Applying effective risk management into project management - case governmental ICT service organization

Sami Moilanen

2019 Laurea

Laurea University of Applied Sciences

Applying effective risk management into project management, case governmental ICT service organization

Applying effective risk management into project management - case governmental ICT service organization

Sami MoilanenSami Moilanen
Security Management
Bachelor's Thesis
May, 20192019

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

Sami Moilanen

Applying effective risk management into project management - case governmental ICT service organization

Year 20192019 Pages 322

The developmental objective of this thesis was to create a project risk management framework and process for a Finnish governmental ICT service organization. Knowledge base was based around risk management, project management, internal documentation and policy of the case organization, and expansive learning theory. This study used qualitative and developmental methods such as literature review, document analysis, and co-creational workshops.

The outcome of this thesis was the creation and visualization of project risk management framework and process. The process implementation has been and explained and a plan presented for finalizing the design and implementing the new process. Next steps schedule is presented at the results of this thesis. The case organization has a well described and functioning project management system where implementing the risk management process is cost efficient. Developing the reporting of risks accordingly with risk criteria and used tools and techniques will be the last piece in designing the process which can then be implemented, evaluated and improved.

Keywords: risk management, project management, project risk management, risk management framework, risk management process

Table of Contents

1 Introduction

The case organization had identified that there was no specific framework or process for managing project risks in the within case organization. Risk assessments varied in for example, quality, how they were monitored, reported, and at what level they were made (for example, tied to strategic risk management and the continuity of the organization or process specific). There were some tools and pieces of information however the outcome is was not satisfactory.

This was a project-based development thesis and the thesis was a part of a larger development of risk management at the case organization. The development objective of this thesis was to establish an effective process for project risk management at the case organization. To do that the following had to be stablished:

- How could risk management be applied effectively in project management in the case organization?

The objective of this thesis was to standardize the project risk management process at the case organization by applying risk management framework into project management and creating a process description with recommendations for implementation. After this research and development, we hoped to have described a set framework and process for project risk management at the case organization which can be completed by design and implemented for review and improvement. The exclusions were considered, and I suggestions offered in those parts to achieve a thorough framework.

1.1 Scope, exclusions & limitations

The scope of this thesis was applying ISO31000 risk management standard and COSO ERM based risk management framework into project management at the case organization. Exclusions in this thesis were risk analysis (risk assessment tools & techniques, risk criteria) and reporting principles. These will be defined by the case organization. The scope of risk management will be defined by the case organization. Project Management framework were already defined by the case organization.

Limitations in this thesis included: The best practices approach was not the main research area, but the goal was to have a guideline for project risk management that can be developed further in the future. Some of the literature reviewed was written with the assumption that the reader knows the basics of project -or risk management. Other standards or frameworks outside the two biggest were not researched, and the effectiveness of this study couldn't fully be measured within this study. As this project was part of larger development of risk management at the case organization there were internal and external demands.

2 Project Risk Management

The case organization is a Finnish governmental ICT service organization offering various financial, and other software and services to other governmental actors and private sectors. According to Murray (2011) ICT includes information technology along with integrations of communications -and data technologies. ICT has a broader meaning than it used to due to new applications of technology. The case organization employs between 500-1000 people. Internal and external demands for this thesis are explained in Figure 1 where the first column presents internal demands, and the second column external demands.

INTERNAL DEMANDS	**EXTERNAL DEMANDS**
The existing risk management policy of the case organization does not mention project risks	As the case organization is a part of the Finnish Government the compliance of rules and regulations is highlighted
The case organization expects to get a concrete set of actions to develop the project risk management process	The case organization handles classified information and so information security is highlighted
Included in a larger development project of risk management at the case organization	The Ministry of Finance regulates the case organization and they have comprehensive demands and instructions on various security aspects stated by VAHTI (the Government Information Security Management Board)
	The Ministry of Finance also has a risk management policy that bounds the case organization however they do not yet state clear demands or advice on project risk management

Figure 1. Demands for thesis. 2019

Internal demands for this thesis come from the case organizations need and expectations. This project is also a part of a larger development of case organization's risk management and therefore risk criteria, and risk assessment tools and techniques have been excluded from

this thesis and will be develop later in the year. Compliance with rules and regulations is important for the case organization. The case organization handles classified information and information security is highlighted. The governing Ministry may later include project risk in their risk management policy. The Finnish government risk management framework follows ISO 31000 and is attached to appendices along with a glossary for the thesis terminology in Finnish, see appendix 1 and 2.

This thesis included developing and plans for implementing a new organizational process. The need for a new process was identified and a new model designed as visualized in the expansive learning cycle (see Figure 2). Expansive learning is a theoretical approach to developmental research and according to Engeström (2004, 13) a communal process where a new operational model is developed and implemented.

Figure 2. Expansive learning cycle (Engeström 2004, 61)

The expansive learning cycle includes other steps as examining and implementing the new model, reflecting the process, and consolidating the practice. Examining and implementing the new model means evaluating and testing the model with implementing new tools and solutions. After reflecting the process, the new practice can be verified.

The thesis process is visualized in Figure 3. The framework includes risk management and project management theory, the case organization's existing procedures and demands for the thesis, as well as theoretical background of developmental methods used in this thesis. The thesis process is visualized in the middle of the framework including introduction to the development objective, developmental methodology, and the empirical outcome of this thesis.

