LAUREA

Organisaatio X:n tietohallinto-osaston riskienhallinnan kehittäminen

Aitta, Matti

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Organisaatio X:n tietohallinto-osaston riskienhallinnan kehittäminen

Matti Aitta
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Tammikuu, 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Matti Aitta

Organisaatio X:n tietohallinto-osaston riskienhallinnan kehittäminen

Vuosi 2010 Sivumäärä 44

Opinnäytetyön tarkoituksena oli kehittää Organisaatiolle X:lle helppokäyttöiset riskienhallintamallit ja opettaa niiden käyttö tietohallinto-osaston asiantuntijoille.

Opinnäytetyöni toteutin työelämälähtöisenä toimintatutkimuksena. Työ koostui aineiston keruusta, asiantuntijoiden haastatteluista ja riskienarvioinnista. Aineiston keruu aloitettiin tutustumalla kirjallisuus- ja internetlähteisiin sekä yrityksessä aikaisemmin käytössä olleeseen riskienhallintamalliin. Tämän jälkeen yhdessä asiantuntijoista koostuvan työryhmän kanssa uutta riskienhallintamallia testattiin ja muokattiin vastamaan Organisaatio X:n tietohallinto-osaston tarpeita.

Tämän toimintatutkimuksen tavoitteena oli ratkaista organisaation käytännön ongelma ja samalla luoda uutta tietoa, jota organisaatio voi jatkossa hyödyntää. Kun olimme luoneet Organisaatio X:lle sopivan riskienhallintamenetelmän, käytimme sitä kahden merkittävän IT-järjestelmän riskienarviointiin. Näiden kahden riskienarvioinnin aikana muokkasimme vielä riskienhallintamenetelmän lopulliseen muotoon. Siitä tuli kevyempi ja helppokäyttöisempi kuin aikaisemmin käytössä olleesta riski-indeksi riskienhallintamallista. Uudessa riskienhallintamallissa yhdistettiin vanhan riski-indeksi mallin, POA:n, PK-haavaan ja aivoriihen parhaat ominaisuudet.

Työssäni vastattiin asetettuun tutkimuskysymykseen, eli Organisaatio X:n riskienhallintamallia onnistuttiin kehittämään parempaan suuntaan. Yrityksellä käytössä ollut riskienhallintamalli oli toimiva, mutta sen käyttö koettiin hankalaksi. Riskienhallintamallia muokattiin ja yksinkertaistettiin. Uudella riskienhallintamallilla päästään samaan lopputulokseen kuin vanhalla, mutta ilman turhaa, ja hyödyttömäksi koettua numeerista dataa. Uutta riskienhallintamallia on helpompi käyttää, ja myös riskienhallinnan projektiryhmä on tätä mieltä.

Asiasanat: Riskienhallinta, Tietoturvallisuus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Security Management Programme

Matti Aitta

Developing the risk management in the Organisation X data administration unit

Year 2010 Pages 44

The purpose of this thesis is to produce easy to use risk management models for Organisation X and teach specialists of the data administration unit how to use them.

The thesis was completed as a work-oriented functional study. The project consists of data gathering, interviewing the specialists and a risk analysis. Gathering the data began with familiarizing oneself with the literature and the internet sources of information, as well as studying Organisation X's earlier risk management model. After that a group of data administration specialists was gathered with whom the reshaped risk management model was tested and edited to meet the needs of the data administration unit.

The purpose of this study was to solve a practical problem in the organisation and at the same time create new information, which the organisation could put to later use. When the new risk management model for Organisation X was created, it was used to evaluate the risks of two significant IT systems. During these two risk management projects, the new model was edited to its final shape. The new risk management model is lighter and easier to use than earlier "risk index" model. The new risk management model merged the best attributes of the old "risk index" model, PPA (=Potential Problem Analysis), PK-haava (= small and middle size enterprises vulnerable analysis) and the brainstorming process.

This thesis offers an answer to the research question, which means that Organisation X's risk management model was successfully developed further. The earlier risk management model was functional, but it was heavy and difficult to use. The model was reshaped to make it easier and lighter to use. With the new risk management model, the same conclusions can be reached as with the earlier model, but without unnecessary and useless numerical data. The new risk management model is easier to use, as was also stated by the risk management project group.

Key words: Risk management, Data security

Sisällys

1 Johdanto

Opinnäytetyön tarkoituksena on kehittää Organisaatiolle X:lle helppokäyttöiset riskienhallintamallit ja opettaa niiden käyttö tietohallinto-osaston asiantuntijoille.
Tämä on tärkeää Organisaatio X:lle siksi, että vanhan riskienhallinmallin käyttö oli hankalaa ja tämän johdosta merkittävimpien IT-järjestelmien riskienhallinta ei ollut ajan tasalla.
Tärkeimpänä päämääränä tämän opinnäytetyön toteuttamiselle on Vahti 2003/07 mainittu lause: ”Tietoturvallisuusjärjestelyiden tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys” (Vahti 2003/7). Jos merkittävimpien IT-järjestelmien riskienhallinta ei ole ajan tasalla ja asianmukaisesti suoritettuna, ei edellä mainittu lause myöskään päde.

Opinnäytetyöni toteutan työelämälähtöisenä toimintatutkimuksena.
Organisaatio X:ssä ratkaistava käytännön ongelma on vanhentunut riskienhallinta merkittävien IT-järjestelmien osalta. Tarkoituksena on tarkastaa heidän käytössään oleva riskienhallintamalli ja tarpeen mukaan uudistaa sitä. Tämän toimintatutkimuksen tavoitteena on ratkaista organisaation käytännön ongelma ja samalla luoda uutta tietoa jota organisaatio voi jatkossa hyödyntää.

Työ koostuu aineiston keruusta, asiantuntijoiden haastatteluista ja riskienarvioinnista.
Aineiston keruu on tärkeää, jotta voidaan tutustua vallitseviin käytäntöihin ja erilaisiin riskienhallintamenetelmiin, jotta niistä voidaan valita Organisaatio X:n tarpeisiin soveltuvat työkalut. Työn alussa tutustutaan myös organisaatiossa tällä hetkellä käytössä oleviin riskienhallintamenetelmiin ja katsotaan, voidaanko niitä hyödyntää tai yhdistää toisiin menetelmiin.

Toinen opinnäytetyön menetelmistä on asiantuntijoiden haastattelut. Asiantuntijoita haastatellaan, jotta saataisiin tietoa tietohallinto-osaston riskeistä ja näin ollen voitaisiin valita sopivin riskienhallintamenetelmä.

Viimeinen työmenetelmä on riskienarviointi. Uutta riskienhallintamenetelmää on tarkoitus käyttää kahden merkittävän IT-järjestelmän riskienarviointiin, jotta saadaan tietoa uuden riskienhallintamenetelmän puutteista ja vioista ennen sen lopullista muokkaamista.

1.1 Tausta, tavoitteet ja rajaukset

Toimeksianto

Organisaatio X:ssä on tarkoitus uudistaa IT-ympäristön jatkuvuussuunnitelmaa 2010 keväästä alkaen osana valtionhallinnon ICT-varautumisen projektia.
Osana jatkuvuussuunnitelmaa arvioidaan merkittävimpien IT-järjestelmien riskit uudestaan.
Ollessani työharjoittelussa Organisaatio X:ssä tehtäväni oli käydä läpi VAHTI työryhmän luoma

eVARE tietoturvatasomittariosto ja selvittää, millä tietoturvatasoille Organisaatio X:n tietoturva-asiat ovat. Suurimmat puutteet löytyivät riskienhallinnasta. eVAREn (2008, 2b) mukaan valtionhallinnon organisaation tulee toteuttaa riskienhallintaa vähintään kerran vuodessa tai suurten muutosten yhteydessä. Näin ei kuitenkaan ole tehty, johtuen riskienhallintatyökalujen ongelmista: ne todettiin hankalaksi käyttää. Näin ollen päätettiin, että teen opinnäytetyöni aiheesta: ” Organisaatio X:n tietohallinto-osaston riskienhallinnan kehittäminen”. Opinnäytetyön tarkoituksena on kehittää Organisaatiolle X:lle helppokäyttöiset riskienhallintamallit ja opettaa niiden käyttö tietohallinto-osaston asiantuntijoille.

Rajaukset

Opinnäytetyö rajataan koskemaan Organisaatio X:n tietohallinto-osaston riskienhallintaa. Tarkoitus on hallita riskejä ennalta tunnistetuista merkittävistä IT-järjestelmistä.

Opinnäytetyön merkitys kohdeorganisaatiolle

Tämä hanke on organisaatiolle tarpeellinen, jotta he saavat vietyä organisaation tietoturvatasot valtionhallinnon eVARE mittariston vaatimalle tasolle. Tarpeellisia tietoturvatasoja ei saavuteta, ellei riskienhallinta ole asianmukaisessa kunnossa. Organisaatio X voi jatkossa käyttää luotua riskienhallintamallia myös muiden merkittävien IT-järjestelmien riskienhallinnassa

1.2 Työskentelymenetelmät

Opinnäytetyöni toteutan työelämälähtöisenä toimintatutkimuksena. Ojasalo, O., Moilanen, T. & Ritalahti, J. (2009, 58) mukaan toimintatutkimus on osallistavaa tutkimusta, jonka tarkoituksena on ratkaista käytännön ongelmia ja saada aikaan muutosta. Organisaatio X:ssä ratkaistava käytännön ongelma on vanhentunut riskienhallinta merkittävien IT-järjestelmien osalta. Tarkoituksena on tarkastaa heidän käytössään oleva riskienhallintamalli ja tarpeen mukaan uudistaa sitä. Tämän toimintatutkimuksen tavoitteena on ratkaista organisaation käytännön ongelma ja samalla luoda uutta tietoa jota organisaatio voi jatkossa hyödyntää.

Toimintatutkimus on lähestymistapa, jossa ollaan kiinnostuneita siitä, miten asioiden pitäisi olla, eikä niinkään siitä, miten ne ovat. Asioita ei siis vain kuvata, vaan tavoitteena on vallitsevan tilanteen muuttaminen. Tutkimuksen ja kehittämisen kohteina toimintatutkimuksessa on yrityksen toimintatavat ja itse toimintatilanne. Ojasalo ym. (2009, 58) mukaan toimintatutkimuksiin liittyy voimakkaasti käytännönläheisyyden vaatimus. Toimintatutkimuksen tyypillisiä piirteitä ovat ongelmakeskeisyys, tutkittavien ja tutkijan aktiivinen rooli toimijoina muutoksessa sekä tutkittavien ja tutkijan välinen yhteistyö.

Työ koostuu aineiston keruusta, asiantuntijoiden haastatteluista ja riskienarvioinnista.

1.2.1 Aineiston keruu

Aineiston keruu aloitettiin keräämällä aihepiiriin liittyvää kirjallisuutta ja internetlähteitä. Aineistoa kerättiin myös organisaation tietokannoista, mistä löytyi muun muassa aikaisemmin tehtyjä riskianalyysejä merkittävistä IT-järjestelmistä ja riskienhallintamenetelmistä. Riskienhallinnasta ja sen metodeista löytyi myös paljon ajankohtaista kirjallisuutta.

1.2.2 Asiantuntijoiden haastattelut

Haastattelut toteutettiin yksilöhaastatteluina. Ne tehtiin, jotta saataisiin tietoa tutkinnan kohteista, eli riskianalyysin kohteena olevista merkittävistä IT-järjestelmistä. Riskienarvioinnin jälkeen tehtiin vielä täsmähaastatteluja saamaan yksityiskohtaisempia vastauksia esille nousseista asioista.

1.2.3 Riskienarviointi

Aluksi tutustuttiin riskienarvioinnin teoriaan kirjallisuus- ja internetlähteistä. Tämän jälkeen tutustuttiin organisaatiossa vallitseviin riskienhallintakäytöntöihin. Seuraavaksi katsottiin valtionhallinnon ohjeita organisaatioiden riskienhallinnasta ja sitä kautta lähdettiin miettimään miten vallitseva käytäntö saataisiin yksinkertaistettua.

2 Keskeiset käsitteet ja terminologia

Opinnäytetyössäni käytetään paljon ammattikielen lyhenteitä. Tähän osioon olen listannut keskeisemmät käsitteet ja lyhenteet. Lyhenteitä myös kerrataan työn edetessä aina kun niitä käytetään ensimmäistä kertaa.

Riskienhallinta on seurauksiltaan merkittävien riskien järjestelmällistä määrittelyä ja niihin varautumista. Merkittäviä riskejä ovat ne, joista tietoisuus vaikuttaa tai vaikuttaisi organisaation johdon päätöksentekoon. Riskienhallinta on prosessi, joka nivoutuu toimintoihin, joiden riskejä käsitellään.

Tietoturvallisuudella tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista.

DFS = Distributed File System, Suom. ennakoiva seuranta

DoHa = Dokumentin Hallinta
DoS = Denial of Service, Suom. palvelunestohyökkäys
eVARE = Valtionhallinnon ICT-varautumisen kehittämishanke
ICT = Information, communication and technology. Suom. TVT = Tieto- ja viestintäteknologia
IPS = Intrusion prevention system, Suom. tunkeutumisenestojärjestelmä
PK-RH = Pienten ja keskisuurteen yritysten riskienhallinta. Suomalainen internetsivusto, josta löytyy kattavaa tietoa ko. aiheesta
POA = potentiaalisten ongelmien analyysi
THS = Tiedonhallintasuunnitelma
UPS = Uninterruptible Power Supply. Suom. katkoton virtalähde
XaHa = Organisaatio X:n asianhallintajärjestelmä
YETTS = Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia

3 Valtionhallinnon ICT-varautuminen

Valtionhallinnon toiminta on verkostoitunutta. Se toteutuu niin julkishallinnon sisällä kuin yhteiskunnan muiden toimijoiden kanssa myös maailmanlaajuisesti. Hallinnon palvelut ja toiminnot rakentuvat tietoteknisten peruspalvelujen ja sovellusten varaan. Myös perusrekisterit ja muut tietovarannot näyttelevät tärkeää roolia. Näiden toiminta riippuu jatkuvasti enemmän ja enemmän tietoliikenteen toimivuudesta ja sähkön saatavuudesta. Valtionhallinnon sisäisistä ja ulkoisista palvelutoimittajista muodostuva verkosto ylläpitää tätä palveluverkostoa.

Toiminnan ja palvelujen jatkuvuuden takaaminen ja tiedon turvaaminen edellyttävät palveluverkoston varautumista ICT-toiminnan (Information, Communication and Technology. Suom. TVT = Tieto- ja viestintäteknologia.) häiriötilanteisiin. Oleellista on varmistua, että palveluverkosto pystyy normaaliajan vakavissa häiriötilanteissa ja YETTS:n (Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia) mukaisissa erityistilanteissa jatkamaan toimintaansa häiriöttä ja vaatimusten vaatimalla tavalla. Normaaliolojen häiriötilanteita varten suunnitellut toimintamallit ja ratkaisut ovat perusta erityistilanteiden hoitamiselle ja toiminnalle poikkeusoloissa.

Valtionhallinnon organisaatiot pyrkivät kaikessa toiminnassaan ottamaan huomioon VAHTI 2/2009 ohjeessa kuvatut ICT-varautumisen periaatteet. Tärkeintä on, että kaikessa organisaatioiden, toimintojen, palveluiden ja järjestelmien kehittämisessä otetaan jo esitutkimusvaiheessa mukaan toiminnan jatkuvuuden hallinnan ja tiedon turvaamisen aspekti. Tämä mahdollistaa kustannustehokkaan toiminnan tarpeista lähtevän varautumisen häiriötilanteisiin ja poikkeusoloihin.

