jamk.fi

ICT CONTINGENCY ON FINNISH ORGANIZATIONS

SURVEY FOR ICT CONTINGENCY PLANNING

Pasi Tarvainen

Master's Thesis
December 2013

Information Technology

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s) TARVAINEN, Pasi	Type of publication Master’s Thesis	Date 23.11.2013
	Pages 69	Language English
		Permission for web publication ( )

Title
ICT Contingency on Finnish Organizations

Degree Programme
Master´s Degree Programme in Information Technology

Tutor(s)
KOTIKOSKI, Sampo

Assigned by
Resolute ISMS Oy, Technology Director Arto Väisänen

Abstract
The importance of ICT contingency and resiliency planning has significantly increased during the last years. The threats for ICT systems have expanded and changed due to rapid technological development. For the public sector, including the governmental authorities and municipalities, there has been very little new information on this since 2009 and the pilot study for ICT contingency survey by the Ministry of Finances. After the publishing of the pilot study, the public sector has been under major reconstruction.

In the thesis the current situation of ICT contingency and resiliency planning was researched. The research carried out by using a survey. The survey was based on the pilot study the Ministry of Finances survey which was updated. Major updates consisted of the addition of background material with VAHTI and KATAKRI guidance. Within the survey the business aspect and analysis were investigated and implemented for the assigner corporation.

The results show that ICT contingency plans and the current organizational state are heavily impacted by the organizational size and the organizational position of the survey candidate. ICT contingency planning in general is a described process for many organizations; however, it is not finalized. There is a need for external auditors and reviewers but the organizations cannot use the resources until the public guidance is up to date and unified.

Keywords
ICT Contingency, Planning, VAHTI, KATAKRI

Miscellaneous

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) TARVAINEN, Pasi	Julkaisun laji Opinnäytetyö	Päivämäärä 23.11.2013
	Sivumäärä 69	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty

Työn nimi

ICT jatkuvuus suomalaisissa organisaatioissa

Koulutusohjelma

Informaatioteknologian ylempi korkeakoulututkinto

Työn ohjaaja(t)

KOTIKOSKI, Sampo

Toimeksiantaja(t)

Resolute ISMS Oy, Tekninen Johtaja Arto Väisänen

Tiivistelmä

ICT-jatkuvuuden ja -jatkuvuussuunnitelmien merkitys on viime vuosina kasvanut merkittävästi. ICT-järjestelmiin kohdistuvat uhkakuvat ovat laajentuneet ja muuttaneet muotoaan. Kuitenkaan suomalaisessa julkishallinnossa ei ole sitten vuoden 2009 selvitetty ICT-valmiussuunnittelun tai -jatkuvuussuunnittelun tilaa. Valtionvarainministeriön vuoden 2009 esitutkimushankkeen tulosten julkaisun jälkeen suomalainen julkishallinto on myllerryksessä.

Opinnäytetyössä selvitettiin ICT-valmiussuunnitelmien nykytilaa ja niiden luomiseen käytettyä pohjamateriaalia. Työssä käytetty kysely pohjautui suurelta osin valtionvarainministeriön vuonna 2009 käyttämään kyselyyn sillä erotuksella, että nykyiset VAHTI- ja KATAKRI-ohjeistukset oli otettu huomioon. Työn ohessa toimeksiantajalle arvioitiin valmiussuunnittelun liiketoimintamahdollisuuksia.

Työssä selvisi ICT-valmiussuunnittelun näkemysten eroaminen organisaation koon ja vastaajan organisaation aseman mukaisesti. Kokonaisuutena arvioiden ICT-jatkuvuussuunnittelu on tiedostettu, mutta keskeneräinen prosessi. Ulkopuolisen tahon suorittamille katselmuksille ja auditoinneille olisi kysyntää, mutta liiketoiminnan toteutuminen vaatii ohjeistuksen yhtenäistymistä.

Avainsanat (asiasanat)

Jatkuvuussuunnittelu, palautuminen, VAHTI, KATAKRI

Muut tiedot

INDEX

INDEX 1

FIGURES 2

TABLES 3

ACRONYMS 4

1 INTRODUCTION 5

1.1 Resolute ISMS Oy 5

1.2 HANSEL and KL-Kuntaliitto frame agreement 5

1.3 HANSEL Ltd. 6

1.4 KL-Kuntahankinnat 6

2 ICT Contingency and Readiness Planning 8

2.1 Contingency Planning 10

2.2 Comparison of NIST 800-34 and NIST 800-34 Rev. 1 13

2.3 VAHTI AND KATAKRI – Governmental Guidance in Finnish regulations 14

2.4 ISO/IEC STANDARDS 16

2.5 RESEACH TOPIC 18

3 RESEARCH METHODS USED 19

3.1 Strategy 19

3.2 Quantitative 20

3.3 Qualitative 20

3.4 Questionnaire 21

4 CONTINGENCY PLAN ASPECTS USED IN THESIS 22

5 Methods for Data Collection 24

5.1 Designing the Questionnaire 24

5.2 Selecting the Survey Candidates 24

6 RESULTS 26

6.1 Quantitative results and analysis 26

6.2 Profiling Analysis 37

6.2.1 Question 7 Services and ICT-infrastructure 39

6.2.2 Question 8 ICT Readiness 44

6.2.3 Question 9, Information systems and readiness 49

6.3 Qualitative analysis of results 53

6.4 Comparison between Pilot study and thesis 54
7 CONCLUSIONS 56
REFERENCES 58
APPENDIX 1 - Pilot Study for ICT contingency planning – Original Questionnaire 60
APPENDIX 2 – Questionnaire for ICT Contingency Planning 63

FIGURES

FIGURE 1 - BIA Analysis 12
FIGURE 2 Strategy differences part 1 (Denscompe, 2012, 5) 19
FIGURE 3 Strategy differences part 2. (Denscompe 2010, 6) 20
FIGURE 4 Structure of survey candidates 25
FIGURE 5. ICT Services 28
FIGURE 6. ICT Services and Infrastructure 30
FIGURE 7. ICT Services and Infrastructure - Survey group........................... 31
FIGURE 8. ICT services analysis 31
FIGURE 9. ICT Contingency, Question 8, ICT planning 32
FIGURE 10. ICT Contingency, Question 8, ICT Planning - Survey pool 33
FIGURE 11. ICT Contingency, Question 9, organizational guidance 34
FIGURE 12. ICT Contingency, Question 9, Survey pool 35
FIGURE 13. Question 10, General data 36
FIGURE 14. Question 10, Survey pool 37
FIGURE 15 Organizational sizes 38
FIGURE 16 Question 7, Less than 100 persons, Experts 39
FIGURE 17 Question 7, Less than 100 persons, Managers 40
FIGURE 18 Question 7, more 100, Experts 42
FIGURE 19 Question 7, more than 100, Managers 43
FIGURE 20 Question 8, less than100, experts 45
FIGURE 21 Question 8, less than 100, Managers 46

FIGURE 22 Question 22, companies with more than 100 experts................. 47
FIGURE 23 Question 8, more than 100, managers 48
FIGURE 24 Question 9, Less than 100, Experts.. 49
FIGURE 25 Question 9, less than 100 employees in the company, Managers 50
FIGURE 26 Question 9, companies with more than 100 employees, Experts' views 50
FIGURE 27 Question 9, more than 100 employees in the company, Managers 51
FIGURE 28. Dilbert view of point (Dilbert, 2013).. 57

TABLES

TABLE 1. Distribution of survey candidates based on the organization......... 26
TABLE 2. Distribution of organizational positions.. 27
TABLE 3. Use of external consulting in general 28
TABLE 4. Use of External consulting, survey pool 29
TABLE 5. Use of External consulting, survey pool 29
TABLE 6. Average on Question 9 34
TABLE 7 Average on Question 7 based on organizational size < 100........... 41
TABLE 8 Average on Question 7 based on organizational size, > 100.......... 44
TABLE 9 Question 9, averages on answers.. 52

ACRONYMS

BIA	Business Impact Analysis
NIST	National Institute of Standards and Technology
KATAKRI	Finnish National Auditing Criteria
VAHTI	Finnish Governmental Information Security Guidance
ICT	Information and Communications Technology

1 INTRODUCTION

1.1 Resolute ISMS Oy

Resolute ISMS Oy is a Finnish network equipment reseller that was founded in 2010. Resolute focuses on reselling, consulting and installation. As a new and growing company customer satisfaction is the main concern. Resolute wants to be customer's trusted advisor in no matter too small.
Resolute has grown during the first years. In the latest fiscal year Resolute made a revenue of 5.8M€ and a positive profit. Current personnel count is 11 and Resolute is committed to increase to 13 in calendar year 2013.

1.2 HANSEL and KL-Kuntaliitto frame agreement

Resolute participates in two major joint procurement agreements. Both of these agreements have major client base in public sector. Both agreements will give a solid base for the thesis background material as they give separate views for the public sector.

On governmental side the Hansel agreement is most used. It has been dictated by governmental side that all government institutes and organizations should use the Hansel agreement.

On communities and cities the most widely used joint procurement agreement are the KL-Kuntaliitto's agreements. They differ from Hansel by being offered via a separate organization. This is due to the Finnish regulations where it is stated that communities can only acquire goods without tender if they acquire them from their own organization. This has worked with KL-Kuntahankinnat, which is owned by its customers.

1.3 HANSEL Ltd.

Based on Hansel web pages they describe themselves as follows.

“Hansel Ltd is the central procurement unit of the Finnish Government. It is an expert organization with 70 staff members, which puts the products and services required by the public administration out to tender and maintains the related framework agreements.” (Hansel web pages)

Hansel is a non-profit procurement unit, which oversees the procurement and aids its customers on many matters.

“Hansel’s customers have the opportunity to make acquisitions without separate tendering processes by joining the framework agreements administered by Hansel. Central procurement implemented under the framework agreements generates considerable savings for the Finnish Government through both procurement process costs and pricing. In addition to framework agreements, Hansel Ltd provides consultancy services for its customers’ autonomous procurement. Such services consist mainly of legal expertise, and services related to the practical implementation of procurement processes in cases of autonomous procurement.” (Hansel web pages - company)

1.4 KL-Kuntahankinnat

KL-Kuntahankinnat is a community and municipalities owned joint procurement unit. Kuntahankinnat is an easy way for its owners to purchase any goods under the joint procurement agreement. KL-kuntahankinnat describes them as follows.
”As a joint procurement company KL-Kuntahankinnat Oy acts on behalf of its local government clientele by putting procurement contracts and framework

agreements out to tender, by conducting negotiations and managing contracts and, within the limits of its resources, by offering clients expert services in public procurement." (KL-Kuntahankinnat web pages)

2 ICT Contingency and Readiness Planning

ICT contingency and readiness is a systems capability to adopt and remedy from unwanted situations. This capability is based on planning and actions under common process. There are similarities on readiness planning to any other planning methods and similar process approach is usually recommended.

Based on the NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems the information system is described in the following way.
” Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, disk drive failure) to severe (e.g. equipment destruction, fire). Much vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the organization’s resiliency effort; however, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by providing
effective and efficient solutions to enhance system availability.” (NIST 800-34 Rev 1, page 3)

Ministry of Finance has made in 2011 a pilot study about ICT contingency planning in local government. This study also contained questionnaire and workshops. The questionnaire in this thesis is on the actual questionnaire in order to give research background to the subject.

The pilot study describes its aim. “The aim is to ensure that ICT contingency planning is cost-effective and a coordinated part of daily activities in each individual municipality, so that the continuity of local government services can be secured in the required manner even in abnormal circumstances, in emergency situations as specified in the Strategy for Securing the Functions Vital to

Society and in exceptional situations.” (Pilot Study for ICT contingency planning, Page 7)

After the publication of the pilot study there have been very limited resources to analyze the readiness of the current state of local governments. This has been a major issue in market analysis.

Finnish local government structure is undergoing a major change as this thesis is. The Finnish Ministry of Finance has nominated a Kuntauudistus-project, which aims to change and consolidate the structure of Finnish local government. This project tries to unify and merge Finnish municipalities into bigger units in order to provide basic services to their inhabitants. One major aspect is to create a solid structure for health care and social services including services for the elderly.

Due to the Kuntauudistus project and mergers of local municipalities be seen a need for consultation services and professional aid for contingency and readiness can be seen. The major aspect of this thesis focuses on finding the demand for these business needs and a way to obtain the right packaging for professional services.

As Finland is a dispersed country the ICT systems are usually wide spread in terms of distance and variety. One example of a very critical system is patient information system. The major vendor in the Finnish market is Tieto with its Effica system. Usually the Effica system is operated from vendor’s data centers and the actual system and its operations maybe unmanned by using organization. There might be none or only little resilience or readiness planning considering the system. It might be identified as one of the key systems but there might be no influence on recovery planning in order to identify what needs to be enabled in order to ensure that the system is back on-line. From this example it can be seen that there might be a lack of structural approach on Business Impact Analysis, BIA.

2.1 Contingency Planning

Contingency planning is a key point to sustain ICT systems in an event that might endanger the system.

Contingency planning can be separated into certain process steps. Like all other ICT processes these processes will create a process spiral that will eventually generate a new process. The lifecycle of contingency plan according to NIST looks very similar to any other ICTlifecycle.

The model contains seven progressive steps as follows below:

1. **Develop the contingency planning policy statement.**
A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

2. **Conduct the business impact analysis (BIA).**
The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.

3. **Identify Preventive Controls.**
Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4. **Create contingency strategies.**
Thorough recovery strategies ensure that the system may be recovered quickly and effectively after a disruption.

5. Develop an information system contingency plan.

The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

6. Ensure plan testing, training, and exercises.
Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

7. Ensure plan maintenance.
The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.
(NIST 800-34 Rev. 1 page 13.)

In the Finnish pilot study there can be a great deal of information about the state of readiness; however, due the nature of the study it is very limited on actual guides or tips. Based on the study it can be found that the work for contingency has been started; however, there is little or no information whether the work has actually been finished.

Based on the study and on-work experience it can be said that contingency policy statements are usually written into ICT policy.

Figure 1 from The Pilot Study shows that from 172 communities 77% declare that they have conducted the BIA and have successfully identified the key ICT systems. Yet, it remains unsure if anything is done for these systems.

KUVA 25. Tilanne toiminnan kannalta kriittisten tietojärjestelmien tunnistamisen osalta (Lähde TIVA kysely). 172 kuntaa vastasi kyselyyn.

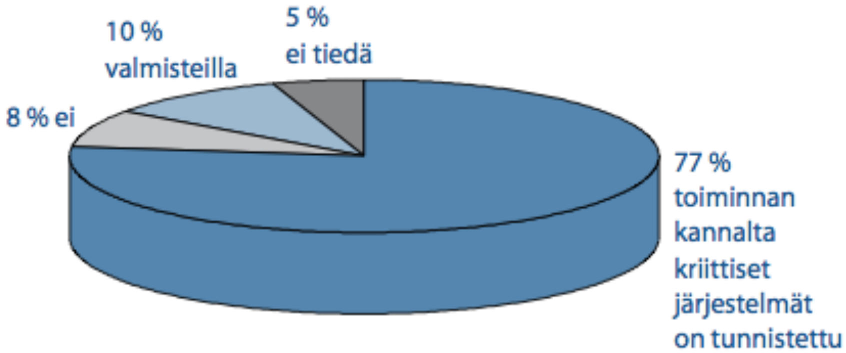


FIGURE 1 - BIA Analysis

On this thesis the focus is more on the technical side. Usually local governments have actually conducted the BIA. This is done either because of healthcare projects like e-resepti (e-prescription) demands it or it is based on some other administrative ruling. What has been seen on the field is that the work for contingency planning is usually interrupted or it has been set aside. The actual documentation or preventive controls usually lack details or the details are not even documented.

Based on the pilot study there are several key factors why the current situation is what it is. Following key factors are raised based on the study. (Pilot Study for ICT contingency planning, page 38)

- Lack of ICT Administration

  This is true in especially small municipalities. Also some of the municipalities have consolidated the ICT Administration into external establishments. This makes the ICT administration dispersed and responsibilities might vanish or they are not clearly defined.

- Lack of guidance from governmental level

> On many cases the ICT administration feels that there are not enough guidance, tips or guides provided in order to develop ICT strategy or contingency planning.

There are guidance and criteria like VAHTI or KATAKRI II. Local governments and municipalities as well as external establishments have found those way too complicated or feel that they do not suite for business purposes.

2.2 Comparison of NIST 800-34 and NIST 800-34 Rev. 1

On the 2010 the NIST 800-34 was updated to revision 1. At that time to contingency planning guide and the security controls for contingency were not align. The revision added the NIST SP 800-53 Rev. 3 link to 800-34. Also the FIPS compliance requirements were added to the document.

Swanson describes the overall changes in her presentation in the following way

- Revision 1 covers three common types of platforms, making the scope more inclusive (Client/servers, Telecommunications systems, and Mainframes).
- There is a bigger focus on the Information System Contingency Plan (ISCP) as it relates to the differing levels of FIPS 199 impact levels.
- General Support Systems (GSS) and Major Applications (MA) categories have been removed.
- Introduces the concept of resiliency and shows how ISCP fits into an organization's resiliency effort.
- Works to more clearly define the different types of plans included in resiliency, continuity and contingency planning.
- Throughout the guide, call out boxes clarify the specific differences and
- Relationships between COOP and ISCP.

