HAAGA-HELIA
ammattikorkeakoulu

Information Security Plan for SAP HCM

Kirsi Anturaniemi

Thesis
Degree Programme in Information Technology
2013

HAAGA-HELIA
University of Applied Sciences

Abstract

8.11.2013

Degree Programme in Information Technology

Author Kirsi Anturaniemi	**Group or year of entry** 2012
The title of thesis Information security plan for SAP HCM	**Number of pages and appendices** 35+1
Supervisor or supervisors Niina Kinnunen	

The importance of information security increases in companies and organizations as electronic processes, service channels and tools become more common. This trend can also be seen in company support functions like human resources management. A growing part of personnel data management and employment lifecycle processes are executed and maintained in electronic systems. Therefore both employees and authorities are more and more interested in how information security is managed in organizations, especially concerning those processes where sensitive personal data is handled.

The purpose and target of this thesis work was to define based on literature review the general elements of an information security plan, find out specific requirements for Human Resources information system security, and based on the theory create information security assessment and plan for SAP HCM solution for the target company.

The theory part was collected during winter 2012-2013. The empirical part was conducted during year 2013. Data collection for the empirical part was carried out using interviews, workshops and documentation reviews as research methods. Long duration of the data collection was due to a significant structural transformation that the organization went through during summer 2013. Remarkable changes in the roles and responsibilities within the target company also affected end results.

The structure of the information security plan was formed based on the literature review, and based on the formed structure the thesis writer conducted information assessment and created the information security plan for the target company SAP HCM solution. Based on the assessment, the level of information security in the target solution is on an adequate level, and the company has sufficient control mechanisms in use. However, some development items were found and recommendations for the company made in the thesis results, for example, concerning governance model and user authorization management.

Key words
Information security, data protection, data privacy, personal data

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

8.11.2013

Tietojenkäsittelyn koulutusohjelma

Tekijä tai tekijät Kirsi Anturaniemi	**Ryhmä tai aloitusvuosi** 2012
Opinnäytetyön nimi Information security plan for SAP HCM	**Sivu- ja liitesivumäärä** 35 + 1
Ohjaaja tai ohjaajat Niina Kinnunen	

Tietoturvan tärkeys ja merkitys yrityksissä kasvaa koko ajan sähköisten prosessien, palvelukanavien ja työkalujen lisääntyessä. Tämä trendi on huomattavissa myös yritysten tukiprosesseissa, kuten henkilöstöhallinnossa. Yhä suurempi osa yrityksen henkilöstöhallintoon liittyvistä prosesseista hallitaan ja hoidetaan sähköisten prosessien avulla. Tämän seurauksena sekä käsiteltävät työntekijät että viranomaiset osoittavat kasvavaa kiinnostusta yrityksen tietoturvaan, erityisesti niiden sovellusten ja prosessien osalta joissa käsitellään luottamuksellisia henkilötietoja.

Tämän opinnäytetyön tavoitteena on selvittää kirjallisuuskatsauksen kautta tietojärjestelmän tietoturvasuunnitelman yleinen rakenne ja sisältö, sekä mitä erityispiirteitä sisältyy henkilötietoa käsittelevien järjestelmien tietoturvaan. Lisäksi tavoitteena on suorittaa tietoturvakatselmointi ja sen perusteella luoda tietoturvasuunnitelma kohdeyrityksen henkilötietojen hallintaan tarkoitetulle SAP HCM – järjestelmälle.

Opinnäytetyö toteutettiin produktina. Työn teoreettinen osuus on valmisteltu talvella 2012 – 2013 tutustumalla kirjallisuuteen. Empiirinen osa on toteutettu vuoden 2013 aikana. Empiirinen tiedonkeruu on tehty henkilöhaastatteluin, keräämällä ja analysoimalla dokumentaatiota sekä toteuttamalla työpajasessioita. Empiirisen osan pitkään ajalliseen kestoon ja työn lopputulokseen vaikutti kohdeyrityksessä tehty merkittävä organisaatiomuutos, joka astui voimaan kesän 2013 alussa.

Teoreettisen pohjan perusteella muodostettiin tietoturvasuunnitelman runko, jonka mukaan toteutettiin tietoturva-analyysi ja tietoturvasuunnitelma kohdeyrityksen SAP HCM -järjestelmälle. Analyysin mukaan kohdeyrityksen tietoturvan taso kohdejärjestelmän osalta oli riittävässä kunnossa, ja yrityksellä oli olemassa suhteellisen kattavat tietoturvariskien hallintamekanismit. Parannusehdotuksiakin kuitenkin löytyi, mm. tietoturvan hallintamalliin sekä käyttövaltuushallintaan liittyen.

Asiasanat
Tietoturva, tietosuoja, henkilötiedot, henkilörekisterit

Index

1 Introduction

Information is essential part of business operations, and business in general is nowadays highly dependent on information systems and the data stored in them. Therefore also concept of information security has raised its priority in business operations. This same raise of priority applies also to support processes in business operations, for example to Financial or Human Resources management. As electronic processes and common information systems become more common in organizations, increasing interest can be seen to information security and data privacy issues concerning employee and employment data management. In my profession as Human Resources system concept owner I have seen that interest grow in recent years both from employees and authorities side.

Information security as a term means the protection and back-up of information and systems and services used in maintaining information, in order to manage risks that are directed towards them. The objective for protecting information is to secure it from threats and accidents arising e.g. from software and hardware errors, unintentional and intentional user mistakes, natural disasters and other accidents. Protection is achieved by administrative, technical and other measures, which must be planned to cover both normal and emergency conditions. (Ministry of Finance 2009, 9.) In question of Human Resources information systems, those mentioned requirements and objectives are even enlarged by strict regulations and legal obligations to protect confidential and sensitive personal data. This sets great expectations for HR organizations to put focus on information security matters.

For me as thesis writer, the interest for this topic raised from my own work experiences, as I have been involved in implementing different Human Resources information systems in international companies and complex, multi-national system environments. System entities are often very large, and involve numerous parties, end users, interfaces and integrations. For person involved in such system implementations, it is important to understand information security risks which are targeted towards Human Resources systems, from different sources and looking at many angles, and how those risks can be reduced.

Targets for this thesis work are to define the elements of an information security for Human Resources information systems in general, and based on those elements create information security assessment and plan for SAP HCM solution in the target company.

2 Information security

2.1 Definition of information security

Traditional definition of information security is based on the value of information. In traditional definition information security consists of three elements: confidentiality, availability and integrity. (Hakala, Vainio & Vuorinen 2006, 4.)

The purpose of **confidentiality** is that information is accessible only for those people who are authorized to handle it. If a non-authorized user can access the information, confidentiality is lost. Methods for maintaining confidentiality include protecting systems and data storages with authentication tools, such as user IDs, passwords and encrypting. (Hakala et al. 2006, 4.)