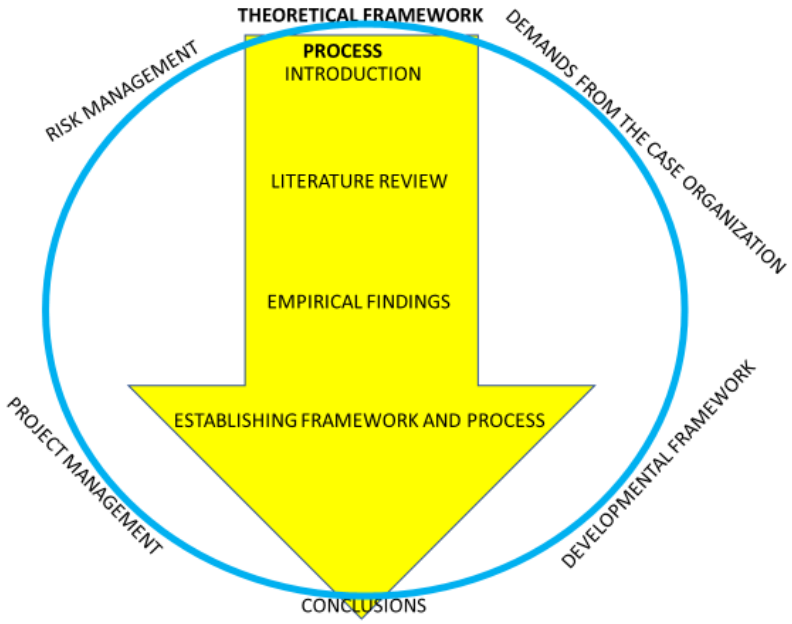


Figure 3. Thesis process. 2019

The main theoretical framework for this thesis comes from risk management and project management. Projects are considered according to ISO 27500 (2012, 3) a set of co-ordinated activities with a start and end date, designed to achieve an objective or objectives. According to Lock (2013, 1) project management is the management discipline that ensures a successful outcome of a project by planning, organizing, and controlling the resources like personnel and money. The word apply, and application are used in this thesis as 'something put to use', and not for example, a request, or a program. (Merriam-Webster 2019).

2.1 Risk Management

According to Hopkin (2017, 71) risk management standards set an overall approach to risk management with the description of risk management process and a suggested framework whereas the frameworks might be limited in describing the process itself. By including both aspects in this research, I hoped to set the best possible approach for the case organization. COSO ERM and ISO 31000 are among the best-established risk management approaches (Hopkin 2017, 74). They are also approaches that are currently utilized in the case organization.

ISO 31000 is an international standard for risk management created by the International Organization for Standardization designed to provide an organization a framework and process to manage risk. (ISO website - Accessed 30.1.2019). COSO ERM is an enterprise risk management framework created by the Committee of Sponsoring Organizations of the Tradeway Commission. (COSO Integrated Framework; Executive summary. 2004).

COSO ERM has been updated regularly however I am not using the latest version of COSO ERM because I cannot get full access to the newest 2017 version within the parameters of this research. The basic principles of risk management in COSO ERM remain the same and this is not a significant limitation for this research since:

- The updated framework provides greater insight into business strategy and incorporating ERM in strategic planning (Proviti ACCESSED 6.2.2019), which is not the concern in this research. The new COSO ERM clarifies the importance of enterprise risk management in strategic planning (COSO 2017, 6) whereas ISO 31000 can be applied to project levels (ISO 2018, 13).

- We have identified within the case organization prior to this that the COSO ERM is quite heavy framework to use however we want to reflect the ISO 31000 to COSO ERM for the best possible decision and result in applying project risk management.

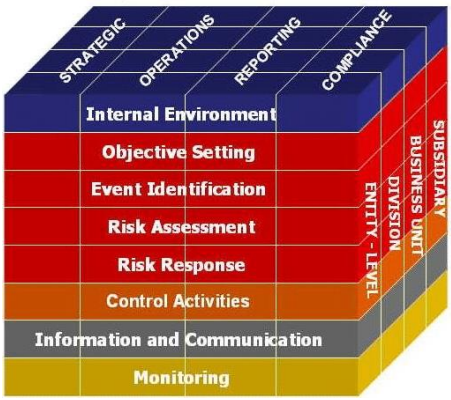


Figure 4. COSO Framework (Moeller 2011, 55)

Figure 5. COSO Framework (COSO 2017, 5)

Major change in COSO ERM 2017 is the modelling of their framework which went from Cube (see s

4 page 10) to Helix (see figure 5 page 10) however the components of the framework remain the same (COSO 2017, 5). COSO emphasizes the importance of governance, risk, and compliance (Moeller 2011, 21) in setting an enterprise risk management framework. According to Moeller (2011, 25) risk management is one component of that and includes: Risk assessment and planning, Risk identification and analysis, Risk response, and Risk monitoring. “Enterprise risk management is a process effected by an entity’s board of directors, management and other personnel applied in strategic setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” (COSO ERM 2011, 53).

Figure 6. ISO 31000 Framework (ISO 2018, 9)

According to ISO 31000 (2018, 9-10) top management is responsible for implementing the framework and issuing a policy to establish risk management approach. They also need to ensure enough resources to risk management activities and assign authority, responsibility, and accountability at different levels of the organization. This is supported by COSO ERM which starts from the strategic level and environmental settings of an organization. The implementation and proper support from top management will help in for example, aligning the risk management with the organization’s objectives and strategy, addressing all obligations, systematic risk monitoring, development of risk criteria, and communication to stakeholders. The ISO framework (see figure 8, page 11) resembles the Plan-Do-Check-Act model (see figure 7, page 11) that according to American Society for Quality is used for project planning and continuous improvement when carrying out change (2019).

Figure 7. PDCA model (American Society for Quality – ACCESSED 7.2.2019)

ISO 31000 explains risk management as a process part of the leadership of any organization and is designed to assist in setting strategy, achieving objectives, and help in informed decision making. Risk management is associated with all activities within the organization and should help in how the organization is managed at all levels. Risk management includes interaction with stakeholders and considers both the internal and external environment of the organization. In its simplest form risk management is the activities that control an organization in regards of risk. (ISO 31000 2018, 5).

Both ISO 31000 and COSO ERM explain risk management as a process that crosses many levels of an organization and includes protecting value and controlling risk. According to ISO (2018, 6) a risk is the effect of uncertainty on objectives. This means that there might be a deviation from what is expected, negative or positive, and that it results in opportunities or threats. Risk controls are the measures that affect the risk for example, policy, processes, guidelines and other activities that maintain or modify the risk. (ISO 31000 2018, 7)

According to Moeller (2011, 32) risk management is a four-step process involving Risk identification, assessment of risks (quantitative or qualitative), risk prioritization and plan for risk response, and risk monitoring. According to ISO 31000 (2018, 13) risk management process should be a fundamental part of management and decision making. The process should be applied into the structure, operations, and processes of the organizations. It can also be applied at strategic, operational, programme, or project levels. (ISO 2018, 13)