  (Swanson, A., Page 5)

Also the concept of resilience has been defined more clearly. Swanson and the Department of Homeland Security define the resiliency as following way.

- Department of Homeland Security (DHS) defines resiliency as the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions”.
- Resiliency is not a process, but rather an end-state for organizations.
- Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions.
- An effective resiliency program includes risk management, contingency and continuity planning, and other security and emergency management activities.
  (Swanson, A, Page 6)

One of the main arguments made in Swanson’s overall presentation is clear, precise and accurate definition of resilient organization.

The Goal of A Resilient Organization: Continue Mission Essential Functions at All Times During Any Type of Disruption (Swanson A, Page 6).

It can be said that achieving the definition is successful demonstration of ICT Contingency planning.

2.3 VAHTI AND KATAKRI – Governmental Guidance in Finnish regulations

The Council of State on 2007 established the Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI, to guide and co-ordinate ICT security and principals. (VAHTI hankerekisteri, 30.7.2013)

The structure of regulations and main responsibilities are described on the VAHTI's Annual Report 2012. The VAHTI's Annual Report describes as following.

"The Ministry of Finance directs and coordinates the development of information security across local and, more particularly, central government. The Government Information Security Management Board (VAHTI), appointed by the Ministry, is responsible for Government cooperation, steering and development efforts in this area. VAHTI sets all the main policy guidelines for information security and cyber security in central government. Different administrative branches and levels of administration are represented in VAHTI." (VAHTI's Annual Report 2012, page 11)

As can be seen, the VAHTI is more focused on the big picture and coordinating the structure of the ICT security field. The public sector is highly steered and projects are currently going and producing documents and guidance. This is guided in Finland by regulations. VAHTI's Annual report states that the Public Sector ICT function (JulkICT) operating directly under the Ministry's top leadership is responsible for the guidance and development of public administration ICT. The act on information management guidance in public administration (Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011) underscores the role and responsibility of the Ministry of Finance for steering ICT operations in the whole public sector. (VAHTI's Annual Report 2012, page 11).

VAHTI's role in Finnish ICT field is very strong. It is considered to be one of the highest authorities in the public sector ICT. The majority of the publications are high on level quality and valued trough tout the ICT field. The actual guides are constructed in very similar way as for example the NIST guide mentioned earlier.

KATAKRI or Kansallinen Tietoturvakriteeristö presents the criteria for governmental and public sector in order to unify the processes when cooperating together. Ministry of Defense states out that these criteria can also be used as a tool for corporations in their own security platform. (Kansallinen turvallisuusauditointikriteeristö (KATAKRI) – web pages 30.7.2013)

KATAKRI is a detailed question based template in order to evaluate the organizational readiness and state in order to co-operate with governmental entities. As Resolute is a KATAKRI II Audited corporation the level of details is well known. It can be seen that KATAKRI is not suitable for contingency work unless all the documentation is ready and usable. In KATAKRI there are multiple good evaluation questions for ICT contingency. The main issue with KATAKRI is that the questions are too detailed for initial contingency planning. Therefore KATAKRI II questions are directly used for any questionnaire.

2.4 ISO/IEC STANDARDS

ISO/IEC 27002:2005 is the newest standard from ISO that establish guidelines and general principles for initiating and, implementing and maintaining, and improving information security management in an organization (ISO/IEC 27002:2005, Abstract)

While ISO/IEEC 27002:2005 is focused on information security the business continuity management is a key aspect of it.
The structure of standard is very similar to NIST model with small differences based on the fact that 27002:2005 is an information security standard. NIST contingency planning takes no difference why interruption of normal business function happens where ISO/IEEC focuses on continuity on InfoSec field.

In some cases these two points of view are the same, however, the majority contingency of use cases are not based on information security. For example, in municipalities the electricity problems might initiate the contingency plans, yet the systems are completely safe from information security viewpoint. Although it must kept in mind that information security planning and contingency planning have more common ground than differences.

The ISO standard defines the objective of Information security aspects of business continuity management by following way:

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. (ISO/IEC 27002 page 95)

It is very similar to all other sources that describe the continuity. The main difference in the ISO approach is that it strongly advises to keep the Information security aspect on the side.

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. (ISO/IEC 27002, page 95)

ISO defines that the control for continuity is merely a process that is managed by the organization. The standard does not define methods but gives guidance in order to implement such a process. It can be seen that ISO standard gives a very similar framework to any other reference model. One major difference in ISO standard is the process and plan ownership. As everything is defined more or less as a process the ownership is always present.

During the year 2013 ISO published a newer revision of the 27002 standard. New revision of the standard is ISO/IEC 27002:2013.

2.5 RESEACH TOPIC

This thesis aims at discovering the state of the actual contingency planning. The focus will be on contingency planning details and on developing the contingency plan.

The idea was to analyze the state of the market and find out whether there was a business case for offering professional services in order to create, develop and maintain contingency as a service.

The research questions chosen for this Master's thesis are as follows:

- What is the current state of contingency planning?
- Is there enough in-detail information in order to create, develop and maintain contingency plans?
- Is there a market for professional services in contingency planning?

The research contains an actual analysis for the market and a control group. The control group is formed from undisclosed governmental and private entities. These entities will be selected from Resolute's client base and they will receive the same questionnaire as the research group.

There will also be selected amount of workshops based on actual customer case. Some results from these workshops are presented in the conclusion part. These workshops are under heavy non-disclosure agreements. The actual material from these workshops cannot be revealed. Workshops are conducted with the research group as well as with the control group.

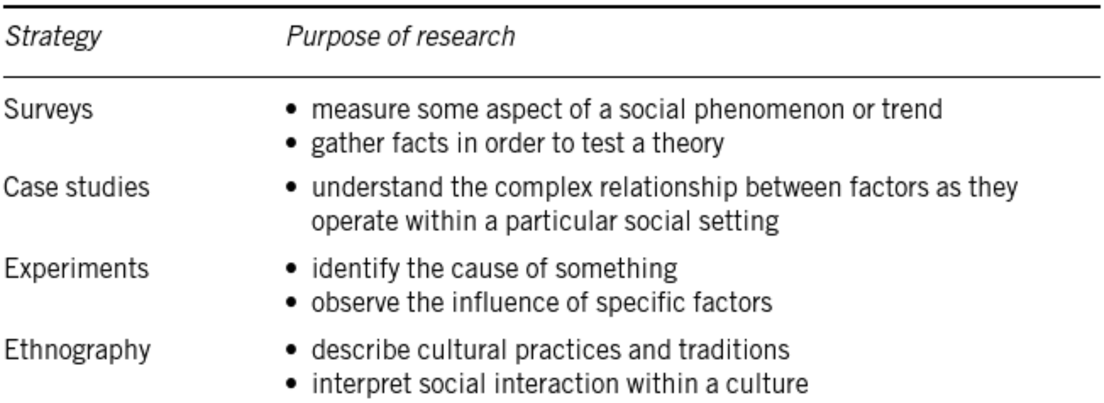
3 RESEARCH METHODS USED

This thesis there will uses a mixture of research methods due to nature of this subject. By only using the quantitative method the result might disperse. Qualitative method is conducted by workshops and it is designed to be the control method for the questionnaire.

3.1 Strategy

For the research strategy Denscompe states out that A Research strategy is different from research method. (Denscompe 2010, 4) In this thesis there are no single strategy. A question in this field cannot be formed only to be multiple-choice answer nor the case studies show enough statistical data.

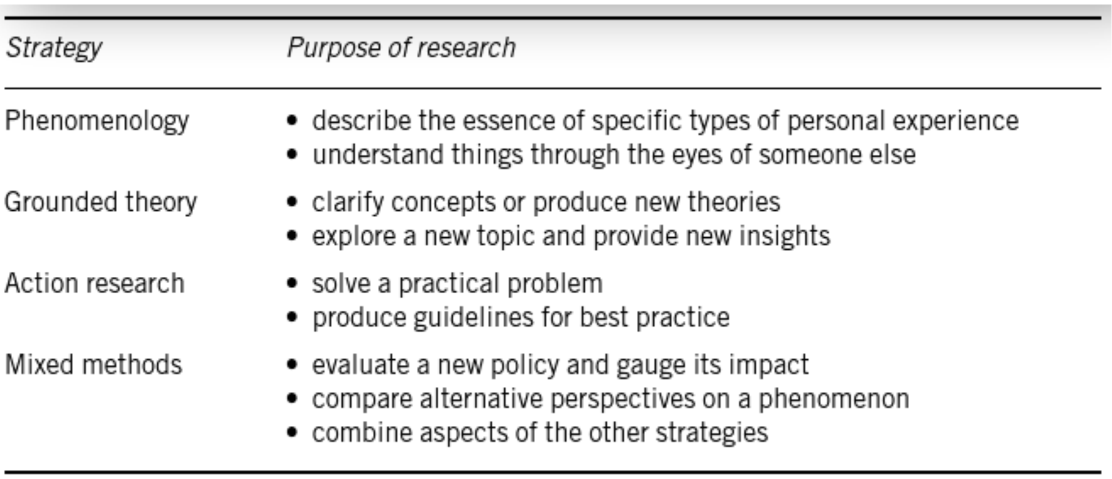
Figures 2 and 3 from Denscompe illustrate the different strategies versus purpose of the research.



Strategy	*Purpose of research*
Surveys	• measure some aspect of a social phenomenon or trend • gather facts in order to test a theory
Case studies	• understand the complex relationship between factors as they operate within a particular social setting
Experiments	• identify the cause of something • observe the influence of specific factors
Ethnography	• describe cultural practices and traditions • interpret social interaction within a culture

FIGURE 2 Strategy differences part 1 (Denscompe, 2012, 5)

As Figure 2 states out, not only Surveys or Case Studies provides enough data and reference material. Figure 3 shows more choices for strategy selection.



Strategy	*Purpose of research*
Phenomenology	• describe the essence of specific types of personal experience • understand things through the eyes of someone else
Grounded theory	• clarify concepts or produce new theories • explore a new topic and provide new insights
Action research	• solve a practical problem • produce guidelines for best practice
Mixed methods	• evaluate a new policy and gauge its impact • compare alternative perspectives on a phenomenon • combine aspects of the other strategies

FIGURE 3 Strategy differences part 2. (Denscompe 2010, 6)

As can be seen, the mixed methods suit this kind of work best. The mixed method allows the researcher to combine strategy and methods from different strategies.

3.2 Quantitative

Quantitative research is used in the thesis as a main research method. As described in Davies's book the blanket term ´quantitative research´ conceals the fact that, within it, there are two methodologically related but very different approaches: survey research and experimental research. (Davies 2007, 51).

The thesis mainly uses the survey as a method. Quantitative method is chosen based on a variety of factors. One main factor is that the previous pilot study used this method and therefore the previous results can be used as background material. Quantitative methods give the ability to scale to answers and use numerical data in order to gain data from survey.

3.3 Qualitative

Qualitative method is used in the thesis in small sample way. The samples are gathered from workshops with the customers and mainly used as reference or control material. Problem with the qualitative method in thesis is that people tend to either emphasize or underestimate organizational status. Therefore the qualitative method is more of analytic then a surveys form.

The main reason for using qualitative method only for controlling and evaluating the data is pointed out on Davies book. “There is no such thing as objective reality because everything is understood and interpreted through the eyes, ears and brain of analyst from special social context” (Davies 2007, 156)

Yet much can be achieved by using the qualitative method. One key aspect is to gain material from the survey and use that against the workshop analysis. Nevertheless, it might be a problematic to analyze the data from two different methods; however, it will widen the scope.

3.4 Questionnaire

The questionnaire was based on Pilot study. In the questionnaire there are three different question types. The first one is plain Yes or No question, the second is proposition with different values ranging from “Cannot say” to “Yes or completely agree”. The third type was free answers. The third type of questions was also used in qualitative method workshops.

4 CONTINGENCY PLAN ASPECTS USED IN THESIS

The thesis uses some key components from contingency planning that are used to evaluate the state of contingency planning.

The first major component is the Business Impact Analysis, the BIA. Without formal BIA it is not possible to create any kind of contingency planning due the fact that it is not known what systems or components are needed for the business or core activities. The role of the BIA cannot be overestimated. All the preceding planning is based on the BIA and the procedural methods rely on successful and up to date BIA.

Once the BIA is updated and completed the second key aspect is the contingency strategy. This is the first stage of contingency planning where heavy financial and resource decisions are to be made. Similar to information security the contingency planning is always a compromise between the resources and impact. The resources in contingency planning can be divided into three major categories.

- Manpower or personnel resources. These resources include the in-house personnel and 3rd party contractor.
- System resources. These resources include the spare parts, co-locations, replication systems and all ITC components needed for strategy.
- Financial resources. These include both the preventive control of financial resources and the budget for contingency planning itself.

Based on these categories the strategy is formed. Strategy can define the use of 3rd party consultants as backup, roles and responsibilities of personnel and use of co-locations or disaster recovery sites.

The third key aspect is the maintenance of the contingency plan. It is the most crucial part of contingency planning. If the plans are outdated they present a major risk and damage the whole planning. If the BIA changes the contingency plans has to be updated.

The three aspects are easily identified and therefore they form a solid base for the thesis questionnaire. Also, for the market analyzing the strategy part is important as it forms the financial foundation for external resources.

One main aspect for whole thesis is to identify if organizations have succeeded in building contingency plans and also if they have found out the main reason for their plans.

5 Methods for Data Collection

As stated out earlier in the thesis this study uses a mixed method approach as the research strategy.

5.1 Designing the Questionnaire

The questionnaire is based on the pilot study's questionnaire. The key aspects were chosen and maintained also on the new questionnaire. This was carried out in order to create material for analyzing the results.

In addition to original questions, some new ones were also added. These questions were added in order to see how well the current situation is handled by using the tools like KATAKRI and VAHTI.

The questionnaire was built using Webropol tool provided by JAMK University of Applied Sciences. The tool is web-based and very intuitive to use.

All the questions were rewritten into Webropol and the actual questionnaire is attached into the thesis as Appendix II.

5.2 Selecting the Survey Candidates

Survey candidates were chosen from Resolute ISMS Oy client base. The candidates were chosen based on their organization. Initially the client base was split into two parts. Figure 4 shows the structure of surveys candidates.

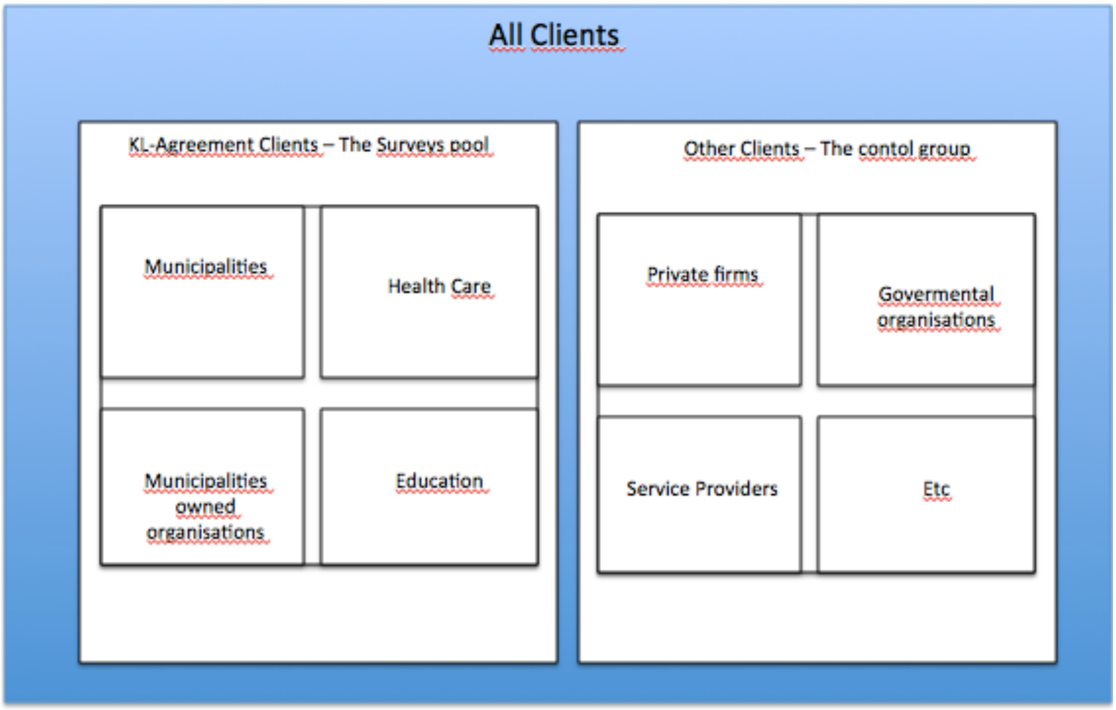

All Clients
KL-Agreement Clients – The Surveys pool
Municipalities
Health Care
Municipalities owned organisations
Education
Other Clients – The contol group
Private firms
Govermental organisations
Service Providers
Etc

FIGURE 4 Structure of survey candidates

After the initial segmentation was done the final candidates were chosen. At this point there were 111 unique organizations. The participating organizations had 292 unique surveys candidates.

The survey was sent to candidates 1st of October 2013. The survey was closed 16th of October. At this time the total amount of survey candidates who had replied was 80.

6 RESULTS

6.1 Quantitative results and analysis

The result part is divided into two different categories. In the first part the results are analysed and presented on a quantitative form and in the second category more qualitative way. Quantitative results are based on the survey as described and the qualitative part is based on the workshops and actual customer data.