Availability means that information is accessible when needed, and is in correct format for the user to be able to utilize information. Availability is maintained by securing that performance of information systems is good enough, and system usability fits the purpose. (Hakala et al. 2006, 4.)

The concept of **integrity** means that information is accurate and does not contain intentional or unintentional mistakes, caused by either user or system. Integrity is maintained by utilizing input restrictions, check-ups and methods for monitoring errors. (Hakala et al. 2006, 4.)

However, nowadays this traditional definition for information security is seen too narrow, and in extended definition that is used currently widely, traditional definition is complemented with two more elements: non-repudiation and access control. (Hakala et al. 2006, 5).

Non-repudiation means the system ability to recognize system users and save action log information. The objective for securing non-repudiation is usually either to ensure that the origin of the data is authentic, or prove whether information is used unauthorised. Certificates, protocols and verification methods are the most common means used for protecting non-repudiation. (Hakala et al. 2006, 5.)

Access control consists of the methods by which the infrastructure used for managing information is controlled. Individual users' authorization to data is covered in definition of confidentiality; access control focuses on the safety of networks and devices and authentication required for handling and accessing the data. Access control methods include e.g. restricting the usage of networks and prohibiting use of company devices for personal use. (Hakala et al. 2006, 5-6.)

Information security is commonly confused to term data protection. These two have common elements, but in practise what differs them is that data protection is about protecting individual's data privacy and integrity, whereas information security is about the means and methods how that data is protected. However, it is not sensible to talk about information security without referring to concept of data protection, as they are essentially linked together. (Laaksonen, Nevasalo & Tomula 2006, 17.)

2.2 Value of information security in organization

Companies and organizations are lead by information. In order to ensure that valuable information is accurate, timely and intact, and do not end up into rivals knowledge, information security matters have great importance for organizations. Most companies have experienced some harm caused by viruses, malwares, and attacks or even by own peoples actions, and know that the consequences can be costly. (Raggad 2010, 6.)

At its best, well-maintained information security can bring company competitive advantage. For example, implemented information security culture enables continuity and stability of business. Also, in many businesses good information security improves company's position in tendering, as information security requirements are more and more common in tenders. (Laaksonen et al. 2006, 18.)

Vice versa, whereas well-maintained information security can bring benefits to organization, poor information security may cause serious damage to operations and business, and lead even to remarkable financial losses. Failing in information security may also ruin organizations reputation and public image, and lead to lack of trust in the markets. (Laaksonen et al. 2006, 19.)

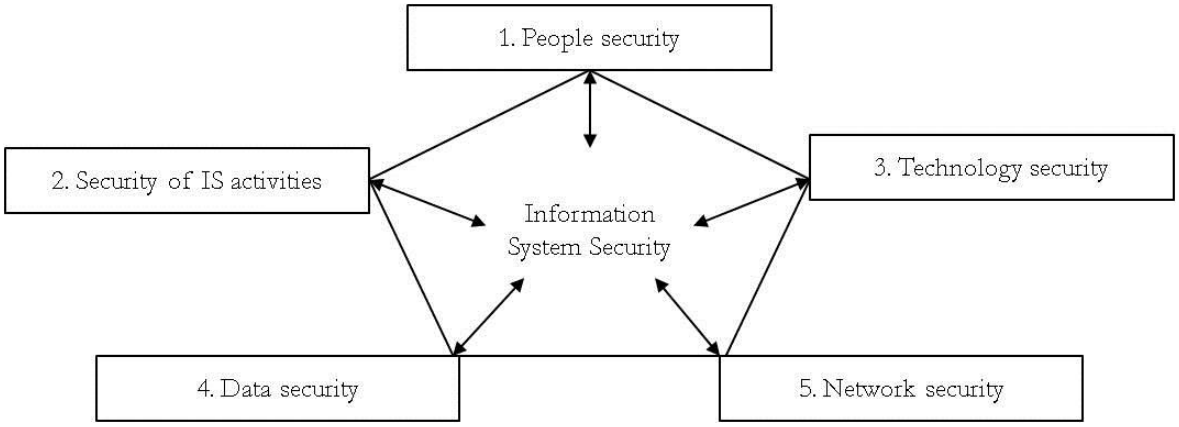
Information security consists of many small actions that are part of everyday activities. Well-maintained information security is part of organizational culture, where everyone understands the meaning of information security and act to gain and maintain it. These acts contain both technical and administrative tasks, and require systematic and purposeful approach. (Laaksonen et al. 2006, 17.)

Information security is regulated by many international norms and guidelines. For example OECD has prepared a guideline of information system and information network security principles already in 1992. In US noted law is Sarbanes-Oxley act (SOX), which was established after remarkable misappropriations were revealed in so called Enron case. SOX act sets very strict regulations for listed companies of how confidential information must be handled. In European Union, there are several directives in which information security matters are handled, and which set guidelines for national legislations. Also in Finland, there are several laws guiding information security, and Ministry of Finance has created guidelines named VAHTI for providing instructions both for public and private organizations on information security matters. (Laaksonen et al. 2006, 23-26.)

Both national and international legislation sets requirements for organizations on how it should take care of its information security. Many times these requirements are given on general level, and it leaves much room for the organization to define what is the desired level and preferred means for their information security. (Laaksonen et al. 2006, 18.)

2.3 Security of an information system

Information system in this context means the solution entity meant for producing, generating and managing information. The entity consists of five resource elements, as illustrated in picture 1: people, activities, data, technology and network. In order to protect information, all these elements need to be protected. (Raggad 2010, 11.)



Picture 1: Security of an information system (Raggad 2010, 11).

People security aims to protect system from its users' mishaps. Unintentional damages can be prevented and reduced by instructing, educating and training users, and by communicating security policies clearly in organization. Intentional damages can be restricted by narrowing down user rights by authorisations and checking users' suitability and background in recruiting process. (Raggad 2010, 17; Ruohonen 2002, 5.)

Security of system activities is a wide area, withholding all the procedures for improving security in system environment, maintenance, support and development, and enhancing continuity. Basically, activity security includes all the methods that enable system to be used safely. Important part is the management and documentation of information security elements. Administrative and organizational security actions focus on creating policies and guidelines, planning actions, training and instructing users and measuring operations. (Raggad 2010, 13; Ruohonen 2002, 5.)

Technology security means protecting the solutions and programs used in maintaining the information, as well as hardware that are used in maintaining the system, e.g. computers, routers, servers etc. Protection methods include e.g. licence management, access controls and authentications, maintaining action logs, maintenance services, warranty procedures and lifecycle management. (Ruohonen 2002, 5.)

