jamk.fi

Assessing maturity of disaster recovery planning

Case study

Mika Ylikangas

Master's thesis
May 2017
Technology
Degree programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Ylikangas, Mika	Master's thesis	May 2017
		Language of publication: English
	Number of pages: 67	Permission for web publication: yes

Title of publication

Assessing maturity of disaster recovery planning

A case study

Degree programme

Degree programme in Information Technology, Cyber Security

Supervisor(s)

Karjalainen, Mika

Assigned by

Kansaneläkelaitos

Abstract

The idea for this study came from an interest to research disaster recovery planning as a process and how the maturity of the planning process can be measured. Maturity of a process can be described in terms of predictability and risk. The more mature the process, the more predictable it is, and the more manageable are the risks.

The research tasks were to choose the approach for the thesis, perform a literature review, choose appropriate framework for assessing maturity and conduct a study on maturity of Kansaneläkelaitos disaster recovery planning process.

The implementation method was based on a qualitative approach. Qualitative research aims to provide a deeper understanding of phenomena under study. Case study tradition was chosen as conceptual framework for researching maturity of Kansaneläkelaitos disaster recovery planning.

Two suitable frameworks were studied; one for general process maturity assessment and one for assessment of contingency planning maturity which was chosen as a framework from which the research was implemented. The research consisted of a self-assessment survey sent to the chosen Kansaneläkelaitos employees whose responsibilities are related to disaster recovery planning and a semi-structure interview of coordinator of IT security in Kansaneläkelaitos.

Results for the case study are declared to be confidential on the grounds of protecting security arrangements and preparation for emergency conditions. In a general level, the framework appeared understandable for the audience and the distribution of survey responses was relatively low in each survey category.

Keywords/tags (subjects)

Disaster recovery plan, continuity plan, cyber security

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Ylikangas, Mika	Opinnäytetyö, ylempi AMK	toukokuu 2017
	Sivumäärä 67	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: kyllä

Työn nimi

Assessing maturity of disaster recovery planning

A case study

Tutkinto-ohjelma

Degree programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Karjalainen Mika

Toimeksiantaja(t)

Kansaneläkelaitos

Tiivistelmä

Tutkimusaihe syntyi kiinnostuksesta toipumissuunnitteluun prosessina sekä siihen, kuinka suunnitteluprosessin kypsyyttä voidaan mitata. Prosessin kypsyys voidaan ymmärtää ennakoituvuuden ja riskin kautta. Mitä kypsempi prosessi, sitä ennustettavampi se on, ja sitä hallittavampia ovat riskit.

Tutkimustehtävinä olivat lähestymistavan valinta, kirjallisuuskatsauksen tekeminen, sopivan kypsyystason arviointimallin löytäminen ja case-tutkimuksen tekeminen Kansaneläkelaitoksen toipumissuunnittelun kypsyystasosta.

Tutkimuksen toteuttamistavaksi valittiin laadullinen lähestymistapa. Laadullinen tutkimus tähtää syvemmän ymmärryksen hankkimiseen tutkittavasta ilmiöstä. Case-tutkimusperinne valittiin malliksi millä Kansaneläkelaitoksen toipumissuunnittelun kypsyyttä tutkitaan.

Kahta sopivaa arviointimallia tutkittiin; ensimmäinen on yleinen prosessien kypsyystason arviointiin käytetty malli ja toinen nimenomaan jatkuvuussuunnittelun arvioimiseen käytetty malli, joka myös valittiin käytettäväksi tutkimuksessa. Tutkimus sisälsi itsearviointikysymyspatteriston, joka lähetettiin Kansaneläkelaitoksessa jatkuvuussuunnittelun kanssa tekemisissä oleville. Lisäksi tutkimus sisälsi puoli-strukturoidun Kansaneläkelaitoksen IT-tietoturvallisuuden koordinaattorin haastattelun.

Case-tutkimuksen tulokset ovat luottamuksellisia, koska ne liittyvät turvallisuusjärjestelyihin ja valmistautumiseen poikkeusolosuhteisiin. Yleisellä tasolla valittu arviointimalli vaikutti tutkittavista ymmärrettävillä ja vastausten hajonta oli suhteellisen pieni jokaisessa kategoriassa.

Avainsanat (asiasanat)

Toipumissuunnittelu, jatkuvuussuunnittelu, kyberturvallisuus

Muut tiedot

Contents

Figures

Tables

1 Introduction

The purpose of this thesis was to find a method or a framework to measure the maturity of the disaster recovery planning process. The aim of the maturity evaluation is to improve process quality. The maturity can be defined in terms of predictability and risk. The more mature the process, the more predictable it is, and the more manageable are the risks. The motivation for this thesis comes from the working life and the perspective of the thesis will be practical. A case study is conducted on the findings of this research.

1.1 Background

Disaster recovery plans aim to restore IT operations back online after serious disruptions. Disaster recovery planning is considered a part of the concept of cyber security (National Institute of Standards and Technology, 2014). At first glance, it might be surprising to see disaster recovery planning included into cyber security; however, in fact it is an essential part of cyber security providing the final assurances that even in the case of disruption, IT operations can be restored into working order.

The idea for the thesis subject, disaster recovery planning, came when the author was writing a disaster recovery plan for the system he was responsible for in his job in the Social Insurance Institute of Finland (Kansaneläkelaitos). For the writer, personally, coming from the technical background, the area of process development and improvement was not familiar and the experience to develop a disaster recovery plan was very enlightening in a sense that he realized process development, along with technical excellence, is indeed vital for ICT organization performance.

1.2 About the problem of disaster recovery planning

The disaster recovery planning as a concept can be easily confused with business continuity planning. There are also several concepts linked to disaster recovery and business continuity such as risk management. Also, the scope of disaster recovery covers all levels of organization starting from the higher management to the technical people responsible for implementing the disaster recovery plans. Each level

of an organization has its own perspective and language which might make the disaster recovery planning difficult without organized approach.

When discussing the possibility for writing a master's thesis for the subject with the employer, it was noticed that there is a mutual need for research in the area of maturity of disaster recovery planning. For Kansaneläkelaitos, the need was to gain introspection and understanding about the actual planning process related to the disaster recovery plans. A case study was therefore conducted for the maturity of disaster recovery planning in the ICT department of Kansaneläkelaitos

1.3 How this thesis is organized

This thesis comprises eight chapters. After this chapter, the research methodology, ethical and confidentiality issues related into this thesis are explored. In the disaster recovery planning chapter, the concepts and terminology of disaster recovery planning are discussed. In assessing disaster recovery planning chapter, ways to measure the maturity of disaster recovery planning are investigated. In the organization chapter, the Kansaneläkelaitos ICT environment is presented. In the case study chapter, the structure of the case study to be implemented is planned. In the final chapters the results and the findings are discussed. The case study data is included in the appendix of this thesis. The glossary in the appendix contains the essential terms and definitions.

2 Research methodology

Eriksson and Kovalainen (2014) state that formulating appropriate research questions is an integral part of the design of a research.

2.1 Research problem

In this thesis, the broad research problem is how to measure the maturity of the ICT disaster recovery planning. This by itself can be considered a problem too wide and elusive to be studied. The scope and width of the research need to be limited by dividing the research problem into following research tasks:

1. Make a literature survey to find out methods to measure the maturity of the ICT disaster recovery planning
2. Analyze these methods for contexts they are usable and find out the most suitable method for Kansaneläkelaitos
3. Make a practical case study to measure the maturity of the ICT disaster recovery planning in the ICT department at Kansaneläkelaitos

This division into question enables to divide the study into manageable parts each having their own role and contribution to the whole thesis.

2.2 Measuring maturity of ICT disaster recovery planning

There are several maturity evaluation frameworks in software industry, for example the Capability Maturity Model CMM (Paulk, 1995). The purpose of these frameworks is to improve the quality of products and improve predictability of the schedule and the outcome of the processes. Generic frameworks developed for different purposes might be used to evaluate the maturity of the ICT disaster recovery planning. This study strives to find out if there are specially tailored frameworks for ICT disaster recovery planning or only generic frameworks for this purpose, and to make an informed choice of a framework suitable for ICT disaster recovery planning in the ICT department at Kansaneläkelaitos.

2.3 Research approach and research methods

The research methodology consists of a literature review about the subject and a case study in which the findings made from the literature survey are applied to the case study, which enables to gain a deeper understanding in what kind of issues arise when measuring the maturity of the ICT disaster recovery planning. The case study was conducted on the disaster recovery planning process of Kansaneläkelaitos ICT production services.