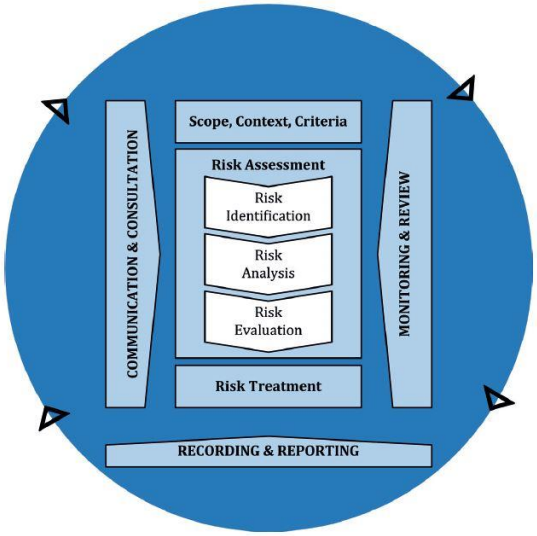


Figure 8. ISO 31000 Process (ISO 2018, 13)

The ISO 31000 risk management process is illustrated in figure 8, page 11. According to ISO (2108, 13) "The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risks." The risk management process in practice is iterative (ISO 2018, 13). According to ISO 31000 (ISO 2018, 9) the effectiveness of risk management depends on the integration into governance of the organization and requires support especially from the top management. The existing risk management practices and processes should be evaluated, and any gaps addressed within the framework. The framework should be customized to the needs of the organization. (ISO 2018, 9)

Both ISO 31000 (see figure 8 page 12) and COSO ERM (figure 5 page 10) focus on the same principle which is designing the framework for the organization at hand and implementing a process to identify and handle risk. The design phase should include the internal and external operational environments and the task at hand. The process of risk management includes objective setting, risk identification, risk evaluation, and risk response and monitoring in both frameworks (see COSO ERM Framework – Figure 4 page 10 & ISO 31000 Process – Figure 8 page 12) even though they are visualized differently. The framework revolves in establishing the context of risk management including risk criteria and monitoring & reporting principles whereas the process focuses on risk assessments and risk treatment.

2.2 Project Management

Project management framework is defined by the case organization. There are three types of projects defined by the case organization depending on the objectives and length of the

project, and for example, if it's a development project of something existing, or a completely new undertaking. The project tracking tool that currently includes an electronic risk assessment tool is used for all three types of projects, so the applied risk management framework will cover all projects that are covered by the project management framework of the case organization. (Projektien määrityslista 2017, 1-4)

Most projects at the case organization are some type of information communications technology projects whether it is designing a new platform or developing parts of existing software's. The average project length is between 6 to 12 months. At any given moment there is about 20 to 30 ongoing projects. (Case Organizations project data base 2019)

The projects in the case organization have the following steps:

PROJECT PHASE	**INCLUDING**
Setting the project	Preliminary budgeting, project number, opening the project in the project tracker, etc.
Preparing the project	Project plan, specified budgeting, determine project responsibilities etc.
Execution	Progression reporting, meetings, etc.
Implementation	Progression reporting, decision of moving to production, etc.
Finalization	Final reporting, etc.

Figure 9. Case Organization Project Steps. 2019

Each project has a directory board including directors from each unit that is working with the project, and an assigned project manager. Project personnel varies depending on the project and it might include outside contractors and specialists. Some projects are shared projects with other governmental organizations and might be directed from the governing ministry. (Projektiroolit 2017, 4)

2.3 Risk Management in Project Context

According to ISO 31000 (2018, 15) risk identification is identifying and describing the risks that might help or prevent in achieving objectives. According to Moeller (2011, 33-35) risk

identification should cover all possible risks that might affect operations, emphasis on risks affecting enterprise (strategic risks, operational risks, finance risks, ICT risks). The process needs to occur in multiple levels of the organization and techniques can be for example, brainstorming. (2011, 33-35)

According to Brown & Chong (2000, 40) project risks are classified as having one of the three negative effects; “Quality”, “Cost”, and / or “Time”. This means each risk relates to failure to achieve objectives, budget, or schedule. The risk analysis needs to reflect this to effectively estimate the risks. Often the risks will affect all of the aspects (quality, cost, time) and the biggest risk driver is overlooked (Kwak & Stoddard 2004, 919). Also, moving towards quantitative risk analysis would be beneficial for more quality data. This means for example, combining previous data to be able to mathematically calculate the likelihood and impact of the risks should be utilized. Risks in business environment are usually assessed qualitatively and subjective to assessment (Brown & Chong 2000, 39). This means the outcome of risk assessments is affected heavily by the participants performing it, so it is important to have knowledge and possible previous data. According to ISO 31000 (2018, 7) likelihoods means the probability of something happening. In risk management the likelihood is measured objectively or subjectively, qualitatively or quantitatively, and it is described as words or as frequency.

According to ISO 31000 (2018, 16) risk analysis is done after risks have been identified to determine whether the risks should be treated and how. The risk analysis process should include the likelihood and consequences of an event, as well as the magnitude of said events along with evaluation of existing measures to control the risk. As risk analysis is mostly subjective things like quality of information, assumptions and exclusions made, and how the risk analysis is executed should be documented and reported to the decision makers. According to COSO ERM (2011, 13) risk assessment is the process that involves risk analysis and setting risk controls. According to ISO (2018, 13) risk assessment is the process of risk identification, risk analysis, and risk evaluation. According to Moeller (2011, 37-39 & 45-50) quantitative or qualitative assessment of risks should include significant risks impacting the organization with analysis of likelihood and significance of risk. Techniques can be for example, brainstorming and questionnaires. According to ISO 31000 (2018, 7) consequence is the outcome that affects objectives. Consequences can be certain or uncertain, and they can result in opportunities or threats.

“Risk analysis is like drawing a map of potential hazards and outlining the damage they could cause. Risk management is taking the map and deciding how to avoid the hazards.” (Brown & Chong 2000, 68). The quote simplifies the risk management however both aspects (risk analysis and avoiding hazards) are included in risk assessment thus not making risk management a separate action. Brown & Chong (2000, 224) identified three important stages of a project where risks and cost benefits should be evaluated. These are “Project initiation”, “Execution phase”, and “Project close down”. This is further supported by Kwak & Stoddard (2004, 916) where

research of failed software projects showed that the actualized risks would have been able to be mitigated with an early identification and procedures towards the high-risk elements identified. This shows the importance of systematic approach to assessing project risks already in the early phases of a project.

