Master's thesis

Business Information Systems

2013

Teemu Keiski

DEVELOPING SECURITY IN THE SYSTEM DEVELOPMENT LIFECYCLE

– Agenteq Solutions Oy

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Systems (MBA)

May 2013 | 82 pages

Esko Vainikka

Teemu Keiski

DEVELOPING SECURITY IN THE SYSTEM DEVELOPMENT LIFECYCLE - AGENTEQ SOLUTIONS OY

Information security is an increasing concern in the software development business in the EU. Legislation and regulation is an ongoing change due to the EU data protection regulation proposal. Customers and authorities pose also increasing demands for the software vendors.

Information security adds to the overall quality of software and is a characteristic valued by the customers. However, information security is not just about the technical solutions but it is also about the people and processes. This poses challenges to the management of a software development company if it is not prepared for in the risk management approach.

This study was commissioned by Agenteq Solutions Oy and it begins with an overview of the company. The objective was to study the potential of security development in the system development life cycle through the current process maturity level in the company. This study was conducted also to create change. The theory section examines the risk management and information security challenges of a software company.

The practical part consists of implementing a security development project in the company and results to an information security policy and a risk assessment implementation. This leads to the evaluation of the current status on information security activity in the company from the risk management perspective.

The practical section introduces what was learned during the project. The results of the security development project are described. Development suggestions are also made. The secondary objective of this study is to prepare the company also for responding to the information security assurance needs presented for example by the VAHTI guidance.

KEYWORDS:

Information security, risk management, system development life cycle, software development, process development.

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Business Information Systems (YAMK)

Toukokuu 2013 | 82 sivua

Esko Vainikka

Teemu Keiski

TIETOTURVALLISUUDEN KEHITTÄMISTOIMET OHJELMISTOKEHITYKSEN ELINKAARESSA – AGENTEQ SOLUTIONS OY

Tietoturvallisuus on ohjelmistoliiketoiminnan lisääntyvä huolenaihe EU:n alueella. Lainsäädäntö ja määräykset ovat muutosprosessin alaisia johtuen EU:hun suunnitellusta uudesta tietosuoja-asetuksesta. Asiakkaat ja viranomaiset esittävät jatkuvasti uusia vaatimuksia ohjelmistotoimittajille.

Tietoturvallisuus on ohjelmiston laatua parantava elementti. Asiakkaat arvostavat tietoturvallista ohjelmistoa. Tietoturvallisuudessa ei kuitenkaan ole kyse vain teknologiasta vaan myös ihmisistä ja prosesseista. Tämä luo haasteita ohjelmistoyritysten johdolle, jos tähän ei ole riskinhallinnassa varauduttu.

Tämän tutkimuksen toimeksiantaja oli Agenteq Solutions Oy. Tutkimus alkaa yrityksen yleisesittelyllä. Tavoitteena oli tutkia tietoturvallisuuden kehittämismahdollisuuksia ohjelmistokehityksen elinkaaressa yrityksen nykyisen prosessikäytännön kautta. Tutkimuksen tavoitteena oli myös luoda muutospohjaa. Teoriaosuus käsittelee riskinhallintaa ja ohjelmistoyrityksen tietoturvallisuushaasteita.

Tutkimuksen käytännön osuus sisältää tietoturvallisuuden kehittämisprojektin toteutuksen yrityksessä ja johtaa tietoturvapolitiikan käyttöönottoon sekä riskikartoituksen toteutukseen. Tämän tuloksena yrityksen tietoturvatoimien tämänhetkinen tila arvioidaan riskinhallinnallisesta näkökulmasta.

Käytännön osiossa kerrotaan myös projektin aikana opitut asiat. Kehittämisprojektin tulokset esitetään ja kehitysehdotuksia tehdään. Tutkimuksen toissijainen tavoite oli valmistella yritystä vastaamaan tietoturvallisuuden varmentamisvaatimuksiin joita muun muassa VAHTI-ohjeistus asettaa.

ASIASANAT:

Tietoturvallisuus, riskinhallinta, ohjelmistokehityksen elinkaari, ohjelmistokehitys, prosessikehitys.

CONTENT

FIGURES

TABLES

1 INTRODUCTION

1.1 Agenteq Solutions Oy

Agenteq Solutions Oy (later Agenteq Oy), founded in 1999, is a software company located in Salo, Helsinki, Rauma and Savonlinna. Agenteq Oy provides software development, consultant and subcontracted work services for customers in Finland. The main customer line is real estate and the communication sectors (Agenteq Solutions Oy 2012a). The main product is Tampuuri (Suomen Talokeskus Oy 2012a). Agenteq Oy operates as a product development company for real estate markets. The company also provides services for software project customers. The project business was a major line before the Tampuuri product gained its current success. The project customers range from public to sports organisations.

The turnover of Agenteq Oy was approximately 6.3 million euros in 2012, and the company currently has 59 employees. Agenteq Oy is owned by Suomen Talokeskus Oy, which is an engineering office providing various types of specialist services for real estate renovation, maintenance and energy management (Suomen Talokeskus Oy 2012a). Suomen Talokeskus Oy was previously responsible for the development of the Tampuuri product but the responsibilities were transferred to Agenteq Oy in 2008, which included sales, marketing and contractual obligations (Agenteq Solutions Oy 2012b). Suomen Talokeskus Oy is now focusing on providing services to Tampuuri in addition to their traditional services.

Organisation

The organisational structure of Agenteq Oy in 2012 is described in figure 1. The company is divided into three business units which operate with software development.

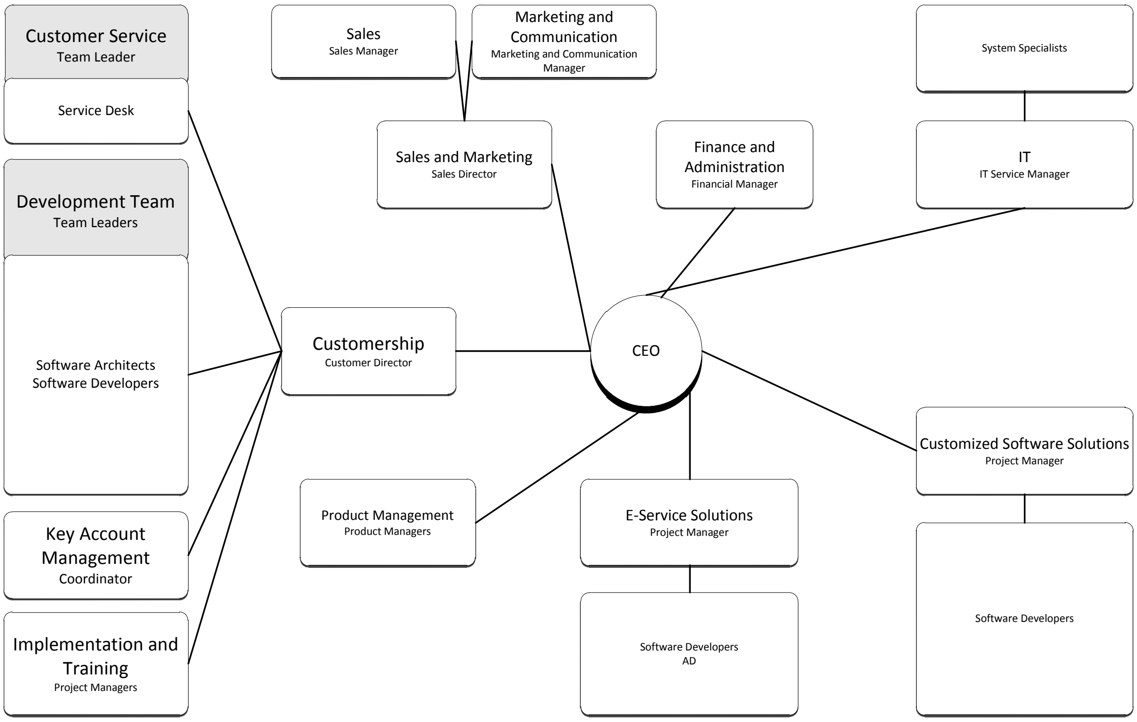


Figure 1. Organisational structure of Agenteq Oy in 2012 (Agenteq Solutions Oy 2012c).

The customership unit develops the Tampuuri product together with product management, and focus on the real estate industry. The e-service solutions unit provides e-services on top of Tampuuri but also on top of other products such as the Latomo publishing system. The e-service solutions unit is also heavily involved in the real estate industry. The customised software solutions unit operates independently servicing customers in other industries. The other units exist as overall support to these business units.

The information security policy

Agenteq Oy implemented an information security policy during 2012. Planning of the policy started in March 2012 and it was finalised and published in August 2012. The information security policy was created by an information security development group (also referred to later as the steering group) consisting of the CEO, the IT Service Manager and the main researcher of this development. However, it was finalised, revised and accepted by the management group and the CEO (J Borenius 2012, pers. comm. 20 August).

The information security policy is relevant from a development work perspective since it created the framework which specifies the scope and position of information security. It also gives the mandate for working in the company to improve information security. The information security policy is an important guideline for this development work. Agenteq Oy’s information security policy specifies the goals, demands of the operating environment, risk management, significance of information security, and the information security activity in the company. The three lines of relevant information to be protected are specified as:

- Information owned by customers
- Information concerning customers, in possession of Agenteq Oy’s personnel
- Information concerning Agenteq Solution Oy’s own business (Agenteq Solutions Oy 2012d).

It is stated that Agenteq Oy is in the middle of legislative requirements as it processes customer’s personal data in its products. However, customer demands and expectations have also increased to the level, which justifies the acknowledgment and development of information security. It also enforces the search for an overall better process where information security forms an integrated part. (Agenteq Solutions Oy 2012d.)

While being developed the role of the information security policy was to guide the upstream process which for example consisted of finding and documenting the relevant pieces of information in possession of the company. The actual development work started right after the policy was finalised and published.

1.2 Tampuuri product

Tampuuri is a web-based information system for real-estate business actors such as housing managers, real estate service companies, public sector organisations, property management companies, rental service companies, associations, and major real estate owners (Agenteq Solutions Oy 2012e). Tampuuri is a so-called real estate information system which is an information system developed specifically for real estate administration and management. Real estate information systems help parties related to real estate property to manage information related to administrating, managing and developing the various real estate functions. (Suomen Talokeskus Oy 2012e.)

Tampuuri is provided as a SaaS-service which means that Agenteq Oy is also responsible for the operating and maintenance of the system. Most of the customers use Agenteq Oy’s hosting model. However, some of the customers also have also acquired a dedicated installation. These are hosted in the customer’s own environment. From a customer’s point of view, acquiring Tampuuri is procuring software from the cloud. Some integration solutions, for example banking software, blur this line because not all operational software is included in Tampuuri. The customer also needs to integrate some of their own software into Tampuuri in order for the processes to work completely. This is seen as vertical integration.

There is currently an evolving necessity to get closer to a cloud service model. Agenteq Oy is relocating from the single customer’s context to multi-customer services and processes and provides e-services. Networking and integration occurs at the Tampuuri-installation level that will involve connecting and integrating Tampuuri customers. This is seen as creating a Tampuuri cloud which could mean accessing data at a network level and using this wider-scale access for providing branch-level information services. For example, a performance analysis of actors on a certain area would create more business opportunities by connecting customers with each other when they could offer peer services. (Borenius 2012.)

From a technical standpoint, the Tampuuri product is implemented with Microsoft technologies including the .NET framework and a SQL Server database.

1.3 Context of the development work

1.3.1 Operating environment pressure

Growth has pushed Agenteq Oy to a level where current working methods are not adequate enough. There are continuous development needs must be prioritised and addressed. Over the last couple of years the company has reached a total of 50 employees. Simultaneously, global news reports feature network security breaches and information disclosures almost daily. This has raised concerns in the management about the effort the company has placed on information security. The new CEO of Agenteq Oy started in his position at the beginning of 2012. He has actively started working on developing information security awareness within the company.

The attitude towards software development companies has tightened concerning information security. The data protection ombudsman Reijo Aarnio has stated an open question. He questions that if software companies still develop software after the implementation of the new EU data protection regulation they may not fulfil the legal requirements. According to Aarnio, there have been cases over the years where the software has not made it possible to take care of the legal obligations. The intention of the software development industry is relevant in a situation where legal authorities are receiving new powers to react to illegality. An important consideration is that the current legislation obliges the data controller, but the new data protection regulation proposal is changing this with the “privacy by design” and “privacy by default” obligations. Aarnio believes this brings new business opportunities to the entire industry. (Aarnio 2012.)

The customers of Agenteq Oy are data controllers in their core business in which they set up a personal data file for their own use. The customers are real estate business actors, for example, housing companies, which have legal authority to set up a personal data file. (Personal Data Act 22.4.1999/523.)

Agenteq Oy is under the requirements of the Personal Data Act for any implementation cases of the Tampuuri product as the company’s employees convert data from the customer’s old environment to the newer Tampuuri environment. This is the case when this conversion concerns personal data of the customer’s customers (customers of the data controller). In this case Agenteq Oy is a data processor which processes the personal data on behalf of the data controller. (Personal Data Act 22.4.1999/523.)

Another consideration is the e-services which Agenteq Oy provide to its customers to supplement the Tampuuri product. These services have specific elements which mean they must meet the requirements of the Act on the Protection of Privacy in Electronic Communications. These services match the definition of a value added service. Such a service is based on the processing of identification or location data but with another purpose than provisioning of a network service or communication service. (Act on the Protection of Privacy in Electronic Communications 16.6.2004/516.)

The nature of Agenteq Oy’s business is reaching a point where the integration of business processes between Tampuuri customers is becoming a key feature. Customers need features which connect them to other business actors such as their own customers and suppliers. However this also brings challenges since this must happen securely and also efficiently. While data is being transferred from one system to another, Agenteq Oy’s role is to also take responsibility for security on behalf of the customer. The existing database boundaries are not adequate any longer. The entire Tampuuri environment is seen as an ecosystem where multiple service providers could exist and this requires refreshed thinking. (Borenius 2012.)

1.3.2 Processes in focus

There are three processes which are focused upon in this development work. They are the new feature development process, operator process and customer support process. Software development, distribution, support and maintenance are performed in numerous steps in these processes. Therefore, the main practical security activity is performed, or should be performed, in these steps as well. These processes form the core of Agenteq Oy's software development lifecycle. This has implications for the company's customers which look at this from a buyer's perspective since Agenteq Oy is a software vendor for them. There also exists the implementation project process – led by the customership unit - but its role exists when customers initially implement Tampuuri for their use. The project managers involved in implementation projects are business specialists, not technical persons. The technical implementation work arrives at the IT unit in Agenteq Oy with the data conversions from the old software format to Tampuuris and software development being performed by the Tampuuri's development team. These tasks are included in the tasks for new feature development process (sprints) described in chapter 1.3.3. The implementation project process is a little out the context for this development work and therefore it is not covered in detail. However, from the system development life cycle (SDLC) perspective the existence of the process is acknowledged. The SDLC is a structured methodology which can be used by an organisation to effectively develop an information system (NIST 2008, 5).

The actors in the three processes are described in Table 1.

Table 1. Actors in the main processes.