Data security requires protecting the data content itself, in practise files and databases containing the information. Protecting methods are e.g. backup copying, using virus

protection programs, user access management and restricting changing the data by utilizing user profiles. (Ruohonen 2002, 4.)

Network security focuses on protecting the networks where system data is being transferred– both internal and external – from unauthorized modification, destruction or disclosure. Common methods used are isolating networks using firewalls and proxy servers and encrypting the information. (Raggad 2010, 19; Ruohonen 2002, 4.)

Protection of an information system requires protecting all these elements which jointly produce the information.

2.4 Special security requirements for Human Resources information systems

As Human Resources information systems maintain and manage sensitive personal data, which is usually protected by national or international legislation, the information security requirements for HR systems are relatively high. **Personal data** in this context comprises all information related to a natural person that describes his/her persona, features and characters, or even his/her family members and people living in same household. In practice, most of the information related to e.g. employee and employment data is comprehended being personal data. (Laaksonen et al. 2006, 32.)

When dealing with personal data, information security should be aligned with all HR objectives, operational model and processes, and all HR professionals should be aware of the legal and ethical issues that are related to the use of personal data in HR information systems (Wong & Thite 2012, 527).

The information security and privacy questions related to Human Resources information system can be divided to two main categories: 1) what kind of information can and may be collected and stored in the system and 2) who may access and maintain the data (Wong & Thite 2012, 529). In the following is a brief introduction to both mentioned items.

2.4.1 Regulations for collecting personal data

In most of the countries, allowed data content and the information security requirements regarding personal data are regulated by legislation. In Finland, there are several laws setting guidelines for personal data management, most important ones being Personal Data Act (523/1999) and Act on the Protection of Privacy in Working Life (759/2004).

Personal Data Act (523/1999) is a general law which has to be applied to all activities handling personal data, if no other law gives more detailed requirements. The purpose of Personal Data Act is to protect individuals' privacy and fundamental rights when maintaining personal data, and to promote good practices of data processing methods. (Laaksonen et al. 2006, 31.) The act states three principles which apply to the whole life cycle of personal data management. First principle, **duty of care** means that organization must obey laws and regulations when handling personal data, practice good data processing methods, and act all the times so that it does not jeopardize data privacy. Second principle, **planning obligation** states that organization must plan and define why personal data is collected, how it is done, and what data management processes are. Third principle of **purpose limitation** determines that organization may use personal data solely for the purpose to what it is defined (planning obligation). (Laaksonen et al. 2006, 38-39.)

Two fundamental requirements for implementing data protection in an organization according to Personal Data Act are 1) to ensure that the purpose for handling personal data is clearly defined and 2) to plan the practices and processes for maintaining personal data in a manner that data security is ensured in all process phases (Data Protection Board, 2013).

As for the purpose for handling personal data, collecting and maintaining personal data must be described so that it clearly indicates what controller's task it is required for. The purpose should explain why collecting personal data is necessary, what task or objective the personal data serves, and what party in organization owns the register. In this context owning the register means that the party is responsible for the data itself and its information security. (Laaksonen et al. 2006, 35-36.)

Examples of typical collector tasks (Data Protection Board, 2013) are e.g. personal data file that employer has regarding employees and recruitment candidates, patient registry that healthcare units have for managing treatment procedures, personal data files that social services have for managing statutory tasks like daycare and care for the elderly or customer files that company has regarding maintaining client information.

Based on description of purpose, it can be evaluated what are necessary and adequate data elements to be collected, and what are the safety level requirements for those data elements (Data Protection Board, 2013). As for planning the practices and processes for maintaining personal data, Personal Data Act (523/1999) 32nd section sets principles for how organizations must implement the information security requirements:

> The controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. The techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures.

It is notable that the act does not set any concrete measures and tasks for protecting the information. This puts the pressure for organization to define what are the adequate actions and methods for data protection, and what reasonable costs for the protection are.

Planning of practices and processes should be done considering and taking into account the whole register. According to Data Protection Board (2013), it should be evaluated who can maintain personal data and when, what kind of data can and may be collected, how the rights of a data subject are ensured, and is the organization responsible of making notifications to Data Protection Board. (Data Protection Board, 2013.)

As end result, controller should prepare Description of File, where is described the purpose for processing the personal data, content for the register, regular sources for information and regular destinations of disclosed data, and principles how the data is secured. In addition, in Description of File must be nominated the controller's responsible person for register. (Data Protection Board, 2013.)

Act on the Protection of Privacy in Working Life (759/2004) is meant for ensuring employee's privacy even when working for an employer, on employer's premises and using employer's tools and equipment. Act sets also principles on how employee data is handled, about tests and check-ups that may be performed for employee, technical surveillance on working place, and accessing employee's emails. The decisions and actions which employer makes may not contravene employee's privacy. (Laaksonen et al. 2006, 49-50.)

On European level the guiding regulation for information security and personal data protection is **European Union Data Protective Directive** (95/46/EY). Directive sets means and boundaries for maintaining personal data, and declares principle that personal data can be transferred within European Union member countries without restrictions. Directive requires that all European Union member countries are obliged to create national regulations for standardising data privacy protection. (Laaksonen et al. 2006, 26.)

2.4.2 Regulating user access

For Human Resources information systems, the biggest challenges in information security matters are often related to user access management. Databases, servers, networks and software can usually be protected with technical measures and controls, but protecting system from unauthorized or adverse use is more difficult and complicated. In addition, HR information systems must comply with Personal Data Act requirement of planning obligation in a way that only people who have justified need to display and maintain personal data may do so.

Personal Data Act sets also requirement that personal data must be kept flawless. When collecting personal data in information systems, the data integrity must be followed up and ensured regularly. User access management is essential for ensuring that data and information changes are controlled and done by an authorized party. (Laaksonen et al. 2006, 40.)

Access to Human Resources information systems (HRIS) is typically administrated utilizing concepts of users, user groups and user roles. HRIS users can be roughly divided to two categories: employees and non-employees. Typical user groups in employee category are HR professionals, managers, analysts, technical staff and employees themselves. HR professionals are most commonly the users collecting and maintaining the personnel data. Manager users typically use HRIS data for leading their teams' work and for decision-making purposes. Analysts are people whose work tasks consist of examining, analysing and reporting the data and who provide supporting information for organisations processes, e.g. resourcing and workforce planning. Technical staff ensures that system is usable, available and up-to-date in technical perspective. Employees, if enabled as users, usually manage limited personal information utilizing self-service functionalities. (Bedell, M., Canniff, M. & Wyrick, C. 2012, 60-63.)

Non-employee user category includes job seekers, suppliers and partners. Job seekers are those who log in to company's recruitment system and register themselves as candidates, and are therefore potential employees. Partners and suppliers are most commonly external parties who participate to HR processes, e.g. payroll providers, recruitment agencies and benefit administrators. (Bedell et al. 2012, 61.)

