact
People Processes Vendors and external threats Technology Others	Existing weakness in technology, processes or other ares.	Actual risk – an event with adverse consequences and likelihood less than 100%	Scored likelihood on a qualitative scale	Scored impact on a qualitative scale

Threat event and severity were removed from the table at this stage. Threat event provides more information on the origin of the risk and is a part of a deeper analysis. Severity will be assessed in the analysis step. Discussing also them at this point, would make workshops too 'heavy' and overloaded. Also, these fields can be derived from data gathered in risk identification.

Documentation is recommended to keep quite light, so it would not take too much time and the results of the workshops would be more easily compoundable. When conducting workshops, chosen qualitative scales should be presented in the beginning.

5.4.3 Risk analysis

This step is where risks' severity is being assessed and possible deeper analysis for the key risks is carried out. Key activities of this step are:

- Categorizing risks means removing redundancies when compounding tables from the workshops and categorizing risks by impact or likelihood. Some risks considered insignificant or irrelevant to the assessment purpose should be removed.
- Assessing severity is done using RAG matrix approach for the smaller risks.
- For the key risks, more thorough analysis is concluded. Impact and likelihood are assessed in a qualitative and quantitative way together with the end users and/or business owner.

This step can be kept very simple in the future if no unexpected or new key risks have risen during the identification. If more thorough analysis is required, the risk identification table can be complemented with 'threat event' column, which will provide more information on the risks origin.

5.4.4 Review

This is the step derived from risk evaluation from ISO 31000 risk assessment process. It consists of couple key activities:

- The risk assessment is being reviewed against criteria set in the preparation phase. Things like degree of coverage and fitness to the purposes are evaluated. This is done using common sense with no sophisticated tools or techniques. If not sufficient, more analysis or another iteration may be conducted.

- The previous activity can be carried out either by the performer of the risk assessment him-/herself or together with management. However, the assessment must be presented and ‘accepted’ by the management of the case department. The management then reports the risk further on through the organizational software.

Considering, that the process proposition is drawn for the department use only, this step is more of a quick check if the outcome actually is appropriate. The context established in the beginning can be used as a kind of a check-list for the final review.

Mitigation actions can be also decided here, or in the previous step during the workshops, if appropriate.

5.4.5 Responding to the risks

Next, risks are being addressed. The management decides on what risks to accept, transfer or mitigate and brings mitigation plans into action. This part was out of the scope of this thesis.

5.5 Learnings and improvement suggestions

Some learning points can be turned into advice for the future.

As the theory states, before building up the risk management process, it is essential to ensure the previous step is fully implemented and is adopted by the employees. Since the regularity of the risk assessments was one important goal of this case study, the proper implementation of the process is a key success factor.

Communicating extensively analyzed risks with explicit values is more efficient and easier do understand across the organization – the measurement of the impact is the kind they understand (money).Regular assessments are also stated in the guidelines of the case organization, and literature on the risk management best practice. Therefore, the management of the case department should include this into their year activity clock.

In the future, when the process of risk assessment will be well adopted in the case department and will have a standard procedure, bigger cross-function workshops might be considered. Possibly in this case, the analysis of the risks (in qualitative approach) could be conducted in the same workshop. The downside of this arrangement is that it would be time-consuming and would occupy a large percentage of the department's employees at once.

The same assessment methods and scales can be used in the future, unless the circumstances change. More thorough analysis takes place in case of new significant risks and changed circumstances of previously recognized key risks – to reassess their impact and likelihood. It is also very useful to do, if the risks touch on ongoing big projects and need to be communicated across the organization or be an input into cross-department decision making.

When the risk assessment process in the case department gains more maturity, the identification and assessment could be done via checklist, formed based on the documented risks of the previous assessments. It is important to compile from several previous assessments, not one, to ensure more objective coverage. It is also important to keep in mind, that to be on top of the operational risks, more thorough assessments (e.g. in workshops) should still be carried out regularly or when the environment of the case department changes significantly.