Tietojärjestelmäratkaisut ja -palvelut koostuvat sovelluksista, tietovarannoista, tietoverkoista, muusta ICT-infrastruktuurista ja niiden oheisjärjestelmistä, tietoturvallisuudesta sekä niihin liittyvästä ylläpidosta, järjestelmähallinnasta ja teknisestä tuesta.

ICT-varautumisen kehittämisen tärkeimpänä tavoitteena on se, että organisaatiot pystyvät toiminnan tarpeiden mukaisesti ja takaamaan palvelujensa häiriöttömän jatkuvuuden ja tiedon turvaamisen normaaliolojen häiriötilanteissa, YETTS-erityistilanteissa ja poikkeusoloissa. Valtionhallinnossa sekä sen käyttämissä ja tuottamissa palveluissa on käytössä yhtenäiset toteutusvaatimukset sekä keinot ja menetelmät vaatimusten täyttämiseen. ICT-varautumisen tulee olla kustannustehokasta ja koordinoitua, sen tulee olla osa kunkin hallinnonalan jokapäiväistä toimintaa. ICT-varautuminen toteutetaan osana tietohallinnon, tietoturvallisuuden, turvallisuuden ja yleisen varautumisen kokonaisuutta.

ICT-toiminnan tärkein perusedellytys on sen käyttövarmuus ja turvallisuus. Palvelujen tulee myös toimia eri turvallisuustilanteissa niille asetettujen käytettävyysvaatimusten mukaisesti. Häiriö- ja erityistilanteiden hallinta edellyttää tunnistettuja ja yhtenäisesti sovittuja vaatimuksia koko palveluverkostossa. Julkishallinnon palveluissa lähtökohtana on, että kaikkien toimijoiden tulee osaltaan täyttää nämä vaatimukset (VAHTI 2/2009).

3.1.1 Valtionhallinnon ICT-varautumisen kehittämishanke - eVARE.

eVARE on VAHTI työryhmän tekemä lista, jossa käydään läpi ICT-varautumiseen liittyvät tietoturvatasot. eVARE:ssa on otettu huomioon kaikki tärkeät tietoturvallisuuteen liittyvät asiat liittyen johtamiseen, toiminnan ohjaukseen ja toimintamalleihin, henkilöstön ja henkilöstöresurssien hallintaan, kumppanuusverkostoon, prosesseihin ja järjestelmäympäristöihin, ICT-jatkuvuuden hallintaan, tietoturvallisuuden hallintaan ja mittaamiseen. Kaikissa kohdissa on määritelty perustason-, korotetun- ja korkean tason vaatimukset (Halonen, K. 2009).

4 Riskienhallinta

Juvonen, M., Korhonen, H., Ojala, M., Salonen, T. & Vuori, H. (2005, 7) mukaan riski tarkoittaa vaaraa tai uhkaa. Riski sisältää ajatuksen siitä, että jotain epäedullista voi tapahtua henkilölle itselleen, jollekulle toiselle henkilölle tai jollekin omaisuudelle. Riskiin liittyy kolme tekijää, jotka vaikuttavat siihen, millaisena sen koemme. Nämä kolme tekijää ovat: tapahtuman epävarmuus, tapahtumaan liittyvät odotukset ja tapahtuman laajuus ja vakavuus. Riskin lähtökohtana voidaan pitää sitä, että tapahtumaan liittyy epävarmuutta. Jos tapahtuman, toimenpiteen tai muun vastaavan seuraus tai tulos on ennalta tiedossa, kyseessä ei ole riski. Vaikka lopputulos olisi negatiivinen, se ei ole riski, jos se tiedetään etukäteen. Epävarmuuden aste eli vahingon sattumisen todennäköisyys voi vaihdella eri tapahtumien kesken hyvin paljon.

Suominen (1999, 9) kertoo kirjassaan, että riski merkitsee niitä vaaratekijöitä, joille ihmiset ovat alttiina tietyllä hetkellä. Synonyymeinä riskille käytetään suomenkielessä usein vahingonvaaraa tai vahingonuhkaa. Riskinä voidaan pitää sitä mahdollisuutta, että päämääräksi asetettu positiivinen tavoite ei toteudu. Kirjan mukaan teoreettisessa ajattelussa riski yhdistetään tulokseltaan erilaisten, onnistuneiden ja epäonnistuneiden, tapahtumien vaihteluksi. Riskiin liittyy poikkeuksetta tapahtumien todennäköisyyksien arviointi. Onnistuneita tapahtumia voidaan kutsua toivotuiksi ja epäonnistuneita ei-toivotuiksi. Riskin luonteeseen kuuluu se, ettemme voi ainakaan tarkasti olla perillä ei-toivottujen tapahtumien sattumisesta (Suominen 1999, 9-10).

Pk-yritysten riskienhallintaan keskittynyt Internetsivusto PK-RH kertoo, että riski on ensisijaisesti vahingon mahdollisuus. Lähes kaikki riskit ovat ihmisten aiheuttamia ja siksi niihin voidaan vaikuttaa ja varautua ja niiltä voidaan suojautua. Riskeissä ei ole kyse kohtalosta, vaan arkipäivän pienistä asioista. Jos riskeihin ei ole osattu, huomattu tai ehditty ajoissa kiinnittää huomiota, ne pääsevät yllättämään. Pienetkin häiriöt voivat käynnistää tapahtumaketjun, joka uhkaa koko yrityksen toimintaa. Riskejä otetaan usein myös tietoisesti ja harkiten, esimerkiksi ajan ja vaivan säästämiseksi. Riski voi liiketoiminnassa olla myös mahdollisuus. Yritystoiminta edellyttää järkevää riskien ottamista.

Työssäni käytän PK-RH:n riskin määritelmää. Työympäristö ja valitut riskianalyysin kohteet ovat juuri sellaisia, joiden suurimmat riskit muodostavat ihmisten välillisesti luomat riskit. Suurimmat riskit johtuvat ihmisten asiantuntemuksen puutteesta tai heidän tekemistään vahingoista. Yrityksessä otetaan myös tietoisia riskejä jotka on tunnistettu. Tunnistettu riski otetaan, koska katsotaan edullisemmaksi hyväksyä se kuin yrittää poistaa sitä.

4.1.1 Riskienhallinnan vaiheet

Liiketoiminnan jatkuvuussuunnittelun ja ICT-varautumisen työkirjan (Iivari & Laaksonen 2009, 124) mukaan riskienhallinnan tarkoitus on tuottaa päätöksentekijöille tietoa ja ymmärrystä erilaisista tekijöistä, jotka voivat negatiivisesti vaikuttaa toimintoihin ja lopputuotoksiin, jotta he voivat tehdä tietoisia päätöksiä riskienhallintaan liittyvien toimien toteuttamiseksi. Riippumatta siitä, minkälaisia riskejä arvioidaan, riskianalyysit noudattavat yleensä samaa kaavaa ja niihin liittyvät samanlaiset vaiheet.

Iivari ym. (2009, 125) kirjan mukaan, riskienhallinta alkaa riskienhallintakehikon määrittelystä. Tämän vaiheen tarkoitus on tehdä riskianalyysien suorittaminen mahdollisimman helpoksi kaikille osapuolille sekä varmistaa tulosten yhteismitallisuus. Tässä vaiheessa tehdään työkalut uhkien tunnistamiselle, niiden toteuttamisen todennäköisyyden sekä vaikutusten määrit-

tämiselle, siis riskien määrittämiselle. Samalla laaditaan myös uhka- ja haavoittuvuusluettelot valittuja riskianalyysi kohteita silmällä pitäen.

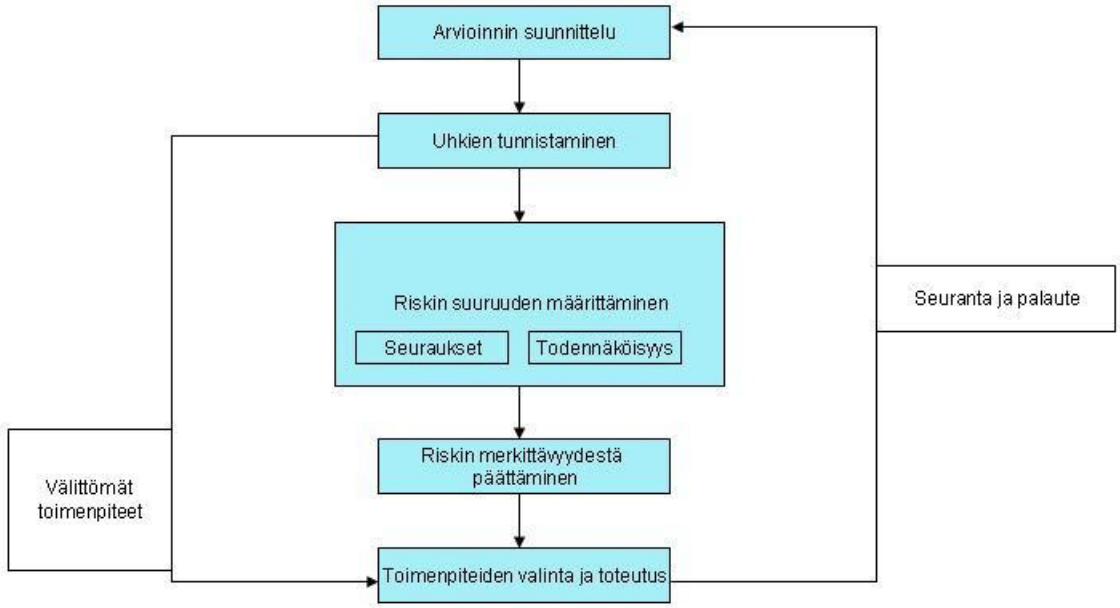
Iivari ym. (2009, 125) kertoo että riskienhallinta alkaa riskianalyysin tekemisellä. Riskianalyysi alkaa aina uhkien tunnistamisesta. Tällä tarkoitetaan yleensä ottaen sellaisten uhkien kartoittamista, jotka voivat vaikuttaa tarkastelun alaisiin toimintoihin tai käytössä oleviin tuotantovaroihin negatiivisesti. Riskejä voidaan kartoittaa erilaisten tarkistuslistojen avulla tai työkalujen, kuten potentiaalisten ongelmien analyysin avulla. Erilaisia tunnistettavia riskejä ovat esimerkiksi tulipalot, luonnonmullistukset, murtovarkaat tai tyytymättömät työntekijät. Riskien tunnistamisessa voi käyttää myös erilaisia riskiluetteloita, joita esimerkiksi PK-RH:n sivuilta löytyy paljon.

Iivarin ym. (2009, 126) mielestä riskien tunnistamisen jälkeen on tärkeää arvioida niiden toteutumisen todennäköisyys. Apuna toteutumisen todennäköisyyttä arvioitaessa kannattaa käyttää PK-RH:n sivuilta löytyvää arviointitaulukkoa, jossa työryhmä määrittelee riskin todennäköisyyden ja kuinka suuren vahingon sen toteutuminen aiheuttaa. Näin saadaan numeerinen arvo, kuinka vaarallinen riski on kyseessä. Usein riski luokitellaan 1-5 joista 1. on pieni riski ja 5. sietämätön. Uhkien toteutumisen todennäköisyyteen vaikuttavat tarkastelun kohteen haavoittuvuudet ja toisaalta todennäköisyyttä pienentävät olemassa olevat kontrollit eli suojaustoimenpiteet. Ennen riskien toteutumisen todennäköisyyden arviointia voi siten olla hyödyllistä analysoida tarkastelun kohteen haavoittuvuudet sekä arvioida olemassa olevien suojaustoimenpiteiden vaikutukset. Tämän jälkeen voidaan määrittää jäljelle jäävä riski.

Riskianalyysissa on tarkoituksenmukaista pyrkiä tunnistamaan ja arvottamaan niiden toimintojen ja tuotannontekijöiden eli varojen arvo, herkkyys ja kriittisyys, joita tunnistetut riskit uhkaavat. Erityisen tärkeää on tunnistaa toimintojen ja varojen joukosta tärkeimmät ja toiminnalle kriittisimmät. Kun suojattavat ja turvattavat varat ja toiminnot on tunnistettu ja arvotettu, tulee seuraavaksi arvioida, mikä on mahdollisten tappioiden ja vahinkojen maksimimäärä, jos riskit käyvät toteen. Tähän arvioon tappioista ja vahingoista tulee luonnollisesti sisällyttää myös toimintojen ennalleen palauttamisesta aiheutuvat kustannukset (Iivari ym 2009, 127).

Riskienhallinnan viimeisessä vaiheessa pyritään tunnistamaan kustannustehokkaat tavat, joilla on mahdollista pienentää ja hallita riskejä. Näitä voivat olla esimerkiksi organisaation uudet toimintatavat tai tekniset ja fyysiset toimenpiteet. Riskienhallinta on tasapainoilua riskien toteutumiskustannusten, suojauskustannusten ja vaihtoehtoisten riskien välillä. Riskianalyysin viimeisessä vaiheessa dokumentoidaan riskien arvioinnin tulokset ja kehitetään toimintasuunnitelma riskien hallintaan. (Iivari ym 2009, 128).

Alla olevassa kuvassa on kuvattu yllämainitut riskienhallinnan vaiheet.



Kuva 1 Riskienarvioinnin ja hallinnan vaiheet (Vahti 2003/07).

4.1.2 Riskityypit

Iivari ym (2009, 129) toteaa, että riskit voidaan luokitella useilla eri tavoilla. Riskit voidaan jakaa sisäisiin ja ulkoisiin riskeihin, teknisiin ja ei-teknisiin, toiminnallisiin ja ei-toiminnallisiin. Riskien luokitteluakin tärkeämpää on se, että kaikki tärkeimmät riskit saadaan tunnistettua ja niiden vaikutus arvioitua. Luokittelu on vain tapa esitellä ja jakaa kaikki tunnistetut riskit tietyllä tavalla. Riskien luokittelu voi tulla myös suoraan liiketoiminnasta tai toimialalta, jonka edunvalvontaorganisaatio tai muu toimija on saattanut koota erilaisia toimialaa koskevia riskejä tietyin perustein jaoteltuihin ryhmiin.

Iivari ym (2009, 129) kirjaan viitaten yrityksen sisäiset riskit ovat yleensä joko ihmisten aiheuttamia riskejä, onnettomuuksia tai teknologisia riskejä. Suurin osa ihmisten aiheuttamista riskeistä on yrityksen sisäisten toimijoiden, kuten työntekijöiden, alihankkijoiden tai tavaran toimittajien vahingossa tai tarkoituksellisesti aiheuttamia. Esimerkkejä yrityksen työntekijöiden aiheuttamista riskeistä ovat tiedostojen tuhoutuminen, lakot, tai tahalliset vahingonteot. Onnettomuudet ja teknologiset riskit liittyvät usein ihmisten aiheuttamiin riskeihin, mutta eroavat niistä sillä, että ne eivät yleensä ole tahallisia, vaan vahingossa aiheutettuja. Esimerkkejä onnettomuuksista ovat tulipalot ja tietoliikennekatkokset. Teknologiset riskit taas liittyvät tekniikan pettämiseen, kuten tietojärjestelmien vikaantumiseen tai sisäverkon toimimattomuuteen. Vaikka kaikkiin sisäisiin riskeihin ja onnettomuuksiin ei voida mitenkään varautua, on kuitenkin hyvä, että kaikki riskit on tiedostettu ja otettu huomioon suunnittelus-

sa ja suunnitelmien testaamisessa. Jos joku riski joskus käy toteen, ollaan kuitenkin paljon paremmissa lähtöasetelmissa, kun käytössä on testattu ja harjoiteltu suunnitelma onnettomuuden vaikutusten pienentämiseksi ja jatkuvuuden turvaamiseksi, vaikka toteen käynyt riski ei olisikaan aivan samanlainen kuin mihin on varauduttu.