The survey results are presented here. Due the nature of the survey some questions are analysed against the so-called reference group and some questions results are only presented.

The N for replicants is 80. The distribution of candidates based on the organization is presented on Table 1. The answer rate for surveys was 27.3%. For the Survey pool the N=48 and for the control group the N=32.

TABLE 1. Distribution of survey candidates based on the organization.

	Organization	**%**
Municipality or City	26	32.50 %
The municipality or city-owned enterprise	5	6.25 %
Health Care organization	1	1.25 %
Govermental Entity	24	30.00 %
Educational Entity	16	20.00 %
Enterprise	8	10.00 %

Table 1 shows that the majority of the candidates who had replied to the survey were from public sector. The distribution between the survey pool and the control group was 48 answers to the surveys pool and 32 answers to the control group.

The questionnaire was sent to different personnel groups. The distribution of candidate's organisational position is presented on Table 2. The majority of candidates were on expert or specialist level as expected. Yet it can be seen that the distribution is very uniform and gives a solid view for all organizational levels.

TABLE 2. Distribution of organizational positions

	Organizational Position of Survey Candidate	**%**
Executives or Directors	10	12.50 %
Middle Managers / Team Leaders	20	25.00 %
Experts or Subject Matter Specialists	47	58.75 %
Other	3	3.75 %

If the distribution were compared to normal organization, the survey pool would create a medium-sized enterprise focused on professional services. This actually describes a normal ICT-organization in Finnish public sector.

Figure 5 presents how organizations produce their ICT-services.

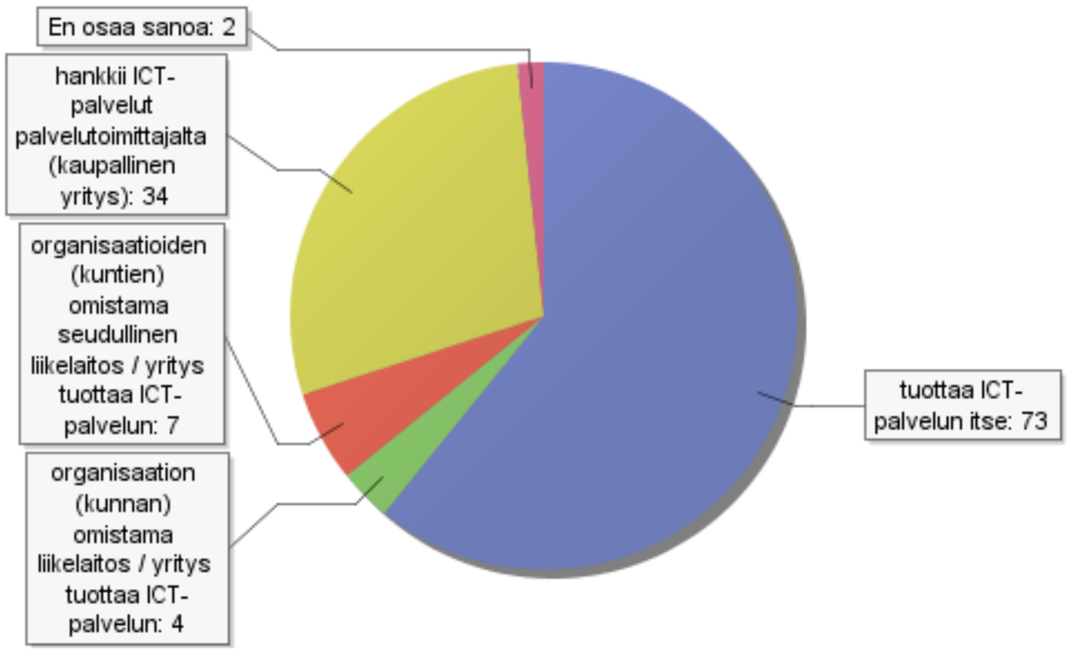


FIGURE 5. ICT Services

The majority of organizations produce their ICT in mixed ways, probably based on the ICT service. The amount of outsourcing is actually quite low.

The use of external auditing is presented in general and then split into survey group and control group. Table 3 presents the general data.

TABLE 3. Use of external consulting in general

	YES	NO	Total	Average
Has your organization used by third parties ICT preparedness planning?	31	49	80	1.612
Has your organization used by third parties ICT audits?	57	23	80	1.287

In general, less than a half has used external consulting on contingency planning; however, over a half has used external help or consulting on audits. The auditing process explains this; however, it also shows that the need for external consulting for planning is present in the current market in general.

Table 4 shows the actual municipalities as a survey group.

TABLE 4. Use of External consulting, survey pool

	YES	NO	Total	Average
Has your organization used ICT preparedness planning produced by third parties ?	11	37	48	1.770
Has your organization used ICT audits organized by third parties?	30	18	48	1.375

In the survey pool results differ from the general result and from the control group presented in Table 5. There is a minor standard variation on the result; however, the trend can be seen. The control group uses external help also during the contingency planning while the survey pool does not.

Table 5 shows the control group.

TABLE 5. Use of External consulting, survey pool

	YES	NO	Total	Average
Has your organization used ICT preparedness planning carried out by third parties?	20	12	32	1.375
Has your organization used ICT audits provided by third parties?	27	5	32	1.156

In the survey pool the results are very similar. There is some minor standard variation on the result; however, the trend can be seen. Also, the control group is much more active on auditing the ICT-services.

For services and ICT-infrastructure the questions were asked by giving a sliding answer. The answers were based on values from 0-5, ranging from 0 as in cannot not say to number 5 as in Yes or all. Figure 6 shows the piled answers for ICT services and infrastructure.

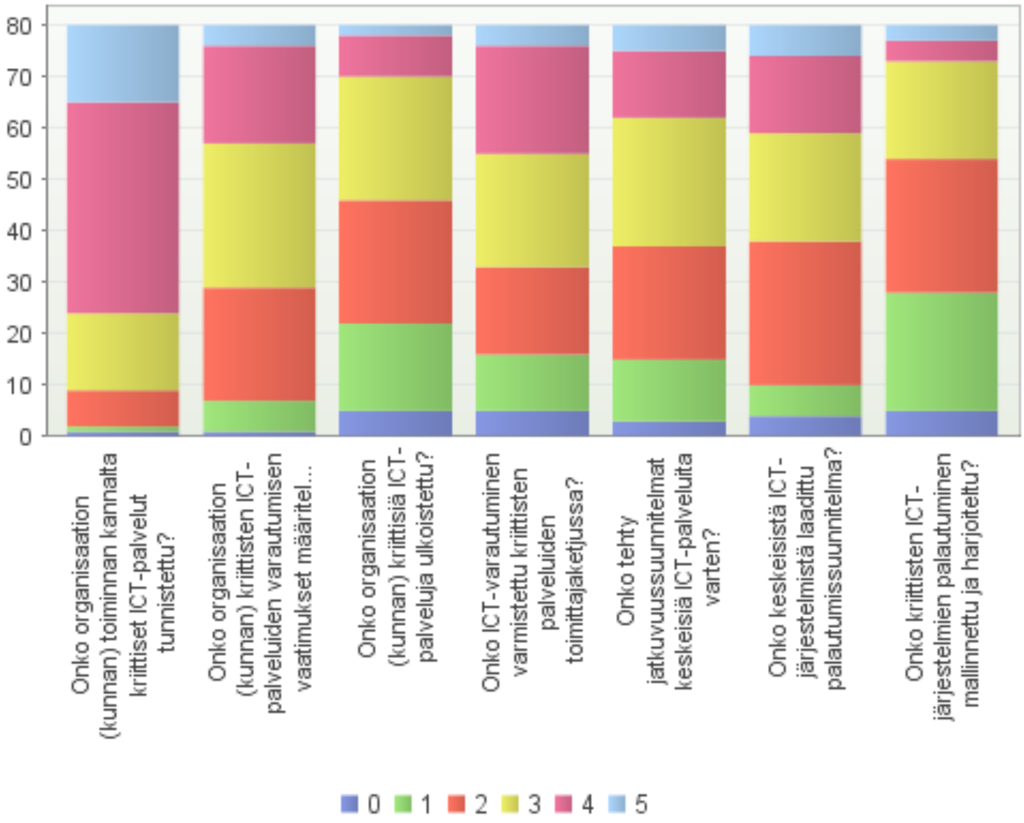


FIGURE 6. ICT Services and Infrastructure

The most significant area is the main answer. There are some variables that are very interesting. The first column shows the results for identifying the critical ICT services.

This is a mandatory component for BIA analysis and ICT contingency planning. The majority of the candidates has chosen to answer in the minimum way. This means that organizations have very little knowledge or understanding about their own ICT systems.

The second interesting variable is the sixth column. That column contains the result for whether the ICT contingency plans are deployed. This is also answered in a minimum way.

Figure 7 indicates the question for the survey group. This figure indicates that the results are even more dispersed.

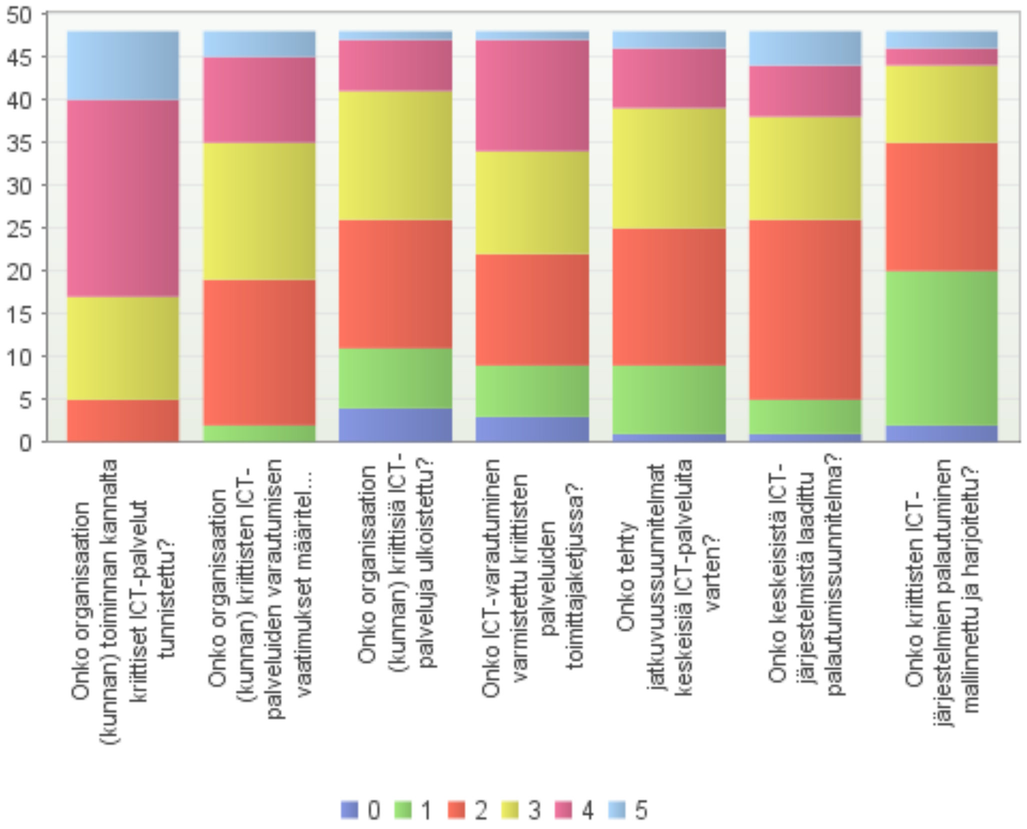
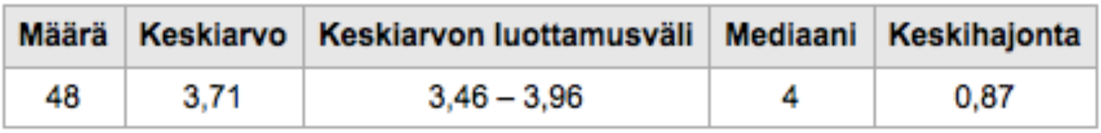


FIGURE 7. ICT Services and Infrastructure - Survey group

In the survey pool the candidates find it a little easier to identify the critical ICT services; however, at the same time the actual ICT contingency is deployed in lesser way. Statistical analysis reveals that the median result is 4. This means that surveys group has identified the critical ICT systems. Figure 8 shows the median analysis.



Määrä	Keskiarvo	Keskiarvon luottamusväli	Mediaani	Keskihajonta
48	3,71	3,46 – 3,96	4	0,87

FIGURE 8. ICT services analysis

Figure 9 presents the ICT contingency results. The candidates were asked to evaluate their ICT contingency and the support material. Figure 8 presents the general data.

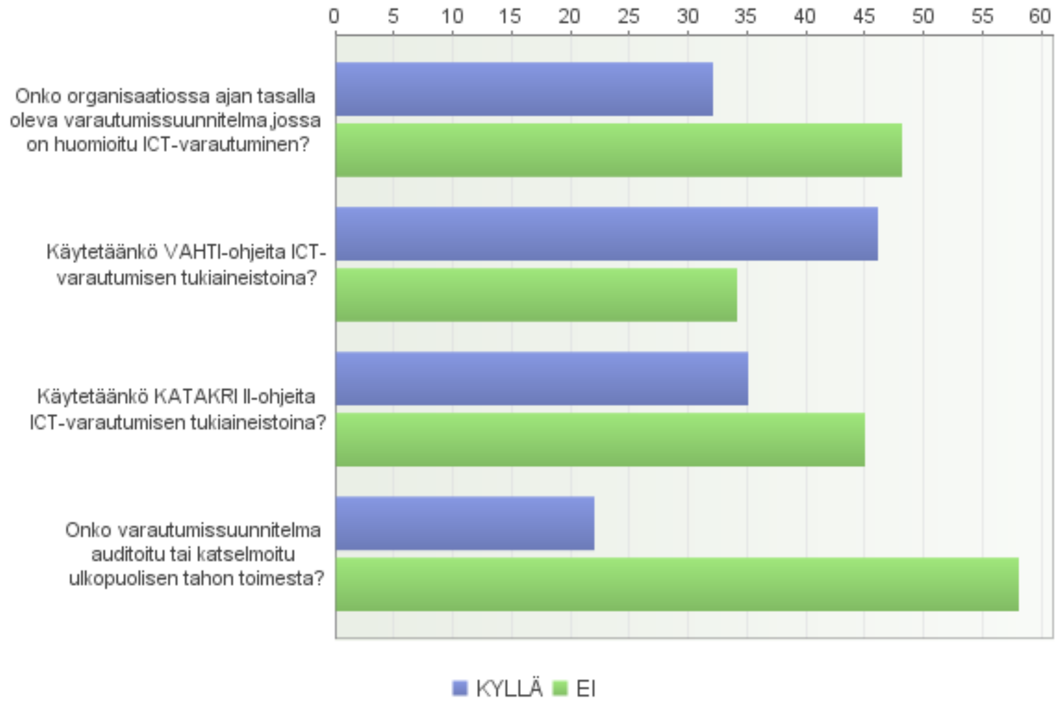


FIGURE 9. ICT Contingency, Question 8, ICT planning

In general, the majority of candidates answered that VAHTI and KATAKRI or either one or the other was used while planning the contingency plans. The majority used VAHTI guidelines in order to build the contingency plans. A disturbing result for this question was the fact that way over a half did not have an up-to-date ICT contingency plan. The question is built in the way that it emphasized the up-to-date wording, however, the result is still surprising. Only a small part of the survey’s candidates had reviewed or audited the ICT contingency plans.

Figure 10 shows the same results for the survey group.

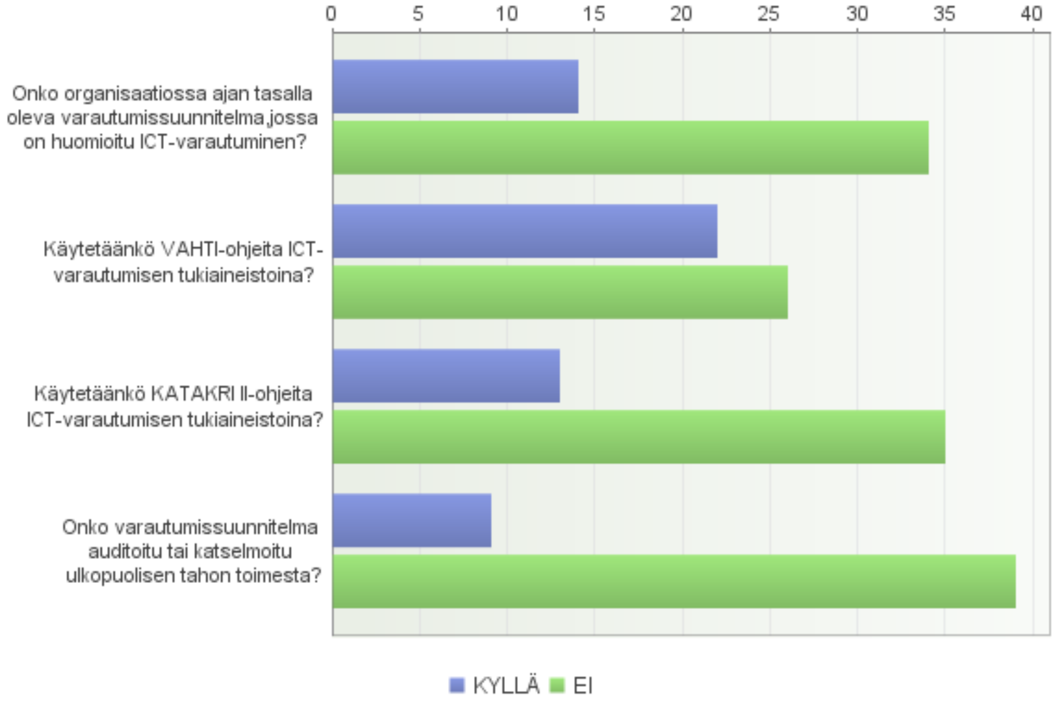


FIGURE 10. ICT Contingency, Question 8, ICT Planning - Survey pool

The figure 11 illustrates that the trend is very similar to the general data. The only major difference is the importance of VAHTI guidance in the planning.