The wide variety of HRIS user subcategories creates very complex demands for user role creation, user access management and authorisation. All these user subcategories have different needs regarding the width of information, and need to use the system in different extent. Users are assigned to security roles based on their user category and/or subcategory, and roles restrict or allow user to access data. As an example, a user role can define that certain processes and personal data elements are available and/or editable for HR professional role, but not for manager or employee role. In addition, role can define whose data user can access, for example whether user can see only own data, subordinates' data or even wider range of employees. (Bedell et al. 2012, 71-73.)

2.4.3 Regulations for responsibilities in personal data protection

In organization, personal data is usually maintained in one or several registers, and the organization which maintains the register is called controller. Controller is responsible

for complying with laws and regulations related to personal data protection, and is responsible for organizing necessary actions and means to ensure data security. It is notable that controller is always organization, not individual person or employee. (Laaksonen et al. 2006, 34.)

It is recommended that every organization should nominate a data protection officer for each of the registers that maintain personal data. The role for the data protection officer is to ensure that all the actions required by laws and regulations are done in organization, and the requirements for data security protection are fulfilled. Data protection officer should participate in planning and follow-up of data maintenance processes, support both maintainers and registered employees in data security matters, and report to management about the status and development needs in personnel data protection. Role is also to inform necessary parties if any violations or deviations against regulations should appear. (Vanto 2011, 184-187.)

Many European countries have already regulations regarding organizations' responsibility of naming data protection officers. For example, in Sweden it is recommended for all organizations to nominate data security officer (personuppgiftsombud), and in Germany, every organization which has more than 10 people managing personnel data is required to nominate data protection officer (datenschutzbeaufragte). In France, when nominating a data security officer (le correspondant informatique et libertés) it must be informed to national data protection board and employee union representatives. (Vanto 2011, 185-186.) It is expected that requirement for nominating data security officers to organization will be included in European Union directives in coming years.

However, it is to be noted that nominating data protection officer does not reduce the responsibility for controller of the personal data register. The overall responsibility of the register and how it is maintained remains on the controller. (Vanto 2011, 187.)

3 Information security plan

The target and purpose for creating an information security plan for a system is to ensure that all aspects and elements of an information system are secured well enough and with reasonable efforts, compared to risks that are recognized to threaten the system security (Ruohonen 2002, 6).

Information security involves the whole organization and its personnel, not only top management or ICT staff. Furthermore, only technical and physical means cannot ensure sufficient level of security; essential part of creating an information security plan is to focus on people and their behaviour. (Laaksonen et al. 2006, 19.) In the next chapters are described the most common elements of information security plan.

3.1 Information security objectives

The first task when creating an information security plan is to define objectives for information security of the target system. Management should decide the desired state for information security level, and define its significance for organisation. The target state and importance should be reflected and maintained in strategy, operational guidelines and policies, e.g. in risk management and information security policy. Based on these guidelines and principles, organisation can prepare practical information security instructions that act as governance for processes and employees. (Ministry of Finance 2009, 11.)

Based on principles and guidelines given, information security plan should set desired level for information security for all parts of the target system. Evaluation should be based on acceptable risk level and required security level, as well as acceptable cost level for security improvement. Based on the importance of each system element, the objectives for information security are set. However, objectives should be set only to a level where they can be realistically achieved. If objectives are set unrealistically high, that will not only frustrate the parties involved, but also lessens the credibility and reliability of information security plan, and ultimately creates false image of the level of system security. (Ruohonen 2002, 6.)

Objectives should also create layers for information security, i.e. have many different actions and measures combined for ensuring system security. For example, telecommunications could be protected both by using firewalls and proxy servers, but also by using intrusion detection systems. (Ruohonen 2002, 6.)

Information security plan must have listed the actions that will aim to cover selected objectives and manage risks. Risk-driven security plans usually handle three kinds of security controls: **technical controls**, **operational controls** and **management controls** (Raggad 2010, 26). Those are explained in following chapters.

3.2 Management controls

Management controls focus on management of the information system and its security in total, and management of potential risks for the system (Raggad 2010, 26).

Preliminary task for creating an information security plan and setting management controls is **risk assessment and evaluation.** Information security analysis and plan should be based on analysis of potential risks. Target for risk analysis is that all the risks that might affect the system and its usage are recognized and identified. Identified risks are then classified by their impact and probability, and contingency actions are prioritized based on severity of risk. (Hakala et al. 2006, 79; Ruohonen 2002, 7.)

Risk analysis can be roughly divided to two phases: identifying risks and classifying them. In risk identification, all potential threats and risks are systematically recognized and listed. It is important to analyze the risks from several perspectives: present and potential future risks, internal and external risks, and unintentional and intentional risks. Then, the recognized risks are analyzed against the probability that they are realized, and impact they have if and when realized. (Hakala et al. 2006, 79-80; Ruohonen 2002, 7.)

Common security risks that should be at least taken into account are (Wong & Thite 2012, 524-525)

- Human error: user enters the data incorrectly or accidentally removes the data. This risk prospers especially if system is not well developed or users are not adequately trained.
- Misuse of computer systems: person is able to get unauthorized access to system.
- Theft: the information content is stolen for adverse purposes.
- Computer-based fraud: data entry or processing routines are modified, which ends up to erroneous data.
- Viruses, trojans and worms: these are common external threats, and are targeted to either damage the system functionality or the data content.
- Hackers: external accesses the network or computer unlawfully.
- Natural disasters: for example fire, flood or lightning destroys or disrupts facilities or hardware.

It requires from an organization a proactive information security plan to manage these threats and risks (Wong & Thite 2012, 525).

In order to get risk assessment comprehensive and realistic, it is recommendable to involve participants from different parts of organization to participate risk identification and evaluation. Workshops and working groups have turned out to be effective methods for risk identification. Diverse perspectives and opinions bring out risks from various angles. Looking from other perspective, the risk and its impact may vary and look totally different. (Laaksonen et al. 2006, 121.)

Information security plan should be reviewed and updated often enough for ensuring that the set objectives for information security are valid and match the recognized risks; on regular basis, and especially when changes to system are done (Ruohonen 2002, 12).

Technical and organizational controls need to be re-evaluated and updated regularly to ensure that they fulfill current contextual, legal and technical requirements. Regular follow-up and auditing is also needed for ensuring that all employees act according to laws and regulations, principles set by controller and practical work instructions given when maintaining personal data. (Vanto 2011, 139.)

Information security should also be measured. If possible, organisation should set indicators that can measure achievement in information security management both on annual basis and over longer period. The level of information security as well as the risk management of identified risks should be evaluated regularly, for example by internal auditing. The target for measuring is to ensure that organisation is complying with laws and regulations, implements the risk management plan, and operates daily processes in a well-guided manner. (Ministry of Finance 2009, 12.)

