jamk.fi

Incident management in multi-vendor environment

Interview-based case study

Mika Haapakoski

Master's Thesis
May 2018
School of Technology, Communication and Transport
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author	Type of publication	Date
Haapakoski, Mika	Master's thesis	May 2018
		Language of publication: English
	Number of pages: 50	Permission for web publication: x

Title of publication

Incident management in multi-vendor environment

Degree programme

Master´s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Kotikoski Sampo, Hautamäki Jari

Assigned by

Hassinen Tarmo, Telia Finland Oyj

Abstract

A substantial number of organizations has changed from using a single supplier and dedicated services to using multiple service providers with their service provided from a shared platform. Dealing with multiple vendors has brought challenges to run the IT infrastructure of a company. The focus needs to be on various places and a great deal of work needs to be done to make the operational processes function smoothly. Therefore, also incident management with multi-sourced environment has extended ever-increasingly. The parties might not know their own or another service provider's role in the environment or they do not understand the customer's business goal and how their own actions can affect the customer's performance.

The objective of the study was to sort out what the main challenges and obstacles in the companies are today. The questions needing answers were: what is the current state to perform incident management process in multi-vendor environment, how is the cooperation with stakeholders treated and which areas could be improved.

The research was started by reading previous studies, articles and literature. The research method was chosen to be several interviews with the personnel from different companies. The questions for the interview were generated by going through auditing tools, guides and standards and selecting the suitable parts that form the interview frame for the research.

As a result, the research achieved important knowledge and understanding that benefits the professionals working in multi-vendor environment. The interview questions and answers will help the readers to widen their interests in thinking how these things have been dealt in their own organization.

Keywords

Multi-vendor environment, incident management

jamk.fi

Kuvailulehti

Tekijä	Julkaisun laji	Päivämäärä
Haapakoski, Mika	Opinnäytetyö, ylempi AMK	Toukokuu 2018
		Julkaisun kieli Englanti
	Sivumäärä 50	Verkkojulkaisulupa myönnetty: x

Työn nimi

Incident management in multi-vendor environment

Tutkinto-ohjelma

Master´s Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Sampo Kotikoski, Jari Hautamäki

Toimeksiantaja(t)

Tarmo Hassinen, Telia Finland Oyj

Tiivistelmä

Useat yritykset ovat vaihtaneet yhden toimittajan ja dedikoitujen palveluiden ympäristöistä monitoimittajaympäristöön ja palveluiden käyttämiseen jaetuilta alustoilta. Useiden palveluntarjoajien käyttö on tuonut haasteita yrityksen IT-infrastruktuurin ylläpitämiseen. Huomion tulee olla monessa paikassa ja vaatii paljon työtä, jotta toimintaprosessit toimisivat sujuvasti. Siksi myös vianhallinnan rooli monitoimittajaympäristössä on kasvanut yhä suuremmaksi. Osapuolet eivät välttämättä tunnista omaa tai toisen palveluntarjoajan roolia asiakkaan ympäristössä tai eivät ymmärrä asiakkaan liiketoiminnan tavoitteita ja miten oma tekeminen vaikuttaa asiakkaan toimintaan.

Tutkimuksen tavoitteena oli selvittää, mitkä ovat nykyisin yritysten suurimpia haasteita ja esteitä. Tutkimuskysymykset, joihin oli vastattava, olivat: mikä on nykyinen vianhallinnan tila monitoimittajaympäristössä, miten yhteistyötä sidosryhmien kanssa hoidetaan ja mitä alueita voisi parantaa.

Tutkimustavaksi valikoitui haastattelut eri yritysten henkilöstölle. Haastattelun kysymykset luotiin käymällä läpi auditointityökaluja, oppaita ja standardeja, joista valittiin sopivat osat, jotka muodostavat tutkimuksen haastattelukehyksen.

Tutkimus tuotti tärkeää tietoa ja ymmärrystä alan ammattilaisille, jotka työskentelevät monitoimittajaympäristössä. Haastattelukysymykset ja -vastaukset auttavat lukijoita luomaan ajatuksia siitä, miten kyseisiä asioita käsitellään omassa organisaatiossa.

Avainsanat

Monitoimittajaympäristö, vianhallinta

Content

Figures

Tables

1 Introduction

Back in the days, services were carefully customized for business customers. Today, the majority of the companies have outsourced several functions to multiple vendors. Besides, working on decreasing costs, vendor management should also build a strong relationship with the service providers.

It can be said that incident management has always been a part of companies' IT service continuity management process. For most of the companies, the service management is based on Information Technology Infrastructure Library (ITIL), a global detailed set of practices for IT service management (ITSM). When all participants use the same framework, everyone can be sure that the service management is handled in a common, widely known way and it is easy to handle.

Nowadays, incident management process is studied well, and its roles should be well known among the participants; the customer knows where to contact when having problems with the services, and the service provider knows how to process the fault ticket from the start to the end. Difficulties have arisen when a customer has multiple service providers since they are not familiar with each other, and especially, when the division of responsibilities and tasks is not clear for every party.

There are many researches about the same topic. Incident management is a well-known topic and area of study; therefore, the theory part of this thesis does not focus on that in great detail; instead the benefits and disadvantages of multi-vendor environment will be presented using previous researches and articles.

The purpose of this thesis is to analyze through customer interviews how the incident management process has been taken into consideration particularly in multi-vendor environments and how it can be improved by all the parties. The study hopefully helps people working in the field to focus on the customers' needs and to encourage service providers to have conversations with the client to thoroughly understand what the customer's current situation is and most of all, what their business goal is.

One of the questions is if the interviewees and their organization have a clear understanding of the stakeholders and their relations and requirements for each other, and if all the interested parties have the knowledge of each other's way of working and if everyone has the same goal. The idea is also to find out what kind of development ideas can be found.

The survey was implemented by interviewing various business customers including persons from IT-management, IT-specialist and Chief Information Security Officer. The research data consists of the interviews, and it has been analyzed in this survey. The investigation of the subject itself helps to understand the customers, their needs and the situation, and on top of that to improve Telia's own services, as a service provider.

The idea was to go through known and prestigious standards and guides. The material included VAHTI guidance created by the Finnish Ministry of Finance, ISO/IEC 27001 standard, and KATAKRI 2015 – National security auditing criterion by Finnish Ministry of Defence. The previously mentioned material sets the goal for good practices, requirements and guidelines for management of ICT environment.

Both incident management and multi-vendor management have previously been studied more as individual researches. There are plenty of blogs and articles written by big actors within IT, researches of the area and e.g. one University Bachelor's Thesis has almost the exactly same topic as this thesis; however, it focused on literature review and compare the problems and resolutions of both incident management and multi-vendor environment.

2 Literature review

This Chapter presents the background and basis for the research. It introduces the definition of concepts the study is based on.

2.1 Incident management

An information security incident is a security event or events that can harm or prevent the organization from functioning. Information security incident management has an effective and consistent approach to detect, handle, report and learn from the incidents. (ISO/IEC 27000 2018)

The processes of incident management have been studied widely. There are numerous amounts of material on how to manage IT services. The more critical the service is, the more important it has become to return to its normal state after disturbances. For decent IT service management, a company needs a good process model. ITIL is a globally recognized and used set of detailed practices and framework. (ITIL 2018)

2.2 Multi-vendor environment

A vendor is a company that sells services. This section introduces the benefits and the challenges of a company outsourcing services to multiple vendors. The outsourcing has grown from the 1960s when computer bureaus were selling mainframe time to other companies for data processing. Today, an organization might outsource practically everything except their core business. (Sparrow 2003)

Mathias Sallé (2004) from HP Laboratories opens in his review the evolution of IT function. Figure 1 shows the timeline as three stages from being a technology provider, then a service provider and, to an increasing extent, the ambition to become a strategic partner of the customer. IT Governance means true business partners enabling new business opportunities. At this stage, the services and processes are fully integrated providing improvements to the service quality and business agility. (Sallé 2004)

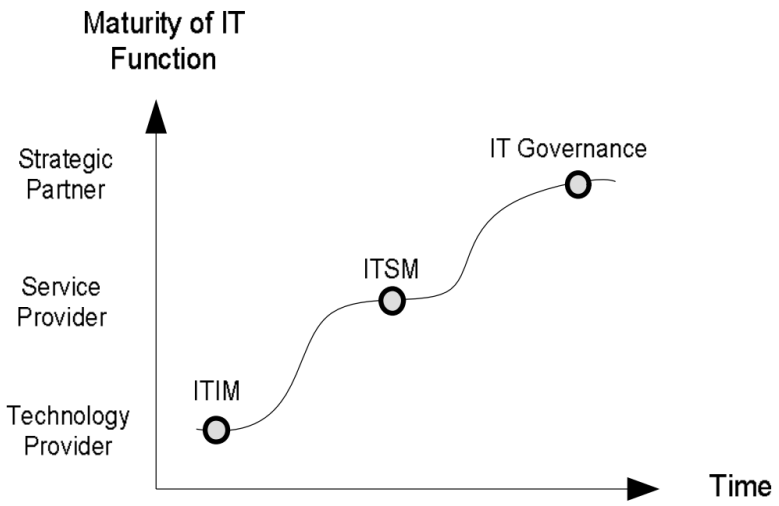

Figure 1. Evolution of the IT Function within organizations (Sallé 2004)

The new way of working and business strategies have changed the usage of single vendors into multi-vendor environments. Externalizing IT services to multiple service providers has brought new challenges into managing the services. As like Gavin Payne wrote in Microsoft's Technet blog 2015, organizations nowadays tend to buy what is best for their company, not only from a single vendor but from whoever has the desired product to fill the needs. (Payne 2015)

Researchers at Gartner predicted in 2014 that organizations will be demanding more from vendors to obtain more value to achieve the desired business goal. The focus is not anymore on the cost optimization and service-level agreements but more on the advanced vendor management programs. Efficient tools to automate processes and to provide accurate reporting, tracking and risk management will be appreciated. (Sullivan & Qureshi 2014)

Gartner's prediction was right, at least in some extent. Even though two companies integrate into each other, the change can create problems. Sometimes the organizations are not ready, however, they have decided to take the risk which might also bring unexpected costs and stress for the personnel. In the long run, it should, of course, increase profitability and facilitate the use of resources.

Info-Tech Research Group company provides tools and guidance to building vendor management (VM) and an improvement plan. They state that in the future, VM will become the core component of the whole service management. Integration of all

components into IT operations will be critical to success, however, sufficient control and monitoring of the third-party service providers is still needed. (Info-Tech 2018)

Today, most of the service providers have almost the same prices for their services, self-service portals, service level agreements, and the same availability. Improvements have become an automation of processes, outsourcing services and virtualization.

As customers are outsourcing their services, they demand more from the vendors. It is clearly not enough to have secured the own end-devices, data security and a firewall in place. It must be ensured that the service providers have their services armed with skilled engineers to run intrusion detection systems (IDS), advanced threat protection (ATP) and a next-generation firewall (NGFW). This is to assure that the multi-sourced environment will have capabilities for decent incident and risk management.

The time of using only one vendor is long gone. Multi-vendor environment has brought new possibilities enabling wide coverage of services. At the same time, it brings unfamiliar problems and the matters to take into consideration are wider.

2.3 Service integration and management

Outsourcing has increased enormously and at least the author of this thesis has not heard of any listed company that has not outsourced at least some part of a company's business to another company. The reason for outsourcing is to reduce costs. Since enterprises have multiple service providers and a substantial number of services are produced by different vendors, it has become a difficult and laborious task to handle for some of the companies.

Usually, the situation appears as shown in Figure 2, where the customer has multiple service providers both internal and external, of which some if not all, have their own suppliers as well. The chain can be much longer, however, with this Figure the idea should be clear for everyone.

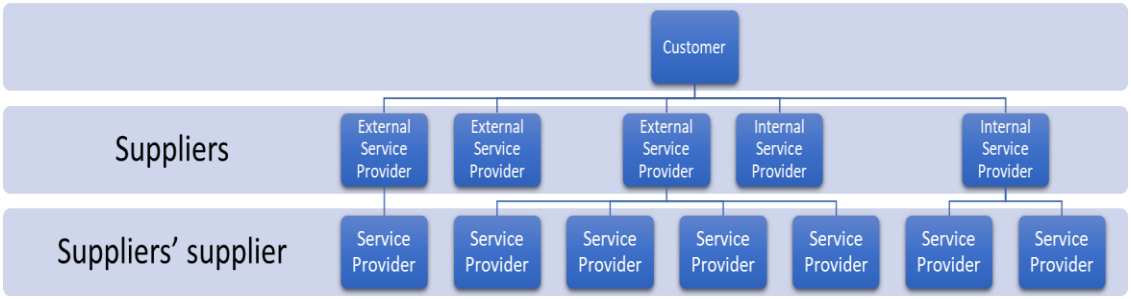

Figure 2. Supply chain

If there is a problem, there is a solution. Service Integration and Management (SIAM) is one answer to the challenges of multi-vendor environment and a respond to the customers' changing business requirements. It integrates multiple suppliers and services to provide a single point of contact for the whole environment. Basically, SIAM provider handles the operational tasks with all suppliers and integrates all services into one monitoring tool. This way, the whole vendor management can be outsourced, and a real benefit of outsourced services is obtained. IT management and SIAM service provider need a well-functioning cooperation to meet the business needs, to understand the business goals and to make sure that every vendor knows their role and what is expected from them. Figure 3 displays the customer on top and a service integrator in the middle taking care of both external and internal service providers.

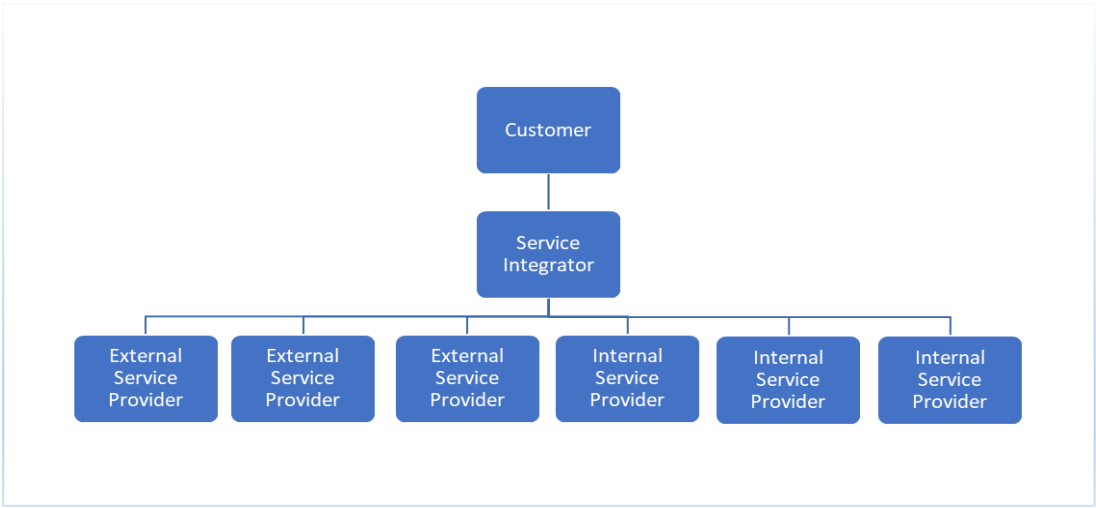

Figure 3. SIAM layers

There are four ways to produce SIAM. A company can have an internal service integrator where the company itself produces the service integration, or an external service integrator where a third-party company handles the service integration without any service delivery responsibilities. In a hybrid service, the integrator, the client and one of the service providers are responsible for the service integration. The lead supplier service integrator has the same benefits as externally sourced integration, however, it has a faster set-up process, since this supplier is also one of the external service providers. (Tenkamaa 2017)

2.4 Tools for service improvement and management

There are several well-known methods and tools for IT service management and continuous improvements, namely PDCA (Plan Do Check Act) Cycle, OODA loop (Observe, Orient, Decide, Act) and COBIT framework. It is to be expected that at least one of these tools is introduced and used by the interviewed organizations.

2.4.1 PDCA

Plan, do, check, and act (PDCA), is a four-step model and like a circle, it has no end, i.e. the cycle should be repeated to achieve continuous improvement. The model can be used for projects, developing process, product or service, or just any kind of change implementation. The procedure starts with planning and recognizing the need for change, followed by steps to test and review and analyze the results. Last, and before starting the process again, to act based on what has been learned. Figure 4 describes the cycle in its simplest way. (Tague 2004, 390-392)

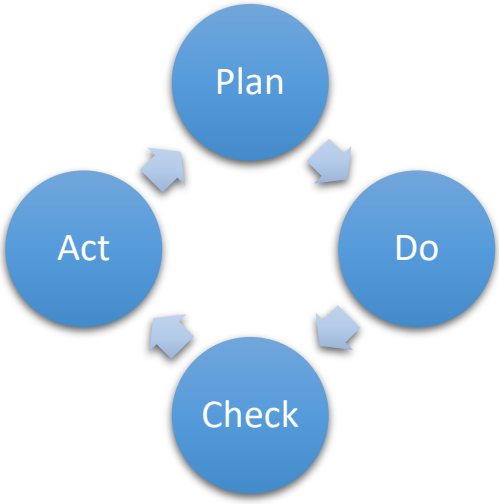

Figure 4. PDCA cycle

2.4.2 OODA loop

The professionals in the field of security, such as Bruce Schneier, speak for the use of decision cycle of observe, orient, decide, and act (OODA), loops (Schneier 2014). OODA loop was developed by the United States Air Force Colonel John Boyd. OODA loop has been recognized to be the best way to learn to think, make up innovative ideas and to combine them to learn new things. Figure 5 explains the OODA loop that starts with scanning the threats to observe the environment. The orientation encapsulates all information, e.g. education, culture, experiences, analysis and their synthesis. Decisions are made based on knowledge. By constantly monitoring the success of doing the right or wrong as well as good or bad decisions, the know-how is shaped and ways to act are constructed. The loop continues based on the learned. (Hammond 2012)

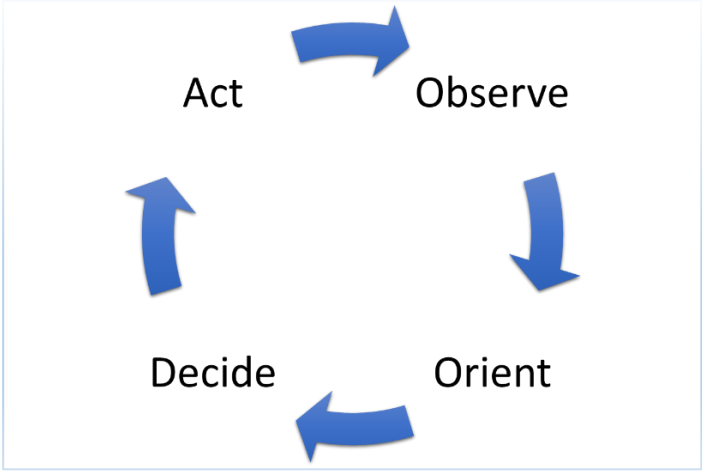

Figure 5. OODA loop

2.4.3 COBIT 5

COBIT 5 is a business framework for the governance and management of enterprise IT. It enables companies to maximize the value and minimize the risks. The framework includes globally accepted principles, practices, analytical tools and models. IT management and the governance can use COBIT to understand stakeholder needs, roles and relationships, covering the enterprise from end-to-end and to create an appropriate environment. (COBIT 2012)

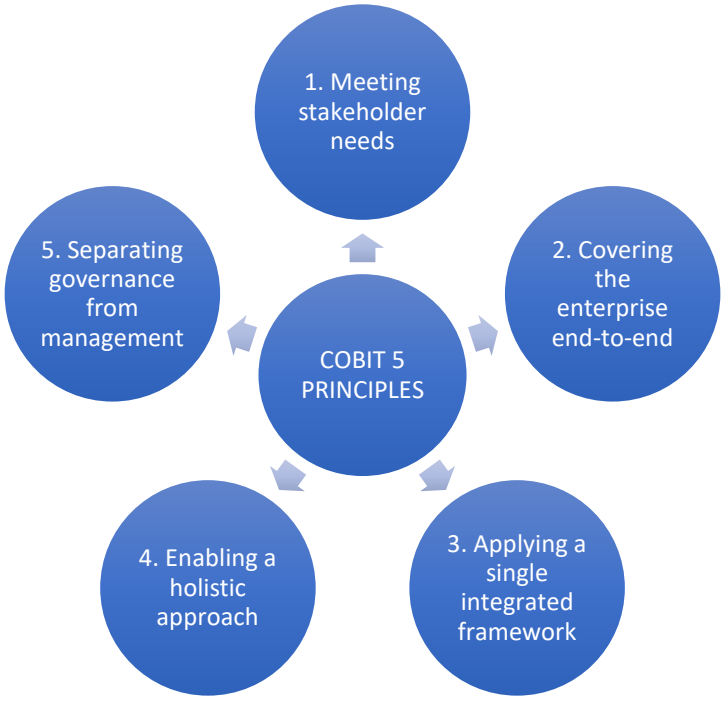

Figure 6. COBIT 5 Framework (COBIT 2012)

COBIT 5 summarizes that information is a key resource for all enterprises. It is based on five key principles shown in Figure 6. COBIT 5 provides all required tools to manage different objectives and goals, and it can be customized to suit the enterprise's processes and practices. The five principles enable the company to optimize information and technology investment and use it for the benefit of stakeholders. (COBIT 2012)

2.5 Tools for information security

A few well known and respected guides and standards were used to develop and produce the interview questions for this thesis. All the materials contain similar technical description and methods to manage incident situations, and instructions how to cooperate in a multi-vendor environment.

Considering the goal of this thesis, the most important requirements and guides were molded into a survey and modified into interview questions as seen in Appendix 1. Additionally, the interview questions are discussed more precisely in Chapter 4.

2.5.1 ISO/IEC Standard

The joint technical committee for International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publishes international standards to ensure efficiency, safety and quality for products and services. (ISO 2017)

The International Standard ISO/IEC 27001:2013 specifying Information Security Management Systems (ISMS) and ISO/IEC 27002:2013 is a standard for good practices in information security. Both standards are confirmed to be Finnish national standards. (ISO/IEC 27001:2013 and ISO/IEC 27002:2013)

The standards were used in this thesis to provide guidance for information security in supplier relationships as well as management of information security incidents and improvements. The ISO27002:2013 states that an organization should ensure that they have incident response personnel with responsibility, authority and competence

to manage an incident. The monitoring and review of supplier services helps to create and maintain an agreed level to ensure the service delivery is in line with supplier agreements.

2.5.2 VAHTI guide

The Ministry of Finance (Finland) published VAHTI guide in February 2017 called Management of data security breach situations, Ministry of Finance publications (8/2017). The guide will help an organization to develop collaboration and communication between the organization and its stakeholders in incident management. It contains information on how to setup data security breach handling processes from observing to analyzing and from reaction to communication. (Ministry of Finance, VAHTI 2017)

VAHTI guide provides information such as responsibilities and roles for organization's internal and external communication during an incident or data security breach situation. It also brought up the fact that all internal and external personnel are responsible for detecting and informing about a problem.

2.5.3 Katakri

Katakri is a national security audit tool for authorities. The tool brings together the minimum requirements for secure information handling. It has been created by the Ministry of Defence (Finland) in cooperation with other important authorities.

The audit tool can be used to assess a company's security arrangements, to support and develop safety measures and to ensure that security requirements are considered. Katakri 2015 Security Audit Tool was approved by Finland's National Security Authority in March 2015. (Ministry of Defence, Katakri 2015)

A few quotes from Katakri (Ministry of Defence, Katakri 2015) used to develop this the survey questions for this thesis are listed below:

"The organisation has defined the tasks and responsibilities of security management."

"Dependencies on external factors have been identified in the organisation as well as their effects on its functions. The effects of organisation's activities on others have been identified."

"Through security event management it is ensured that the organisation is able to function efficiently in exceptional situations by minimising damage and restoring the situation to normal. Effective management of security events requires sufficient allocation of resources."

2.6 Other studies

Managing a multiple-vendor environment can be very challenging and chaotic if it is not managed in a proper way. A clearly defined vendor management process is an important investment. Hence, the subject has been studied by other researchers and experts in this field. One of the challenges is the understanding of interdependencies between outsourced functions.

Riina Heikkilä (2014) from the University of Jyväskylä studied incident management in multi-vendor environment in her bachelor's thesis *Critical Challenges of Incident Management and their Solutions in Multisourcing Environment*. Heikkilä (2014, 24) summarized the two elements using a literature overview and combined the major problems and their resolutions. The result was that there are three critical challenges that need focus: interdependence, complexity and achievement of business goals.

Heikkilä (2014, 13) found several ways of meeting the challenges. The interdependence of all components in incident management can be made easier, e.g. utilizing High Reliability Theory (HRT) techniques and considering the limited rationality of decision making. Complexity can be dealt with dynamic decision making throughout the whole organization and both service providers and the customer must cooperate at the process level. To achieve the business goals, the organization should utilize the Business Impact Analysis and to have a centralized management for outsourced vendors. (Heikkilä 2014, 20-21)

Alfredo Reyes (2015) from Aalto University, studied in his master's thesis *Outsourced incident management services, the security service providers perspective of incident management in multi-vendor environment*. Reyes summarizes that most critical challenges are the identification of needed services, the interaction of multiple service providers during an incident, lack of skilled personnel and knowledge transition of customer services when a service provider is changed. (Reyes 2015, 77)

There is more than one perspective on how to see the advantages and disadvantages whether one is a customer or a service provider, however, the author is quite sure that both sides can agree on the main challenges.

When the incident management is partially outsourced, most of the interviewees in Reyes's thesis (2015, 78) think that the benefits are more man-power, managerial skills, multiple sources of intelligence, specialized services and a global perspective on threats. The disadvantages are reduction of staff and overlaps when there are no clear lines of responsibility. Small and medium-sized organizations that do not require specialized services can benefit by outsourcing the incident management, when the service provider has the knowledge of today's threats and the infrastructure to deal with it. Large organizations often need more unique services and demands tailored solutions, which are not easily achieved. (Reyes 2015, 78)

Without considering the size of the company, based on author's personal experience, the IT infrastructure of an organization can be produced and executed by only a few staff members as long as they have skilled professionals as an outsourced resource. An organization still needs their own IT management that understands the company's business goal and is responsible for the service environment.

Markus Vuorinen from Laurea University of Applied Sciences wrote his master's thesis in 2011 called *IT Service Management Transformation to Utility Computing* which is a summary of two publications; *Multi-Supplier Integration Management* and *Service Standardization to Utility model*. The research presents a model that can be used for managing a multi-vendor environment based on Hewlett-Packard's framework Enterprise Service Management (ESM) and Information Technology Service Management (ITSM). (Vuorinen 2011, 2-3)

"If any of the suppliers is not compliant with company requirements for IT suppliers they should not be used. Noncompliant service providers would make corporate services weak if some of the providers can't commit to tools, SLA's or processes required." – (Vuorinen 2011, 3)

Vuorinen's research states that in order to make multi-vendor environment possible four criteria are required: processes, governance and policies need to support multi-supplier operations; the reasons to choose multiple service providers need to be defined; the services mature enough to be produced in a multi-supplier environment should be evaluated; and for the last, when previous stages are clear, the organization should prefer a phased approach for migration into a multi-vendor model. (Vuorinen 2011, 2-3)

A responsibility assignment matrix is a commonly used model in projects to describe and clarify the responsibilities and roles of certain parties. Responsible, accountable, consulted and informed (RACI) are the most typically used roles in the matrix. (Haughey 2018)

An organization using multiple service providers could consider using a RACI model for every party to understand their responsibilities and their role in the whole environment. Table 1 below simplifies the RACI model. Suppliers might consist of service providers, Security Operation Center (SOC), SIAM integrator etc.

Table 1. RACI matrix (example made by the author)

Task	Customer	Supplier 1	Supplier 2	Supplier 3
Monitoring of all services	I	A/R	C	C
Incident management	I	A/R	C	C
Incident escalation	A/R	C	C	I
Permanent fix	A	C	C	R
Root Cause Analyze	I	R	C	A

The number of studies of multi-vendor environment and its challenges shows that the subject is interesting and recognized to be a real area with much room for development. The previously presented researches are just a small sample of all the studies; however, these presented studies gave a good perspective for this research and helped to find another way to study the subject.

3 Background and research basis

Chapter 3 introduces the reasons to choose this research topic. The expected goals to be achieved by the research are presented, followed by the research questions that this research strive to answer.

3.1 Motivation

The motivation for this kind of study emerges from working life. The author is currently working with business customers, and most of them have plenty of service providers. Challenges have been noticed; especially if the services are not acquired from only one service provider but the service consists of multiple suppliers. This has made it difficult to have an overall view of the supplier chain and to point out who is responsible of which part.

One example is cloud-based services that need the service providers for the connection, firewall and the actual cloud service. If the end-user complains a service is not working, the problem can sometimes be found already in the end-user's laptop, however, usually the troubleshooting is started on the service provider side. What if the problem affects more than one person, office or country? What is the next step to manage the situation? The better the service provider knows his client and the better he knows what services the environment consists of, the better the overall service can be.

3.2 Research objectives

The goal of this research was to get a clear understanding of the customers' current situation of handling incident management processes in a multi-vendor environment. The aim is to find out if the stakeholders have something to develop in their daily business. Simultaneously, the customer gains practice and invites reflection by answering the questions.

The scope of the study is to focus on the incident management in a multi-vendor environment at present time, even though the interview also contains questions from a

development perspective. This is to understand if the interviewees have a conception how the potential problems should be dealt with and if they have something the service providers could improve instantly.

3.3 The research questions

The objective is to find answers to these questions:

What is the current state of performing incident management process in multi-vendor environment?

How is the cooperation with stakeholders treated and which areas could be improved?

These are the main research questions for this thesis. The questions used for the customer interviews all supported these questions.

3.4 Customer interviews

The research assignment was given on behalf of the author's employer Telia Finland. When the problem was introduced it was clear to involve customers in the research. One option was to have a mail survey for multiple respondents which would have made the research a quantitative research; however, it was decided to use a more personal and reliable method such as interview. The reason for this was to get the customer's own voice heard and understand the experiences and meaning behind the answers.

As McNamara (1999) writes "Interviews are particularly useful for getting the story behind a participant's experiences." This is true, and it was also noticed during the interviews that it is easy to make specifying or clarifying questions if the response was not clear enough at the first time. Simultaneously, the respondent elucidated the answer and backgrounds of the reply.

According to Hirsijärvi, Remes & Sajavaara (2007, 199-201) an interview is a unique method of collecting data that is in direct linguistic interaction with the subject being studied. It has both advantages and disadvantages. A great advantage, comparing to

other data collection methods, is the possibility to clarify and deepen the gotten information. The reliability of the interview can be undermined by the fact that the interview tends to provide socially desirable answers. Foddy (1995, 118) states that the interviewee may want to appear as a reliable person. In this research the interviewee might leave certain matters unresponsive or disregard completely of the deficiencies that exists.

4 Evaluation of the results of the surveys

The research was carried out by investigating the literature such as ISO/IEC standards, VAHTI and KATAKRI, and forming interview questions from the studied material. Other similar studies were also reviewed and used to compare the research methods. Additionally, other previous studies gave a good insight of what had already been done with what kind of results.

4.1 Research methodology

The thesis is a qualitative research. Its starting point is to describe real life and understand the research items. Qualitative research tries to explore the subject as comprehensively as possible, whereas the quantitative research method examines the information numerically answering the questions how many, how much and how often. (Hirsijärvi et al. 1997, 131-133)

The topic processes the target persons' feelings and experiences. Hence it was concluded to choose qualitative research to serve the whole study well. The author tried to collect the research data by natural and real-time interviews to get as authentic material as possible. By interviews he wanted to give the interviewees the possibility to open their feelings, knowledge and to get descriptions of real life situations more accurately.

In a qualitative research, it is common that there are only a few cases to be investigated, and therefore the focus is on analyzing the cases as thoroughly as possible. Since the number of interviewed persons was small, it can be called as discretionary sampling. The discretionary sampling focuses only on examining certain objects and collecting data. (Eskola & Suoranta 2008, 18)

To investigate the performance of employees' experiences in companies it was clear to approach the phenomenon using interviews. A questionnaire was also a considered method for data acquisition, however, it was then decided that as interviews are more interactive, the responses are therefore more accurate. Additionally, with

discussion the questions could be clarified if there was a possibility for misunderstanding or if the interviewee's answer needed focus. The disadvantage might be that this way not all questions are equal to all respondents. The author is still quite sure that the questions were understood correctly, since no one seemed to be uncertain or suspicious about the inquiry. The diversity of the answers is explained by the various kinds of environments or the interviewee's position in the company, which means that they are at looking the settings from a unique perspective.

The interviews contained questions about how the collaboration works between the company and its stakeholders and about incident management processes including the matter that are in an unsatisfactory condition, which after all might be a sensitive subject. This fact might affect the answers given, however, since the interviewees did not represent their employer, they discussed their own experiences, and it was clear that their identity and the employer are classified as confidential material.

The theme interview was suitable for this kind of interview since it is a kind of combination of an interview form and an open interview. With pre-defined questions it was easy to make progress through the interview.

4.2 Gathering data

The material of this thesis was gathered from four interviews of different companies' employees, who represented themselves in that company; they did not represent the company itself. Five persons were interviewed, and their titles were IT Systems Experts, IT Manager, IT Specialist and Chief Information Security Officer. They worked in various industries and the companies' size ranged from 500 to 50 000 employees.

When the persons were contacted for the first time to ask if they were interested in this kind of interview, the main idea and context of this survey were discussed. When each interview time was agreed, the interview questions were sent (Appendix 1) with an invitation to the survey (Appendix 2) and the consent form (Appendix 3) by email to the interviewee so that the person had time to examine the material before the actual meeting.

The interviews were carried out in January 2018. The material was introduced by going through the title, reason and goals of the thesis. The consent form was also displayed and requested to fill in and return. The interviewee had the possibility to make questions and interrupt the interview at any point.

During the interview, the findings were written down simultaneously. The researcher's own personality is a research and data gathering tool, which are used to get most out of the interviewed person. The importance of observation is to gain interviewees trust and the ability to remain neutral. (Järvinen & Järvinen 2004, 145-147)

It is possible that the interviewer's own knowledge and experiences on the subject affect the interview and the way the conversation proceeds. It is important to remember to focus on the interview questions and make sure that the conversation does not end up in the wrong direction or out of the topic.

4.3 Construct of the interview questions

There are multiple ways to implement interview questions. With a precise planning of the questions it is possible to enable a successful research. There are several types of questions, such as scale-based questions, multiple choice questions and open questions. In this interview, the open questions were chosen because they give the respondent the opportunity to express their opinion openly. Concise questions tend to have better effects than long ones, and therefore there is less opportunity to understand the question the wrong way.

4.4 Analysis of the interview data

This section presents the questions and findings from the interviews. The interviewees represent themselves and talk about their experiences in their organizations, i.e. the interviews are not officially assigned by the companies in question. The questions are presented as they were in the interviews. The questions are divided into four themes: backgrounds, incident management process, stakeholder co-operation and development. Each theme and question is discussed separately.

The questions can be found in Appendix 1 in Finnish. This section presents the analysis part, and the questions are translated into English.

4.4.1 Backgrounds

The interview questions were started by defining the interviewees' backgrounds. Nevertheless, the point was not to compare the companies' situation or way of working but to combine the results and to find possible unifying phenomena. The number of interviewed persons was also a reason for not comparing their answers among themselves.

The interviewees worked in industry sectors consisting of metal-, energy-, construction- and insurance industries. The number of staff in companies varied from 500 employees to over 50 000 employees.

As stated earlier, the positions of the interviewed persons in the companies were IT Specialist, IT System Experts, IT Management and Chief Information Security Officer. They all worked within the IT sector and were involved in incident management processes with experience of multi-vendor environment.

4.4.2 Incident management process

The questions about incident management processes try to find out how the organizations manage their security events. The first question simply asks the interviewee's opinion of the status how to deal with security breaches. The question presented an easy start even though it is a very important one. The next questions discuss the roles and responsibilities of the company and its suppliers.

According to the previous studies and researches, communication within and beyond the organization is very important, which is why it was decided to ask if the organization has defined the process for communication.

Does your organization have the appropriate way to deal with security breaches?

The author wanted to start the approach to incident management process by asking if the organization has an appropriate way to deal with security breaches. All the answers were positive, and everyone said they have appropriate processes. One of the respondents added that even though they have defined the responsibilities, it is hard to make sure that everyone follows them.

How does your organization define the group for security vulnerability processing and have the employees' responsibilities been defined?

The second question was about how the organization has defined the security vulnerability processing group and the personnel's responsibilities. Two of the respondents said they do not have a clear responsibility, and a specific group to handle cyber threats is not in use; however, the lack has been notified and the situation is to be improved.

One of the organizations has a cyber security management group for critical situations, including Chief Information Security Officer, Security Managers and stakeholders from various areas. There is also an organization which have an outsourced SOC with the responsibility for security vulnerabilities; however, the organization itself has not defined a specific security vulnerability processing group.

Who or which party is responsible for detecting, communicating and starting an incident management process?

All these organizations have outsourced their Security Operations Center (SOC), Service Desk (SD) or Service Integration and Management (SIAM), and therefore they have the responsibility for detecting, communicating, and starting an incident management process. Additionally, the organization itself has responsibilities e.g. in public relations.

One of the respondents underlined that every person in the organization has the liability to inform their observations of possible threats or deviation, and the personnel knows how to act in those situations.

How is external and internal communication handled? Do the parties know where to communicate, when to communicate, to whom to communicate and who will communicate?

Internal and external (i.e. public) communication has its rules in every organization. There is a responsible person or group in every organization that handles the public communication, and this seemed to be in order with every organization.

One interviewee said their internal communication has its difficulties since it does not have a precise manual and operating model. They have much more considerations on how much to inform internally. There can be occasions when they reveal too much; or even the opposite, the communication is insufficient. The desire was that the internal communication could be as formal as external communication.

4.4.3 Stakeholder cooperation

This subchapter contains the most important questions concerning the thesis's research questions: the current state to perform incident management process in multi-vendor environment and the cooperation with stakeholders. The literature review highlighted the major difficulties arising in the multi-vendor environment.

The interview questions aim at the knowledge of how the multi-vendor environment is really working and what might be the vicissitudes or problem areas. It also asks if the interviewee has ideas for improving the cooperation with the suppliers.

How has your organization defined relevant external and internal stakeholders concerning information security?

All the interviewees state that their organization has defined relevant external and internal stakeholders concerning information security. One of the respondents presented that everything is on the service providers' hands. Another company added that they still have some deficiency regarding IT management; however, this will be improved in near future.

How are the data security requirements of these stakeholders defined?

The data security requirements for the stakeholders has been defined; however, there are some questions related to the agreements. One interviewee has a challenge with their requirements changing during the contract period, and the requirement documentation should be updated for all service providers. The question is whether the service provider needs to follow the new requirements or is it just a customer's wish. Sometimes the new requirements need arrangements and action in service providers services, which brings the question if the expenses will be charged and from whom.

One of the organizations has its security politics and guides for their internal and external stakeholders. Additionally, EU General Data Protection Regulation (GDPR) has been taken into contracts and contractual obligations. Technical protection has been made for internal stakeholders' tools, and security guidance for personnel.

Another organization has gone through the security requirements with its biggest service providers. Their stakeholders have also been audited by a third-party auditor.

How does your organization master the interdependencies of all stakeholders, are they documented and known to all parties?

The documentation of all the stakeholders seems to be in order in all of the researched organizations. Stakeholders are supposed to know at least their own responsibility for the continuity of the customer's service. Additionally, exercises are held with the internal stakeholders.

One organization controls their stakeholder dependencies with SIAM, which includes configuration management database (CMDB), contact details for all parties, solution architecture pictures etc. Service monitoring is located also in SIAM.

How can transparency and cooperation between different suppliers be improved?

Transparency and cooperation improvements between suppliers varied among the organizations, two of them claim to have everything ready; these are the ones that have SIAM or very close cooperation with SD in use.

The other organizations raised more issues to be developed. In a multi-sourced environment, the suppliers' responsibilities are one question when e.g. the hardware and software is supplied by different vendors, and there comes a need for updates for either one. This situation could be handled with more precise contracts, the interviewee states and adds that the agreed operational models and communication are very important.

Another respondent explains almost the same: he has noted that security issues are often whitewashed and kept in secret. Openness and transparency for errors and vulnerabilities is very important. Hackers or criminals are always one step ahead; therefore, the sharing of identified weaknesses will help to combat the security breaches.

Has your organization been training incident management process between stakeholders' representatives? If yes, then how?

The last question concerning stakeholder cooperation deals with training or practicing the incident management process with the stakeholders. One of the interviewees did not have the information if the company has trained or not. Another interviewee said they have not yet trained; however, it will be taken into consideration and the agenda of the organization includes the collaboration between IT and business.

Two of the organizations has been training cooperation; one with driven by an external security service provider and the other just with the internal stakeholders as a simulated situation exercise; however, if they see it necessary, they will invite the external stakeholders to participate in the exercise as well.

4.4.4 Development

How is the recovery of security vulnerabilities considered in business continuity and recovery plans, including reporting, communication and learning?

One of the organizations has extremely comprehensive recovery plans. The requirements meeting regulatory requirements are in order and in place. Another organiza-

tion has a disaster recovery plan for critical services, and documentation of Data Center and Cloud services. The need for risk management has been recognized and contains documentation of data security breaches, its study and the learning process.

The third interviewee told that all data security breaches are reported. Serious issues are addressed through the problem management process. The necessary changes and update of the action plans are considered case by case e.g. the Ransomwares, where the internal communication has been enhanced to avoid these situations. One of the interviewees did not have the knowledge of their current procedures.

How are your business goals considered in the multi-vendor environment?

The three interviewees' answers were very similar: the need comes from the business. They provide guidelines, then it is the IT's responsibility to choose the supplier, which is cost-effective and has the best services that respond to the business needs. One of the interviewees answered that this is not his territory.

What kind of requirements does your business place on incident management and are they met?

Generally, the service levels and response times are defined in conjunction with the business. Another interviewee admitted that there is always a need for improvement. The Service Level Agreements (SLA), defined in the contract, are being monitored and seek to hold the services in agreed level.

One organization wanted to bring out that their business requires a remote access to their offices or factories to monitor communication breaks and other devices under surveillance.

How could the overall view of a multi-vendor environment be improved?

To combine all answers, the improvements would be openness, clear responsibilities and faster communication. When an incident involves a multiple supplier, everyone should understand their role and check their own domain.

End-to-end monitoring ensures the view for performance. Improvements of transparency of every service provider involved in problem management situation would

help solving the security event faster. The transparency also affects change management processes because the problems often occur after something was changed; however, not all the parties in the organization know if something was changed.

One interviewee had thought about an internal centralized unit responsible for all planned activities and their impacts on the services. The organization with SIAM mentioned that the only thing that needs improving is SIAM.

How would you develop the current operating models for service providers?

One of the respondents wanted to develop collaboration between the service providers in incident management and change management. One of the interviewees raised the issue with practices in follow-up meetings, since all service providers tend to work in their own way. Their desire is to have a common set of indicators from the customer for everyone to see and the customer's goal, at which every vendor should aim.

One of the respondents would like to generally have more information, things that are interesting in security point of view. He would like to know e.g. if the service providers personnel participate in technical trainings and when the company makes security improvements to their own environment e.g. strong authentication and technical capabilities.

One of the interviewee stated that there are no bigger development needs, since SIAM gathers all the necessary information. One aspect of development could be the reduction of service providers.

Would you like to discuss something else?

There are recognized issues to improve the security perspective, and the support comes from the business. One interviewee wanted to raise the differences between the past and present, since years ago the service providers had only dedicated services; however, nowadays most of the services are run from shared platforms, where customization and security are significantly impeded.

One of the respondents would like to raise the security awareness to everyone, including end-users. Everything cannot be prevented; however, it is more important to

know what can be done or cannot be done, and how to deal with potential incident situations. Sharing information about security threats to stakeholders is one matter according to one of the respondents.

4.5 Observations of the interviews

Whether the interviewed persons were working in medium-sized or large companies, they all still operate with the same kind of issues. Generally, all researched organizations have their environment in order; however, what I have seen at work and what these interviews confirmed, was that the trivial things matter. If there is one party in the supply-chain that does not handle its responsibilities or understand its role, the whole service might lose its efficiency.

Based on responses of incident management processes, we can expect that all interviewed persons understand their own organization's deficiency in certain processes and what the most critical areas needing immediate improvements are. It was not surprising that the IT department must find solutions based on how much the business management provides resources, e.g. budget for managing the services. The risk management is an important matter to discuss and both IT and business management need to understand how much money and resources needs to be invested to prevent security vulnerabilities at an adequate level.

I was very happy to find answers, e.g. that every person of the organization has an obligation to report the security event they have detected. This was something that came up in literature review when I studied VAHTI guide, which states that the first security vulnerability can be observed by anyone, such as an employee, a partner or an external user of the network service.

It seemed like the organization with SIAM had fewer issues to think and worry about. The service provider for SIAM was an external supplier who basically takes care of the processes and operational tasks. Therefore, the IT department was rather small with just a few staff members; however, they could use their time to develop their services.

The interviews showed that the customer wants to know about the service provider's development of IT personnel's skills. They are interested in knowing when experts attend courses and perform a certificate. The knowledge deepens the customer's confidence in the service provider's expertise. In fact, the customer assumes that when they buy a security service or a telecommunication service, they also receive a professional service at the same time. It is not only about the product, it is about the whole service and experience that counts.

The respondents were eager to improve the transparency and cooperation with different service providers. This is something I have noticed in my own work as well. I am interested in participating in a meeting with all my clients' stakeholders and to develop our processes to achieve the goals. There is also a possibility to train the communication and processes with each other in e.g. cyber security exercises.

One of the approved and respected actors in the cyber domain is JYVSECTEC, an independent cyber security research, training and development center. With their exercises, an organization and its stakeholders can develop the personnel's abilities to detect and understand cyber threats, to practice in a secure environment and to improve organizations' ability to function in emergency situations. (JYVSECTEC 2018)

End-to-end monitoring of the networks, applications and performance of services was also one point that came up. Commonly, the network is the first point of blame, however, in fact the problem can be located from the user endpoint all the way in the data center where the service is produced. There are tools for this kind of monitoring and one of them is Riverbed's End-to-End Performance Management. (Riverbed 2018)

The interview questions and results are summarized in the Table 2, Table 3 and Table 4 below. They are categorized into the same themes as in the interview.

Table 2. Incident management process

Questions	Results
Does your organization have the appropriate way to deal with security breaches?	All the respondents answered that they have appropriate ways to deal with security breaches.
How does your organization define the group for security vulnerability processing and have the employees' responsibilities been defined?	One of the organizations has a cyber security management group for critical situations. Three of the respondents stated that they do not have a well-defined group to handle security vulnerabilities, but the lack has been considered. One of them have an outsourced SOC with the responsibility for security vulnerabilities.
Who or which party is responsible for detecting, communicating and starting an incident management process?	Outsourced service providers for SOC, SD or SIAM have the responsibility. Additionally, the organization itself has responsibilities e.g. in public relations. One of the respondents underlined that every person in the organization has the liability to inform their observations of possible threats.
How is external and internal communication handled? Do the parties know where to communicate, when to communicate, to whom to communicate and who will communicate?	Internal and external (i.e. public) communication has its rules in every organization. There is a responsible person or group in every organization that handles the public communication, and this seemed to be in order with every organization.

Table 3. Stakeholder cooperation

Questions	Results
How has your organization defined relevant external and internal stakeholders concerning information security?	All the interviewees state that their organization has defined relevant external and internal stakeholders concerning information security.
How are the data security requirements of these stakeholders defined?	The data security requirements for the stakeholders has been defined; however, there are some questions related to the agreements.
How does your organization master the interdependencies of all stakeholders, are they documented and known to all parties?	The documentation of all the stakeholders are in order. Stakeholders are supposed to know at least their own responsibility for the continuity of the customer's service.
How can transparency and cooperation between different suppliers be improved?	The organizations with SIAM or close cooperation with SD claim to have everything ready. The other organizations raised more issues to be developed, e.g. the suppliers' responsibilities and transparency.
Has your organization been training incident management process between stakeholders' representatives? If yes, then how?	At least half of the respondents' organization has been training the cooperation with their stakeholders. The training has been held by an external security service provider or internally as a simulated situation exercise.

Table 4. Development

Questions	Results
How is the recovery of security vulnerabilities considered in business continuity and recovery plans, including reporting, communication and learning?	Most of the respondents had the necessary information documented. Any deficiencies have been taken into account.
How are your business goals considered in the multi-vendor environment?	The need and guidelines come from the business. It is IT's responsibility to choose the most suitable supplier, not forgetting the cost-effectiveness.
What kind of requirements does your business place on incident management and are they met?	The service levels and response times are defined in conjunction with the business. The Service Level Agreements (SLA), defined in the contract, are being monitored and seek to hold the services in agreed level.
How could the overall view of a multi-vendor environment be improved?	The improvements are openness, clear responsibilities for each party and faster communication. When an incident involves a multiple supplier, everyone should understand their role and check their own domain. Improvements of transparency of every service provider involved in problem management situation would help solving the incidents faster.

(continues)

Table 4 (continues)

Questions	Results
How would you develop the current operating models for service providers?	Development of collaboration between the service providers. Unified meeting practices for all service providers. Sharing the information if the service provider attends to third party trainings or have obtained e.g. a new certificate.
Would you like to discuss something else?	There are recognized issues to improve the security perspective. The importance of sharing information was raised by the respondents. The security awareness is to be made responsible for everyone, including end-users.

4.6 Comparing to hypothesis

The literature review in Chapter 2 corresponded to the analysis made of the customer interviews. Unfortunately, none of the interviewees informed about their usage of tools for service improvements and management; however, on the other hand, it was not directly asked during the interview. Although the tools were not mentioned, I am quite sure the organizations have used them to organize themselves and their processes.

Most of the literature was many years old, and the companies and service providers still deal with the same topics, e.g. incident management processes and every party's role in multi-vendor environment, sharing the information and being transparent throughout the organization and with all the stakeholders.

The exciting part of this research was to find out if the previous studies support the findings of this research. The interviewed persons had the same kind of difficulties as the literature review in Chapter 2 mentioned: the transparency of all the processes and stakeholders, the clear roles and responsibilities of each party, and understanding the business goals. On other hand, many of the interviewees were aware of their challenges and were already studying the options for improvement.

5 Conclusions and discussion

It is important for research to produce useful information for business use. Through this research, I have worked to produce new information that could be used to develop our services but also to deepen the relationship between the service provider and the customer.

5.1 The thesis process

Based on the number of interviews, the research is not to be generalized. However, I am certain the respondents were honest and could be relied on, since with most of the interviewees, we have done business together for a long time. This is also a fact that can be taken into consideration: Is the interview more or less reliable when the interviewer is familiar with the interviewee?

With the interview, I was able to help the respondent to understand what I meant with the question, and at the same time, I got the possibility to ask and ensure I had understood the answer correctly. The respondent watched over everything I wrote and got the possibility to correct my sentences.

The aim of this thesis was to increase knowledge and understanding of the professionals working in multi-vendor environment. Through the research I got plenty of information as well. I hope that this thesis and its interview questions and answers will help the readers to expand their interests in thinking how these matters have been dealt with in their own organization.

The research was an interesting and challenging experience. The process began in autumn 2017 by waking up with the idea of this type of study. We had a brainstorming session with my colleagues to get the baseline for my research and completed a mind map with all the desired pieces that eventually brought together the whole study.

The theme of interview questions I defined by myself by studying the ISO27001, Katakri and VAHTI that have been introduced in this thesis. The interview questions

were sparred by my tutor at work. The interview frame was clearly structured, and it worked smoothly during the interviews. It also helped to analyze the interviews later.

The timetable of the research was quite in line with the plans. A slight delay was caused during the theory part of the research, since it was more difficult as expected to find previous studies and theory of this subject and to analyze it. As references, mostly English studies were used; however, also Finnish studies of incident management and multi-sourced environments.

5.2 Experiences of the research

This research helped me to understand in what kind of field my customers work. The interviews taught a great deal about the customers' environment, their varied situations dealing with multi-vendor environment, and especially the development part which can be used at work.

The literature review taught at the same time a part of the history of the IT environment, and the present situation with multiple service providers; also, something about the future of the vendor management was studied, which was the most interesting topic to learn about.

5.3 Suggestions for further research

During the research, several further research ideas emerged in my mind. The purpose of this research was to study business customers' thoughts and experiences from their perspective. The number of respondents was five persons from four companies. They represented themselves, not their employers, which made it easier for the interviewee to give sincere and truthful answers. Thus, a further research challenge could be a wider sample of interviewees.

This research aimed at respondent's anonymity by mixing up the answers gotten from the interviews. One might want to make a more detailed partition of the organizations or even compare the answers with each other. Then the study could help to understand the differences between large and smaller companies.

During the study I also thought about making the interview within the same company but for people in various positions. This could reveal if there is a great deal of various kinds of thinking, different opinions and ways to work inside the company.

Another research method might be a quantitative approach with a questionnaire with a significantly larger number of respondents. The researcher needs to learn how to select the right types of survey questions and how to motivate the respondents to participate.

References

A Business Framework for the Governance and Management of Enterprise IT. 2012. COBIT website. Accessed on 24 February 2018. Retrieved from http://www.isaca.org/cobit/pages/default.aspx

Eskola J. & Suoranta J. 2008. *Johdatus laadulliseen tutkimukseen* [Introduction to qualitative research]. Tampere: Vastapaino.

Foddy, W. 1995. *Constructing questions for interviews and questionnaires*. Theory and practice in social research. 3rd. ed. Cambridge: Cambridge University Press.

Hammond, G. 2012. *On The Making of History: John Boyd and American Security*. Air Force Academy archive. Accessed 18 February 2018. Retrieved from https://web.archive.org/web/20140327071401/http://www.usafa.edu/df/dfh/docs/Harmon54.pdf

Haughey, D. 2018. RACI Matrix. Project Smart official website Accessed 20 March 2018. Retrieved from https://www.projectsmart.co.uk/pdf/raci-matrix.pdf

Heikkilä, R. 2014. Häiriönhallinnan haasteet ja niiden ratkaisut monitoimittajaympäristössä [Critical Challenges of Incident Management and their solutions in Multisourcing Environment]. Bachelor's Thesis. University of Jyväskylä. Department of Computer Science and Information Systems. Accessed 11 January 2018. Retrieved from https://jyx.jyu.fi/dspace/bitstream/handle/123456789/43226/Riina%20Heikkil%E4.pdf?sequence=1

Hirsjärvi, S., Remes, P., & Sajavaara, P. 2007. *Tutki ja kirjoita* [Research and write]. 13th. ed. Helsinki: Tammi.

Info-Tech. 2018. *Get Ready for the Evolution of Vendor Management*. Official website. Accessed 13 March 2018. Retrieved from https://www.infotech.com/research/ss/get-ready-for-the-evolution-of-vendor-management

ISO 2017. ISO official website. Accessed 12 January 2018. Retrieved from https://www.iso.org/about-us.html

ISO/IEC 27000. Fifth edition 2018-02. Accessed 8 April 2018. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

ITIL. 2018. Official website. Accessed 12 January 2018. Retrieved from https://www.axelos.com/best-practice-solutions/itil

JYVSECTEC. 2018. Official website. Accessed 11 February 2018. Retrieved from https://jyvsectec.fi/en/services/cyber-exercises/

Järvinen, A., & Järvinen, P. 2004. *Tutkimustyön metodeista* [Research methods]. Tiedekirjakauppa TAJU.

McNamara C. 1999. *General Guidelines for Conducting Research Interviews*. Accessed 3 March 2018. Retrieved from https://managementhelp.org/businessresearch/interviews.htm

Ministry of Defence, Finland. 2015. Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. Accessed 12 January 2018. Retrieved from http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Ministry of Finance, Finland 2017. VAHTI 8/2017. Accessed 10 January 2018. Retrieved from http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf

Payne, G. 2015. Microsoft Technet Blog. *The pros and cons of multi-vendor technology environments*. Accessed 11 January 2018. Retrieved from https://blogs.technet.microsoft.com/uktechnet/2015/07/20/the-pros-and-cons-of-multi-vendor-technology-environments/

Reyes, A. 2015. Outsourced incident management services. Master's Thesis. Aalto University. School of Science. Accessed 10 January 2018. Retrieved from https://aaltodoc.aalto.fi/bitstream/handle/123456789/19040/master_Reyes_Zuniga_Alfredo_2015.pdf?sequence=1

Riverbed. 2018. *End-to-End Performance Management*. Riverbed official website. Accessed 11 February 2018. Retrieved from https://www.riverbed.com/pl/solutions/end-to-end-performance-management.html

Sallé, M. 2004. *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing*. Accessed 3 January 2018. Retrieved from http://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf

Schneier, B. 2014. *The Future of Incident Response*. IEEE Journals. Accessed 18 February 2018. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924685

SFS-ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. 2017. Accessed 20 February 2018. Retrieved from http://www.iso27001security.com/html/27001.html

SFS-ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. Accessed 12 January 2018. Retrieved from http://www.iso27001security.com/html/27002.html

Tenkamaa J. 2017. *Service Intergration and Management (SIAM)*. A course by Wakaru. Jyväskylä 28.12.2017.

Sparrow E. 2003. *Successful IT Outsourcing: From Choosing a Provider to Managing the Project*. Springer-Verlag London Limited.

Sullivan, G. & Qureshi R. 2014. *2014 Strategic Road Map for Vendor Management*. Gartner research. Accessed 11 March 2018. Retrieved from https://www.gartner.com/doc/2764417

Tague, Nancy R. 2004. *The Quality Toolbox*. 2nd. ed. ASQ Quality Press.

Vuorinen, Markus. 2011. IT Service Management Transformation to Utility Computing. Master's Thesis. Laurea University of Applied Sciences. Master Degree in Information Systems. Accessed 18 March 2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-2011060210749

Appendices

Appendix 1.The interview questions in Finnish

Aloitus

- Tutkimuksen tarkoitus ja tulosten käyttö
- Luottamuksellisuus ja suostumuslomake

Taustatiedot

- Millä toimialalla työskentelet?
- Mikä on asemasi yrityksessä?
- Mikä on yrityksen henkilökunnan lukumäärä?

Tietoturvapoikkeamien hallinta

- Onko organisaatiollanne asianmukaiset tavat käsitellä tietoturvapoikkeamia?
- Miten organisaatiossanne on määritelty tietoturvapoikkeamien käsittelyryhmä ja onko henkilöiden vastuut määritelty?
- Kuka tai mikä taho on nähdäksesi vastuussa tietoturvapoikkeaman havainnoinnista, viestimisestä ja vianhallintaprosessin aloittamisesta?
- Miten ulkoinen ja sisäinen viestintä hoidetaan? Onko osapuolilla selvillä mistä viestitään, milloin viestitään, keiden kanssa viestitään ja ketkä viestivät?

Sidosryhmäyhteistyö

- Miten organisaationne on määritellyt tietoturvallisuuden kannalta olennaiset ulkoiset ja sisäiset sidosryhmät?
- Miten näiden sidosryhmien tietoturvallisuutta koskevat vaatimukset on määritelty?
- Miten organisaationne hallitsee kaikkien sidosryhmien riippuvuudet toisistaan, onko ne dokumentoitu ja kaikilla osapuolilla tiedossa?
- Millä tavalla läpinäkyvyyttä ja yhteistyötä eri toimittajien kesken voisi parantaa?
- Onko teidän organisaatiossa harjoiteltu sidosryhmien edustajien kesken tietoturvapoikkeamien prosessia? Jos kyllä, niin millä tavalla?

Kehittäminen

- Miten tietoturvapoikkeamista toipuminen on otettu huomioon jatkuvuus- ja toipumissuunnitelmissa, sisältäen raportoinnin, viestinnän ja oppimisprosessin?
- Miten liiketoimintanne tavoitteet on otettu huomioon monitoimittajaympäristössä?
- Millaisia vaatimuksia liiketoimintanne asettaa häiriönhallinnalle ja täyttyvätkö ne?
- Miten monitoimittajaympäristön kokonaisnäkymää voisi parantaa?
- Millä tavalla kehittäisitte nykyisiä toimintamalleja palveluntarjoajien suhteen?
- Haluatteko vielä kertoa jotain?

Lopetus

- Kiitokset

Appendix 2. Invitation to the survey in Finnish

Arvoisa vastaanottaja

Moni yritys on ulkoistanut IT-palveluitaan useille eri toimittajille, jotka tuottavat palveluja asiakkaalle monitoimittajaympäristössä. Tällaisen ympäristön häiriönhallinta on tullut erittäin tärkeäksi osaksi palveluiden jatkuvuuden kannalta.

Opiskelen Jyväskylän ammattikorkeakoulussa (ylempi AMK) Cyber Security – tutkintoa. Teen opinnäytetyötä aiheesta tietoturvapoikkeamien hallinta monitoimittajaympäristössä. Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma, jonka perusteella tieto, palvelu, luottamuksellisuus tai käytettävyystaso on tai saattaa olla vaarantunut. Tutkimuksen tavoitteena on löytää parhaita käytäntöjä asiakkaan ja palveluntarjoajan välillä erityisesti tietoturvapoikkeamien prosesseissa.

Kerään aineistoa haastattelemalla eri yrityksien henkilöstöä, jotka ovat tekemisissä monien eri palveluntarjoajien kanssa. Haastattelun tarkoituksena on saada arvokasta tietoa kokemuksista monitoimittajaympäristössä ja sen häiriönhallintaprosessien toimivuudesta ja kehitysmahdollisuuksista.

Haastattelukysymykset olen valinnut tutkimalla kolmea eri teosta; ISO-standardia, VAHTI-ohjetta ja Katakria.

- Kansainvälinen ISO/IEC 27001:2013 standardi (Information technology. Security techniques. Information security management systems. Requirements)
- Valtiovarainministeriön 8/2017 julkaisema VAHTI-ohje Tietoturvapoikkeamatilanteiden hallinta, jonka avulla organisaatio voi kehittää oman organisaation ja sidosryhmien yhteistyötä tietoturvapoikkeamien hallinnassa.
- Katakri 2015, Tietoturvallisuuden auditointityökalu viranomaisille. Katakri pitää sisällään vähimmäisvaatimuksen kansallisista säädöksistä ja kansainvälisistä velvoitteista.

Pyydän Sinua osallistumaan tähän tutkimushaastatteluun. Osallistumisesi on täysin vapaaehtoista ja takaan materiaalin luottamuksellisen käsittelyn.

Ystävällisesti

Mika Haapakoski

Appendix 3. Interview Consent Form in Finnish

Mika Haapakoski
K9028@student.jamk.fi
Master's Degree Programme in Information Technology
JAMK University of Applied Sciences

Haastatteluun suostuminen

Suostumus Mika Haapakosken opinnäytetyötutkimukseen osallistumisesta. Tutkimus selvittää tietoturvapoikkeamien prosesseja ja parhaita käytäntöjä asiakkaan ja palveluntarjoajan välillä.

Olen saanut tietoa tutkimuksen tavoitteesta ja suostun kertomaan omakohtaisia kokemuksia ja mielipiteitä ennalta tutustumaani haastattelurunkoon. Tutkimukseen osallistuminen on vapaaehtoista ja minulla on oikeus kieltäytyä osallistumiseni missä vaiheessa tahansa.

Ymmärrän myös, että tietoni ja haastatteluni materiaali käsitellään luottamuksellisesti ja sitä käytetään vain tutkimustarkoitukseen. Haastattelu tullaan tekemään anonyymisti, eikä yksittäinen vastaaja ole tunnistettavissa.

Aika _____

Paikka _____

Suostun osallistumaan tutkimukseen:

_____

Osallistujan allekirjoitus

_____

Nimen selvennys