Question 9 on the survey was designed to gather data about organizational awareness and guidance. The results of this question are presented in Figure 10.

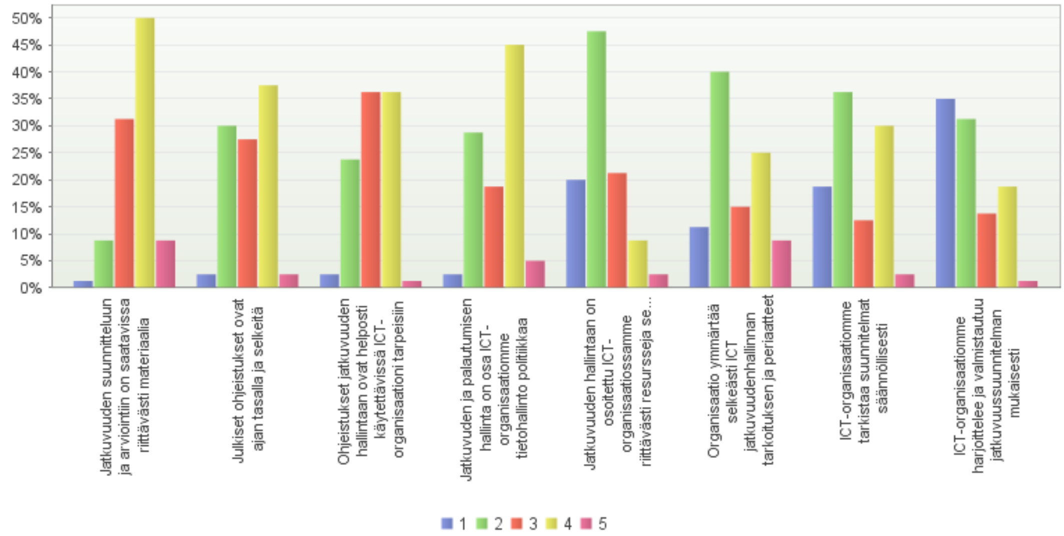


FIGURE 11. ICT Contingency, Question 9, organizational guidance

In general, the organizational guidance and awareness are in a relatively good state.

Table 6 shows the averages on this question based on the general data.

TABLE 6. Average on Question 9

Question	**Mean value**
For the contingency planning and evaluation there is sufficent material available.	3.6
Public guidance is up to date and precise	3.1

Question	Mean value
Continuity and recovery management is part of the ICT organization's information management policy	3.2
Continuity management has shown to ICT organization adequate resources and support.	2.3
The organization clearly understands the purposes and principles of the ICT continuity management	2.8
ICT organization reviews the plans on a regular basis	2.6
ICT organization is practicing and preparing a business continuity plan within regular schedule	2.2

It can be seen from the figure and from the table that guidance from central government and from organization itself is considered to be sufficient. In the organizations the lack of resources for contingency planning is clearly stated. Another aspect is that all candidates indicated the lack of exercise for remediation. It seems that many organizations lack the resources for maintaining the contingency plans. In free text form included into this question many of the candidates described the lack of resources for both planning and maintaining the plans. Figure 12 shows the survey group's answers, which are very similar to all survey candidates' answers.

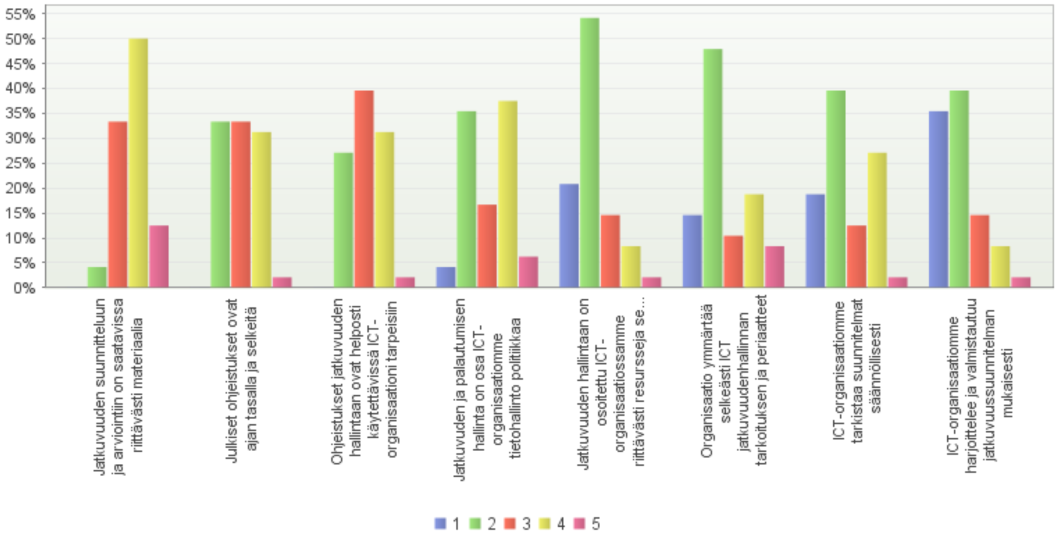


FIGURE 12. ICT Contingency, Question 9, Survey pool

In the question 10 the candidates were asked to evaluate risk management. The results are presented in Figure 13. The questions were Yes or No questions. Figure 13 shows that general data from all candidates does not have much variation and answers are divided quite evenly between all questions.

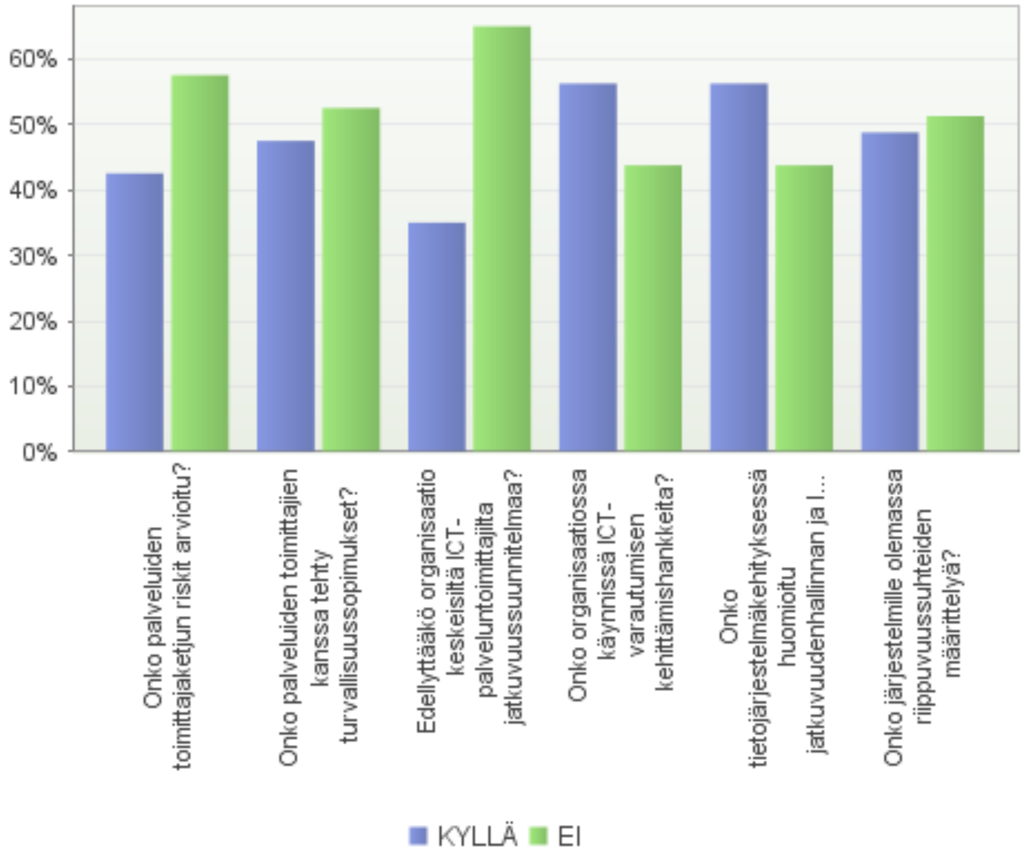


FIGURE 13. Question 10, General data

It seems that in the general data for example ICT Contingency projects are on-going for almost half of the data. Figure 14 shows the survey pool data. The results vary a great deal from general data.

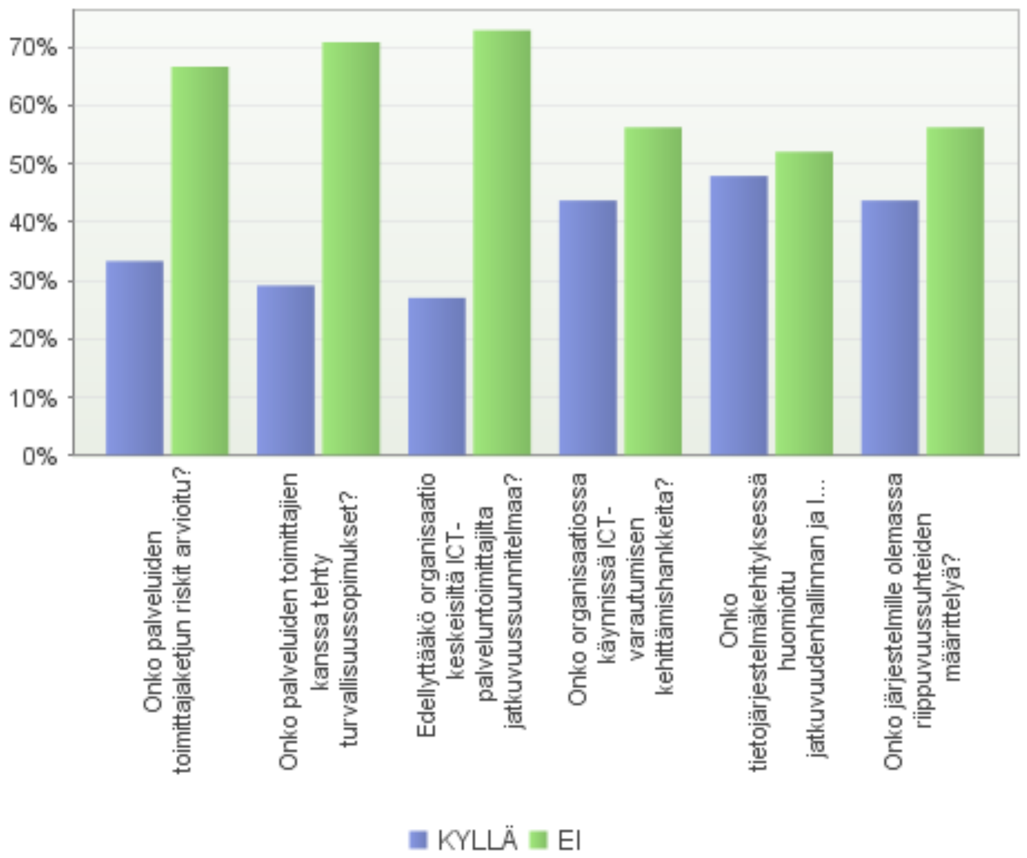


FIGURE 14. Question 10, Survey pool

The results for survey pool are quite different. Contingency projects are on goingly similar to all survey candidates. The major difference is in supplier chain management and requirements. This seems to be taken care of in the control group, however, the survey pool is not considering suppliers' ICT contingency as an important matter. Why this is, it cannot be explained. For the ICT contingency point of view the supplier chain management and risk analysis are becoming more important due to the nature of complexity of systems.

6.2 Profiling Analysis

The results were analysed based on a profile that has two variables. From this profile certain questions were chosen to the analysis. The profile contains two base variables and survey results are compared with this. The profile provides for four different answer groups. Main variables are organizational size and candidate's position on organization.

Organizational distribution was presented on Table 2 earlier. Figure 15 shows the size of the organizations.

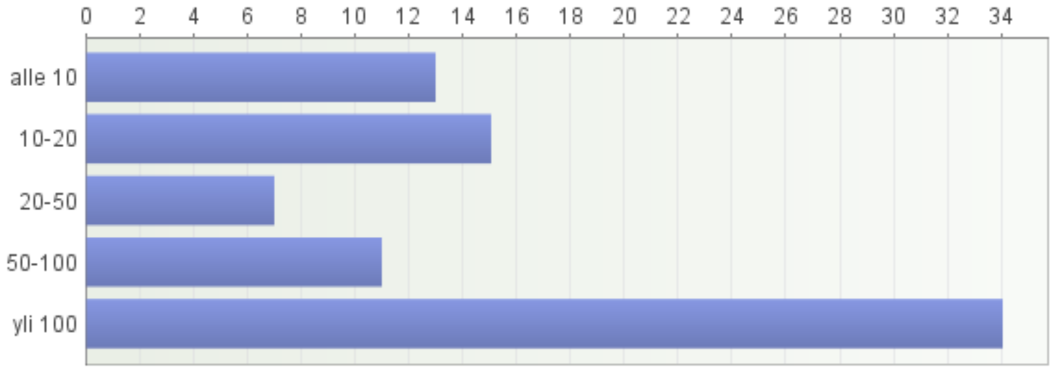


FIGURE 15 Organizational sizes

Organizations with less than 100 employees and organizations 100 or more in personnel were chosen for the construct profile. Then organizational positions are chosen based on the organizational size. Organizational positions are also divided into two groups. The experts and specialists are in one group and managers and directors are in the other group.

While the profile is set in this way it provides a way to analyse results based on organisational size and compare the results from the point of viewof the organizational level.

Different profiles had following N-values

- Less than 100, Experts N=24
- Less than 100, Managers and Directors N=22
- More than 100, Experts N=23
- More than 100, Managers and Directors N=11

Questions chosen for analysis were Question 7, 8 and 9. Question 7 was about Services and ICT-infrastructure. The results are presented on piled bar charts with percentage. The first figure, Figure 16 presents the Experts and Specialists from less than 100 sized organizations.

6.2.1 Question 7 Services and ICT-infrastructure

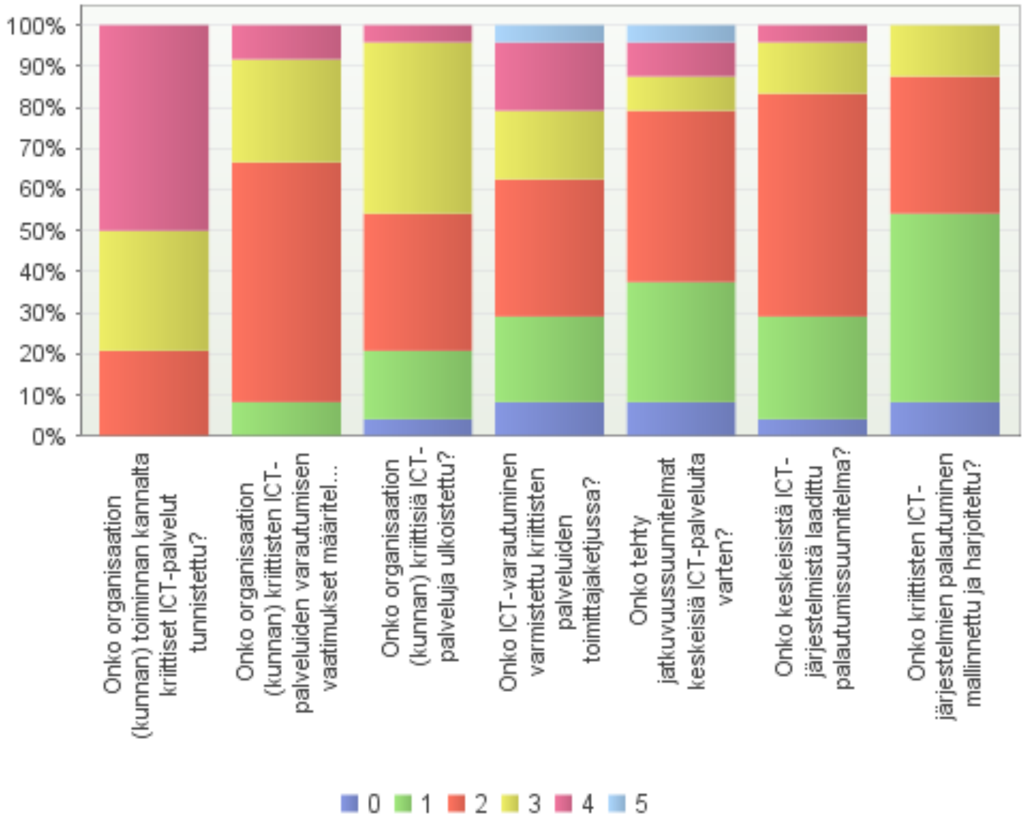


FIGURE 16 Question 7, Less than 100 persons, Experts

Figure 17 presents the data from same organizations but from manager's point of view.

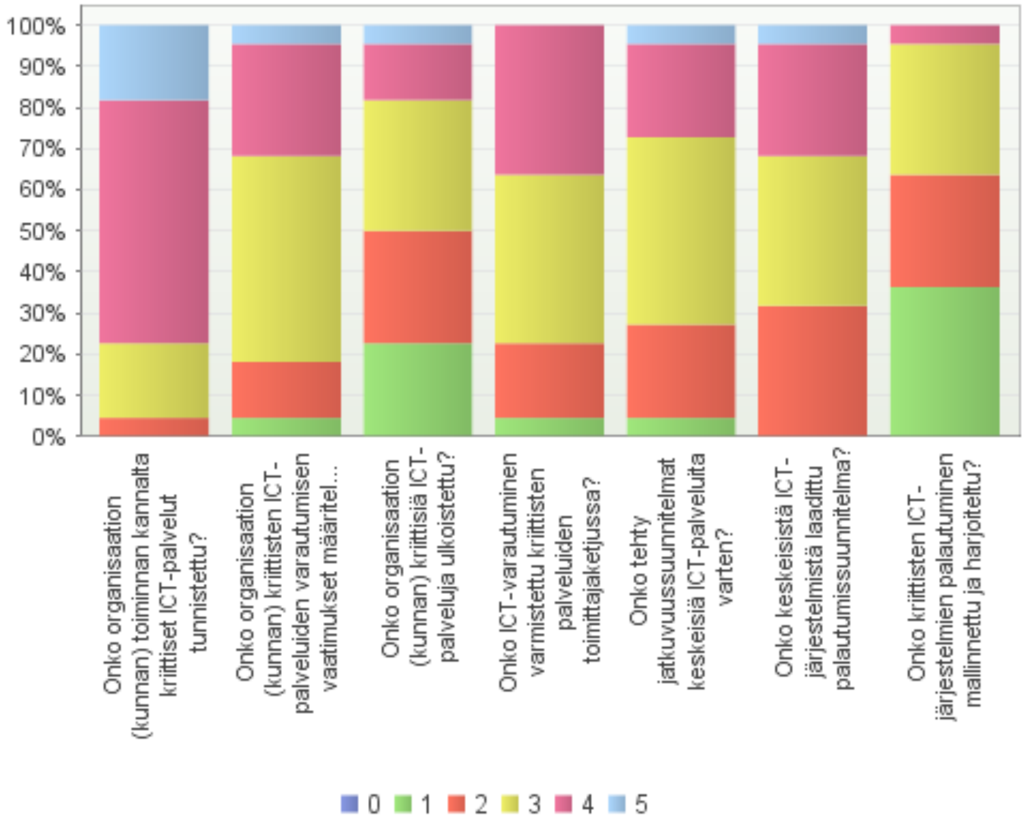


FIGURE 17 Question 7, Less than 100 persons, Managers

The answers were summarized on Table 7, which shows the average on all choices on both experts and managers.

TABLE 7 Average on Question 7 based on organizational size < 100

Question	Experts	Managers
Have the critical ICT-services been identified?	3	4
Have the requirements for ICT continuity been specified by time criticality and the availability of the service?	2	3
Have any critical ICT-services been outsourced?	2	3
Has the ICT-continuity been verified within the supplier chain?	2	3
Is there a continuity plans for mission critical ICT-systems?	2	3
Is there a remediation plan for mission critical ICT-systems?	2	3
Is the remediation modeled and exercised for most critical ICT-systems?	2	2

Table 7 illustrates that the managers seem to perceive the current situation as more positive than the experts.

Figure 18 shows Question 7 from 100+ organizations experts.

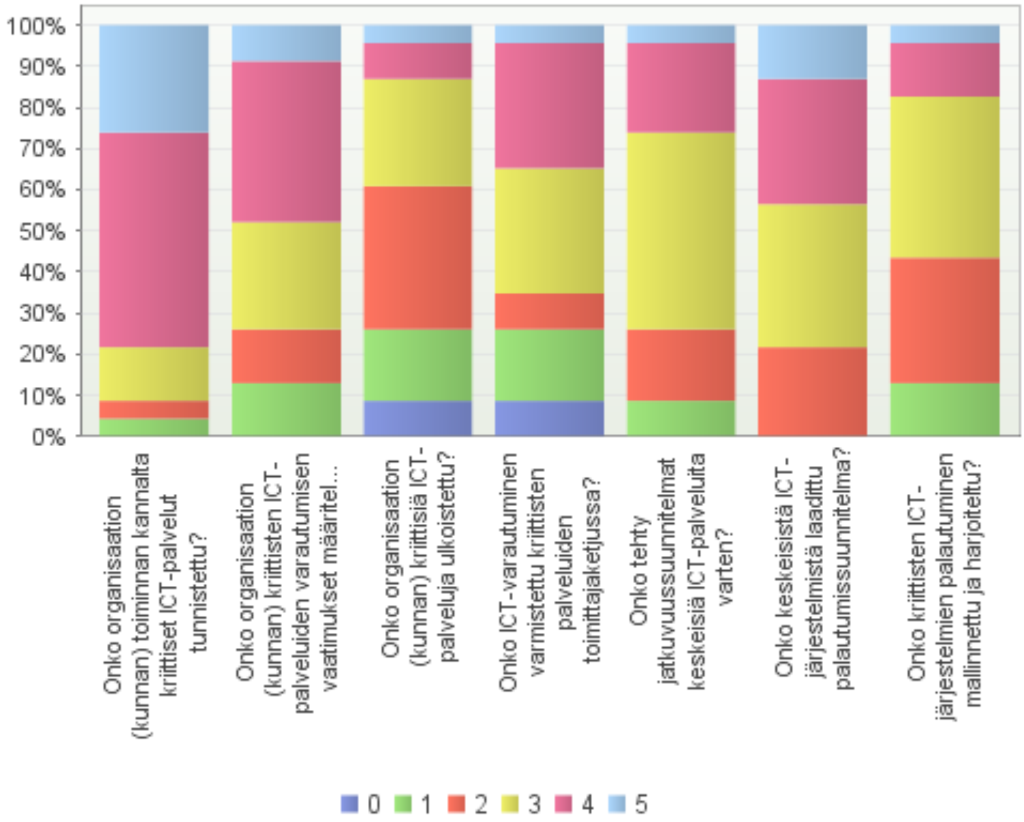


FIGURE 18 Question 7, more 100, Experts

Figure 19 presents the data from the same organizations but from manager’s point of view.

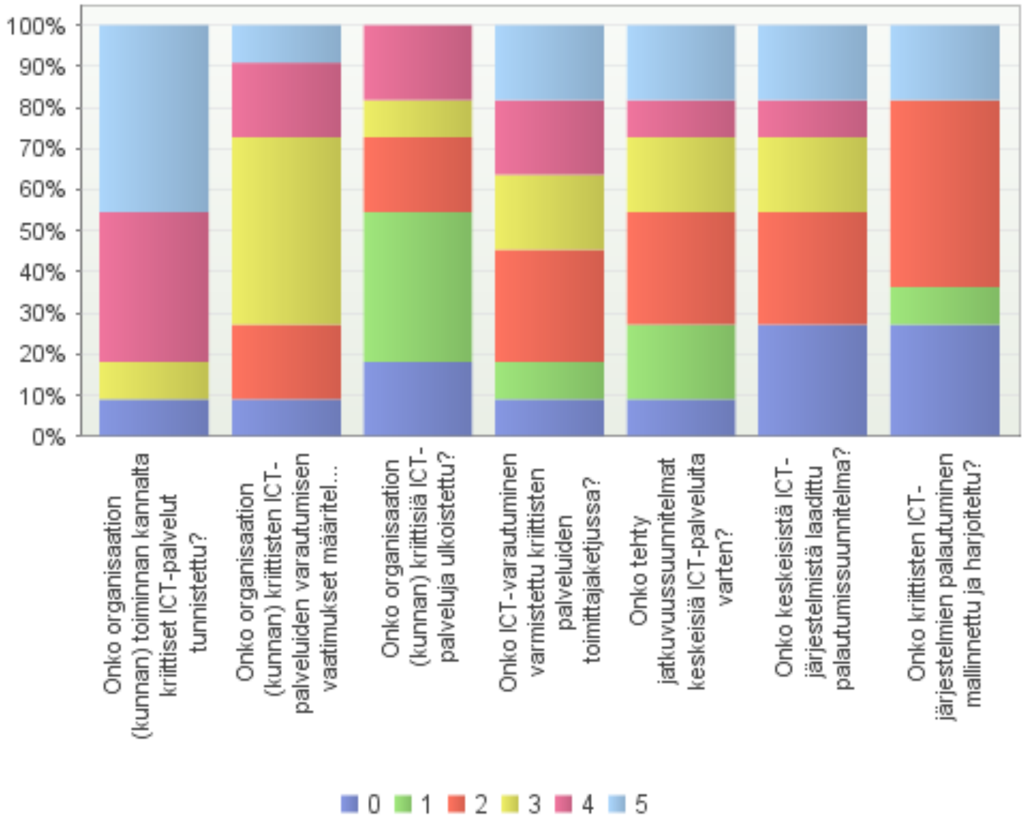


FIGURE 19 Question 7, more than 100, Managers

Answers were summarized on table 8, which shows the average on all choices of both experts and managers

TABLE 8 Average on Question 7 based on organizational size, > 100

Question	Experts	Managers
Have the critical ICT-services been identified?	4	4
Have the requirements for ICT continuity been specified by time criticality and the availability of the service?	3	3
Have any critical ICT-services been outsourced?	2	2
Has the ICT-continuity been verified within the supplier chain?	3	3
Are there continuity plans for mission critical ICT-systems?	3	3
Is there a remediation plan for mission critical ICT-systems?	3	2
Is the remediation plan modeled and exercised for most critical ICT-systems?	3	2

Profiling a summary from question 7 is interesting. In smaller organizations experts and managers see ICT contingency slightly differently. Managers and directors seem to have either a better overall picture or experts are more critical for contingency plans.

For organizations more than 100 persons the experts and managers share the common view. The results are almost identical except for rehearsal of ICT system contingency. Surprisingly, the experts see that remediation phase has been exercised and modelled.

6.2.2 Question 8 ICT Readiness

As for Question 8, the main idea was to see if there are any differences how the organizational levels see the material used in the readiness planning. The results are shown in bar charts and percentage is used on scale. Figure 20 illustrates less than 100-employee organizations and experts.

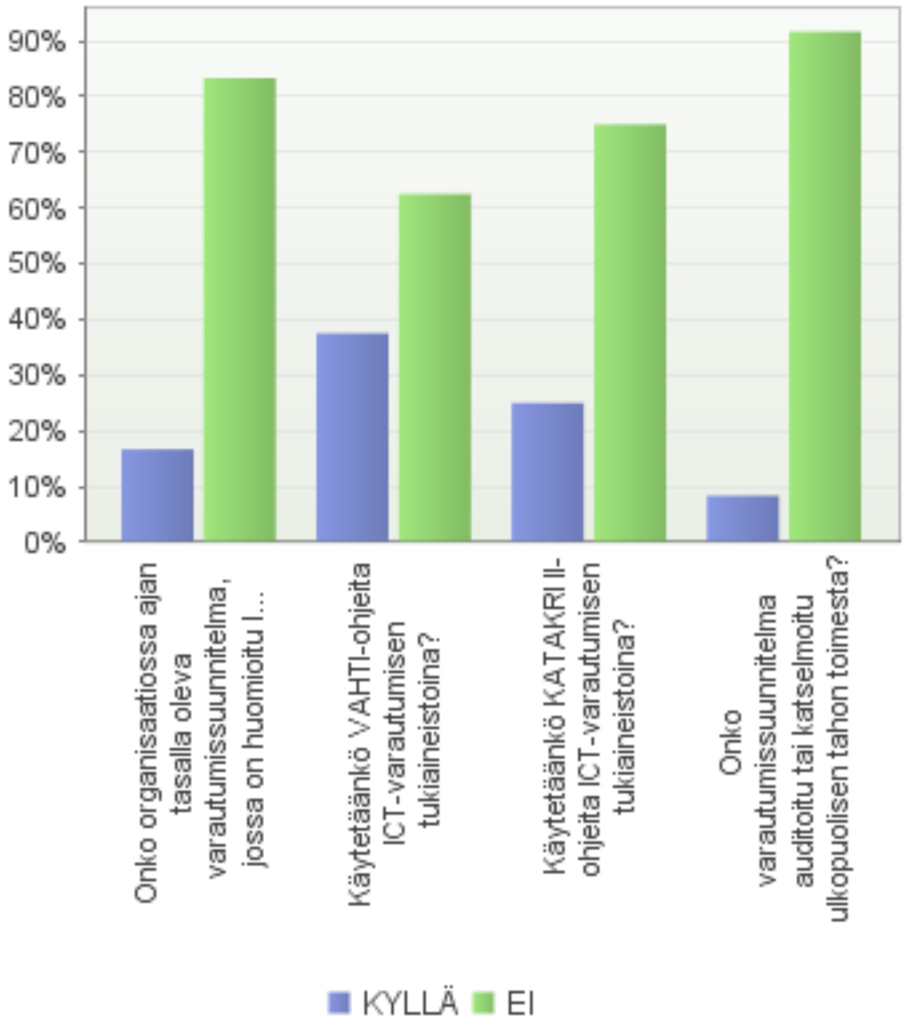


FIGURE 20 Question 8, less than100, experts

The results do not differ from the whole data. Figure 21 shows data for managers with less than 100 employees.

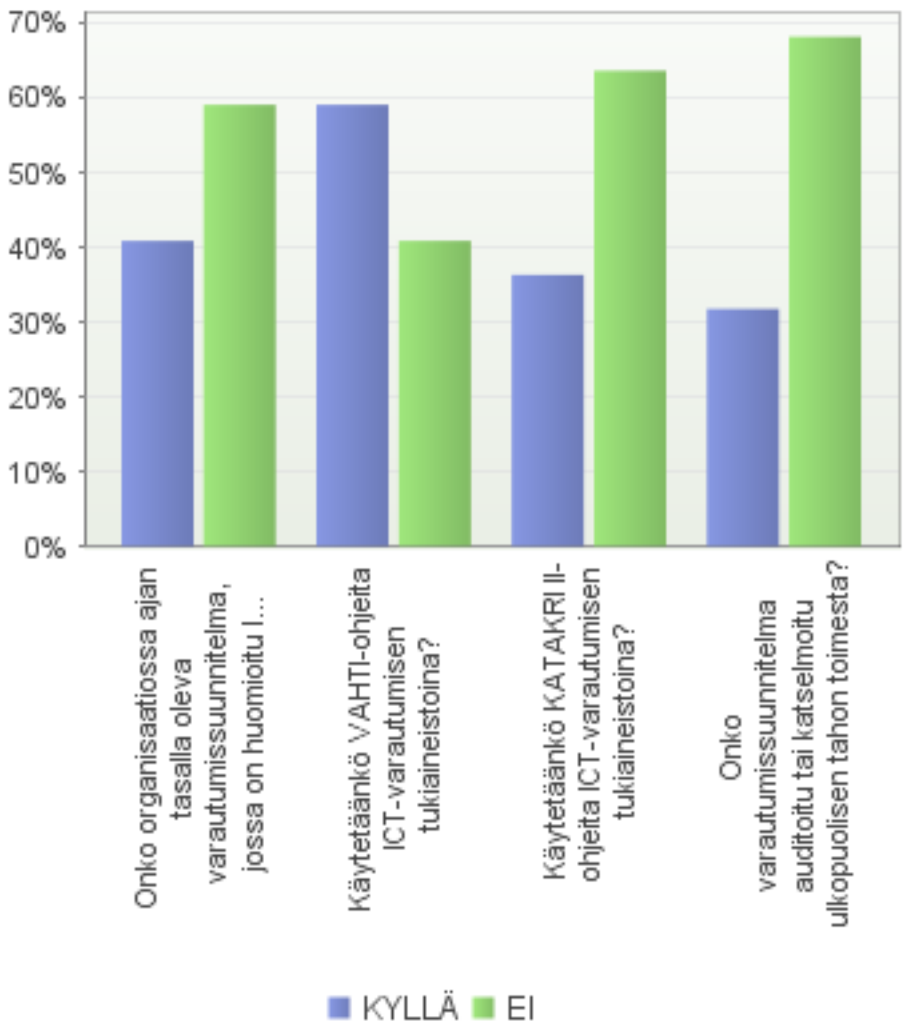


FIGURE 21 Question 8, less than 100, Managers

The largest difference is in the use of the background material. The managerial level has used much more VAHTI and KATAKRI material. This might be explained by lack of information flow. The experts have conducted their work for ICT contingency according to VAHTI and KATAKTRI, however, they do not know it because the overall ICT contingency planning schema is not clear or communicated clearly enough.

Figure 22 shows organizational experts in larger companies.

