Opinnäytetyö (AMK)

Tietojenkäsittely

Tietojärjestelmät

2011

Jussi Salminen

TIETOTURVAN RISKIALUEET SAP-YMPÄRISTÖSSÄ

– CASE HK Ruokatalo

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Tietojärjestelmät

Toukokuu 2011 | Sivumäärä: 43

Ohjaaja: Tuomo Helo

Tekijä: Jussi Salminen

TIETOTURVAN RISKIALUEET SAP-YMPÄRISTÖSSÄ – CASE HK RUOKATALO

SAP ERP R/3 on toiminnanohjausjärjestelmä (ERP), joka integroi yrityksen kaikki liiketoiminta-prosessit yhteen järjestelmään. ERP-järjestelmän käytöstä saatavan hyödyn lisäksi yritykset kohtaavat myös uusia riskialueita, joiden takia riskien hallinta joudutaan määrittämään uudelleen.

Opinnäytetyön tavoitteena oli kuvata SAP-ympäristön riskialueita sekä käytäntöjä, joilla mahdollisia uhkakuvia voitaisiin pienentää. Asioita tutkittiin sekä yleisen tason että HK Ruokatalon näkökulmasta. Teoriaosuudessa keskityttiin ERP-järjestelmien toimintaan yrityksen käytössä, SAP ERP:n riskialueisiin, riskihallinnan kontrolleihin, toimintatapoihin sekä standardeihin. Käytännön osiossa analysoitiin HK:n SAP ERP-ympäristön riskialueita kerättyjen teoriamateriaalien pohjalta. Osiossa esitettiin HK:n kannalta merkittävimmät riskialueet, niiden seuraukset sekä toimenpiteet, joilla riskejä voidaan pienentää.

Opinnäytetyön teoreettinen viitekehys koostui SAP ERP:n tietoturvamateriaaleista ja asiantuntijahaastattelun tuloksista. Empiirisen osuuden tutkimustulokset ja päätelmät perustuivat teoriaosuuden ja toimeksiantajan kanssa käytyjen haastatteluiden analysointiin.

Johtopäätöksissä pohdittiin SAP ERP-järjestelmän osa-alueita, joihin HK Ruokatalon kannattaa tulevaisuudessa kiinnittää huomiotaan. Pohdinnassa esitettiin myös huomioita yleisellä tasolla sekä kuvattiin ISO/IEC 27001- ja 27005-standardit, joiden avulla yritykset voivat rakentaa riskien hallintoaan.

SAP ERP:n yleisimpiä riskialueita ei voida suoraan osoittaa, sillä jokainen SAP-ratkaisu riippuu täysin asiakasyrityksen rakenteesta ja liiketoimintavaatimuksista, ja vaihtelevat näin tapauskohtaisesti. Materiaalien pohjalta voidaan kuitenkin todeta, että merkittävä osa riskeistä periytyy jo järjestelmän käyttöönoton ajalta. Suurin osa ongelmista johtuu huonosti tehdyistä määrittelyistä ja liian aikaisesta käyttöönotosta. Yritykset saattavat riittää, että kunhan vain järjestelmä toimii tuotannossa.

ASIASANAT:

ERP, SAP, riskihallinta

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Information Systems

May 2011| Total number of pages: 43

Instructor: Tuomo Helo

Author: Jussi Salminen

FIELDS OF DATA SECURITY THREATS IN SAP-ENVIROMENT – CASE HK RUOKATALO

SAP ERP R/3 is enterprise resource planning-system (ERP) which integrates all business processes to one system. In addition to the benefit what comes from the use of ERP-system, the customer companies will also face new fields of threats, which intimidate to define the risk controlling all over again.

The objective of this thesis was to describe the risk domains of SAP-enviroment in general level and in use of HK Ruokatalo and practices which reduce these risks. The theoretical part described about ERP-system's functions within the company, and the risk domains of SAP ERP's, and the controls of risk management, and the practices and standards. On the empirical part the risk domains of HK's SAP-enviroment were analysed based on the theoretical materials. The section describes the significant risk domains with the consequences and the risk reducing practices from HK Ruokatalo's point of view.

The theoretical context of the thesis consists of SAP ERP's data security materials and the results of consultant interview. The research results and conclusions of the empirical part are based on analyses of theoretical part and interviews.

On the conclusions there were deliberated the fields of SAP ERP-systems which HK Ruokatalo should be giving their focus on. On the conclusions presented also observations on the general level and described ISO/IEC 27001 and 27005 standards, which the companies can use to build up their risk management.

The common risk domains of SAP ERP's cannot be proved directly because every SAP-settlement depends completely on the customer company's structure and business requirements, and can fluctuate on case-specific. Nonetheless there can be stated based on materials that the significant part of risks are descended from the implementation. The considerable parts of problems come from badly made definitions and hasten implementation. Companies may be satisfied as long as the system is running on production

KEYWORDS:

ERP, SAP, risk management

SISÄLTÖ

1 JOHDANTO 6

2 SAP-YMPÄRISTÖN TUOMAT MUUTOKSET 8

2.1 ERP:n tuoma tehokkuus ja muutos 8

2.2 SAP-ympäristö yrityksen käytössä 9

2.3 SAP ERP tietoturvan näkökulmasta 10

2.4 SAP-ympäristön kontrollit ja turvallisuuskäytännöt 11

2.4.1 SAP-kontrollit 12

2.4.2 SAP-ympäristön turvallisuuskäytännöt 12

2.4.3 SAP-ympäristön ohjainkehys 14

3 RISKIENHALLINTA YRITYKSISSÄ 15

3.1 Riskienhallintaprosessi 16

3.2 Riskien käsittely 17

4 SAP-YMPÄRISTÖN RISKIALUEET 19

4.1 Menetyksen riskit 20

4.1.1 Syötetyn datan laadun riskit 20

4.1.2 Master Datan ylläpitoon liittyvät riskit 21

4.2 Prosessiriskit 21

4.3 Tekniset riskit 22

4.4 Juridiset ja teollisuusalan asetuksista johtuvat riskit 23

4.5 Organisatoriset riskit 25

4.5.1 Käyttäjäoikeudet 25

4.5.2 Henkilöstön toiminta 26

4.5.3 Määritykset ja vaatimukset 27

5 SAP-YMPÄRISTÖN RISKIALUEET HK-RUOKATALOSSA (SALATTU) 29

6 JOHTOPÄÄTÖKSET (SALATTU OSIN) 30

6.1 Johtopäätöksiä yleisellä tasolla 30

6.2 Johtopäätöksiä HK Ruokatalon SAP-ympäristöstä (SALATTU) 31

LÄHTEET 32

LIITTEET

Liite 1. Petri Paavolan haastattelupohja

Liite 2. Tuomo Suonkosken haastattelupohja 1

Liite 3. Tuomo Suonkosken haastattelupohja 2
Liite 4. Tuomo Suonkosken haastattelupohja 3

KUVIOT

Kuvio 1. Potentiaalisiin riskeihin vaikuttavat tekijät 10
Kuvio 2. Riskien hallinnan kulku 16
Kuvio 3. Riskien hallinnan prosessimalli 18
Kuvio 4. Riskialueiden jaottelu 19

1 JOHDANTO

Tämän opinnäytetyön tutkimuskohteina ovat HK Ruokatalon SAP-ympäristön merkittävät tietoturvariskit ja niiden mahdolliset seuraukset. Työn tavoitteena on esittää toiminnassa olevan SAP-ympäristön merkittävimpiä riskialueita sekä esittää tarkemmin 2-3 riskiä jokaiselta HK:n SAP-ympäristön riskialueelta. Mitkä ovat riskit, mitkä ovat vaikutukset niiden toteutuessa sekä miten riskien toteutuminen voitaisiin estää.

Opinnäytetyö on toteutettu toimeksiantona HK Ruokatalo Oy:lle. HK Ruokatalo on osa HKScan-konsernia ja vastaa Suomen tuotannosta ollen yksi suurimmista lihan, lihavalmisteiden, valmisruokien ja siipikarjatuotteiden toimittajista maassamme. HK Ruokatalo on myös yksi suurista yrityksistä Suomessa, jotka käyttävät liiketoiminnassaan SAP ERP-toiminnanohjausympäristöä. SAP ERP on ollut HK Ruokatalon käytössä vuodesta 1998. Aluksi käytössä oli vain SAP ERP R/3, mutta vuosien saatossa mukaan on otettu lukuisia moduuleita.

Opinnäytetyö on osa SAP Korkeakouluyhteistyötä ja SAP Tietoturva-hanketta, jota toteutetaan yhdessä HK Ruokatalon kanssa. Korkeakoulujen opetus- ja tutkimustoiminnan käytössä on myös SAP laboratorio, jossa voidaan testata useita SAP ratkaisuja ja toimintoja. Empiirisessä osuudessa ollaan hyödynnetty myös SAP laboratorion antamia mahdollisuuksia, ja testattu esimerkiksi muutamia transaktioita. Yhteistyöhankkeella saadaan suurta hyötyä niin opiskelijoille kuin HK Ruokatalolle, sillä tehtävät tutkimukset ja analysoinnit eivät vie resursseja heidän omalta henkilöstöltään, ja opiskelijat saavat samalla merkittävää kokemusta ja kontaktia työelämään.

SAP-ympäristö integroi yrityksen kaikki liiketoimintaprosessit yhteen, reaaliaikaisesti päivittyvään, järjestelmään. On äärimmäisen tärkeää, että käytössä olevan SAP-järjestelmän luottamuksellisuus, eheys ja käytettävyys ovat ja pysyvät varmistettuna, sillä pienimmätkin ongelmat näissä saattavat vaikuttaa välittömästi koko yrityksen liiketoimintaan ja tuotantoon.

Tutkimusmenetelminä käytän kirjallisuuskatsauksia sekä SAP:n tietoturva-asiantuntijan ja opinnäytetyön toimeksiantajan haastatteluja. Työn teoriapohjana käytän riskienhallinnan standardeja, SAP:n tietoturvaa käsitteleviä teoksia ja Logican SAP-tietoturvahenkilön Petri Paavolan kanssa käymääni keskustelua Hämeenlinnassa 8.2.2011. Petri Paavola tekee työkseen SAP:n tietoturvatehtäviä Logican asiakasyrityksille. Hänellä on lähes 10 vuoden työkokemus SAP:n tietoturva-alueelta, niin Puolustusvoimien kuin Logicankin palveluksessa. Empiirisessä osuudessa esitän materiaalien ja haastattelujen perusteella HK Ruokatalon kannalta merkittävimpiä riskejä SAP-ympäristössä.