Risk monitoring means monitoring that all components of the framework are working properly and should be a continuous process involving reporting and feedback (Moeller 2011, 84-86). According to ISO (2018, 18) monitoring and review is done to assure and improve the quality and effectiveness of the implemented process, and it must be a designated responsibility. The monitoring and periodic review of risk management process should be a planned part of the risk management process and include analyzing information and providing feedback. (ISO 2018, 18). According to COSO ERM (2011, 282) risk monitoring in project context means the monitoring of previously identified risks and new risks during the project and to take preventative actions or changes when required.

3 Methodology

According to Bryman (2008, 366) qualitative research is a research method that emphasizes the context like meaning of words, rather than the amount of data (quantity). I used qualitative research methodology that included literature review of risk management and project management, and a document analysis on the current state of project risk management and project management in general at the case organization. According to Bowen (2009, 27) document analysis is a qualitative research method with a systematic approach to analysing documents to give them meaning and/or to gain understanding of the data.

According to Oliver (2012, 5-6) literature review is a research method where the broader view of a subject is researched to find out correlations to the more narrowed research that is being conducted. The purpose of literature review is to show how the research fits to broader context and whether there is something to be added for example, future prospects, or just to justify the research. I used qualitative methods because quantitative research would work well for example, for analysing market data or getting more accurate risk analysis data, however risk management is highly contextual and thus qualitative methods are used.

Qualitative methods used were developmental methods and included co-creation, like workshops. The workshops were semi-structured in a sense that there was a specific objective for each workshop around the application of the framework for the case organization's needs. Some of the workshops were more structured when for example, testing a toolkit, or doing a SWOT analysis, however some were just general discussion and sharing and gathering ideas. According to Gurel (2017, 995) SWOT analysis is a strategic tool for situational analysis to

analyse the internal factors (strengths & weaknesses) and external factors (opportunities & threats) of an organization, a project, a plan or a business activity.

Co-creational and developmental methods in this research included workshops and brainstorming with different parties such as colleagues, risk management consultants and auditors. According to Engeström (2004, 80-81) co-creation is a method where different parties come together and create new ideas with shared knowledge. According to Association for Qualitative Research (ACCESSED 2.1.2019) brainstorming is a creative process to develop ideas and solutions for problems, usually done in groups. The evaluation of the ideas and/or solutions is usually separated from the generation of the ideas and/or solutions to promote the participants to think freely.

The purpose of the workshops was to gain better understanding of the needs of the case organization regarding project risk management. They were conducted to meet the internal demands of the case organization. The first workshop was conducted with steps 1 and 2 of the expansive learning cycle (see figure 1, page 15) to question and analyse the current state of project risk management at the case organization. The second and third workshops relate to step 3 designing a new model.

4 Identifying problems and best practices

This thesis included developmental workshops that are presented in Figure 10. The first column identifies the workshop, the second column when it was conducted, the third and fourth columns show the objective and outcome. Co-creational methods included brainstorming and SWOT analysis.

WHAT	**WHEN**	**OBJECTIVE**	**OUTCOME**
Workshop 1	Jan 2019	Assessment of the current state of project risk management	Identification of issues, solutions, and future prospects
Workshop 2	Feb 2019	Assessment of approach based on theoretical framework	ISO 31000 based project risk management framework and process
Workshop 3	Fen 2019	Clarifying the risk assessment process of projects	Identification of actions, timeframe, and assigned responsibilities

Figure 10. Thesis workshops. 2019

The first workshop was conducted in 22.1.2019. The duration was 2 hours and included two participants of the internal auditors of the case organization with a total of 3 participants. The objective was to assess the current stage of project risk management of the case organization. The work shop was semi structured and included reviewing the existing model and determining future prospects. We identified three problems with our current project risk management during the workshop.

One major problem was the level where the risk assessments are made in project context. They vary and most relate to the strategic risks and goals of the organization however there is a problem with that: If only major risks to the organization are being considered in project risk assessments the project itself is not being secured. For example, a lot of risks that could be severe and even end a project were still irrelevant for the continuity of the organization thus not being monitored or even taken into consideration in the risk assessments. Also, the risk matrix that is being used is a 5x5 with no explanations of the likelihood and/or consequences. For the risk assessments to be accurate and comparable there needs to be set values, or at least documentation of the flow of though behind the risk assessments. This relates to the problem number one and the scale of consequences (pointed towards the project vs. organization in general). Another thing that came up is that whenever there is a risk matrix like 3x3 or 5x5 being used there is a "risk" that people play safe and go with the middle value. If we were to use 4x4 or 6x6 matrix it would force to assess the risks more thoroughly.

Problems 1&2 can be deleted with settling on a risk matrix and determine the values. Suggested values for likelihood in project risk assessments is to use percentages instead of text (every 10 years, etc.) which works well in other risk assessments like assessing process risks whereas the nature of project work requires a value like <8%, or 25-49% chance of happening. Values for consequences need to be determined and they need to be project specific highlighting the quality, budget, and schedule of the project. Because continuity of the organization is very important the consequence value 5 could include disruptions for the organization and their goals. Reporting of risks is tied to the risk values and reporting principles need to be assessed when developing the risk matrix. For example, risks with a value of 15 and more go straight to chief security officer / board of directors for assessment, along with risks with a possible consequence of 5.

We identified also that the overall project risk management process has no guideline on when and how the risk assessments are being made and by who, and there is no framework for monitoring and reporting project risks. This means that there are projects with no risk assessments made, whereas some projects have several but no reporting of risks. If risk assessments were standardized the data could be utilized in the future allowing for improved accuracy etc. The

risk mitigated with a project risk policy that dictates the following: Who does risk assessments, when are they made, how they are made, how risks are monitored and reported.

The second workshop was conducted with two security specialists from the case organization on 12.2.2019 to assess our approach to project risk management based on ISO31000 and COSO ERM. The duration of the workshop was 2 hours and we analyzed risk management frameworks and their suitability for the case organization's needs. The SWOT analysis is presented in Figure 11 page 18.