Yrityksen ulkoiset riskit ovat yleensä joko luonnonmullistuksista tai ihmisten teoista aiheutuneita riskejä tai vahinkoja. Esimerkiksi erilaiset liikkumiseen ja kuljettamiseen liittyvät onnettomuudet ja kuten kolarit. Rautatie- tai lento-onnettomuudet ovat harvinaisia, mutta mahdollisia. Suurin osa yrityksen ulkopuolisista riskeistä voi tuntua teoreettisilta ja kaukaa haetuilta, mutta viime vuosien tapahtumat ovat osoittaneet, että mihin tahansa yrityksen ulkopuolelta tulevaan uhkaan pitää ja kannattaa varautua. Esimerkkejä yrityksen ulkopuolelta tulevista ihmisten aiheuttamista riskeistä ovat terrorismi, hakkerointi, pommiuhkaukset ja kidnappaukset. Esimerkkejä teknologisista riskeistä ovat katkot Internet-palveluntarjoajan palvelussa, puhelinverkon toiminnassa tai sähkönjakelussa. Ihmisten aiheuttamat ulkoiset riskit eroavat sisäisistä riskeistä siten, että niissä riskin aiheuttavat yrityksen ulkopuoliset ihmiset (Iivari ym 2009, 129).

4.1.3 Riskienhallinnan tulokset

Iivari ym (2009, 135–137) käyttää kirjassaan taulukkoa esittämään riskienhallinnan tulokset. Taulukkoon on listattu kaikki organisaation, tai halutun kohteen toimintaa uhkaavat riskit, niiden vaikutukset, todennäköisyys ja niihin varautuminen. Merkittävimpiä riskejä, joita voidaan torjua tai joihin voidaan reagoida, kannattaa avata omissa taulukoissaan. Laadittava riskitaulukko tai matriisi perustuu aina yrityksessä laadittuun riskienhallintaan ja henkilöiden haastatteluihin. Tämän lisäksi on tietenkin huomioitava organisaation ulkopuolisista tahoista aiheutuvat riskit, varsinkin jos organisaation toiminta tai palvelu on riippuvaista eri sidosryhmistä.
Riskienhallinta tulee suorittaa säännöllisesti, vähintään kerran vuodessa tai aina suurempien muutoksien yhteydessä (eVARE 2008, 2b). Analyysissä on hyvä käydä lävitse aikaisemmin kartoitetut riskit ja päivittää niiden tila sekä selvittää, onko uusi mahdollisia riskejä ilmaantunut. Merkittävien muutoksien yhteydessä on aina arvioitava, tarvitseeko järjestelmien suojauksiin tehdä muutoksia. Yritykseen kannattaa perustaa suurempi riskimatriisi tai -tietokanta, jolloin riskien käsittely ja dokumentointi on tehokkaampaa (Iivari ym 2009, 135–137).

4.1.4 Riskienhallintakeinot

Iivari ym (2009, 146–148) mielestä riskienhallinnan strategisena tavoitteena on sovittaa mahdollisesti toteutuvien riskien haitalliset vaikutukset yrityksen toimintaan ja riskien torjumisen aiheuttamiin suoriin tai epäsuoriin kustannuksiin. Kaikkia riskejä ei voida hallita samalla ta-

valla, eikä edes samoja riskejä kaikessa toiminnassa välttämättä hallita keskenään samalla tavalla. Toisessa prosessissa riski voi olla hyväksyttävä, kun taas jossain toisessa tapauksessa se hoidetaan vakuuttamalla.

Käytännössä riskienhallintastrategiat valitaan edellä esitetyn liiketoiminnan keskeytysvaikutusanalyysin tulosten perusteella. Tietenkin valinnoissa huomioidaan myös lakisääteiset velvoitteet ja muu normisto, sillä kaikkiin riskeihin varautuminen ei ole vapaaehtoista.
Jos yrityksen normaalissa toiminnassa ja toimintaympäristössä havaitaan uusia riskejä, joita ei aiemmin ole huomioitu, on aina valittava strategia, jonka mukaan kyseinen uusi riski kussakin toiminnassa halutaan hallita. Yleensä yrityksellä on mahdollisuus käyttää ainakin seuraavia keinoja.

1. Riski voidaan välttää luopumalla tietystä toiminnasta. Joitakin riskejä ei haluta ottaa ja ne voidaan poistaa lopettamalla riskialtis toiminta. Näin voidaan tehdä silloin, kun samalla ei luovuta jostain merkittävästä mahdollisuudesta.

2. Riskin välttäminen kahdentamalla. Laitteiden tai muiden kahdentamisella saavutetaan monissa tapauksissa hyvä toimintavarmuus. Kaikissa tapauksissa kahdennus ei kuitenkaan välttämättä tuo lisää toimintavarmuutta tai se tulee liian kalliiksi riskin suuruuteen nähden.

3. Riskin voi välttää ulkoistamisella. Ulkoistamisella on joissakin tapauksissa saavutettavissa huomattavasti parempi toimintavarmuus pienemmällä investoinnilla. Yrityksen koon mukaan suurempien palveluntarjoajien tarjoamat ulkoistuspalvelut voivat olla kokonaistaloudellisesti edullisempia, koska ne ovat tehokkaampia.

4. Riskin aiheuttaman vaikutuksen minimointi. Vaikutuksia minimoimalla pyritään torjumaan tai vähentämään yrityksen toiminnalle riskien toteutumisesta aiheutuvaa haittaa. Tällaisia järjestelyitä ovat esimerkiksi varmuuskopiointi, kahdentaminen tai fyysisen turvallisuuden parantaminen.

5. Riskin siirtäminen. Vakuutuksien avulla on mahdollista siirtää riskien toteutumisesta aiheutuvia taloudellisia menetyksiä. Toiminnan jatkuvuuden kannalta on kuitenkin pääasiassa käytettävä muitakin keinoja. Vakuutukset eivät yleensä korvaa välillisiä vahinkoja eivätkä toiminnan keskeytymisestä aiheutuvia kustannuksia. Keskeytysvakuutuksilla tosin on mahdollista kattaa ainakin osa edellä mainituista vahingoista. Keskeytysvakuutukset tehdään aina tapauskohtaisesti, joten on mahdotonta antaa yksiselitteisiä ohjetta siitä, mitä niiden avulla voidaan vakuuttaa ja mitä ei. Keskeytysvakuutusta kannattaa kuitenkin harkita yhtenä jatkuvuudenhallintaan liittyvänä riskienhallintakeinona. Vakuutuksista tulee vielä huomata, että

monesti useat luonnonvoimien aiheuttamat vahingot kuuluvat vakuutusyhtiöillä force majeur -pykälään.

6. Riski hyväksytään. Yleensä pienet riskit voidaan hyväksyä, jos niiltä välttymistä ei voida hoitaa helposti. Se, mitä yhdessä yrityksessä pidetään pienenä riskinä, ei välttämättä ole sitä toisessa yrityksessä. Hyväksyttävän riskin suuruuteen vaikuttavat muun muassa organisaation koko, toimiala ja riskinsietokyky. Riski voi olla pieni vain kolmesta syystä: riski on vaikutuksiltaan pieni, riski on todennäköisyydeltään pieni tai riski on sekä vaikutuksiltaan että todennäköisyydeltään pieni.

Yrityksen ei kannata ottaa strategiakseen kaikkien resurssin kahdentamista, ellei se toiminnan luonteen tai taloudellisten resurssien kannalta ole järkevää. On hyvä tiedostaa, että strategisista vaihtoehdoista on mahdollisuuksien mukaan käytettävissä kaikki vaihtoehdot, ja melkein aina näin kannattaakin toimia. Käytännössä tämä voisi yrityksen kannalta tarkoittaa esimerkiksi sitä, että:

- laitteisto ja toiminta on vakuutettu
- tärkeät tilat on palo- ja murtosuojattu
- keskeisimmät laitteet ja resurssit on kahdennettu
- yrityksen tärkeästä tietosisällöstä on riittävän tuoreet varmuuskopiot
- yrityksen paloherkissä tiloissa on asianmukaiset alkusammutusvälineet

(Iivari ym 2009, 146–148.)

5 Organisaatio X:n tietohallinto-osaston riskienhallinta

Organisaatio X:ssä on aina pyritty hallitsemaan ja miettimään riskejä, mutta dokumentaatio ja varsinainen riskienhallintamalli on ollut epäkäytännöllinen ja vaikea käyttää. Seuraavassa on listattu Organisaatio X:ssä olleet riskienhallintamallit.

5.1 Riskienhallintamalli vuodelta 2002

Organisaatio X:n tietohallinto-osaston viimeisin kokonaisvaltainen riskien tunnistaminen ja -analysointi tehtiin vuonna 2002. Tämä tehtiin ATK-jatkuvuussuunnitellun yhteydessä. Tällöin käytiin lävitse kaikki tietohallinto-osaston merkittävät komponentit ja niiden riskit arvioitiin ja niistä laadittiin jatkuvuussuunnitelmat. Riskienarvioinnin teki Organisaatio X:n riskianalyysi-osasta yhteistyössä tietohallintayksikön asiantuntijoiden kanssa. Suunnitelmasta ei käy ilmi, kuinka riskienarviointi on suoritettu, mutta vastauksista päätellen se on toteutettu työryhmämuotoisena riskienarviointina. Eli riskit on tunnistettu ja niistä riskianalyysin projektipäällikkö on poiminut mielestään oleelliset riskit. Suunnitelmassa ei ole mitään numeerisia riski-

luokituksia, vaan riskit on määritelty yleisiksi uhkakuviksi, järjestelmäkohtaisiksi uhkakuviksi ja realistiksi riskeiksi.

Yleiset uhkakuvat on määritelty seuraavasti. ”Organisaatiosta riippumatta voidaan luetella erilaisia organisaation toimintaa vaarantavia uhkakuvia, jotka ovat mahdollisia kaikissa organisaatioissa, kuten:

- Tulipalo
- Vesivahinko
- Laiterikko
- Pitkäkestoinen sähkökatkos
- Tietokonevirusepidemia
- Tietojärjestelmän valtaus
- Sabotaasi
- Yrityskuvan vahingoittuminen
- Yksilön työmotivaation häiriöt ja työetiikan mureneminen”

Järjestelmäkohtaiset uhkakuvat on määritelty seuraavasti. ”Tietojärjestelmän toteuttamistavasta riippumatta voidaan luetella järjestelmäkohtaisia uhkia, kuten:

- Tiedon eheyden menetys
- Tiedon paljastuminen
- Tietosuojan rikkoutuminen
- Tallenteen menettäminen
- Laitteen menettäminen
- Oheislaiterikko
- Levyrikko
- Ohjelmiston vakava toimintavirhe
- Laitteiston vakava toimintavirhe
- Käyttöoikeusrikkomus
- Laitevarkaus”

Realistiset uhkakuvat on määritelty seuraavasti. ” Atk-yksikössä saatujen kokemusten ja käytyjen keskusteluiden pohjalta (kiinnittämällä huomiota Organisaatio X:n toimialaan, fyysiseen toimintaympäristöön, toimitiloihin, tietoverkon rakenteeseen, konesaliin, palvelimiin, sovelluksiin ja työasemiin), voidaan nostaa esille ainakin seuraavat Organisaatio X:lle tyypilliset atk-toiminnan jatkuvuutta vaarantavat uhkat, kuten:

- Atk-konehuoneen tuhoutuminen tai vakava vaurioituminen (tulipalo/vesivahinko)
- Yksittäisen palvelimen rikkoutuminen
- Tiedostopalvelin, missä normaalit varmistukset/palautukset
- Tietokanta- ja sovelluspalvelimet, missä erityisvarmistukset

- Erityispalvelimet (palomuuri, etäpalvelin)
- Tietoliikennelaitteen rikkoutuminen (reititin, kytkin, hubi, mediamuunnin)
- Työaseman tai kannettavan rikkoutuminen
- Ulkoisten tietoliikenneyhteyksien katkeaminen
- Ohjelmistojen tietoturva-aukkojen ilmaantuminen
- Virusinvaasio/hyökkäys
- Palvelunestohyökkäys
- Järjestelmään tunkeutuminen
- Tietoliikenteen kuuntelu
- Sähkökatkos
- Kerrosjakamon vahingoittuminen
- Nauhavaraston vahingoittuminen
- Kaapeloinnin vahingoittuminen
- Henkilöriski

Kyseisessä suunnitelmassa riskit on analysoitu enemmän yleisellä kuin yksityiskohtaisella tasolla. Kyseessä on koko tietohallinto-osaston jatkuvuussuunnitelma eikä siinä edes ole yritetty mennä yksityiskohtiin. Ainoastaan merkittävimpien järjestelmien suurimmat riskit on tunnistettu ja analysoitu. Riskien pohjalta on luotu jatkuvuussuunnitelma palautumissuunnitelmineen, mutta riskien poistamisen ja ennaltaehkäisyn aspekti on jätetty kokonaan pois. Käytännössä suunnitelma kertoo, miten toimitaan jos jokin suurimmista riskeistä realisoituu, ei niinkään sitä, miten riski voitaisiin poistaa tai minimoida.

5.2 Riski-indeksi malli vuodelta 2007

Vuonna 2007 laadittiin valtionhallinnon tukiorganisaatiosta tulleen riski-indeksi mallin mukaisesti riskienarviointidokumentti yrityksen sähköpostijärjestelmästä. Siinä riskienarviointimallina käytettiin riski-indeksi mallia, jota sähköpostijärjestelmän riskienarvioinnissa käytettiin seuraavasti:

- Tarkastelukohteelle listattiin sen riskeihin vaikuttavat uhkatekijät. Uhkatekijät arvioitiin kohdekohtaisesti ja siinä hyödynnettiin Organisaatio X:n valmistelemia yleisiä uhkatekijöitä ja niiden riskejä.
- Yksittäisistä uhkatekijöistä arvioitiin kunkin uhkatekijän riski-indeksi (osariski)
- Osariskit painotettiin sen mukaisesti, miten suuri niiden vaikutus oli ko. kohteen kokonaisriskiin
- Kokonaisriski laskettiin yksittäisten uhkatekijöiden osariskien painotettuna keskiarvona

Organisaatio X:n riskiarvioinnissa yksittäisen uhkatekijän riski lasketaan riski-indeksinä. Riski-indeksi mallin erityispiirteitä ovat:

- Riskin komponentit visualisoidaan väreillä ja kootaan taulukkoon. Taulukosta nähdään yhdellä silmäyksellä yleiskuva kokonaisriskistä (mitä vihreämpi, sitä matalampi riski)
- Riskissä huomioidaan todennäköisyyden ja välittömän vahingon suuruuden lisäksi vahingosta toipumisaika sekä se, voiko riski realisoitua heti vai vasta myöhemmin. Tämä jälkimmäinen arvio mahdollistaa myös ns. rappeutumis-riskien arvioinnin.
- Riskille lasketaan numeerinen arvo. Tämä arvo normitetaan siten, että minimi-riski saa arvon 0 ja maksimiriski saa arvon 100.