3.3 Operational controls

Operational controls focus on those security methods and mechanisms which are implemented and executed primarily by people (Raggad 2010, 26). Operational controls include the principles and guidelines given for system users and administrators, for example instructions for documentation and documentation maintenance, instructions on compulsory maintenance tasks (e.g. backups, virus protection), instructions that have to be delivered to end users when allowing access to system, and instructions for end users on how to handle exceptional cases, e.g. if user notices a system error. (Ruohonen 2002, 7-8.)

Primary purpose for operational controls and information security instructions is to help the system users and administrators maintain and handle personal data according to laws and regulations and organization's internal principles and agreed objectives. Secondary purpose may be presenting third parties like authorities, Data Protection Board or business partners that organization gives value for correct maintenance of personal data. (Vanto 2011, 189.)

Instructions should be written in a manner that they are understandable and clear, and leave no room for interpretation. Therefore it is not recommended e.g. just to copy act or directive to instructions as such, but to explain and open the requirement of law. Instructions should be reviewed regularly, for example yearly, to ensure that they follow latest regulations. (Vanto 2011, 190.)

Notable is that system information security plan should not include the instructions themselves; instructions should be individual documents to which information security plan references to (Ruohonen 2002, 9).

Protecting physical environment sets ground for other information security protection methods. Without safe and secured environment, information security cannot be reliably verified. Protecting physical environment include tasks like access control in premises, restricting access to physical storages of data, and managing access rights regarding leaving employees. (Vanto 2011, 139.)

Physical environment protection targets to prevent that information contained in premises is not destroyed, damaged or stolen. Physical protection should take into account at least following risks: theft, fire or sudden rise of temperature, flood or water damage, power failure and dust. Also, access to protected areas should be controlled and registered, and access rights including keys should be managed. (Laaksonen et al. 2006, 126.)

All physical environments are not equally important. Most commonly for example facilities used by research and development unit, ICT or top management are considered to require higher level of protection. Physical environments should be evaluated regularly, e.g. along with risk assessment, and development actions for improving security should be implemented for example in connection with regular reconstruction and renovation activities. Priority classification of premises is a good tool for recognizing those environments which require higher level of protection. (Laaksonen et al. 2006, 125.)

Personnel security targets to protect information against errors and misuse done by employees, intentionally or unintentionally. Employees' job descriptions should be well-defined and clear, and responsibilities set so that dangerous work combinations (e.g. same person can request and approve data) are not formed. (Laaksonen et al. 2006, 138.) User authorization, user access and user roles must be defined so that they meet the information requirements of work tasks. User should only be able to manage data that s/he needs in his/her work tasks. (Laaksonen et al. 2006, 43.)

When a new employee is hired, supervisor should go through company information security policy and principles for maintaining information security together with employee, and get employees documented confirmation that s/he accepts and obeys the rules (Laaksonen et al. 2006, 142). Users who maintain personal data extensively should sign Non Disclosure Agreements. All users should also follow instructions and principles given regarding maintaining information security, and participate in training about information security requirements and legislation regulating personal data management. (Vanto 2011, 139.)

Maintenance controls include those processes which target to ensure that system maintenance is controlled and monitored, and all changes that are done to system are tested, approved by relevant parties, and documented. This ensures that the system is always in desired state, and all functionalities can be reviewed via updated documentation. (Laaksonen et al. 2006, 154.)

All changes, whether they are changes to functionality, security program updates, error fixes or version upgrades, should follow change management process. All change requests should be done in writing, and analyzed by several people. Essential thing to ensure is that changes cannot be implemented, tested and approved by same party. Also transporting changes between environments should not be allowed to be done by developers themselves. There should also be a roll-back plan existing, in case problems arise and after done changes system must be reverted back to earlier status. (Laaksonen et al. 2006, 154-155.)

All measures that aim to ensure safeguarding the accuracy and completeness of information are also part of operational controls. Measures targeting to users act in a manner which improves integrity include e.g. access control, data classification instructions, input/output controls and reconciliation routines. (Raggad 2010, 145; Wong & Thite 2012, 523,)

Continuity planning is important part of information security management. Target for continuity plan is to ensure that business processes can continue, not only in normal situation but also after exceptional disturbances. Continuity plan contains regular

management and maintenance activities, which enhance continuity of the system. (Laaksonen et al. 2006, 228.)

Information must be protected in a way that it remains intact and is available for those who need it in their work tasks. This means that data must be secured against accidents and disasters, or other unexpected and sudden disruptions. Most convenient way for protecting data is to regularly and automatically create system copies and back-ups from the target system, and store them in a safe environment. It is good to test the restoring process every now and then, to make sure that back-up systems work OK, and check that restored data can be read normally. (Laaksonen et al. 2006, 169.)

It is recommended to include a recovery plan in continuity plan. Recovery plan describes how system is returned to condition where it can be operated if system faces a risk that ends to damaging the system. The recovery plan should aim to implement measures that ensure that system security can be restored to original level, as little data as possible is lost, and same risk is prevented to happen in future. (Ruohonen 2002, 9-10.)

3.4 Technical controls

Instructions and policies form a significant part of information security planning, but are not alone yet sufficient means for protection. In addition to guidelines and process control, also technical measures are required for ensuring information security.

Technical controls include those actions which are taken to improve information security by using equipment, installations and software. Technical controls require also that network and infrastructure matters are planned in a way that they support information security and protection. (Laaksonen et al. 2006, 172.)

Technical controls and instructions include system related items as for example computer and system settings (e.g. firewalls), user ID settings and user ID management procedures, network structure and settings and program installation instructions and settings (Ruohonen 2002, 7-8).

Personal Data Act 32nd section requires that personal data register must be protected in a manner that illegal attempts to access the equipment where data is stored and especially attempts to manipulate the data immediately launch an alarm to the controller. In practice, not many organizations manage to meet this requirement as technical methods are not comprehensive enough. In minimum, organization should utilize firewalls and system logs, and regular follow up of the log information. (Laaksonen et al. 2006, 42.)

Data transfer between information systems e.g. via interfaces or integrations must be secured so that the data content does not disappear or alter in the process. In practice the controller must be able to reliably monitor the quality of data transfer with predefined controls. (Laaksonen et al. 2006, 42.)

Identification and authentication is a combination of methods, processes and technical measures which enable controlling users and equipment that have access to information. Identification and authentication aim to ensure that only parties authorized by content or system owner have access to information and systems. (Laaksonen et al. 2006, 173.)