STRENGTS COSO ERM: Internal auditing and financial sector Strategic risk management ISO 310000: VAHTI-guidelines follow this easy and "light" to use	**WEAKNESSESS** COSO ERM: cost vs. benefit in project work harder to comprehend ISO 310000: Requires design in applying
OPPORTUNITIES COSO ERM: Comprehensive model with examples ISO 310000: cost vs. benefit in project work	**THREATS** COSO ERM: Too much work ISO 310000: Industry standard

Figure 11. SWOT Analysis of COSO ERM & ISO 31000 (2019)

We identified that COSO ERM is comprehensive model with various examples and theory best suitable for strategic risk management and building an enterprise risk management model. We also identified that ISO 31000 is easier to implement with shared knowledge. We view COSO

ERM as too time consuming to use and decided to follow ISO 31000 principles as the main frame. This workshop was part 3 of the expansive learning cycle "Designing a new model" (see Figure 2, page 7)

The third workshop was conducted with a security specialist, and a project manager of the case organization. The workshop was conducted 19.2.2019 and lasted two hours. The topics were also discussed with the director of compliance and risk management and members of project directory boards. of the case organization. The objective was to clarify the risk assessment process of projects at the case organization. We discussed who should participate in risk assessments, when they should be made, and how could risks be monitored. The outcome is presented in Figure 12 page 19 with the topic presented in the first column, when it should be done in the next column, responsibility in the third, and finally a more thorough explanation of what should be included.

WHAT	**WHEN**	**RESPONSIBILITY**	**INCLUDING**
PRINCIPLES	Setting the project	Directory Board	Project length, size and importance, risk criteria, relations to other projects, reporting principles
HIGH RISK ELEMENTS	Setting the project	Directory Board & Project Manager	Preliminary risk assessment, high risk elements of project
RISK ASSESSMENT	Set intervals	Project Manager	Quality, Budget, Schedule, relations to other risks and continuity of the organization
MONITORING	Continuous	Directory Board & Project Manager	Actions and updates on changes in internal & external environment, new risks, changed risks, effectiveness of risk treatment
REPORTING	According to criteria	Project Manager	Documentation of risk assessments and treatment, high risk elements

Figure 12. Workshop 3 Outcome. 2019

The projects vary in length and size so there are no definitive solutions however a clear guideline can be established. The project manager is responsible for execution of each project and reaching the project objective, so they should be responsible for conducting risk assessments

including inviting the relevant stakeholders. The schedule, budget, and quality requirements of each project are defined by the directory board of each project, so they should be included since they have the most authority for risk treatment. The directory board should define at the beginning of the project the principles for risk management in that project. Risk reporting should be arranged accordingly, continuous monitoring and reporting of changes, new risks, and scheduled updates / reporting to the directors. Project and risk correlations to other projects and the organizations strategic objective should be considered and documented as well.

5 Applying the framework into project management

Suggested project risk management framework and process follow the ISO 31000 guidelines. The ISO 31000 Framework and the ISO 31000 process (see figure 8, 12) have several steps that require customization according to the case organizations internal and external context (ISO 2018, 12-13). This thesis is part of the design and implementation phases of the ISO 31000 Framework (see Figure 6, page 11) The framework requires periodic evaluation so that aspect has been discussed. Improvement and monitoring of the framework should be continuous for it to be adaptable to internal and external changes. According to ISO (2018, 14) the scope of risk management activities should be defined within an organization. Things to consider when planning are for example, objectives and expected outcomes, time and location specific factors, risk assessment tools and techniques, resources and responsibilities, records to be kept, and relations to other projects, processes, and activities (ISO 2018, 14).

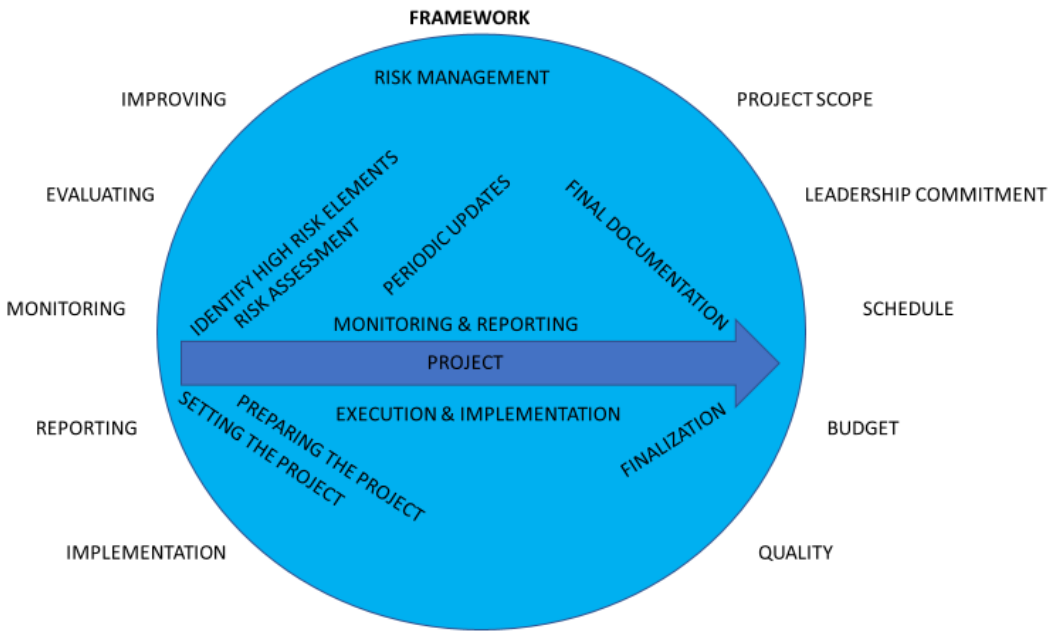


Figure 13. Visualization of Project Risk Management Framework. 2019

The case organization's Project Risk Management Framework is presented in Figure 13 page 20 with process steps in the middle. The objectives and outcomes at the case organization are governed by the project portfolio of including budget, schedule, and quality demands. The project directory board should plan the risk management process for each project with the project manager at the preparing phase and before setting the project. Relations to other projects and activities should be considered including strategic importance and resources. The context should also be considered especially since there are larger projects that have several stakeholder groups.

Risk criteria is excluded from this thesis and is developed further in the future. According to ISO (2018, 15) the criteria needs to be defined to be able to evaluate the significance of risk. The criteria should be customized to the specific purpose and scope of activity which in this case is projects at the case organization. Risk criteria must be set before starting the risk assessment process and needs to be continually reviewed for changes or improvement. (ISO 2018,15)

5.1 Risk Assessments and treatment

According to ISO (2018, 15) "Risk assessment is the overall process of risk identification, risk analysis and risk evaluation." The process should be systematic and utilize the best available information in collaboration with the knowledge and views of stakeholders (ISO 2018, 15). The project directory board includes project owners and should be included. The project manager should facilitate the risk assessments and include relevant stakeholders to participate. Other stakeholders could be ICT, programmers, communications specialists, risk consultants, and other project personnel.