2 SAP-YMPÄRISTÖN TUOMAT MUUTOKSET

2.1 ERP:n tuoma tehokkuus ja muutokset

Nykypäivän alati kehittyvässä maailmassa niin yksityishenkilöt kuin yrityksetkin voivat joutua vakavien tietoturvahyökkäysten kohteeksi. Virukset, hakkerit ja haittaohjelmistot ovat kehittyneet siinä missä turvajärjestelmätkin, ja yleensä ne ovat jopa askeleen edellä. Tästä johtuen yritysten tulisikin ottaa tietoturvallisuus vakavasti, mutta vain harvalla organisaatiolla on sisäistettynä aktiivinen turvallisuuskulttuuri. (Choi ym. 2009, 2.)

Suurilla yrityksillä on nykypäivänä oltava toimintaa tehostavia IT-järjestelmiä - kuten ERP-järjestelmä – pysyäkseen kilpailukykyisinä markkinoilla. ERP-järjestelmät (Enterprise resource planning) automatisoivat ja integroivat yrityksen suurimmat liiketoimintaprosessit samaan toiminnanohjausjärjestelmään. Tämän järjestelmän kautta informaation ja toimintojen jakaminen yrityksen sisällä on äärimmäisen helppoa reaaliaikaisessa ympäristössä. ERP-järjestelmä muuttaa yrityksen liiketoimintaprosesseja automatisoimalla tehtäviä, kuten valtuuttamalla käyttäjiä aloittamaan liiketoimintoja sekä seuraamaan niiden kulkua järjestelmässä. (ISACA 2009, 1-3.)

Ennen ERP-aikakautta yritysten järjestelmät oli usein asetettu liiketoimintojen ja osastojen ympärille. Jokaisella osastolla, kuten myynnillä, tuotannolla ja laskutuksella, oli omat erilliset järjestelmänsä. Nämä järjestelmät kehittyivät itsenäisesti erossa toisistaan ilman minkäänlaista yhteyttä. Tällaiset järjestelyt aiheuttivat esimerkiksi ajanhukkaa, ylimääräisiä kuluja ja informaation tuplautumista. Työprosessit sisälsivät suurta manuaalista käsittelyä, kun informaatiota siirrettiin osastojen välillä, joten aikaa ja voimavaroja kului paljon. (ISACA 2009, 1-3.)

ERP-järjestelmät taas ovat täysin liiketoimintalähtöisiä, ja ne keskittyvät ja rakentuvat liiketoimintaprosessien ympärille. ERP-järjestelmät syntyivät tarpeesta integroida erilliset myynti-, materiaaliresurssien suunnittelu-, ja talousjärjestelmät toisiinsa. Näiden toimintojen integraatio suunniteltiin tukemaan yritysten

liiketoimintaprosesseja ja suuntaamaan resurssinsa koko organisaation käyttöön. SAP ERP on markkinoiden suurin ja tunnetuin ERP-järjestelmä. (ISACA 2009, 1-3.)

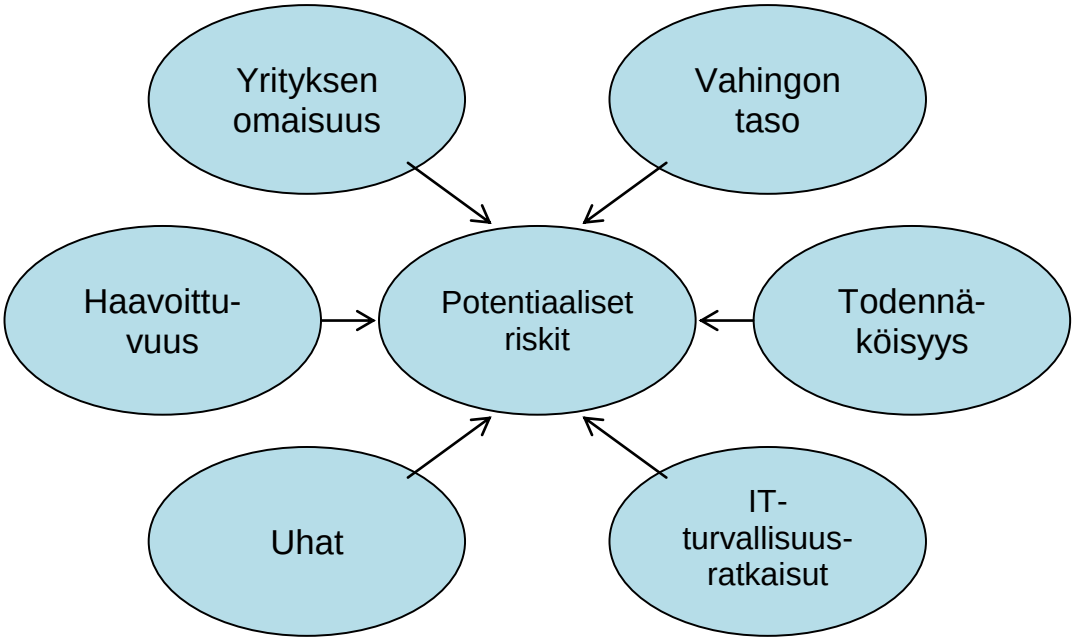
2.2 SAP-ympäristö yrityksen käytössä

Yritykset saavat ERP-järjestelmän käyttöönotosta merkittävää tehokkuutta liiketoimintaprosessien suorittamiseen. Suurimpia syitä käyttöönottoon ovat integroidut ja reaaliaikaiset finanssi- ja asiakastilausinformaatiot, tuotanto prosessien standardointi ja nopeutus, inventaarion väheneminen sekä henkilöstöinformoinnin standardointi. (Korc & Wailgum 2008.) ERP-järjestelmän tuomat tehokkuudet eivät kuitenkaan ole ainoita asioita, jotka tulevat käyttöönoton mukana.

Lisää tehokkuutta tuovien ja työskentelyä helpottavien apuvälineiden mukana tulee usein myös uusia uhkia ja mahdollisia ongelmatilanteita, eikä SAP-järjestelmä ole tässä poikkeus. SAP:n tarjoaman erinomaisen tehokkuuden mukana tulee esimerkiksi raskas ja monimutkainen IT-infrastruktuuri. Järjestelmävaatimukset SAP:lle ovat merkittävät, ja yrityksen IT-, kehitys- sekä turvallisuusarkkitehtuurit tulevat muuttumaan järjestelmän käyttöönoton yhteydessä. Yritysten IT-osastot ovat yleensä jumiutuneita vanhoihin tapoihinsa, joten taidot ja koulutukset vaativat merkittäviä päivityksiä muutosten tapahtuessa. (Choi ym. 2009, 2.)

2.3 SAP ERP tietoturvan näkökulmasta

SAP:n tietoturvassa puhutaan samoista asioista kuin tietoturvan yhteydessä yleisestikin eli luotettavuudesta, eheydestä, yksityisyydestä, jäljitettävyydestä sekä käytettävyydestä. (SAP 2011c.)



Kuvio 1. Potentiaalisiin riskeihin vaikuttavat tekijät (Karin & Linkies 2011, 40.)

Kuviossa 1 esitetään SAP-ympäristön potentiaalisiin riskeihin vaikuttavat tekijät, Riskialueet vaihtelevat yrityksen omaisuuden, haavoittuvuuksien, uhkien todennäköisyyksien, vahingon tasojen sekä IT-turvallisuusratkaisujen perusteella. (Karin & Linkies 2011, 40-41.) IT- Logican SAP-tietoturvasiantuntija Petri Paavolan mukaan SAP-järjestelmän suurimpia ja merkittävimpiä riskejä ei voida kuitenkaan suoraan sanoa tai kuvata, sillä jokaisella yrityksellä on omat IT-ratkaisut, ja niiden myötä myös omat ongelmansa sekä riskinsä. Käytössä olevat IT-järjestelmät ja niiden ylläpito on vaihtelevat yrityksittäin, ja tällöin myös haavoittuvuudet ovat yksilöllisiä. (Petri Paavola 8.2.2011, haastattelu.)

Riskianalyysien tavoite on selvittää näiden tekijöiden perusteella potentiaalisesti merkittävimmät riskit. IT-turvallisuusratkaisut, potentiaaliset riskit ja potentiaalisten riskien koko vaikuttavat kaikki toisiinsa. (Karin & Linkies, 2009, 40.)

Petri Paavolan mukaan voidaan todeta, että suurimmat riskit johtuvat ihmisistä, eivät SAP:n teknisistä ratkaisuista. (Petri Paavola 8.2.2011, haastattelu.) Tämä sama pätee yleisesti myös muihinkin IT-järjestelmiin. Ongelmia ilmenee helposti kun teknologia ja ihminen kohtaavat, vaikka IT-ympäristö olisikin turvattu parhaimmalla mahdollisella tavalla. (Walsh 2008.)

Yrityksille toimitettujen SAP-pakettien mukana tulevat kaikki tarvittavat komponentit turvallisen järjestelmäympäristön toteutukseen. Ongelmat saattavat nousta siitä, että muuhun IT-arkkitehtuuriin ei ole kiinnitetty tarpeeksi huomiota. Yksittäisenä järjestelmänä SAP ERP on toimiva ja turvallinen, mutta järjestelmä altistuu heikkouksille kun se liitetään tuotantoon, yrityksen tietoverkkoon ja muuhun IT-arkkitehtuuriin . Mahdolliset ilmenevät ongelmat johtuvat tällöin kuitenkin SAP-järjestelmän ulkopuolisten tekijöiden tietoturvatasoista, kuten tietoliikenteen suojauksista. Esimerkkinä voidaan sanoa, että SAP käsittelee kaikki käyttäjät samanlaisina kirjautumistilanteessa. Se ei tutki tarkemmin, että käyttääkö kirjautuja etäyhteyttä tai onko kirjautujalla ylipäänsä oikeuksia yrityksen verkkoon. Jos kirjautuja on päässyt yrityksen verkkoon sisään ja kirjautuu oikeilla tunnuksilla, niin pääsy on taattu. Tällaisten tilanteiden ongelmat pohjautuvat IT-arkkitehtuurin muiden osien heikkouksiin ja vuotoihin. (Petri Paavola 8.2.2011, haastattelu.)

2.4 SAP-ympäristön kontrollit ja turvallisuuskäytäntöjä

SAP-ympäristön kontrollit ja turvallisuuskäytännöt ovat apuvälineitä ja toimenpiteitä, jotka helpottavat saavuttamaan turvallisen SAP ERP-ympäristön pienentämällä mahdollisia riskejä. Tulen käyttämään kontrolleja ja turvallisuuskäytäntöjä empiirisessä osuudessa esittämään mahdollisia parannusehdotuksia HK Ruokatalon käytössä olevan SAP-ympäristön turvallisuuden parantamiseksi.

2.4.1 SAP-kontrollit

Kontrollit ovat yrityksen tietovaroja suojaavia toimenpiteitä, jotka vaihtelevat tapauskohtaisesti. Ne voivat vaihdella teknisistä toimenpiteistä valtuutustoimenpiteisiin tai hallinnollisiin prosessiratkaisuihin. (Karin & Linkies 2011, 45.)