There is a possibility, the process will not get practiced regularly enough if the responsible person is not pointed. Therefore, the management of the department should consider naming the person responsible for the risk assessments in the future. His/her responsibility would be preparing and carrying out the risk assessment, documenting the risk and their evaluations and reporting the to the management.

6 Conclusion

This study was conducted as a case study for ICT department in a large organization. It addresses the challenge the department was having with the risk assessment process. The solution is based on the current state analysis and the existing knowledge on the risk management and risk assessment processes, and best practice for the implementation of the risk management process. The current state analysis was conducted through interviews and the weaknesses in the current situation were explored, based on which relevant theory was selected, and a solution was formed.

The objective of the study was to ensure the secure service production within the department and to support meeting the strategy of the company. The executed risk assessment exercise provided a comprehensive picture on the risk environment and enables more informed decision-making. The process proposition can be used for the future assessments ensuring regularity in the risk management, which was the goal.

6.1 Evaluation of the proposed solution and risk assessment exercise

By providing the process proposition for the regular risk assessments, the case study support the strategic objectives of the organizations and industry regulation requirements. Giving a thought that the case department had no process for thorough risk assessments before the proposed process was decided to be kept simple and light. This is also in line with the best practice of risk management. Regardless of its straightforward approach, the proposed process serves all the needs of the case department, so the objective is met.

In addition, the outcome of this study was also conducted, and operational risk assessment was documented. The need for the thorough risk assessment was coming externally from the organization, but also from internal needs of the case department. They wanted to improve their processes in order to achieve their goal of becoming the best ICT department in the country. It was also longed-for in development and investment activities. As the case department works closely cooperating with its customer department, it was essential to communicate the risks also to them.

The outcomes of this study were taken into use immediately, which shows that the study was useful for the case department.

The study was an interesting learning process for myself, as I was not well familiar with risk management best practice before. If I had a chance to run the risk assessment the next time, I would improve it by arranging cross-function workshops, as it allows deeper and more objective assessment of the risks already during identification phase.

7 Sources

Anderson, R.J., Frigo, M. L., 2011, *Embracing Enterprise Risk Management: Practical Approaches for Getting Started.* The Committee of Sponsoring Organizations of the Treadway Commission (COSO). [Online] Available from:https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf [Accessed 24 May 2017]

Basel Committee on Banking Supervision, 2014, *Review of the Principles for the Sound Management of Operational Risk.* [Online] Available from: http://www.bis.org/publ/bcbs292.pdf [Accessed 24 May 2017]

Basle Committee on Banking Supervision, 1998. [Online] Available from: http://www.bis.org/publ/bcbs42.pdf [Accessed 24 May 2017]

Erola, E., Louto, P., 2000, *Riskit Voimavaraksi – liiketoimintariskien hallinta yrityksessä.* Helsinki: Oy Edita Ab.

Girling, Philippa X., 2013, *Operational Risk Management – A Complete Guide to a Successful Operational Risk Framework.* eBook: ProQuest. [Online] Available from https://ebookcentral.proquest.com/lib/metropolia-ebooks/reader.action?docID=1404585 [Accessed 24 May 2017]

International Organization for Standardization, 2016, *ISO in brief.* Geneva: ISO. [Online] Available from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/isoinbrief_2015.pdf [Accessed 24 May 2017]

Ilmonen, I., Kallio, J., Koskinen J., Rajamäki, M., 2010, *Johda riskejä – käytännön opas yrityksen riskienhallintaan.* Pössneck: GGP Media GmbH.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P., Talala, T., 2014, *Yrityksen riskienhallinta.* Helsinki: Finanssi ja vakuutuskustannus Oy (FINVA)

Lark, J., Nikonov, V., 2015, *A practical guide for SMEs.* Geneva: ISO. [Online] Available from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_31000_for_smes.pdf [Accessed 24 May 2017]

NIST and U.S. Department of Commerce, 2012, *Guide for conducting risk assessments.* Gaithersburg: National Institute of Standards and Technology. [Online] Available from: https://rmf.org/images/stories/rmf_documents/sp800_30_r1.pdf [Accessed 24 May 2017]

Appendix 1. Current state analysis interview question list

What are the responsibilities of the department?