Risk assessments should be first conducted during early phases of a project to avoid failure in early identification and mitigation of high-risk elements (Kwak & Stoddard 2004, 916). This further highlights the importance of systematic approach to risk management and is included in the scope of risk management which is set before setting a project. Risk assessments should be conducted periodically to effectively monitor risks and treatment measures, for example once a month. This doesn't require much resource allocation because most of the relevant stakeholders have periodic meetings within each project. Project risk management process is visualized in Figure 8 page 24 with preliminary risk assessment at the beginning of the project, periodic updates with continuous monitoring throughout the execution and implementation of the project, ending to final risk assessment and reporting of the project process.

Risk assessments should identify risks related to the quality, cost, and time aspects of each project (Brown & Chong 2000, 40). Risk analysis and risk evaluation may include several techniques however risk criteria must be set to be able to effectively document, monitor, and

develop the risk management process (ISO 2018, 16). According to ISO (2018, 17) risk treatment is selecting and implementing options to address risk. This may lead to for example, avoiding risk, taking risk, removing the risk source, changing the likelihood or consequence, sharing the risk, or accepting the risk. Risk evaluation and risk treatment must be documented, and remaining risks communicated to decision makers and other relevant stakeholders. Risk treatment plans must be specific and include responsibilities and accountabilities, proposed actions and expected outcomes, required resources and performance indicators, and reporting and monitoring of said actions. (ISO 2018, 18)

5.2 Monitoring and reporting principles

According to ISO (2018, 18) monitoring and review is done to assure and improve the quality and effectiveness of the implemented process, and it must be a designated responsibility. The monitoring and periodic review of risk management process should be a planned part of the risk management process and include analyzing information and providing feedback. (ISO 2018, 18). The case organization is considering an internal business controller to plan a review process for risk management functions. The communication and consultation aspect of the framework is included in monitoring and review and recording and reporting. The purpose is to provide knowledge to decision makers and to get feedback about the process (ISO 2018, 14).

According to ISO (2018, 19) the risk management process and its outcomes should be documented and reported to provide information for decision making, to improve the risk management process, and to communicate about risk management activities and outcomes. The use, sensitivity, and internal and external contexts should be taken into consideration when creating and handling these documents. Reporting principles will be defined by the case organization and should include cost, frequency, and timeliness of reporting, reporting method, and relevance of information to objectives and decision making (ISO 2018, 19).

ID	RISK (DESCRIPTION)	CAUSES	CONSEQUENCES	L	P	T	RESPONSE PLAN	RESPONSINILITY	OWNER	NOTES (CHANGES & RECORDS OF ACTIONS)	CLOSED

Figure 14. Risk report. 2019

According to Dalcher & Harris (2009, 90) project risks should be registered for tracking and recording risk management actions. The risk register should include the following: Reference number for the risk, Description of the risk, Risk analysis, Risk assessment, Priority ranking, Risk response plan (actions to tackle the hazard), Ownership of the risk, Updated outcomes of actions, and Closure date. This is visualized in Figure 14 page 22 with a system that could be utilized in risk assessments as well. Risk ID can be a number or other id to sort risks. The risk is described, and possible causes and consequences explained. “T” stands for the total risk score

which is calculated with the help of a risk matrix and according to risk criteria by Likelihood times Potential outcome. A detailed risk response plan is written with assigned responsibility and owner for each risk. Any changes and effectiveness of risk treatment is documented.

6 Results

The project risk management framework is visualized in Figure 13 page 20. The framework should be included and in line with the overall scope of the case organizations risk management. As there are different types of projects and changes in the operational environment the risk management framework and process must be dynamic and compatible to change. This is ensured by determining risk management principles to each project including the project scope and budget, quality and schedule demands. Risks are monitored constantly and reported accordingly to reporting principles. Effectiveness of the process is ensured by gathering feedback during reporting or when doing risk assessments.

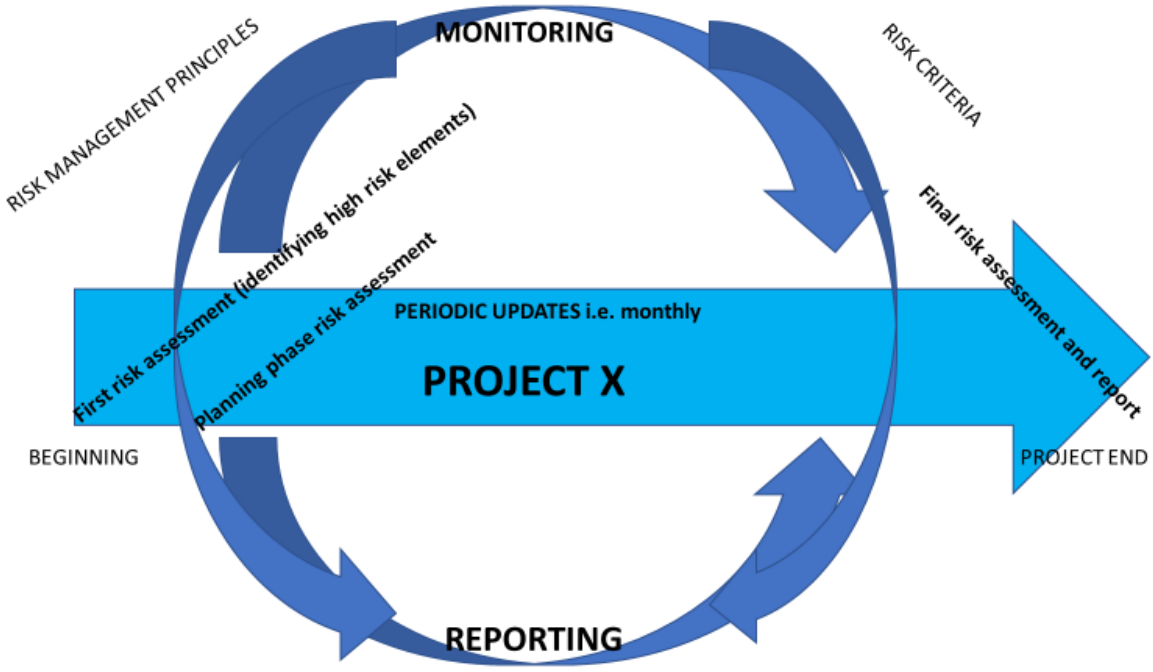


Figure 15. Project Risk Management Process. 2019

The risk management process is visualized in Figure 10 page 26. Risk management principles and risk criteria is established, and the first risk assessment is done in the beginning of the project. The risk assessment is updated in the planning phase of the project and then regularly according to set principles and when something unexpected that might have an impact on the quality, budget, or schedule of the project occurs. Risk monitoring is continuous, and reporting is done according to risk criteria and reporting principles of the project and case organization.