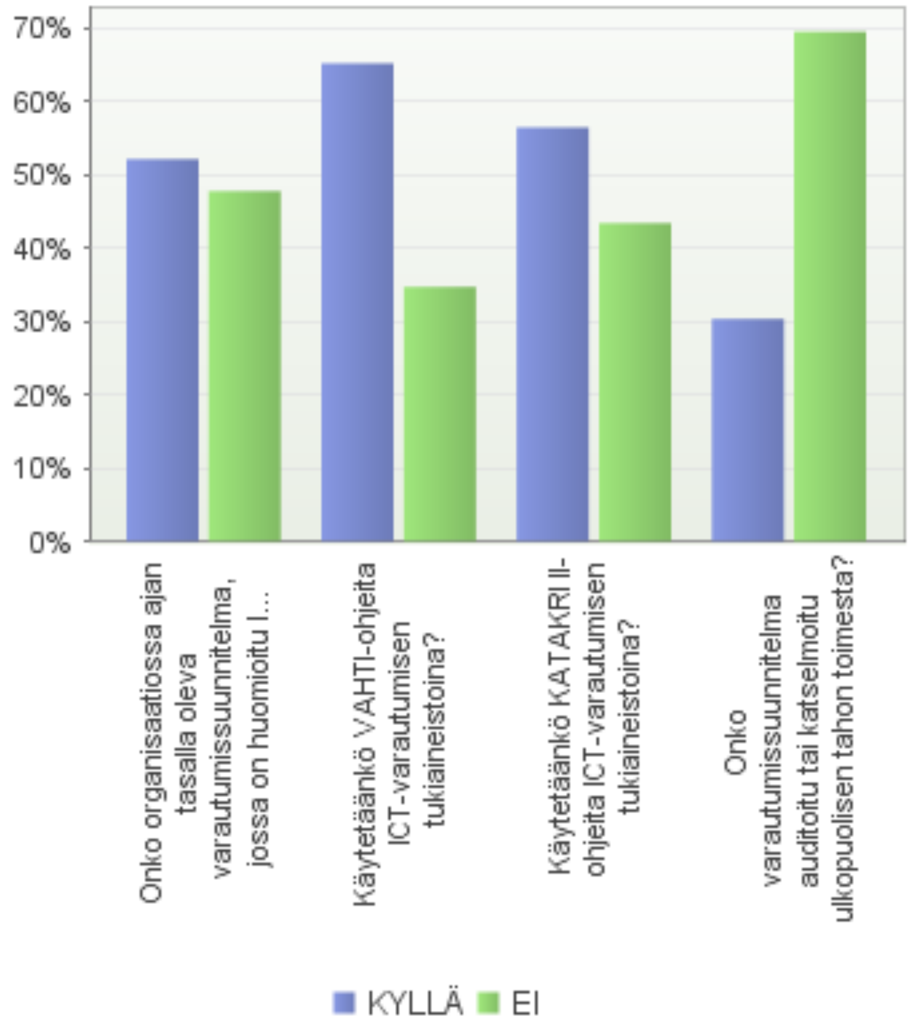


FIGURE 22 Question 22, companies with more than 100 experts

When compared to experts group in a company with less than 100 employees the experts in the larger organizations group use more widely VAHTI or KATAKRI.

Figure 23 has the data from managers with 100 or more employees.

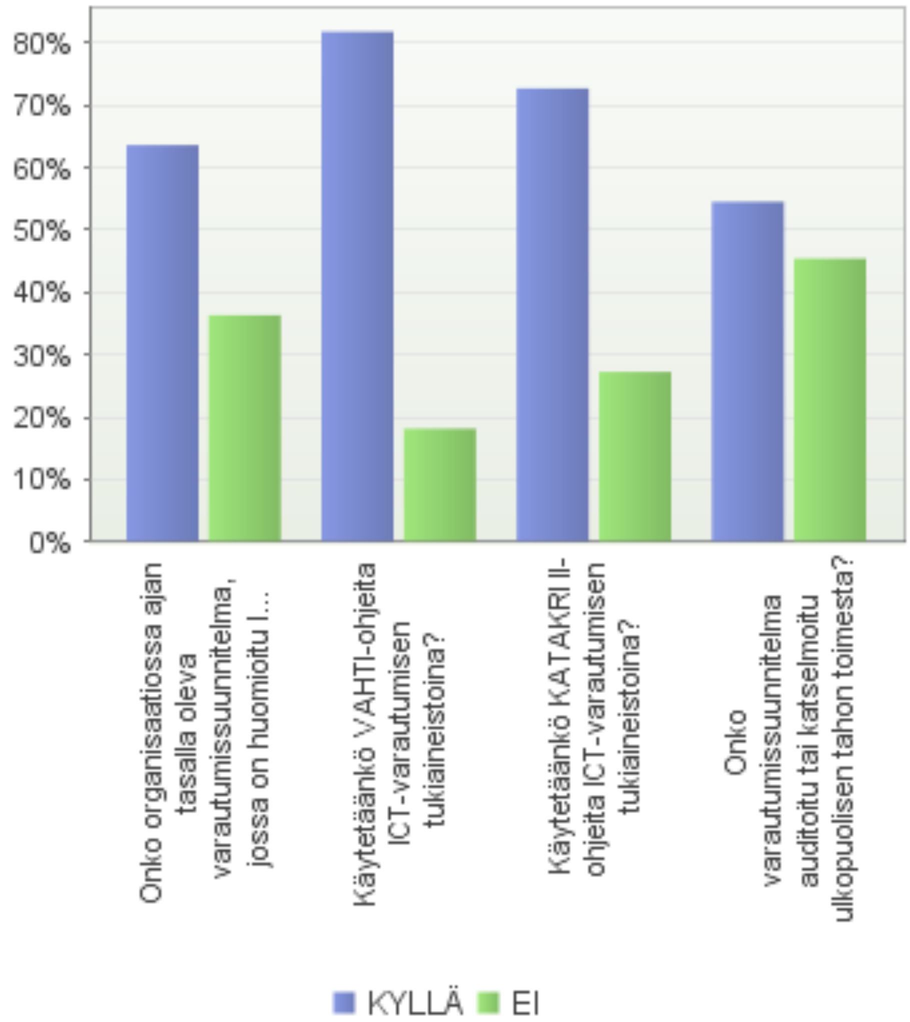


FIGURE 23 Question 8, more than 100, managers

These results vary when compared to profiling groups and also for general data. They can be analysed so that managers and directors in larger organizations are very aware of the governmental regulations, have the resources and the will to implement the ICT contingency and readiness as stated in the official guidance.

6.2.3 Question 9, Information systems and readiness

In this question 9 candidates were given multiple choices to answer based on their readiness level.

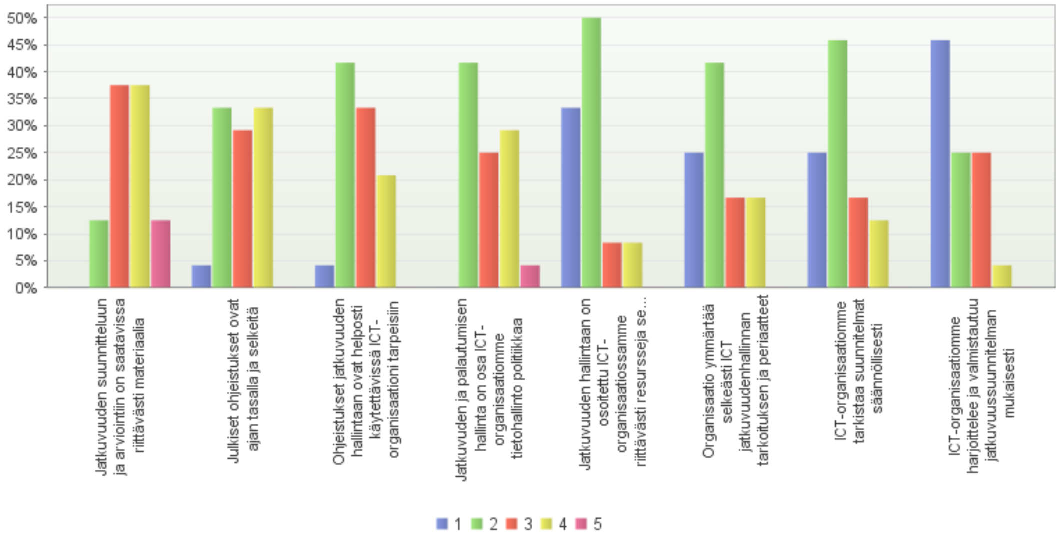


FIGURE 24 Question 9, Less than 100, Experts

The results show very clearly that experts in small organizations feel that that lack of resources is the main reason for ICT contingency gap. Figure 25 shows the managers’ answers.

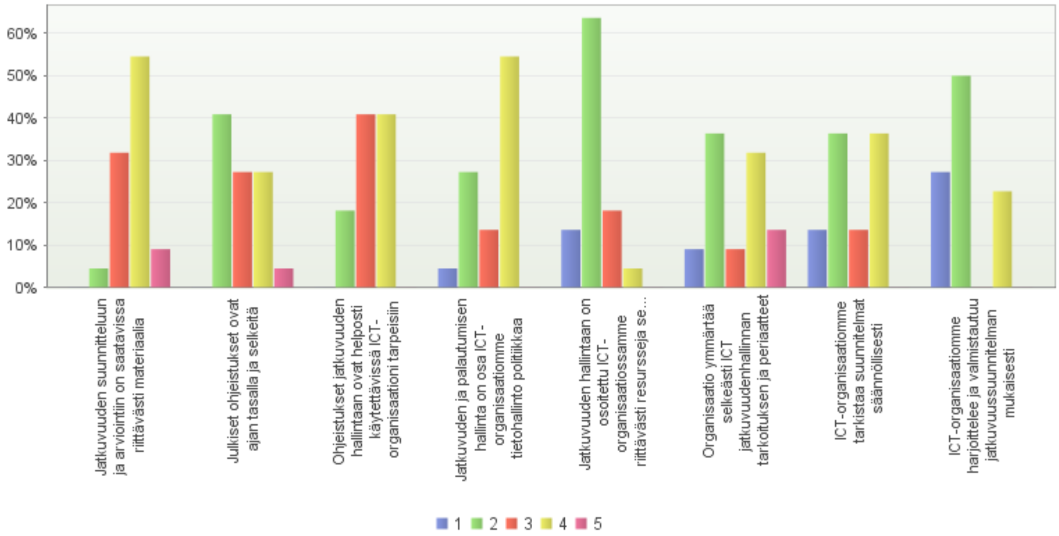


FIGURE 25 Question 9, less than 100 employees in the company, Managers

Managers feel much like the experts. It can be seen clearly that the major difference is on the ICT policy question. Managers feel that ICT contingency is a clear and major point of organizational policy, the experts, however, have a different view. In larger organizations the situation is a bit complex. Figure 26 shows the experts' opinions.

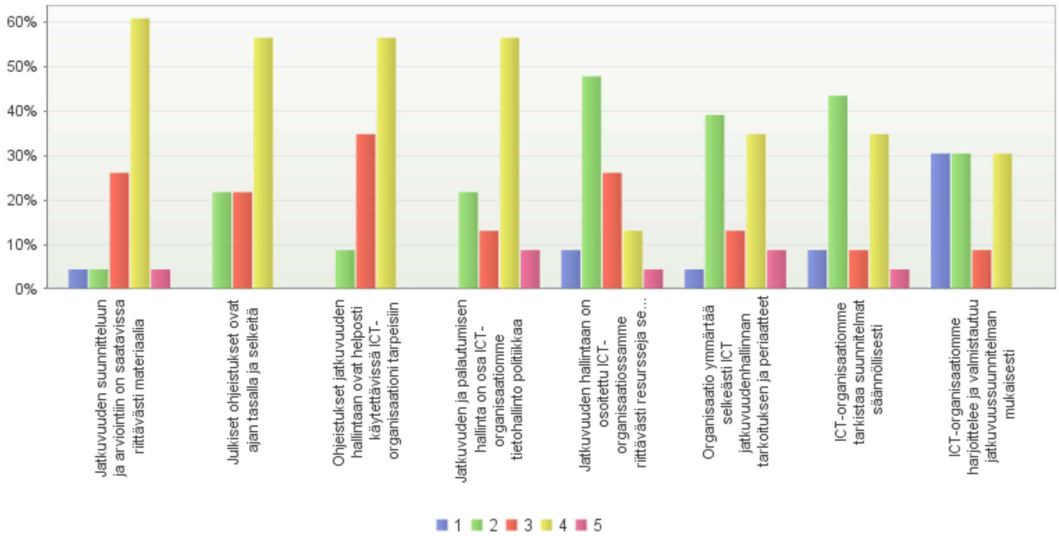


FIGURE 26 Question 9, companies with more than 100 employees, Experts' views

The experts feel that they have enough material and the guidance is clear and precise for their needs. This differs largely from smaller organizations, which might be due to the fact that larger organizations are more governmental entities and, therefore the experts need to use and know the governmental guidance better than experts in smaller organizations. Figure 27 presents the managerial view in larger organizations.

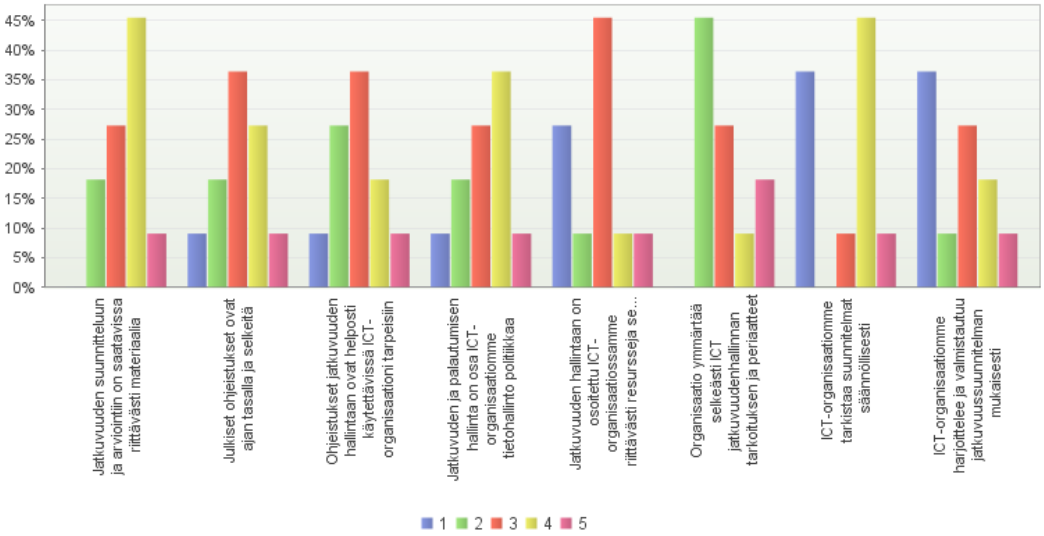


FIGURE 27 Question 9, more than 100 employees in the company, Managers

The managerial staffs see the situation slightly differently. It can be seen that the guidance from VAHTI and KATAKRI might be more technical than administrative. This would conclude the results, as they differ quite largely in the guidance part. Yet, it can be seen managers feel that enough resources are allocated for ICT contingency, and reviews and rehearsals are adequate.

Table 9 summarizes the averages on profiles.

TABLE 9 Question 9, averages on answers

	<100 Experts	<100 Managers	>100 Experts	>100 Managers
For the contingency planning and evaluation there is sufficient availability of material	3.5	3.7	3.6	3.5
Public guidance is up to date and precise	2.9	3.0	3.4	3.1
Contingency guidelines are readily available on the ICT needs of the organization	2.7	3.2	3.5	2.9
Continuity and recovery management is part of the ICT organization's information management policy	3,0	3.2	3.5	3.2
Continuity management has been shown to ICT organization with adequate resources and support.	1.9	2.1	2.6	2.6
The organization clearly understands the purposes and principles of the ICT continuity management	2.3	3.1	3.0	3.0
ICT organization reviews the plans on a regular basis	2.2	2.7	2.8	2.9
ICT organization is practicing and preparing a business continuity plan within regular schedule	1.9	2.2	2.4	2.6

Table 6 presents the mean average for the complete survey. The profiled answers are quite similar; however, it can be seen that different organization sizes and organizational positions cause the tendency to see matters differently.

6.3 Qualitative analysis of results

Based on the workshops and reviews of the actual contingency plans the quantitative results are considered credible. The major difference between the questionnaire and workshop is the way in which data is collected.
On the questionnaire the questions are mainly asked on the basis “is there or how do you see”. This approach works fine on the questionnaire; however, the workshop and reviews actually gave a better insight to the actual level of contingency and ICT-planning.

During the workshops it became very clear that organizations had very different views on BIA-analysis and contingency planning. Therefore it could be stated be that the qualitative part gives somewhat misguided results due to the fact that contingency planning varies a great deal among the organizations.

During the workshops organizations were asked about their plans and the plans were reviewed. Some aspects were not written into the plans themselves but were present in the other material. This proved that many organizations might have their contingency planning in a better state than the one they actually can see.

One of the key aspects that was found out during the qualitative data gathering was the disappointment for public guidance and precepts. This was the major complaint because the organizations felt that they were instructed to do plans and guides without any help or advice from the central government.

The majority of the complaints can be verified by analysing the quantitative data. Two main reasons arose from this field. Organizations informed that for example KATAKRI II or VAHTI criteria were not suitable or they could not understand the criteria. Another main complaint was about the scaling and understanding the crisis scenarios. VAHTI and KATAKRI are designed to be tools for contingency and ICT-security planning. Municipalities felt that their contingency and ICT-planning has to start from a different point of view than KATAKRI and VAHTI. For small municipalities the main risks are loss of electricity and telecommunications, not a governmental crisis situation.

Based on that fact many of the answers on Quantitative can present the right point of view.

One of the key points is also the resourcing. This was also confirmed by the qualitative part that the survey pools' answers about lacking resources are correct. Many of the answers gained in both workshops and from the qualitative part of the surveys confirmed that municipalities lack personnel, time and knowledge in order to build, maintain and develop ICT contingency plans.

Governmental guidance was given a poor grade during the workshops. This was based on the complaints and examples given. The lack of a baseline for planning and constantly changing auditing parameters was identified as for both the qualitative and quantitative part. There was no difference between the survey pool and control pool for this part.

6.4 Comparison between Pilot study and thesis

The comparison between the pilot study and thesis was carried out via a qualitative analysis. This was due to the fact that the publication did not contain values about the survey conducted.

The results are very similar in the thesis, as they appear to be into study. The needs for ICT and contingency are similar and the results of the thesis are consistent. Conclusions on the pilot study are that the need for strategy and guidance is significant.

It can be seen that the objective for centralized guidance and strategy are not achieved during the time period between the pilot study and the thesis. The need for general guidance and specific detailed implementation scenarios is identified.

For the service providers the current situation is still very hard. The lack of centralized guidance and auditing has generated a situation where ICT contingency planning is individual for every customer based on their situation. This makes the ICT contingency planning difficult for both the customer and service provider.

7 CONCLUSIONS

Based on the material and data gathered, the state of readiness and contingency planning is very dispersed. There are organizations that have the necessary resources in order to plan, build and maintain up-dated plans and materials.

On the other hand, there are organizations that see the importance of contingency planning; however, at the same time they recognize the lack of resources in order to keep up with the constantly changing requirements.

Central government needs to urgently realize the lack of baseline in the whole ICT guidance field. Vertical organizations have to realize the need of co-operation and information sharing. Currently it seems that many organizations do not have contacts outside their own organization in order to review or audit the contingency material. The use of external auditing should be made easier and it should involve both external consults and subject matter experts from similar organizations.

The need for common guidance and best practises is eminent. This includes both, the general guidelines and the detailed examples. KATAKRI and VAHTI are a good way to start, however, it seems that both of those are way too complex and hard to understand.

The auditors and auditing entities should be better trained and organized so that single audit could give credit for multiple instances.

Readiness planning and contingency can also described in the way the comic Dilbert does it. Figure 15 shows one approach to this issue.

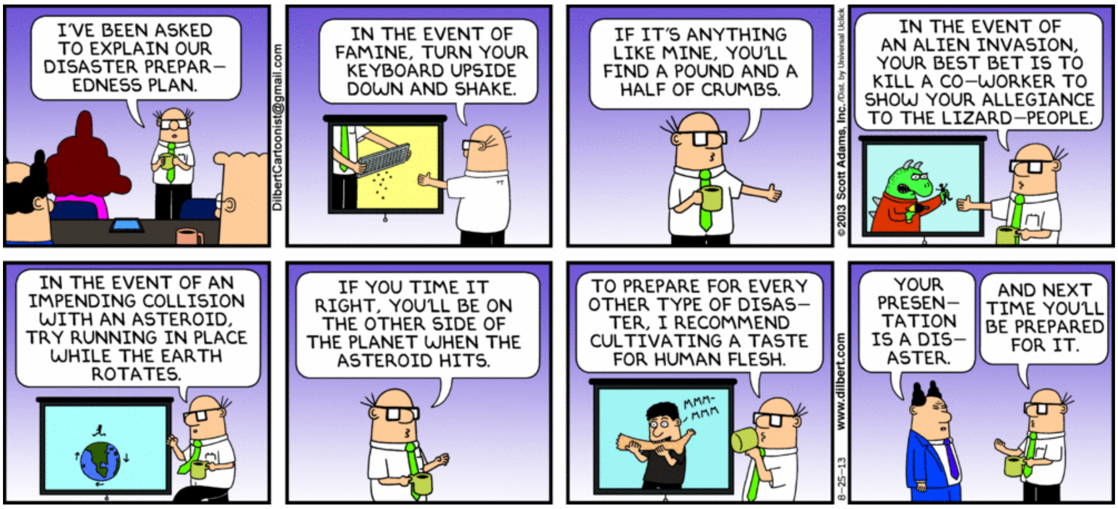

I'VE BEEN ASKED TO EXPLAIN OUR DISASTER PREPAR-EDNESS PLAN.
IN THE EVENT OF FAMINE, TURN YOUR KEYBOARD UPSIDE DOWN AND SHAKE.
IF IT'S ANYTHING LIKE MINE, YOU'LL FIND A POUND AND A HALF OF CRUMBS.
IN THE EVENT OF AN ALIEN INVASION, YOUR BEST BET IS TO KILL A CO-WORKER TO SHOW YOUR ALLEGIANCE TO THE LIZARD-PEOPLE.
IN THE EVENT OF AN IMPENDING COLLISION WITH AN ASTEROID, TRY RUNNING IN PLACE WHILE THE EARTH ROTATES.
IF YOU TIME IT RIGHT, YOU'LL BE ON THE OTHER SIDE OF THE PLANET WHEN THE ASTEROID HITS.
TO PREPARE FOR EVERY OTHER TYPE OF DISAS-TER, I RECOMMEND CULTIVATING A TASTE FOR HUMAN FLESH.
MMM-MMM
YOUR PRESEN-TATION IS A DIS-ASTER.
AND NEXT TIME YOU'LL BE PREPARED FOR IT.
DilbertCartoonist@gmail.com
©2013 Scott Adams, Inc./Dist. by Universal Uclick
www.dilbert.com
8-25-13

FIGURE 28. Dilbert view of point (Dilbert, 2013)

As Wally points out, the base lining of the readiness and contingency plan is important. It can even be a disaster; however, next time we know it and are better prepared.

REFERENCES

Bowen P., Gallup, D., Lynes D., Phillips, A Swanson, M., NIST Special Publication 800-34 Rev 1. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Denscombe, Martyn. 2010 Good Research Guide : For small-scale social research projects (4th Edition). Berkshire, GBR: McGraw-Hill Professional Publishing . http://site.ebrary.com/lib/jyvaskyla/Doc?id=10441962&ppg=257

Davies, Martin Brett. 2007 Doing a Successful Research Project ; Using Qualitative or Quantitative Methods. New York: Palgrave Macmillian, 2007

Dilbert, web pages
http://dilbert.com/strips/comic/2013-08-25/ 25.8.2013

Hansel web pages
http://www.hansel.fi/en 16.7.2013

Hansel web pages - company
http://www.hansel.fi/en/company 16.7.2013

Hankerekisteri web pages
http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iId=12914 30.7.2013

ISO/IEEC 27002:2005 Abstract
http://www.iso.org/iso/catalogue_detail?csnumber=50297

ISO/IEEC 27002:2005

INTERNATIONAL STANDARD ISO/IEC 17799:2005. 2007. ISO/IEEC 27002:2005, Technical Corrigendum 1 to ISO/IEC 17799:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1,
Information technology, Subcommittee SC 27, IT Security techniques. 2007

Kansallinen turvallisuusauditointikriteeristö (KATAKRI)
http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_%28katakri%29 referred to 30.7.2013

KL-Kuntahankinnat web pages
http://www.kuntahankinnat.fi/en 25.8.2013

Pilot Study for ICT contingency planning
ICT-varautumisen esitutkimushanke. 2011. Kuntien ICT-varautuminen. Valtiovarainministeriön julkaisuja 5/2011. HELSINKI: Valtionvarainministeriö. referred to 21.7.2013
https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/03_kunnat/20110118Kuntie/Kuntien_ICT-varautuminen.pdf

Swanson, A., 2010, NIST SP 800-34, Revision 1 – Contingency Planning Guide for Federal Information Systems, referred to 9.11.2013,
http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations/2-2b-contingency-planning-swanson-nist.pdf

VAHTI’s Annual Resport 2012
VAHTIn toimintakertomus 2012, VAHTI 3/2013. VAHTI 3/2013. HELSINKI: Valtiovarainministeriö.
referred to 30.7.2013
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20130603VAHTIn/name.jsp

APPENDIX 1 - Pilot Study for ICT contingency planning – Original Questionnaire

Kyselyn taustamuuttujiin liittyvät kysymykset olivat:

— kunnan asukasluku

— työntekijöiden määrä

— tietohallinto-organisaation koko

— kunnan varautumisorganisaation miehitys

— tietojärjestelmien lukumäärä

— kunnan varautumistoiminnan resursointi

Organisaatio (esim. kunta) hankkii keskeiset ICT-palvelut seuraavasti:

A= tuottaa ICT-palvelun itse

B= organisaation (kunnan) omistama liikelaitos / yritys tuottaa ICT-palvelun

C= organisaatioiden (kuntien) omistama seudullinen liikelaitos / yritys tuottaa ICT-palvelun

D= hankkii ICT-palvelut palvelutoimittajalta (kaupallinen yritys)

E= en osaa sanoa

Johtaminen

1. Onko ICT-varautuminen osa kunnan (organisaation) hallinnonalojen toiminnan ja talouden suunnittelun prosessia, vuosikelloa (tavoitteiden asettaminen, resurssit, mittarit, raportointi)?

2. Huomioidaako ICT-varautumisessa YETTS:n uhkakuvat?

3. Ovatko ICT-palveluiden ohjausmekanismit selkeät ja toimivat häiriötilanteissa?

4. Onko kunnassa (organisaatiossa) ajan tasalla oleva varautumissuunnitelma, jossa on huomioitu ICT-varautuminen?

5. Onko kunnan ICT -varautumisen tilannekuva selkeä kunnan toiminnan kannalta?

6. Käytetäänkö VAHTI-ohjeita ICT-varautumisen tukiaineistoina?

7. Kunnan ICT-varautuminen on jätetty yksinomaan tietohallinnon vastuulle?

8. Onko kunnan IT-johtaja kunnan johtoryhmän jäsen?

Riskienhallinta ja ICT-varautumisen vaatimukset

1. Asetetaanko kunnassa ICT-varautumiselle riskien arviointiin perustuvat riittävän selkeät kehittämisen tavoitteet?

2. Onko palveluiden toimittajaketjun riskit arvioitu?

3. Onko palveluiden toimittajien kanssa tehty turvallisuussopimukset?

4. Edellyttääkö kunta keskeisiltä ICT-paveluntoimittajilta jatkuvuussuunnitelmaa?

103

5. Onko kriittisten tietojärjestelmäpalveluiden ja ICT-infrastruktuurin tukitoiminnot

tunnistettu ja kuvattu?

Palvelut ja ICT-infrastruktuuri

1. Millä osa-alueilla on kunnan ICT-varautumisessa havaittu puutteita?

2. Onko kunnan (organisaation) toiminnan kannalta kriittiset ICT-palvelut tunnistettu?

3. Onko kunnan (organisaation) kriittisten ICT-palveluiden riippuvuudet muista ICT-palveluista, infrastruktuurista ja esim. julkishallinnon yhteisistä tietojärjestelmistä tunnistettu?

4. Onko kunnan (organisaation) kriittisten ICT-palveluiden varautumisen vaatimukset määritelty aikakriittisyyden ja palvelun saatavuuden mukaan?

5. Onko kunnan (organisaation) kriittisiä ICT-palveluja ulkoistettu?

6. Onko ICT-varautuminen varmistettu kriittisten palveluiden toimittajaketjussa?

7. Onko tehty jatkuvuussuunnitelmat keskeisiä ICT-palveluita varten?

8. Kuinka suuri osuus keskeisistä ICT-palveluista on ulkoistettu?

9. Onko ICT-varautumisen osaamistarpeet tunnistettu?

10. Onko kunnalla valmius ottaa omaan haltuun ulkoistettuja ICT-palveluja YETTS-erityistilanteissa?

11. Koska on viimeksi sopimusosapuolten (eri ICT-palveluntoimittajat) kanssa tarkasteltu sopimuksen toteutumista ja jatkuvuudenhallinnan tarpeita?

12. Huomioidaanko järjestelmähankinnoissa ICT-varautusmisen vaatimukset?

ICT-varautumisen kehittämisen mallit

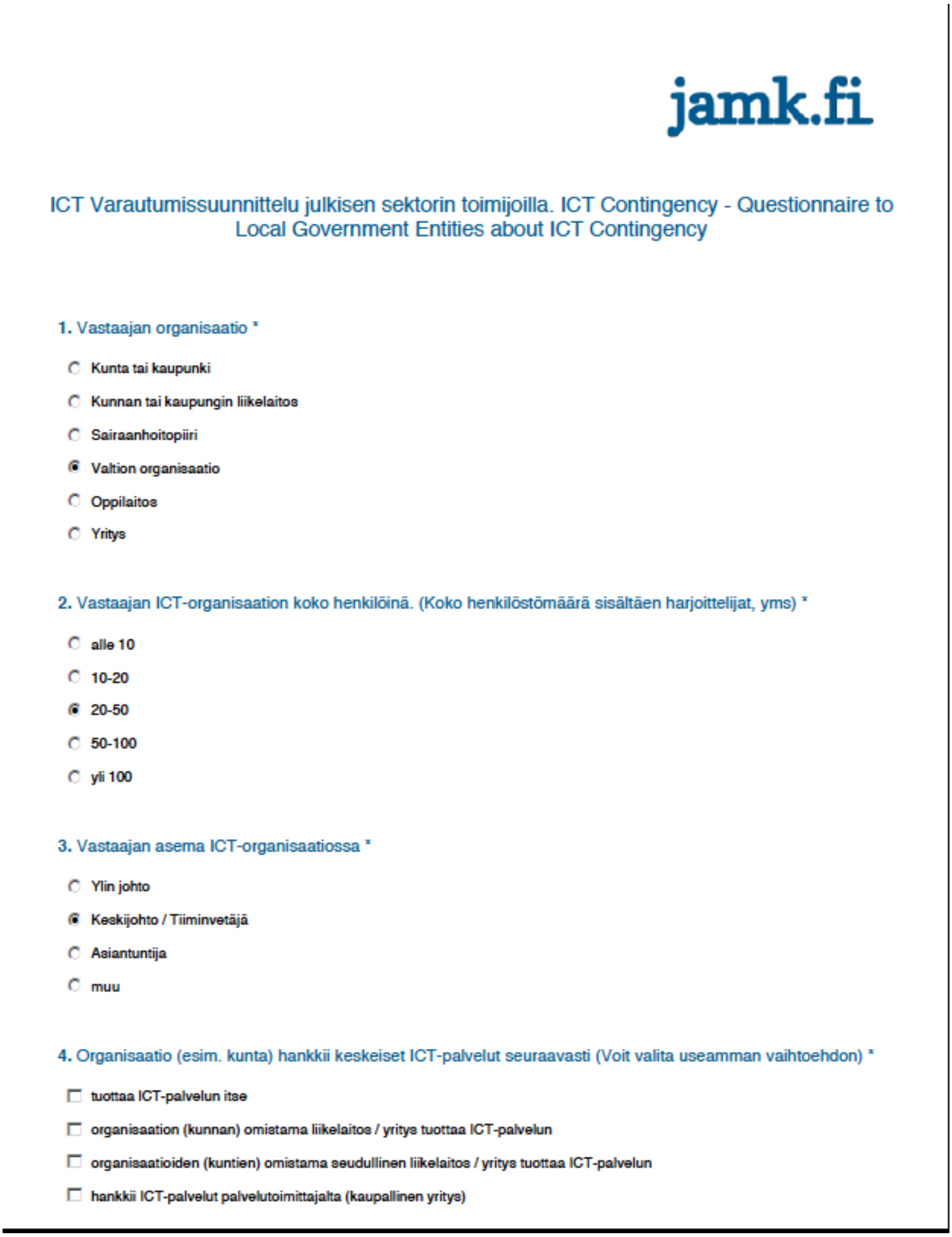
1. Onko kunnassa käynnissä ICT-varautumisen kehittämishankkeita?
2. Käytetäänkö ICT-varautumisen kehittämisessä standardoitua tai parhaisiin käytäntöihin perustuvaa mallia?
3. Onko tietojärjestelmäkehityksessä huomioitu jatkuvuudenhallinnan ja ICT-varautumisen vaatimukset?
4. Soveltuvatko valtionhallinnon ICT-varautumisen vaatimustasot arvionne mukaan kunnan ICT-varautumisen tavoitetasojen perustaksi, mittaamiseen ja kehittämiseksi?
5. Koska viimeksi on kunnan ICT-varautumistoiminta tarkastettu tai sitä on arvioitu?
6. Seurataanko ICT-varautumiseen käytettäviä resursseja?
7. ICT-varautumisen hallinta ja kehittäminen yhdestä palvelupisteestä (kuntarajat ylittävä yhteistyö) tukee YETTS toimeenpanoa?

Jokaiseen kysymykseen sisältyi vapaamuotoinen palaute.