User identification is usually based on user ID and either a password or other authentication method connected to user ID. Organization should define and implement a password policy, and describe clear processes how to procedure password changes e.g. in case of password expiration or loss. Passwords should also be protected by encryption or other protection method. Special attention should be placed for protecting and monitoring administrator user IDs, as these IDs usually have non-restricted access to all system functionalities. (Laaksonen et al. 2006, 175-176.)

User authorization is one of the most important processes regarding information security. Authorization management contains creating new user rights, changing user rights and removing user rights and closing accounts. In addition, authorization management contains monitoring and reviewing authorizations. (Laaksonen et al. 2006, 151.)

The principle for authorization is very simple: user should get authorization only to those items which s/he needs in performing work tasks. When employee's work tasks change, all access rights should be re-evaluated and redefined to meet new work requirements. Unnecessary access rights should be removed. Also, when employee leaves the organization, process should take care that access rights are immediately inactivated. (Laaksonen et al. 2006, 143.)

User authorization approval should be centralized and responsibility assigned to system or content owner of the target system. System administrators should have clear instructions on who is allowed to order user rights or changes to authorizations. User right requests should be done always in written format, e.g. using structured form, and documented requests archived in a way that it is possible to review afterwards who has requested user rights and when. (Laaksonen et al. 2006, 151.)

System monitoring is used for several purposes. Monitoring can be executed real time, when focus is more on system availability, network slowdowns and current data load. It can also be done afterwards, when target is usually error detection and handling based on information collected to log files. In addition, network monitoring is important method for identifying possible intrusions and attacks. (Laaksonen et al. 2006, 192.)

There are several methods available for how networks can be protected and monitored. Network should be separated from other networks using a firewall. In addition, it is recommendable to even separate internal network to smaller pieces, and divide own network area to systems or functionalities that have different level requirements for information security, e.g. utilizing priority rating for the systems. (Laaksonen et al. 2006, 182.)

Virus detection systems should be placed for supporting the protection of the system. Virus protection programs should cover both workstations and servers, and virus protection programs should be updated often enough. (Laaksonen et al. 2006, 204-205.)

3.5 Security responsibilities

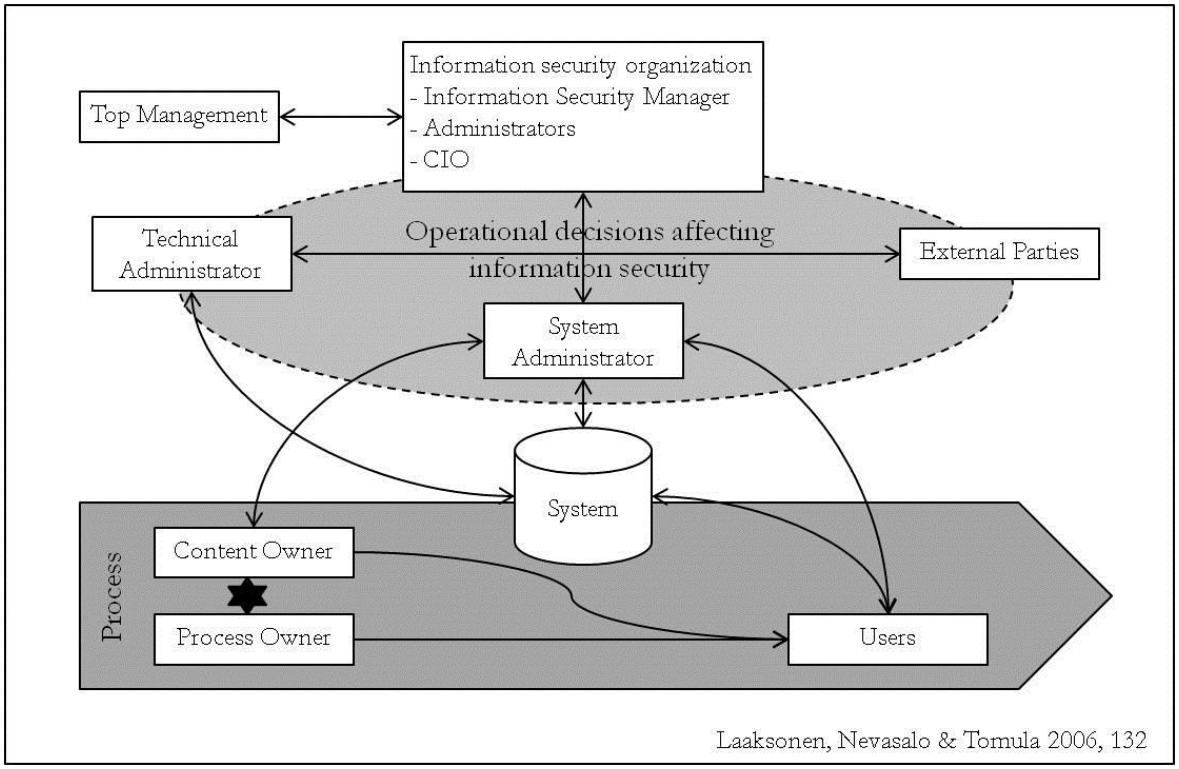
In order to succeed, information security requires first and foremost commitment from management to maintenance and development of information security. Management must ensure that enough and suitable resources are allocated for information security and data protection work. Furthermore, by creating a transparent management model that supports information security management, and a culture that supports high information security, management sets an example that involves and encourages personnel to implement information security on their behalf. (Ministry of Finance 2009, 11.)

Information security policies and practices in organization are part of overall IT governance model. IT Governance model guides all ICT related operations, and sets principles for organizing, evaluating and prioritizing tasks and development actions. Well-organized operations include clear and defined responsibilities and comprehensive communication. (Laaksonen et al. 2006, 121.)

Information security must be maintained in all levels of organization: top management must have clear understanding of risks and security threats, supervisors must manage questions regarding information security in daily tasks and operations, and employees must understand the instructions and requirements for their own actions. However, overall planning and follow-up of information security and guiding policies is clearly on management responsibility. Based on measured results and evaluation, management should continuously analyse how set targets are achieved and what parts of information security should be further developed. (Laaksonen et al. 2006, 122.)

Resourcing the information security tasks is essential in information security planning. Management is responsible for reserving enough resources for performing and implementing security activities. However, it is important that organization has nominated responsibles for information security matters, which can discuss with management and present the needs and requirements in a way that management can understand them and evaluate the proper resource needs. Nominated information security organization is responsible for coordinating the tasks, preparing instructions and guidelines, and organizing necessary training. It also monitors operations, and reports the status of

information security items to top management. (Laaksonen et al. 2006, 20, 131.) Following picture 2 (Laaksonen et al. 2006, 20, 132) illustrates the relationships between parties in information security organization:



Picture 2: Relationships between information security organization and other actors

Content owner is usually person who creates or produces information. When information is related to business processes, owner is usually the person responsible for the process, even though s/he personally does not produce the data itself. Content owner defines the security level of the information and who can maintain or access it. Content owner also ensures that data is reliable and available for those who need it. Process owner is responsible for ensuring that information security is taken into account in all phases of the process, and people who participate the process are aware of information security requirements. (Laaksonen et al. 2006, 20, 132-134.)

Every system should also have nominated administrator. Administrator ensures that the system works correctly, and the data which system processes is accurate. Usually administrator is also responsible for training other users. Regarding information security, administrator often is the one managing other users' authorisations, but s/he should not be the one approving access rights. That task should belong to system, content or

process owner. In addition to administrator, organization can nominate also separate technical administrator, who supports the system and platform where it is run. (Laaksonen et al. 2006, 20, 134-135.)

When listing tasks and actions, the information security plan should also list responsibilities for each mentioned security item. This will clear up the tasks between each party, and create transparent path for each task. In addition, if information security organization is properly communicated to personnel, employees know to whom to turn to if and when they face an issue or a problem regarding information security matters (Laaksonen et al. 2006, 131; Ruohonen 2002, 9.).

4 Implementing information security plan for SAP HCM

In this chapter is described the process how an information security assessment and plan was implemented to target company. The target company is Finnish-based, internationally operating service company, which has operations currently in 11 European countries. Its annual turnover is approximately EUR 1 900 million, and it employs around 28 000 professionals. Company's business comprises of several different business areas.

4.1 Target system

SAP Human Capital Management is a part of SAP AG's Enterprise Resource Planning (SAP ERP) system. SAP Human Capital Management system (later SAP HCM) has been in use in target company since 2005. The system was first implemented as a part of overall SAP ERP implementation in Finland, and master data template was originally set up from Finnish perspective. Later in 2010, a global template was created, and SAP HCM rollouts for company's foreign subsidiaries were implemented.

Currently company's SAP HCM is in use in all 11 operating countries, and it withholds data regarding all approximately 28 000 currently active employees, and an archive of terminated employments. SAP HCM is considered as a master system for employee, employment and organisational data in the target company.

Target company's SAP HCM solution is implemented in Finnish and English languages. The solution has at the moment approximately 2 100 end users, which range from managers and superiors to assistants and HR professionals. Every user is granted one or several user roles in the SAP HCM system, according to his duties in the company. Regardless of duties, permission from the user's higher superior is needed for granting access and individual user ID to the user. In addition, HR professionals, who as per their job duties and role in organization have wider access to personal data, have undersigned individual NDA agreement related to managing personal and organizational data.

Following SAP HCM functionalities are in use in target company: Organizational Management (OM), Personnel Administration (PA), Enterprise Portal (MSS/HR Admin), Adobe HCM Processes and Forms, Business Information Warehouse (BW), Performance Management (MBO) and partly also Time Management (PT) and Personnel Development (PD).

4.1.1 Interfaces and integrations

The SAP HCM system has standard ALE integrations in use to following other SAP ERP modules that are in use in the company: E-Recruiting, BW Reporting, Finance & Controlling (FICO), and CRM. Data that is transferred in integrations includes general employee data, some basic organizational and job data, and contact information. Exception is BW integration, which transfers larger amount of data; basically most of employee, organisation and transaction data for reporting purposes.

There are also altogether 45 interfaces to other internal and external systems, e.g. to local payroll systems, purchasing and invoice management systems, and to systems related to time management and production operations. 13 of those interfaces are inbound, and 32 are outbound.

4.1.2 Maintenance and development

System maintenance in target company has been outsourced to external maintenance partners since 2008. In overall, there are currently two partners: one maintaining servers and platforms, and one maintaining the SAP HCM solution and SAP NetViewer portal, which acts as the end user access layer. Partners have their operations run in Finland, elsewhere in Europe and outside EU countries. Application maintenance partner changed in 2013 during the writing of this thesis, and as the time of writing the transition process was still on-going.

System maintenance and monitoring processes in the target company follow ITIL practises. Also system development and change management follow ITIL best practise methods and company's project management model. Company does not have internal SAP basis consultants or developers; instead development services are sourced from trusted vendors. After development, all changes and releases are tested in a separate

test environment before they are taken into production. New functionalities are taken into production according to a pre-decided release schedule, and by following Release Management processes.

4.2 Current state of information security planning

Company has valid IT Governance model and information security policy created, supplemented by related templates and document models. There is also a generic template for information security plan existing. However, as it is designed to fit and cover several different types of systems, the template gives some space for adjusting the result document to fit the target system.

Target company has made information security analysis and business continuity plan at the time when SAP HCM was initially implemented back in 2005, but those plans have not been updated ever since, and are nowadays somewhat outdated. No specific review of security controls has been conducted for company SAP HCM solution.

Numerous rules of behaviour have been made for SAP HCM users, both for end users and administrator users. There are also instructions existing e.g. regarding using sensitive personal data in manager's work, Change Management and Release Management instructions, and common information security guidance and policies. Most of the instructions are available for users in company intranet and document management systems. Company has also valid Description of File existing.

4.3 Planning

The thesis planning started in winter 2012-2013 by collecting the theory part and background data. When planning the information security plan content, the company's existing information security plan template was utilized, but it was reviewed against the theory base which was collected for this thesis work, and modified a little. Furthermore, as some of the parts in the plan were set as company mandatory, but are not common elements in generic information security plan based on literature review, information security plan index also includes items which have not been introduced in this thesis. The index of the implemented information security plan can be found as thesis appendix 1.

During planning phase, thesis writer decided to exclude external partners' information security evaluation out of the scope of this information security assessment, as information security matters related to external partners are specified in very detail in the associated service agreements between the target company and external service providers.

4.4 Realization

Risks were recognized and assessed in two internal workshops, which were held in October 2013 and lead by thesis worker. Workshop participants were selected to represent different functions in organization, and to include participants from different user groups: HR professionals, ICT professionals and business representatives. First workshop concentrated on identifying information security risks, and second one evaluating and classifying them.

As a result of these risk workshops, altogether 11 risks were identified. All identified risks were evaluated and given estimate of the significance: probability of risk to be realized, and impact if risk is realized. In addition, existing controls to reduce risks were recognized and listed, and workshop participants also identified possible new measures and controls for diminishing risks. Risks and findings were summarized and included in information security plan document.

Other information and content to the information security assessment document was collected from several sources. Management controls, such as operational instructions, rules of behavior and information security policies were mostly available in company intranet. Most parts about operational controls like personnel security, maintenance controls and audit trails were gathered by interviewing relevant people in organization.

Information about physical and environmental protection as well as telecommunications, network and interface information was mostly gathered from technical documentation, which is stored in company internal document management system. In addition, some related people in IT organization were interviewed for clarifying interdependencies and gaining more detailed information. Information about technical con-

trols, such as identification, authentication and authorization were available for thesis writer by her job role, as thesis writer acts as content owner of the target system.

Information was collected and interviews held during spring 2013 and autumn 2013. Organization went through remarkable transformation in its operations during summer months, which caused slight changes and delays for execution of this assessment, mostly due to changes within roles and responsibilities within the company.

After information security assessment and plan was written, thesis writer sent it for review in few selected people in organization for validating that content is correct and verifying that document contained all necessary information.

5 Discussion

5.1 Results and conclusions

As mentioned earlier, implemented information security plan follows the company's existing information security plan template. Based on theory base, company template includes all basic elements that are generally seen necessary in information security plan. In the following is described a brief comparison.

Based on literature review, most common elements for information security plan are: objectives, management controls, operational controls, technical controls and security organization. All these mentioned items were included in company template, but it deviates so that objectives and information security organization are included in a template in chapter called System description, which in addition to two mentioned items contains also general information about target system and its purpose, and about system environment, setup and landscape. Index for implemented information security plan then contained five main chapters: System description, Management controls, Operational controls, Technical controls, and Evaluations and recommendations.

Risk evaluation was included in the chapter Management controls. Altogether 11 risks were identified in workshops. Most of them were related to user access management and user authorization. This could be expected, because of the nature of information which sets high demands for confidentiality, and because of strict legal requirements for management of personal data. For identified user access management and authorization risks, several existing and new technical controls were identified. Some risks were also identified regarding system maintenance; for those risks it was recognized that company has already covering operational controls existing.

Based on evaluation made in risk workshops and assessment made on grounds of interviews and documentation, the overall status of information security management in target company SAP HCM solution is in adequate and satisfactory level. For the most significant identified risks, proper security controls exist and risks can be reduced to acceptable levels with current controls and measures. However, there is also some room for improvement and development.

On grounds of theory basis, most important development item for company is to create a governance model for managing information security regarding target system. Company has valid general information security policies and guidelines existing and overall ICT governance model defined, but that is not sufficient when focusing on information security of a one single system. Company lacks an organ whose responsibility is to follow-up and measure information security risks towards SAP HCM, organ which would also be responsible of organizing corrective actions and reporting information security status to top management (as presented in chapter 3.5).

Following recommendations were made for organization based on information security evaluation and assessment.

- Continuity plan should be renewed to meet current requirements. During making this information security assessment and plan, company came to conclusion that it is more sensible to create a totally new continuity plan, instead of updating the old one, due to done international roll-outs and expanded interface and user amounts.
- Current Description of File needs minor updates, and needs to be translated in English.
- There should be more systematic and regular process for checking correspondence between the job functions of users and their roles in the system to avoid too wide-ranging access rights, e.g. due to job role changes. Company has already made actions towards this development, and is currently connecting SAP HCM user ID management to Identity Management (IDM) system. There is an opportunity to utilize job roles in IDM to automatically control and assign user roles. This development pursue should be continued.
- It should be considered if password policy for SAP HCM solution needs to be renewed to comply with company general password policy.
- It should be evaluated whether SAP HCM entity should be connected to company GRC tool (Governance, Risk & Compliance), which is in use in some other SAP modules for managing and monitoring system accesses. This would help in identifying if some user has dangerous combinations in user rights.

– Company should create a process for regularly evaluating and updating information security plan and continuity plan, e.g. on yearly basis.

5.2 Future development items

The plan is not yet final and needs to be continued even after thesis work. At the time of thesis writing, organization underwent significant structural transformation, which affected all support functions in company, including HR and ICT organizations. Roles, responsibilities and processes within organization were considerably changed, which affected performing the assessment. As the situation was seen to continue fluctuating still for future coming months but thesis needed to be finished, thesis writer and supervisor decided to freeze assessment scope to the time of October 2013, being aware that after all changes in organization will be finalized and transformation complete, the assessment needs to be adjusted and updated accordingly. However, it was seen beneficial that the structure and basic content for assessment was created already in this thesis, despite the fact that content needs to be updated quite soon.

As for the biggest development item, i.e. creating a governance organ for SAP HCM information security, thesis writer got interested in this theme and decided to continue this theme in her master's thesis. Plan is to create a common governance model for all target company HR information systems as master's degree graduation work. This would benefit organization not to only control information security matters, but to control whole maintenance concept and technology development roadmap.

References

Bedell, M., Canniff, M. & Wyrick, C. 2012. Systems Considerations in the Design of a Human Resource Information System: Planning for Implementation. In Kavanagh, M., Thite, M. & Johnson, R. (editors). Human Resource Information Systems. Basics, Applications and Future Directions. 2nd ed. Sage Publications Inc.

Data Protection Board. Tietoa rekisterinpitäjälle. Available at: http://www.tietosuoja.fi. Read: 6.1.2013.

European Union Data Protective Directive (95/46 EY)

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo. Jyväskylä.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja: ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy, Helsinki.

Ministry of Finance 2009. Effective Information Security. A Summary of General Instructions on Information Security Management. The Government Information Security Management Board (VAHTI) 5/2009. Edita Prima Plc. Helsinki.

Personal Data Act. 22.4.1999/523.

Raggad, B. G. 2010. Information Security Management. Concept and Practice. CRC Press. Boca Raton.

Ruohonen, M. 2002. Tietoturva. Docendo. Jyväskylä.

Vanto, J. 2011. Henkilötietolaki käytännössä. WSOYpro Oy. Helsinki.

Wong, Y. and Thite, M. 2012. Information Security and Privacy in Human Resource Information Systems. In Kavanagh, M., Thite, M. & Johnson, R. (editors). Human Re-

source Information Systems. Basics, Applications and Future Directions. 2nd ed. Sage Publications Inc.

Appendices

Appendix 1: Index for company information security plan

1. SYSTEM DESCRIPTION
1.1. System Name/Title
1.2. Assignment of Security Responsibility
1.3. General Description/Purpose
1.4. System Operational Status
1.5. System Environment
1.6. Telecommunication Network Arrangements
1.7. General Description of Information Sensitivity
1.8. System Interconnection/Information Sharing
2. MANAGEMENT CONTROLS
2.1. Risk Assessment and Management
2.2. Review of Security Controls
2.3. Rules of Behavior
3. OPERATIONAL CONTROLS
3.1. Personnel Security
3.2. Physical and Environmental Protection
3.3. Production Input/Output Controls
3.4. Continuity Planning
3.5. Maintenance controls
3.6. Audit Trails
4. TECHNICAL CONTROLS
4.1. Identification and Authentication
4.2. Authorization
4.3. Data Handling Controls
4.4. Availability controls
5. EVALUATION/RECOMMENDATIOS/OPEN ISSUES