When the project ends, a final risk assessment is documented for gathering data and improving the process.

Next steps for implementation of the project risk management framework are establishing risk criteria, and reporting and monitoring principles. After that the framework and process can be implemented to the case organization by training and facilitation. Feedback can be gathered for example, during risk assessments and reporting, and improvement can continue. Next steps are visualized in Figure 16 page 24 with the task presented in the first column, schedule in the next and notes in the last.

NEXT STEPS	**WHEN 2019**	**NOTES**
RISK CRITERIA	March-April	Developing framework and deciding on a 5x5 Matrix vs. 4x4 or 6x6 Matrix. Percentual likelihood for projects. Risk management context and risk appetite & tolerance. Criteria tied to reporting and monitoring?
REPORTING PRINCIPLES	April-May	Documentation requirements, standardized method for consistency.
MONITORING PRINCIPLES	April-May	Continuous risk monitoring and scheduled and assigned monitoring of effectiveness of the framework
TRAINING AND AWARENESS	May-July	Training the principles and familiarizing guidelines for key personnel such as project managers and directory board.
FACILITATING IMPLEMENTATION	August	Continue training by facilitating risk assessments. Gather feedback and improve.

Figure 16. Next Steps Schedule. 2019

7 Conclusion

The objective was to establish an effective process for project risk management at the case organization. I managed to establish a concrete project risk management framework (presented in Figure 9 page 19) and a project risk management process (see figure 10 page 26). I stayed well within the timeframe and collaborated with stakeholders fluently. Implementing the framework and process does not require additional resources from the case organization so this cost effectiveness is good. The effectiveness can be viewed differently for example, getting quantitatively many results or qualitatively good results. In this case effectiveness could be for example, cost effectiveness compared to resources required and results in identifying and treatment of risks to protect value.

Expansive learning cycle (Figure 2 page 7) continues with finalizing the process, evaluating and implementing it in steps 3-5. Next steps that are visualized in Figure 16 locate these steps that are also visualized in ISO 31000 Framework Figure 6 page 10. ISO 31000 requires monitoring of the effectiveness of the process and next steps are implementing and evaluating the process and then continuing improving it. The effectiveness of the process can be monitored continuously and evaluated periodically for example, between set reporting intervals.

The case organization should reflect their possibilities and attitude towards risk, the company strategy, and relevant stakeholders like the governing Ministry when setting the risk criteria. Tools and techniques are offered for example, by VAHTI. However, the project management tool used by the case organization is under improvement so setting on for example, reporting principles is not yet ideal. Risk criteria and used techniques should be established and reporting principles may then be linked to these.

8 References

Printed sources

Brown, E & Chong, Y. 2000. Managing Project Risk – Business Risk Management for Project Leaders. Financial Times: Prentice Hall

Bryman, A. 2008. Social Research Methods – 3rd edition. Oxford

Dalcher, D & Harris, E. 2009. Strategic Project Risk Appraisal and Management. Gower

Engerström, Y. 2004. Ekspansiivinen oppiminen ja yhteiskehittely työssä. Vastapaino

Hopkin, P. 2017. Fundamentals of Risk Management – 4th edition. Kogan Page Limited

ISO31000:2018 Risk Management - Guidelines

ISO27500:2012 Guidance on Project Management

Kwak Y & Stoddard, J. 2004. Project risk management – lessons learned from software development environment. Technovation 24

Lock, D. 2013. Project Management – 10th edition. Gower

Moeller, R. 2011. COSO ENTERPRISE RISK MANAGEMENT – Establishing Effective Governance, Risk, and Compliance Process - 2nd edition. John Wiley & Sons, Inc. New Jersey

Oliver, P. 2012. Succeeding with your literature review: A handbook for students. Open University Press: 1st edition

Project Management Institute. 2000. A Guide to the Project Management Body of Knowledge – 3rd edition. Project Management Institute

Vahti 1/2017 Ohje Riskienhallintaan. Valtiovarainministeriö

Electronic sources

American Society for Quality – What is the Plan-Do-Check-Act Cycle? ACCESSED 7.2.2019

https://asq.org/quality-resources/pdca-cycle

Association for Qualitative Research. ACCESSED 2.1.2019

https://www.aqr.org.uk/glossary/brainstorming

Bowen, G. 2009. Document analysis as qualitative research method. ACCESSED 26.1.2019

https://www.academia.edu/8434566/Document_Analysis_as_a_Qualitative_Research_Method

COSO Enterprise risk management: Integrating with strategy and performance – Executive summary 2017. ACCESSED 7.2.2019

https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Financial Executives International - COSO: From Cube to Helix, What Does This Mean for Organizations? ACCESSED 7.2.2019

https://www.financialexecutives.org/Influence/Committees/Governance,-Risk-Compliance/News/COSO-From-Cube-to-Helix,-What-Does-This-Mean-For.aspx

Murray, J. 2011. Cloud Network Architecture and ICT ACCESSED 4.2.2019

https://itknowledgeexchange.techtarget.com/modern-network-architecture/cloud-network-architecture-and-ict/

Committee of Sponsoring Organizations of the Tradeway Commission. 2004. Enterprise Risk Management – Integrated Framework; Executive summary. ACCESSED 30.1.2019

https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Gurel, E. 2017. SWOT Analysis; A Theoretical Review. ACCESSED 6.2.2019

https://www.researchgate.net/publication/319367788_SWOT_ANALYSIS_A_THEORETICAL_REVIEW