SAP-ympäristön kontrollit voidaan jakaa neljään kategoriaan:

- Luontaiset kontrollit
- Muokattavat kontrollit
- Turvallisuuden kontrollit
- Manuaaliset kontrollit

Luontaiset kontrollit ovat järjestelmän mukana tulevia työkaluja, joita ei pystytä muokkaamaan. Näihin kontrolleihin kuuluvat dokumenttitasojen kirjaukset (aika, päivä ja käyttäjä), ohjelmistomuutosten historian tallennus ja käyttäjäprofiilien sekä roolitusten muutoshistorian tallennus. Muokattavat kontrollit ovat apuvälineitä, joita voidaan sallia, estää tai muokata konfiguraation avulla. Turvallisuuden kontrollit hallinnoivat käyttäjäpääsyjä SAP-järjestelmään. Manuaaliset kontrollit taas ovat järjestelmän ulkopuolisia apuvälineitä, joita käytetään täydentämään tai korvaamaan järjestelmässä olevia kontrolleja. (Choi ym. 2009, 328.)

2.4.2 SAP-ympäristön turvallisuuskäytännöt

Yritysten ja organisaatioiden vaatimusten takia turvallisuusmittarien, monitorien sekä prosessien kehittäminen on äärimmäisen tärkeää. IT-turvallisuuden pitäisi keskittyä tarkastelemaan kokonaiskuvaa eikä vain yhtä osa-aluetta. Keskittyminen yhteen osa-alueeseen johtaa usein vain väliaikaiseen tai rajalliseen suojaamiseen. (Karin & Linkies 2011, 60.)

SAP ERP:tä käsittelevässä materiaalissa esitetään SAP:n turvallisuusstrategian parhaimpia käytäntöjä, joita soveltamalla voidaan saavuttaa hyvät turvallisuustasot. (Karin & Linkies 2011, 60-78.) Näiden käytäntöjen tarve ilmenee vaatimuksista, jotka ovat jokaisella yrityksellä ja organisaatiolla, ja niillä avulla pyri-

tään aina keskittymään kokonaisturvallisuuden kriittisimpiin osiin. Kaikki turvallisuuden osa-alueet - teknologia, sovellustaso, prosessit, organisaation rakenne, käyttäjät, yritys ja kommunikaatiopartnerit – tulisi ottaa huomioon, tutkia riskit huomioon ottaen ja suojata huolella. Nämä voidaan saavuttaa määrittämällä yhteiset turvallisuuskäytännöt yrityksen sisälle. Ensimmäinen askel on luoda turvallisuusstrategia, johon pohjautuu kaikki käytännöt.

Parhaat käytännöt voivat koostua esimerkiksi seuraavanlaisista toimintatavoista:

- objektien ja riskienhallinnan analysointi
- strategiat
- turvallisuuskonseptit
- arvioinnit
- suunnittelut
- informaatio-omistajuuden periaatteet ja identiteettihallinto.

Karin & Linkies 2011, 77.)

Objektien analysoinnin avulla määritellään SAP-ympäristön tärkeitä kontrolleja ja yhteisiä sääntöjä. Riskienhallinnan analysointi auttaa tunnistamaan SAP-ympäristön, sovellusten, organisaation ja lakivaatimusten riskejä. Turvallisuuskonseptit auttavat ennakoimaan tulevaa ja auttavat tekemään päätöksiä. Arvioinnit pitävät sisällään turvallisuusratkaisujen analysointia, joita suorittamalla voidaan varmistaa järjestelmän käytettävyyttä. Suunnittelun avulla voidaan parantaa käytössä olevia turvallisuusratkaisuja esimerkiksi arvioinnissa esiin tulleiden asioiden perusteella. Informaatio-omistajuuden periaatteet ja identiteettihallinto pitävät sisällään muutamia käyttäjäoikeuksien ylläpitoa helpottavia komponentteja kuten SAP Profile Generatorin. Nämä ovat esimerkkejä SAP:n turvallisuusstrategian parhaimmista käytännöistä. (Karin & Linkies 2011, 60-78.)

2.4.3 SAP-ympäristön ohjainkehys

Kontrollien ja turvallisuuskäytäntöjen ohella voidaan puhua myös SAP-järjestelmän ohjainkehyksestä. Yrityksen pitää määritellä uudelleen riskienhallinnan lähestymistapansa, jotta voidaan ottaa huomioon SAP ERP-ympäristön tuomat uudet riskit. Ohjainkehyksen avulla voidaan helpottaa riskien arvioinnin ja siihen sisältyvien kontrollien toimintaa. Ohjainkehys koostuu seuraavista viidestä osa-alueesta:

- Liiketoimintaprosessi-ohjaimet, jotka sisältävät järjestelmän automatisoidut ja manuaaliset kontrollit.
- Sovellusturvallisuus, joka sisältää käyttäjähallinnan: käyttäjäprofiilien ylläpidon, turvallisuusparametrien ja käyttäjäpääsyjen myöntämisen sekä poistamisen.
- Ohjelmistorajapinta ja konversio-ohjaimet, jotka sisältävät datakonversion kontrollit
- Teknologiainfrastruktuuri, joka sisältää teknologiatasoa ympäröivät ohjaimet: serverit, käyttöjärjestelmät, tietokannat.
- Projektihallinto, joka sisältää muutoshallinnan ja projektitoiminnan.

Nämä muodostavat yhdessä kehyksen, jolla voidaan käsitellä SAP ERP:n riskienhallintaa. Jotkut ohjainkehyksen osa-alueista sisältyvät SAP-ympäristöön ja voidaan laittaa toimimaan automaattisesti, kun taas osa toimii vain manuaalisesti ja tarvitsee pohjakseen yrityksen tietoturvastrategian ja käytännöt. (ISACA 2009, 49-50.)

3 RISKIENHALLINTA YRITYKSISSÄ

Yrityksen tietoturvallisuuden ylläpitämisen tärkein osa on riskien hallinta. Sen tärkeimpänä tehtävänä on riskien ja uhkien toteutumisten mahdollisuuden pienentäminen hyväksyttävälle tasolle, sillä kokonaan uhkia harvemmin saadaan poistettua. Riskienhallintaa voisi yksinkertaisesti kuvata liiketoimintojen uhkien tunnistamisena, hallinnointina ja minimointina. (Ronald & Russell 2003, 15.) Yritykset keskittyvät liian usein vain yhteen osa-alueeseen kokonaiskuvan sijasta. Näin saavutetaan mahdollisesti onnistumista yhdellä osa-alueella, mutta saatetaan epäonnistua tietoturvallisuuden kokonaiskuvassa.

Yritystä uhkaavien riskien tunnistaminen edellyttää seuraavien kysymysten läpikäymistä:

- Mitkä ovat yrityksen todelliset uhat?
- Mitkä ovat uhkien mahdolliset seuraukset0?
- Kuinka usein uhka saattaa esiintyä?
- Kuinka vakuuttuneita voidaan olla siitä, että uhka toteutuu?

Järjestelmien jatkuvasta kehityksestä johtuen yrityksiin kohdistuvia tietoturvauhkia ilmenee jatkuvasti yhä enemmän. Järjestelmiltä odotetaan nykyään kattavaa palvelutarjontaa, niin etäyhteysmahdollisuuksien kuin ohjelmistorajapintojen piiristä, sillä toiminnanohjausjärjestelmien pitää pystyä kommunikoimaan toisten järjestelmien kanssa, jotta yhteistyö asiakkaiden tai toimittajien kanssa on tehokasta. (SFS 2009b, 14.)

Kehittyvien järjestelmien ja uhkien takia tietoturvariskien hallinnan tulisi olla jatkuva prosessi yrityksen toiminnassa. Toimintamallin tulisi sopia organisaation toimintaympäristöön ja olla linjassa yrityksen yleisen riskien hallinnan kanssa. Prosessissa tulisi määritellä arviointiympäristö, arvioida ja käsitellä riskejä, sekä toteuttaa suosituksia ja päätöksiä riskien käsittelysuunnitelman mukaisesti. (SFS 2009b, 14.)

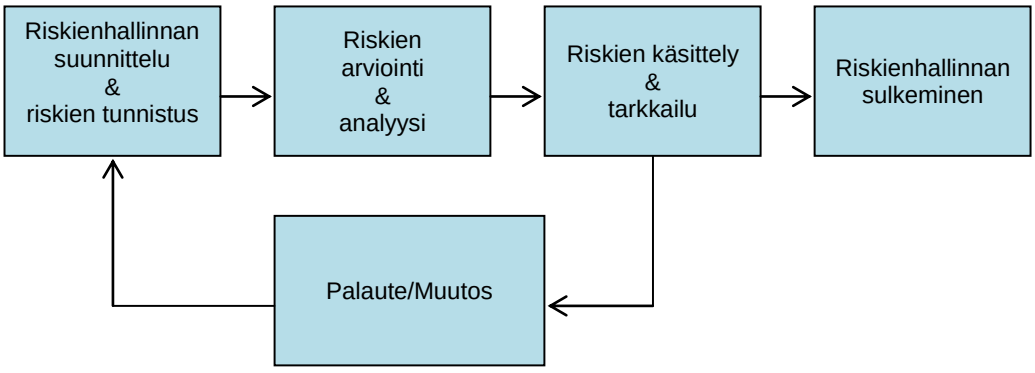
Tietoturvallisuutta vähätellään yleensä yrityksissä ja ajatellaan tulevaisuuden huolena. Se ajatellaan asiana, joka tarvitsee huomiota vain, kun tietoturva on

oikeasti uhattuna tai yrityksen hallinnon suorittaessa jokavuotista auditointia. Hyvä tietoturvataso voitaisiin saavuttaa varmistamalla, että turvallisuuslähtöinen työskentely on käytössä infrastruktuurin jokaisella osa-alueella, ja näin myös päivittäisessä työskentelyssä. Yritysten olisi hyvä sisäistää ajatusmaailmakseen fraasi: ”IT mahdollistaa liiketoiminnan, ja tietoturvallisuus mahdollistaa IT:n, joten tietoturvallisuus on perusta liiketoiminnan mahdollistamiselle.” Tämä pitäisi sisäistää äärimmäisen tarkasti myös käyttöönotettaessa SAP-ympäristöä sekä myös sen ollessa tuotannossa. (Choi ym. 2009, 2-3.)

Organisaation henkilökunnan käsitys tietoturvan ja turvavalvontamekanismien tärkeydestä on turvahallinnan osa, jota usein väheksytään. Suurin osa turvahallinnan resursseista kuluu valvontamekanismien valvontaan, riskien arviointiin ja turvallisuuden hallintaan, ja aikaa riittävään koulutukseen ei aina löydy. Ihmisten ollessa usein turvallisuuden heikoin lenkki, olisi erittäin tärkeää ylläpitää turvakoulutuksen tasoa ja varmistaa, että henkilöstö tietää tekojensa vaikutukset yrityksen tietoturvatasoon. (Ronald & Russell 2003, 25.)

3.1 Riskienhallintaprosessi

Tietoturvariskien hallintaprosessi muodostuu arviointiympäristön määrittämisestä, riskien arvioinnista, riskien käsittelystä, riskien hyväksynnästä, riskeistä viestimisestä sekä riskien tarkkailuista ja katselmoinnista. (ISO 2009b, 14.)



Kuvio 2. Riskienhallinnan kulku (Choi ym. 2009, 19.)

Kuviossa 2 kuvataan riskienhallintaprosessin vaiheet: riskienhallinnan suunnittelu, arviointi, käsittely ja tarkkailu. Riskienhallinnan suunnittelussa muodostetaan arviointiympäristö ja suunnitelmat, joiden perusteella riskejä arvioidaan, sekä tunnistetaan mahdolliset riskit. Riskien arvioinnissa määritellään mahdolliset riskitasot. Käsittelyssä ja tarkkailussa yritetään saada riskit mahdollisimman hyväksyttävälle tasolle. Nämä muodostavat riskienhallinnan normaalin kulun, johon kuuluu tarkka dokumentointi, joka askeleella. (Choi 2009, 19.)

Hallintaprosessia voidaan soveltaa koko yritykseen, johonkin erilliseen osaan (esim. yhteen osastoon, yhteen toimipaikkaan, yhteen palveluun), johonkin tietojärjestelmään, toiminnassa oleviin tai suunniteltuihin tai erityisiin valvonnan osa-alueisiin. (SFS 2009b, 14.)

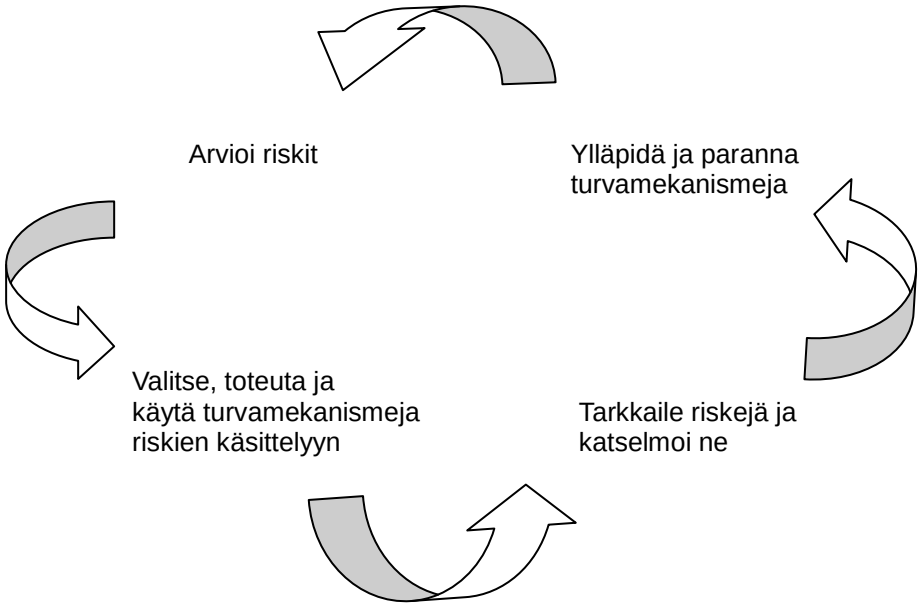
3.2 Riskien käsittely

Riskien analysoinnin tehokkuus riippuu arvioinnin tuloksista. Tehdyillä toimenpiteillä ei välttämättä saada jäljelle jäävää riskiä heti hyväksyttävälle tasolle, jolloin saattaa olla tarpeen toistaa riskiarviointi muutetussa arviointiympäristössä ja sen jälkeen tehdä uusia riskien käsittelytoimia. (SFS 2009b, 18.)

Riskin hyväksynnässä täytyy varmistaa, että yrityksen johto yksikäsitteisesti hyväksyy jäljelle jäävät riskit. Jotta hallintaprosessi olisi mahdollisimman tehokasta, tulisi koko hallintaprosessin ajan viestiä riskeistä ja niiden käsittelystä asianosaisille johtajille ja henkilöstölle. Jo tiedot tunnistetuista riskeistä voivat olla äärimmäisen arvokkaita, koska niiden avulla voidaan hallinnoida häiriöitä ja auttaa pienentämään mahdollisia vahinkoja. (SFS 2009b, 18.)

ISO/IEC 27001-standardin mukaan tietoturvallisuuden hallintajärjestelmän kattavuuden, rajojen ja arviointiympäristön puitteissa toteutettujen turvamekanismien tulisi perustua riskien arviointiin. Tämä vaatimus voidaan toteuttaa tietoturvariskien hallintaprosessilla, joka voidaan toteuttaa onnistuneesti monien eri toimintamallien mukaisesti. Organisaation tulisi valita

toimintamalli, joka parhaiten sopii organisaation olosuhteisiin kussakin prosessin vaiheessa. (SFS 2009a, 16.)



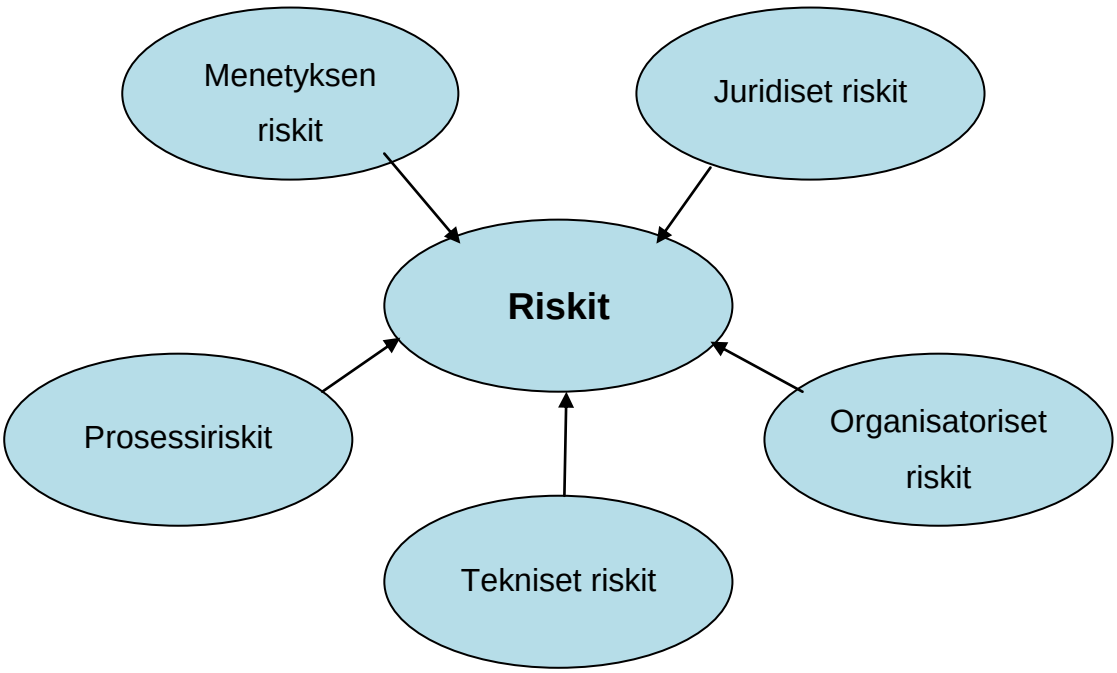
Kuvio 3. Riskien hallinnan prosessimalli (SFS 2009a, 6.)

ISO/IEC 27001-standardissa esitettävä kuvio 3 havainnollistaa hyvin riskien hallintaprosessin jatkuvaa toimintaa. Tavoitteena on yrityksen liiketoiminnan tehokkuuden ja vaikuttavuuden jatkuva seuranta sekä parantaminen. (SFS 2009a, 6.)

4 SAP-YMPÄRISTÖN RISKIALUEITA

SAP ERP-järjestelmän käytöstä saavutetaan merkittäviä hyötyjä yritykselle, mutta sen mukana ilmaantuu uusia riskejä ja yrityksen riskiprofiili muuttuu huomattavasti. Tästä johtuen kontrolloidun ympäristön merkitys tulee tärkeäksi turvallisuuden takaamiseksi. (ISACA 2009, 38)

Suurimpia ja merkittävimpiä SAP-ympäristöön kohdistuvia riskejä on suoralta kädeltä erittäin vaikea sanoa, sillä yritykseen kohdistuvat uhat ovat aina tapauskohtaisia. Kokemusten pohjalta voidaan kuitenkin esittää riskialueita, joissa useimmiten ongelmia esiintyy. Miltei kaikki SAP-ympäristössä esiintyvät ongelmat periytyvät jo käyttöönottovaiheesta, jolloin prosessoinnit, määrittelyt ja roolitukset on suunniteltu, toteutettu ja testattu usein kovan kiireen vuoksi liian vähällä huomiolla. (Petri Paavola 8.2.2011, haastattelu.)



Kuvio 4. Riskialueiden jaottelu (Karin & Linkies 2011, 44.)

Riskianalyysin keskittyessä enimmäkseen dataan, IT-järjestelmiin, prosesseihin ja työntekijöihin, ovat riskit yleisesti jaettu kuvion 4 mukaisiin luokkiin. Käytän työssäni tätä luokitusta riskialueiden rajauksessa. (Karin & Linkies 2011, 41-43.)

4.1 Menetyksen riskit

Menetyksen riskit ovat uhkakuvia, joiden seuraukset johtavat yrityksen omaisuuden menetykseen. Tärkeiden tietojen hukkuminen, datan muuttuminen tai vahingoittuminen sekä irtaimiston häviäminen ovat yleisiä esimerkkejä näistä riskeistä. Yrityksen omaisuuteen kuuluu erittäin tärkeänä osana yrityksen tietovarat, joihin keskitytäänkin puhuttaessa SAP ERP:stä. (Karin & Linkies 2011, 41.)

Riskien toteutumiset voivat johtaa korjautumattomiin menetyksiin, kuten äärimmäisen kalliisiin toimenpiteisiin tai yrityksen maineen menetykseen. Pahimmassa tapauksessa seurauksena voi olla jopa yrityksen kaatuminen, ja tämän takia riskienhallinnan yhtenä pääpainona onkin välttää menetystä. (Karin & Linkies 2011, 41)

4.1.1 Syötetyn datan laadun riskit

Datan yhtenäisyys SAP-järjestelmässä on äärimäisen tärkeää, koska toiminnanohjausjärjestelmien sydämenä on usein yksi keskitetty tietokanta. Muista järjestelmistä syötetty data saattaa olla epätarkkaa, keskeneräistä tai kaksinkertaista, joka voi aiheuttaa toiminnallisia ongelmia automatisoidummassa ja integroidummassa ympäristössä. Ulkopuolisten osapuolten päästessä käsiksi esimerkiksi yrityksen laskutus- sekä rahoitusinformaatioon Internetin kautta, datan laadun ja yhtenäisyyden merkitys kasvaa huomattavasti. (ISACA 2009, 47.)

Esimerkkinä voitaisiin esittää teollisuusyrityksen toimittajarekisterin kääntämistä SAP-järjestelmään. Kyseinen rekisteri voi sisältää vanhentuneita faksitietoja, jotka pitäisi siirron yhteydessä tarkistaa. Ilman tietojen tarkistusta tämä voi johtaa myöhemmin väärin kohdistettuihin ja hukattuihin fakseihin. Sama ongelma voi tulla esimerkiksi tilauksissa virheellisten asiakastietojen tai laskutustietojen kanssa. (ISACA 2009, 47.)

4.1.2 Ylläpitoon liittyvät riskit

Master Data on perustietoa, joka on pohja kaikille yrityksen liiketoimintaoperaatioille. Sisältää esimerkiksi dataa asiakkaista, tuotteista, työntekijöistä, materiaaleista ja toimittajista. Master Data vaikuttaa dokumenttien ja transaktioiden tehokkaaseen liikkumiseen järjestelmän läpi, ja täten voi myös vaikuttaa yrityksen moniin liiketoimintaprosesseihin, kuten kirjanpitoon, myyntiin, ostoon ja toimituksiin. Tästä johtuen Master Datan ylläpitoon ja laadun varmistamiseen liittyvät riskit ovatkin osa merkittävimpiä uhkia yrityksessä. Master Datan syötön tai muutoksen ollessa virheellistä, keskeneräistä, epätarkkaa tai väärinajoitettua vaikutukset voivat olla merkittäviä. (ISACA 2009, 98-151.)

4.2 Prosessiriskit

Prosessiriskit ovat seurauksia toiminnoista, jotka häiritsevät sisäisiä liiketoimintaprosesseja, ulkoisia liiketoimintatransaktioita sekä kommunikaatiota. Prosessien etenemisen heikentyminen voi johtaa suuriin rahallisiin menetyksiin tuotannon katkeillessa. SAP ERP on rakennettu toimimaan liiketoimintaprosessien ehdoilla, joten turvallisuus, käytettävyys ja toimivuus tulisi olla suunniteltu äärimmäisen tarkkaan. Pahimmillaan toteutuvat riskit voivat johtaa yhteistyökumppanien menetyksiin tai keskeytyneeseen tuotantoon. (Karin & Linkies 2011, 42.)

Prosessidokumentoinnin puuttuminen on yleensä pohjimmainen syy prosessien keskeytymisille tai vajavaisille prosessisuunnitteluille. Prosessidokumentteihin ja –suunnitteluun sisältyy osaltaan myös käyttäjävaltuuksien suunnittelu, jotta liiallisia oikeuksia ei jaettaisi. (Karin & Linkies 2011, 42.)

Petri Paavolan mukaan huonosti tehdyt ja suunnitellut prosessit ovat yleisin ongelma yritysten SAP-ratkaisuissa. Huonosti tehty prosessi menee helposti läpi tuotannossa, ja vaikutukset voivat näkyä vasta pitkä ajan päästä. Suurimmat ongelmat voidaan poistaa jo alkuvaiheessa kunnollisella analysoinnilla, testauksella ja ”Mitä jos jotain tapahtuu?”-ajatusmaailmalla. Liian usein ajatellaan, että riittää kunhan prosessit pyörivät tuotannossa. Prosessit pitäisi olla määritelty ja

testattu mahdollisimman aikaisessa vaiheessa. (Petri Paavola 8.2.2011, haastattelu.)

Prosessien riskialueita ovat:

- myyntitilausten prosessointi
- lähetysten, laskutusten, tuotepalautusten ja säädösten seuranta
- maksukuittausten keräys ja prosessointi
- hankinta
- tuotannon kulujen prosessointi
- tuotannon ja kustannusten prosessointi
- raakamateriaalien hallinnointi
- lopputuotteiden käsittely ja lähetys.

Merkittävimpiä riskejä ovat prosessointi väärillä, vaillinaisilla, epätarkoilla tai väärinajoitetuilla tiedoilla. Seuraukset riippuvat prosessien alueista, mutta johtavat yleisesti prosessin epäonnistumiseen ja menetyksiin. (ISACA 2009, 98-151.)

4.3 Tekniset riskit

SAP-ympäristön suurimmat huolenaiheet koskevat enemmänkin organisaatiota kuin teknisiä asioita. Teknisten riskien toteutuminen on yleensä oire yrityksen yleisen IT-arkkitehtuurin haavoittuvuudesta. Seurauksina voivat olla ongelmat datan varastoinnissa ja prosessien jatkuvuuksissa, jotka johtavat informaation häviämiseen. (Karin & Linkies 2009, 42; Petri Paavola 8.2.2011, haastattelu.)

SAP ERP katsotaan yleisesti yksinään pakettina, joka on täysin toimiva ja turvallinen annetuilla ohjeistuksilla ja säädöksillä. Tekniset asiat SAP:n näkökulmasta ovat täysin kunnossa ja turvattuja. Ongelmia ja uhkia voi tosin ilmetä heti kun SAP-ympäristö aloittaa toiminnan ulkopuolisen järjestelmän kanssa. (Petri Paavola 8.2.2011, haastattelu.)

Yrityksillä voi olla myös vaatimuksia tai tarpeita, jotka eivät toteudu yrityssovelluksilla ja SAP-ympäristössä eivätkä esimerkiksi tarvittavat informaatiosiirrot toimittajille tai asiakkaille onnistu. Tästä syystä

ohjelmistorajapinnat ovat vakiintuneet transaktioinformaatioiden siirroissa järjestelmien välillä. (ISACA 2009, 48.)

Ohjelmistorajapinnat tuovat mukanaan riskejä informaation eheydelle sekä tarkkuudelle. Jos rajapintoja ei ole kontrolloitu tehokkaasti, on mahdollisina uhkina epätarkan, puutteellisen, luvattoman tai huonosti ajoitetun informaation pääsy SAP-järjestelmään tai sieltä ulos. Ohjelmistorajapintojen ajoitus voi usein olla äärimmäisen merkittävää, varsinkin jos käytössä on lukuisia ohjelmistorajapintoja, jotka pitää suorittaa lyhyen prosessointijakson aikana. (ISACA 2009, 48.)

Muutosten tekeminen järjestelmän toimintaan on myös suuri riskitekijä, sillä SAP ERP on luvattu toimivan turvallisesti alkuperäisten asetusten ja ohjeiden kanssa. Esimerkiksi ABAP/4-datahakemistoon tehtävillä muutoksilla voi olla merkittäviä seurauksia koko järjestelmässä, sillä vaikutus voi helposti levitä enemmän kuin yhteen clientiin. (ISACA 2009, 183-184.)

Hyväksi käytäntönä onkin varmistaa, että mikään muutos ei pääse tuotantoympäristöön ilman kunnollista testausta, sillä virheitä löytyy melko varmasti aina ensimmäisellä kerralla. Esimerkiksi testaamattomien muokattujen transaktiokoodien avulla saatettaisiin testiympäristössä päästä aktiviteetteihin, joihin peruskäyttäjillä ei normaalisi olisi valtuuksia. (ISACA 2009, 178.)

Teknisesti SAP:ssa ei ole suuria vikoja ja uhkatekijöitä, ja toimitetussa paketissa on kaikki työkalut turvallisuuden varmistamiseksi. Järjestelmän kytkeminen muuhun IT-arkkitehtuuriin ja mahdolliset koodimuutokset voivat altistaa ongelmille. Nämä mahdolliset ongelmat taas riippuvat täysin muun IT-arkkitehtuurin tietoturvatasosta eikä niinkään SAP:n ongelmista. (Petri Paavola 8.2.2011, haastattelu.)

Tekniset ongelmat johtuvat pikemminkin esimerkiksi siitä, että tietoliikenneverkkoa ei ole asianmukaisesti suojattu. Esimerkiksi SAP:lle käyttäjä on aina käyttäjä. Se ei erottele etäyhteydellisiä käyttäjiä työasemakäyttäjistä, joten oikeuttomat pääsyt johtuvat enemminkin suojaamattomista etäyhteyksistä sekä väärin

määritellyistä roolituksista kuin SAP ERP:n turvaheikkouksista. (Petri Paavola 8.2.2011, haastattelu.)

4.4 Juridiset ja teollisuusalan asetuksista johtuvat riskit

Juridisiin ja teollisuusalojen asetuksista johtuviin riskeihin kuuluvat lähinnä ongelmat, jotka aiheutuvat yrityksen toimiessa niiden vastaisesti. Yrityksen tietyt toiminnat voivat johtaa suuriin kustannuksiin ja seuraamuksiin yritysjohdossa. (Karin & Linkies 2011, 42-43.)

Asiantuntija Petri Paavolan mukaan SAP ERP tukee useiden maiden ja teollisuusalojen lainsäädäntöä ja asetuksia, joten suurta riskitekijää tällä alueella ei pitäisi olla. SAP ERP perustuu pääosin omiin standardeihinsa, mutta ne ovat äärimmäisen lähellä ja toimintakykyisiä yleisesti käytössä olevien standardien kanssa. Tämä johtuu pääosin siitä, että suurin osa nykyisin käytössä olevista standardeista ei ollut vielä olemassakaan, kun aloitettiin SAP ERP:n kehittely. (Petri Paavola 8.2.2011, haastattelu.)

Mahdollisia ongelmia voi kuitenkin esiintyä, jos yritys toimii oman maansa rajojen ulkopuolella, eikä ole täysin tietoinen toisen maan lakikäytännöistä ja asetuksista. Se mikä toisessa on sallittua voi toisessa olla laitonta. Esimerkiksi USA:ssa työntekijöiden sähköpostien sisällön kontrollointi on sallittua, kun taas Euroopassa ei. (Walsh 2008.)

Tulevina vuosina juridiset ja teollisuusalojen omat asetukset voivat tulla myös tiukentumaan. Syitä ovat esimerkiksi.:

- finanssimaailman kriisit
- tietoturvallisuuden ja finanssiraportoinnin muutokset
- kansalliset ja kansainväliset konkurssit

(Karin & Linkies 2011, 42-43.)

4.5 Organisatoriset riskit

Kuten aiemmin jo todettiin, niin suurimmat SAP-ympäristön huolenaiheet koskevat organisaatiota ja inhimillisiä tekijöitä enemmän kuin teknisiä asioita. Yhdeksi suurimmista riskien aiheuttajaksi voidaankin nimetä organisatoriset riskit. Nämä ovat myös äärimmäisen tärkeitä määriteltäessä kokonaisriskiä, sillä ne vaikuttavat suoraan työntekijöihin, yhteistyökumppaneihin ja IT-sovellusten käyttäjiin. (Karin & Linkies 2011, 42; Petri Paavola 8.2.2011, haastattelu.)

Organisatorisiin riskeihin kuuluvat esimerkiksi SAP-sovellusten virheellinen käyttö inhimillisten virheiden takia, roolitusten virheellinen valtuutus, auktorisointikomponenttien virheellinen ylläpito ja määritykselliset ongelmat. (Karin & Linkies 2011, 42.)

4.5.1 Käyttäjäoikeudet

SAP-järjestelmän suurimpia hyötyjä yritykselle on saada kaikki liiketoimintaprosessit integroitua yhteen, reaaliajassa toimivaan järjestelmään. Tämä kuitenkin tuo käyttäjien hallinnointiin uusia potentiaalisia uhkia ja merkittäviä vaatimuksia. Yrityksen tuodessa tuotantoon liiketoimintaprosesseja yhteen integroivan sovelluksen, käyttäjien tarvitsee mahdollisesti päästä käsiksi ylimääräisiin tietoihin ja prosessifunktioihin. (ISACA 2009, 46.)

ERP-järjestelmät ovat suunniteltu sallimaan langattomia tai etäältä tapahtuvia pääsyjä sekä kenttä- ja myyntihenkilöstön että asiakkaiden ja toimittajien toimesta. Tämän tasoinen pääsy myyntipisteistä suoraan järjestelmään auttaa osaltaan pitämään järjestelmää ajan tasalla. Toisaalta kasvava etäpääsy voi luoda ympäristön, jossa järjestelmä on alttiimpi hakkeroinnille tai muulle pahantahtoiselle peukaloinnille. Etätyöskentelyn mahdollisuus kasvattaa myös väärän tiedon pääsyn todennäköisyyttä järjestelmään esimerkiksi myyjien toimesta kiireisessä myyntipisteessä. (ISACA 2009, 46.)

Käyttäjien tunnistaminen on yksi syy miksi SAP:n lukuisien turvallisuusparametrien asettelut tulevat tarpeeseen. Käytössä on salasanoja, tunkeutujan sulkuja

ja superkäyttäjän sallimista, jotka asianmukaisesti asetettuna palvelevat järjestelmän suojaamisessa. Asianmukainen käyttäjätunnistusten suunnittelu tietoturvapolitiikan ja työroolien pohjalta on järjestelmän eheyden kannalta merkittävää. Eräitä tärkeitä huomioon otettavia tekijöitä ovat roolien erottelu sekä henkilöstön pääsyn salliminen vain niihin transaktioihin, joita he tarvitsevat työtehtävissään. (ISACA 2009, 46.)

Käyttäjien oikeudet muodostuvat käyttäjäprofiileille annetuista rooleista. Rooleille liitetään oikeuksia ja transaktioita, jotka profiileissa yhdistettyinä muodostavat käyttäjille heidän oikeutensa. Suurimpia ongelmia roolituksissa, profiileissa ja auktorisoinnissa ovat vaillinainen määrittely ja ylläpito. Roolituksien tuomia auktorisointeja ei mietitä tarpeeksi kattavasti, ja näin liiallisia oikeuksia voi tulla hyvinkin helposti. (Petri Paavola 8.2.2011, haastattelu.)

SAP:ssa roolit rakentuvat niin, että roolille sallitaan tietyt oikeudet ja pääsyt. Roolituksissa ei käytetä teknisesti oikeuksien estoa, vaan tarvittavat oikeudet sallitaan tapauskohtaisesti. Tämä voikin tuoda ongelmia annettaessa käyttäjäoikeuksia, joita ei ole asianmukaisesti määritelty. Profiilit ovat roolien unioneita, joissa voimakkaammat auktorisoinnit voittavat. Toinen roolitus voikin hyväksyä jotain mitä toisessa roolissa ei ole haluttu antaa. (Petri Paavola 8.2.2011, haastattelu.)

Roolitusten ylläpito, suunnittelu ja testaus ovatkin tärkeää yrityksen tietoturvan kannalta, ja se pitää toteuttaa kunnolla käyttöönotosta lähtien. Yrityksissä pitäisi olla henkilö, joka ymmärtää roolituksista kokonaisvaltaisen kuvan. Mihin roolit on kohdennettu ja miten rakennettu? Ovatko toiminnallisuudet hyviä? Liian usein yrityksissä ei kuitenkaan kiireiden tai kustannusten takia panosteta riittävästi suunnitteluun. (Petri Paavola 8.2.2011, haastattelu.)

4.5.2 Henkilöstön toiminta

Yrityksen johdon aktiivisen osallistumisen puuttuminen on asia, joka johtaa useimmiten ongelmallisiin tilanteisiin. Projektityöryhmä ja käyttäjät voivat turhautua, jos projektit eivät johdon tuen puuttumisen takia etene. Lopulta

vaikuttavia muutoksia ei välttämättä saada edes toteutettua loppuun asti. Johdon suunnatessa yrityksen resursseja toisiin tarpeisiin, voi projekti jäädä jäihin pitkäksikin aikaan tuottavuuden samalla kärsien. (ISACA 2009, 40.)

Selkeän projektijohdon puuttuminen voi johtaa myös liiketoimintaosastojen ja IT:n välille syntyviin konflikteihin, ja vaikuttavaa lopputulosta ei saavuteta. Asianmukaisen resursoinnin puuttuminen johtaa varmasti siihen, että koko käyttöönotto- tai muutosprojekti menettää merkityksensä. (ICASA 2009, 40.)

Resursseja pitäisi jakaa asiankuuluvat määrät myös prosessien sekä käyttäjähallinnan ylläpidon hoitoon. Liian usein yrityksissä ei ole panostettu resursoimaan näihin tehtäviin henkilöitä, joilla olisi tarvittavan kokonaisvaltaista kuvaa liiketoimintaprosesseista. Tämä johtaakin usein liian vaillinaisiin roolituksiin tai prosesseihin, jolloin ne eivät täytä välttämättä yrityksen liiketoimintavaatimuksia. (Petri Paavola 8.2.2011, haastattelu.)

Yrityksen johdon tuki tarvitaan myös yleisen tietoturvakulttuurin ajamiseen yrityksen sisällä. Tähän päästään erilaisten ryhti-kampanjoiden muodossa. Hyvä käytäntö on tehdä tietoturvasta koko yrityksen asia, ja vähentää näin työntekijöiden mielikuvaa, että se olisi vain johdon työkalu työskentelyn seuraamiseen. (Petri Paavola 8.2.2011, haastattelu.)

4.5.3 Vaatimukset ja määritykset

Yritys voi ajautua leikatessaan liikaa resursseja tai ottaessa muutoksia liian aikaisessa vaiheessa käyttöön tilanteeseen, jossa järjestelmän yksityiskohtia tutkiessa tai pahimmillaan jo tuotannossa ollessa huomataan, että SAP-ratkaisu ei pysty käsittelemään suurimpia osia heidän liiketoimintaprosesseistaan. Suurimpia syitä tähän ovat, että yritys on ollut liian riippuvainen konsulteistaan, ja ei ole välttämättä ohjannut määritys- ja suunnitteluprojektia asianmukaisella tarkkuudella. Nämä voivat johtaa siihen, että suunnittelun kaikkiin osa-alueisiin ei ole panostettu tarpeeksi. (ISACA 2009, 43.)

Järjestelmätoimittajat voivat esittää järjestelmäratkaisunsa tai

muutosehdotuksensa täyttävän liiketoimintavaatimukset. Vaatimuksia ei kuitenkaan ole välttämättä asianmukaisesti määritelty tai tehokkaasti yksityiskohtaistettu. Järjestelmän ja liiketoimintaprosessien tarpeiden välillä olevien ristiriitojen seuraukset voivat tulla yrityksille erittäin kalliiksi, riippumatta siitä mikä väärinymmärrykseen on alun perin johtanut. (ISACA 2009, 43.)

5 SAP-YMPÄRISTÖN MERKITTÄVIMMÄT RISKIALUEET HK RUOKATALOSSA (SALATTU)

6 JOHTOPÄÄTÖKSET (SALATTU OSIN)

6.1 Johtopäätöksiä yleisellä tasolla

Ensimmäisiä havaintoja, joita tein työni alkutaipaleella oli se, että SAP ERP:n merkittävimpiä ja selkeimpiä riskialueita ei voida yleisellä tasolla suoraan osoittaa. Tähän tosiasiaan olen työni aikana päätynyt useampaan otteeseen. SAP ERP-järjestelmä – kuten kaikki toiminnanohjausjärjestelmät – on monimutkaisen arkkitehtuurin päälle rakennettu liiketoimintaohjelmisto. Kaikki liiketoimintaprosessit on integroitu yhteen suureen kokonaisuuteen, jossa yksikin pieni ongelma voi pahimmassa tapauksessa lamauttaa koko tuotannon. Rakennettuja SAP-ratkaisuja on yhtä monta kuin on SAP:n asiakasyritystäkin. Jokaisella yrityksellä on omat ympäristönsä ja IT-arkkitehtuurinsa, jotka ovat suunniteltu ja määritelty yrityksen rakenteen, liiketoimintaprosessien ja –vaatimusten perusteella.

Materiaalien, tekemieni haastatteluiden sekä analyysien perusteella voin kuitenkin todeta, että SAP ERP-ympäristön merkittävimmät riskit periytyvät yleisimmin jo käyttöönottovaiheesta asti, ja pohjautuvat usein inhimillisiin tekijöihin. Yritykset pyrkivät liian usein saamaan järjestelmiään tai tehtyjä muutoksia mahdollisimman nopeasti tuotantoon, jolloin tärkeät määrittelyt ja testaukset jäävät taka-alalle. Määrityksiin ja ylläpitoon ei resursoida, joka voi nopeasti johtaa myös siihen, että prosessit eivät täytä muuttuneita liiketoimintavaatimuksia. Yrityksille riittää liian usein tuotannossa pyörivä liiketoimintajärjestelmä, vaikka useita pieniä ongelmia mahdollisesti kuplii pinnan alla.

Yrityksille peruspakettina toimitettava SAP ERP R/3 vakuutetaan SAP:n puolelta olevan turvallinen työympäristö, jos annettuja ohjeistuksia ja määrityksiä noudatetaan. Näin asia myös sinänsä onkin. Tosiasia kuitenkin on, että yksikin SAP-ympäristöön tehtävä muutos voi muuttaa tilanteen toiseksi. Nämä ovat kuitenkin asioita, joita ei voida liiketoimintajärjestelmän kanssa välttää. SAP-ympäristön on pakko toimia tiettyjen ulkoisten järjestelmien tai verkkojen kans-

sa, ja sen alkuperäisiin asetuksiin on tehtävä muutoksia, jotta ympäristö palvelisi parhaiten yrityksen omia tarkkoja liiketoimintavaatimuksia.