2.3.1 Literary review

The literature review is performed about ICT disaster recovery planning and if the need arises, it is expanded into areas of ICT continuity management and ICT risk management. Kansaneläkelaitos expressed some wishes about the literature to be researched. The primary effort of literature research is on scientific literature;

however, also a commercial offer about the subject is studied. Such are, for example, whitepapers published by a consulting companies.

Eriksson and Kovalainen (2014) state that a good literature review

- Deals with the research relevant to the research questions
- Is organized around the research questions
- Provides summary, interpretation, evaluation and criticism of the literature
- Identifies areas of controversy and disagreement in the literature
- Helps formulating or refining the research questions

In this case, a literature review on case study methodology, disaster recovery planning, assessing maturity of processes and Kansaneläkelaitos is performed. In disaster recovery planning, the definitions related to the concept of disaster recovery planning are explored. In assessing maturity of processes, the frameworks used for evaluating maturity of processes such as disaster recovery planning are discussed. In Kansaneläkelaitos, the situation and environment of Kansaneläkelaitos are studied.

2.3.2 Case study

When studying deeper the research problem and research questions, the choice for research methodology came obvious. The research problem and research questions implicated a need for understanding the phenomena around ICT disaster recovery planning. Qualitative research approaches are concerned with interpretation and understanding (Eriksson and Kovalainen, 2014). On the other hand, quantitative approaches are concerned with explanation, testing hypothesis and statistical analysis (Eriksson and Kovalainen, 2014). In the author's opinion, the ICT disaster recovery planning practices in Kansaneläkelaitos are still evolving and a quantitative research approach is not possible in a situation with a great deal of variance in the process. On the other hand, there is a definite need to understand the phenomena more deeply to improve it.

In this thesis, a case study method was used for understanding the theories found in the literature review. The case study was conducted on experiences gained from ICT recovery planning in Kansaneläkelaitos ICT department.

Yin (2014) defines a case study as an empirical inquiry that

- investigates a contemporary phenomenon within its real-life context, when

- the boundaries between the phenomenon and the context are not clear and in which
- multiple sources of evidence are used.

In the author's opinion, the case study provides a possibility to examine and interpret the findings of literature review in a real-world context. Also, Kansaneläkelaitos as an organization was interested in finding out how its ICT disaster recovery planning processes measured against public frameworks used to measure process maturity.

In this case study, only one organization was studied. This type of arrangement is called an intensive case study (Eriksson and Kovalainen, 2014). The main aim of the intensive case study is to research the inner workings of the case itself and not to generalize findings into theory (Stake, 1995, Stake in Denzin, 2005). This is not to be confused with a situation where the findings of the case study are interpreted against a theoretical framework as is the case here.

2.4 Collecting data

The data in the case study will be collected mainly from an interview and a survey.

2.4.1 Interview on disaster recovery planning in Kansaneläkelaitos

The first interview was conducted to get a perspective on how disaster recovery planning is implemented in Kansaneläkelaitos compared to the processes presented in the literature. This interview was carried out with the person responsible for ICT information security office lead in Kansaneläkelaitos. The interview was conducted in a semi-structure manner, i.e. meaning that there is a rough outline of topics handled in the interview. The results of the interview were recorded and a transcript was written.

2.4.2 Self-assesment of disaster recovery planning in Kansaneläkelaitos

The survey was sent to the selected people presenting different levels of organization and different part of specialties related to disaster recovery planning. The purpose of the interview was to understand what the organization perceives as the maturity of disaster recovery planning. This interview was conducted in a highly-structured manner meaning that the same questions are presented to each

interviewee and there are no follow-up questions. The interview questions were formulated from the processes found in the literature review. The interviewees could present their own reflections on the questions but the questions and the choices presented were to be fixed. This survey was implemented as an email survey.

This approach using interviews from different levels of organization offers a possibility to cross check, or triangulate the data collected from the phenomenon from different perspectives. Having multiple sources of data produces a more accurate and diverse view into the subject (Eriksson, Kovalainen, 2014).

2.5 Confidentiality issues regarding case study and results

Some of the data collected were declared to be confidential on the grounds of:

- Information relating to or affecting the realization of the security arrangements of persons, buildings, installations, constructions, and data and communications systems (Act on the Openness of Government Activities 24§,7)
- Information concerning preparations for accidents and emergency conditions, civil defense or its development (Act on the Openness of Government Activities 24§,8)

The thesis author, Kansaneläkelaitos and the JAMK University of Applied Sciences have signed an agreement about the confidentiality of results of the case study. This fact influences also the structure of the thesis. According to JAMK rules, only appendices of thesis can be declared confidential. For this reason, the contents of the case study and the interpretation and the analysis of the results are located in the appendix of the thesis. There is only general discussion in the thesis itself how the findings fit into the theory.

2.6 Ethical perspective

There are several factors related to ethics which need to be examined in this paragraph. Perhaps the most obvious is the role of the researcher in the research. Elliot (1998) mentions at least three different categories related to the researcher role in the activities under research:

- Researcher is neutral and detached from the research subject
- Researcher is a marginally involved participant (participant-observer) in subject to be researched

- Researcher is an active participant and enables changes in the subject to be researched.

The author of this thesis has participated in ICT disaster recovery planning in Kansaneläkelaitos. The level of involvement is, in his opinion, marginal as Elliot (1998) states the participant-observer to be. Eriksson and Kovalainen (2014) state that a neutral and detached role has only contractual obligations to the subject of research. They also indicate that higher involvement brings more problematic issues to be considered.

The author's obligations to Kansaneläkelaitos in the context of this thesis are contractual ones. The author has agreed on writing this thesis under relatively broad scope of measuring maturity of ICT disaster recovery planning. There is also confidentiality agreed since some of the research material is considered confidential material.

Along with the contractual obligations, Schwandt (2007) mentions the extended and complex dealings between the researcher and the researched. In this case the most important aspect is the trusting relationship which should not be violated during the research. In the author's opinion, there is a danger when analyzing and reporting results of the case study research. The number of interviewees is so small and their positions in the organization are such that each person is recognized relatively easily even in the condition of anonymity. Along with this fact, there is a possibility that in some circumstances, the answers of the interview might offend the other participants. This could be in a situation where, for example, there is a contradicting view about some issues in the research.

The author has tried to mitigate these risks by telling the interviewees before the interviews that there is a possibility of a situation where conflicting views are reported in the analysis of the case study. Also, interviewees should be told that even in the condition of anonymity persons could be identified from their responses.

2.7 Analysis of the results

In business research, personal interviews are typically used as the primary data for the research and other types of data are used as a complementary (Eriksson and

Kovalainen, 2014). There are two main strategies for analysis (Yin, 2014). The first is based on pre-formulated theoretical propositions as is in our case study. The second is based on the more direct analysis of the research material. According to Eriksson and Kovalainen, 2014, several researchers are in favor of the second strategy. However, in this case study the objective is to formulate the interview questions against a pre-formulated theoretical proposition since the author's intention is to measure how mature the ICT recovery planning is examined against the selected framework.

Yin (2014) distinguishes several analytic techniques usable in case study research in general. In this case, the most obvious of these is the pattern matching, which means finding patters from the empirical data and comparing them with the theoretical propositions. This is exactly what this thesis aims to do.

Eriksson and Kovalainen (2014) discuss several possible forms of reporting available with case study research. The classical way would be using narrative form, i.e. the report forms a story of sorts with the research question and the story includes a plot and possibly a dialogue. In the author's opinion, this is not a very suitable way of reporting in this case study. From literature review, finding a strong theoretical framework is an expected result ~~from~~ which can be used, and the empirical data collected in the case study does not contain any personable data in a sense that some sort of story could be created.

On the other hand, there are also other kinds of forms of reporting available for this thesis such as three different paths summarized by Stake (1995) and Stake in Denzin (2005). One of them is a simple one-by-one description of the several major components of the case study. In the author's opinion, this is a far more suitable form of reporting in the setting of this case study.

A final note in this chapter is the question of the audience. As stated before, there are confidentiality requirements for the data collected and the contents of their analysis and reporting. The main audience of this thesis is the academic audience. The main body of the thesis is targeted for academic audiences reviewing the thesis. Nevertheless, also a very important audience are the employees in Kansaneläkelaitos interested in ICT disaster recovery planning. The results of the case study will be

used for guiding the ICT disaster recovery roadmap. Therefore, the appendix containing the case study and the detailed analysis is targeted mainly at the audience in Kansaneläkelaitos, not forgetting the academic requirements of the thesis.