What are Operational Risk Management practices in your company?

What are Operational Risk Management practices in your department?

What are the resources of the case department regarding risk management?

What are the goals of the case department regarding operational risk management?

When was the last operational risk assessment carried out?

What was the procedure and the results?

How often it is normally done and what level of identification and analysis?

How were the risks evaluated?

What were the key risks identified?

Appendix 2. Risk identification table

Risk	Event	Impact	Likelihood
Risk 1	Event 1	big	small
Risk 2	Event 2	big	small
Risk 3	Event 3	big	big
Risk 4	Event 4	medium	medium
Risk 5	Event 5	big	medium
Risk 6	Event 6	medium	medium
Risk 7	Event 7	big	medium
Risk 8	Event 8	small	medium
Risk 9	Event 9	big	medium
Risk 10	Event 10	big	small
Risk 11	Event 11	small	medium
Risk 12	Event 12	big	big
Risk 13	Event 13	big	medium
Risk 14	Event 14	small	medium
Risk 15	Event 15	big	big
Risk 16	Event 16	big	big
Risk 17	Event 17	big	small
Risk 18	Event 18	small	small
Risk 19	Event 19	small	small
Risk 20	Event 20	small	big
Risk 21	Event 21	medium	medium
Risk 22	Event 22	big	small
Risk 23	Event 23	small	medium
Risk 24	Event 24	big	medium
Risk 25	Event 25	small	big
Risk 26	Event 26	big	medium
Risk 27	Event 27	big	medium
Risk 28	Event 28	small	big
Risk 29	Event 29	big	small
Risk 30	Event 30	big	big
Risk 31	Event 31	big	small
Risk 32	Event 32	small	medium
Risk 33	Event 33	medium	medium
Risk 34	Event 34	small	small

Appendix 3. RAG matrix, risk analysis

Risk	Impact	Likelihood	Severity
Risk 1	big	small	🟨
Risk 2	big	small	🟨
Risk 3	big	big	🟥
Risk 4	medium	medium	🟨
Risk 5	big	medium	🟥
Risk 6	medium	medium	🟨
Risk 7	big	medium	🟥
Risk 8	small	medium	🟩
Risk 9	big	medium	🟥
Risk 10	big	small	🟨
Risk 11	small	medium	🟩
Risk 12	big	big	🟥
Risk 13	big	medium	🟥
Risk 14	small	medium	🟩
Risk 15	big	big	🟥
Risk 16	big	big	🟥
Risk 17	big	small	🟨
Risk 18	small	small	🟩
Risk 19	small	small	🟩
Risk 20	small	big	🟨
Risk 21	medium	medium	🟨
Risk 22	big	small	🟨
Risk 23	small	medium	🟩
Risk 24	big	medium	🟥
Risk 25	small	big	🟨
Risk 26	big	medium	🟥
Risk 27	big	medium	🟥
Risk 28	small	big	🟨
Risk 29	big	small	🟨
Risk 30	big	big	🟥
Risk 31	big	small	🟨
Risk 32	small	medium	🟩
Risk 33	medium	medium	🟨
Risk 34	small	small	🟩

Appendix 4. Key risk analysis table

This table was alco complemented with qualitative impact and likelihood values, which are only for the use of the case company.

Category	Risk	Vulnerability	Impact	Likelihood
External threats	**Risk 3**	Weakness 1	big	small
Technology	**Risk 5**	Weakness 2	big	small
Technology	**Risk 7**	Weakness 3	big	big
Technology	**Risk 9**	Weakness 4	medium	medium
Processes	**Risk 12**	Weakness 1	big	medium
Processes	**Risk 13**	Weakness 5	medium	medium
Processes	**Risk 15**	Weakness 3	big	medium
Vendors	**Risk 16**	Weakness 5	small	medium
Vendors	**Risk 24**	Weakness 5	big	medium
Vendors	**Risk 26**	Weakness 6	big	small
Vendors	**Risk 27**	Weakness 7	small	medium
People	**Risk 30**	Weakness 3	big	big