Kokonaisriski: 61

Uhkatekijä	Riski-indeksi	tod.näk	vahinko	toipum.	aikajänne	Painotus
Uhkatekijä A	100	3	4	3	3	10 %
Uhkatekijä B	89	3	3	3	3	10 %
Uhkatekijä C	89	3	4	3	2	10 %
X	78	3	4	2	2	10 %
X	78	3	3	2	3	10 %
X	63	2	4	3	3	10 %
X	41	2	3	2	2	10 %
X	33	2	2	2	2	10 %
X	26	2	2	1	2	10 %
X	11	1	2	3	1	10 %
					tarkistus	100 %

= Erittäin suuri vahinko (mustaa luokkaa käytetään vain vahingon suuruuden luokittelussa)
= Todennäköinen / Suuri / Voi tapahtua vaikka heti / Pitkä toipumisaika
= Kohtalainen todennäköisyys / Kohtalainen vahinko / Voi tapahtua jonkin ajan päästä / Keskipitkä toipumisaika
= Epätodennäköinen / Vähäinen / Ei tapahtune kovin nopeasti / Lyhyt toipumisaika

Kuva 2. Riski-indeksi malli. (Organisaatio X:n riski-indeksi malli)

Tähän malliin olisi kuulunut vielä riskienanalysointi, mutta sitä vaihetta ei koskaan toteutettu. Malli olisi ollut PK-haavan mukainen riskianalyysi.
Riski-indeksi malli toteutettiin ainoastaan sähköpostijärjestelmän osalta ja tarkoitus oli joskus tulevaisuudessa toteuttaa se myös muiden merkittävien IT-järjestelmien osalta. Sen tekeminen kuitenkin katsottiin melko hankalaksi ja numeerisen datan määrä liian suureksi ja epäolennaiseksi. Siksi päätimme tietoturvapäällikön kanssa kehittää siitä yksinkertaisemman ja helppokäyttöisemmän version muunnellun POA:n ja PK-haavan avulla. Jos saisimme kehitetty riski-indeksi mallista helppokäyttöisemmän ja käyttäjäystävällisemmän, se motivoisi ja helpottaisi muiden merkittävien IT-järjestelmien riskienarviointia.
Seuraavassa esittelen kattavan riskienhallintamallin, joka on räätälöity Organisaatio X:n tietohallinto-osaston tarpeisiin.

5.3 Organisaatio X:n riskienhallintamalli vuonna 2009

Riskienhallintamallia lähdettiin etsimään kirjallisuudesta ja internetlähteistä. Kohdeorganisaatiolle oli tärkeää se, että menetelmät olisivat VAHTI-työryhmän hyväksymiä. Pohjaa haet-

tiin lukemalla VAHTI 7/2003, jossa annettiin paljon erilaisia ideoita ja menetelmiä kuinka riskienhallinnan voisi toteuttaa. VAHTI ohjeessa nousi esiin POA ja PK-haava, mihin myös vuoden 2007 riski-indeksi malli perustui. POA:an ja PK-haavaan tutustuttiin huolellisesti ja niiden pohjalta muokattiin Organisaatio X:n tietohallinto-osaston tarpeisiin muokattu malli. Seuraavissa kappaleissa esitellään muunneltu POA ja PK-haava.

5.3.1 Potentiaalisten ongelmien analyysi – POA

PK-RH:n (Pk-RH, Potentiaalisten ongelmien analyysi) mukaan POA on tehokas uhkien tunnistusmenetelmä. POA:n tehokkuus perustuu workshop tyyliseen aivoriiheen, missä kollektiivinen informaation tuottaminen tuottaa tehokkaamman tuloksen kuin yksilötyönä tehty. POA:lla pystyy arvioimaan riskit niin koko yrityksestä, yhdestä osastosta tai vaikkapa vain arvioimaan yhtä kriittistä IT-järjestelmää.
POA:n järjestämiseen tarvitaan aluksi henkilö tai riskienhallinnan projektipäällikkö, joka tuntee riskienhallinnan perusteet ja POA menetelmän. Hän päättää, minkä aihealueen riskejä lähdetään arvioimaan ja kokoaa työryhmän. Aiheesta riippuen työryhmän olisi hyvä sisältää ihmisiä alais-, asiantuntija- ja johtoportaasta. Ryhmän ihanne koko on 3-5 henkeä.

Kun POA palaveri aloitetaan, käydään läpi tilaisuuden tavoite ja selvitetään tarkastelun rajaus. Tämän jälkeen projektipäällikkö esittelee riskianalyysin tärkeimmät periaatteet. PK-RH sivuston ohjeen mukaan on tärkeää, että puhutaan asioista, ei ihmisistä. Ketään syyttelemättä ja turhia selittelemättä etsitään avoimesti riskejä sekä mietitään keinoja niiden poistamiseksi. POA:a tehdessä tulee myös muistaa, että riskien tunnistaminen on kaikkien yhteinen etu, eikä tunnistamattomia riskejä voi hallita.

POA:ssa uhkien tunnistaminen tapahtuu muunnellulla aivoriihitekniikalla. Käytännössä se tarkoittaa sitä, että projektipäällikkö antaa aiheeseen liittyviä avainsanoja, joiden tarkoitus on herättää ryhmässä ajatuksia. Avainsanat ovat vihjeitä ja ne on jaettu asioihin sekä niihin liittyviin ilmiöihin ja ongelmiin.

Aluksi projektipäällikkö heijastaa avainsanat seinälle kaikkien nähtäville. Seuraavaksi ryhmä kirjoittaa paperille kolme aiheeseen liittyvää riskiä ja siirtää paperin eteenpäin. Tämän jälkeen kaikki paperin saaneet henkilöt kirjoittavat lisää omia ajatuksiaan paperille toisen ideoista uusia mahdollisia uhkia keksien. Sitten paperi annetaan seuraavalle ja niiden annetaan kiertää niin kauan kuin ideoita riittää. Tässä vaiheessa mielikuvituksen saa päästää valloilleen ja keksiä mitä uskomattomimpia riskiskenaarioita. Jos ryhmä on puhelias, helpompi ja nopeampi keino on heijastaa avainsanat seinälle ja antaa työryhmän keskustella uhkista. Tämän jälkeen ryhmän jäsenet voivat kertoa mieleensä tulevia riskejä jotka tilaisuudesta vastaava henkilö kirjaa ylös. Kun uhkia ei enää keksitä lisää, projektipäällikkö kokoaa ja ryhmittelee

riskit kohteen tai vahingon sattumistilanteen mukaan, esimerkiksi konesalin murto- tai tulipaloriskit.

Kun ryhmittely on tehty, käydään riskit keskustellen läpi. Mikä esille tulleista riskeistä on oikeasti potentiaalinen riski? Mitkä ovat riskien syyt ja mitä siitä voi seurata? Kun riskeistä keskustellaan, yritetään löytää lisää riskejä ja samalla arvioidaan niiden merkittävyyttä. Kun riskejä arvioidaan, pyritään niitä samalla luokittelemaan kolmeen ryhmään. Ei riski: riski on merkityksettömän pieni. Riski hallinnassa: merkittävä riski, joka on tällä hetkellä hallinnassa. Hoidettava kuntoon: merkittävä riski joka vaatii lisäselvitystä tai välittömiä toimenpiteitä. Tässä vaiheessa riskit kirjoitetaan ylös PK-haava yhteenvetolomakkeelle.

Kun kaikki potentiaaliset uhkat on luokiteltu ja kirjattu, otetaan tarkasteltavaksi jatkokäsittelyä edellyttävät ”hoidettava kuntoon” -luokitellut riskit. Analysointia lähdetään tekemään miettimällä niistä aiheutuvan riskin suuruutta. Riskin suuruus riippuu siitä, mitä useammin tai todennäköisemmin se toteutuu ja kuinka suuret vahingot se toteutuessaan aiheuttaa. Riskin arvo lasketaan kaavalla: todennäköisyys x riskin laajuus tai vakavuus (Suominen 1999, 10). Näin riskit voidaan numeerisen arvon perusteella jaotella ryhmiin vähäinen, kohtalainen ja merkittävä. Usein karkea, kolmiportainen luokittelu on riittävä.

	Tapahtuman seuraukset		
Tapahtuman todennäköisyys	vähäiset	haitalliset	vakavat
epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski
mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski

Kuva 3. riskin suuruuden määrittelevä taulukko (PK-RH)

Riskien tunnistaminen ei vielä pienennä riskiä, vaan käytännön toimet riskien välttämiseksi, pienentämiseksi ja siirtämiseksi tulee aloittaa. Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Toimenpiteet aloitetaan luonnollisesti pahimmista riskeistä. Toimenpiteet, jotka poistavat monien ongelmien syitä, ovat etusijalla. PK-haava yhteenvetolomakkeelle kirjataan sovitut toimenpiteet, vastuuhenkilöt ja toteutusaikataulu (PK-RH, Potentiaalisten ongelmien analyysi).

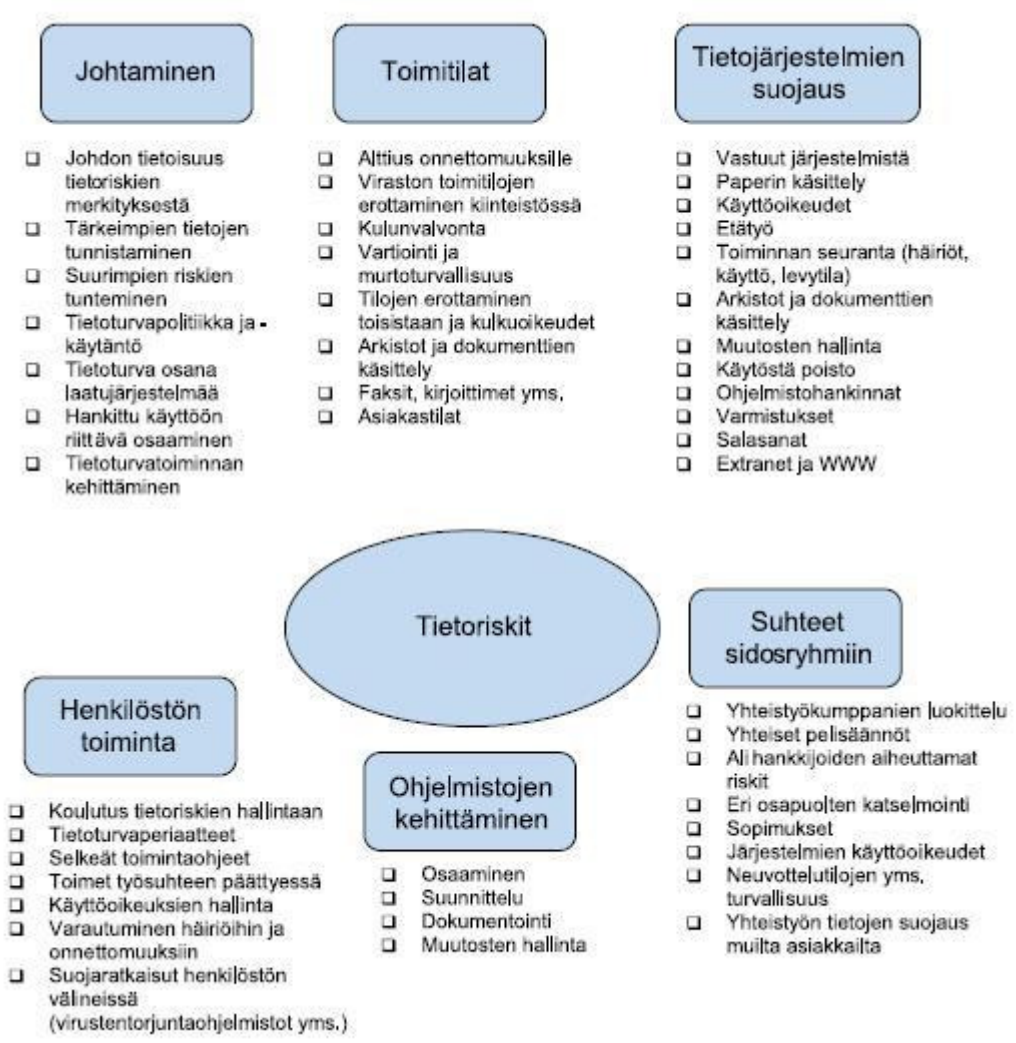
5.3.2 Pk-yrityksen haavoittuvuusanalyysi

Pk-yrityksen haavoittuvuusanalyysi on yksi Pk-yrityksen riskienhallinta- sarjan työvälineistä. Haavoittuvuusanalyysin työvälineisiin kuuluvat työkirjanen, opas menetelmän käyttöön sekä eri riskien tarkempaan määrittelyyn liittyvät työkortit ja taulukot (PK-RH, haavoittuvuusanalyysi).

PK-RH:n mukaan Pk-yrityksen haavoittuvuusanalyysi (Pk-HAAVA) on järjestelmällinen apuväline Pk-yrityksen toimintaan liittyvien riskien tunnistamiseen ja arviointiin sekä jatkossa kehittämistoimenpiteiden suunnitteluun. PK-HAAVAn riskikarttojen avulla saadaan nopeasti karkea kokonaiskuva yrityksen haavoittuvuuksista, eli yrityksen toiminnan jatkuvuuteen liittyvistä riskeistä.

Yrityksen toiminta jaetaan analyysin riskikartoissa kuuden osa-alueen kautta yli 30 alaluokkaan, joihin liittyviä uhkia analyysissä tarkastellaan esimerkkien avulla. Työssäni käytän pääasiallisesti PK-HAAVAn tietoriskeihin suunnattua riskikarttaa. PK-HAAVAn tietoriskikartta ei ole jäykkä tarkistuslista, jossa kaikki riskit olisi pyritty ennakolta kuvaamaan. Tarkoituksena on, että esimerkkien avulla Pk-yrityksessä itse selvitetään omaan toimintaan liittyvät riskit. Käytännössä on havaittu, että menetelmällä saadaan usein selville ongelmia, jotka voidaan helposti poistaa, kun asioita aletaan hoitaa. Toimenpiteet ovat toteutettavissa helposti, eivätkä ne aiheuta juurikaan kustannuksia. Osa ongelmista saattaa silti vaatia lisäselvityksiä, suunnittelua ja investointeja.

Alla esimerkkikuva PK-HAAVAn tietoriskikartasta.



Kuva 4. Esimerkki tietoriskikartasta (PK-RH, haavoittuvuusanalyysi).

PK-HAAVA koostuu seuraavista portaista:

1. Riskien tunnistaminen
2. Riskien arviointi ja priorisointi
3. Kehittämistoimenpiteiden suunnittelu, toteutus ja seuranta

(PK-RH, haavoittuvuusanalyysi.)

Työssäni käytän PK-haavaan tietoriskikartan ja riskienhallintatoimenpiteet -lomakkeen osalta, koska opinnäytetyöni kaksi riskienarviointi kohdistuu ainoastaan kahteen merkittävään IT-järjestelmään koko konsernin sijasta. Riskien tunnistaminen, arviointi ja priorisointi tehdään tästä syystä POA-menetelmällä, koska tarkoituksena on saada helpommin ja nopeammin tarkkoja tuloksia.