3 Disaster recovery planning

In this chapter, different terms and definitions related to the disaster recovery plans are discussed as well as the planning process related to the disaster recovery plans, or contingency plans as it is defined later. Last, the terminology and the planning process are discussed.

3.1 Disaster recovery plan and business continuity plan

The disaster recovery plan (DRP) is defined by U.S. National Institute of Standards and Technology (Swanson et al., 2010) as follows:

"*The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP (Business Continuity) or COOP (Continuity of Operations) plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.*"

In the opinion of the author, it is important to notice that a disaster recovery plan concentrates only at restoring IT assets back online. The definition above does not contain any activities directed outside the provider of the IT services, e.g. the business units or customers utilizing the IT services. As stated in the definition, disaster recovery plan may support business continuity plan which concentrates on the whole business, not just the IT services which may be used to provide business services.

Business continuity plan (BCP) is defined by U.S. National Institute of Standards and Technology (Swanson et al., 2010) as follows:

"*The BCP focuses on sustaining an organization's mission/business processes during and after a disruption. An example of a mission/business process may be an organization's payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.*"

In the author's opinion, it is important to notice that disaster recovery plan and business continuity plan may or may not have a relation with each other. When business processes use IT services to provide service, coordination between business continuity plan and disaster recovery plan may be necessary.

There is also a third term used in the definitions above, a continuity of operations (COOP) plan which U.S. National Institute of Standards and Technology (Swanson et al., 2010) defines as follows:

"*COOP focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.*"

Continuity of operations (COOP) plan was important to define because it was an essential part of earlier definitions, however, it is not discussed further in this thesis because the literature used as main reference does not discuss this type of plans within the context of the thesis (Tipton and Krause, 2007).

In addition to these terms defined earlier, U.S. National Institute of Standards and Technology (Swanson et al., 2010) refers to all these plans as contingency plans.

3.2 Contingency planning process

According to U.S. National Institute of Standards and Technology (Swanson et al., 2010) contingency planning process is defined as follows:

1. Develop the contingency planning policy
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

Following table (Figure 1) illustrates the different phases of the process (Swanson et al., 2010)

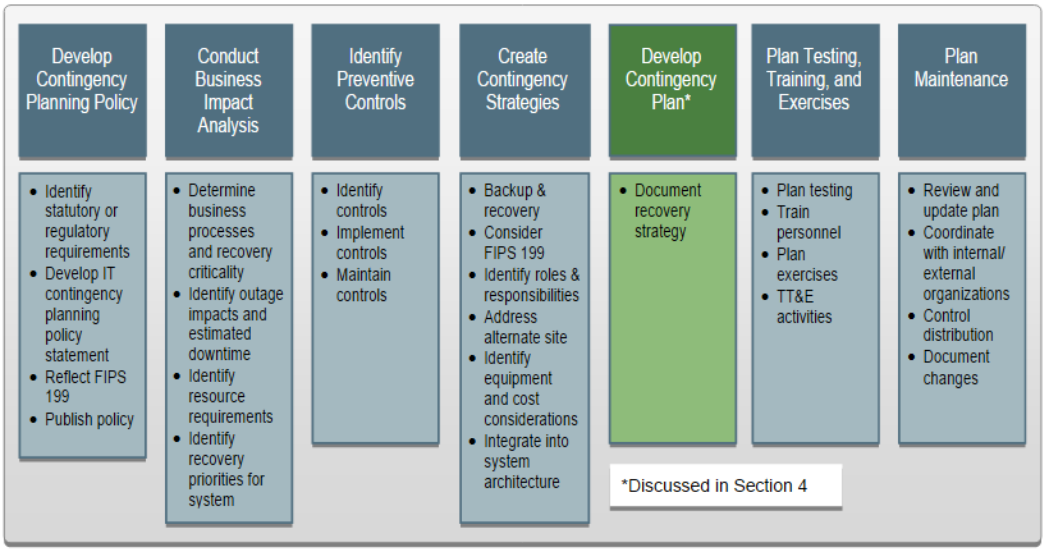


Figure 1. Contingency planning process, U.S. National Institute of Standards and Technology (Swanson et al., 2010)

In the following phases are discussed more in detail (Swanson et al., 2010).

Contingency planning policy

Contingency planning policy statement is the declaration of will by the senior management to implement contingency planning. A part of planning the policy includes the identification of regulatory requirements.

Business impact analysis

Business processes need to be evaluated in terms of criticality and possible downtime impact. Also, dependencies to other business processes and functions

need to be identified to plan for the whole chain of dependencies to reach comprehensive analysis. The business impact analysis is considered to be an essential step in contingency planning process.

Identify preventive controls

There are techniques and processes for reducing the probability and impact of the systems disruption. These controls need to be evaluated in terms of feasibility and criticality of the business process under scrutiny.

Contingency strategies

Strategy can be considered as higher conceptual level planning such as taking recovery issues into consideration in enterprise architecture, technical architecture, maintaining alternate site etc.

Develop contingency plan

This is the actual contingency plan for the system.

Training, testing

To evaluate the contingency plan's fitness for the purpose, it needs to be tested and training needs to be provided so that when the contingency plan is implemented, it will be executed smoothly.

Plan maintenance

The plan must be maintained and reviewed periodically to be effective.

3.3 Conclusions

There appears to be many different terms related to the concept of disaster recovery planning. National Institute of Standards and Technology (Swanson et al., 2010) refers to these terms collectively as contingency planning. Disaster recovery planning refers to the activity planned and performed by the IT function of the organization, and business continuity planning refers to the activity planned and performed by the business departments of the organization.

The planning process appears to be the same in both types of planning. In this thesis, the focus is on the disaster recovery planning and other areas such as business continuity planning are visited only if there is a need to support the focus of the thesis.

The planning process emphasizes participation of all levels of management and continuous improvement. The process provided by the National Institute of Standards and Technology (Swanson et al., 2010) does not seem to be very clear about what steps of the process should be iterated periodically, however, in the author's opinion all these steps are important to be reviewed after some time. The contingency planning policy could perhaps be reviewed less often; however, starting from business impact analysis, reviews should be made in a periodical manner.

4 Assessing maturity of disaster recovery planning

In this chapter, methodologies used to measure the maturity of disaster recovery planning are discussed in more detail. As noticed in the earlier chapter, an important part of the planning process is continuous improvement. In practice, this means that the disaster recovery or contingency plans are reviewed and refined periodically. An important part of this is the awareness of the state of the planning process itself.

First, an introduction on perhaps the best-known maturity evaluation framework (Persse, 2001) the Capability Management Model (CMM) provided by Paulk (1995) is introduced followed by a review of the maturity evaluation framework developed for the contingency planning (Tipton and Krause, 2007). Last, the commonalities and differences of these frameworks are discussed.

4.1 Capability Management Model (CMM)

The Capability Management Model (CMM) was originally started by Humphrey Watts in 1989 (Humphrey, 1989) and continued by Mark Paulk in 1995 (Paulk, 1995).

The main reason for igniting the development of CMM was the quality problems in the software industry said to be developed into a chronic crisis. The main purpose of the CMM was and is to improve by increasing the predictability and reducing the risk.

The definition of mature means an environment where the predictability is high and the risk is low (Persse, 2001).

The CMM contains five levels of maturity which can be considered as ladders. Each ladder consists of the capabilities of the lower ladders. At the lowest ladder, the predictability is low and the risks can be considered high. The following figure illustrates the ladders.

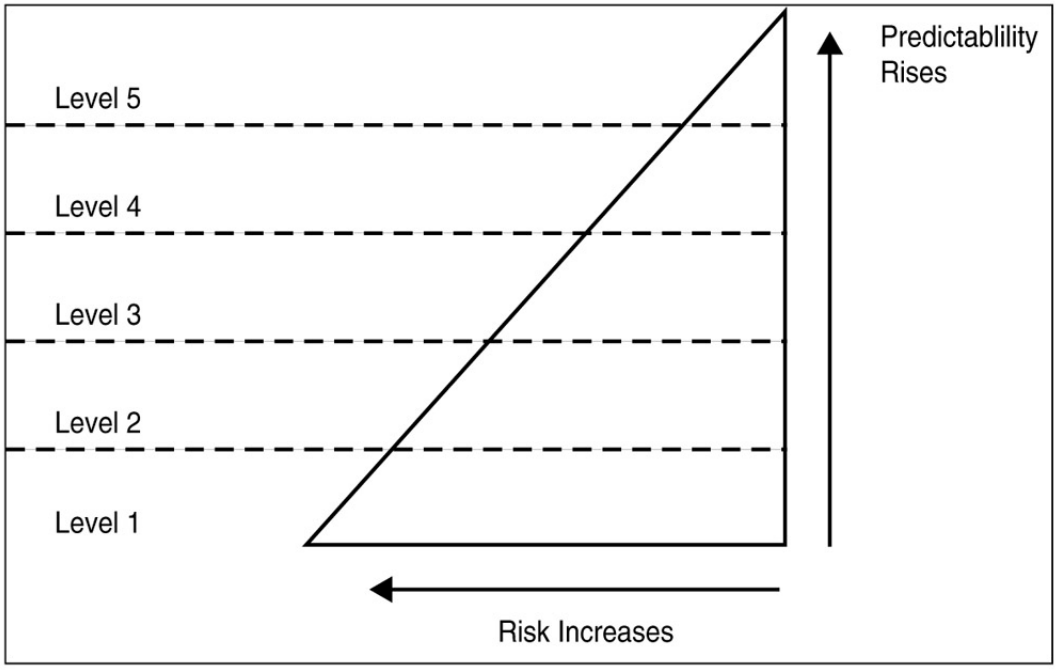


Figure 2. The levels of maturity (Persse, 2001)

Progressing each ladder is defined by the concept of Key Process Area which is examined more in detail in the following sections.

4.1.1 Initial level (1)

Initial level is where every organization initially starts. The main characteristic for the initial level is low predictability. There are no processes defined, or there are processes; however, they are not put into practice. The success or failure at this level is mainly contributed to individuals and their experience. There is little learning taking place at the initial level (Persse, 2001).

4.1.2 Repeatable level (2)

The repeatable level is the beginning of formalization of the processes. At repeatable level, the emphasis is put on standardizing the planning and management of individual projects. The organization has ability to learn from the experiences because of the formalization (Persse, 2001). This level can be considered as project centric level. Key process areas for the repeatable level are (Persse, 2001):

- Requirements management
- Software project planning
- Software project tracking and oversight
- Software quality assurance
- Software configuration management
- Subcontractor management

4.1.3 Defined level (3)

Where repeatable level could be considered as project centric level, defined level encompasses the whole organization. The main characteristic for the defined level is standardization and consistency. At the defined level, two new functions appear in the organization. First is the training function, where management and staff are provided training to the processes and practices to achieve standardization. The second function is the process development function responsible for developing and improving the process development (Persse, 2001). The key process areas for this level are (Persse, 2001):

- Organizational process focus
- Organizational process definition
- Process training program
- Integrated software management
- Software product engineering
- Intergroup coordination
- Peer reviews

4.1.4 Managed level (4)

The main characteristic for the managed level is process measurement. The organization follows the throughput of the processes across all the projects. This is done for the reason for gaining data for the process improvement. This level is the first level which can be considered to have a quantitative approach for the processes.

The outcomes of the processes are predictable (Persse, 2001). The key process areas for this level are (Persse, 2001):

- Quantitative process management
- Software quality management

4.1.5 Optimized level (5)

The optimized level can be considered as the final level where there is no progression to the upper level. The process for the optimized level is ongoing and maintained. The prevention of defects is the main emphasis at this level. However, it is important to notice that the organization does not stop its efforts for process improvement here but the all the needed tools are in place to continuously improve the processes (Persse, 2001). The key process areas for this level are (Persse, 2001):

- Defect prevention
- Technology change management
- Process change management

4.1.6 Conclusions

The CMM is the best-known maturity performance evaluation framework. The maturity can be defined in terms of predictability and risk in processes where mature environments have achieved high predictability and low risk processes. The CMM contains five ladders of different levels of maturity each described by different characteristics where the optimized level is the highest.

In the author's opinion, the optimized level is not automatically worth reaching due to the cost factors involved. In his experience, more these kinds of controls are introduced into the process, the more the costlier the process will be in terms of labor and possibly money. This view is also supported by Tipton and Krause (2007).

Further, the tasks of improving the predictability and lowering the risks concern only to processes inside the organization. If the environment around the organization is turbulent, then the possible gains from the process improvement using CMM can be weakened.

4.2 Maturity assessment framework for contingency planning

Another maturity assessment framework is provided by Tipton and Krause (2007). The framework covers the maturity of both the business continuity and disaster recovery planning. The framework draws from the terminology defined by National Institute of Standards and Technology (Swanson et al., 2010). Tipton and Krause (2007) define disaster recovery planning and business continuity planning as follows:

Disaster recovery planning is a process identifying all the activities by relevant personnel to respond to a disaster and recover IT infrastructure to normal levels.

Business continuity planning is a process identifying all activities to enable organization or business are to continue business at and during the time of disaster.

Tipton and Krause (2007) continue that business continuity plans should by synchronized with disaster recovery plans with the idea of business continuity plans being an extension of disaster recovery plans.

The process including both disaster recovery planning and business continuity planning is called contingency planning. Tipton and Krause (2007) present a process originally from the Disaster Recovery Institute International (DRII) for contingency planning as follows:

1. Perform business impact analysis meaning the analysis of critical business functions. Impact of the outage, dependencies, equipment with time-to-recover-requirements.
2. Perform risk assessment with including preventive actions to reduce the probability and impact of potential incidents
3. Identify recovery strategies by developing risk scenarios and map potential strategies from recovery to the normal operation
4. Select recovery strategy based on perceived threats with time-to-recover requirements.
5. Develop contingency plans including both disaster recovery plans and business continuity plans.
6. Train users to perform tasks identified in the contingency plan
7. Maintain the plans either periodically or based IT or business based needs.

4.2.1 Maturity assesment grid

Tipton and Krause (2007) define five stages of maturity for contingency planning. They include uncertainty, awakening, enlightenment, wisdom, and certainty. Along with the stages they define a second dimension containing the five areas which are Management understanding and attitude, Contingency planning organization status,

incident handling, contingency planning economics, and contingency planning improvement.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Figure 3 Maturity assessment grid (Tipton and Krause, 2007)

The stages and their characteristics are described concerning different areas in the following paragraphs.

4.2.2 Uncertainty (Stage 1)

The main characteristic for the lowest stage is the lack of understanding the importance of contingency planning which is understood solely as a paper implementation. Threats are not analyzed or understood, prevention, detection and recovery are not formally addressed. Contingency planning usually consists only of personnel evacuation plans and simple procedures such as backup and restore procedures (Tipton and Krause, 2007).

The characteristics in different areas (Tipton and Krause, 2007):

Management understanding and attitude: Management does not use risk assessment for incident reduction and does not understand the necessity of contingency planning by blaming circumstances which caused the incident.

Contingency planning organization status: There is no organization or function for contingency planning.

Incident handling: Incident handling is reactive rather than proactive. Even a minor incident could be disastrous.

Economics: Minimal or no funds spent on prevention, the loss is unmanaged and unpredictable.

Contingency planning improvement: No organized contingency planning improvement nor risk reduction activities.

4.2.3 Awakening (Stage 2)

The stage awakening is characterized by the realization of that IT disaster recovery planning has some value, and the realization of inability brings out the need to provide resources to support planning. Reliability is viewed as a product which can be bought from a vendor to solve problems. Technical solutions are preferred rather than determining the actual reliability requirements. A contingency planner is appointed, usually from the IT operations. The creation of disaster recovery plan is typically viewed as an endpoint rather than the beginning of a continuous improvement. The initial focus may be on the most dramatic threat while ignoring the more probable and significant threats. Recovery will focus on IT rather than business operations (Tipton and Krause, 2007).

The characteristics in different areas (Tipton and Krause, 2007):

Management understanding and attitude: Relying on technical solutions.

Contingency planning organization status: Contingency planning function may be appointed with main emphasis being coordination of file backup and restores.

Incident handling: Incident handles and basic statistics are gathered on major incidents.

Economics: Preventive actions are minimal; the impact of the incidents is unpredictable.

Contingency planning improvement: Enterprise policies start to emerge for handling most obvious threats.

4.2.4 Enlightenment (Stage 3)

The stage enlightenment is characterized by the fact that the disaster recovery planning is understood to be necessary, and the resource allocation for the planning is more realistic also. Reliability is not something which can be purchased from the vendor. The management endorses recovery planning formally. Corporate

contingency planning policy and corporate emergency response training are developed, the first ideas of contingency planning having a relation to information security function. The first business impact analyses are attempted and relevant disaster scenarios are developed (Tipton and Krause, 2007).

The characteristics in different areas (Tipton and Krause, 2007):

Management understanding and attitude: Management understands that the disaster recovery plans are necessary for maintaining the service levels. Management supports focus on most critical assets and infrastructure.

Contingency planning organization status: The contingency planner reports to IT operations. The organizational relation is a 'dotted line'. The contingency planner develops corporate policy and implements training.

Incident handling: Better statistics providing clearer view to the threats.

Economics: Preventive actions aim to assure the IT service levels.

Contingency planning improvement: End users have confidence for ability to restore systems. End users expect and rely on higher service levels.

4.2.5 Wisdom (Stage 4)

The stage wisdom is characterized by contingency planning reflecting on more business perspective than the perspective of IT operations. The business has focus in this stage. Now management visibly participates in the planning. Business units are encouraged to participate also. Organizationally contingency planning moves under information security function. Threats are re-evaluated continually based on evolving threats. Legal perspective is considered for each type of incident. Analyzing risks are now more accurate. Enterprise wide threat models are used. The contingency planning becomes a routine (Tipton and Krause, 2007).

The characteristics in different areas (Tipton and Krause, 2007):

Management understanding and attitude: Management participates in and understands the contingency planning. Management makes informed decision. Management encourages business units to identify the requirements for their critical business functions.

Contingency planning organization status: The contingency planning transitions into information security function.

Incident handling: Threats are continually assessed based on threat population and security incidents. Legal actions are planned for each type of incident.

Economics: Preventive actions are continuously managed. Periodic risk analysis undertaken. Reduced losses.

Contingency planning improvement: Risks are evaluated accurately. Contingency planning now emphasizes business continuity. Accurate business impact analyses.

4.2.6 Certainty (Stage 5)

The stage certainty is the final stage of the maturity ladder. This stage is characterized by continuous improvement regarding the processes and participation in public and professional forums. Contingency planning is seen as a solid part of information security function. Management fully supports the contingency planning program. Research and development are funded. Top management participates and is aware of contingency planning program. Incident management data is considered in risk management. Prevention strategies are fully developed. Contingency management program may be utilized in marketing. Proactive contingency planning is in place and continuously refined (Tipton and Krause, 2007).

The characteristics in different areas (Tipton and Krause, 2007):

Management understanding and attitude: Management understands contingency planning as being an essential part of internal controls of an enterprise. Adequate resources are provided.

Contingency planning organization status: Information security officer regularly meets with higher management. Process improvement is a concern.

Incident handling: The causes of business interruptions are determined. Incident data is taken into account in the risk management.

Economics: Prevention is justified. The stability becomes recognized. The loss is minimized.

Contingency planning improvement: Business continuity actions are considered as normal. Process improvement often come from the end users.

4.2.7 Progressing through stages of maturity

Tipton and Krause (2007) define criteria for progressing through the stages of maturity. These criteria are divided into areas specified earlier: Management understanding and attitude, Contingency planning organization status, Incident handling, Economics, and Contingency planning improvement.

Management understanding and attitude

To reach stage awakening (2) management will authorize purchase of technical solutions to increase reliability such as backup tools etc. These technical solutions can be both hardware or software based (Tipton and Krause, 2007).

To reach stage enlightenment (3) management will endorse IT disaster recovery policies and supports development of IT disaster recovery plan or plans. Management will also support training for disaster recovery (Tipton and Krause, 2007).

To reach stage wisdom (4) management will shift focus from IT disaster recovery to the identification and recovery of critical business functions. Management will also start a business impact evaluation to have an understanding of the most critical business functions and IT assets. Management will promote business continuity and invite other parts of the organization to participate to contingency planning activities (Tipton and Krause, 2007).

To reach stage certainty (5) management understands business continuity planning as essential. Management will also provide enough resources and support (Tipton and Krause, 2007).

Contingency planning organization status

To reach stage awakening (2) a contingency planner as appointed. Priority is in recovery of IT operations and worst case scenarios (Tipton and Krause, 2007).

To reach stage enlightenment (3) contingency planning will have additional responsibility to the information security function. Disaster recovery plans are based

on more realistic scenarios. Also, corporate communications are included in the planning (Tipton and Krause, 2007).

To reach stage wisdom (4) contingency planning function will be a part of the information security function. The focus will move from disaster recovery to business continuity. Risk assessment and business impact assessments will be updated periodically. Penetration testing and audit functions will have support. Contingency planning function will network with other organization parts such as configuration management, purchasing etc. (Tipton and Krause, 2007).

To reach certainty (5) top management is involved in continuity planning program. Information security function is responsible for business continuity. Research and development is supported. Business continuity becomes a marketing asset for the organization (Tipton and Krause, 2007).

Incident handling

To reach stage awakening (2) data management problems emerge meaning mainly file recovery. Basic statistics are collected. Contingency planning will concentrate on the most dramatic scenarios (Tipton and Krause, 2007).

To reach stage enlightenment (3) initial business impact assessment is done and time-to-recover requirements are mapped. Detailed statistics gathered from incident reporting process can enable better understanding of the threats making it possible to develop more realistic disaster scenarios (Tipton and Krause, 2007).

To reach stage wisdom (4) threats are continually reevaluated based on the continuous risk assessment and data from the security incident reporting (Tipton and Krause, 2007).

To reach stage certainty (5), incident database will be continuously analyzed to improve the contingency planning (Tipton and Krause, 2007).

Economics

To reach stage awakening (2) management will issue only limited resources for contingency planning, mainly for purchasing technical solutions to improve reliability (Tipton and Krause, 2007).

To reach stage enlightenment (3) expenses are managed and are justifiable (Tipton and Krause, 2007).

To reach stage wisdom (4) expenses are managed and continually justified with periodic risk analyses and more accurate business impact analyses. Anticipated losses will be evaluated using cost and benefit evaluation (Tipton and Krause, 2007).

To reach stage certainty (5) cost saving perspective of fully functioning contingency planning program will be understood (Tipton and Krause, 2007).

Contingency planning improvement

To reach stage awakening (2) contingency planner will implement IT operations plan and develops an initial IT disaster recovery plan (Tipton and Krause, 2007).

To reach stage enlightenment (3) contingency planner develops a robust IT disaster recovery plan. Training program will be commenced for persons participating the recovery actions. Management understands the business benefits for the contingency planning and provide funding for planning activities and risk management (Tipton and Krause, 2007).

To reach stage wisdom (4) risks will be accurately assessed and managed. Research will be commenced. Business continuity training program is developed (Tipton and Krause, 2007).

To reach stage certainty (5) contingency planning activities become normal and continuous activities. Contingency planning will receive input from the end users and from the system owners (Tipton and Krause, 2007).

4.2.8 Conclusions

The CMM (Paulk, 1995) and the framework provided by Tipton and Krause (2007) have obvious similarities in terms of the five-level maturity ladder. The framework provided by Tipton and Krause has an additional dimension for different areas to be evaluated. The CMM can be considered more as a generic framework for software related processed where the framework provided by the Tipton and Krause is geared towards measuring contingency planning. The purpose is this thesis is to concentrate on the maturity of the disaster recovery planning. The framework provided by the

Tipton and Krause initially appeared as unsuitable for the maturity assessment disaster recovery planning. However, when studying the framework further, it became obvious that the organizations usually start their contingency planning programs from disaster recovery planning and as the process matures, the focus will shift towards business continuity, therefore making the framework valid choice.

5 About Social Insurance Institute of Finland (Kansaneläkelaitos)

Kansaneläkelaitos, the Social Insurance Institution of Finland, operates under the supervision of Parliament. The mission of Kansaneläkelaitos is to secure the income and promote the health of the entire nation, and to support the capacity of individual citizens to care for themselves. Typical situations in which customers contact Kela include childbirth, study, sickness, unemployment, and retirement (About Kela, 2016).

5.1 Kansaneläkelaitos ICT environment

Currently Kansaneläkelaitos uses mainly traditional mainframe systems to provide their ICT services. However, there is an ongoing transformation from traditional mainframe-based architecture to contemporary Java-based open environment architecture. Along with the systems, there is also a need to examine the methodology in general how to produce these new kinds of systems in modern architecture. Disaster recovery planning is an important part of ensuring that the systems provide maximum uptime and small downtime in case of some disturbance in the ICT environment.