Actor	Description
Customer	A company operating in the real estate industry and using the Tampuuri product for its business.
Development Team (Production)	Sub-team in the production unit that focuses on the development of certain industry features.

(to be continued)

Table 1 (continues).

Actor	Description
Development Team Leader	Supervisor of the software development team.
Extended Product Management Team	A group consisting of the CEO, Customer Director, Sales Director and all of the product managers.
Operator	Technical personnel focusing on software maintenance and distribution.
Product Manager	A sales-oriented member of personnel who focuses on product features so that they fulfil customer and industry needs.
Sales	Sales Manager or Sales Director that focus on selling new Tampuuri installations.
Support Service Team	A team of service desk people focusing on customer support activities- A team responds to support calls and communicates with the customers, testers and the development team.
Support System	Internal software system in which support tickets are maintained.
Test Team	A team of test engineers focusing on testing new features and distribution versions

The actors are basically relevant stakeholders in the processes (except the support system). Chapters 1.3.3 to 1.3.5 describe these processes in detail.

1.3.3 New feature development process

The first is the new feature development process (Figure 2), which governs software feature development from an idea to delivering a new version. This process is the most complex, and involves the biggest number of actors in the company. The process involves a customer, a sales person, a product manager, the extended product management team, the development team leader, developers from the production team, and testers from the test team.

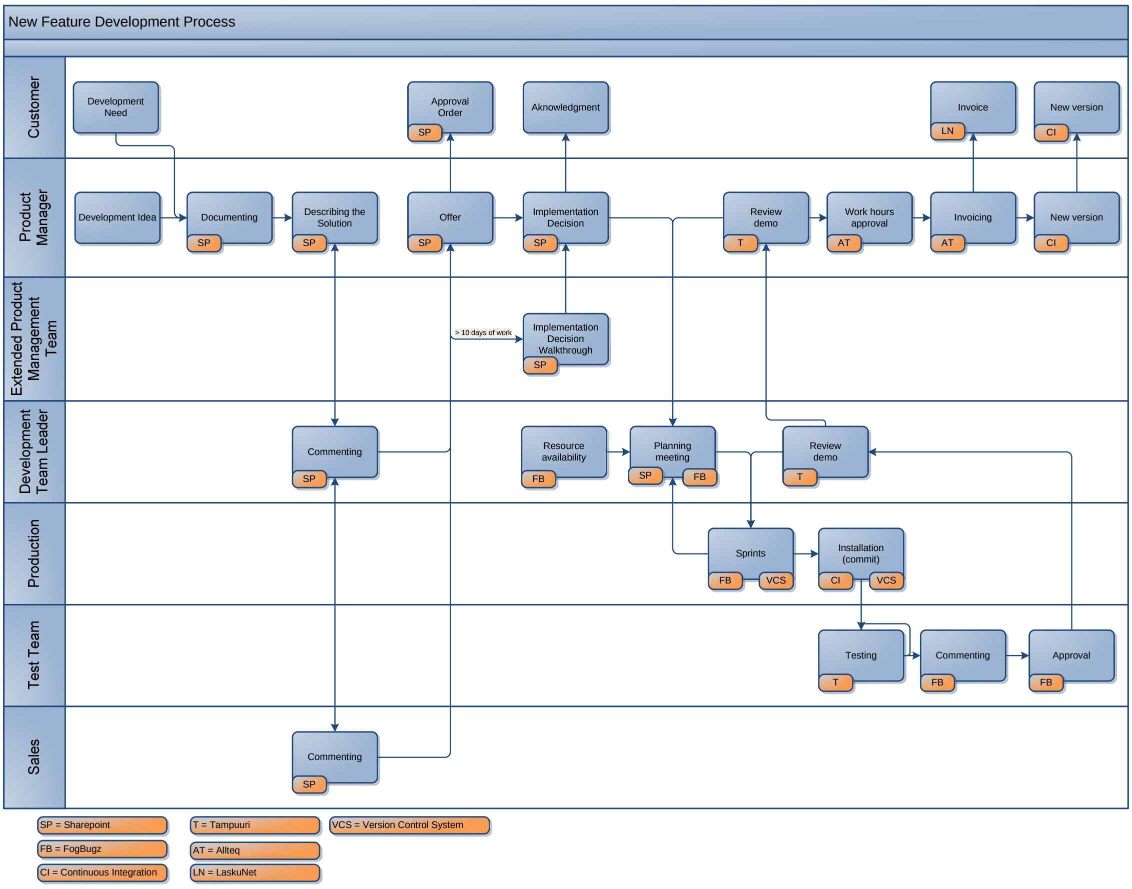


Figure 2. New feature development process (Agenteq Solutions Oy 2012f).

The process starts with an idea from a customer or a product manager. This is then documented and placed in the internal document location dedicated for features from the product management perspective. A support case, described in detail in the operator process subchapter, might also be a source for a development idea. The product manager describes the solution at a business requirement level and asks comments from sales people and the software development team.

In the next step, an offer is made to the customer. In cases where the amount of work exceeds ten days, the idea is also presented to the extended product management team. Based on feedback from the extended product management team the product manager does an implementation decision and the customer will be acknowledged. The acknowledgement contains information about the initially expected delivery schedule. Simultaneously, the development team leader performs an initial resource allocation for the task in question.

The development task advances in accordance with the scrum agile methodology model. As described by Paul (2011, 245), the scrum methodology is based on adjusted-lengths of release cycles, called sprints, to allow the requirement changes on the fly. The software is in constant state of readiness for release after a sprint (Paul 2011, 245). The heart of scrum methodology, as in any agile practise, is early and frequent delivery of working software, close collaboration between developers and customers, self-organising teams and a focus on adaptation to changing circumstances (Bass et al. 2013, 45).

In Agenteq Oy the development team operates in two-week sprints which always start with a planning meeting in which the entire development team and the product manager participate. The development task is processed, along with others, in the planning meeting and in case it is feasible – based on workload and what’s been promised to the customer - it might be chosen to be processed in the sprint to develop a new feature. Processing by the development team includes:

- Requirements clarification
- Development plan creation
- Technical implementation specification creation
- Design
- Coding
- Testing
- Documenting
- Adding and maintaining the source control repository
- Installing the feature to the test site

- Adding the used work hours to the invoicing system.

The test team assesses the feature on the test site and provides their feedback which is taken into consideration in the sprint review demo session viewed by the entire development team. This session ends a sprint. The product manager along with the development team leader either approves or rejects the feature based on implementation documentation and the test team's feedback. If the feature is rejected it is taken automatically for work in the following sprint.

Finally, the work hours consumed to complete the feature are approved and are used as a basis for invoicing the customer. The customer receives an invoice and the feature adds up to the new software version. The feature is installed to the customer within the software distribution version and this is performed in the operator process described in the next subchapter.

1.3.4 Operator process

The aim of the operator process, described in figure 3, is to deliver a new software version or a fix to the customer environment. The customer environment is usually the customer's own test environment and after the customer has accepted the version in their test environment, the process is repeated for the production environment. Actors in the operator process include the development team, an operator which includes people from the IT team, and test team, and the customer.

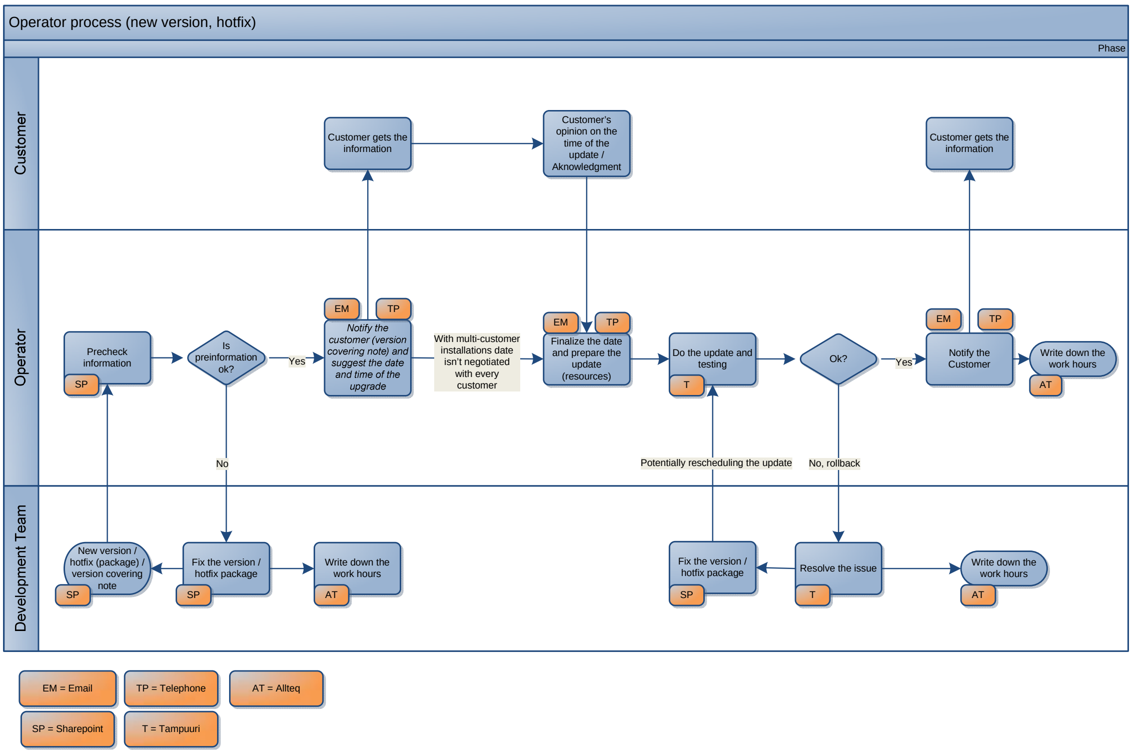

Operator process (new version, hotfix)
Phase
Customer
Operator
Development Team
Customer gets the information
Customer's opinion on the time of the update / Aknowledgment
Customer gets the information
Precheck information
SP
Is preinformation ok?
Yes
No
EM
TP
Notify the customer (version covering note) and suggest the date and time of the upgrade
With multi-customer installations date isn't negotiated with every customer
EM
TP
Finalize the date and prepare the update (resources)
Do the update and testing
T
Ok?
Yes
EM
TP
Notify the Customer
Write down the work hours
AT
Potentially rescheduling the update
No, rollback
New version / hotfix (package) / version covering note
SP
Fix the version / hotfix package
SP
Write down the work hours
AT
Fix the version / hotfix package
SP
Resolve the issue
T
Write down the work hours
AT
EM = Email
TP = Telephone
AT = Allteq
SP = Sharepoint
T = Tampuuri

Figure 3. Operator process (Agenteq Solutions Oy 2012g).

The process starts with the development team (but also with the help of a product manager) writing up a version cover note for the version, or a fix. The operator pre-checks this information and asks the development team to fix this if there are shortcomings. When the version information is ok, the customer is notified about the new version with the version cover note as a reference. If the customer has a dedicated software installation, the time and date of the upgrade is suggested. In cases where there are multi-customer installations, the upgrade date is not negotiated. With the dedicated installation customers, the date and time of the upgrade is finalised by negotiating. The resources are also prepared and allocated for the updates right after the dates are known.

The process proceeds to the actual update step. The software is updated and testers in the operator role also perform tests in the target environment in order to ensure the quality is withheld. If the update has severe critical failures it is rolled back and the development team needs to resolve the issue. This also leads to rescheduling the update. However, if there are issues, they are solved during the update step so rescheduling occurs very rarely. In any case, if the update fails or succeeds, the customer is notified that they can continue their process with the environment or if the update needs to be rescheduled. Every participant in the process also writes up their working hours to the invoicing system. The operator process marks the step when the feature or version is distributed to the customer and is transferred to the customer support process, which is described in the next subchapter.

1.3.5 Customer support process

The aim of the customer support process (figure 4) is to support the customer's procedures with the current software distribution version. Actors in the process include customer, support service team and the development team. The support system is also included as a separate actor because its role is essential in supporting the process by storing the support tickets.

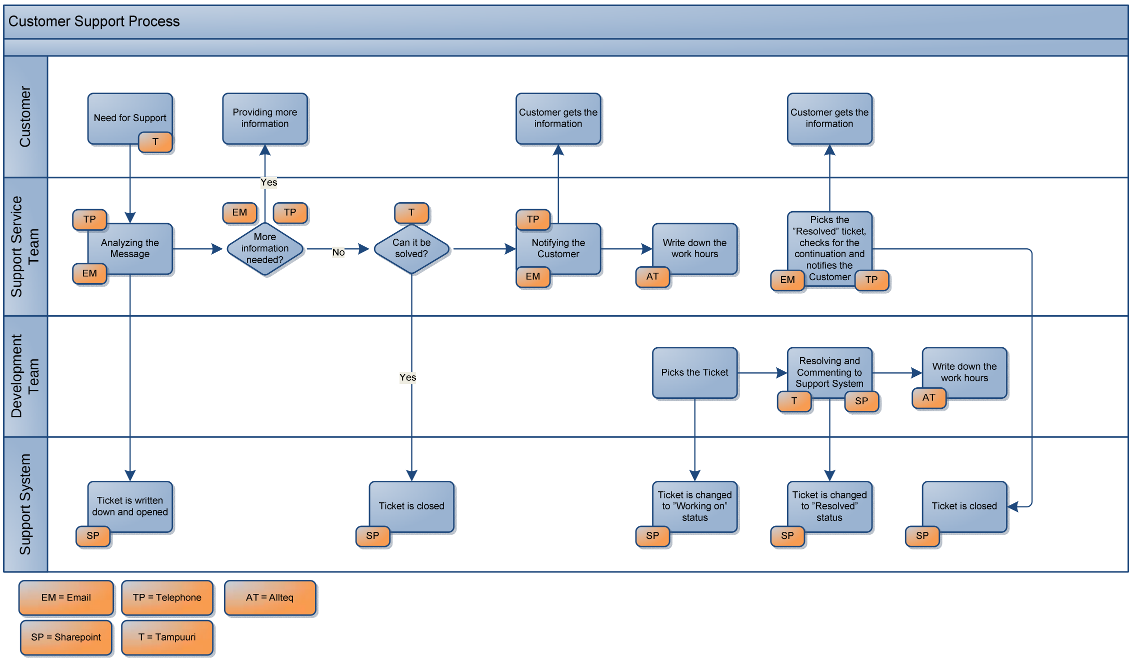

Customer Support Process
Customer
Support Service Team
Development Team
Support System
Need for Support
T
Providing more information
Customer gets the information
Customer gets the information
TP
Analyzing the Message
EM
Yes
EM
TP
More information needed?
No
T
Can it be solved?
TP
Notifying the Customer
EM
Write down the work hours
AT
Picks the "Resolved" ticket, checks for the continuation and notifies the Customer
EM
TP
Yes
Picks the Ticket
Resolving and Commenting to Support System
T
SP
Write down the work hours
AT
Ticket is written down and opened
SP
Ticket is closed
SP
Ticket is changed to "Working on" status
SP
Ticket is changed to "Resolved" status
SP
Ticket is closed
SP
EM = Email
TP = Telephone
AT = Allteq
SP = Sharepoint
T = Tampuuri

Figure 4. Customer support process (Agenteq Solutions Oy 2012h).