International Organization for Standardization: ISO 31000. ACCESSED 30.1.2019

https://www.iso.org/iso-31000-risk-management.html

Merriam-Webster -dictionary ACCESSED 2.1.2019

https://www.merriam-webster.com/dictionary/application

The Ministry of Finance – Risk Management Policy ACCESSED 31.1.2019

https://vm.fi/riskienhallinta/riskienhallintapolitiikka

PROTIVIV – Updated COSO ERM Framework ACCESSED 6.2.2019

https://www.protiviti.com/US-en/insights/bulletin-vol-6-issue-2

Unpublished sources

Internal documents of the case organization

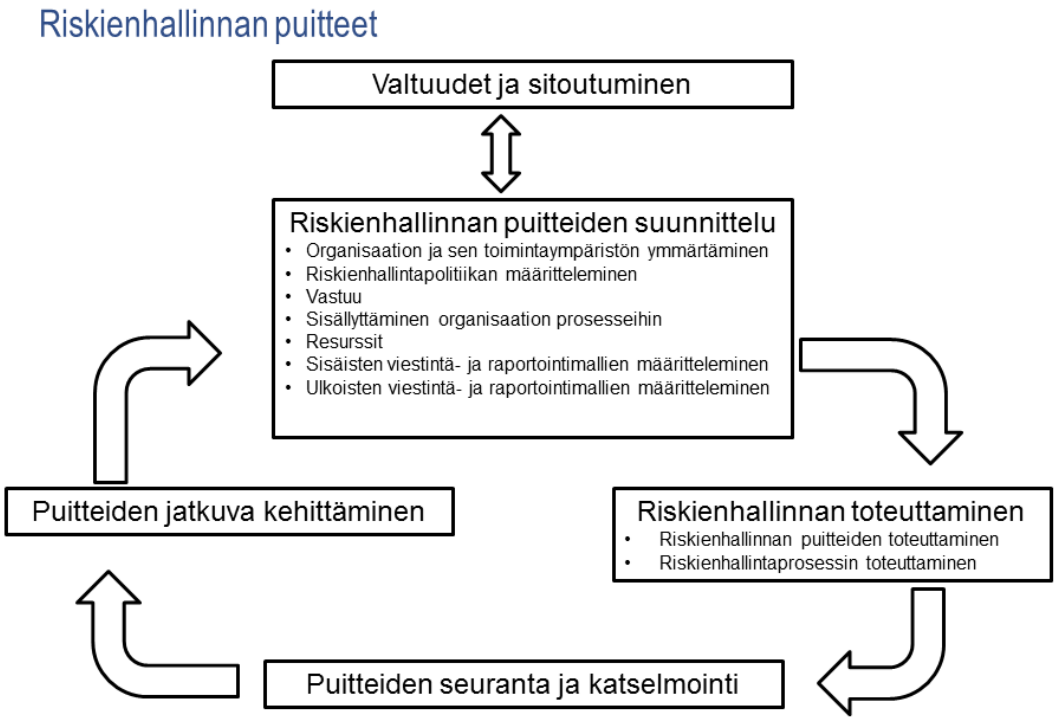
- Intranet 2019

- Hankesalkku 2019
- Risk Management Policy 2018
- Projektien määrityslista 2017
- Projektiroolit 2017
- Hankesalkun käyttöohje 2017

9 Figures

10 Appendices

Appendix 1: Finnish government risk management framework



ISO 31000, riskienhallinnan puitteet, SFS:n luvalla

Appendix 2: Finnish government risk management glossary

LIITE 2 KÄSITTEIDEN MÄÄRITELMÄT

[Seuraavassa hakemistossa on riskienhallinnan keskeisimpiä käsitteitä määrittelyineen. [Virasto voi valita itselleen olennaisimmat ja täydentää tarvittaessa.]

Jäännösriski	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
Riski	Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun vaikutukseen verrattuna.
Riskianalyysi	Prosessi, jolla pyritään ymmärtämään riskin luonne ja määrittämään riskitaso. Riskianalyysi on riskin merkityksen arvioinnin ja riskin käsittelyä koskevien päätösten perusta. Riskianalyysi sisältää riskin suuruuden arvioinnin.
Riskien arviointi	Kokonaisprosessi, joka kattaa riskien tunnistamisen riskianalyysin ja riskin merkityksen arvioinnin
Riskien käsittely	Riskin muokkaamisprosessi, jossa päätetään erimerkiksi seuraavista toimenpiteistä: - riskin torjuminen tai poistaminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa - riskin ottaminen tai lisääminen jonkin mahdollisuuden saavuttamiseksi - riskin lähteen tai syyn poistaminen - todennäköisyyden muuttaminen tai todennäköisyyteen vaikuttaminen - seurausten muuttaminen tai vaikutuksiin varautuminen - riskin jakaminen toisen osapuolen tai osapuolten kanssa - riskin säilyttäminen ja sietäminen tietoon perustuvalla päätöksellä
Riskien tunnistaminen	Riskien havaitsemisen ja kuvaamisen prosessi
Riskienhallinta	Koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta.
Riskienhallintapolitiikka	Organisaation päättämät ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet.
Riskienhallintaprosessi	Hallintaperiaatteiden, -menettelyjen ja -käytäntöjen järjestelmällinen soveltaminen toimintaympäristön määrittelemiseen, riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan sekä viestintään ja tiedonvaihtoon.
Riskienkäsittelysuunnitelma	Johdon hyväksymä dokumentoitu riskien käsittelyn vastuutettu toimenpidesuunnitelma
Riskikriteerit	Säännöt, joiden perusteella riskin merkittävyys arvioidaan yhdenmukaisesti. Riskikriteerit perustuvat organisaation tavoitteisiin ja sen toimintaympäristöön. Riskikriteerit voivat olla johdettu standardeista, laeista, toimintaperiaatteista ja muista vaatimuksista.
Riskiluokitus	Arvioitavan kohteen luokittelun apuväline.
Riskimatriisi	Riskimatriisin avulla luokitellaan riskin suuruus tapahtuman seurausten vakavuuden ja esiintymisen todennäköisyyden perusteella. Matriisi auttaa hahmottamaan riskin merkittävyyttä ja miten riski sijoittuu suhteessa toisiin riskeihin.
Riskin hallintakeino	Riskiä muuttava toimenpide. Hallintakeinoja ovat kaikki riskiä muuttavat prosessit, toimintaperiaatteet, laitteet, käytännöt tai muut toimenpiteet. Hallintakeinoilla ei aina välttämättä ole haluttua tai oletettua muutosvaikutusta.
Riskin merkityksen arviointi	Prosessi, jossa riskianalyysin tuloksia riskikriteereihin vertaamalla määritetään, onko riski tai sen suuruus hyväksyttävä tai siedettävä. Riskin