6 Tärkeimmät IT-järjestelmät

Organisaatio X:n toiminta kulminoituu pitkälti sähköisten IT-järjestelmien päivittäiseen käyttöön. Käytössä on useita tärkeitä ja merkittäviä järjestelmiä. Yrityksen merkittävämpiä IT-järjestelmiä ovat sähköposti, XaHa, konesalin palvelimet ja palvelinympäristöt, nimipalvelin, tietoliikenneyhteydet ja varmuuskopioinnin mahdollistava ohjelmisto ja palvelimet. Suurin osa merkittävimpien järjestelmien komponenteista on kahdennettu ja sen ansiosta itse laitteet eivät ole kovin riskialttiita. Kahdennettuja laitteita on esimerkiksi keskuskytkin, sähköpostipalvelin ja palomuuri. Laitteistoa testataan ennalta suunnitellulla tavalla useamman kerran vuodessa. Samalla testataan varalaitteisto.

7 Riskienarviointi ja haastattelut

Uutta riskienhallintamallia päätettiin kokeilla kahden merkittävän IT-järjestelmän riskienarvioinnin yhteydessä avulla. Riskienarvioinnin kohteiksi valittiin kaksi merkittävää IT-järjestelmää: Organisaatio X: asianhallintajärjestelmä (XaHA) ja konesalin palvelinympäristö.

7.1 XaHa

7.1.1 Järjestelmän kuvaus

Järjestelmän kuvaus on tehty Organisaatio X:n järjestelmäpäällikön haastattelun pohjalta. XaHa on sovellus, joka toteuttaa asiakirjojen tiedonhallintaa ja sen avulla voidaan ottaa talteen asian käsittelyyn liittyvät kirjaamistiedot ja asioiden käsittelyn vaiheisiin liittyvät toimenpidetiedot. Sitä käyttävät Kirjaamo ja Organisaatio X:n työntekijät omilta työpöydiltään. Tyypillinen asian käsittelyn kulku: asian avaus (Kirjaamo) asian toimenpiteet (Osasto) ja asian päätös (Kirjaamo). Toimenpiteiden suorittamiseksi voidaan perustaa tarvittaessa työnkulku, jota voidaan erikseen seurata. Sovelluksen edellä kuvattu osuus sisältää asiakirjojen elinkaaren, asian käsittelyhistorian ja arkistoinnin, sekä tarvittaessa seulonnan ja hävittämisen.

Tiedonhallinnan mekanismina on organisaation tehtäväluokitteluun perustuva asiakirjallisten prosessien hoitamisen suunnitelma (THS, myös nimeä Tiedonhallintasuunnitelma tai eAMS-käytetään), joka jakaa Organisaatio X:n työn pääryhmiin, tehtäväryhmiin ja ne edelleen asiaryhmiin (asian hoito) ja aiheryhmiin (aiheiden hallinta). Asiaryhmiin on mallinnettu asioiden hoitamisen prosessit. Aiheryhmiin on mallinnettu toiminnan tuloksena muuten kuin asian käsittelyssä syntyvät tai toiminnassa tarvittavat aineistot. Volyymiltaan Aiheenhallinta on suurin sovellusalue dokumenttien määrällä laskettuna.

Asian käsittelyä ja aiheenhallintaa varten THS sisältää tiedonhallinnan vaatimat oletusmetatiedot. XaHa-sovelluksessa on mekanismi, jolla suunnitellut metatiedot periytetään talteen otettavalle asiakirjalle silloin, kun valitaan sen konteksti (Aiheryhmä, Asiaryhmä) ja asiakirjan käyttötarkoitus (Asiakirjatyyppi). Perintämekanismi on XaHan tiedonohjausjärjestelmä (TOJ).

THS:n ohjaus voidaan ulottaa muihinkin sovelluksiin, jota asian käsittelyn yhteydessä tarvitaan.

Tiedon hallinnan lisäksi XaHa on seurantatyökalu ja sen avulla voidaan seurata yksittäisen asian käsittelyn vaiheita. XaHasta voidaan saada raportteina asiankäsittelyyn liittyviä tietoja käsittelyajoista, käsittelijöistä ja lukumääristä. Näitä tietoja voidaan käyttää mm. työjonojen hallintaan ja optimointiin.

XaHa on asian käsittelyn osalta roolipohjainen järjestelmä, jossa käyttörajoitukset on ulotettu asiakirjoihin saakka, jolla viime kädessä varmistetaan tiedon näkyminen juuri kyseistä tietoa tarvitseville käyttäjäryhmille ja käyttäjille.

Tavoitetilassa on saada Kansallisarkiston lupa pitkäaikaiseen sähköiseen säilyttämiseen, asian käsittelyn sähköistäminen sekä tiedon julkaisu Intranettiin ja käsittelyssä olevien asioiden perustietojen julkaisu e-diaarin muodossa Organisaatio X:n Web-palvelussa. THS:n ohjaus voidaan laajentaa koskemaan muitakin tietojärjestelmiä. Tiedon esittäminen intranetissä toimii, mutta eDiaari on vielä piirustuspöydällä.

XaHassa on selainkäyttöliittymä työpöytineen ja Windows-liittymä resurssienhallinnassa. Office-sovellusten tallennustoiminto mahdollistaa XaHa-talletuksen suoraan sovelluksesta. Myös Outlook sähköpostiin on liittymä. XaHaan voidaan tallettaa satoja erilaisia tiedostotyyppejä ja luoda eri tyypeille omat avausmetodit. Lisäksi on mahdollista käyttää XaHan kanssa muita Organisaatio X:n OpenText-ohjelmia (Järjestelmäpäällikön haastattelu, 2009).

7.1.2 XaHan riskianalyysi

XaHan riskianalyysi suoritettiin 19.10.2009. Riskianalyysiin tekemiseen osallistui tietoturvapäällikkö, järjestelmäpäällikkö, järjestelmäasiantuntija ja tietohallintosihteeri. Riskianalyysin projektipäällikkönä toimi Laurean turvallisuusalan opiskelija Matti Aitta. Tilaisuuden alussa esiteltiin käytettävä menetelmä, kohteen rajaus ja riskienhallinnan perustat lyhyesti. Riskienhallinta menetelmänä käytettiin Organisaatio X:n tietohallinto-osastolle räätälöityä mallia, joka on kuvattu ylempänä. Rajaus koski XaHaa ainoastaan järjestelmän osalta, joten tulipalot yms. jätettiin rajauksen ulkopuolelle, koska niitä on käsitelty jo muissa riskienarvioinneissa.

Muunneltu POA toteutettiin niin, että asiasanat heijastettiin seinälle kaikkien nähtäville. Asiasanoina käytettiin seuraavia: tiedot, kokemukset, asiantuntijat, sähköposti, arkistot, tietokoneiden tietokannat, ohjeet ja käsikirjat, tavallinen käyttäjä, tietomurto, koulutus, tahallinen väärinkäyttö, kahdentaminen ja varmuuskopiot.

Sen jälkeen työryhmän jäsenet kertoivat vuorotellen järjestelmän erilaisia riskejä, jotka kirjattiin ylös ja niistä keskusteltiin. Tilaisuus meni hyvin ja kaikki saivat vuorollaan puheenvuoron. Loppujen lopuksi työryhmä löysi n.40 riskiä.

Tärkeimmät löydetyt uhat olivat:

- Toimittajat ja heidän asiantuntemus
- Ohjelmassa mahdollisesti valmiiksi olevat virheet
- Toimittaja Y:n käytössä olevat henkilöresurssit
- Toimittaja Y:n riippuvuus muutamasta avainhenkilöstä
- Toimittaja Y ei testaa tuotetta riittävän kattavasti ennen toimittamista
- XaHan avainhenkilöt: yrityksessä vain kaksi ihmistä jotka ovat järjestelmän pääkäyttäjiä
    - Organisaatio X:n ylläpidon omat räätälöinnit XaHan suhteen
    - Organisaatio X:n ylläpidon jatkuvuus (jos kaikki avainhenkilöt ovat poissa, järjestelmään ei voida tehdä muutoksia.)
    - Järjestelmän hallittu alasajo ja ylösajo vaativat asiantuntijuutta
    - Organisaatio X:n tietohallinto-osaston ulkoistaminen
- Käyttäjät: kirjaajat voivat estää koko järjestelmän käytön muilta käyttäjiltä (rikkomalla THS-puun THS-työkalulla [THS = Tiedon Hallinta Suunnitelma].)
- Järjestelmän arkkitehtuuri - laitteita ei kahdennettu, mutta varmuuskopioitu
- Suorituskyky ja kapasiteetti (jos suorituskyky ei riitä, kaikkien käyttö estyy)
- Toimittaja Y menee konkurssiin
    - Suomessa ainoastaan yksi toimittaja kyseiselle järjestelmälle
- Työasemapakettien laatu (toimittaja Z oyj)
- XaHan pilotointi
- Palvelimeen ja tietotekniikkaan liittyvät riskit
- Tuotteen elinkaari - toimittajan tuki loppuu tuotantoversiolle
- Ylläpitosopimus tekemättä (jatkokehitystä)
- Löydetäänkö takuuaikana kaikki virheet (takuu 9 kuukautta, sen jälkeen korjaukset maksavat)
- Hakkerit ja virukset
- Saastuneen tiedoston tallentaminen käyttäjän oikeuksilla
- Käyttövaltuudet

Seuraavaan vaiheeseen ja tarkempaan tarkasteluun valittiin seuraavat uhat:

- Toimittajat ja heidän asiantuntemus
- Ohjelmassa mahdollisesti valmiiksi olevat virheet
- Toimittaja Y:n käytössä olevat henkilöresurssit

- Toimittaja Y:n riippuvuus muutamasta avainhenkilöstä
- Toimittaja Y ei testaa tuotetta riittävän kattavasti ennen toimittamista
- XaHan avainhenkilöt: yrityksessä vain kaksi ihmistä jotka ovat järjestelmän pääkäyttäjiä
    - Organisaatio X:n ylläpidon omat räätälöinnit XaHan suhteen
    - Organisaatio X:n ylläpidon jatkuvuus (jos kaikki avainhenkilöt ovat poissa, järjestelmään ei voida tehdä muutoksia.)
    - Järjestelmän hallittu alasajo ja ylösajo vaativat asiantuntijuutta
    - Organisaatio X:n tietohallinto-osaston ulkoistaminen
- Käyttäjät: kirjaajat voivat estää koko järjestelmän käytön muilta käyttäjiltä (rikkomalla THS-puun THS-työkalulla.)
- Järjestelmän arkkitehtuuri - laitteita ei kahdennettu, mutta varmuuskopioitu
- Suorituskyky ja kapasiteetti (jos suorituskyky ei riitä, kaikkien käyttö estyy.)

Työryhmä arvioi, että yllämainitut uhat ovat merkittävimmät ja niitä on syytä tarkastella lähemmin. Uhkia arvioitiin Pk-haavassa olevan kaavakkeen avulla (Liite 1). Ensiksi valittiin arvioitava uhka. Seuraavaksi mietittiin yhdessä, mistä uhka mahdollisesti voisi johtua, eli uhkat syyt. Tämän jälkeen arvioitiin uhkat pahimmat seuraukset, eli mitä uhkan realisoituminen voisi pahimmillaan aiheuttaa. Seuraavaksi arvioitiin riskiluokka uhkan suuruuden määrittelevän taulukon avulla (Kuva 3). Tämän jälkeen joko mietitään millä toimenpiteillä uhkia voitaisiin minimoida, jätetäänkö se jäännösriskiksi vai onko se jo hoidossa.

Seuraavassa avaan esille tulleet uhat.

Riski 1. Toimittajat ja heidän asiantuntemus.
Riskit: ohjelmassa valmiiksi olevat virheet, toimittaja ei testaa tuotetta riittävän kattavasti, toimittajan käytettävissä olevat henkilöresurssit ja toimittajan riippuvuus muutamasta avainhenkilöstä. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä: 4.
Organisaatio X:n XaHan toimittaa Toimittaja Y. Toimittaja Y on ainoa Suomessa toimiva yritys, joka toimittaa kyseistä järjestelmää. Työryhmä kyseenalaisti Toimittaja Y:n asiantuntemuksen, koska XaHassa on koekäytön, ja varsinaisen käytön aikana havaittu paljon virheitä, joista osa on ollut kriittisiä. Tästä johtuen Toimittaja Y:n asiantuntijat ovat joutuneet tulemaan Organisaatio X:n tiloihin tekemään tarvittavia korjauksia koodiin. Työryhmän mielestä järjestelmän tulisi olla käyttövalmiina ja testattuna jo toimitusvaiheessa. Jos järjestelmä tulee virheellisenä, lisää se työmäärää Organisaatio X:ssä. Järjestelmän ylimääräisen testaus ennen käyttöönottoa lisää työmäärää. Työryhmä uskoo, että ongelmat Toimittaja Y:n päässä johtuvat henkilöstöresurssien puutteesta ja siitä johtuvasta motivaation puutteesta testata järjestelmää. Vain muutama avainhenkilö toimittajan päässä osaa tehdä tarvittavia muokkauksia järjestelmään. Pahimmassa tapauksessa toimimaton ja testaamaton järjestelmä rik-

koontuu ja sinne tallennetut tiedot katoavat. Ratkaisuksi tähän ongelmaan työryhmä määrittelisi jatkossa sopimukseen sanktioita, jos järjestelmä ei toimi sovitulla tavalla. Toimittajan taas tulisi testata järjestelmää enemmän omatoimisesti ennen sen toimittamista.

Riski 2. XaHan avainhenkilöt Organisaatio X:ssä, Organisaatio X:n ylläpidon omat räätälöinnit XaHan suhteen, ylläpidon jatkuvuus. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Organisaatio X:n omat XaHa asiantuntijat ovat jatkoräätälöineet XaHaa yrityksin omiin tarpeisiin. XaHaa on mm. räätälöity yhteensopivaksi muiden organisaation ohjelmien, palveluiden ja palvelimien kanssa. Tehtyjä muutoksi ei ole dokumentoitu kunnolla, joten ainoastaan organisaation kaksi asiantuntijaa ovat täysin tietoisia tehdyistä muutoksista. Jos nämä henkilöt eivät ole paikalla ja jotain menee vikaan, kukaan muu kuin Toimittaja Y:n asiantuntija ei voi auttaa.
Jos kaikki avainhenkilöt ovat poissa, ei järjestelmään voida tehdä muutoksia.

Organisaatio X:n järjestelmän hallittu alasajo ja ylösajo vaativat asiantuntijuutta.

XaHa ajetaan alas neljä kertaa vuodessa kvartaalipäivitysten, tarpeellisten päivitysten- tai huoltotöiden yhteydessä. XaHan pystyy ajamaan alas/ylös ja päivitykset hoitamaan ainoastaan XaHan avainhenkilö tai Toimittaja Y:n asiantuntija. Näin ollen avainhenkilöiden puuttuminen johtaisi siihen, ettei järjestelmää voitaisi päivittää tai huoltaa, tai mahdollisen kaatumisen jälkeen ajaa takaisin toimintakuntoon.

Organisaatio X:ssä on ollut puhetta siitä, että tietohallinto-osasto ulkoistettaisiin organisaatiomuutoksen yhteydessä. Näin ollen yritykseen ei jäisi yhtään XaHa avainhenkilöä. Ongelmaksi muodostuisi se, että kaikki yllä mainitut uhat voisivat toteutuessaan johtaa toiminnan keskeyttämiseen. Jos tietohallinto-osasto ulkoistettaisiin, tehtäisiin sopimus Toimittaja Y:n kanssa asiantuntijapalveluista. Työryhmän mukaan ongelmaksi tässä muodostuu se, että sen voi ulkoistaa ainoastaan Toimittaja Y:lle. Tämä muodostaisi uudenlaisen riskin koska toimittajan tuki on erittäin epävarmaa ja reagointiaika on pitkä verrattuna omiin asiantuntijoihin.