The customer support process starts when a customer expresses the need for support by contacting the support personnel via telephone or e-mail. The customer's message is analysed and a support ticket is opened in the support system. If more information is needed from the customer, he or she is notified and asked to provide the necessary information. If customer support can solve the ticket with the given information, the customer is given a solution and the ticket is closed. If customer support cannot solve the ticket, the customer is notified that the ticket has been transferred to another responsible development team for solving the issue.

The development team actively follows the assigned support tickets during their working shift. The development team takes a support ticket under working status and aims to resolve it as quickly as possible. When the issue is resolved, the development team writes comments to the ticket and changes the ticket to a resolved status. The support service team follows tickets resolved by the development team. The support service team answers the customer with a solution and closes the ticket. If there are any issues, the ticket is returned to the development team for further inspection. Participants of the customer support process actively write down their working hours to the invoicing system.

1.4 Research process

1.4.1 Research problem and philosophy

Agenteq Oy has no known method for finding and documenting the security development needs in the SDLC, which could be understood by every hierarchical level of the organisation. The level of security risk has been unclear for the management and the related processes have been fragmented and informal. This has made managing risk difficult in practise. The response to potential problems is more reactive than proactive because the problem area is unknown. There has also been an element of reactive culture which Knapp (2010, 220) defines to be simply reacting to events occurring each day. This is a sign of a lower-level of process maturity in general (Knapp 2010, 62). Problems come up mostly in customer interactions where it is often too late from being prevented and the company reputation is in jeopardy of being tarnished. The goal is to improve the recognition of security development needs and integrate risk management in the company software development processes so that it becomes a process as well.

The philosophical assumption of this thesis is interpretivism. Interpretivism builds on the belief that social reality is subjective. Social reality is shaped by human perception. The researcher cannot be separated from what’s being researched. The reality is impacted by the act of researching it. (Collis and Hussey 2009, 57.)

This thesis is carried out by an employee in a software development company. In practise it is impossible to separate the researcher from the company operations for the duration of conducting the research. This is supported by the criticism of positivism stated by Collis and Hussey (2009, 56) that it is impossible to separate people from the social context in which they exist.

From an epistemological assumption standpoint in interpretivism it is attempted to minimise the distance between the researcher and that which is researched. On the other hand, in positivism, it is believed that that only what is observable and measurable can be considered as valid knowledge. Therefore an independent and objective stance is required. (Collis and Hussey 2009, 59.)

This is another argument favoring interpretivism since the researcher has a very short distance to what’s being researched. The researcher acts in the company processes that are being researched. Some form of participative enquiry is very likely to be needed because the research topic requires co-operation with other workers in the company.

In interpretivism the research is an inductive process where interpretive understanding of social phenomena is created in a specific context (Collis and Hussey 2009, 57). This arguments for interpretivism from a research problem standpoint since the purpose is to develop an understanding.

1.4.2 Research method

The research method is action research. Applied research uses the action research methodology to find an effective way to bring conscious change in a partly controlled environment (Collis and Hussey 2009, 81). Action research combines theory and practice through change and reflection (Avison et al. 1999, 94). Action research acknowledges that the social world is constantly changing (Collis and Hussey 2009, 81). The researcher and research are part of this change through involving researchers and practitioners acting together in cycles of the iterative research process (Collis and Hussey 2009, 81; Avison et al. 1999, 94).

Action research focuses on research in action and it is collaborative and democratic by its nature (Coghlan and Brannick 2010, 5). By emphasising collaboration between researchers and practitioners, action research is a promising research method for information systems (Avison et al. 1999, 95). The central idea is that action research uses a scientific approach to study important social or organisational issues together with those who experience these issues directly through nature (Coghlan and Brannick 2010, 5). Action research can be used to address complex problems and concerns of practitioners while contributing to the science (Avison et al. 1999, 95; Collis and Hussey 2009, 81). Members of the system being studied participate actively in the cyclical process of action research by impacting on the research focus and engaging in the action and inquiry (Coghlan and Brannick 2010, 5; Collis and Hussey 2009, 81).

Action research consists of a certain sequence of events and an approach to problem solving. From an event sequence perspective it comprises of iterative cycles of:

- Gathering data
- Feeding data back to those concerned
- Analyzing the data

- Planning action
- Taking action
- Evaluating that leads to data gathering.
  (Coghlan and Brannick 2010, 5.)

In action research the overall process is performed jointly (Coghlan and Brannick 2010, 5). The researcher wants to try out a theory with practitioners in real-world situations, gain feedback from this, modify the theory as a result and try it again (Avison et al. 1999, 95). From a problem solving perspective, action research applies fact-finding and experimentation to practical problems requiring action solutions. The desired outcomes are not just immediate solutions but also learning from intended and unintended outcomes. (Coghlan and Brannick 2010, 5.)

A model of the action research cycle is described in figure 5.

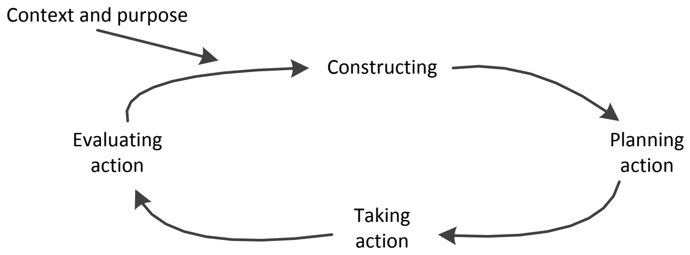


Figure 5. An action research cycle (Coghlan and Brannick 2010, 8).

The context and purpose step is a pre-step in the action research cycle. The step consists of placing questions on the importance and context of the action. The second important consideration is the relationships to those who the questions related to the cycle concern. From the main steps, constructing means forming an understanding what the issues are. The planning action step is a consistent follow up and in line with the previous steps in order to plan the action implementation. Taking action is the step for implementing the plans collaboratively. Evaluating action is the step to examine the outcomes of the action to see if the original action plan was fitting. Did the action match the understanding (construction)? Was the action taken in an appropriate manner? What feedback does the next cycle require? (Coghlan and Brannick 2010, 8 – 10.) In practise, when performing action research, there are multiple cycles occurring concurrently (Coghlan and Brannick 2010, 10). Figure 6 illustrates this.

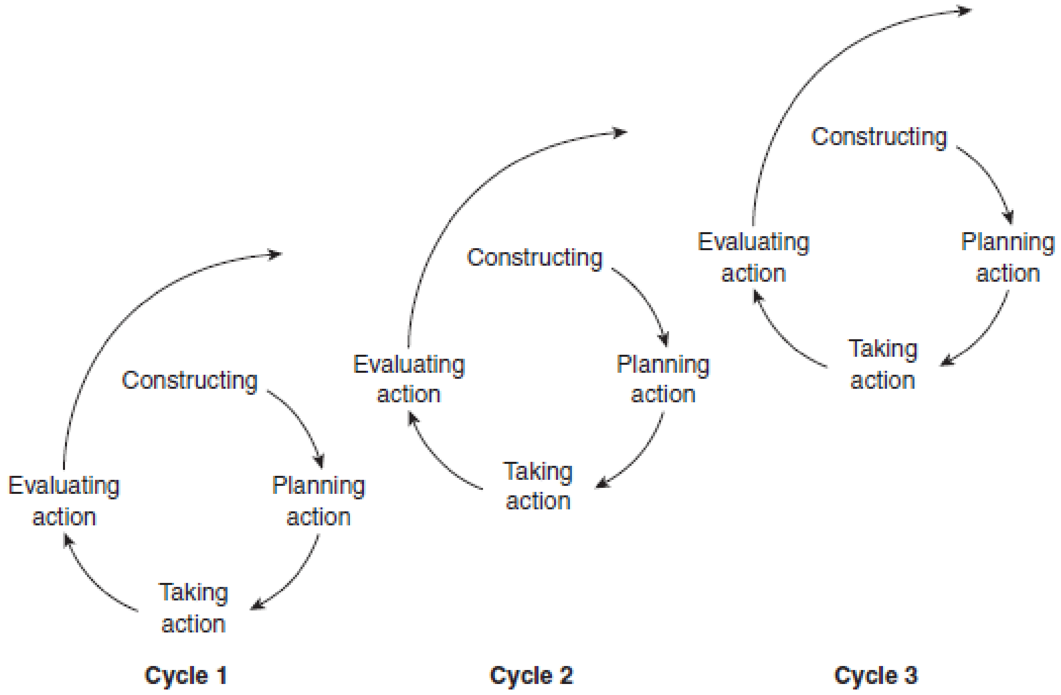


Figure 6. A spiral of action research cycles (Coghlan and Brannick 2010, 10).

The reasoning for selecting action research is that the method is similar to the agile development methods used in Agenteq Oy. Agile software development methods are incremental and iterative. This is seen as a frequent deployment of software in increments, as good collaboration between customers and developers, and as a focus on adapting to changes. (Bass et al. 2013, 43 – 44.) These are qualities strongly relating to action research. The goal is to create change, which is always created in action research. The action research contributes to the planned change process because it has collaborative inquiry and learning built in. (Coghlan and Brannick 2010, 70.) In action research the role of the researcher is dual because the researcher is not separate from the system being researched. The researcher is part of the system as a member of the organisation and as a researcher which can be challenging and also create conflict situations because these roles have varying requirements. (Coghlan and Brannick 2010, 119.)

Data collection methods are in line with the research questions in the research problem. These are listed in table 2.

Table 2. Research questions and data collection methods.

Problem / Research question	Data collection methods
How to find, understand and document the security development needs in the SDLC?	• Information security risk assessment • CEO interview • Asset and process documentation
How to manage risks in the SDLC?	• Information security risk management • Information security best-practises material analysis • Self-assessment
How to turn risk management in the SDLC into a process?	• Information security risk assessment result analysis • Information security best-practises material analysis • Self-assessment • Recommendations and implementations based on previous analysis

The methodology for this is to use data triangulation which means collecting data from different sources or at different times (Collis and Hussey 2009, 85).

2 SECURITY RISK MANAGEMENT

“Security is a measure of the system’s ability to protect data and information from unauthorised access while still providing access to people and systems that are authorised”. A simple approach to characterise security is with confidentiality, integrity and availability. Confidentiality means protecting data or services from unauthorised access. Integrity means protecting data or services from unauthorised manipulation. Availability means keeping the system available for legitimate use. (Bass et al. 2013, 147.)

Business and information processing with systems has risks like any other human activity. These cannot necessarily be removed but their likelihood can be decreased, their impacts can be mitigated, and one can prepare for them or willingly be unprepared for some of the risks. (Hakala et al. 2006, 90.) NIST, National Institute of Standard and Technology, (2002, 1) states that a risk is an impact with negative consequences of the exercise of vulnerability when both the probability and impact of occurrence are considered. A total risk is the likelihood or probability of an unwanted, unintended or harmful event which is computed using factors including the asset value, threat and vulnerability (Paul 2011, 20).

An asset is an item which is valuable to the organisation, the owner of the asset (Landoll 2011, 26). Assets can be tangible, which means they are physically perceivable (example: software code). Assets can also be intangible which means they are more abstract (example: brand reputation). Loss of an asset can jeopardise the organisation’s capability to accomplish its mission. (Paul 2011, 16.) A vulnerability is a flaw that may possibly allow a threat agent to exploit it (Landoll 2011, 29). A vulnerability can also be accidentally triggered (NIST 2002, 12). Vulnerabilities play an important role in risk management and assessment because they are instrumental in risk determination; both existing risk and residual risk (Landoll 2011, 29). A threat is the possibility of a threat source or threat agent to successfully exercise a particular vulnerability (NIST 2002, 12). A threat source or a threat agent is an actor, being anyone or any-thing, human or nonhuman, having the potential to materialise the threat. A threat source intentionally causing a threat to happen is referred to as attacking. (Paul 2011, 18.)

A control is a method to manage the risk and it includes activities, guidance and organisational structures (Hakala et al. 2006, 420). Controls are mechanisms to mitigate the threats to assets (software and systems) (Paul 2011, 19). Residual risk is the risk that remains after the implementation of safeguards (controls). It is a very important element because it is the risk that will be inherited and the organisation's management needs to understand the concept that they need to accept the residual risk. (Hakala et al. 2006, 108; Landoll 2011, 33.) Residual risk should be less than the acceptable risk (Hakala et al. 2006, 92).

These concepts of risk management are described in figure 7. The flow is such that the owners value their assets and wish to minimise the risk to them. Threat agents wish to abuse assets. Threat agents may increase threats that again increase risk to these assets. Threats may exploit vulnerabilities leading to a risk to the assets. These vulnerabilities might be known or unknown to the owners. Known vulnerabilities can be mitigated by implementing controls which reduce the risk to the assets. Controls themselves can also pose risk – by having vulnerabilities - to the assets. (Paul 2011, 25.)

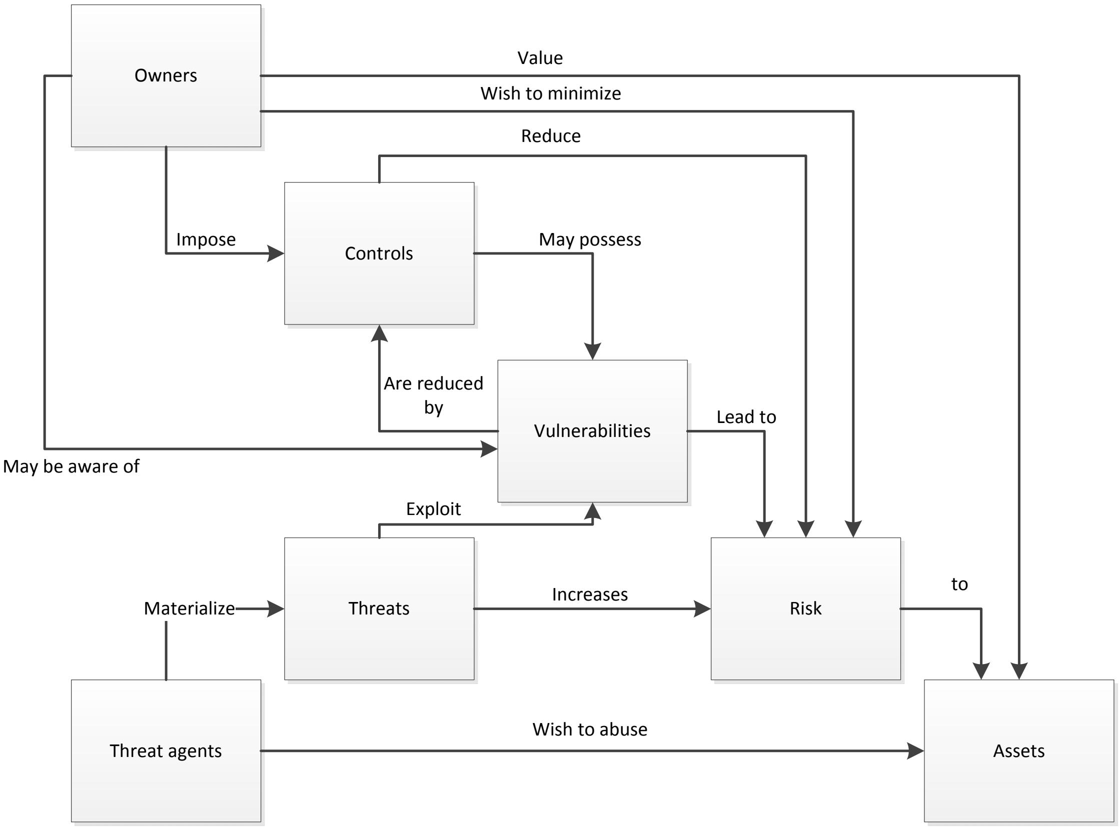


Figure 7. Risk management concept flow (Paul 2011, 25).

Information security risk is one component of organisational risk which can consist of many types of risks such as legal liability risks, and program management risks, etc. Information security risk is commonly linked to the operation and usage of information systems. (NIST 2011, 1.)

Risk management is the process of identifying risk, assessing risk and reducing risk (NIST 2002,1). The goal of risk management is to reduce a risk to an acceptable level (Paul 2011, 18 – 19). Risk management, however, does span more than the protection of IT assets as the intention is to protect the entire organisation. Risk management, in the context of software security, is balancing between IT assets and the cost of implementing security controls, so that the risk can be handled. (Paul 2011, 15 - 16.) Risk management, along with setting the criteria for acceptable risk is the responsibility of an organisation's management. However, in practice the evaluation criteria is created and defined by the information management unit of the organisation. (Hakala et al. 2006, 90.)

NIST (2011, 8) expands the definition of the risk management process to consist of four components: framing risk, assessing risk, responding to risk and monitoring risk. The relationship of these components is described in figure 8.

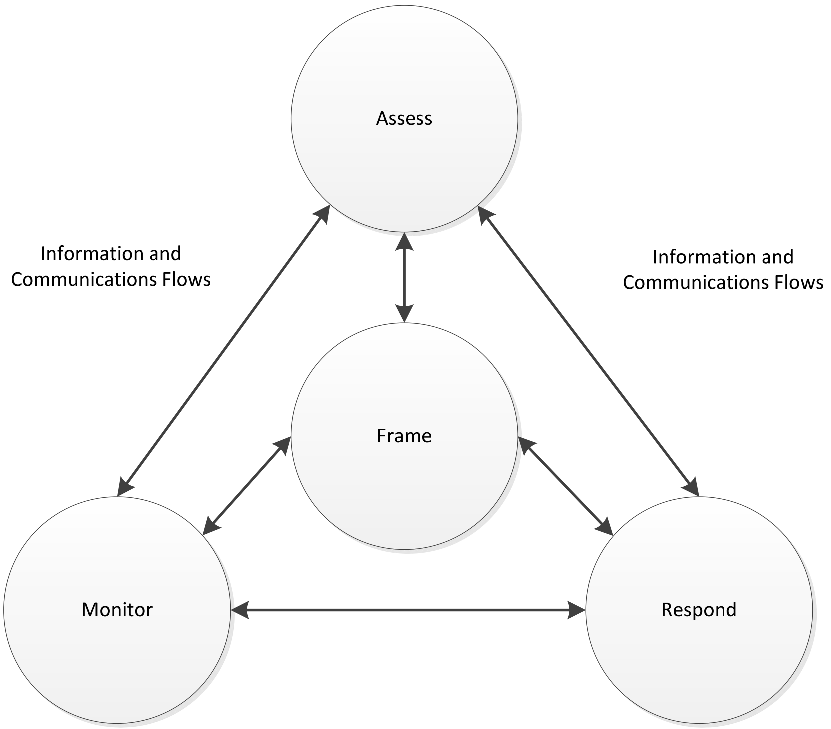

Assess
Information and Communications Flows
Information and Communications Flows
Frame
Monitor
Respond

Figure 8. Risk management process (NIST 2011, 8).

The risk framing component is when an organisation establishes a risk context. It means describing the environment in which risk based decisions are made. The ultimate aim is to produce a risk management strategy which sets the boundaries for risk-based decisions. The risk assessment step specifies how organisations assess risk in the context specified in the framing component. (NIST 2012, 4 – 5.)

In a security risk assessment, the components include an organisation’s threat environment, the asset values, the system’s criticality, the security controls and vulnerabilities and the expected impact of any loss are reviewed. The step provides further recommendations for risk reduction. (Landoll 2011, 4.) The end result is a determination of risk (NIST 2012, 5). Based on it, senior management can determine if additional controls are required (Landoll 2011, 4).

Responding to risk is the third component. Its role is to address how risk is responded to after it is determined based on the risk assessment results. The purpose is to create an organisation-wide risk response by developing alternative courses of action, determining appropriate courses of action (considering the organisation's risk tolerance) and implementing selected courses of action. (NIST 2012, 5.)

The fourth component is risk monitoring. The purpose is to monitor the risk over a period of time to create an understanding of what is the effectiveness of ongoing risk responses and verify that information security requirements are derived from and traceable to the organisational mission. An important task is to also identify the changes in the risk environment and consider an organisation's information systems. (NIST 2012,5.)

Risk management integration into an organisation's SDLC is essential to make it work effectively. An organisation wants to minimise the impact of risk and have a clear basis for decision making. These are important reasons for implementing risk management for IT systems (NIST 2002, 4.) The key thing is to realise that information security activities can bring lots of valuable input into IT system management and development, which enables risk identification, planning and mitigation activities. A risk management approach for systems and projects means integrating security early and throughout the established SDLC. This enables security to be developed as an integral part of the system. (NIST 2008, 4.) The system development lifecycle or software development lifecycle (which is the synonym) consists of five steps. These steps are described in table 3.

Table 3. SDLC steps (NIST 2002, 5; NIST 2008, 13 – 37).

SDLC step	Description
Initiation	The need, purpose and scope for the software is expressed and documented. The software requirements are developed.
Development / Acquisition	The software is designed and developed (or procured).

(to be continued)

Table 3 (continues).

SDLC step	Description
Implementation / Assessment	The software is configured, enabled, tested and verified for production use.
Operation / Maintenance	The software performs its function in a production environment and is being modified through potential hardware and other (code) changes or additions as well as by changes to organisational practices.
Disposal	The system is shut down and data is archived and moved to another (new) system.

The related risk management activities for SDLC steps are described in table 4.

Table 4. SDLC steps and related risk management activities (NIST 2002, 5; NIST 2008, 13 – 37).

SDLC step	Risk management / security activity
Initiation	Identified risks are used in developing the software requirements, including the security requirements so that it is ensured that threats and potential functionality and integration constraints are considered in line with the requirements. Security is looked at through business risks.
Development / Acquisition	Identified risks are used to support security analyses of the software. This might have an impact on the architecture and design of the software. Security requirements are being analysed, security architecture is designed and functional and security testing is being completed.
Implementation / Assessment	Risk management supports the assessment of the software by comparing software implementation against the requirements and within the operational environment. Management of identified risks must be decided before software is moved to operation. Software is integrated to its environment, security controls are tested, and the accreditation is completed.
Operation / Maintenance	Risk management activities are performed in line with software being re-authorised and monitored for performance in a periodic process. The software is reassessed when the IT has faced major changes in the operational environment such as new features are developed and tested, or new hardware is added or replaced. The software's operational readiness is reviewed, the system configuration is managed and the processes and procedures for monitoring of the system are being set up.

(to be continued)

Table 4 (continues).

SDLC step	Risk management / security activity
Disposal	Risk management activities are performed for disposable or replaceable software components so that disposal is performed properly, and that residual data is being handled appropriately and migration to new system happens securely. Closing out of any contracts happens at this stage. Disposal must happen within a transition plan and the needed archiving and sanitisation must be considered before execution.

It is important from Agenteq Oy's perspective to realise the mapping of company processes (described in chapter 1.3 and related subchapters) to SDLC steps because this focuses the risk management activities. The mapping is described in table 5.

Table 5. Mapping SDLC steps and Agenteq Oy's SDLC processes.

SDLC step	Agenteq Oy's process
Initiation	New feature development process
Development / Acquisition	New feature development process
Implementation	New feature development process , implementation project process, operator process
Operation / Maintenance	Customer support process, operator process
Disposal	No specific documented process

Agenteq Oy's implementation project process is acknowledged here. However, in the context of this development work it means the implementation of new features for customer installations, and not implementing new Tampuuri installations as it also concerns Agenteq Oy's product fulfillment scenarios. From an overall security perspective acknowledging the implementation project process is very important but it falls out of the scope of this development work because the impact of implementation projects (to the overall security) occurs through the existing, previously described processes. An important finding is also that a documented process does not exist for the disposal step of the SDLC.

Risk assessment

Risk assessment is a component of the organisational risk management process. The role of risk assessment is imperative in ensuring that leaders and managers make informed decisions that support the missions and business functions of their organisations. (NIST 2012, 1.) Risk assessment is an analysis of the current state of security, implemented through controls that protect an organisation's assets, and a review of the probability of losses to those assets (Landoll 2011, 23). Risk assessments can be performed on three levels: on an organisation level, on a mission/business process level, and on an information system level (NIST 2012, 1). On the lowest, the information system level, risk assessment can be used to determine the information system's vulnerability to attacks through identifying functionality aspects which might need deep security review (Microsoft Corporation 2012, 20). On the two higher levels, organisations use a risk assessment to evaluate risks at the organisation and management level (NIST 2012, 1). The significance of a risk assessment on these levels is described in table 6.

Table 6. Risk assessment at organisational levels (NIST 2012, 18 – 20).

Level	Risk assessment's significance
Organisational	• Focus on organisational operations, assets and individuals • Support for strategies policies, guidance and processes • Results are communicated to organisational entities at other levels
Mission / Business process	• Focus on missions/business process protections and resiliency requirements • Guidance for information system usage and help for managing information security architecture • Results are communicated to organisational entities at other levels

(to be continued)

Table 6 (continues).

Level	Risk assessment's significance
Information System	• The scope is specified by the missions / business process level context and the SDLC • Evaluates predicted vulnerabilities and predisposing conditions which might affect the information system's confidentiality, integrity and availability • Results are communicated to organisational entities at other levels

The next issue to be covered is the risk assessment process in the security context. A simplified description of this process is outlined in figure 9.

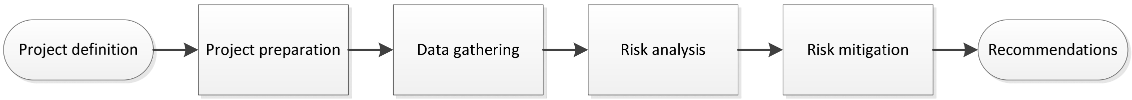


Figure 9. Security risk assessment process (Landoll 2011, 24).

The first step in the security risk assessment process is project definition. At this point the project scope must be decided, taking into consideration the impacting factors such as budget, the project's objective, and what it is being assessed for, for example, the covered assets, the controls, and the boundaries of the project. The second step is project preparation in which a team is selected and introduced to the organisation. The factors impacting a team members selection includes the expertise and experience of the candidate. Other related tasks are reviewing the business mission, mapping assets, identifying critical systems, identifying threats and determining expected controls. (Landoll 2011, 23 – 25.)

The third step is data gathering in which data is collected at an administrative, technical, and physical level about the effectiveness of current security controls. This step is the most comprehensive of them all. The fourth step is risk analysis. Risk analysis is a review of the gathered data and the result is an analysis of the risk to the organisation. The risk assessment team determines asset values, system criticality, potential threats, existence of vulnerabilities, and calculates the risk for each threat/vulnerability pair. There are various methods for this step so calculations and presentations of risks can vary greatly (Landoll 2011, 23 – 31.) Landoll (2011, 31) also states that deriving and presenting the risk can be performed quantitatively or qualitatively. However, NIST (2012, 14) includes definition of semi-quantitative risk calculation and states that all of these approaches have their advantages and disadvantages.

The quantitative method relies on using specific formulas and calculations to determine the value of the security risk (Landoll 2011, 31). This is based on using numbers and this type of assessment mostly benefits if cost-benefit analyses of alternative risk responses are being developed (NIST 2012, 14). The advantage here is objectivity and the ability to express in money, whilst the downside is that the calculations can be very complex and achieving accurate values can be difficult (Landoll 2011, 14). NIST (2012, 14) also adds that the quantification process is probably not reliable if there is any uncertainty in determination of the values and that sometimes the costs might outweigh the benefits of a quantitative approach. On the other hand, the qualitative method relies on subjective measures in asset valuation (Landoll 2011, 31). This method is based on using non-numeric categories or levels (for example: low, medium, high) (NIST 2012, 14). This has the advantage of being easy to understand and in most of the cases, it provides an accurate enough indication of the security risk to an organisation (Landoll 2011, 31). The communication to decision makers is also easier (NIST 2012, 14). The downside here is that there is subjectivity which might mean that management does not trust the given information (Landoll 2011, 31). NIST (2012, 14) adds that due to the range of smaller values, it might make the relative prioritisation or comparison of the risks difficult.

The semi-quantitative assessment, described by (NIST 2012, 14) brings the benefits of both quantitative and qualitative methods. This happens by using scales whose values and meanings are not maintained in other contexts. The results are separated into bins or scales which can be translated to qualitative terms but also allow for the relative comparisons of the risks themselves. An example is giving 35 points to one risk whilst issuing 70 to the other. The 70-

point risk is seen to be a lot more significant than the lower scoring risks. For example, 90 points refers to a very high risk assuming there is a methodology to give risks points this way. However, the combined method requires expert judgment in assigning the values. (NIST 2012, 14.) These risk assessment approaches are summarised in table 7.

Table 7. Risk assessment approach summary.

Approach	Advantage	Disadvantage
Quantitative	• Objectivity • Can be expressed in money	• Complexity • Reliability based on determination of values • Difficult to get accurate values
Qualitative	• Easy to understand and communicate • Adequate enough in most cases	• Subjectivity • Might lack management trust • Relative prioritisation and comparison can be difficult due to small value scale
Semi-quantitative	• Benefits of both methods • Translates well to both quantitative and qualitative scales	• Requires expert judgment in assigning the values

The fifth step in risk assessment process is risk mitigation. In this step a team develops recommendations for safeguards so that the identified risks can be reduced to an acceptable level. A safeguard, also called a countermeasure is used to reduce the risk to an organisation’s assets. They are categorised as preventive, defective or corrective. (Landoll 2011, 31 – 33.) These categorisations are described in table 8.

Table 8. Safeguard summary (Landoll 2011, 33).

Safeguard type	Description
Preventive	Deter undesirable events
Detective	Indicate occurrence of undesirable events through identifying conditions
Corrective	Correct the damage caused by undesirable events

The process involves a mapping of safeguards to threat/vulnerability pairs, determining the reduction of risk, determining the cost of the safeguards and grouping these safeguards as solution sets. An important step is to also consider the residual risk since this indicates if the risk falls below the tolerance level. This way, it tells if the safeguard or control was effective enough. (Landoll 2011, 31 – 33.) The concept of residual risk is summarised in table 9.

Table 9. Residual risk summary (Landoll 2011, 34).

Type	Description
Static	Always exists
Dynamic	May be reduced by implementing safeguards

It is important to realise that despite implementing all the possible security controls, there is always a residual risk. In other words there is never 100% security. (Landoll 2011, 33.)

The final and sixth step is risk resolution and reporting. During this step, a report is developed for the project sponsor. The report should provide clear information to all parties involved such as the executives and management. Senior management determines the resolution of the identified risks. (Landoll 2011, 23 – 35.) Landoll (2011, 34) also states that risk resolution is a key concept in security risk assessment. The possible risk resolutions are summarised in table 10.

Table 10. Risk resolution summary (Landoll 2011, 35).

Concept	Definition
Risk resolution	A decision by senior management on how to resolve the presented risk
Risk reduction	Reducing the risk to the organisation to an acceptable level through implementing additional security controls or improving existing controls
Risk acceptance	A decision by senior management to accept the risk based on business reasons
Risk transference	Transferring the risk to another organisation by outsourcing or getting an insurance

Organisations typically wish to manage their risks. There are five options to achieve it. An organisation can ignore the risk which means nothing is performed for the risk. An organisation can avoid the risk which means avoiding the actions that might realise the risk. An organisation can mitigate the risk when controls are implemented to reduce the risk to an acceptable level. An organisation can accept the residual risk and the business continues. This usually happens when the cost of implementing controls outweighs the potential impact of the risk itself. (Paul 2011, 24.) Landoll (2011, 5) describes this as the security risk mitigation step in the risk management process. The key is to inform the senior management so that they can make security-risk based decisions (Landoll 2011, 5). A security risk can be accepted if senior manager believes it is in the best interest of the organisation (Landoll 2011, 34). An organisation can also address the risk by transferring it to a third party. This can be the case when the cost of implementing security controls exceeds the cost of the potential impact of the risk itself. (Paul 2011, 24.)

In summary, one of the most important things of a risk assessment is the communication and information sharing. Information produced from a risk assessment should be effectively communicated and shared at all risk management levels. (NIST 2012, 22.) Landoll (2011, 395) also states that a risk assessment project is not complete without documenting and reporting the results. The risk assessment process should create an ongoing communication and information sharing process amongst stakeholders in the organisation (NIST 2012, 22). Although the risk assessment team may have a good view of the risks effecting the organisation, these must be conveyed to the whole organisation (Landoll 2011, 395).

3 INFORMATION SECURITY CHALLENGES IN A SOFTWARE COMPANY

Software security is more than just writing code (Paul 2011, 22). This comes from the fact that software development itself is a lot more than writing code. As McConnell (2004, 3 – 4) lists, there are many activities that belong to the context of software development which are not just about writing code. Good examples are software architectures, system testing or maintenance. Mentally, these are easily grouped as programming (McConnell 2004, 4). One of the reasons is that programming is the only activity that is guaranteed to be completed within the software development process since some projects may lack the requirements, design and testing phases due to a lack of time (McConnell 2004, 7). From a security perspective, some of the vulnerabilities are found in source code, but that is only a small portion of the overall risk since process and people related risks must also be considered (Paul 2011, 22). A process is where people do activities and a disciplined process is imperative in adding security to software (Howard and LeBlanc 2003, 23).

Secure software development consists of three elements: best practises, process improvements, and metrics which have a goal to minimise security-related vulnerabilities and to also detect and eliminate them as early as possible in the SDLC (Microsoft Corporation 2012, 7). However, risk management integration in the SDLC is key to having a secure software development process. The risk management in software development is challenging, because it is not an exact science and it is still a maturing area. The asset value or data value determination can be very subjective. The trouble is that determining the chance of similar security breaches within an organisation in comparison to those few which are published is almost impossible. Customers often look for guilty personnel if a breach occurs and despite what a contract indicates, they consider the real risk belonging to the software provider. (Paul 2011, 22.) VAHTI 01/2013 guidance on information security in software development states that the requirements for software development in an organisation consist of six things which are listed in table 11 (translated).

Table 11. Requirements for a software development organisation (Valtiovarainministeriö 2013, 32 - 41).

Requirement	Definition
Strategy and resourcing	• An organisation supports information security work by having an information security strategy • An organisation must recognise the key roles in information security and reserve enough resources for security implementation
Policies	Policies are guidelines for the entire organisation. • An organisation needs at least an information security policy but other policies might be required as well
Risk management	In the software development lifecycle steps it is good to examine the threats to the software being developed and the controls/safeguards to mitigate these risks. • Risk management and project know-how has a central role in software development, despite the development model being used
Know-how and education	The know-how of the software developers is crucial for secure software development. • Every employee must have education and awareness training in software security to have competence for their work • An organisation needs to have people specialised in security and to be able to advice the other employees
Technical software development environment	The software development environment must also be protected. It must: • Comply with security principles and best practises • Include access management • Include patch management
Business Continuity Management	Depending on the criticality of the software, there might be various requirements for the confidentiality, integrity and availability of the system. These should be incorporated already in the software design phase and be noted in the risk management and continuity planning phases.

Security awareness is raised in the VAHTI 01/2013 guidance on top of these requirements. It has been researched that user compliance with IS policies and instructions is a multifaceted construct. In addition to knowledge and skills, it relates to motivation and to organisational issues such as management, power and politics. (Puhakainen 2006, 139.) On the other hand, to change a person's security behavior, the person should be guided towards self-management and responsibility of one's own actions (Nykänen 2011, 275). Nykänen (2011, 275) continues that in the security training, the context of new knowledge and skills should be bound to a larger whole to improve the adaptability and utilisability in other environments. With this, the trained skills will cause a deeper and more effective learning experience whilst creating significance. A human often only needs a simple concrete explanation how and why one must operate in a secure manner. (Nykänen 2011, 275.) This is in line with Karjalainen (2011, 157) who states that security training sessions need to use a different argumentation or persuasive messages, according to the different types of violations. All in all, it can be concluded that security awareness and compliance have a lot to do with how an employee is positioned in the organisation and how he or she feels about working there. Management needs to be an active participant in security development and any deviations need to be raised in a practical manner. The root causes of the problems must be found and the employee's own responsibility in the course of action should be emphasised. These practical findings should be used as a source for internal education and awareness training. Self-management can be achieved by encouraging people to make independent decisions in work. This is generally acceptable knowledge, but none the less good to internalise in a software development organisation as well.

Another aspect is the organisational culture. Kivelä (2011, 208) has found that in a growing company special attention should be given to the openness of the feedback between supervisors and employees, since the greatest development potential comes from reflection and feedback. He also found that personnel should more openly examine what they do, including the results, and failures, in order to inspect the flaws in their own actions (Kivelä 2011, 208). Although the study was limited to the companies being studied, the results were trendsetting, and in this context are very interesting. Referring back to Nykänen's (2011, 275) findings, self-responsibility is key to changing security behavior. It can also be said based on Kivelä's findings, that this is most likely to be true in growing companies such as Agenteq Oy. Adding these factors into the company including the quality of the feedback and the potential for truthful feedback is a key factor here.

Organisational learning is also an interesting factor in the context of this development work, since action research is about learning in action (Coghlan and Brannick 2010, 5). With information security it is also about learning as an organisation in this case. Suominen (2011, 136 - 137) found that a company operating heavily within a customer interface is expected to immediately understand its customers and their needs. Such a company is on the initial steps to have a certain intensity of learning (Suominen 2011, 136 – 137). The description of this type of company is very similar to Agenteq Oy. An additional finding was that the principles adopted in such a company were not because of pedagogical education but because of a leadership type of management (Suominen 2011, 137). This also supports the view that management is at the heart of organisational learning regarding information security as well.

Theory summary

The key composite idea from the previous theories is to align Agenteq Oy's information security activities to the company processes in order to make it integrated into the SDLC. The internal information security development project started with this development work and has a lot to do with risk management activities in general, and creates a basis for the initial information security management system. However, the major practical role for this work is focused on the risk assessment side and to obtain the required information for the initial risk management. The company's steps to the managed future from information security perspective are developed based on this work. The challenges regarding information security awareness, information security policy compliance, information security culture and general organisational culture and learning is something that needs to be acknowledged to make the project successful.

4 DEVELOPMENT PROCESS OVERVIEW

4.1 Process overview

The research setup is described in figure 7. The core groups in the research process were the customer support and operator, Tampuuri development, product management and implementation project groups. They formed the research group. The steering group was a management group. These are clarified in chapter 5.

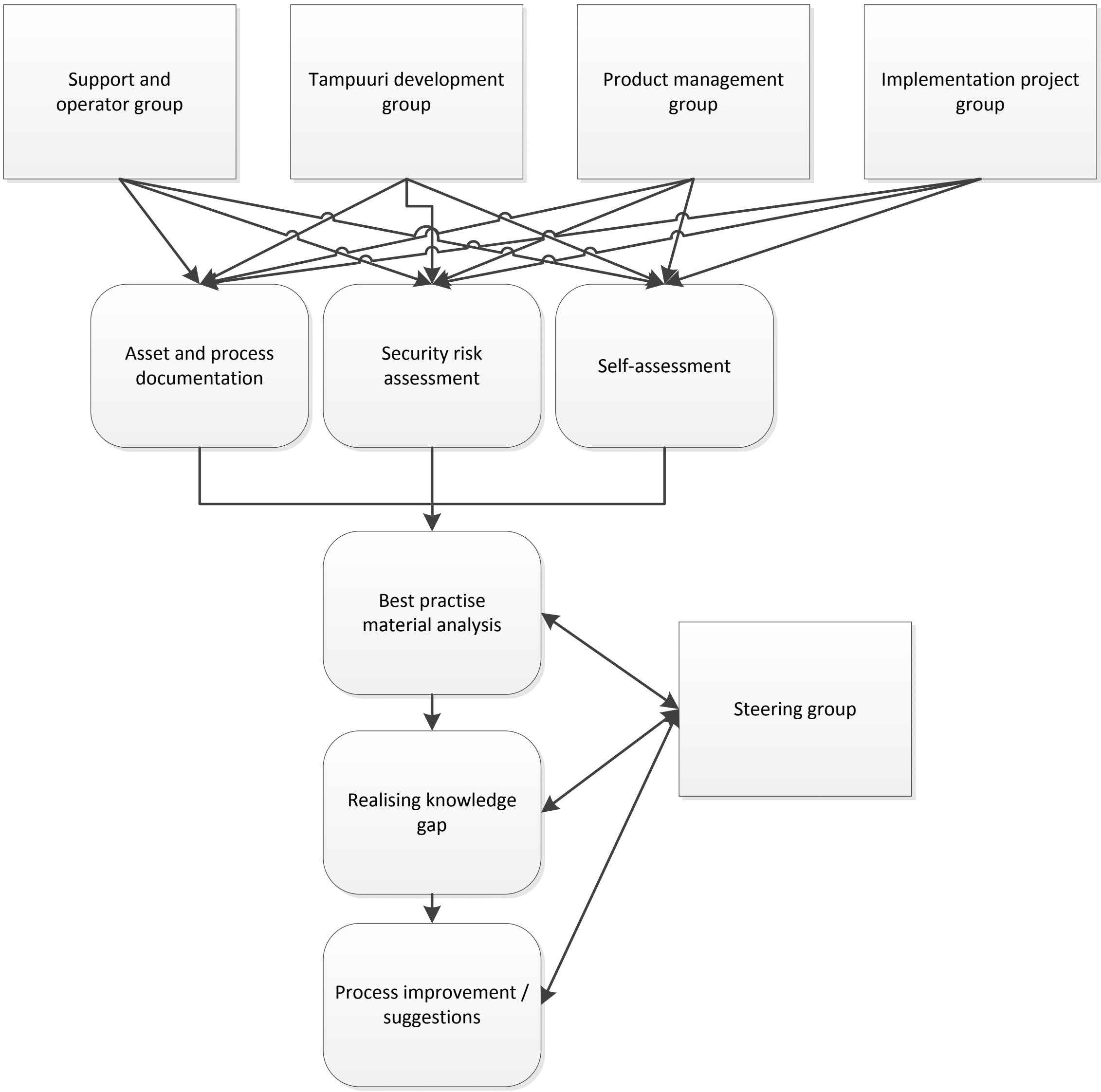

Support and operator group
Tampuuri development group
Product management group
Implementation project group
Asset and process documentation
Security risk assessment
Self-assessment
Best practise material analysis
Steering group
Realising knowledge gap
Process improvement / suggestions

Figure 10. Research setup.

The research group did the first brainstorming of the assets. The group also checked that the process flowcharts were up to date and represented the real environment the people work in. Next the group performed the actual security risk assessment and these sessions ended with a group's self-assessment of the current information security practices in Agenteq Oy. The results gathered through these steps were documented and structured into the working area of the steering group for further processing. Risks were documented so that that they could be easily understood and communicated. The results were then discussed with the research group with the best practice security knowledge as a reference to find the potential solutions and make suggestions to the group itself. This was used as a basis to understand the knowledge gap and form the understanding of needed development steps. This process is expanded upon in chapter 5.

4.2 General timeframe of the process and iterations

The overall process started in February 2012 with the project launch executed by Agenteq Oy's CEO during the first steering group meeting. The process occurred in the three main iterations which were preceded by initiation iteration and followed by the closing iteration. These are summarised in table 12.

Table 12. Main iterations of the development work.
(S= steering group, R = research group, MR = main researcher).

	Initiating 02/12 – 03/12	First iteration 04/12 – 07/12	Second iteration 08/12 – 12/12	Third iteration 1/13 – 05/13	Closing 05/13
1. Initialisation	Project launch, InfoSec policy initiation (S)				
2. Literature	Gathering information (MR)	Gathering information (MR)	Gathering information (MR)	Gathering information (MR)	
3. Information security policy	Planning (S)	Development (S)	Launch (S)	Security guidance development (S)	
4. Security reference material		Developing (MR)	Developing (MR) Presentations (MR)	Best practise material analysis (R)	

(to be continued)

Table 12 (continues).

	Initiating 02/12 – 03/12	First iteration 04/12 – 07/12	Second iteration 08/12 – 12/12	Third iteration 1/13 – 05/13	Closing 05/13
5. Assets and process documentation		Brainstorming and checking (R)	Risk assessment	Risk assessment result analysis	
6. Management interview			CEO Interview (MR)	Used in determining the level of risk list	
7. Risk assessment and self-assessment	Determining the suitable assessment method (MR)		Meetings with the research group (R)	Internal site for the risk list (MR), result analysis (S)	
8. Best practise material analysis				Analysis meetings (R)	

(to be continued)

Table 12 (continues).

	Initiating 02/12 – 03/12	First iteration 04/12 – 07/12	Second iteration 08/12 – 12/12	Third iteration 1/13 – 05/13	Closing 05/13
9. Realising knowledge gap				Analysis meeting result discussion (S)	
10. Exit					Action part closed
11. Elicit results					Elicit results and writing the report

The model for this type of an action research iteration reporting was taken from a publication by Iversen et al. (2004, 411). During the spring of 2012 the development process was being prepared. This occurred simultaneously with the management finalising the new information security policy. The main initial literature and pre-understanding for this development work was gathered in spring 2012. New information was being generated and found all the time due to the action research methodology. The new information security policy was launched in August 2012 which also started the action phase of this development process. The action phase lasted until May 2013 when the development work was finalised.

5 DEVELOPMENT PROCESS DETAILS

5.1 Initiating iteration

The project started in February 2012. Agenteq Oy's CEO approved the project plan and it was decided that the steering group for the project consisted of the CEO, the IT Service Manager, and the main researcher. The steering group and the responsibilities are stated in table 13.

Table 13. Steering group.

Member	Responsibility
CEO	Administrative security
IT Service Manager	IT Security
Main researcher	Software security

It was understood in the early stages based on description by Hakala et al. (2006, 7) that the first item needed was the information security policy for the company. From the development work's perspective it was a context-creating factor but also a prerequisite for the action steps to be implemented. Hakala et al. (2006, 7) state that developing an information security policy is the responsibility of the organisation's top management.

The information security policy was required to be publicly under development before the actual security development work could start in the company. It was acknowledged in the steering group that in order to argument for the change and further security development actions and to get personnel involved, the information security policy document must be developed to support that. Paul (2011, 27) states that a security policy is an instrument which can provide the needed enforceability.

At that time the information by Hakala et al. (2006, 8-9) about the information security policy was available. However, there was difficulty in understanding what do areas of information security policy mean in practise. How should they be expressed in order for it to work in the best way from an organisation's perspective? How can the message be translated into action and not to contain just phrases? It was the same worry as stated by Hakala et al. (2006, 8). A practical model was needed and the development work started by looking for what kind of implementations had already been conducted by other organisations. The best model was found in the VAHTI 2/2011 guidance by Valtiovarainministeriö (2011, 29 - 30). The development work continued based on it.

Although chapter 2 of this development work discusses what risk management is, there is not much information from this perspective since formal risk management activities do not yet exist. Neither does it cover the situation where a software provider wants to consider the risk from a service perspective. How to manage the risk that a software provider may impose on its clients? Therefore, some initial difficulty was to understand how to get there from the basis of having informal risk management activities. As was discussed in chapter 2, information security risk is a component of organisational risk. This was a confusing factor, since Agenteq Oy's management certainly understood what risk management is from a business perspective. However, the practical components to manage information security risks were missing. Based on NIST (2008) it was understood that a consideration of the system development lifecycle was needed to try to find the elements in the company's software development processes which match the elements in the NIST (2008) definition of SDLC. This argumentation and the process mappings were discussed in chapter 2.

The need for the company to perform a risk assessment was raised during this time. It was realised that security risk management is key to solve these issues. Through implementing the information security policy and risk assessment for the SDLC, an initial understanding of the risk level is obtained. NIST (2002, 1) states that the risk management process is the process of identifying, assessing and managing risk, and therefore implementing these steps through risk assessment creates the initial understanding what the current risk landscape consists of. In Agenteq Oy’s context this can also be categorised as an experiment to understand information security.

Although the initial focus was just to do the risk assessment once, it was acknowledged that working through it, a continual process and better understanding could be achieved. The CEO demanded that information security would be an integrated process. Considering based on chapter 2 that the risk management process consists of framing risk, assessing risk, responding to risk and monitoring risk, the assessment and response were in focus here and the idea was to see how they impact on understanding the framing of risk. The decision was to perform the first risk assessment focused on the Tampuuri product because it is the company’s flagship product having an entire SDLC which can be mapped to the NIST (2008) definition of SDLC.

Considering NIST (2011,1) stated that information security risk is commonly linked to the operation and usage of information systems, with Agenteq Oy it is linked to the operation and development of the Tampuuri product in the context of this development work. NIST (2012, 1) states that risk assessments can be performed on three levels (organisation, business process, information system). These levels were reflected because an initial understanding of Agenteq Oy’s organisation-wide security risk assessment was being initiated through implementing a risk assessment on a business process-level related to the Tampuuri product. That itself represents the information system level. As discussed in chapters 1.2 and 1.3, this setting is also likely to be true to Agenteq Oy’s customers due to Tampuuri being such a relevant product in their business. The technical IT side managed by the IT Service Manager was decided to be beyond the scope of this development work.

The next thing to look for was the suitable method for the risk assessment. After inspecting a few options it was determined to be the Octave Allegro (later Allegro) method. This was accepted by the CEO. This was important just as Caralli et al. (2007, 23) state since gaining senior management sponsorship is a critical factor to the success of an Allegro risk assessment.

Allegro was selected since it is tailored for organisations which do not have the time or resources to do a full-scale risk assessment. Allegro does not require extensive risk assessment knowledge and it focuses on information assets from usage, storage, transportation, processing and an exposing perspective. Allegro is supplemented with free material such as guidance, worksheets, and questionnaires and it can be performed in a workshop-style. (Caralli et al. 2007, 4 - 5.) In Agenteq Oy's case, the risk is all about the customer's information in the Tampuuri product and the fact that the company does not have deep knowledge of risk assessments. Caralli et al. (2007, 28) also claim that Octave Allegro can be used in the SDLC for the information assets that support a process that an organisation wants to automate. The solution is to capture the security requirements of the assets that support business requirements. Gaps in the current control structure can be identified and this information can be used to incorporate the missing controls to the set of requirements. (Caralli et al. 2007, 28.)

Agenteq Oy acknowledged that it needs a risk assessment method that is easy to understand, is well-structured, and still produces meaningful results. Allegro seemed to fulfill this criteria. The first step in Allegro is to establish the risk measurement criteria (Caralli et al. 2007, 17 - 18). The CEO of Agenteq Oy did this task. This is precisely in line with what Hakala et al. (2006, 90) mention, where setting the criteria for risk is the responsibility of the organisation's management. The distinction to the definition by Hakala et al. (2006. 90) was that these were discussed with the information management unit, represented by the IT Service Manager, but the CEO did the required decisions by himself. It is an important factor here that Allegro is a semi-quantitative method. The semi-quantitative assessment and calculation method was discussed in chapter 2. When the CEO sets the risk criteria, the management trust, and an expert judgment issues can be mitigated. This is a clear benefit in Allegro because it stimulates and involves the management too.

Although the information security policy work recently started, the CEO was able to define the information lines most important for the company so that these can be worked on and be used in the initial risk assessment preparation steps. The definition of the information lines include, as Paul (2011, 26) and Hakala et al. (2006, 8) state, the assets Agenteq Oy sees as being valuable and must be protected. These information lines were discussed in chapter 1.1 and they represent the central targets in Agenteq Oy’s information security just as Hakala et al. (2006, 8) describe.

It was decided that the development project should be announced internally in the company and it was essential that the personnel participate actively. A major announcement campaign by all the members of the steering group was performed in the company events and announcements. Paul (2011, 27) states that successful implementation of a security policy requires marketing efforts. The goals of the management need to be communicated through the policy to the end users (Paul 2011, 27). It was acknowledged that personnel must want to want to work towards better the information security, so that they can be self-responsible. This was in line with what Nykänen (2011, 275) states that self-responsibility is key to changing security behavior. The decision was to include people from all the relevant operative groups. This is in line what Hakala et al. (2006, 81) state by selecting the personnel participating in the risk assessment, the goal should be to strive for a representative cross-section of the organisation's staff. This was shortly described in chapter 4.1. The structure of the research group was decided by the CEO. This structure is outlined in table 14.

Table 14. Research Group

Operative Unit	Personnel
Customer support and operator	Customer support team leader, two system specialists
Tampuuri development	Development team leaders (technical modules, financial modules)
Product Management	Product Managers (technical, financial, e-services)
Implementation	Project Manager

From the Tampuuri perspective this is the most representative set of personnel there can be. These people are the ones working in Agenteq Oy’s SDLC. The initiating iteration ended in continuing the work with the information security policy.

The activities in the initiating iteration were related to the first two steps of the risk assessment process described in chapter 2. The initial steering group work matched what is described in the project definition step. The scope, boundaries, and initial understanding of the assets were materialised. This meant that the risk assessment would focus on the assets based on the information security policy. The project preparation step consisting of the risk assessment team selection and its introduction was also implemented.

5.2 First iteration

The first iteration continued with the development of the information security policy. The key elements of the first draft of the information security document were perceived. These elements were related to the information security management system, information security education and instructions, informing, monitoring, and working in emergency conditions.

Managing and supervising of the information security is a process in which a management system is established to respond to the security needs created by the operations of the organisation and changes in its operational environment. The information security management system (later referred to as ISMS) is a documented entity based on the operations and business risks of the organisation formed by the practices. An ISMS is authorised by the top management. An important element in implementing an ISMS is to define its rights and responsibilities. The personnel responsible for the information security should be named and their authority should be defined clearly and explicitly. (Hakala et al. 2006, 106 – 109.)

In order for the information security to be integrated as discussed in chapter 2, it was decided that information security must be included in all the work instructions and reporting. In practice this means that every instruction and assignment template has a position for information security argumentation and it has to become clear that information security was considered before the task, during the task and after the task. The elements related to the information security management system and operations for emergency conditions were left out at this point. This was not in line with what Hakala et al. (2006, 8 - 9) stated but it was left to be determined based on the further steps of this development work.

The actual work related to preparing for the risk assessment started at this iteration. This work consisted of brainstorming the assets of Agenteq Oy in the research group which mapped to the information lines stated by the information security policy. It was stated in chapter 2 that the second step of the risk assessment, - project preparation -, includes the mapping of the assets. Landoll (2011, 85) states that identifying the assets to be protected is a key step in preparing for a risk assessment. This is a necessary precursor to understanding the overall risk (Landoll 2011, 85). The research group also reviewed the process flowcharts which represent the processes they work in since the assets naturally have connections to these processes. These flowcharts were discussed in chapters 1.3.3 to 1.3.5. It is important to note that the flowcharts also contain information about the relevant information system or the information source.

The third important activity stated in this iteration was the development of the security reference material for the company. The key idea was that the material would serve later during the development work but also leave concrete results to the company in a way that can be utilised by the personnel in their work. The material was mostly based on Paul (2011) and OWASP (2012) guidance. The material was written to cover the security elements of the entire software development lifecycle. The elements related to real-world challenges of personnel in Agenteq Oy were included as much as possible. It was stated in chapter 3 about that the new knowledge found in security training should be bound to a larger entity. Key in the developed material was to have relevance in the context where the personnel work in Agenteq Oy. The material was developed to be simple and concrete (although there were lots of it). In chapter 3 it was also discussed that a human often only needs a simple concrete explanation as to why and how one must operate in secure manner. The material was developed with this in mind. Material development continued in the third iteration.

5.3 Second Iteration

The second iteration started with the launch and implementation of the new information security policy which consisted of a major marketing campaign for the cause. It was first accepted in the management group and then announced by the CEO as was stated in chapter 1. Simultaneously, the steering group was nominated to be the information security authority in Agenteq Oy. One tool was to establish a mechanism for personnel to inform the steering group about the security deviations. Personnel were encouraged to report even the smallest cases and considerations. Management played an active role in security development as was suggested in chapter 3. Management also actively marketed the new policy which is required for it to be successful (Paul 2011, 27). By establishing a mechanism to report security deviations, the personnel were encouraged to be self-responsible and this was the right thing to do here based on Nykänen (2011, 275). An important fact is that by implementing a reporting channel the aim was to create the tooling for risk monitoring and responding. These are elements of the risk management process which were discussed in chapter 2. The strong idea was that the risk landscape must be researched first, before any concrete action can be implemented. This brings new knowledge which can be used to frame the risk in the management process.

The iteration continued with an interview with the CEO. The initial questions presented are outlined in table 15.

Table 15. CEO Interview questions

Question
1. What is the goal for Agenteq Oy in 3 - 5 year timeframe?
2. How does the predicted future line with the new information security policy, and with the goals for the information security?
3. What expectations does the management have for the SDLC?

The reasoning behind these questions was to obtain background information for communicating the goals of management which, as stated by Paul 2011, 27), is an important factor. It was also performed to guide the further steps of this development work, especially the risk assessment and its result processing. As discussed in chapter 3, the management is at the heart of the organisational learning. This meant trying to find the elements which are in management interests. That was a mechanism to gain support for activities but to also create a basis for the potential suggestions to be made. An important finding from the CEO interview was that a process-based approach is appreciated in the management since Agenteq Oy does not have a strong strategy-based approach. Another consideration was that management acknowledged that the new EU data protection regulation proposal might cause pressures for Agenteq Oy. The third important finding was that embracing information security culture is the greatest expectation for the SDLC by the management. (Borenius 2012.)

The iteration then continued with the actual risk assessment. The initial work involved setting the risk criteria. This was already performed by the CEO as was discussed in previous chapter about the initiating iteration. Assets and processes were documented as a preparation for this process in the first iteration. The risk assessment was performed with the research based on the Octave Allegro process. The Octave Allegro process is described in figure 11.

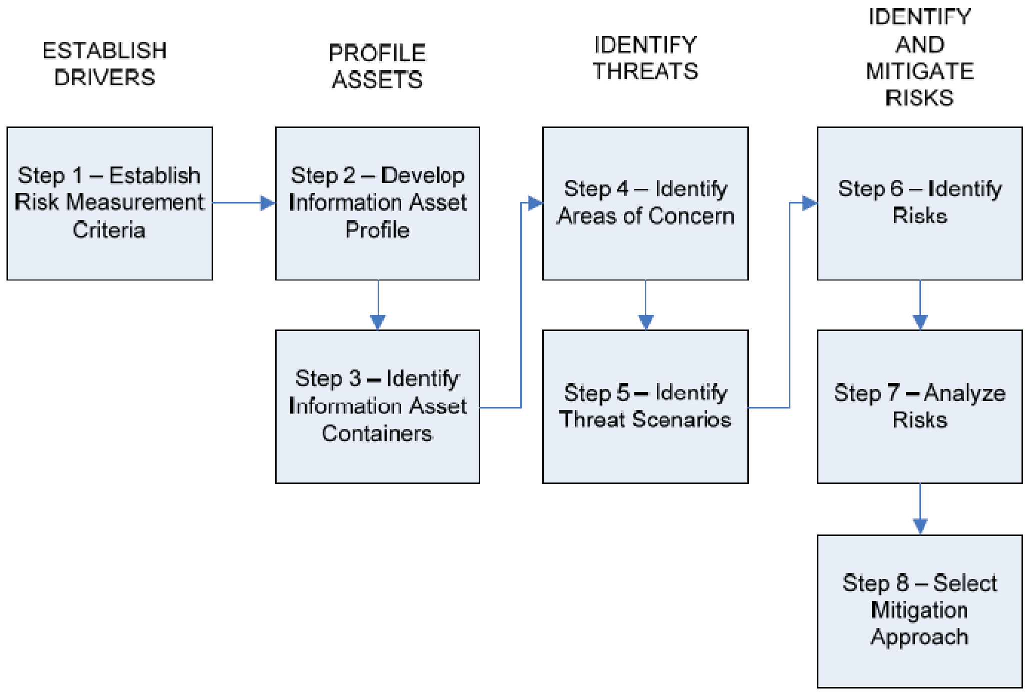

ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Figure 11. Octave Allegro process (Caralli et al. 2007, 4).

This was already initially opened up from a research perspective in figure 10, and the participating research group was described in table 14. The risk assessment was implemented through meetings with the research group. Every target group had its own dedicated meetings. This was supported by the fact that Allegro is designed for this type of use (Caralli et al. 2007, 4). The activity implemented in Agenteq Oy is outlined in table 16.

Table 16. Octave Allegro risk assessment process application in Agenteq Oy (Caralli et al. 2007, 32 - 64).

Octave Allegro step	Implementation in Agenteq Oy
1. Establish risk measurement criteria	Established by the CEO.
2. Develop information Asset profile	Chosen from the most critical assets brainstormed in the first iteration. The selection was based on the information security policy categorisation which was meant to keep it consistent to overcome the selection and valuation issues stated by Caralli et al. (2007, 24).

(to be continued)

Table 16 (continues).

Octave Allegro step	Implementation in Agenteq Oy
3. Identify information Asset containers	The containers were brainstormed in the risk assessment meetings. The developed process documentation was used in determining these so that the focus was on organisational processes.
4. Identify areas of concern	Overall broad concerns on the conditions that could affect assets were recorded. The scenarios occurred previously in real-world situations were preferred.
5. Identify threat scenarios	Threat scenarios were considered based on the previous knowledge on occurrences in real-world situations.
6. Identify risks	Risk identification was performed as suggested by the method.
7. Analyse risks	This was completed in the risk assessment meetings, but also later in the steering group result processing meetings. Value was assigned to describe the extent of impact to an organisation based on the risk measurement criteria.
8. Select mitigation approach	This was completed later in the result analysis meetings of the research group result discussion but decided by the steering group, especially for the most critical risks.

An exception to the Octave Allegro process was that the last step, the mitigation approach selection, was left to later meetings in next iterations where the results of the risk assessment in general were opened up. The highest risks were promptly reacted to by the steering group with an action plan. This Allegro process matches the elements of Landoll's definition of the last steps risk assessment process discussed in chapter 2. These mapped steps were data gathering, risk analysis, risk mitigation and recommendations.

This iteration also contained a surprise factor. One of the Agenteq Oy's major customers had performed a security audit for the Tampuuri product. This revealed threats and risks which were taken into serious consideration in the context of this development work. Timing for this was actually excellent because it complemented the knowledge about the risks in the Tampuuri product.

After the risk assessment meetings a TUTTI self-assessment tool by Rousku (2012) was used by the research group. A self-assessment was conducted to gather information on how the current information security level is understood by the personnel in Agenteq Oy. These were the questions from the TUTTI tool. The presented questions are listed in table 17 (translated).

Table 17. Self-assessment questions (Rousku 2012).

Question
1. Has the right kind of information security attitude and culture been formed into your organisation?
2. Is a regular information security education arranged used to inform for the personnel?
3. Does the management and supervisors demonstrate a good example of commitment to the information security, support the information security work and have understood its significance and are interested in it?
4. Are the assets to be protected, relevant processes and related information systems of significance to the organisation's activity been described?
5. Is the personnel instructed and educated to use the agreed procedures and to recognise the information material to be protected, classified and processed based on the confidentiality, integrity and availability requirements of the material?
6. Does an operations model exist for potential occurrence of security deviations and abuse as well as does a plan exist for other kind of error conditions in your organisation?

The assessment is to be repeated later to measure the success of security development activities in the future. The self-assessment is important in measuring the information security management performance from a personnel's perspective.

5.4 Third iteration

The third iteration started with an organisation change in Agenteq Oy. Figure 12 outlines the new organisation.

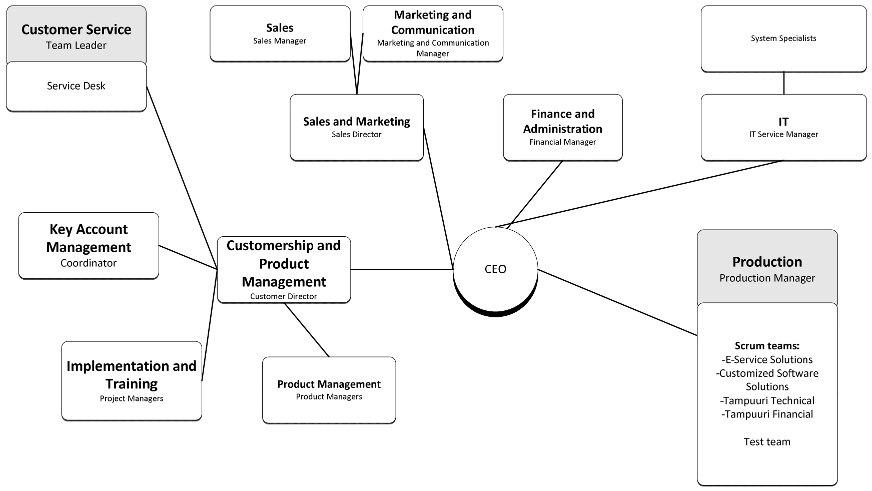


Figure 12. Organisational structure of Agenteq Oy in 2013 (Agenteq Solutions Oy 2013).

The major change was moving production so that it was performed in a single unit. From a security development perspective this is a good thing since implementing development actions can now be performed consistently to all product development processes. These were separate before the change which was one reason to focus this development process to the Tampuuri development at first. Now the lessons learned with Tampuuri can be applied to other products through the same management. The organisation change had no impact on the research group's or steering group's role.

The third iteration consisted mostly of analysing the results of the risk assessment, and the steering group doing the overall security development and response actions based on the results so far. The steering group established a centralised intranet site for managing the gathered risk list and for guiding the risk response activity. The model for the risk list was chosen to be a risk-action list described by Iversen et al. (2004, 402). It is a prioritised list of risk items with related resolution actions. Argumentation was mostly the fact stated by Agenteq's CEO in the interview that a process is preferred over a strategy. The only downside was the lack of strategic oversight explained by Iversen et al. (2004, 402) but the decision was conscious based on the management's statement.

During the iteration a VAHTI 1/2013 guide related to software development was published (Valtiovarainministeriö 2013). It turned out to be very solid basis for Agenteq Oy to develop its own security guidances. The Sales Director of Agenteq Oy mentioned in a discussion that over 30% of the offer base (calculated monetarily) would benefit from Agenteq Oy being VAHTI-compliant (A Alkila 2013, pers. comm. 23 April). This greatly gave business value for security development in Agenteq Oy.

Over the iteration the steering group conducted meetings to find out solutions to the most critical risks. The approach has been to solve the risks in a prioritised manner. This is in line in high-level with what Iversen et al. (2004, 415) explain about the four-step process. However, using the word ‘strategy’ may not probably the right one in this context. The situation regarding a risk is characterized. The risk is reanalysed to assess where the most serious (real) risk is when the potential misjudgments by the research group are also found. The actions are prioritised and then taken. (Iversen et al. 2004, 415.)

The research group conducted a new set of meetings to find out potential risk mitigation actions from the best practice materials to the risks found out in the risk assessment. The materials used were based on VAHTI 1/2013 (Valtiovarainministeriö 2013) and SAMM 1.0 (OWASP 2009). These results were documented on the risk-action list for the consideration and analysis of the steering group. This matched with what Landoll described as developing recommendations discussed in chapter 2 and also Octave Allegro’s select mitigation approach step (Caralli et al. 2007, 58 – 64). The residual risk which was discussed in chapter 2 was also evaluated to gain an understanding of the effectiveness.

5.5 Closing

The closing iteration consisted of eliciting results, making development suggestions and writing the thesis report. Results were collected from the steps of the development process. Development suggestions were made for the information security management model and for integrating security activities in the Agenteq Oy’s processes. These were presented at the management for actions.

6 RESULTS

6.1 Research problem perspective

The first research question was how to find, understand and document the security development needs in the SDLC. Based on the results it can be stated that in an execution of a risk based-approach in an organisation, a risk assessment as a component of the risk-management process is a key. A well-structured and supported risk assessment method using business criteria can cover this need entirely. When this is performed systematically in a process, it serves the management of the company. Adding the continual know-how development together with the monitoring the operational environment this helps to achieve this purpose. The know-how development should be measurable to ensure it serves the objectives of the organisation.

The second research question was how to manage risks in the SDLC. This can be performed through establishment of the tasks and responsibilities so that information security is managed in an integrated manner supported by the best practises. The information security activities in processes must be defined, documented and measured. The observed risks should be managed with the best of the organisation in mind. A two-way discussion, reflection and open feedback between the management and personnel should be encouraged.

The final research question was how to turn risk management in the SDLC into a process. This is performed by integrating risk management into the management processes. It can be supported with the establishment of a year clock.

6.2 Data and information perspective

The results consist of data, material, and learning gathered on the steps of the development work. One of results was the asset documentation in a mind map format and the process documentation. The process documentation was already covered in chapter 1. The detailed asset documentation is beyond the scope of this report for business secrecy reasons but the number of assets per information line can be described. The assets are summarised in table 18.

Table 18. Assets based on the information security policy categorisation.

Information line	Number of assets
Information owned by customers	22 assets
Information concerning customers, in possession of Agenteq Oy’s personnel	10 assets
Information concerning Agenteq Oy’s own business	13 assets

The greatest number of assets on the first area is explained by the fact that information owned by the customers is the highest priority. Therefore the greatest effort was placed on brainstorming and evaluating those assets. The developed security reference material covered the entire software development lifecycle, but also future considerations. These materials are listed in table 19.

Table 19. Developed security reference materials.

Material	Usage
Information security integration into investments	Considerations for the software feature planning
Information security requirements	Considerations for the software feature specifications
Secure software design	Considerations for the software feature design phase
Secure software development	Considerations for the software feature development phase
Secure software testing	Considerations for the software feature testing phase

(to be continued)

Table 19 (continues).

Material	Usage
Software implementation	Considerations for the software feature implementation phase
Software distribution, maintenance, and disposal	Considerations for the software feature distribution, maintenance and disposal phase
Information security with agile methods	Guidance for integrating information security in the agile methods used in Agenteq Oy
The new EU data protection proposal	Preparation for the future changes

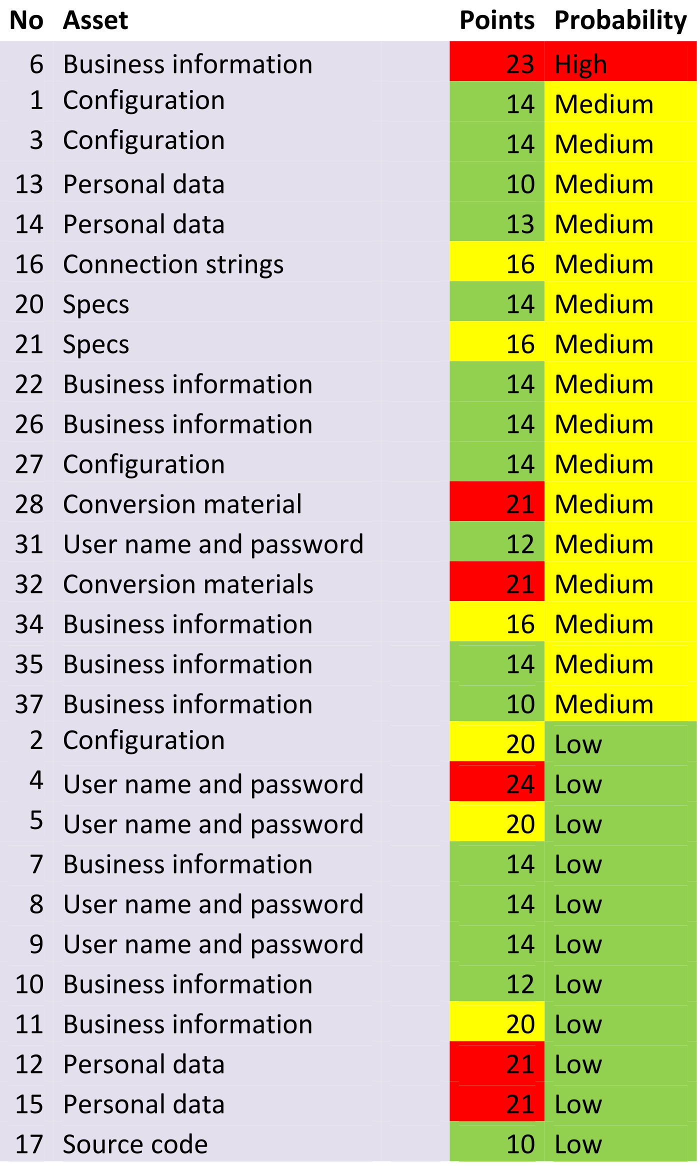
The materials cover the phases of the SDLC. Company-specific matters such as the security integration into investments, information security integration into the agile methods, and the new EU Data Protection proposal were also covered. These materials were made available to the entire personnel immediately after they were finalised, and they were used in the best-practise material analyses together with the external materials. The idea was that material could be used in the daily work. Porvari (2012, 204) suggests that it is extremely important that personnel explores the information security material and supervisors should monitor this.

The launch of the new information security policy also created change in the information security climate of Agenteq Oy. Due to the visible push from the management side the personnel also demonstrated increased activity and interest in the matter. This proved the point that management activity is key in embracing security. Sydänmaanlakka, who is an experienced professional on human resource management, has stated in an interview that applying information so that things are getting into practise is a manager's responsibility (Tyykiluoto 2013). The organisational culture, called after in the management interview, is greatly dependent on the actions of the management. Considering what was discussed in chapter 3, this calls for continuous and open discussion about the information security between the management and the employees. Embracing reflection and feedback as suggested by Kivelä (2011, 208) is important to keep an on-going discussion. The conclusion is that the implementation of the information security policy demonstrated a leadership type of management explained by Suominen (2011, 137) which is why it worked out so well. The implementation enabled and justified the personnel to be self-responsible. This actively encouraged reporting the security deviations and participating in the discussion. It was a lesson of organisational learning demonstrating the management's role. This was supported by the results of the later self-assessment which suggested that the general actions based on the implementation of the new information security policy have raised the awareness level of information security in Agenteq Oy. However, the results also demonstrated that the practical actions impacting on the daily work of the personnel are also required. The precise self-assessment results are left out for business secrecy reasons.

The results from the management interview were already discussed in chapter 4 because they had a direct impact on the research process. The emphasis on processes, embracing information security culture and acknowledgement of the new EU data protection regulation proposal were the key findings. While the lack of strategic direction was an interesting finding, Porvari (2012, 197) states that information security management is performed through process management with a connection to the business management. From this perspective security development in processes is achievable with the current management principles. However, Trott (2012, 292) states that a business strategy consists of what the company might do, what the company can do and what the company should do. From an information security perspective, a strategy is seen as a long period plan which guides the information security work in software development at all levels of the organisation and it should not be separate from the core actions (Valtiovarainministeriö 2013, 31 – 33). From this perspective it should be noted that risk management activities could help in understanding the drawbacks the company might encounter. Implementing a risk management activity could be a part of the change to have a strategic direction. A strategy is emphasised with the information security and with the risk management, which suggests that they could help in achieving a strategic approach. It was discussed in chapter 2 that the aim of a risk framing component in the risk management process is to produce a risk management strategy and to create a basis for risk-based decisions. In this context this supports the view that business decisions could be better justified if the risk is considered consciously.

The risk assessment produced a list of risks. The result summary is listed in table 20.

Table 20. Risk assessment results.



No	Asset	Points	Probability
6	Business information	23	High
1	Configuration	14	Medium
3	Configuration	14	Medium
13	Personal data	10	Medium
14	Personal data	13	Medium
16	Connection strings	16	Medium
20	Specs	14	Medium
21	Specs	16	Medium
22	Business information	14	Medium
26	Business information	14	Medium
27	Configuration	14	Medium
28	Conversion material	21	Medium
31	User name and password	12	Medium
32	Conversion materials	21	Medium
34	Business information	16	Medium
35	Business information	14	Medium
37	Business information	10	Medium
2	Configuration	20	Low
4	User name and password	24	Low
5	User name and password	20	Low
7	Business information	14	Low
8	User name and password	14	Low
9	User name and password	14	Low
10	Business information	12	Low
11	Business information	20	Low
12	Personal data	21	Low
15	Personal data	21	Low
17	Source code	10	Low

18	Source code	14	Low

(to be continued)

Table 20 (continues).

No	Asset	Points	Probability
19	Connection strings	16	Low
23	Business information	16	Low
24	Business information	16	Low
25	Business information	16	Low
29	Conversion material	21	Low
30	Bank payment material	20	Low
33	User name and password	14	Low
36	User name and password	14	Low

For this report the risks are left out for business secrecy reasons but the asset or the information area is included. The risks were valued based on criteria given by the management (discussed in chapter 5.1). Table 21 describes the risk valuation.

Table 21. Risk valuation.

Points	Probability	Interpretation
Low	Low	Low risk
Medium	Low	Notable impact, low risk
High	Low	Significant impact, notable risk
Low	Medium	Notable risk
Low	High	Notable risk
Medium	High	Significant risk
Medium	High	Significant risk
High	Medium	Significant, almost critical risk
High	High	Critical risk

The risk assessment results revealed that there exists 1 critical risk, 5 significant risks, 23 notable risks and 8 low risks. Based on the results it can be stated that risks exist quite evenly and equally in the assessed areas. Business information was a general asset category used if an asset could not be categorised more precisely or if the risk was of a general type. This contributes to the number of risks related to that asset. Based on the results analysis discussion and evaluation, almost all of the risks had countermeasures which could have been applied and which would have mitigated the risks. The countermeasures were mostly preventive and detective and apply at process level described by Landoll (2011, 382). Most of the risks would have been significantly mitigated if countermeasures would have been applied. Certainly the static residual risk discussed in the end of the chapter 2 always exists. A chance of human error is a common example of a static residual risk.

The results of the risk assessment suggested that the integration of information security activity in the company processes has not been strong in Agenteq Oy: This was especially evident from the management perspective. Porvari (2012, 212) states that information risks are business risks and they should be examined by the top management. Porvari (2012, 200) states that information security management should be integrated into the general management processes. This suggests that management processes should get data from the processes in the organisation in order to do information-based decisions which support information security.

Agenteq Oy does not have an ISMS as was stated in the discussion about the information security policy. The responsibilities related to information security are not stated practically so that it would be meaningful for the personnel. This is not in line with what was discussed in chapter 3. The VAHTI 1/2013 guidance starts from the fact that the responsibilities must be stated and the resources be allocated (Valtiovarainministeriö 2013, 32 - 33). This is supported by Hakala et al. (2006, 109) in the discussion about an ISMS.

The information security policy does state that every person working in Agenteq Oy is responsible for information security but the practical point is missing. This was evident from the results of the self-assessment. For example the job descriptions and the process tasks do not have a specification of the related and required information security activities. The view to information security has been technical when the resolutions have been left to the experts as discussed by Porvari (2012, 212). Porvari (2012, 197) also states that information security must be integrated into the daily activity. This means taking it into the activities of the business units, processes and personnel (Porvari 2012, 197). From the SDLC perspective this is supported by the NIST (2008) as was discussed in chapter 2. The integration of information security into the SDLC consists of practical activities performed by the humans in the company processes. This activity requires reflection and feedback as suggested by Kivelä (2011, 208). This is supported by Porvari (2012, 212) by stating that management should enable two-way communication. The personnel should be trained into the information security but the training should be measured (Porvari 2012, 213).

During the risk assessment process some new information was learned about the personnel. In the brainstorming session by the customer support and operator group it was realised that the members of this group have also a good basis for the risk management activities since they have completed an ITIL (Information Technology Infrastructure Library) v3 certification. Paul (2011, 47) states that the security framework guidance in ITIL is very closely aligned to the information security standards. Porvari (2012, 200) states that best practises support the information security. This suggests that a further implementation of ITIL practises might be a development option for Agenteq Oy in order to support information security activities.

The Tampuuri development team leaders and product managers represent middle-management in Agenteq Oy. Their role is significant in working between the company layers - between the management and the personnel. The role of a team leader is significant in enabling the team work. Virkki (2012, 255) claims that the middle-management can have a major impact on business transformation based on their solutions. From Agenteq Oy’s perspective the SDLC is at the heart of the business. Therefore it can be deduced that the role of middle-management in developing the SDLC is significant in Agenteq Oy. The top management should note this fact when planning the future actions.

As a summary the research process educated Agenteq Oy about what is usually performed in processes and with what information. This creates the basis for recognising and evaluating the potential risk scenarios. A lot of organisational learning has happened as was already discussed. A lot of related risks were found and also the countermeasures to them where recognised. Together with the received feedback this suggests that implementing a risk assessment was necessary. It also suggests that the risk assessment should be renewed in the near future and be integrated into the company processes. It was also acknowledged better what the personnel think about the information security. This helps guiding the management actions. The resulted change consisted of the implementation of the new information security policy and the further related action. The information security policy authorised working for the information security in the company which is a very important consideration for future development activities.

7 DISCUSSION

7.1 Summary

The objective of this development work was to find tools for developing the security in the SDLC of Agenteq Oy and to create change. This was approached with the means of the action research method. The research was performed together with the key personnel in Agenteq Oy. The theory for the development work was researched from the literature which consisted of articles, books, dissertations, legislation, guidance and best practice material. Some of the material was found by searching from the Internet but also based on the announcements of dissertations by the universities and through academic search.

The process started in February 2012 and focused initially on development of the information security policy for the company. The steering group and research (focus) group was named. The research group started to focus on the preparations for the risk assessment including asset and process documentation. Subsequently with the research process ongoing, the development of security reference material for Agenteq Oy was performed.

The new information security policy was launched in August 2012. This started the action phase in the research which consisted of implementing a risk assessment in the company, interviewing the management, and implementing a self-assessment. The results of the risk assessment were documented for the processing, and also for recognising the countermeasures which would suggest the security development needs in the company.

The spring 2013 consisted of processing the results and implementing countermeasures. The results initiated a security guidance material development in the company which is still ongoing. Based on the overall results of the research, development suggestions were made to the management of Agenteq Oy. The research process ended in May 2013. However, from company perspective this started a process which should continue as long as the company exists.

During the research process new information was found due to the action research methodology. This pointed that the results were not based only on the initial theory. The new theory found through implementing action in practise contributed also to the results. Occurrences over the course of the project had impact on the outcome. It made the comparison of the situation-specific information to the theory challenging because the business itself required prompt actions. The cumulative understanding of the original theory and learned new theory was sometimes hard to understand in practise.

7.2 Development suggestions

Simultaneously with the results, a detailed development suggestion material was handed to the management of Agenteq Oy. The first suggestion was to have a stronger integration of the risk management into the current company management processes. The management group of Agenteq Oy has regular meetings and they could have risk management activities in the agenda. The data about the risk environment could be made available for the management if tasks and responsibilities would be defined in the processes in order to produce observable data which can be measured. That would happen through implementing an ISMS system. This was the second suggestion. Implementing control activities in the processes would create data for the management decisions but also for the personnel for self-management. Implementation of these suggestions has a strong relationship to the ongoing enterprise resource planning system (ERP) renewal project in Agenteq Oy. The observability can be ensured by collecting these needs as requirements for the ERP renewal. Based on this research, the suggestion for software development companies working with agile methodologies is that the use of action research is a well-argumented and considerable option.

7.3 Limitations and validity

This development work was limited to the information side of the risk environment. It focused to the research problem from a software development life cycle perspective. The technical IT side was beyond the scope of this development work. These are sides of the same coin and related to the software development life cycle, and they need each other. Information security consists of multiple elements.

Due to the approach to research the problem from a company-specific point of view the generalisability of the results is limited. Action research does not aim to create universal knowledge (Coghlan and Brannick 2010, 149). The results can be extrapolated from a software-development oriented and growing company point of view. However, the style of management and therefore the processes vary between companies which should be noted when making comparisons. These are the significant factors which can be focused on as stated by Coghlan and Brannick (2010, 149).

This research is valid because it produced answers to the research problem which was to find solutions for developing information security in Agenteq Oy. The information is based on theory found in literature but also based on the new knowledge generated within the research process. This is in line with the action research aim to produce practical new knowledge (Coghlan and Brannick 2010, 36). The results support the information security policy of Agenteq Oy which was also an initial objective.

The results of the risk assessment and the further actions are applicable only to Agenteq Oy. The criteria for the risk assessment were company-specific when the results were as well. However, the structural elements of integrating information security based on the results are generalisable knowledge.

7.4 Further research

An interesting subject for further research would be to find how greatly information security could be developed through implementation of a new ERP system. Software development companies do develop ERP systems for their customers but an ERP system for a software development company is an interesting concept from many research perspectives, in addition to the information security.

REFERENCES

Aarnio, R. 2012. Ohjelmistoteollisuudelle mahdollisuus. Tietosuoja 3/2012, 3.

Act on the Protection of Privacy in Electronic Communications 16.6.2004/516.

Agenteq Solutions Oy 2012a. Tuotteet ja palvelut. Consulted 8.12.2012. http://www.agenteq.fi/tuotteetjapalvelut/.

Agenteq Solutions Oy 2012b. Lyhyesti – Agenteq.fi. Consulted 18.11.2012. http://www.agenteq.fi/lyhyesti.

Agenteq Solutions Oy. 2012c. Organisational structure. Salo.

Agenteq Solutions Oy. 2012d. Information security policy. Salo.

Agenteq Solutions Oy 2012e. Tampuuri | Etusivu. Consulted 8.12.2012. http://www.tampuuri.fi.

Agenteq Solutions Oy. 2012f. New feature development process. Salo.

Agenteq Solutions Oy. 2012g. Operator process. Salo.

Agenteq Solutions Oy. 2012h. Customer support process. Salo.

Agenteq Solutions Oy. 2013. Organisational structure. Salo.

Avison D.; Lau F.; Myers M.; Nielsen P. A.; 1999. Action Research. Communications of the ACM Vol. 42. No 1/1999. 94 – 97.

Bass, L.; Clements, P.;Kazman, R. 2013. Software Architecture in Practice, Third Edition, New Jersey: Pearson Education.

Borenius, J. 2012. Interview: Tietoturvan kehitysprojekti.

Caralli, R; Stevens, J.; Young, L.;Wilson, W. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Hanscom: Software Engineering Institute. Consulted 17.2.2012. http://www.sei.cmu.edu/reports/07tr012.pdf.

Coghlan D. and Brannick T. 2010 Doing Action Research in Your Own Organisation, 3rd edition, London: Sage Publications.

Collis, J. and Hussey, R. 2009 Business Research, Third Edition, Basingstoke: Palgrave Macmillan.

Hakala, M.; Vainio, M.; Vuorinen, O. 2006. Tietoturvallisuuden käsikirja, Porvoo: Docendo.

Homma toimii: Huono johtaminen on myrkynkylvöä. 2013. Puheen iltapäivä. Journ. Tyykiluoto, R. Presented 29.4.2013. YLE Puhe. Consulted 3.5.2013. http://areena.yle.fi/radio/1891958.

Howard, M. and LeBlanc, D. 2003. Writing Secure Code, 2nd Edition, Redmond: Microsoft Press.

Iversen, J.; Mathiassen, L.;Nielsen, P. 2004. Managing Risk in Software Process Improvement: An Action Research approach. MIS Quarterly. Vol. 28, No 3, 395 – 433.

Karjalainen, M. 2011. Improving employees’ information systems (IS) security behavior. Toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior. Ph.D. University of Oulu.

Kivelä, J. 2011. Kasvuyrityksen organisaatiokulttuuri. DsC. Tampere University of Technology.

Knapp, D. 2010. The ITSM Process Design Guide. Fort Lauderdale: J. Ross Publishing.

Landoll D. 2011. The Security Risk Assessment Handbook, Second Edition, Boca Raton: CRC Press.

McConnell, S. 2004. Code Complete, 2nd Edition, Redmond: Microsoft Press.

Microsoft Corporation. 2012. Microsoft Security Development Lifecycle Process 5.2. Consulted 1.10.2012. http://www.microsoft.com/en-us/download/details.aspx?id=29884.

NIST. 2002. Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30. Consulted 9.11.2012. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

NIST. 2008 Security Considerations in the Information System Development Life Cycle, Rev. 2, NIST Special Publication 800-64. Consulted 9.11.2012. http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

NIST. 2011. Managing Information Security Risk: Organisation, Mission and Information System View, NIST Special Publication 800-39 Consulted 30.3.3013. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

NIST. 2012. Guide for conducting Risk Assessments. NIST Special Publication 800-30 revision 1. Consulted 30.3.3013. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

Nykänen K. 2011. Evaluation of the effectiveness of information security training on the information security behavior of individuals and organisations. Ph.D. University of Oulu.

OWASP. 2012. OWASP Top Ten Project. Consulted 19.7.2012. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

OWASP. 2009. Software Assurance Maturity Model. Consulted 14.11.2012. http://www.opensamm.org/downloads/SAMM-1.0.pdf.

Paul, M. 2011. Official (ISC)2® Guide to the CSSLP, Boca Raton: CRC Press.

Personal Data Act 22.4.1999/523.

Porvari, P. 2012. Information security in business management, processes and personnel activity. D.Tech. Aalto University.

Puhakainen P. 2006. A design theory for information security awareness.Ph.D. University of Oulu.

Rousku, K. 2012. TUTTI – tietoturvallisuuden itsearviointiväline. Consulted 19.10.2012. http://ict-tuki.fi/tutti/.

Suomen Talokeskus Oy 2012. Suomen Talokeskus Oy | Talokeskus. Consulted 8.12.2012. http://www.talokeskus.fi > Yritys > Suomen Talokeskus Oy.

Suomen Talokeskus Oy 2012b. Kiinteistötietojärjestelmä | Talokeskus. Consulted 8.12.2012. http://www.talokeskus.fi > Tampuuri > Kiinteistötietojärjestelmä.

Suominen, J. 2011. Kohti oppivaa organisaatiota – konstruktion muodostaminen johtamisen ja oppimisen välisistä riippuvuussuhteista. D.Sc. Turku School of Economics.

Trott, P. 2012. Innovation Management and New Product Development. Harlow: Pearson Education.

Valtiovarainministeriö. 2011. Johdon tietoturvaopas, VAHTI 2/2011. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2013. Sovelluskehityksen tietoturvaohje, VAHTI 01/2013. Helsinki: Valtiovarainministeriö.

Virkki, M. 2012. Actor groups in the transformation of the dominant business unit in a corporation – The emergence of Kemira GrowHow. Ph.D. Aalto University.