(The Pilot Study, 2011, 102-103)

APPENDIX 2 – Questionnaire for ICT Contingency Planning

The questinnaire was send to participants on 1.10.2013.



jamk.fi

ICT Varautumissuunnittelu julkisen sektorin toimijoilla. ICT Contingency - Questionnaire to Local Government Entities about ICT Contingency

1. Vastaajan organisaatio *

○ Kunta tai kaupunki

○ Kunnan tai kaupungin liikelaitos

○ Sairaanhoitopiiri

● Valtion organisaatio

○ Oppilaitos

○ Yritys

2. Vastaajan ICT-organisaation koko henkilöinä. (Koko henkilöstömäärä sisältäen harjoittelijat, yms) *

○ alle 10

○ 10-20

● 20-50

○ 50-100

○ yli 100

3. Vastaajan asema ICT-organisaatiossa *

○ Ylin johto

● Keskijohto / Tiiminvetäjä

○ Asiantuntija

○ muu

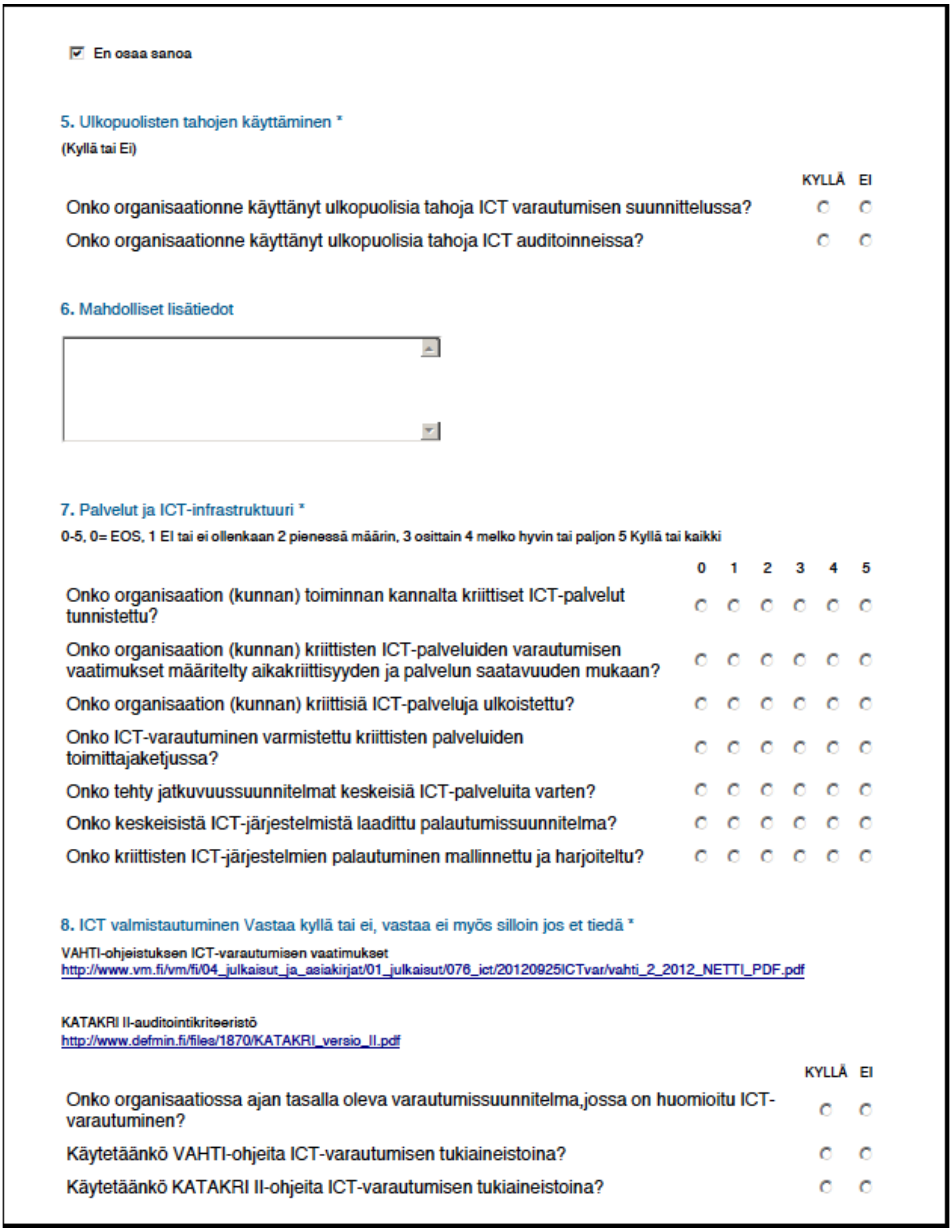
4. Organisaatio (esim. kunta) hankkii keskeiset ICT-palvelut seuraavasti (Voit valita useamman vaihtoehdon) *

☐ tuottaa ICT-palvelun itse

☐ organisaation (kunnan) omistama liikelaitos / yritys tuottaa ICT-palvelun

☐ organisaatioiden (kuntien) omistama seudullinen liikelaitos / yritys tuottaa ICT-palvelun

☐ hankkii ICT-palvelut palvelutoimittajalta (kaupallinen yritys)



☑ En osaa sanoa

5. Ulkopuolisten tahojen käyttäminen *

(Kyllä tai Ei)

	KYLLÄ	EI
Onko organisaationne käyttänyt ulkopuolisia tahoja ICT varautumisen suunnittelussa?	○	○
Onko organisaationne käyttänyt ulkopuolisia tahoja ICT auditoinneissa?	○	○

6. Mahdolliset lisätiedot

7. Palvelut ja ICT-infrastruktuuri *

0-5, 0= EOS, 1 EI tai ei ollenkaan 2 pienessä määrin, 3 osittain 4 melko hyvin tai paljon 5 Kyllä tai kaikki

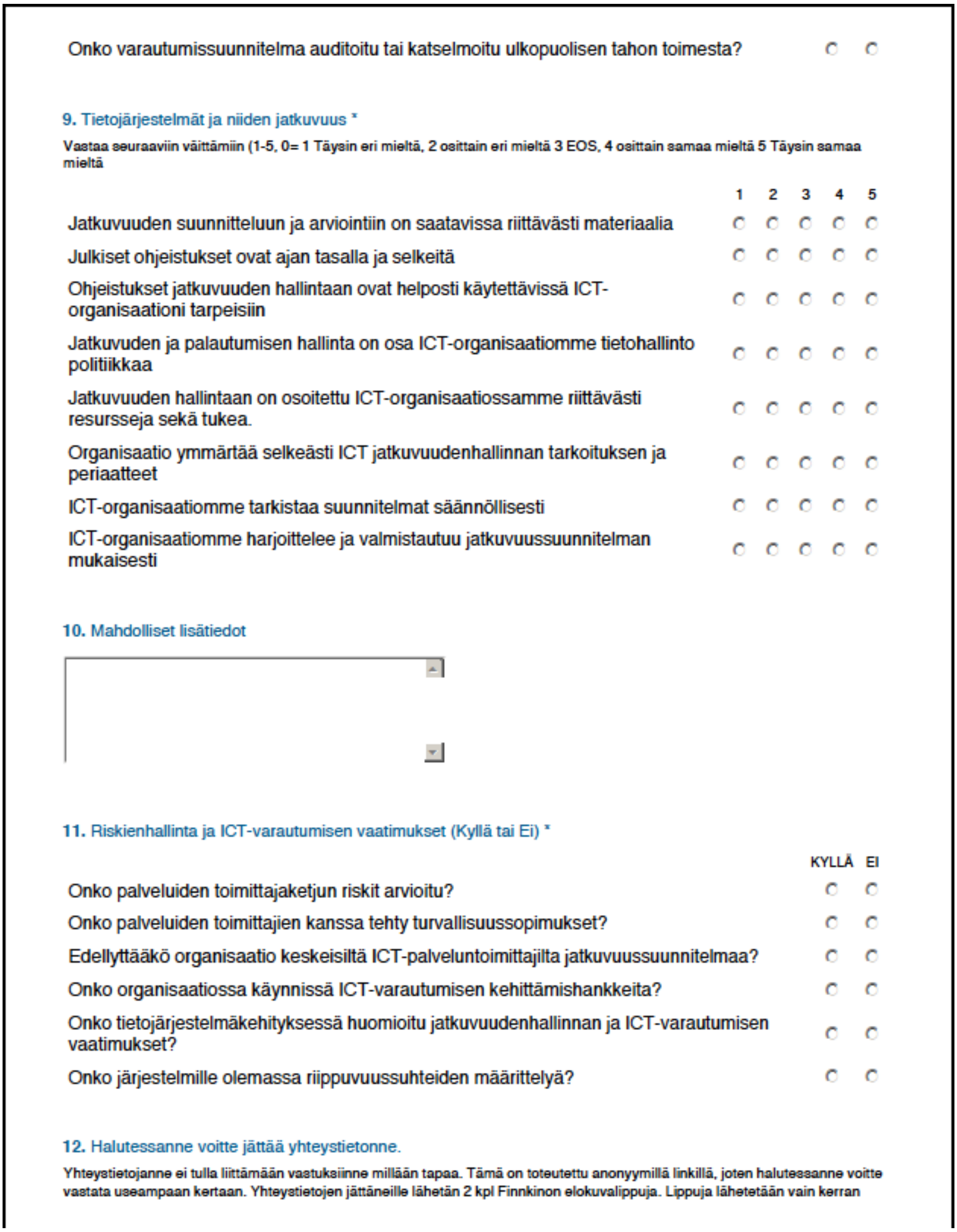
	0	1	2	3	4	5
Onko organisaation (kunnan) toiminnan kannalta kriittiset ICT-palvelut tunnistettu?	○	○	○	○	○	○
Onko organisaation (kunnan) kriittisten ICT-palveluiden varautumisen vaatimukset määritelty aikakriittisyyden ja palvelun saatavuuden mukaan?	○	○	○	○	○	○
Onko organisaation (kunnan) kriittisiä ICT-palveluja ulkoistettu?	○	○	○	○	○	○
Onko ICT-varautuminen varmistettu kriittisten palveluiden toimittajaketjussa?	○	○	○	○	○	○
Onko tehty jatkuvuussuunnitelmat keskeisiä ICT-palveluita varten?	○	○	○	○	○	○
Onko keskeisistä ICT-järjestelmistä laadittu palautumissuunnitelma?	○	○	○	○	○	○
Onko kriittisten ICT-järjestelmien palautuminen mallinnettu ja harjoiteltu?	○	○	○	○	○	○

8. ICT valmistautuminen Vastaa kyllä tai ei, vastaa ei myös silloin jos et tiedä *

VAHTI-ohjeistuksen ICT-varautumisen vaatimukset
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20120925ICTvar/vahti_2_2012_NETTI_PDF.pdf

KATAKRI II-auditointikriteeristö
http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

	KYLLÄ	EI
Onko organisaatiossa ajan tasalla oleva varautumissuunnitelma,jossa on huomioitu ICT-varautuminen?	○	○
Käytetäänkö VAHTI-ohjeita ICT-varautumisen tukiaineistoina?	○	○
Käytetäänkö KATAKRI II-ohjeita ICT-varautumisen tukiaineistoina?	○	○



Onko varautumissuunnitelma auditoitu tai katselmoitu ulkopuolisen tahon toimesta?	○	○

9. Tietojärjestelmät ja niiden jatkuvuus *

Vastaa seuraaviin väittämiin (1-5, 0= 1 Täysin eri mieltä, 2 osittain eri mieltä 3 EOS, 4 osittain samaa mieltä 5 Täysin samaa mieltä

	1	2	3	4	5
Jatkuvuuden suunnitteluun ja arviointiin on saatavissa riittävästi materiaalia	○	○	○	○	○
Julkiset ohjeistukset ovat ajan tasalla ja selkeitä	○	○	○	○	○
Ohjeistukset jatkuvuuden hallintaan ovat helposti käytettävissä ICT-organisaationi tarpeisiin	○	○	○	○	○
Jatkuvuden ja palautumisen hallinta on osa ICT-organisaatiomme tietohallinto politiikkaa	○	○	○	○	○
Jatkuvuuden hallintaan on osoitettu ICT-organisaatiossamme riittävästi resursseja sekä tukea.	○	○	○	○	○
Organisaatio ymmärtää selkeästi ICT jatkuvuudenhallinnan tarkoituksen ja periaatteet	○	○	○	○	○
ICT-organisaatiomme tarkistaa suunnitelmat säännöllisesti	○	○	○	○	○
ICT-organisaatiomme harjoittelee ja valmistautuu jatkuvuussuunnitelman mukaisesti	○	○	○	○	○

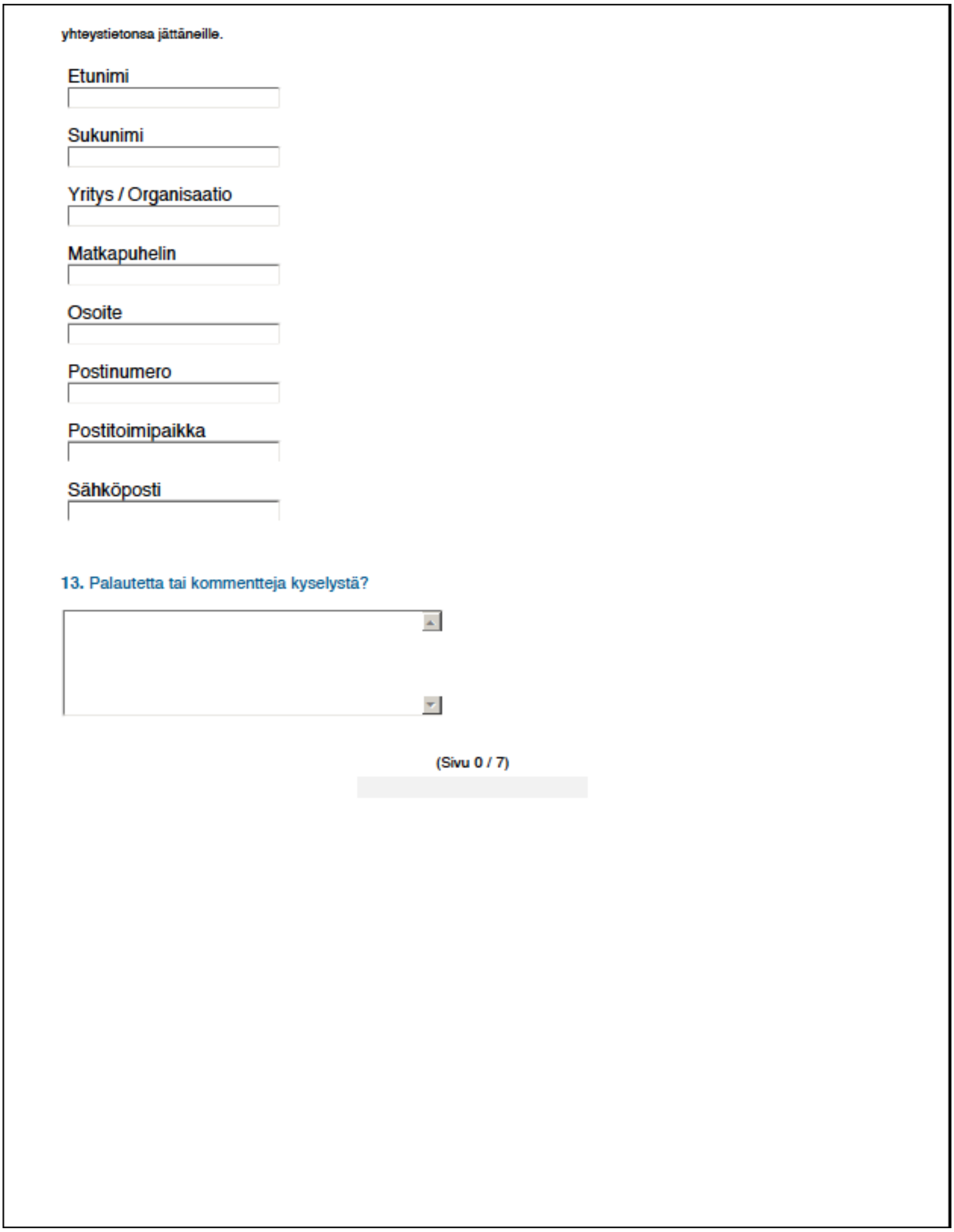
10. Mahdolliset lisätiedot

11. Riskienhallinta ja ICT-varautumisen vaatimukset (Kyllä tai Ei) *

	KYLLÄ	EI
Onko palveluiden toimittajaketjun riskit arvioitu?	○	○
Onko palveluiden toimittajien kanssa tehty turvallisuussopimukset?	○	○
Edellyttääkö organisaatio keskeisiltä ICT-palveluntoimittajilta jatkuvuussuunnitelmaa?	○	○
Onko organisaatiossa käynnissä ICT-varautumisen kehittämishankkeita?	○	○
Onko tietojärjestelmäkehityksessä huomioitu jatkuvuudenhallinnan ja ICT-varautumisen vaatimukset?	○	○
Onko järjestelmille olemassa riippuvuussuhteiden määrittelyä?	○	○

12. Halutessanne voitte jättää yhteystietonne.

Yhteystietojanne ei tulla liittämään vastuksiinne millään tapaa. Tämä on toteutettu anonyymillä linkillä, joten halutessanne voitte vastata useampaan kertaan. Yhteystietojen jättäneille lähetän 2 kpl Finnkinon elokuvalippuja. Lippuja lähetetään vain kerran



yhteystietonsa jättäneille.

Etunimi

Sukunimi

Yritys / Organisaatio

Matkapuhelin

Osoite

Postinumero

Postitoimipaikka

Sähköposti

13. Palautetta tai kommentteja kyselystä?

(Sivu 0 / 7)