Toimenpiteeksi riskiin 2 työryhmä totesi, että oma asiantuntevuus on välttämätön, tai sopimuksessa pitää määritellä korvaava toimintatapa.

Riski 3: käyttäjät. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3. Käyttäjäryhmä Kirjaajat voivat estää koko järjestelmän käytön muilta käyttäjiltä. Tiedostonhallinta työkalulla he pystyvät tekemään muutoksia, eli käytännössä he pystyvät tuhoamaan tiedosto - ja kansiorakenteet joko vahingossa tai tahallaan. Jos näin käy, tiedostot pystytään

useimmiten palauttamaan muutamassa tunnissa. Tämä riski on joskus toteutunut organisaatiossa.
Xaha-järjestelmään tämä vaikuttaa seuraavasti: XaHan käyttö estyy ja joudutaan palaaman edellisen illan tilanteeseen - asiat joudutaan perustamaan uudestaan ja dokumentit joudutaan kohdistamaan aiheryhmään.
Toimenpiteeksi riskiin 3 työryhmä ehdottaa kirjaajien työkalujen kehittämistä ja lisäkoulutusta.

Riski 4. Järjestelmän arkkitehtuuri: laitteita ei ole kahdennettu, mutta ne on varmuuskopioitu. Todennäköisyys: mahdollinen. Seuraukset: haitalliset. Riskiryhmä 3.
Työryhmän mukaan laitteita ei ole kustannustehokasta kahdentaa, vaan pelkkä hyvin hallittu varmuuskopiointi riittää. Laiterikko aiheuttaisi hetkellisen käyttökatkon ja tiedostot pitäisi palauttaa. Vastaava laite rikkimenneen tilalle saataisiin jo muutamassa tunnissa. Laiterikkoa ei muutenkaan pidetä kovin todennäköisenä, joten laitteiston kahdentaminen ja kaksien laitteiden päivittäminen tulisi merkittävän kalliiksi riskiin nähden.
Toimenpiteeksi riskiin 4 työryhmän mukaan riittää se, että järjestelmän tiedot varmuuskopioidaan järjestelmällisesti.

Riski 5. Suorituskyky ja kapasiteetti. Todennäköisyys: mahdollinen. Seuraukset: vähäiset. Riskiryhmä 2.
Aikaisemman järjestelmän, DoHan (DoHa = Dokumentin hallinta), jonka XaHa korvaa, yhteydessä Toimittaja Y ilmoitti tietyt laitevaatimukset, joilla DoHan pitäisi toimia. Organisaatio X oletti, että heidän laitteistonsa suorituskyky ja kapasiteetti riittäisivät myös XaHan pyörittämiseen. Olettamus johtui siitä, että DoHa oli raskaampi järjestelmä. Ongelmia kuitenkin ilmeni XaHan kanssa ”time out” häiriöilmoituksina. Syyksi toimittaja Y ilmoitti, että jos käyttäjät ajavat liian montaa XaHa sovellusta samaan aikaan, ei laitteiston suorituskyky riitä. Käytännössä Toimittaja Y ilmoitti Organisaatio X:n laitteistojen olevan riittämättömät vasta järjestelmän toimittamisen jälkeen.

Syyksi tähän työryhmä arvioi sen, että Toimittaja Y ei ollut huomioinut datan määrän kasvua testeissään. Toimittaja Y:n asiantuntijat eivät olleet arvioineet minkälaista kapasiteettiä järjestelmä tulee vaatimaan.
Toimenpiteeksi riskiin 5 Organisaatio X:än on tilattu uusi tietokantapalvelin. Ohjeistusta XaHan käytössä tulisi lisätä ja menettelytapoja muuttaa kevyempään suuntaan. Kaikkein kuormittavinta tiedostonhallintatyökalua pyritään käyttämään virka-ajan ulkopuolella, jottei muiden käyttäjien XaHan käyttö hidastuisi.

Riski 6. Toimittaja Y menee konkurssiin. Todennäköisyys: epätodennäköinen. Seuraukset: vähäiset. Riskiryhmä 1.

Toimittaja Y on Suomen ainut toimittaja kyseiselle järjestelmälle. Jos yritys menisi konkurssiin, toimittajan tuki XaHalle loppuisi. Työryhmän mukaan tämä on kuitenkin epävarmaa, koska toimittaja toimii myös kuudessa muussa maassa ja sen toiminta on varmalla pohjalla. Sillä on paljon asiakkaita ja liikevaihto on suuri.
Ei vaadi toimenpiteitä.

Riski 7. Työasemapakettien laatu. Todennäköisyys: epätodennäköinen. Seuraukset: vähäiset. Riskiryhmä 1.
Toimittaja Z toimittaa kaikki Organisaatio X:n ohjelmistopaketit. Organisaatio X:ssä ohjelmat asennetaan kaikkiin koneisiin keskitetysti, koska se on nopeampaa ja helpottaa versioiden hallintaa. Toimittaja Z toimittaa ohjelmistopaketit, mistä Organisaatio X asentaa ne keskitetysti. Välillä näissä ohjelmistopaketeissa on ollut virheitä, jotka ovat estäneet XaHan käytön tai kaataneet koko järjestelmän. Vika saadaan korjattu nopeasti uudella päivityksellä, mutta saattaa aiheuttaa useamman tunnin katkoksen joillakin työasemilla ja tietoja saatetaan menettää.
Toimenpiteeksi riskille 6 työtyhmä ehdottaa, että Toimittaja Z sopimuksiin lisätään kohta sanktioista jos näin vielä tulee käymään.

Riski 8. XaHan pilotointi. Todennäköisyys: epätodennäköinen. Seuraukset: vähäiset. Riskiryhmä 1.
XaHaa ei saada aikatauluun mennessä asennettua ja testattua, eivätkä käyttäjät opi käyttämään sitä.
Riski ei toteutunut.

Riski 9. Palvelimeen ja tietotekniikkaan liittyvät riskit. Todennäköisyys: mahdollinen. Seuraukset: vähäiset. Riskiryhmä 2.
Riskiä on käsitelty muun riskienhallinnan yhteydessä. Riskiä on minimoitu mm. huoltosopimuksilla ja kahdentamisilla. Riski on minimoitu pieneksi ja toteutuessaan saattaisi aiheuttaa käyttökatkon XaHan toimintaan. Ei vaadi lisätoimenpiteitä.

Riski 10. Tuotteen elinkaari. Todennäköisyys: epätodennäköinen. Seuraukset: vähäiset. Riskiryhmä 1.
Toimittaja Y:n tuki loppuu tuotantoversiolle. Tämä ei tule toteumaan vielä moneen vuoteen ja siinä vaiheessa vaihdetaan järjestelmää, toimittajaa tai ostetaan uusi versio.

Riski 11. Takuuaika. Todennäköisyys: epätodennäköinen. Seuraukset: vähäiset. Riskiryhmä 1.
Löydetäänkö takuuaikana kaikki virheet? Takuu kestää yhdeksän kuukautta ja sen jälkeen korjaukset maksavat. Työryhmän mielestä yhdeksässä kuukaudessa kaikki kriittisimmät virheet löytyvät. Ei vaadi lisätoimenpiteitä.

Riski 12. Hakkerit ja virukset.
Riskiä on käsitelty muun riskienhallinnan yhteydessä. Asia on hoidettu niin fyysisellä palomuurilla kuin jokaiselta työasemalta löytyvällä ohjelmisto-pohjaiselta virustorjunnalta. Ei vaadi lisätoimenpiteitä.

Riski 13. Saastuneen tiedoston tallentaminen käyttäjän oikeuksilla.
Mahdollista, mutta epätodennäköistä. Virustorjuntaohjelma tunnistaa saastuneen tiedoston ennen tallennusta. Ei vaadi lisätoimenpiteitä.

Riski 14. Käyttövaltuudet.
Riski syntyy, jos käyttäjälle määritellään vahingossa pääkäyttäjän oikeudet. Organisaatio X:ssä on tiukka käyttöoikeuksienhallintapolitiikka ja sitä valvotaan. Ei vaadi lisätoimenpiteitä.

7.2 Konesalin palvelinympäristö

7.2.1 Järjestelmän kuvaus

Järjestelmän kuvaus perustuu Organisaatio X:n järjestelmäasiantuntijan haastatteluun.

Konesali on palvelinkoneiden keskittymä ja siellä sijaitsevat myös tietoliikenteen solmukohdat. Konesali on erikseen ilmastoitu ja sen sähkön saanti on varmistettu. Konesali on suojattu fyysisillä hälytinlaitteilla, kulunvalvonnalla sekä automaattisella palonilmoitin- ja sammutinlaitteistolla.
Palvelinkoneet jakavat palveluita niitä tarvitseville käyttäjille ja koneille. Palvelinkoneiden tärkeimmät palvelut ovat: levyjakopalvelut, ohjelmistopalvelut, käyttäjätunnistuspalvelut ja yhteiskäytäntöpalvelut.
Konesalissa sijaitsee 18 fyysistä palvelinta, joiden sisällä toimii 130 virtuaalista palvelinta.

Palvelinympäristö tarkoittaa sitä massaa joka koostuu palvelinkoneista ja niiden tuottamista palveluista.

Virtuaalipalvelin on ohjelmallisesti tuotettu palvelinkone jonka päällä toimii käyttöjärjestelmä. Sen sisällä toimii varsinaiset palvelut. Jotta voidaan pitää yllä virtuaalipalvelimia, pitää olla minimissään yksi fyysinen palvelin. Fyysisessä palvelimessa voidaan pyörittää x määrää virtuaalisia palvelimia. VM ware exm -ympäristö toimii käyttöjärjestelmänä virtuaalisille järjestelmille.

Virtuaalisten palvelinten käyttäminen säästää aikaa, rahaa ja vaivaa. 50:tä virtuaalista palvelinta voidaan pyörittää 6 fyysisen laitteen sisällä (Järjestelmäasiantuntija haastattelu, 2009).

7.2.2 Konesalin riskikartoitus

Konesalin riskianalyysi aloitettiin 2.10.2009 riskikartoituksen merkeissä. Riskianalyysista tehtiin tarkoituksenmukaisesti kaksiosainen: ensiksi kartoitettiin ja tunnistettiin riskit ja seuraavassa palaverissä ne arvioitiin ja analysoitiin. Riskianalyysiin osallistui tietoturvapäällikkö, järjestelmäpäällikkö ja kaksi järjestelmäasiantuntijaa. Riskianalyysin projektipäällikkönä toimi Laurean turvallisuusalan opiskelija Matti Aitta. Tilaisuuden alussa esiteltiin käytettävä menetelmä, kohteen rajaus ja riskienhallinnan perustat lyhyesti. Riskienhallinta menetelmänä käytettiin Organisaatio X:n tietohallinto-osastolle räätälöityä mallia, joka on kuvattu ylempänä. Rajaus koski periaatteessa koko konesali, koska sen rajaaminen pelkkään konesalin palvelinympäristöön olisi jättänyt pois oleellisia riskejä ja uhkia.

Muunneltu POA toteutettiin niin, että asiasanat heijastettiin seinälle kaikkien nähtäville. Asiasanoina käytettiin seuraavia: Tulipalo, vesivahinko, laiterikko, pitkäkestoinen sähkökatkos, tietokonevirusepidemia, tietojärjestelmän valtaus, sabotaasi, yrityskuvan vahingoittuminen, yksilön työmotivaation häiriöt ja työetiikan mureneminen, tiedon eheyden menetys, tiedon paljastuminen, tietosuojan rikkoutuminen, tallenteen menettäminen, laitteen menettäminen, oheislaiterikko, levyrikko, ohjelmiston vakava toimintavirhe, laitteiston vakava toimintavirhe, käyttöoikeusrikkomus ja laitevarkaus.

Sen jälkeen työryhmän jäsenet kertoivat vuorotellen järjestelmän erilaisia uhkia, jotka kirjattiin ylös ja niistä keskusteltiin. Tilaisuus meni hyvin ja kaikki saivat vuorollaan puheenvuoron. Loppujen lopuksi työryhmä löysi n.30 uhkaa.

Löydetyt uhat olivat:

- Konesalin fyysinen palvelinympäristö
    - Ilmastointi
    - vesisammutus
    - tulipalo
    - vesivahinko
- Kulunvalvonta. Sisäinen henkilöriski. Avaimia ei ole montaa
- Sisäinen henkilöriski, sabotaasi
- Palvelunestohyökkäykset
- Hakkerointi
- Virukset
- Roskaposti
- Tiedon eheys, varmistaminen ja palautukset
    - Laiterikot

    - Laitteiston ikä. Laitteistolle pitäisi määritellä maksimi käyttöikä, jotta vaihtaminen uudempaan sujuisi mutkattomasti
- Ohjelmistojen päivitykset, esimerkiksi Open Text
- Palvelinten päivitykset, erityisesti firmwaret (laiteohjelmat)
    - Tietoturvapäivitykset, varsinkin jos tulee toimimaton tai viallinen päivitys
- Käytön valvonta
- Integroituvuus hankaloittaa toimintaa
- Riippuvuus avainhenkilöistä
    - Dokumentaation puute. Varmistuksista puuttuu.
- Palvelujen maantieteellisen kahdennuksen puute. Eri pisteissä tapahtuva kahdennus
    - Huonosti toimiva kahdennus voi olla riski
- Toimittajan tuen puuttuminen ja laatu
    - Huoltosopimusten puuttuminen ja sopimusten huono sanktiointi & sopimuspykälät
- Jäädytetyt järjestelmät.
- Käyttöoikeuspolitiikka
- Tietoverkonsegmentoinnin puute
- Verkon solmupisteiden kriittiset komponentit joita ovat: palomuuri, hakemistopalvelu, keskuskytkimet, internetyhteys ja levyjärjestelmät
- Sähkönsyöttö ja virranvarmistus mukaan lukien UPS (UPS= Uninterruptible Power Supply. Suom. katkoton virtalähde.)
- Ohjelmisto ongelmat.
- Henkilöstön osaamattomuus
- Laitteistojen kahdennuksen puute.
- Automaattinen valvonta on puutteellista

Kriittiset uhat jotka valittiin riskianalyysin kohteeksi:

Riski 1. Konesalin fyysinen palvelinympäristö. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3.
Konesalin fyysiseen palvelinympäristöön kohdistuu monenlaisia riskejä. Suurimmiksi riskeiksi katsottiin: ilmastoinnin vioittuminen, vedellä toimiva sprinklerijärjestelmä, vesivahinko ja tulipalo. Riski toteutuu todennäköisemmin seuraavien skenaarioiden kautta. Jos serveri kärähtää ja ilmastointi pettää, saattaa se aiheuttaa mahdollisen tulipalon. Sprinklerit sammuttavat tulipalon, mutta aiheuttavat samalla vesivahingon. Vesivahinko saattaa aiheutua myös rikkoutuneesta putkesta. Pahimmillaan tämä voi aiheuttaa sen, että konesali tuhoutuu täysin ja tiedot katoavat ja toiminta keskeytyy pitkäksi aikaa. Toimenpiteeksi työryhmä ehdotti sammutusjärjestelmän vaihtamista elektroniikka ystävällisemmäksi.