5.2 IBM mainframe architecture

Kansaneläkelaitos has operated IBM mainframes since the 1960s. The operations were mainly batch processing. After some benefit schemes introduced in the 1970s required human judgement, the computing terminals were installed to Kansaneläkelaitos offices across the country. In the 1980s, the ICT production facilities were relocated to Jyväskylä mainly because of continuity and security. For

example, the auxiliary power enabled operations to continue for months during disruptions. There was also a possibility for duplication of computing systems when the secondary datacenter was built. After more new benefit schemes there was a need to digitalize document handling for sharing work across the country, thus enabling cost savings. Around year 2000, the Internet services became available for the public and every benefit was available for the public on the Internet around 2010 (Kelakanava, 2016a).

5.3 Other systems

The SAP system was taken into use in 2007. The SAP replaced the old administrative systems produced in Kansaneläkelaitos. The SAP further automatized the internal administrative tasks at Kansaneläkelaitos (Kelakanava, 2016a).

5.4 National health archive

Kansaneläkelaitos joined the building services for the national health archive (Kanta) in around 2005. Since then, Kanta services have been expanded very quickly and extensively in Kansaneläkelaitos. Kanta services are currently a significant part of the ICT services at Kansaneläkelaitos. The first electronic medical prescriptions were issued in 2010 (Kelakanava, 2016a, 2016b).

5.5 IT service management in Kansaneläkelaitos

Kansaneläkelaitos produces hundreds of ICT services for the public, organization customers and for Kansaneläkelaitos itself. To ensure controlled operations, Kansaneläkelaitos utilizes best practices in IT Services Management (ITSM). Using defined processes ensures methodical and holistic management of ICT services. IT Infrastructure Library (ITIL) has been used as a guide to plan the processes (Kokkinen, 2016).

6 Implemention of case study

As stated in the chapter covering research methodology, a qualitative approach has been used. The study comprises two interviews, one semi-structured interview for outlining the general situation of disaster recovery planning in Kansaneläkelaitos and one structured self-assessment survey for gaining perspective of maturity of disaster recovery planning in Kansaneläkelaitos.

6.1 Interview on disaster recovery planning in Kansaneläkelaitos

The structure of the interview is based on the contingency planning process by U.S. National Institute of Standards and Technology (Swanson et al., 2010) presented in chapter **Virhe. Viitteen lähdettä ei löytynyt.**, paragraph 3.2.

Before the actual questions, the contents and the purpose of the interview were discussed with the interviewee. The ethical considerations discussed in chapter 2, paragraph 2.6 were also discussed with the interviewee.

The interview questions focused on following different areas as shown in Table 1.

Table 1. Interview questions by each area.

Area	**Questions**
Contingency planning policy	In what kind of circumstances was the disaster recovery planning or contingency planning initiated in Kansaneläkelaitos? What is the role of the management in starting disaster recovery planning?
Business impact analysis	What kind of formal analysis was conducted on the criticality of the services included in the disaster recovery planning? Were the impacts of the disruption and estimated downtime assessed? Were the resources included in the service mapped? Were the priorities in the recovery discussed?
Preventive controls	What preventive controls are in place? Are they technical or administrative in nature?

Contingency strategies	What kind of backup and restoration approaches are there? What is the expectation of loss of data in case of disruption? Are there alternate sites? What is their role in contingencies?
Information system contingency plan	What kind of disaster recovery plans have been written? What do they contain? Is business perspective included?
Testing, training, and exercises	What kind of approach was taken in testing the disaster recovery plans? How was the training conducted? What kind of exercises have there been?
Plan maintenance	How are the disaster recovery plans maintained? What is the input for plan maintenance?

6.2 Self-assessment of disaster recovery planning in Kansaneläkelaitos

The structure of the survey is based on a maturity self-assessment framework provided by Tipton and Krause (2007).

6.2.1 Survey setup

Before the actual questions, the contents and the purpose of the survey were informed the interviewees. The ethical considerations discussed in chapter 2, paragraph 2.6 were also informed to the interviewees.

After discussions, the persons participating in the survey with the tutor of the thesis in Kansaneläkelaitos, it was decided that the following list of people were to be contacted as described in Table 2.

Table 2. Interviewees and their role in the organization

Interviewee	**Role in organization**

Pertti Nieminen	Head of the ICT production unit. ICT production unit is responsible for providing operating services for Kansaneläkelaitos ICT systems excluding the National health archive (Kanta) services. Along with the operating services, ICT production unit is participating in development of methodology related to operating the ICT environment. For example, developing IT service management processes based on Information Technology Infrastructure Library (ITIL).
Aki Kokkinen	Group manager in Kansaneläkelaitos Kanta services. Responsible for ICT production in Kansaneläkelaitos Kanta services. ICT production of Kanta services and other Kansaneläkelaitos ICT services are not integrated because legislative reasons.
Seppo Larkiala	Senior IT specialist in ICT production unit. Process manager, ITSM-processes.
Jukka Korpi-Tassi	Group manager in ICT production unit, customer support team. Process manager, Incident management process and other ITSM-processes
Maarit Tammela	Business analyst in Customer relations system unit. Responsible for Kansaneläkelaitos online services for pharmacies.
Ville Taponen	Chief security officer in Kansaneläkelaitos
Kari Arkko	Senior ICT specialist in Application development unit, ICT information security office lead.
Jarmo Männikkö	Senior ICT specialist in Technology unit. Supporting ICT services, mainframe database specialist.
Ilari Saikkonen	Senior ICT specialist in Technology unit. Supporting ICT services, network specialist.

These employees work in different levels of the organization in the ICT services from management to the ICT specialists who write and implement the ICT recovery plans, which enabled to form a comprehensive situation picture of ICT recovery planning.

6.2.2 Categorization of data

For the purposes of analyzing data, the data gathered needed to be categorized. The data is categorized based on the person's responsibilities in the organization, which enables to understand further how the disaster recovery planning is perceived in the organization. Following coding scheme was used to categorize the data as illustrated in Table 3.

Table 3. Coding scheme for responsibilities in organization.

Code for responsibilities in organization	**Typical relevant work titles**	**Description**
System work	IT specialist, Senior IT specialist	Person works in maintaining the IT systems. Perspective is technical.
Service work	Service manager, System analyst, Process manager	Person works in area of IT services or ITSM-processes. Perspective is both technical/system related and administrative.
Team lead	Group manager	Person works as a team leader. Perspective is administrative.
Unit lead	Business unit manager, security officer	Person is responsible and 'owns' some contingency planning related area such disaster recovery planning or information security. Perspective is administrative.

The categorization described here is not mutually exclusive. For example, group managers can act as team leaders, service managers and process managers.

Due to the wide nature of the questions in the survey, it was probable that some interviewees were not able to answer all the areas in the survey. In this case, it was encouraged to leave that category open and enter a comment where the interviewee states having no experience about the subject.

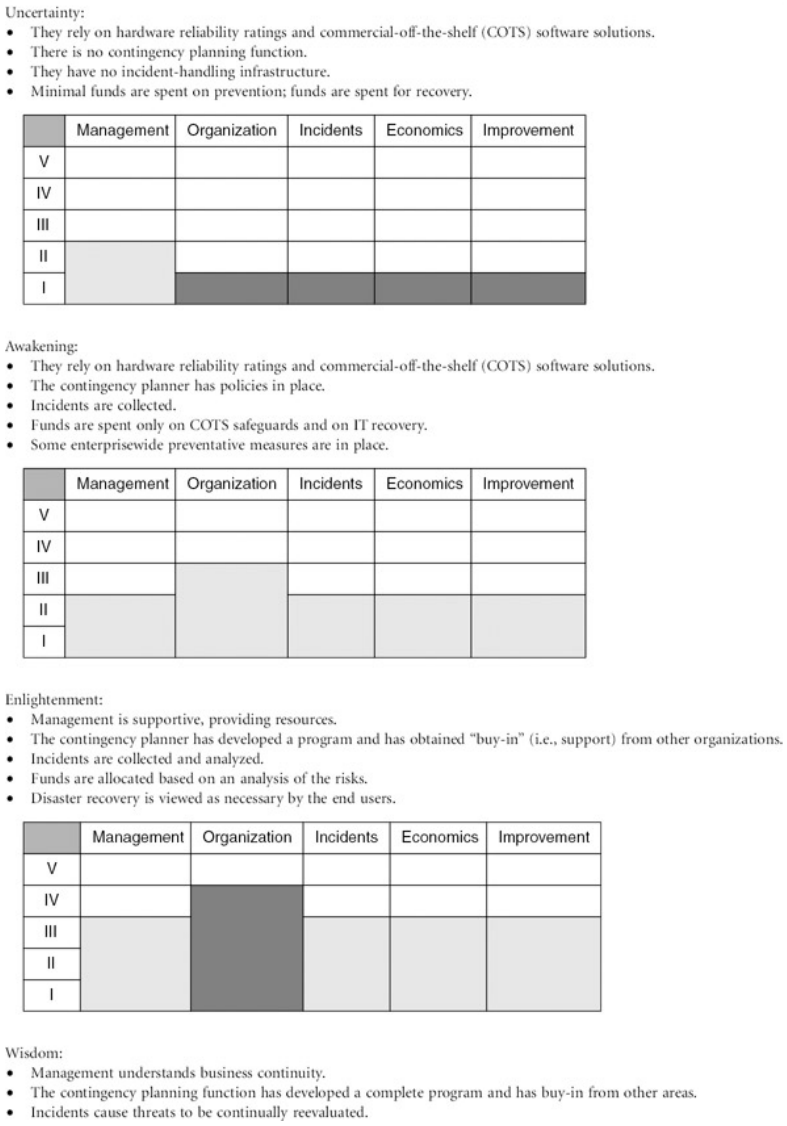
6.2.3 Survey

The interviewees were asked to give their opinion on the maturity of disaster recovery planning in Kansaneläkelaitos. The interviewees were to evaluate the maturity in areas described in Chapter 4, subsection 4.2.

The interviewees were given predefined characteristics of each stage of maturity to form their own opinion of the maturity in different areas. The characteristics are discussed in chapter 4, 4.2.7. The interviewees had the possibility to reflect on the level of maturity in each area.

The survey is a Microsoft Word document containing the name and the title of the interviewee and, of course, the areas of maturity evaluated with different stages of maturity forming essentially a grid where to fill the answers. The survey can be found in Appendix 2.

The following example (Figure 4) is from Tipton and Krause (2007) and illustrates the assessment of the maturity levels. Note the characteristics for each stage of maturity (Uncertainty, Awakenment, Enlightenment and Wisdom).



Uncertainty:
- They rely on hardware reliability ratings and commercial-off-the-shelf (COTS) software solutions.
- There is no contingency planning function.
- They have no incident-handling infrastructure.
- Minimal funds are spent on prevention; funds are spent for recovery.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Awakening:
- They rely on hardware reliability ratings and commercial-off-the-shelf (COTS) software solutions.
- The contingency planner has policies in place.
- Incidents are collected.
- Funds are spent only on COTS safeguards and on IT recovery.
- Some enterprisewide preventative measures are in place.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Enlightenment:
- Management is supportive, providing resources.
- The contingency planner has developed a program and has obtained "buy-in" (i.e., support) from other organizations.
- Incidents are collected and analyzed.
- Funds are allocated based on an analysis of the risks.
- Disaster recovery is viewed as necessary by the end users.

	Management	Organization	Incidents	Economics	Improvement
V					
IV					
III					
II					
I					

Wisdom:
- Management understands business continuity.
- The contingency planning function has developed a complete program and has buy-in from other areas.
- Incidents cause threats to be continually reevaluated.

Figure 4. Example of contingency planning self-assessment survey (Tipton and Krause, 2007)

7 Conclusions

In the earlier chapters, research methodology, disaster recovery planning and related concepts, ways to assess maturity of disaster recovery planning and Kansaneläkelaitos as an organization were explored.

As stated earlier, there appears to be many different terms related to the concept of disaster recovery planning. National Institute of Standards and Technology (Swanson et al., 2010) refers to these terms collectively as contingency planning. Disaster recovery planning refers to the activity planned and performed by the IT function of

the organization, and business continuity planning refers to the activity planned and performed by the business departments of the organization.

Qualitative approach was chosen for this thesis and a case study was conducted on the maturity of disaster recovery planning in Kansaneläkelaitos. The case study report was declared confidential on the grounds of protecting security arrangements and preparation for emergency conditions. The case study report is included Appendix 3, but is only available for Kansaneläkelaitos and inspectors of this thesis.

The maturity assessment framework introduced by Tipton and Krause (2007) was chosen over CMM (Paulk, 1995) as a basis for the case study. A supporting interview was conducted with Kari Arkko, an ICT specialist who acts as a coordinator in ICT security office in Kansaneläkelaitos.

8 Discussion

When writing a disaster recovery plan on system I was responsible in Kansaneläkelaitos, I found out that writing a disaster recovery plan is not a trivial task. That inspired me to write this thesis on assessing the maturity of disaster recovery planning.

Writing in a scientific manner first time in twenty years was not initially easy. Fortunately, everything was not forgotten from earlier studies and I could choose, in retrospect correctly, a qualitative approach for this thesis.

Studying background material for this thesis proved slightly frustrating at the beginning. There appeared to be not much scientific coverage on the disaster recovery planning and the assessing maturity of processes. The sources I found usable were mainly of management style by their nature. Eventually the framework provided in the book Information Security Management Handbook, Sixth Edition, Volume 1 (Tipton and Krause, 2007) was chosen as a framework where the research was based on.

The research comprised of one interview with the coordinator of ICT security office in Kansaneläkelaitos and one maturity assessment survey sent via email to employees in various positions related to Kansaneläkelaitos ICT services.

The interview was a semi-structured interview based on a National Institute of Standards and Technology planning process for contingency planning (Swanson et al., 2010). The purpose of the interview was to provide supplementary information for the results of maturity assessment survey. In my opinion, the process proved suitable for the purpose and provided relevant information to supplement the results of the survey.

After the interview, the maturity assessment survey was prepared and sent to the survey participants via email. Along with the survey, there was a cover letter explaining the background of the research, ethical considerations and return instructions.

The distribution of maturity assessments was quite small in each category of the survey. In my opinion, this indicates that the survey audience did not have difficulties to understand the categories and the stages of maturity.

The interview results provided another perspective to the disaster recovery planning in Kansaneläkelaitos. In my opinion, the interview told about several issues found also in the survey. Also, when looking the interview results now in retrospect, the interview itself is informative and contributes to the qualitative nature of this thesis. Having multiple sources of data produces a more accurate and diverse view into the subject (Eriksson, Kovalainen, 2014).

References

About kela. Accessed on 30 October 2016. Retrieved from http://www.kela.fi/web/en/about-kela.

Denzin, N. K., Lincoln, Y. S., Greenwood, D. J., Levin, M., Fine, M., Weis, L., . . . Marcus, G. E. 2005. *The sage handbook of qualitative research.* (3rd ed.). Thousand Oaks Calif. : Sage Publications,.

Elliott, J. 1988. *Educational research and outsider-insider relations. International Journal of Qualitative Studies in Education, 1*(2), 155-166. doi:10.1080/0951839880010204.

Eriksson, P., & Kovalainen, A. 2008. *Qualitative methods in business research.* Los Angeles, Calif. London: Sage.

FINLEX ® - ajantasainen lainsäädäntö: Laki viranomaisten toiminnan julkisuudesta 621/1999. Accessed on 26 October 2016. Retrieved from http://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

Humphrey, W. S. 1989. *Managing the software process.* Reading, Mass: Addison-Wesley.

Kelakanava. 2016a. *Kanta-palvelut nyt ja tulevaisuudessa, marina lindgren.* Accessed on 11 March 2017. Retrieved from https://www.youtube.com/watch?v=8mD9gmhOmwM.

Kelakanava. 2016b. *Tehokkaat tietojärjestelmät, ICT-johtaja markku suominen.* Accessed on 24 January 2017. Retrieved from https://www.youtube.com/watch?v=SK8fl5qMiGM.

Kokkinen, A. 2016. *Kela, OPER syysseminaari 2016.* Accessed on 11 March 2017. Retrieved from https://www.slideshare.net/THLfi/aki-kokkinen-kela-oper-syysseminaari-2016.

Leong Lai Hoong, & Marthandan, G. 2011. *Factors influencing the success of the disaster recovery planning process: A conceptual paper. 2011 International Conference on Research and Innovation in Information Systems,* 1-6. doi:10.1109/ICRIIS.2011.6125683.

National Institute of Standards and Technology. 2014. *Framework for improving critical infrastructure cybersecurity.* Accessed on 21 December 2016. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Paulk, M. C. 1995. *The capability maturity model :: Guidelines for improving the software process.* Reading MA: Addison-Wesley.

Persse, J. R. 2001. *Implementing the capability maturity model.* John Wiley & Sons.

Schwandt, T. A. 2007. *The sage dictionary of qualitative inquiry.* Sage.

Stake, R. E. 1995. *The art of case study research.* Thousand Oaks Calif. : Sage,.

Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. 2010. *Contingency planning guide for federal information systems. NIST Special Publication 800-34 Rev. 1,*

Tipton, H. F., & Krause, M. 2007. *Information security management handbook, sixth edition, volume 1.* CRC Press.

Yin, R. K. 2014. *Case study research : Design and methods.* (5th ed ed.). Los Angeles: SAGE.

Appendices

Appendix 1. Glossary of essential terminology

Term or definition	**Explanation**
Business continuity plan	Business continuity plan focuses on sustaining an organization's mission/business processes during and after a disruption
Business impact analysis	Business impact analysis evaluates business processes in terms of criticality and possible downtime impact
Contingency plan	An umbrella term for disaster recovery plans and business continuity plans
Disaster recovery plan	Disaster recovery plan mitigates to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period
ICT	Information and communications technologies
IT	Information technology
ITIL	Information technology infrastructure library. A set of industry best practices for ITSM
ITSM	IT service management. Policies, processes and procedures for design, deliver, operate and control information technology (IT) services.
Kansaneläkelaitos	Social insurance institution of Finland
Process maturity	Maturity can be defined in terms of predictability and risk. The more mature the process, the more predictable it is, and the more manageable are the risks.
SAP	Abbreviation from Systeme, Anwendungen und Produkte in der Datenverarbeitung Aktiengesellschaft. In context of this thesis, SAP can be considered as system covering Kansaneläkelaitos management.
ST-IV	One of security classification of documents. ST-IV means restricted access for documents is required.

Appendix 2. Self-assessment of disaster recovery planning

Survey of maturity of disaster recovery planning in Kansaneläkelaitos

Mika Ylikangas, Degree programme in cyber security, Jyväskylän ammattikorkeakoulu

Please return to **kari.arkko@kela.fi**

Your responsibilities in Kansaneläkelaitos (please mark all applicable with x):

Responsibilities	**Typical relevant work titles**	**Description**
	IT specialist, Senior IT specialist	Person works in maintaining or developing the IT systems. Perspective is technical.
	Service manager, System analyst, Process manager	Person works in area of IT services or ITSM-processes. Perspective is both technical/system related and administrative.
	Group manager	Person works as a team leader. Perspective is administrative.
	Business unit manager, security officer	Person is responsible and 'owns' some contingency planning related area such disaster recovery planning or information security. Perspective is administrative.

Management understanding and attitude means how the management sees the role of contingency planning. How much resources are given to contingency planning. What is the management support for contingency planning?

Please read the characteristics below and write your assessment what is the level of maturity in this area and why	

To attain Stage 2:

- Management will approve the procurement of vendor-supplied, "built-in" software solutions to increase system reliability (i.e., backup software, configuration management tools, tape archiving tools, etc.).
- Management will approve the procurement of vendor-supplied, "built-in" hardware solutions to increase system reliability (i.e., equipment with high mean-time-between-failure ratings, inventorying spare line-replaceable-units, etc.).

To attain Stage 3:

- Management will endorse IT disaster recovery policies.
- Management will support development of robust IT disaster recovery plans.
- Management will support disaster recovery training for operations personnel.

To attain Stage 4:

- Management will shift its focus from IT disaster recovery to the identification of and recovery of critical business functions.
- Management will commission a detailed business impact assessment(s) and gain a clear understanding of the critical business functions and IT infrastructure.
- Management will obtain an understanding of the absolutes of business continuity planning and become able to make informed policy decisions.
- Management will promote business continuity.
- Management will empower organizational elements to augment the enterprise's contingency planning program consistent with the business unit's needs.

To attain Stage 5:

- Management will understand that business continuity planning is an essential part of the enterprise's internal controls.
- Management will provide adequate resources and fully support continual improvement of the business continuity planning program, to include internal research and development.

Contingency planning organization status means how the disaster recovery, or contingency planning is organized at the moment. Is there assigned responsibility in

the organization. How is the contingency planning reported to the management? Are business people involved with contingency planning?

Please read the characteristics below and write your assessment what is the level of maturity in this area and why	

To attain Stage 2:

- Management will appoint a contingency planner
- Emphasis will be placed on the recovery of IT operations from a worst-case disaster.

To attain Stage 3:

- The contingency planning function will be matrixed to the corporate information security function.
- The Disaster Recovery Plan will be based on recovery from more realistic disasters as well.
- Disaster recovery will include the ability to recover corporate communications.

To attain Stage 4:

- The contingency planning function will be transitioned into the corporate information security function.
- Focus will change from IT disaster recovery toward business continuity.
- Risk analyses and business impact assessments will be updated periodically, and penetration and audit capabilities will be supported.
- The contingency planning function will develop strategic alliances with other organizations (i.e., configuration management, product assurance, procurement, etc.).

To attain Stage 5:

- Top management will regularly meet with the information security officer regarding business continuity issues.
- Through internal research and development, contingency planning will be able to address technical problems with leading-edge solutions.

- Contingency planning's role will expand into the community to augment the enterprise's image.
- The enterprise will be noted for its ability to consistently deliver on time.

Incident handling meaning how situations which might need activation of recovery plans are handled. How are incidents tracked in the organization? How are the incidents utilized in contingency planning?

Please read the characteristics below and write your assessment what is the level of maturity in this area and why	

To attain Stage 2:

- Data management issues (file recovery) gain visibility.
- Rudimentary statistics will be collected to identify major trends.
- Contingency planning will focus on response to a high-visibility dramatic incident.

To attain Stage 3:

- An initial business impact assessment will have been performed to determine the relative criticality of IT assets and services, and to reveal the business's time-to-recover requirements.
- Based on detailed statistics available due to implementation of a formal incident reporting process, the information security threat can be better identified, thus enabling the development of more realistic disaster scenarios.

To attain Stage 4:

- Threats will continually be reevaluated based on the continually changing threat population and on the security incidents enhancing the accuracy of the risk analysis.
- Thorough business impact assessments will be conducted across the entire enterprise.

To attain Stage 5:

- Incident data will be continually analyzed and fed back to continually improve the information security process.

Economics meaning the economic resources in relation of disaster recovery, or contingency planning. How is the planning funded?

Please read the characteristics below and write your assessment what is the level of maturity in this area and why	

To attain Stage 2:

- Management will provide contingency planning only limited funding, allocated primarily for the procurement of higher reliability equipment supplied by vendors touting their "built-in" reliability

To attain Stage 3:

- Expenditures will be managed and justified, funding IT disaster recovery activities selected as a result of a risk analysis.

To attain Stage 4:

- Expenditures will be managed and continually justified through periodic risk analyses and business impact assessments of greater accuracy, identifying additional or more cost-effective recovery strategies in response to the continually changing threat environment.
- Losses will be anticipated through cost/benefit trade-offs.

To attain Stage 5:

- The cost-savings aspect of a completely implemented contingency planning program will be thoroughly understood and realized.
- Contingency planning expenditures will be justified and reduced, being partially funded through its contribution to marketing.

Contingency planning improvement meaning the plans to improve the recovery, or contingency planning. Is there continuous effort or system in place where contingency planning is improved in sustained and gradual manner.

Please read the characteristics below and write your assessment what is the level of maturity in this area and why	

To attain Stage 2:

- The contingency planner will begin to implement and document IT operations procedures and develop an initial IT disaster recovery plan.

To attain Stage 3:

- The contingency planner will develop a robust IT disaster recovery plan.
- A training program will be offered for recovery personnel to increase the likelihood of a successful recovery of the IT assets.
- Management will understand the "business case" for contingency planning.
- Management will fund the contingency planning activities of risk analysis, risk reduction initiatives; business impact assessment, and audits.

To attain Stage 4:

- Risks will be accurately evaluated and managed.
- Contingency planning/recovery research activities will be initiated to keep up with the rapidly changing environment.
- A continual, detailed business continuity training program will be developed.

To attain Stage 5:

- The contingency planning activities (e.g., risk analyses, risk reduction initiatives, business impact assessment, audits, training, research, etc.) will become normal, continual activities.
- The contingency planning function will obtain desirable contingency planning improvement suggestions from end users and system owners.

Appendix 3. Kansaneläkelaitos, case study results

This appendix describes the results of the case study conducted on the Kansaneläkelaitos disaster recovery planning maturity. The appendix is classified as ST-IV (use restricted) on the grounds of:

- Information relating to or affecting the realization of the security arrangements of persons, buildings, installations, constructions, and data and communications systems (Act on the Openness of Government Activities 24§,7)
- Information concerning preparations for accidents and emergency conditions, civil defense or its development (Act on the Openness of Government Activities 24§,8)

The appendix is delivered for inspection as a separate copy.