Petri Paavolan kanssa käymäni haastattelun ja tutkimieni materiaalien pohjalta voin myös todeta, että yleisimmät SAP-ympäristön tietoturvatehtävät ovat erilaisten raporttien ajamista ja analysointia. SAP-ympäristön turvallisuudesta vastaavat henkilöt seuraavat lukusia raportteja, joilla monitoroidaan esimerkiksi miten järjestelmä toimii, miten data liikkuu, mitä muutoksia on tehtyä ja kenen toimesta. (Petri Paavola 8.2.2011, haastattelu.)

6.2 Johtopäätöksiä HK Ruokatalon SAP-ympäristöstä (SALATTU)

LÄHTEET

Calder, A. & Walkins, S. 2008. IT Governance – A Manager's Guide to Data Security and ISO27001/ISO27002. 4th edition. London: Kogan Page.

Choi, M.; Cox, P.; Hirao, J.; Hirao, J.; Passer, S.L. & Wun-Young, L. 2009.SAP Security Configuration and Deploment – The It Administrator's Guide to Best Practices. Burlington: Syngress Publishing, Inc.

HK Ruokatalo Oy 2010. Viitattu 20.11.2010 http://www.hkscan.com/

ISACA Serving IT Governance Professionals. 2009. Technical and Risk Management Reference Series Security, Audit and Control Features SAP ERP 3rd Edition. Rolling Meadows:ISACA.

Karin, H. & Linkies, M. 2011. SAP Security and Risk Management. 2nd edition. Boston: Galileo Press.

Korc, C. & Wailgum, T. 2008. ERP Definition and Solutions. Viitattu 19.4.2011 http://www.cio.com/article/40323/ERP_Definition_and_Solutions?page=1&taxonomyId=3009

Ronald, L & Russell, D. 2003. Tietoturva sertifikaatti – CISSP. The CISSP Prep Guide – Mastering the Ten Domains of Computer Security. Suom. Suominen, E. Edita: Helsinki.

SAP 2011a. Components & tools of SAP Netweaver – SAP Netweaver Business Process Management. Viitattu 13.5.2011.
http://www.sap.com/platform/netweaver/components/sapnetweaverbpm/index.epx

SAP2011. SAP Korkeakouluyhteistyö Suomessa. Viitattu 25.5.2011. http://www.sap-unialliance.fi/index.php?option=com_content&view=article&id=64&Itemid=43&lang=fi

SAP 2011b. SAP Related documents and articles by topic. Viitattu 13.5.2011.
http://www.sdn.sap.com/irj/scn/articles-topic

SAP 2011c. Security and Identity Management. Viitattu 23.4.2011
http://www.sdn.sap.com/irj/sdn/security > Compliance

SFS 2009a. SFS-ISO/IEC 27001 – standardi.

SFS 2009b. SFS-ISO/IEC 27005 – standardi

Walsh, K. 2008. The ERP Security Challenge. Viitattu 13.5.2011. http://www.csoonline.com/article/216940/the-erp-security-challenge

Logican SAP-tietoturvasiantuntijan haastattelu Hämeenlinnassa 8.2.2011

Haastattelijat: Jussi Salminen & Janne Pekkanen

Haastateltava: Petri Paavola - Logica

Merkittävistä uhkista yleisesti:

- Mitkä Logica näkisi olevan merkittävimpiä tietoturvariskejä käytössä olevassa SAP-ympäristössä? ”Jokapäiväisessä käytössä”
- Miten SAP:n tietoturvaa käytännössä toteutetaan ja valvotaan?
- Eteen on tullut, että SAP käyttää erilaisia tietoturvaparametreja (salasanapituuden, jne.), kun taas toiset ERP-järjestelmät käyttävät erillisesti asennettavia tietoturvapaketteja. Käyttöönotettaessa ja käytössä ollessa, onko SAP-yleistietoturvallisessa kunnossa vai pitääkö sitä hioa tapauskohtaisesti huimasti? Esim. pitääkö rajapintoja ulkoisten ohjelmien kanssa säädellä erikseen? Vai onko toimitettava paketti ns. ”kunnossa”?
- Materiaaleissa painotetaan, että yritysten pitäisi nykyisin sisäistää tietoturva-kulttuuria kattavasti ja tehokkaasti koko yrityksen sisällä, jotta tietoturva pysyisi parhaalla mahdollisella tasolla. Työntekijöitä kouluttaa ja pitää tietoisena vastuistaan, johto sitouttaa tietoturvapolitiikkaan, jne. Vaikuttaako yrityksen tietoturvapolitiikan taso SAP-ympäristöä käyttöönotettaessa ja käytössäkin ollessaan järjestelmän turvallisuuden lopulliseen tasoon?

Käyttäjät/roolitukset/etätyöskentely:

- Käyttäjille jaetaan työkuvan mukaisesti tarvittavat roolit ja profiilit SAP:n, jotta käytössä on vain tarvittavat toiminnot ja moduulit. Profiilien ja roolien turvallisuuteen ja oikeuksiin vaikuttavat tietenkin niitä ylläpitävät tahot, sekä profiilien/roolien määrittelyjen tarkkuus ja perusteet. Mitkä ovat merkittävimpiä uhkia käyttäjien/tunnusten puolelta? Onko merkittäviä uhkia vaikka profiilit olisivatkin asianmukaisesti rajattu? Esim. etätyöskentely tarpeet tuovat ainakin osaltaan uhkia, jne.

Sap-tietoturvatyökalujen kartoittaminen ja arviointi:

- SAP:n omat tietoturva työkalut (ohjelmistot, transaktiot), mitkä ovat tärkeimpiä? Mitä ohjelmia käytännössä käytetään?
- Käytetäänkö joitakin kolmannen osapuolen ohjelmia, jos niin mitä? Kuinka tärkeitä ne ovat? Pärjääkö SAP:n omilla työkaluilla?
- Voiko suositella jotakin hyvää kirjallisuutta tai sivustoja?
- Miten suojaudutaan ulkoisilta uhilta? Kuinka SAP on suojattu ulkoisia uhkia vastaan? Pitäisikö siihen kiinnittää enemmän huomiota? Miten suojaudutaan sisäisiltä uhilta? Painottuuko tietoturva enemmän sisäisten vai ulkoisten uhkien torjuntaan?
- Kuinka yleisiä ovat tietomurrot?

Empiirisen osuuden aloitushaastattelu 30.3.2011

Paikka: HK Ruokatalo Turku

Osallistujat: Jussi Salminen & Tuomo Suonkoski

Aiheena: Empirian aloitus, ensimmäisten riskialueiden kartoittaminen, tulevat tapaamiset.

Kysymykset ovat läpikäytäviä aihealueita, ja niitä käytetään keskustelun runkona.

MENETYKSEN RISKIT

1. Onko HK:n asiakas- tai yhteistyökumppaneilla mahdollisuus syöttää dataa HK:n SAP-järjestelmään? Ja tuleeko järjestelmään muutenkin ulkopuolelta/muista järjestelmistä paljon materiaalia/syötettä? Onko dataa esim. e-palveluissa, jollain tapaa lukittu vain luku-mahdollisuuteen?

    - Esim. Onko mahdollisuus syöttää WWW-sovelluksista tai muuten ylipäätään syöttää tilauksia SAP:hen (tai ylipäänsä mitään tietoa.)

2. Vastaako Master Datan luomisesta ja ylläpidosta tietyt henkilöt/tiimi?

    - Onko nämä valtuutettu oikein? Muutos oikeudet pitäisi rajata henkilöille, jotka ymmärtävät niiden muutoksista johtuvat seuraukset.
    - Näiden oikeutusten käsitteleminen tosin kuuluu myös roolituksiin, joita käsitellään myöhemmin, mutta niillä voi olla suora merkitys Master datan eheyteen.

3. Onko Master Datan ylläpidon vastuut jaettu erikseen osa-alueisiin esim. materiaalihallinnolla omansa, jne.?

    - Tehokkain kontrolli on yleisesti rajata oikeudet henkilöille, joilla on käsitys kyseisen moduulin toiminnasta ja muutosten seurauksista.
    - Esim. jos varastoinnin master datat eivät pysy ajan tasalla tai asianmukaisena voi seurauksena olla moninkertaisia tuotetietoja aiheuttamassa sekaannuksia

4. Päivitetäänkö Master Datan tietoja tasaisin väliajoin eli pidetäänkö ne ajan tasalla?

5. Onko datan nimeämisissä jotain nimeämiskäytäntöjä? Esim. toimittajien nimissä → Estää päällekkäisiä toimittajatietoja.

6. Seurataanko datan laatua tasaisin väliajoin? Onko jaksottaisia tarkistuksia? Esim. Master Datan muutoksista kertovien raporttien vertailuna?

   - Merkittävimmät riskit liittyvät Master Datan ylläpitoon ja laadun varmistamiseen
   - Datan syötön ja muutoksen ollessa virheellistä, keskeneräistä, epätarkkaa tai väärinajoitettua, vaikutukset voivat olla merkittävät.

PROSESSIEN RISKIT

1. Onko liiketoimintaprosesseista tehty jonkin tason prosessidokumentointia, joiden pohjalta ne toimii ja niiden toimintaa voidaan tarkistaa? Ovatko prosessit linjassa yleisen yritystoimintastrategian kanssa?

2. Valvotaanko prosessien kulkua ja sujuvuutta tasaisin väliajoin? Valvotaanko kirjauksia ja kuittauksia?

3. Onko liiketoimintaprosessien määrityksiin määritelty asianmukaisesti määrityksiä, ehtoja ja asetuksia? Esim. asiakkailla tietyt luottorajat, jne. Ja päivitetäänkö/ylläpidetäänkö näitä tietoja tasaisin väliajoin?

4. Hoitaako prosessien seuraamista ja ylläpitoa, joku tietty henkilö/tiimi? Esim. prosessikohtaisesti tai yleisesti?

5. Onko oikeudet luoda, muuttaa, poistaa, blokata ja avata uudelleen tilauksia (eri prosessien tilauksia) rajattu tietyille henkilöille työkuvansa perusteella?

Empiirisen osuuden toinen haastattelu 7.4.2011

Paikka: HK Ruokatalo Oy

Paikalla: Jussi Salminen & Tuomo Suonkoski

Aiheet: Tekniset riskit, juridiset ja teollisuusalan asetuksista johtuvat riskit

Kysymykset ovat läpikäytäviä aihealueita, ja niitä käytetään keskustelun runkona.

TEKNISET RISKIT

1. Onko SAP ERP:n alkuperäisesti toimitettuun pakettiin tehty paljon koodimuutoksia tai lisäyksiä?

2. Jos on, niin ketä ne ovat tehneet ja millaisella testauksella?
3. Tehdäänkö muutoksia/asetusten uudelleen määrittelyjä yleisesti paljon?
4. Onko konfiguraatio ja ohjelmistomuutokset rajattu pois tuotantojärjestelmästä? (Sama kysymys tulee myöhemmin IMG:n kohdassa vastaan)

   → Jatkokysymys: Materiaalin mukaan standardi SAP on rakennettu vähintään kolmen clientin ja järjestelmän päälle. Yhtä käyttää SAP itse, ja kahta muuta asiakasyritys. Tekninen client patchien ja päivitysten asennukseen, ja sovellus-client kehitys-, laatu- ja tuotantojärjestelmiä varten. Onko näin myös HK:lla? Eli onko HK:lla olemassa (ja käytössä) päivitys-, kehitys- ja testaus-ympäristöt erillään itse tuotannosta?

5. Onko HK:lla käytössä ulkoisia liiketoimintajärjestelmiä, jotka toimivat SAP-ympäristön kanssa yhdessä? Tapahtuvatko tiedon siirrot automaattisesti vai manuaalisesti?
6. Jotkut voivat ajatella myös teknisiin riskeihin liittyvän esim. liian monimutkaiset käyttöliittymät. Onko näistä noussut esiin ongelmia?
7. Monitoroidaanko SAP-sovellusten, tietokannan ja käyttöjärjestelmän turvallisuutta? Esim. yrityksen yleisen tietoturvapolitiikan/strategian mukaisesti?

8. Seurataanko näiden suoritusta/toimintaa?
9. Jos ongelmia ilmaantuu, niin hoituuko korjaus nopeasti? Eli säilytetäänkö käytettävyys loppukäyttäjille tehokkaasti?
10. Suoritetaanko päivityksiä (sovellus- ja turvallisuustasolla) ajoittain?
11. Ovatko kaikki tekniset ratkaisut HK:n käsissä? Tässä yhteydessä tarkoitetaan itse ”rautaa”.
12. Ovatko tallennusmediat (serverit, tietokannat, jne.) HK:n puolesta vai onko ulkoistettu ratkaisu?
13. Varmuuskopiointi? (Hoidetaanko tasaisin väliajoin, jne.)
14. Onko työntekijöillä etäyhteysmahdollisuuksia, esim. työkoneellaan kotoaan?

Voisi myös keskustella auditoinnin kannalta keskeisistä työkaluista ja apuvälineistä:

Seuraavat asiat ovat materiaalissa esitelty SAP ERP:n perussovellus-infrastruukturin kuuluvaksi:

1. IMG (Implementation Guidea) ja/tai OMM (Organization Management Modelia)?
2. ABAP/4 Workbench ja/tai TMS (Transport Management System)?
3. CCMS (Computer Center Management System)?
4. PFCG (Profile Generator) ja SA (Security Administration)?

JURIDISET JA TEOLLISUUSALAN ASETUKSISTA JOHTUVAT RISKIT

Kysymyksiä tästä ei materiaalin perusteella oikein nouse. Sisältyy hyvin riskialueisiin, mutta SAP:n kannalta en keksi kysyttävää. Mahdollisesti tapaamisessa nousee uusia näkökulmia tähän asiaan.

EMPIIRISEN OSUUDEN HAASTATTELU 26.4.2011

Paikka: HK Ruokatalo Oy

Paikalla: Jussi Salminen & Tuomo Suonkoski

Aiheet: Organisatoriset riskit

Kysymykset ovat läpikäytäviä aihealueita, ja niitä käytetään keskustelun runkona.

ORGANISATORISET RISKIT:

Käyttäjäoikeudet

Käyttäjäoikeus-riskit liittyvät miltei jokaiseen yrityksen tietoturvariskialueeseen. Oikeutukset nousevat esiin kaikissa liiketoimintaprosesseissa, tilauksissa, jne. Yleensäkin kaikissa SAP:n kanssa työskentelyä vaativissa asioissa.

- Miten käyttöoikeuksien, roolien ja auktorisointiobjektien määrittely ja toteutus hoidetaan?
    - Esim. uuden moduulin tai toiminnallisuuden tullessa HK:n SAP-ympäristöön, miten tarvittavan roolituksen muodostaminen tehdään? Ketä määrittelyn tekee, toteuttaa, testaa, jne.? (Projektiluontoisena?)

- Miten oikeuskäytännöt etenevät HK:lla? Mahdollisimman tarkasti. Onko jotenkin tähän suuntaan?: Oikeuksien tarve ilmenee → esimies tekee oikeuspyynnön (lomakkeella?) → mahdollisia hyväksyntöjä → käyttäjäoikeusvaltuutetulle, joka kyseiset oikeudet antaa.
    - Annetaanko jokaiselle työntekijälle yksilölliset oikeudet vai käytetäänkö tietyn työtehtävien oikeus/roolipohjia?

- Onko oikeudet rajattu työvelvollisuuksien mukaan ja ylläpidetäänkö rajauksia/oikeusmäärityksiä kokoajan?
    - Työntekijöille annetaan vain ja ainoastaan heidän työssään tarvitsemansa oikeudet?

- Päivitetäänkö oikeuksia pyyntöjen mukaan esim. lisäykset ja poistot, vai seurataanko käyttäjien oikeutuksia muuten? Seurataanko kenelle annettu mitäkin ja ketä tekee mitäkin mm. muutosraporttien pohjalta?

- Seuraako tai käsitteleekö oikeutuksia jotkut muutkin tahot?
    - Esimerkiksi konsultit? Käytetäänkö jossain oikeusasioissa esim. konsulttien apua määrityksissä tai toteutuksissa.

- Onko ns.superkäyttäjiä/-tunnuksia paljon käytössä? SAP_ALL tai SAP_NEW? Ketkä näitä käyttää ja missä tilanteissa? Seurataanko niiden käyttöä?

- Onko HK:lla SAP-tunnuksiin liittyen dokumentointia ja ohjeistusta?
    - Käyttäjätunnuksien ja salasanojen nimeämiset, käytännöt, jne?
    - Onko käyttäjätunnushallinnasta tiettyjä käytäntö- jä/ohjeistusta/dokumentointia?

Henkilöstön toiminta ja vaikutukset

SAP-ympäristön suurimpia uhkia ovat inhimilliset riskit, eivät niinkään tekniset. Ihmisten virheellinen SAP:n käyttö (tahallinen tai tahaton) on merkittävä riski, ja voi johtaa liiketoimintaprosessien heikkenemiseen.

Tietoturvakulttuurin omaksuminen yleiseksi käytännöksi on nykyään nousussa yrityksissä. Tietoturvasta tehdään jokaisen juttu, ei olen enää vain johdon tai IT-osaston syöttämää pakkopullaa.

- Onko HK:lla olemassa ns. tietoturvakulttuuri eli peruskäyttäjät/työntekijät ymmärtävät sen merkityksen ja sitä noudatetaan päivittäisessä työskentelyssä?

- Minkä tasoisia käytäntöjä ja strategioita HK Ruokatalolla on koskien SAP ERP:tä ja tietoturvaa yleisesti?

- Seurataanko yleisesti henkilöstön/työntekijöiden työskentelyä ja käyttäytymistä SAP:n kanssa?
    - Miten työskentelevät? Tekevätkö asiat kuten pitää ja tarkkaavaisesti?
- Seurattiinko datasyötteitä ja korjataanko ilmenevät virheet nopeasti? Saako yksittäiset henkilöt syöttää tilauksia/toimintoja ilman, että menee muun tarkistuksen läpi?

- Pidetäänkö työntekijöiden tietoturvatietoutta yllä tasaisin väliajoin?
    - Tietoturvakoulutusta yleisesti?
    - SAP:n osalta? Aiemmin kävi ilmi, että suoranaista SAP-koulutusta ei ole järjestettynä esim. vuositasolla.

- Liiketoimintaosastojen ja IT:n välille syntyvät konfliktit projekteissa ja uudistuksissa voivat joskus tuoda suuria ongelmia. Vaikuttavaa lopputulosta ei saada kun yhteisymmärrystä ei saavuteta.
    - Onko muutos/kehitysprojekteissa mukana henkilöstöä myös itse tuotannosta? Eli ns. liiketoimintalähtöisiä henkilöitä? Työtehtävissään SAP:tä käyttäviä ihmisiä.
- Onko HK Ruokatalolla SAP-ympäristön pääkäyttäjiä?
    - Minkälaisia vastuualueita heillä on? Mitä tehtäviä pääkäyttäjyys sisältää?
    - Onko heidän toimintaansa valvottu? Esim. vahvistaako/tarkistaako heidän tekemiään päätöksiä tai toimintoja kukaan?
    - Ovatko he enemmänkin IT-henkilöstöä vai tuotantohenkilöitä? Asialla voi olla merkitystä siinä, että onko heidän käsittelemänsä asiat teknisiä vai prosessipohjaisia asioita.

Määrittelyt ja asetukset

Suurimpia ongelmia ERP-järjestelmien ja kaikkien liiketoimintalähtöisten sovellusten kanssa työskentelyyn tuovat vaillinaiset määrittely-, suunnittelu-, testaus- ja käyttöönottovaiheet.

Liian usein turvaudutaan liiaksi konsultteihin, joilla ei ole loppujen lopuksi täysin tarkkaa kuvaa yrityksen liiketoimintaprosesseista, jotta järjestelmän määrittely voitaisiin hoitaa mahdollisimman hyvin.

- Miten muutokset, päivitykset ja käyttöönotot toteutetaan HK:lla? Millainen määrittely- ja suunnitteluprosessi?
    - Osallistuvatko toimittajat/konsultit näihin projekteihin? Millä tasolla?
    - Onko mahdollista tietyissä hätätilanteissa päästä muokkaamaan tuotantoympäristöä? Onko tämänkaltaista tullut ikinä vastaan?

Muuta

- Minkälaisia käytäntöjä/menettelytapoja HK:lla on koskien SAP ERP:iä? Onko niitä?
    - Tätä ei syvällisesti tarvitse avata, lähinnä yleisesti.
    - Onko siis jonkin tasoisia määrityksiä (kirjallisia) liittyen SAP:n?
- Minkä tasoista yhteistyötä ulkoisten toimittajien kanssa?
    - Ylläpitoa ja neuvontaa?
    - Muu yhteistyö? Esim. neuvotteluja uusista ratkaisuista? Yleensä muista aiheista kuin ylläpidosta johtuvista asioista?
    - Ovatko sovellustoimittajat pysyneet samoina vai onko kilpailutettu usein?