Riski 2. Sisäinen henkilöriski, sabotaasi & kulunvalvonta. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3.
Henkilökunta voi omalla toiminnallaan joko ennaltaehkäistä tai välillisesti tai välittömästi aiheuttaa melkein minkä tahansa riskien toteutumisen. Jos henkilökuntaa päättää tahallisesti tehdä jotain, on sitä käytännössä mahdotonta estää tapahtumasta millään turvajärjestelyillä. Henkilökunnan tulisi myös tarkemmin katsoa, ketä he päästävät taloon sisään ja kuinka he valvovat omia vieraitaan. Pahimmillaan kyseinen riski voi aiheuttaa melkein mitä vaan aina henkilövahingoista, tiedon tuhoutumiseen ja toiminnan keskeytymiseen. Työryhmän mielestä tätä olisi parasta ennaltaehkäistä panostamalla henkilökunnan hyvinvointiin ja viihtyvyyteen työpaikalla. Esimiehillä on myös iso rooli siinä, miten heidän alaisensa töissä viihtyvät. Esimiehet voivat myös tarkkailla alaisiaan ja etsiä merkkejä epäilyttävästä käytöksestä. Organisaatio X:ssä on myös tapana tehdä kaikille tietohallinnon työntekijöille suppea turvallisuusselvitys.

Riski 3. Palvelunestohyökkäykset. Todennäköisyys: mahdollinen. Seuraukset: haitalliset. Riskiryhmä 3.
Palvelunestohyökkäys (DoS = Denial of Service) tarkoittaa sitä, että talon ulkopuolinen taho hyökkää sen verkkoa vastaan tuhansien kaapattujen tietokoneiden armeijalla tarkoituksenaan kuormittaa verkkoa niin paljon, että sen käyttö estyy. Pahimmillaan tämä saattaa aiheuttaa sen, että sähköpostin lähetys estyy, tietoliikenneyhteydet eivät toimia ja palomuuri kaatuu ylikuormittumisen seurauksena. Organisaatio X:n internetsivusto toimii erillisellä palvelimella, joten se ei ole vaarassa kaatua, vaikka itse organisaation verkkoa vastaan hyökättäisiin. Organisaatio X:llä on käytössä yhden gigabitin yhteys, joten verkon kaatuminen ja tietoliikenneyhteyksien menettäminen ei ole todennäköistä. Todennäköisesti palvelunestohyökkäys aiheuttaa vain hidastuneen ulos- ja sisäänpäin kulkevan liikenteen hidastaen näin jokapäiväistä toimintaa. Työryhmä ehdottaisi, että yritykseen hankittaisiin tunkeutumisenestojärjestelmä (IPS = Intrusion prevention system).

Riski 4. Hakkerointi. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3.
Riskinä on se, että talon ulkopuolinen taho pääsee organisaation sisäverkkoon joko tietoturva-aukkoa hyväksikäyttäen, henkilökunnan virheen kautta tai tunkeutumalla itse yritykseen. Jos joku pääsee tunkeutumaan organisaation sisäverkkoon, voi hän käytännössä tehdä mitä vain. Pahimmillaan hän voi varastaa tietoja ja saastuttaa työpisteitä esimerkiksi viruksilla tai troijalaisilla. Työryhmän mukaan tämä voidaan parhaiten estää panostamalla kulunvalvontaan, kouluttamalla henkilökuntaa ja asentamalla aina uusimmat kriittiset tietoturvapäivitykset.

Riski 5. Virusepidemia. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Riski syntyy, kun virusten kehittelijät keksivät uuden virustyypin, jota uusimmat virustorjuntaohjelmat eivät kykene havaitsemaan. Tällöin virus pääsee leviämään ja saastuttamaan yri-

tyksen tietokoneet. Pahimmillaan tämä aiheuttaa sen, että tiedot saastuvat, tuhoutuvat tai joutuvat vääriin käsiin. Työryhmän mielestä parhaiten viruksia vastaan voitaisiin suojautua monitasoisella virussuojauksella, kouluttamalla henkilökuntaa ja ohjeistamalla heitä olemaan avaamatta liitetiedostoja tai menemään epäilyttäville sivustoille.

Riski 6. Roskaposti. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3. Roskaposti on yleisesti mainostajien käyttämä tapa saavuttaa miljoonia kuluttajia hetkessä. Roskaposti saattaa myös sisältää viruksia ja pahimmillaan se voi tukkia sähköpostijärjestelmän. Tätä varten roskapostin lähettäjät tarvitsevat tuhansia koneita ns. roskapostipalvelimiksi. Itse roskapostin saaminen ei ole Organisaatio X:lle ongelma, vaan se, että heidän koneensa saastuvat ja ne valjastetaan roskapostipalvelimiksi. Tästä voi pahimmillaan seurata mustalle listalle joutuminen, joka tarkoittaa käytännössä sitä, ettei Organisaatio X:n verkosta pääse tietyille sivuille eikä Organisaatio X pysty lähettämään sähköpostia. Riskin minimoimiseksi työryhmä ehdottaa kaikkien muiden järjestelmien kuin sähköpostipalvelimen SMTP:n (simple mail transfer protocol) pääsemistä ulospäin palomuurin avulla.

Riski 7. Tiedon eheys, varmistaminen ja palautukset. Laiterikot. Laitteiston ikä. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Tiedon eheys, varmistaminen ja palauttaminen ovat yritykselle elintärkeitä asioita. Näiden vaarantuminen saattaa aiheutua esimerkiksi laiterikosta tai vanhentuneesta laitteistosta. Pahimmillaan riskin toteutuminen aiheuttaa sen, että tietoa katoaa, se muuttuu eikä sitä voida enää palauttaa. Työryhmän mielestä varmistuksen ja palautukset tulee saattaa ajantasalle ja ne tulee testata. Myös THS tulee päivittää. Henkilökunnan kouluttaminen ja ohjeistaminen pienentää myös riskiä. Laiterikkoja varten palvelimiin on asennettu ennakoiva seuranta (DFS = Distributed File System) joka ilmoittaa, jos laitteisto käyttäytyy oudosti tai on hajoamassa.

Riski 7. Ohjelmistojen päivitykset. Todennäköisyys: todennäköinen. Seuraukset: haitalliset. Riskiryhmä 4.
Palvelimia pitää päivittää jatkuvasti, jotta niiden tietoturvallisuus ja toiminta voidaan taata. Riskin aiheuttaa se, jos tulee viallinen tai toimimaton päivitys. Jos riski realisoituu, saattaa se aiheuttaa tiedon katoamista, toiminta- ja käyttökatkoja. Organisaatio on varautunut näihin niin, että se asentaa välittömästi vain kriittiset päivitykset ja näin ollen ottaa riskin viallisesta tai toimimattomasta päivityksestä. Muiden päivitysten kohdalle odotetaan, että muualta tulee varmistus, että päivitys on turvallinen ja toimivaa. Ratkaisuksi tähän ongelmaan työryhmä haluaisi testata päivityksiä testiympäristössä ja varmistaa tiedot ennen varsinaista päivittämistä.

Riski 8. Käytön valvonta. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.

Organisaatio X:n tiloissa käy päivittäin monia talon ulkopuolisia toimijoita, esimerkiksi konsultteja, joilla on pääsy kriittisiinkin tiloihin. Riskin aiheuttaa se, ettei konsulttia valvota ja he saattavat tehdä järjestelmään muutoksen tietämättä mihin kaikkeen se vaikuttaa. Pahimmillaan se voi aiheuttaa tiedon tuhoutumista ja käyttökatkoksia. Ulkopuolinen taho voi myös tahallaan saastuttaa organisaation järjestelmän ja valjastaa sen lähettämään haittaohjelmia. Tämä taas saattaa tahrata Organisaatio X:n maineen. Työryhmän mielestä tämä ongelma voitaisiin välttää kouluttamalla ja ohjeistamalla henkilökuntaa vierailijoidensa valvonnassa.

Riski 9. Integroituvuus hankaloittaa toimintaa. Todennäköisyys: mahdollinen. Seuraukset: haitalliset. Riskiryhmä 3.
Kun puhutaan servereistä, järjestelmistä ja niihin liittyvistä ohjelmista ja komponenteista, kaikki liittyvät jollain tavalla toisiinsa. Jos yksikin osa putoaa pois pelistä, ei välttämättä enää mikään toimi. Koska kaikki on integroitua, ei kukaan voi täysin varmuudella tietää miten kaikki liittyy toisiinsa. Testaaminen ja hyväksyminen on monitasoista. Pahimmillaan väärän muutoksen tekeminen saattaa aiheuttaa toiminta- ja käyttökatkoja tärkeissä tietojärjestelmissä. Monitasoisesti integroidun järjestelmän ylläpitäminen ja päivittäminen on monimutkaista. Työryhmä ei osannut keksiä mitään ratkaisua tälle asialle, joten tämä asia jätetään jäännösriskiksi ja sen kanssa eletään.

Riski 10. Henkilöriippuvuus avainhenkilöistä. Todennäköisyys: epätodennäköinen. Seuraukset: haitalliset. Riskiryhmä 2.
Riippuvuus avainhenkilöistä johtuu dokumentaation puutteesta ja siitä, että Organisaatio X ylläpitää omia järjestelmiään. Jos avainhenkilö on tavoittamattomissa ja jotain tapahtuu, ei järjestelmää välttämättä saada palautettua tai sen palauttaminen ainakin hidastuu merkittävästi. Työryhmän mielestä tätä varten tuli laatia varamiesjärjestelmä, kouluttaa enemmän henkilökuntaa ja tehdä ylläpito- ja tukisopimuksia järjestelmien toimittajien kanssa.

Riski 11. Palvelujen maantieteellisen kahdennuksen puute. Todennäköisyys: epätodennäköinen. Seuraukset: vakavat. Riskiryhmä 3.
Organisaatio X ei ole kahdentanut palvelujaan maantieteellisesti kahteen paikkaan, vaan kaikki toimii keskitetysti yrityksen päätoimipisteestä. Riskin muodostaa se, että jos yrityksen päätoimipiste vaurioituu tai toiminta keskeytyy, keskeytyvät myös kaikki palvelut. Työryhmän mielestä vähintään kriittiset palvelut tulisi kahdentaa maantieteellisesti myös yrityksen toiseen toimipisteeseen, mutta tällä hetkellä se ei ole mahdollista resurssien puutteesta johtuen.

Riski 12. Toimittajan tuen puuttuminen ja laatu. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.

Jos jokin järjestelmä ei toimi oikein tai kunnolla, saatetaan tarvita asiantuntija apua ulkopuolelta. Ulkopuolinen apu on kallista eikä laatu aina vastaa odotuksia. Asia saataisiin korjattua lisäämällä uusiin sopimuksiin huoltosopimus pykälä, joka pakottaisi toimittajan tuottamaan stabiilimpia ohjelmia ja laitteita, jotta huoltoa ei edes tarvittaisi. Jos huoltoa taas tarvittaisiin, pitäisi toimittajan tietyn ajan sisällä suorittaa se ilmaiseksi tai edullisempaan hintaan. Sopimuksiin tulisi myös lisätä pykälä sanktioista: jos ohjelma tai laite menee epäkuntoon, tulee se saattaa kuntoon tietyn ajan sisällä, tai toimittajaan kohdistetaan ennalta määrättyjä sanktioita.

Riski 13. Jäädytetyt järjestelmät. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Jäädytetyt järjestelmät ovat vanhoja järjestelmiä, jotka ovat olemassa vain tiettyä toimintoa varten. Jäädytettyjä järjestelmiä ei päivitetä, joten niiden käyttö on tietoturvariski itsessään. Ongelmia tuottaa tulevaisuudessa myös yhteensopivuusongelmat. Ongelmaksi tähän riskiin työryhmä haluaisi päivittää vanhat järjestelmät uusiin, mutta se ei ole mahdollista resurssien puutteen vuoksi.

Riski 14. Käyttöoikeuspolitiikka. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Tiettyihin järjestelmiin on vain yksi administraattori käyttäjätunnus, jota käyttää useampi henkilö. Jos joku käyttäjistä tekee jotain, on häntä mahdotonta jäljittää. Ensinnäkään ei voida varmuudella todeta kuka on ollut sillä hetkellä kirjautuneena sisään, toisekseen administraattori tunnuksilla pystyy tehokkaasti pyyhkimään omat jälkensä. Näin ollen administraattori tunnukset tietävä käyttäjä voi tuhota tai muuttaa tiedostoja jälkiä jättämättä. Paras ratkaisu tähän ongelmaan olisi määrittää jokaiselle administraattori tason käyttäjälle omat, henkilökohtaiset käyttäjätunnukset.

Riski 15. Tietoverkonsegmentoinnin puute. Todennäköisyys: mahdollinen. Seuraukset: vakavat. Riskiryhmä 4.
Tietoturvasegmentoinnin puute on tietoturvauhka palvelinlaitteille. Uhkan muodostaa se, etteivät palvelimet ole omassa palomuurisegmentissään, vaan samassa verkkosegmentissä kuin loppukäyttäjien työasemat. Pahimmilla tämä voi aiheuttaa sen, että saastunut työasema saastuttaa esim. palvelinverkon jossa kaikki tieto sijaitsee. Työryhmän mukaan tämän ongelman saisi ratkaistua erottamalla palvelin- ja työasemaverkot toisistaan palomuuritasolla.

Riski 16. Verkon solmupisteiden kriittiset komponentit. Todennäköisyys: mahdollinen. Seuraukset: haitalliset. Riskiryhmä 3.
Verkon solmupisteiden kriittisiä komponentteja ovat: palomuuri, hakemistopalvelu, keskuskytkimet, internetyhteys ja levyjärjestelmät. Jos jokin näistä vaurioituu, tietojärjestelmät

eivät toimi ja tietoliikenneyhteydet katkeavat. Työryhmän mukaan kaikki muut paitsi internetyhteys on kahdennettu, joten resursseihin nähden tämä riski on erinomaisessa kunnossa.

Muut esille tulleet riski:

Riski 17. Sähkönsyöttö ja virranvarmistus.
Konesali on UPSi, eli akkuvarmistettu. Jos Organisaatio X:stä katkeaa sähköt, siirtyvät serverit toimimaan välittömästi varavirralla. Puoli minuuttia sähköjen katkeamisen jälkeen käynnistyy talon ulkopuolella sijaitseva dieselgeneraattori joka tuottaa sähköä Organisaatio X:lle. Niin kauan kuin dieseliä riittää ja generaattoria toimii, riittää myös sähköä. Näin ollen sähkönsyöttö ja virranvarmistus ovat kunnossa.

Riski 18. Ohjelmisto ongelmat.
Ohjelmistojen puutteelliset tai vialliset päivitykset voivat olla ongelma. Työryhmä ei kuitenkaan koe tätä isoksi riskiksi, koska päivitykset asennetaan vasta kun toinen taho on hyväksynyt ne. Ainoastaan kriittiset päivitykset asennetaan välittömästi ja silloin hyväksytään se riski että se voi olla viallinen.

Riski 19. Henkilöstön osaamattomuus.
Henkilökunta ei tiedä mitä tekee tai tekee jotain tahattomasti väärin osaamattomuuttaan. Työryhmän mielestä tämä ei ole riski, koska Organisaatio X:n tietohallinnon osaston työntekijät ovat oman alansa ammattilaisia.

Riski 20. Laitteistojen kahdennuksen puute.
Työryhmän mukaan tämä ei ole riski, koska melkein kaikki kriittinen on kahdennettu. Ainoastaan blade intra ja internetyhteys ovat kahdentamatta. Näiden kahdentaminen olisi iso kustannus ja riski niiden rikkoontumisesta on pieni.

Riski 21. Automaattinen valvonta on puutteellista.
Työryhmän mukaan näin ei ole. Automaattista valvontaa hoidetaan ohjelmilla: neteye ja hpsim.

8 Pohdintaa

Työssäni vastattiin asetettuun tutkimuskysymykseen, eli Organisaatio X:n riskienhallintamallia onnistuttiin kehittämään parempaan suuntaan. Organisaatiolla käytössä ollut riskienhallintamalli oli toimiva, mutta sen käyttö koettiin hankalaksi. Riskienhallintamallia muokattiin ja yksinkertaistettiin. Uudella riskienhallintamallilla päästään samaan lopputulokseen kuin vanhalla, mutta ilman turhaa, ja hyödyttömäksi koettua numeerista dataa. Uutta riskienhallinta-

mallia on helpompi käyttää, eikä myöskään riskienhallintaan osallistuva työryhmä koe tilaisuutta yhtä raskaaksi kuin vanhassa mallissa.

Uutta riskienhallintamallia kokeiltiin kahden merkittävän IT-järjestelmän riskienarvioinnin yhteydessä ja palaute prosessista oli positiivista. Riskien tunnistaminen ja niiden arvioinnin eriyttäminen eri palavereihin koettiin hyväksi ratkaisuksi. Ihmiset jaksoivat keskittyvä ja päästä parempiin tuloksiin.
Organisaatio X ottaa käyttöön uuden riskienhallintamallin ja sen avulla arvioidaan kaikkien tietohallinto-osaston merkittävien järjestelmien ja prosessien riskit uudestaan.

Kahden merkittävän IT-järjestelmän riskienhallinnan tekemisen yhteydessä organisaation suurimmiksi riskeiksi löydettiin avainhenkilöt ja heidän osaamiseensa liittyvä dokumentaation puute.

Organisaatio X:n riskienhallinnan kehittäminen oli vain yksi moduuli laajemmassa ICT-varautumiseen liittyvän jatkuvuussuunnitelman luomisessa. Tässä opinnäytetyössä tehtiin osa riskienarvioinnin ja tunnistamisen vaiheesta. Aikaisemmassa työharjoitteluvaiheessani Organisaatio X:ssä osallistuin kriittisten prosessin tunnistamiseen. Kun riskienhallinta on kunnossa ja riskit tunnistettuina ja analysoituina, on helpompaa lähteä luomaan jatkuvuussuunnitelmaa.

Kuva 5. Jatkuvuussuunnitelman laatimisen vaiheet (Iivari ym 2009, 117).

Opinnäytetyön laatimisen yhteydessä minua pyydettiin myös osallistumaan jatkuvuussuunnitelman muiden moduuleiden suunnitteluun ja laatimiseen. Seuraavaksi vuorossa olisi toteuttaa riskienhallinta kaikkiin Organisaatio X:n merkittäviin IT-järjestelmiin ja samalla suunnitella liiketoiminnan vaikutusanalyysin tekemistä.

Olen kiitollinen, että sain osallistua Organisaatio X:ssä näin merkittävään ja mielenkiintoiseen hankkeeseen. Uskon, että työskentely tämän projektin parissa merkitsee minulle ammattilista kasvua turvallisuusalan ammattilaiseksi.

LÄHTEET

Halonen, K. 2009. eVARE info. [PDF-Dokumentti]. Viitattu 27.10.2009. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090318CTvara/03_eVARE_info_11_3_2009.pdf>

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2001. Tutki ja kirjoita. 6.-7. painos. Vantaa: Tummavuoren kirjapaino Oy.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tallinna: Raamatutrukikoda.

Juvonen, M., Korhonen, H., Ojala, M., Salonen, T. & Vuori, H. 2005. Yrityksen riskienhallinta. Helsinki: Yliopistonpaino.

Ojasala, O., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOY.

Pk-yritysten riskienhallinta. Haavoittuvuusanalyysi, PK-HAAVA. [www-dokumentti]. [luettu 16.11.2008]. <http://www.pk-rh.fi/tyovalineet/haavoittuvuusanalyysi-1/haavoittuvuusanalyysi>

Pk-yritysten riskienhallinta. Potentiaalisten ongelmien analyysi. [www-dokumentti]. [luettu 16.11.2008]. <http://www.pk-rh.fi/pdf/potentiaalisten-ongelmien-analyysi-tietokortti>

Suominen, A. 2003. Riskienhallinta. Vantaa: Dark Oy.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. eVARE. Valtionhallinnon ICT-varautumisen kehittämishanke. [PDF-Dokumentti] Viitattu 25.11.2009. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090820Lausun/02_VARE_vaatimukset_ver_2_02_20_8_2009_.pdf>

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. VAHTI 7/2003. [PDF-Dokumentti]. Viitattu 27.10.2009. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf>

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. VAHTI 2/2009. [PDF-Dokumentti]. Viitattu 27.10.2009. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090410ICTtoi/Vahti_2_NETTI_%2B_KANNET.pdf>

JULKAISEMATTOMAT LÄHTEET

Järjestelmäasiantuntijan haastattelu 18.10.2009. Organisaatio X. Helsinki.

Järjestelmäpäällikön haastattelu 22.10.2009. Organisaatio X. Helsinki.

KUVALUETTELO

LIITTEET

Riskienhallintatoimenpiteet: suunnittelu, toteutus ja seuranta		Laatija: Matti Aitta		Päiväys: 19.10.2009
Yritys X	Tarkastelun kohde: Yritys X:n asian hallinta	Työryhä: XXXXXX		
Riski tai ongelma	Riskin syyt	Pahimmat seuraukset	Riskin suuruus	**Toimenpiteet**
Toimittajat ja heidän asiantuntemus: virheet ohjelmassa.	Toimittajan osaamisen puute. Henkilöresurssin priorisointi. Toimittajilla riippuvuus muutamasta avainhenkilöstä.	Järjestelmän ei toimi odotetulla tavalla	4	Sopimukset, sanktiot.
Toimittajat ja heidän asiantuntemus: Toimittaja ei testaa tuotetta riittävän kattavasti	Toimittajalla ei ole resursseja. Motivaation puute.	Yritys X:n työ kasvaa, koska joudutaan tekemään toimittajalle kuuluvia töitä. Pahin seuraus: järjestelmä rikkoontuu. Jo kertaallen korjatut virheet tulevat takaisin.	4	Tarkistuslista toimittajalle, jonka he käyvät lävitse ennen tuotteen toimittamista. Toimittaja kuittaa listan, kuka käynyt lävitse.
XaHan avainhenkilöt	• Yritys X:n ylläpidon omat räätälöinnit • Yritys X:n ylläpidon jatkuvuus (jos kaikki avainhenkilöt ovat poissa, järjestelmään ei voida tehdä muutoksia.) • Järjestelmän hallittu alasajo ja ylösajo vaatii asiantuntijuutta. Ulkoistaminen	Jos avainhenkilöt ovat poissa, järjestelmä ei välttämättä ole käytössä. Toimittajan tuki eirttäin epävarmaa ja reagointi aika on pitkä verrattuna omiin asiantuntijoihin. Voi ulkoistaa AINOASTAAN yhdelle toimittajalle.	4	Oma asiantuntevus on välttämätön, tai sopimuksessa pitää määritellä korvaava toimintatapa.
Kirjaajat voivat estää järjestelmän käytön muilta.	THS-työkalun varomaton käyttö.	XaHan käyttö estyy ja joudutaan palaamn edellisen illan tilanteenseen - asiat joudutaan perustamaan uudestaan ja dokumentit joudutaan kohdistamaan uudestaan aiheryhmään.	3	THS-työkalua kehitettävä ja kirjaajia koulutettava.
Järjestelmän arkkitehtuuri: laitteita ei kahdennettu, mutta varmuuskopioitu.	Laiterikko	Järjestelmä ei ole käytettävissä.	3	Laitteet tulisi kahdentaa. Järjestelmän tiedot varmuuskopioidaan.
. Suorituskyky ja kapasiteetti (jos suorituskyky ei riitä, kaikkien käyttö estyy.)	Toimittaja ei ollut huomioinut datan määrän kasvua testeissään. Eivät olleet arvioineet minkälaista kapasiteettiä järjestelmä vaatii.	Käyttäjät saavat "time-out" virheilmoituksia.	2	Uusi tietokantapalvelin on jo tilattu. Ohjeistus ja menettelytavat. Kuormittavaa YHS-työkalua pyritään käyttämään ns. "ruuhka-ajan ulkopuolella".
Tapahtuman	Tapahtuman seuraukset			
todennäköisyys	vähäiset	haitalliset	vakavat	
epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski	
mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä	
todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski	

Riskienhallintatoimenpiteet: suunnittelu, toteutus ja seuranta		Tarkastelun kohde: Yritys X:n konesalin palvelinympäristö		Päiväys: 9.11.2009
Yritys X		Laatija: Matti Aitta		
		Työryhä: XXXXXXX		
Riski tai ongelma	Riskin syyt	Pahimmat seuraukset	Riskin suuruus	**Toimenpiteet**
Konesalin fyysinen palvelinympäristö	Jos serveri kärähtää ja ilmaistointi pettää, saattaa se aiheuttaa mahdollisen tulipalon. Sprinklerit sammuttavat tulipalon, mutta aiheuttavat samalla vesivahingon. Vesivahinko saattaa aiheutua myös rikkoutuneesta putkesta.	Konesali tuhoutuu ja toiminta keskeytyy.	3	Sammutusjärjestelmän vaihto. Tapahtuu ens vuonna.
Sisäinen henkilöriski, sabotaasi & kulunvalvonta	Tahallinen tai tahaton henkilökunnan välittömästi tai välillesesti aiheuttama vahingon teko	Tiedon, laitteiston tai palvelujen tuhoutuminen.	3	Henkilökunnan hyvinvointi ja viihtyvyys työpaikalla. Turvallisuusselvitykset.
Palvelunestohyökkäykset	Palvelunestohyökkäykset johtuvat talon ulkopuolisesta tahoista.	Sähköpostin lähetys estyy, tietoliikenneyhteydet menevät poikki. Palvelunestohyökkäys hidastaa ja estää ulosppäin menevää liikennettä, saattaa kaataa palomuurin, häiritsee tietoliikennettä.	3	turkeutumisen esto järjestelmö IPS
hakkerointi	Ulkopuolinen taho pääsee sisäverkkoon ja voi tehdä mitä vain.	Esimerkiksi varastaa tietoja, saastuttaa työpisteistä, asentaa troijalaisia.	3	kulunvalvonta, kouluttaminen, tietoturvapäivitykset,
virus	Uusi virus verkosta jota virustorjuntaohelma ei tunnista	tiedot tuhouvat, saastuvat, tai joutuvat vääriin käsiin	4	Monitasoinen virussuojaus, sipuli. Päivitetää virustorjuntaa, koulutus, ohjeistaminen
spämmi	Ulkopuolinen taho kaappaa koneen.	Saastunut kone toimii ns. spämmiposti palvelimine ja lähettää spämmi talon ulkopuolelle. Tässät voi seurata se, että stukki voi joutua ns. mustalle listalle.	3	estetään muiden kuin sähköpostipalvelimier SMTP liikenne ulospäin.
Tiedon eheys, varmistaminen ja palautukset. Laiterikot. Laitteiston ikä.	Laiterikot, tiedon menetykset, datan katoaminen, käyttäjien tunarointi.	Tietoa katoaa.	4	Varmistukset, palautuksien testaminen, TH kunnossa, kouluttaminen, ohjeistaminen,. Laiterikkoihin ennakoiva seuranta softapohjaisesti. DFS
Ohjelmistojen ja laitteistojen päivitykset, esimerkiksi open text	Viallinen tai sopimaton päivitys tai päivitys prosessi.	Toiminta- ja käyttökatkoja. Tiedon katoamista.	4	Testataan päivityksiä testiympäristössä ja varmistetaan tiedot ennen päivityksiä. Vain kriittiset päivitykset asennetaan heti, riippu tapauksesta.
Käytön valvonta	Ulkopuolinen instanssi, esimerkiksi konsultti jätetään valvomatta stukin tiloihin. Talon ulkopuolinen konsultti tekee jonkun muutokset, mutta ei tiedä siitä aiheutuvia sivu-vaikutuksia	Tiedon tuhoutuminen, haittaohjelmien levitys, maineen menetys - haittaohjelmien levitys tapahtuu stukin koneilta yms.	4	Henkilökunnan kouluttaminen ja ohjeistaminen. Konsulttien valvonta.
Integroituvuus hankaloittaa toimintaa	Riippuvuudet. Testaaminen ja hyväksyttäminen monitasoista. Ei ymmärrettä täysin järjestelmien yhteyksiä toisiinsa.	Toiminta- ja käyttökatkoja. Tärkeät tietojörjestelmät eivät toimi.Monimutkaista ylläpitoa ja päivityksiä.	3	Asialle ei oikein voi mitään ja sen kanssa pitää elää. Jäännösriki.
Riippuvuus avainhenkilöistä ja dokumentaation puute.	Henkilöresurssit. (stuk ylläpitää omia järjestelmään)	Toipuminen hidastuu.	2	Varamiesjärjestelmä. Kouluttaminen. Ylläpitosopimukset, tukisopimukset
Palvelujen maantieteellisen kahdennuksen puute. Huonosti toimiva kahdennus voi olla riski	Rahasta. Ei ole resursseia.	Tiedot tuhoutuvat pysyvästi, toiminta keskevttyy.	3	Kahdennetaan kriittisiä palveluja maantieteellisesti.
Toimittajan tuen puuttuminen ja laatu. Huoltosopimusten puuttuminen ja sopimusten huono sanktiointi & sopimuspykälät	OSaamattomuus toimittajan päässä, stuk saattaa olla liian pieni asiakas, toimittaja valittu arvioimatta kyseistä riskiä.	Käyttökatkoja, järjestelmän toimimatottumsutta	4	Täsmällisemmät sopimukset, sanktiot, toimittajien ja tuotteiden vaihto.
Jäädytetyt järjestelmät	Järjestelmää ei enään päivitetä, ei kehitetä, ei resursseja - rahaa.	tietoturvariskejä, mm virukset, hakkerit. Järjestelmät eivät toimi tai ole yhteensopivia tulevaisuudessa.	4	Uusia järjestelmät.
Käyttöoikeuspolitiikka	Monimutkaisuus, integroituut moneen järjestelmään,	Tuhota tiedostoja tahallaan tai tahattomasti jälkiä jättämättä. Voi tehdä muutoksia järjestelmään. Ei voida jäljittää tai ei voida yhdistää tekijään varmasti.	4	Kaikille omat, eritellyt administraattori käyttäjätunnukset.
Tietoverkonsegmentoinnin puute.	Tietoturvauhka palvelinlaitteille. Palvelimet eivät omassa verkkosegmentissään, palomuurisegmentissä.	Työasena saastuu ja se saattaa saastuttaa edelleen esim. palvelinverkon. Suurin osa tiedoista on palvelinverkossa.	4	Erotetaan palvelin- ja työasema verkot toisistaan palomuurintasolla.
Verkon solmupisteet: Kriittisiä erilliskomponentteja:, verkon solupisteitä: Palomuuri, AD = active directory, keskuskytkimet, internetyhteys ja levyjärjestelmät		Tietoliikenne kulkee näiden kautta. Tietojärjestelmät eivät toimi ja tietoliikenneyhteydet katkeavat.	3	Kaikki on jo kahdennettu, paitisi internetyhteys. Resursseihin nähden kohtuullisessa kunnossa.

Tapahtuman	Tapahtuman seuraukset			
todennäköisyys	vähäiset	haitalliset	vakavat	
epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski	
mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski	
todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski	