LAUREA

Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän kehittämissuunnitelma S-ryhmälle

Sarpakunnas, Tuomas

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän kehittämissuunnitelma S-ryhmälle

Tuomas Sarpakunnas
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2009

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Tiivistelmä

Tuomas Sarpakunnas

Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän kehittämissuunnitelma S-ryhmälle

Vuosi 2009 Sivumäärä 27

Opinnäytetyö on toiminnallinen kehittämissuunnitelma S-ryhmän riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmästä. Järjestelmä on aikoinaan hankittu tukemaan riskienhallinnan suunnittelua ja turvallisuuden johtamista, mutta sen kehitystyö oli jäänyt kesken. Työn toimeksiantajalla oli tarve selkeälle ja johdonmukaiselle suunnitelmalle järjestelmän käytön ja sisällön kehittämiseksi. Opinnäytetyön raportti toimii samalla itse kehittämissuunnitelmana.

Työ toteutettiin tutustumalla itse tietojärjestelmän sisältöön ja ominaisuuksiin sekä haastattelemalla S-ryhmän riskienhallinnan ja turvallisuusjohtamisen asiantuntijoita, joiden käyttöön tietojärjestelmä on tarkoitettu. Kerättyjen tietojen perusteella määritettiin kehittämissuunnitelman lähtökohta ja toimeksiantajan tarpeet järjestelmälle, joiden pohjalta luotiin ehdotukset kehittämistoimenpiteiksi.

Lähtökohtien määrittelyssä ilmeni tietojärjestelmän ominaisuuksien puutteiden suuri määrä sekä järjestelmän käytön hajanaisuus ja epäsäännöllisyys. Käyttäjähallinta, selkeät käyttäjien roolit ja raportoinnin hankaluus nousivat merkittävimmiksi ongelmakohdiksi, jotka myös heijastuivat toimeksiantajan tarpeissa. Raportointiin kaivattiin monipuolisuutta, selkeyttä, säännöllisyyttä ja luotettavuutta. Järjestelmästä pitää saada oikeasti suunnittelua tukeva työväline.

Toimenpide-ehdotukset jakaantuivat tärkeimpiin, vähemmän tärkeisiin sekä vähiten tärkeisiin ehdotuksiin. Tietojärjestelmän kokeilu, ”pilotointi”, ennalta harkitusti ja suunnitellusti, uusituilla ohjeilla, tarkistetuilla käytänteillä ja käyttäjien selkeytetyillä rooleilla olisi enemmän kuin tarpeellista. Toinen tärkeä toimenpide on raportoinnin korjaaminen monipuolisemmaksi ja selkeämmäksi.

Asiasanat: Kehittämissuunnitelma, riskienhallinta ja turvallisuusjohtaminen, tietojärjestelmä

Laurea University of Applied Sciences
Laurea Leppävaara
Security Management

Abstract

Tuomas Sarpakunnas

Development plan for S-group's Information System of Risk and Security Management.

Year 2009 Pages 27

This thesis is a development plan for the S Group's information system of risk and security management. The purpose of the plan is to write down a clear plan and guidelines for how to improve the usage and features of this particular system in the S Group. The plan consists of the clarification of the present state of the system, the S Group's needs for the system and proposals for the steps of development.

For the development plan, the information system was studied and observations were made about the features it contains. In addition, four specialists of the S Group risk management team were interviewed to define the state of the usage of the system. Through the interviews the S Group's needs for the system were defined. The list of problems and development areas became relatively long.

The main focus areas were the user definitions and roles as well as the problems related to reporting. The reporting needs to be clearer, more versatile, regular and trustworthy. At the moment, the system is not supporting the planning of the S Group's risk management procedures. The most important suggestions for improvement turn out to be a proper piloting project carried out through well-planned and purposeful means, revised guiding and user roles the improvement of the reporting feature. In addition, the plan contains several minor measures of development.

Key words: Development plan, risk and security management, information system

Sisällys

1 Johdanto

Tämä opinnäytetyö on toiminnallinen kehittämissuunnitelma S-ryhmän Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän käytön ja ominaisuuksien parantamiseksi. Työ on tehty S-ryhmään kuuluvalle SOK:n riskienhallintayksikölle, jossa itse olen töissä. Aihe valikoitui opinnäytetyön aiheeksi tunnistettuani tarpeen johdonmukaiselle suunnitelmalle kehittää vastuualueeseeni kuuluvaa tietojärjestelmää. Tietojärjestelmä on hankittu noin viisi vuotta aiemmin riskienhallintayksikköön, mutta sen järjestelmällinen sisäänajo ja kehittäminen olivat jääneet kesken, jolloin järjestelmä ei tuottanut riskienhallinnan ja turvallisuuden johtamiselle riittävästi lisäarvoa.

Miksi tällainen tietojärjestelmä tulisi S-ryhmällä edes olla käytössä? Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän rooli on olla luomassa ja ylläpitämässä hyvää organisaation turvallisuuskulttuuria. Turvallisuuskulttuurilla tarkoitetaan turvallisuutta koskevien arvojen ja asenteiden sekä organisaation turvallisuustoimenpiteiden kokonaisuutta (Leppänen 2006, 49). Hyvä turvallisuusjohtamisjärjestelmä yhdessä hyvän henkilöjohtamisen kanssa johtaa hyvään organisaation turvallisuuskulttuuriin. Turvallisuusjohtamisjärjestelmä sisältyy aina organisaation johtamisjärjestelmään ja hyvä turvallisuusjohtamisjärjestelmä sisältää hyvän turvallisuuden hallintajärjestelmän. Turvallisuuden hallintajärjestelmä on kokonaisuus joka sisältää periaatteita ja päämääriä, ohjeita, oppaita, koulutus- ja tiedotusmateriaalia sekä muuta turvallisuuteen liittyvää dokumentaatiota. (Kerkko 2001, 22-32.) Tietojärjestelmää voidaan pitää osana turvallisuuden hallintajärjestelmää.

Tässä opinnäytetyön raportissa esitellään kehittämissuunnitelman konteksti, tavoitteet jotka suunnitelmalle ja S-ryhmän riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmälle on asetettu, työn toteutuksen kuvaus, kehittämiskohteiden määrittely ja toimintaympäristön tarpeet järjestelmälle sekä toimenpide-ehdotukset järjestelmän kehittämiseksi.

2 Kehittämissuunnitelman taustat

Kehittämissuunnitelman taustat eli kohdeympäristön ja kehittämisen kohteen yksityiskohdat on selvitetty seuraavassa.

2.1 Kohdeyritys

Kehittämissuunnitelman kohdeyritys on SOK eli Suomen Osuuskauppojen Keskuskunta, joka on osa S-ryhmää. S-ryhmä muodostuu SOK:n ja sen tytäryhtiöiden lisäksi 22 alueosuuskaupasta ja 10 paikallisosuuskaupasta. Osuustoiminnan mukaisesti asiakasomistajat omistavat osuuskaupat ja osuuskaupat puolestaan omistavat keskusliikkeenä toimivan SOK:n. S-ryhmän liiketoiminnan tarkoitus on palveluiden ja etujen tuottaminen omistajilleen eli asiakkailleen. S-ryhmän liiketoiminta sisältää marketkaupan, tavaratalo- ja erikoisliikekaupan, liikennemyymälä- ja polttonestekaupan, matkailu- ja ravitsemiskaupan, auto- ja autotarvikekaupan sekä maatalouskaupan. Liiketoiminta-alueet on järjestetty ketjuihin, jotka toimivat valtakunnallisesti. Keskitetyt palvelutoiminnot S-ryhmässä tuottaa SOK ja liiketoiminnan suorittamisesta vastaavat pääsääntöisesti alueosuuskaupat SOK:n omaa liiketoimintaa lukuun ottamatta. SOK:n liiketoimintaan sisältyy ulkomaan marketkauppa Venäjällä ja Baltian maissa, osa kotimaan ja kaikki ulkomaan matkailu- ja ravitsemiskaupan liiketoiminnasta sekä auto- ja autotarvike- sekä maatalouskauppa. Ketjuja ovat muun muassa Sokos, Emotion, Prisma, S-market, Alepa, Sale, Kodin Terra, S-Rautamarket, ABC, Sokos Hotels, Radisson Blu Hotels & Resorts, Holiday Club Spa Hotels sekä Amarillo, Rosso, Fransmanni ja useita muita ravintolaketjuja. Vuoden 2008 lopussa S-ryhmällä oli 1554 toimipaikkaa Suomessa ja 12 ulkomailla. S-ryhmässä työskentelee yli 37 000 työntekijää. (SOK-yhtymä Vuosikertomus 2008.)

Kehittämiskohteena oleva tietojärjestelmä on SOK:n riskienhallintayksikön hallinnoima. SOK Riskienhallinta –yksikkö kuuluu SOK:n hallintotoimintoihin. Riskienhallintayksikkö vastaa S-ryhmän kokonaisvaltaisesta riskienhallinnasta ja sen kehittämisestä sekä niihin liittyvien palvelujen tuottamisesta S-ryhmälle. Yksikön koko on kahdeksan henkeä. SOK Riskienhallinta on opinnäytteen toimeksiantaja ja sen rooli kehittämishankkeessa on keskeinen. (Koskinen 2009.)

2.2 Tietojärjestelmän määrittely

Kehittämissuunnitelman kohteena on tietojärjestelmä, joka toimii työkaluna osana S-ryhmän turvallisuusjohtamisjärjestelmää. Tietojärjestelmä on määritelty ihmisistä ja tekniikasta muodostuneeksi infrastruktuuriksi tiedon varastoimiseksi, käsittelemiseksi, siirtämiseksi,

tallentamiseksi ja hyödyntämiseksi (ISM3 2009). Tietojärjestelmiä käytetään hyödyksi johtamisessa sekä jokapäiväisessä työnteossa.

Tietojärjestelmiä voidaan jakaa käyttötarkoituksensa mukaan eri luokkiin. Luokitukset voivat vaihdella riippuen organisaatioista, mutta tietojärjestelmät voi luokitella esimerkiksi operatiivisiin ja johdon tietojärjestelmiin, päätöksenteon ja ylimmän johdon tukijärjestelmiin sekä toimistoautomaatiojärjestelmiin. Operatiiviset tietojärjestelmät ovat työkaluja joilla kerätään, käsitellään ja tallennetaan suurin osa informaatiosta mitä organisaation päivittäisessä toiminnassa syntyy ja liikkuu. Järjestelmien käsittelemä tieto on yksinkertaista raakatietoa ja järjestelmän toiminnot ovat usein rutiininomaisesti ohjelmoituja. Operatiivisten järjestelmien tulee olla tehokkaita ja nopeita, sillä ne ovat usein organisaatioiden toiminnan kannalta merkityksellisiä. (Turun Yliopisto 1999.)

Johdon tietojärjestelmät helpottavat operatiivisen ja keskijohdon työtä muodostamalla yhteenvetoja ja standardisoituja raportteja, joiden avulla ohjataan organisaation toimintaa. Järjestelmät raportoivat eri toiminnoista ja niissä syntyvistä ja liikkuvista tiedoista. Raportit kertovat usein historiasta ja nykyhetken tilanteesta. Järjestelmien sisältämän informaation luotettavuus on tärkeää, sillä järjestelmien avulla suunnitellaan organisaation tulevaa toimintaa. Johdon tietojärjestelmät voivat itse varastoida tietoja tai tiedot välittyvät järjestelmään muualta. (Turun Yliopisto 1999.)

Päätöksenteon tukijärjestelmät eroavat edellä mainituista järjestelmistä siinä, että ne eivät käsittele ja tue käynnissä olevia prosesseja, vaan niitä käytetään satunnaisesti ja niiden avulla ratkaistaan ongelmatilanteita. Järjestelmiä käytetään luovasti ja kunkin tilanteen edellyttämällä tavalla, joten järjestelmien tulee olla joustavia ja sopeutuvia. Päätöksenteon tukijärjestelmät eivät ole valmiita rakenteellisia kokonaisuuksia vaan kokoelmia tietojenkäsittelyvälineistä, jotka keräävät tietoja sekä organisaation muista järjestelmistä että organisaation ulkopuolelta käytettävissä olevista tietolähteistä. Järjestelmä tukee lyhyen aikavälin tavoitteiden asettelua. (Turun Yliopisto 1999.)

Ylimmän johdon tukijärjestelmät keräävät myös tietonsa useista lähteistä organisaatiosta sekä sen ulkopuolelta ja esittävät tiedot kokonaisuutena tyydyttäen ylimmän johdon informaatiotarpeita. Kun päätöksenteon tukijärjestelmät vaativat käyttäjältä syventymistä ja vuorovaikuttamista järjestelmän kanssa, niin ylimmän johdon tukijärjestelmät tuovat informaation helppokäyttöisesti ja laaja-alaisesti näkyville. Ne myös auttavat pidemmän tähtäimen tavoitteiden suunnittelussa. (Turun Yliopisto 1999.)

Useimmille tutuin näistä eri tietojärjestelmäluokista on toimistoautomaatiojärjestelmät. Nämä järjestelmät tukevat ja helpottavat organisaatioiden henkilöiden päivittäistä

kommunikointia ja asioiden koordinointia. Näitä järjestelmiä ovat muiden muassa atk-päätteen toimistosovellukset kuten tekstinkäsittely-, taulukkolaskenta- ja sähköpostisovellukset. (Turun Yliopisto 1999.)

2.3 S-ryhmän riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän kuvaus

S-ryhmän riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmä on sovellus jota käytetään internet-selaimella ryhmän sisäisessä verkossa. Järjestelmä on käytössä tavaratalo- ja erikoisliikekaupan ketjuissa, matkailu- ja ravitsemiskaupan hotelliketjuissa sekä liikennemyymälä- ja polttonestekaupan ketjuissa. Tietojärjestelmän avulla kerätään tietoa ryhmän toimipaikoissa tapahtuvista poikkeamatilanteista. Järjestelmä varastoi tiedon ja välittää sen sitä tarvitseville. Lisäksi järjestelmän avulla toimipaikat voivat suorittaa turvallisuuden omavalvontaa sähköisten lomakkeiden avulla. Tietojärjestelmässä on myös muita ominaisuuksia, kuten raportointityökaluja poikkeamien ja suoritettujen omavalvontojen tulosten havainnollistamiseksi, sekä turvallisuusaiheista verkko-opiskelumateriaalia. Käytettävissä olevat järjestelmän ominaisuudet ja saatavilla olevat poikkeamailmoitukset ja omavalvonnan tulokset riippuvat käyttäjille määritellyistä oikeuksista. Oikeudet on annettu käyttäjille niillä perustein, että henkilö pystyy näkemään järjestelmästä vain oman työn kannalta tarpeellisia tietoja. Käyttäjätunnukset tehdään henkilökohtaisiksi tai yhteisiksi yksikkötasoisesti. Tunnukseen määritellään käyttäjäryhmä sekä yksikkö. Tunnukseen voidaan yhdistää sähköpostiosoite, joka mahdollistaa sähköposti-ilmoitusten ja –muistutusten lähettämisen. Järjestelmä lähettää käyttäjäryhmän ja yksikkövalinnan mukaisesti sähköposti-ilmoitukset käyttäjille määritellyistä poikkeamailmoituksista sen jälkeen, kun ilmoitus on tallennettu järjestelmään. Järjestelmä on myös ohjelmoitu lähettämään muistutussähköpostit määritellyille käyttäjille toimipaikkojen turvallisuuden omavalvonnan suorittamista varten.

Kun toimipaikassa sattuu jokin normaalista toiminnasta poikkeava tapahtuma, henkilökunta tekee järjestelmään poikkeamailmoituksen. Poikkeamat on jaoteltu valmiiksi eri tyyppeihin, joka helpottaa tilastointia. Eri toimialoille suunnatuissa ilmoituspohjissa on erilaisia, toimialakohtaisia poikkeamatyyppejä. Ilmoitukseen täytetään tapahtuma-aika ja –paikka, havainnon tekijä, tapahtumakuvaus sekä lisätietoina tapahtuman kohde, mahdolliset aineelliset ja henkilövahingot sekä viranomainen jolle tapahtumasta on ilmoitettu. Ilmoitukseen voi myös liittää tiedostoja, jos halutaan arkistoida kuvia tai erillisiä tapahtumakuvauksia.

Tietojärjestelmän turvallisuuden omavalvontaosuus sisältää toimialoittain standardeja eri aihepiireissä. Standardit sisältävät kysymyksiä, joihin omavalvonnan suorittaja voi vastata kunnossa, ei kunnossa tai ei koske kohdetta. Lomake tallennetaan, jonka jälkeen kunnossa

olleet tai kohdetta koskemattomat kysymykset poistuvat näkyvistä ja vastaamattomat tai kysymykset jotka eivät olleet kunnossa jäävät näkyviin. Käyttäjän tulee myös määritellä avoimiksi jääneiden kysymysten kohdalle aikataulu ja vastuuhenkilö asian kuntoon saattamiseksi.

Raportointityökalulla voidaan synnyttää graafisia kuvaajia poikkeamailmoituksista ja suoritetuista omavalvonnoista. Poikkeamista on mahdollista näyttää eri tyyppien lukumääriä niin S-ryhmä-, toimiala-, ketju- kuin toimipaikkatasoisesti. Myös kahden eri tason tai toimipaikan poikkeamien määriä voi vertailla keskenään. Kuvaajiin voi myös suodattaa vain niitä poikkeamia, jotka täyttävät halutut ilmoituksen lisätietojen ehdot. Raportissa voidaan esimerkiksi näyttää vain ne poikkeamat, joiden yhteydessä on tapahtunut aineellisia vahinkoja tai tapahtumat, joista on ilmoitettu jollekin viranomaiselle.

Omavalvontaraportoinnissa voidaan graafisesti esittää omavalvontakysymysten kunnossa - vastausten määrä suhteessa kysymysten määrään eli näkyviin saadaan prosenttiluku. Myös omavalvontaraportoinnissa voidaan valita eri tasoja tai toimipaikkoja vertailtavaksi ja kuvaajaan voidaan valita joko yksittäisiä standardeja tai kysymyksiä aihepiireittäin.

Tietojärjestelmään syötetyt poikkeamailmoitukset arkistoituvat tietokantaan ja niitä voi selailla tietojärjestelmän käyttöliittymässä. Ilmoituksia voi hakea tallennuspäivämäärän, ilmoitustyypin, yksikön tai ilmoitusnumeron perusteella. Ilmoituksen voi avata tarkastelua varten, mutta sitä voi muokata ainoastaan pääkäyttäjien tunnuksilla.

Tietojärjestelmään on sisällytetty myös verkko-opiskelumateriaalia. Valittavana ovat erilliset verkkokurssit paloturvallisuudesta hotellissa ja varastoturvallisuudesta.

Edellä mainituista tietojärjestelmien luokitteluista kehittämisen kohteena oleva S-ryhmän Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmä kuuluu johdon tietojärjestelmiin, mutta sisältää myös operatiivisten tietojärjestelmien ominaisuuksia. S-ryhmän järjestelmää käytetään riskienhallinnan suunnitteluun vertailemalla järjestelmästä saatavia historiatietoja nykyhetken tietoihin. Toisaalta järjestelmä tukee operatiivista toimintaa antaen esimerkiksi tietoa oikeista menettelytavoista turvallisuuden omavalvonnan suorittajille.

3 Tavoitteet ja toteutus

Tämän opinnäytetyön aihe valikoitui tietojärjestelmän kehittämissuunnitelmaksi siksi, että toimeksiantajalla on tarve saada heillä jo käytössään olevasta järjestelmästä toimivampi ja tarkoituksenmukaisempi. Järjestelmän tulisi tukea riskienhallinnan ja turvallisuusjohtamisen suunnittelua päätöksenteon apuvälineenä. Sen avulla pitäisi pystyä helposti keräämään,

säilömään ja esittämään tietoa S-ryhmän niiltä toimialoilta, joilla järjestelmä on käytössä. Seuraavassa on kirjattu toimeksiantajan ja kehittämistyön tavoitteet ja odotukset sekä kuvaus kehittämistyön toteutuksesta.

3.1 Tavoitteet

Toimeksiantajan tavoitteena on, että järjestelmää käyttävien S-ryhmän toimipaikkojen henkilökunta raportoisi kaikki normaalista toiminnasta poikkeavat tapahtumat järjestelmän kautta. Tällöin poikkeamatiedot saavuttaisivat tarvittavat henkilöt ja tahot heti tapahtumien jälkeen valmiiksi dokumentoituna. Tarkoituksena on myös, että järjestelmää voitaisiin suoraan käyttää raportointiin niin toimipaikoissa kuin tukitoiminnoissa. Toimipaikkojen päälliköt voisivat verrata omaa tilannettaan poikkeamien ja turvallisuuden omavalvonnan osalta ketjun tai toimialan yleiseen tilanteeseen. Tukitoiminnoille oleellisempaa ovat tiedot toimialojen ja ketjujen kokonaiskehityksestä, ei niinkään yksittäisten toimipaikkojen tilanteista. Järjestelmän toivotaan olevan ennen kaikkea helppo työväline turvallisuuden omavalvonnan suorittamiseen, jotta toimipaikat eivät kokisi sitä epämiellyttäväksi työtehtäväksi. Järjestelmään tulisi myös jatkossa olla mahdollista liittää mukaan lisää ominaisuuksia ja uusia osioita, kuten työkalu vaarojen arviointiin. Ehkä tärkeimpänä tavoitteena nousee kuitenkin esiin käytön sujuvuus. (Koskinen 2009)

Opinnäytteeseen kuuluvan kehittämistyön tavoitteena on selvittää hyvä ja todenmukainen kuva tietojärjestelmän nykytilasta, jonka sisältö painottuu järjestelmän käyttäjille näkyviin ominaisuuksiin sekä käytettävyyteen. Nykytilan määritykseen kuuluu lisäksi ongelmakohtien selvittäminen. Tavoitteena on myös löytää keinoja ongelmien selvittämiseksi ja järjestelmän kehittämiseksi toimeksiantajan tavoitteiden ehdoilla. Kehittämistoimenpiteistä pyydetään palautetta ja niitä kehitetään tarvittaessa eteenpäin.

Odotukset kehittämistyölle ovat kohtuullisen positiiviset. Työn toimeksi antaneen tahon, eli riskienhallintayksikön rooli järjestelmän hallinnoijana ja kehittäjänä ei aseta kovin tiukkoja rajoja kehittämistoimenpiteiden suunnittelulle. Toisaalta järjestelmän tekninen ratkaisu sekä rajalliset resurssit muutosten tekemiseksi järjestelmän ominaisuuksiin asettavat rajoitteita. Kehittämistoimenpiteitä suunniteltaessa on huomioitava, että kaikki muutokset järjestelmään on tilattava sovellustoimittajalta ja suurten muutosten toteuttaminen vaatii aikaa ja myös budjetti on rajallinen, vaikkei sitä tässä yhteydessä olekaan erikseen määritelty. Järjestelmä on lisäksi jatkuvassa käytössä ja siksi käyttäjät on myös huomioitava muutoksia tehtäessä. Toimeksiantajan toiveissa on pienillä muutoksilla saatava maksimaalinen hyöty keskeyttämättä järjestelmän jatkuvaa käyttöä.

3.2 Kehittämistyön toteutus

Kehittämistyöllä ja –prosessilla on olemassa kriteerit. Kehittämistyön tulee edetä järjestelmällisesti, analyyttisesti ja kriittisesti, siihen pitää sisältyä vuorovaikutteisuutta sekä eettisyyttä. Prosessi etenee siten, että aluksi tunnistetaan kehittämiskohde ja asetetaan tavoitteet. Kehittämiskohteeseen perehdytään tämän jälkeen niin käytännössä kuin teoriassa. Tarkemman kehittämistehtävän valinta ja kohteen rajaaminen tulee tehdä kohteeseen ja siihen liittyvään teoriaan perehtymisen jälkeen, ennen kuin tarkempi lähestymistapa ja kehittämismenetelmät valitaan. Menetelmät voivat olla etenkin työelämän kehittämistyössä monenlaisia. Tavanomaisten tutkimusmenetelmien - kuten toimintatutkimus tai konstruktiivinen tutkimus – lisäksi käyttökelpoisia voivat olla käytännönläheisemmät kehittämismenetelmät, keskusteluihin perustuvat ryhmätyöskentelyt tai ideariihet. Kehittämisprosessin loppuvaiheeseen eli suunnitelmien viemiseen käytäntöön tulisi keskittyä riittävästi, jotta halutun muutoksen saavuttaminen olisi mahdollista. Samalla tehtävä muutosprosessin ja sen tulosten kuvaaminen kirjallisesti kuuluu myös oleellisena osana prosessiin. Lopuksi kehittämistyö eli itse kehittämisprosessi ja sen tulokset tulee arvioida. (Ojasalo, Moilanen & Ritalahti 2009, 24-26.)

Opinnäytetyön aiheen valinnan, hyväksyttämisen ja opinnäytetyösuunnitelman laatimisen ja esittämisen jälkeen aloin toteuttamaan työsuunnitelmaa vahvistamalla käsitystäni kehittämissuunnitelman kohteena olevasta järjestelmästä. Tutustuin tietojärjestelmien perusteisiin ja keräsin tietoa tulostamalla järjestelmästä raportteja ja arvioimalla niiden sisältämän tiedon luotettavuutta ja käytettävyyttä. On syytä huomioida, että kaikki järjestelmän sisältämä tieto on toimeksiantajan luottamukselliseksi määrittelemää, joten sitä ei voi tässä työssä tuoda yksityiskohtaisesti esille. Keräämäni aineiston avulla myöhemmin esitettävä kehittämissuunnitelman lähtökohtien määrittely oli mahdollista.

Järjestelmästä oli saatavilla vain hyvin vähän ohjeita ja muuta kirjallista dokumentaatiota, joten järjestelmän ominaisuuksien kuvailu perustuu suurilta osin perehdytyksessä esimieheltäni suullisesti saamiin ohjeistuksiin sekä omakohtaiseen kokemukseen järjestelmän käyttämisestä. Käyttökokemusta järjestelmästä oli opinnäytetyön aloitusvaiheessa noin kolme kuukautta.

Merkittävä lähde tässä kehittämistyössä on asiantuntijahaastattelut. Haastattelujen perusteella tietojärjestelmän käytön nykytilan ja tavoitteiden määrittely oli mahdollista. Tässä tapauksessa asiantuntijat myös edustavat toimeksiantajan organisaatiota, joten kehittämistoimenpiteitä suunniteltaessa noudatettiin merkittävästi heidän tarpeitaan ja toivomuksiaan. Haastattelin huhtikuun aikana SOK Riskienhallinta-yksikön päällikköä Mikko Koskista sekä hänen yksiköstään yritysturvallisuuspäällikkö Rami Laustolaa ja

tietoturvallisuuspäällikkö Vesa Tupalaa. Lisäksi haastattelin S-ryhmän matkailu- ja ravitsemiskaupan toimialalla turvallisuusasioista vastaavaa kenttäpäällikkö Juha Lindholmia.

Riskienhallintayksikön päällikkö Koskinen on koulutukseltaan tradenomi turvallisuusalan koulutusohjelmasta Laurea-ammattikorkeakoulusta ja on suorittanut myös Dipolin tietoturvallisuuden koulutusohjelman sekä S-ryhmän omia johtamisvalmennuksia. Hän on työskennellyt S-ryhmässä haastatteluhetkellä kuusi vuotta sekä tätä ennen turvallisuusasiantuntijana Engel Palvelut Oy:ssä ja Despe Consulting Oy:ssä. Häneen tehtäviinsä kuuluu SOK Riskienhallinta-yksikön esimiestehtävät ja S-ryhmän kokonaisvaltainen riskienhallinta. Yritysturvallisuuspäällikkö Laustola on valmistunut myös tradenomiksi Laurea-ammattikorkeakoulun turvallisuusalan koulutusohjelmasta, mutta tätä ennen suorittanut poliisin tutkinnon. Hän on työskennellyt järjestyspoliisina ja tutkinta-osastolla Espoon poliisissa ja Turunmaan kihlakunnassa, Helsingin kihlakunnan poliisilaitoksella ulkomaalaispoliisina, Suojelupoliisin kenttävalvontayksikössä ja terrorismintorjuntayksikössä ylietsivänä sekä ennen SOK:n Riskienhallinta-yksikköön tulemista Loomis Arvokuljetuksen turvallisuuspäällikkönä. Laustola vastaa S-ryhmän Mara-liiketoiminnan, KV -liiketoimintojen ja rahankäsittelyyn liittyvän toiminnan yritysturvallisuudesta sekä riskienhallinnasta. Tietoturvallisuuspäällikkö Tupala on koulutukseltaan Vaasan Yliopistosta valmistunut kauppatieteiden maisteri, alanaan tietojärjestelmät ja tuotantotalous. Hän on työskennellyt ennen riskienhallintayksikköä muun muassa KPMG Oy Ab:lla ja Vaasan Yliopiston tietohallinnossa sekä erilaisissa tutkimusprojekteissa. Tupalan vastuulle kuuluu S-ryhmän tietoturvallisuusasiat sekä liiketoiminnan jatkuvuussuunnittelu. Kenttäpäällikkö Lindholm puolestaan on työskennellyt operatiivisissa toimialan kenttätehtävissä noin 20 vuotta. Yllä mainitut tiedot perustuvat haastateltavien omaan kertomukseen.

Haastattelumuodoksi valitsin puolistrukturoidun teemahaastattelun. Haastatteluissa teema ja aihealueet olivat kaikille haastateltaville samoja, mutta kysymysten näkökulmat olivat erilaisia. Juuri teemahaastattelusta puuttuu strukturoidulle haastattelulle ominaiset tarkkaan muotoillut ja järjestellyt kysymykset. Haastateltavien asiantuntijuuden jakaantuessa hieman eri osa-alueisiin, ei tarkkaa ja kaikille samanlaista lomakehaastattelua olisi voitu suorittaa. Sen sijaan loin haastatteluja varten perusrungon, jota käytin jokaisessa haastattelussa, mutta haastattelutilanteessa muotoilin kysymykset koskemaan haastateltavien vastuualueita ja osaamisalaa. Haastattelukysymykset ovat liitteessä 1. (Hirsjärvi & Hurme 2000, 47-48.)

Asiantuntijahaastatteluissa kysyin haastateltavilta tietojärjestelmän käyttökokemusten ja siihen liittyvien tarpeiden lisäksi, mikä merkitys tiedon keräämisellä on riskienhallinnan ja turvallisuusjohtamisen kannalta. Tarkoituksena oli saada käsitys siitä, miten tärkeää tuoreen informaation saaminen yrityksen sadoista toimipaikoista on suunniteltaessa toimenpiteitä riskienhallinnan ja turvallisuuden johtamisen kannalta.

Haastattelujen jälkeen kirjasin kaikki esille tulleet kommentit ja näkemykset tietojärjestelmästä ja järjestelmän sen hetkisestä käytön tilasta. Sen lisäksi listasin myös kaikki haastateltavien esittämät tarpeet järjestelmän ominaisuuksista ja käytöstä. Tämän jälkeen muodostin toimenpide-ehdotukset perustuen haastateltavien näkemyksiin oikeasta tavasta käyttää tietojärjestelmää ja sen ominaisuuksista sekä omiin järjestelmän käyttökokemuksiini.

4 Tiedon kerääminen riskienhallinnan ja turvallisuusjohtamisen kannalta

Tiedonkeruun merkitys turvallisuusjohtamisen ja riskienhallinnan kannalta on asiantuntijoiden mielestä merkittävää. Samoin on myös nykyaikaisen tietojärjestelmän käyttäminen tiedon keräämisen välineenä. Koskinen (2009) sanoo että tietojen kerääminen, hallinta ja käyttö S-ryhmässä riskienhallinnan näkökulmasta liittyvät toiminnan kehittämiseen ja mittaamiseen, toiminnan kehittymisen seurantaan, sisäiseen tiedonvälittämiseen, parhaitten käytäntöjen ja todellisista tilanteista syntyneiden esimerkkien levittämiseen ja ovat päätöksenteon tuki uutta toimintaa suunniteltaessa ja riskienhallintatoimenpiteistä päätettäessä.

Myös Laustola (2009) nostaa tiedonkeruun merkityksen korkealle. Kehittämistoimet voidaan keskittää oikeisiin osa-alueisiin tai kokonaisuuksiin ja oikealla tavalla kun tiedetään kohteiden nykytila. Riskienhallinnan suunnittelijoiden pitää päästä niin sanotusti ruohonjuuritasolle, kerätä ja hyödyntää sieltä saatava tieto. Ilman tiedon analysointia ei kehittyminen ole mahdollista. Saman viittaavat myös Hovi, Ylinen ja Koistinen (2001, 31) tähdentäen, että perustieto ei ole juuri hyödyllistä vaan siitä pitää muodostaa informaatiota. Informaatiossa tieto on esitetty oikeassa yhteydessä ja se vastaa käyttäjän tarpeisiin. Tässä yhteydessä tiedot pitää siis osata jalostaa niin, että niihin voidaan esimerkiksi perustaa riskienhallinnalliset toimenpiteet.

Koska SOK Riskienhallinta-yksikön riskienhallintatyössä ohjataan useita eri kohteita ja kokonaisuuden osia, on kyettävä erottelemaan kerätyistä tiedoista kokonaisuuden kannalta parhaimmat vaihtoehdot ja sovellutukset ja ottamaan ne käyttöön kaikkialla. Tämä on Laustolan (2009) mukaan haasteellista, etenkin silloin jos prosessit eivät ole selkeästi kuvattu eikä niiden riskejä ole analysoitu.

Tietojärjestelmän käyttäminen helpottaa käsin tehtävää työtä, sillä S-ryhmän kokoluokassa tietoja voitaisiin kerätä 1600:stä toimipaikasta. Yhtenäinen järjestelmä mahdollistaa myös tiedon koostamisen ja analysoinnin nopeasti ja monipuolisesti. Tietojärjestelmän haittapuolia on se, että yleisesti ottaen erilaisia järjestelmiä on käytössä paljon. Muutosten tekeminen voi aiheuttaa käytännön kannalta ongelmia tuoden järjestelmien käyttäjille haasteita, kun heidän

tulee omaksua uusia ominaisuuksia. Ominaisuuksien kehittäminen ja muutosten tekeminen on teknisesti helppoa, mutta kokonaisuuden kannalta vaikeaa. Tietojärjestelmät tuovat mukanaan myös aina kustannuksia, vaativat suojausjärjestelyjä ja jatkuvaa kehittämistä. (Koskinen 2009)

Tietoturvallisuuspäällikkö Tupala (2009) tuo esiin näkemyksensä tietojärjestelmistä tietoturvallisuuden hallinnan näkökulmasta. Hän toteaa että tietojärjestelmän tulee ohjata sen sisältämän tiedon käyttöä asianmukaisin suojausmekanismein. Tietoon ei saa päästä käsiksi muut kuin sallitut käyttäjät, tiedot eivät saa muuttua kuin tarkoituksellisesti ja tietojen on oltava saatavilla ohjaamassa ja edistämässä työntekijöiden työntekoa. Luonnollisesti tietojärjestelmän rooli on siis keskeinen hallittaessa siihen liittyviä riskejä.

Käytäntö on osoittanut, että järjestelmien käytössä ohjeistuksien noudattamiseen sisältyy aina myös ongelmia niiden oikeasta tulkitsemisesta. Kun käyttäjiä järjestelmällä on useita, on varmasti myös useita tapoja käyttää järjestelmää ja suorittaa ohjeistettuja toimenpiteitä. Syyt voivat johtua kokemuksen määrästä tai asenteesta toimenpidettä ja siihen liittyviä asioita vastaan. Jos työntekijä ei koe tärkeäksi raportoida eteenpäin normaalista toiminnasta poikkeavaa tapahtumaa ja hänellä on tapana suhtautua ohjeistuksiin välinpitämättömästi, ei hän todennäköisesti silloin kirjaa poikkeamailmoitusta järjestelmään. Tämä johtaa siihen, että järjestelmän sisältämän tiedon luotettavuus kärsii. Koska poikkeamailmoituksen tekeminen ei tapahdu automaattisesti, ei järjestelmän sisältämää tietoa tarkastellessa voida olla täysin varmoja siitä, ovatko kaikki poikkeavat tilanteet raportoitu järjestelmään vai ei. (Laustola 2009.)

Luotettavuuteen liittyy myös virhetilanteet. Virhe voi syntyä joko järjestelmässä, jolloin siihen syötetty tieto muuttuu tai katoaa, tai virheen voi tehdä myös järjestelmän käyttäjä syöttäessään tai tulkitessaan tietoa. Perinteisesti virheitä lähdetään etsimään järjestelmästä, mutta yleensä käyttäjien tekemät virheet ovat yleisempiä. Kriittisiä virheitä voi kuitenkin lähtökohtaisesti sisältyä niin käyttäjiin kuin järjestelmäänkin. Siksi on tärkeää että järjestelmän tietoturvallisuusnäkökulmat otetaan huomioon jo järjestelmää suunniteltaessa. (Tupala 2009.)

5 Kehittämissuunnitelman lähtökohdan määrittely

Kehittämissuunnitelman lähtökohta on määritetty asiantuntijahaastatteluiden sekä järjestelmästä saatavien tietojen perusteella. Tietojärjestelmän on tarkoitettu olevan käytössä matkailu- ja ravitsemistoimialalla hotelliketjujen yksiköissä. S-ryhmässä on myös erillisiä ravintolayksiköitä, mutta niihin tietojärjestelmää ei ole viety. Lisäksi järjestelmä on

rakennettu tavarataloketjun, kauneuden erikoisliikeketjun ja liikennemyymäläketjun käytettäväksi.

SOK Riskienhallinta-yksikön päällikkö Koskinen (2009) kertoo, että tietojärjestelmä otettiin käyttöön, jotta turvallisuuteen liittyvää tietoa voitaisiin kerätä ja hallita koko S-ryhmän noin 1600 toimipaikan verkostossa. Kun järjestelmä hankittiin, asetettiin sille tavoitteita mutta niiden toteutumista ei ole mitattu. Suunnitelmien vieminen käytäntöön jäi toteutumatta kunnolla, koska järjestelmän soveltaminen osoittautui haasteelliseksi. Järjestelmän ylläpito on vienyt kaikki siihen suunnitellut resurssit, jolloin käyttäjistä ja käyttäjäystävällisyydestä huolehtiminen on unohtunut. Sittemmin järjestelmä ja ympäristö ovat muuttuneet, joten tavoitteiden asettelu tulisi tehdä uudelleen. Se kuitenkin on pysynyt ja pysyy muuttumattomana, että järjestelmää hallinnoidaan Riskienhallintayksikössä.

5.1 Poikkeamailmoitukset

Järjestelmään syötettyjen poikkeamailmoitusten tarkastelu osoittaa hyvin, miten järjestelmä on ilmoitusten tekemisen osalta käytössä. Poikkeamailmoitukset on laskettu manuaalisesti tietojärjestelmän tietokannasta ja lajiteltu yksiköittäin, jonka jälkeen lukumäärät on muutettu suhteellisiksi arvoiksi verrattuna ilmoitusten ja toimipaikkojen kokonaismääriin. Näin on menetelty, koska poikkeamailmoitusten lukumäärät ovat ainoastaan opinnäytetyön toimeksiantajan sisäiseen käyttöön tarkoitettua tietoa. Taulukko yksi (1) kuvaa tietojärjestelmään syötettyjen poikkeamailmoitusten suhteellista jakaantumista vuoden 2008 aikana matkailu- ja ravitsemis-, liikennemyymälä- sekä tavaratalo- ja erikoisliiketoimialan välillä. 41,8 prosenttia ilmoituksista tehtiin hotelliketjujen toimipaikoissa, 4,2 prosenttia liikennemyymälöissä, 0,3 prosenttia kauneuden erikoisliikeketjun ja loput 53,7 prosenttia tavarataloketjun yksiköissä. Majoitus- ja ravitsemistoimialan toimipaikoista 33 eri hotellia oli tehnyt ilmoituksia, liikennemyymäläketjusta neljä toimipaikkaa, tavarataloketjusta kolme toimipaikkaa ja kauneuden erikoisliikeketjuun kuuluneista yksi paikka. Taulukko kaksi (2) kuvaa poikkeamailmoituksia tehneiden toimipaikkojen suhteellista määrää verrattuna kyseisen toimialan tai ketjun kaikkien toimipaikkojen määrään. Matkailu- ja ravitsemistoimialan toimipaikoista yli puolet on tehnyt tarkastellulla aikajaksolla ilmoituksia. Muilla aloilla ilmoitusten syöttäminen on huomattavasti vähäisempää.

MaRa-toimiala	Liikennemyymälä	Tavaratalo	Erikoisliike	KAIKKI
41,8%	4,2%	53,7%	0,3%	100%

Taulukko 1. Poikkeamailmoitusten jakaantuminen toimialoille vuonna 2008

MaRa-toimiala	Liikennemyymälä	Tavaratalo	Erikoisliike
57,9%	4,0%	13,6%	6,7%

Taulukko 2. Poikkeamailmoituksia tehneiden toimipaikkojen jakaantuminen toimialoille vuonna 2008

Tarkastelussa tulee ottaa huomioon se, että ilmoitettavia poikkeamatapahtumia ei ole välttämättä tapahtunut ollenkaan kyseisellä aikajaksolla, jolloin järjestelmän tietokantaan ei ole tallentunut yhtään ilmoitusta.

5.2 Turvallisuuden omavalvonta

Turvallisuuden omavalvonnan suorittaminen tapahtuu järjestelmässä ohjatusti ajastetuin sähköpostiviestein, jotka ilmoittavat toimipaikkojen vastuuhenkilöille milloin omavalvonta tulee jälleen suorittaa. Järjestelmän käyttäjähallinnassa tulisi siis jokaiselle toimipaikalle olla käyttäjätunnus ja siihen yhdistetty sähköpostiosoite, jotta automaattinen sähköpostiviesti tavoittaa toimipaikan henkilöstön. Järjestelmästä ei ollut mahdollista selvittää niiden toimipaikkojen tarkkaa määrää, joissa omavalvonnan suorittaminen on tehty ajallaan. Siinä ei ole saatavilla taulukkoa, listaa tai muuta vastaavaa, jolla omavalvonnan suorittaneet toimipaikat voisi tarkistaa. Myöskään järjestelmän käyttäjähallinnan kautta ei suoraan tai helposti saa listaa toimipaikoista ja niihin yhdistetyistä sähköpostiosoitteista tai nimetyistä käyttäjistä.

5.3 Raportointi

Raportointityökaluun on ennalta ohjelmoitu poikkeamailmoituksia, omavalvontaa ja verkkokoulutuksia varten raporttigeneraattorit, jotka muodostavat graafisen raportin käyttäjän valitsemien vaihtoehtojen mukaisesti. Raportit eivät ole kovin monipuolisia, sillä kuvaajavaihtoehdot ovat hyvin rajoitettuja. Lisäksi raportteihin saa näkyviin kerrallaan informaatiota vain yhdestä tai kahdesta kohteesta. Lisäksi raporttien käytettävyys on huonoa, sillä järjestelmä luo raportin ainoastaan kuvana, jonka hyödyntäminen jatkossa on hankalaa ja vaatii muokkausta sopivampaan muotoon riippuen jatkokäytöstä.

5.4 Käytettävyys

Riskienhallintayksikön päällikön mukaan (Koskinen 2009) järjestelmän käytettävyys ei ole kovin hyvä. Sitä käytetään toiminnan seuraamiseen, mutta hänen arvionsa mukaan heikosti, sillä järjestelmästä ei osata ottaa kaikkia hyötyjä irti tai järjestelmä ei tuota sellaista

informaatiota mitä sen pitäisi tuottaa. Poikkeamailmoitusten kirjaaminen ja omavalvonnan suorittaminen on helppoa, mutta muussa käytettävyydessä on parannettavaa. Järjestelmän tuottama lisäarvo ei synny pelkästään käyttäjien kirjauksista vaan järjestelmästä saatavan tiedon avulla tulee pystyä osoittamaan kehityskohteita ja tuloksia. Erityisesti käytettävyys raportoimisessa järjestelmän sisältämistä tiedoista eteenpäin on haaste. Johdon ja toimintaa kehittävien pitää pystyä pääsemään tietoihin käsiksi helpommin kuin nyt, varsinainen johdon rooli puuttuu järjestelmästä kokonaan. Käytön laajuudesta Koskinen toteaa, että käyttö tapahtuu suurelta osalta toimipaikkatasolla ja jonkin verran tytäryhtiöiden ja liiketoiminta-alueiden kehittämisessä.

Oman vastuualueensa tarpeisiin nykyinen järjestelmä vastaa yritysturvallisuuspäällikkö Laustolan (2009) mukaan huonosti. Toimipaikkoja järjestelmä palvelee kohtalaisesti, mutta hänen omien työtehtäviensä kannalta sen ominaisuudet eivät ole riittävät. Järjestelmästä puuttuu automaattisia toimintoja, jotka tuottaisivat raportteja joista saisi nopeasti selkeän kuvan tilanteesta. Nyt käyttäjän pitää itse käydä etsimässä tietoa, joka vie paljon aikaa. Lisäksi hänen mielestään käytössä oleva järjestelmä ei nykyisellään mahdollista tietojen helppoa vertailua toimipaikkojen välillä. Tarvetta on esimerkiksi useamman kuin kahden toimipaikan keskinäiselle vertailulle.

Poikkeamailmoitusten sähköpostijakelu on Laustolan (2009) mielestä hyvä ominaisuus, mutta omavalvonta-osiossa sisällön muokkaamisen mahdollisuuden puuttuminen on huono asia. Sisältöä pitäisi päästä muuttamaan helposti tarvittaessa. Osion kehittämisen lisäksi pitäisi myös luoda toimintatapa omavalvonnan seuraamiseksi ja reagoimiseksi ongelmiin, sillä tähän asti omavalvonnan suorittamista ei ole seurattu.

Yksi osa yritysturvallisuuden kokonaisuutta on tietoturvallisuus, joka on jossain määrin huomioitu myös S-ryhmän riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmässä poikkeamatyypeissä ja turvallisuuden omavalvonnassa. Tietoturvallisuuspäällikkö Tupalan (2009) mukaan järjestelmä sisältää kuitenkin liian vähän asiaa tietoturvallisuudesta. Poikkeamia ei ole määritelty kunnolla, turvallisuuden omavalvonnan tietoturvallisuuden osuus on suppea ja ohjeistus käyttäjille puuttuu. Tämän vuoksi järjestelmä ei tue Tupalan mielestä tietoturvallisuuden johtamista lainkaan. Järjestelmältä odotetaan koostettua tietoa siitä, mitä S-ryhmässä tapahtuu liittyen tietoturvallisuuteen. Myös tietojärjestelmän käytön hajanaisuus johtaa siihen, että tietoa ei saada kattavasti ja luotettavasti kaikilta liiketoiminta-alueilta. Koska järjestelmä ei ole aktiivisessa käytössä kaikilla toimipaikoilla, tieto ei välttämättä kulkeudu SOK:n riskienhallintayksikköön asti, vaan jää toimipaikkaan tai käsitellään vain alueellisesti. Tällä hetkellä tieto kulkeutuu tietoturvallisuuspäällikön korviin useimmiten muuta kautta, eikä tallennu järjestelmään jolloin myöskään järjestelmästä ei ole

saatavissa tilastoja. Tupala sanoo, että keskitetty ratkaisu tiedon keräämisen on parempi kuin tietojen yhdisteleminen eri lähteistä.

Majoitus- ja ravitsemistoimialan kenttäpäällikkö Lindholm (2009) toteaa että tietojärjestelmä ei ole kovin helppokäyttöinen. Toimipaikoilla käyttöoikeuksia on vain esimiehillä, jotka kirjautuvat järjestelmään ja syöttävät poikkeamat. Järjestelmiä yksiköissä on paljon, joten poikkeamien kirjaamisen tulisi olla mahdollisimman yksinkertaista. On olemassa vaara, että poikkeamailmoituksia jää tekemättä koska esimiesten tunnukset ovat hukassa, järjestelmän käytön ohjeistus on puutteellista tai he eivät mahdollisessa kiireessä ehdi kirjata ilmoitusta heti koska kokevat järjestelmän käytön hankalaksi ja aikaa vieväksi. Tämä ei kerro välttämättä esimerkiksi toimipaikan huonosta turvallisuuskulttuurista vaan enemmänkin siitä, että järjestelmiä saattaa olla käytössä liikaa. Tukitoimintoihin liittyviä tehtäviä tärkeämmäksi koetaan tulokseen suoranaisesti vaikuttavat tehtävät, joten poikkeamailmoitus tehdään sitten kun nämä on hoidettu.

Tuki- ja kehittämistoimintojen tarpeita majoitus- ja ravitsemistoimialalla järjestelmän ominaisuudet eivät täytä. Raportteja tarvitaan muun muassa riskianalyysien tekoon, toiminnan suunnitteluun ja poikkeavien tapahtumien seurantaan työsuojelun näkökulmasta. Tällä hetkellä järjestelmän raportointia ei juuri voi edellä mainituissa hyödyntää, sillä tarvittavat tiedot ovat hankalia löytää, niitä ei saa järjestelmästä ulos sopivassa muodossa ja ne eivät välttämättä ole luotettavia. Ajantasaisia ja luotettavia raportteja tarvitaan esimerkiksi silloin kun henkilöitä vaihtuu tai pitää raportoida tilanteista organisaatiossa ylöspäin. (Lindholm 2009.)

Lindholmin (2009) mielestä ongelman järjestelmän tiedon luotettavuudessa aiheuttaa juuri se, että tietojen syöttö ei tapahdu automaattisesti eikä täydellä varmuudella. Hänen kokemuksiensa mukaan tietyt toimipaikat syöttävät tietoja luotettavasti mutta toiset taas eivät ollenkaan. Tämän takia järjestelmästä saataviin yhteenvetoihin ei voi luottaa, johtopäätöksiä tehdessä pitää käyttää hyvin paljon harkintaa.

6 Toimintaympäristön asettamat tarpeet kehittämiselle

Tietojärjestelmä pitää suunnitella rakenteellisesti sellaiseksi, että tietojen käsittely on mahdollista niin kuin on suunniteltu, oli kyseessä minkälainen tietojärjestelmä tahansa. Järjestelmän tulisi ohjata tiedon käsittelyä, sen sisältämän tiedon pysyä luottamuksellisena ja järjestelmän rakenteellisen maailman vastata järjestelmää käyttävien ja hyödyntävien tarpeisiin. Uusittaessa ohjeistuksia liittyen tietojärjestelmän sisältämiin aihealueisiin, tulee myös järjestelmän sisältö päivittää. Esimerkiksi tietoturvapolitiikan päivittyessä, tulee

järjestelmän sisältävän turvallisuuden omavalvonnan tietoturvallisuuteen liittyvät kysymykset tarkistaa ja korjata vastaamaan voimassaolevia käytäntöjä. (Tupala 2009.)

Tietoturvallisuuspäällikön toimessa merkittävää olisi saada tietoon turvallisuuden omavalvonnan tilanteesta kokonaisuutena toimialakohtaisesti. Yksityiskohtaisesti seurattavat asiat vaihtelevat sen mukaan, mihin asioihin tullaan tulevaisuudessa kiinnittämään enemmän huomioita. Pitkällekin aikavälille sijoittuva vertailu on hyödyllistä ja kertoo trendeistä. Kaikki S-ryhmän Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän sisältämä tieto tulisi koostaa eri näkökulmista ja hyödyntää toiminnan suunnittelussa. Myös erikseen tietoturvallisuuteen keskittyviä kyselyitä voisi käyttää turvallisuuden omavalvonnan lisäksi. (Tupala 2009.)

Tupala (2009) on sitä mieltä, että jatkuva raportointi kannattaa rakentaa siten, että se tapahtuu järjestelmässä automaattisesti. Hänen mukaansa raportointia suunniteltaessa olisi hyvä lähteä liikkeelle kvartaaliraportoinnista ja harventaa tai tihentää raportointia aihealueittain, riippuen siitä, mikä kyseiselle aihealueelle sopii parhaiten. Tämän pystyy todentamaan käytännössä kokeilemalla ja analysoimalla tuloksia. Tietoturvallisuuteen liittyen oleellisinta on seurata tapahtumia ja reagoida vakavissa häiriötilanteissa.

Majoitus- ja ravitsemiskaupan toimialan tukitoiminnoissa työskentelevän turvallisuusasioista vastaavan Lindholmin (2009) tarpeet tiedon saannin yksityiskohdista rajoittuvat poikkeamien sähköposti-ilmoitusten osalta merkittävimpiin tapahtumiin, kuten kaikkiin mediakynnyksen ylittäviin, kuolemantapauksiin ja merkittäviin loukkaantumisiin. Oleellista on selkeä ja kuvaava otsikko. Lindholm toteaa että sähköpostia hän vastaanottaa paljon, joten pienimmistä tapahtumista hän ei tietoa tarvitse. Lisäksi liikkuva työ ja sähköpostin käyttö matkapuhelimella vaatii lyhyttä ja informatiivista sähköposti-ilmoitusta. Matkapuhelimella ei voi kirjautua itse tietojärjestelmään tarkastelemaan ilmoitusta. Turvallisuuden omavalvonnan osalta Lindholm tarvitsee käyttöönsä raportteja, joista selviää yhdellä silmäyksellä kaikki omavalvonnan suorittaneet toimipaikat sekä toimipaikkakohtaisesti suoritetut ja suorittamatta jääneet yksityiskohdat. Raportit tulisi saada järjestelmästä ilman käsin suoritettavaa informaation yhdistelemistä. Uutena järjestelmän ominaisuutena Lindholm mainitsee mahdollisuuden kirjata henkilöstön turvallisuuskoulutustilanteen. Turvallisuuteen liittyvien asioiden yhdistäminen samaan ympäristöön olisi käytännön kannalta hyödyllistä.

Uusien järjestelmien käyttöönotosta Lindholm (2009) toteaa, että ne on syytä olla pilotoitu eli kokeiltu käytännössä etukäteen ja merkittävimmät virheet tulee olla korjattu. Tärkeää on myös, että järjestelmä pystyy alusta asti vastaamaan esille nouseviin tarpeisiin. Näin edesautetaan järjestelmän peruskäyttäjiä omaksumaan järjestelmän ominaisuudet ja käyttö vaivatta. Lisämotivointia voi Lindholmin mukaan myös tehdä asettamalla erilaisia kannusteita.

Palkitseminenkin voi tulla kyseeseen, jos henkilöstö ja vastuuhenkilöt ovat aktiivisesti edistäneet työympäristössään uuden järjestelmän käyttöönottoa.

SOK Riskienhallinta-yksikön Laustola (2009) sanoo, että järjestelmästä saatavien raporttien tietojen pitää olla sellaisessa muodossa että asioiden vertailu eri tasoilla asiakokonaisuuksien sisällä onnistuu. Kehittäjille on tärkeää, että kokonaisuuden hallinta on vaivatonta. Järjestelmän tiedoista pitää saada muodostettua joustavasti erilaisia yhteenvetoja, raportteja ja visuaalisesti selkeitä kuvaajia. Myös automaattisesti muodostuvat ja käyttäjille toimitettavat raportit olisivat Laustolan mielestä hyödyllisiä käyttäjille.

Käyttäjien kannalta hyödyllistä olisi jos järjestelmä muistuttaisi turvallisuuden omavalvontaan merkittyjen toimenpiteiden aikataulujen umpeutumisesta. Käytännössä toimipaikan turvallisuusvastaava saisi sähköpostimuistutuksen umpeutuvasta määräajasta suorittaa puutteen aiheuttaneen tilanteen korjaavat toimenpiteet. Lisäksi omavalvonnassa puutteeksi eli avoimeksi jääneen osa-alueen korjaaviin toimenpiteisiin pitäisi joka kerta antaa prioriteetti esimerkiksi arvoilla yhdestä kolmeen (1-3), jolloin yksi on tärkein ja kolme vähiten tärkein. Erillinen puutteiden yhteenvetosivu toimenpide-, prioriteetti- ja määräaikamerkintöineen selkiyttäisi ja helpottaisi omavalvontaa suorittavan työtä. Myös toimintaa ohjaavien tahojen pääsy tälle yhteenvetosivulle edesauttaisi tilanteen seuraamista. Järjestelmän tulisi muodostaa omavalvonnasta automaattisesti ja tietyin väliajoin raportteja, jotka välittyisivät toimipaikan johtajalle automaattisesti. Raportit ilmaisisivat omavalvonnan avoimet kohteet ja niiden korjaamiseksi suunnitellut toimenpiteet määräaikoineen. (Laustola 2009.)

Tarvetta on eri osa-alueiden vertailulle keskenään, kuten tietoturvallisuuden tai paloturvallisuuden välillä tai yksittäisen alueen suhdetta kokonaisuuteen. Tällöin voidaan löytää ne alueet, joilla on eniten puutteita ja joissa tarvitaan ohjausta. Erilaisten raporttien sisältöjen kokeileminen olisi kannattavaa ja se onnistuisi keräämällä tiedot järjestelmästä manuaalisesti. Mutta kun sopiva malli löytyy, siitä pitäisi saada rakennettua automaattisesti tulostuva. (Laustola 2009.)

Laajempaa käyttöä ajatellen on hyvä valmistautua järjestelmän käyttöön muualla kuin suomenkielisillä alueilla. Sisällöt tulisi olla käännettävissä toiminta-alueiden kielille, tai vaihtoehtoisesti englannin kielelle. Tällöin kielikysymykset eivät asettaisi rajoitteita järjestelmän käytölle. Myös käyttäjien koulutukseen ja ohjeistukseen pitäisi kiinnittää huomiota. Peruskäyttäjiä, eli poikkeamailmoitusten syöttäjiä ja omavalvonnan suorittajia ei välttämättä tarvitse erikseen kouluttaa käyttämään järjestelmää. Tälle kohderyhmälle riittää selkeiden kirjallisten ohjeistuksien tekeminen. Niille asiantuntijoille, jotka hyödyntävät

järjestelmästä saatavaa tietoa, erillinen käyttäjäkoulutus voisi olla hyödyllinen. (Laustola 2009.)

Yhteenvetona todettakoon, että järjestelmän sisällön pääasiassa muodostavat poikkeamailmoitukset ja turvallisuuden omavalvonta ovat riittäviä ominaisuuksia, joilla riskienhallintayksikkö ja muut toimialoja ohjaavat tahot pystyvät seuraamaan toimipaikkojen arkea turvallisuusnäkökulmasta. Kehitystä tarvitaan kuitenkin järjestelmään liittyviin toimintatapoihin, erityisesti turvallisuuden omavalvonnan seuraamiseen. Nykyisessä tilanteessa tuloksia ei seurata aktiivisesti johtuen siitä, että järjestelmä ei tarjoa tuloksia suoraan sellaisessa muodossa, että niitä voisi hyödyntää sellaisinaan. Lisäksi omavalvonnan asiasisältö ei enää ole yhdenmukainen voimassaolevan turvallisuusohjeistuksen kanssa. Poikkeamailmoitusten rakenne on riittävällä tasolla, mutta myös tässä ominaisuudessa tulosten raportointi vaatii kehittämistä. Suunnittelua tukemaan tarvitaan raportointia kuukausi-, vuosineljännes- ja vuositasolla, jossa ilmenee ne toimipaikat joissa ohjeiden mukaista poikkeamaraportointia tehdään. Poikkeamailmoituksiin reagoimista pitäisi myös kehittää. Poikkeamailmoitus pitäisi pystyä merkitsemään luetuksi ja lisäämään eri käyttäjien ehdotuksia suoritettavista toimenpiteistä.

7 Toimenpide-ehdotukset

Seuraavassa ovat listattuna toimenpide-ehdotukset, jotka toteuttamalla voitaisiin kehittää järjestelmää ja sen käyttöä tarpeiden mukaisiksi.

Pilottiprojekti

Toimialojen yksiköille tulee antaa yhtenäiset toiminta- ja käyttöohjeet tietojärjestelmän käytön vakinaistamiseksi osaksi yksiköiden toimintatapoja. Järjestelmän käyttäjätasot tulee määritellä ja muodostaa käyttäjätunnukset näiden tasojen mukaisesti. Ohjeistukset tulee toimittaa ja toimintatavat ottaa käyttöön ensin erikseen valittavissa yksiköissä ennen niiden levittämistä koko toimialan yksiköille. Näiltä yksiköiltä kerätään palautetta ja käyttökokemuksia, joiden perusteella ohjeistuksia, toimintatapoja ja järjestelmän sisältöä korjataan ja päivitetään ennen niiden levittämistä laajempaan käyttöön.

Johdon rooli

Johdon rooli järjestelmän käytössä tulee määritellä yhdessä järjestelmän käyttäjätasojen määrityksen kanssa. Määrittelyssä tulisi huomioida johdon tarpeet tiedolle, tiedon saannin helppous ja merkityksellisten yksityiskohtien selkeä erottuminen.

Raportointikäytänteet

Järjestelmän raportointityökalu tulisi parantaa vastaamaan toimintaympäristön tarpeita. Järjestelmästä tulee automaattisesti muodostua valituille käyttäjille ohjautuvat raportit, jolloin henkilöresursseja ei tarvita raporttien tulostamiseen ja kokoamiseen manuaalisesti. Näiden raporttien muodostumisen tiheyttä ja raporttien sisällön laajuutta tulisi pystyä pääkäyttäjän ohjaamaan, sillä eri käyttäjille tulee pystyä antamaan heidän erityistarpeitaan vastaavaa tietoa. Eri käyttäjätasoille tulisi kohdentaa omanlaisensa raportit. Näiden raporttien sisällöt tulisi muodostaa pilottiprojektin yhteydessä, jolloin raporteista saadaan kerättyä palautetta ja raporteista kehitetään lopulliset versiot automaattista jakelua varten. Automaattisten raporttien lisäksi käyttäjillä tulee olla nykyiseen tapaan mahdollisuus itse muodostaa raportteja. Raporttityökalun tulee pystyä joustavasti tarjoamaan käyttäjille erilaisia raportteja siinä määrin, mitä järjestelmän sisältämä tieto mahdollistaa.

Kieliversiointi

Järjestelmän käyttöliittymä ja sisällöt tulee pystyä muuttamaan englanninkielelle käyttäjästä riippuen. Tämä mahdollistaa järjestelmän käytön myös ulkomailla olevissa yksiköissä.

Sisältöjen päivitysohjelma

Järjestelmän pääkäyttäjälle tulee luoda sisältöjen päivitysohjelma, jolla varmistetaan tietojärjestelmän sisältöjen ajantasaisuus ja tarpeellisuus, etenkin liittyen turvallisuuden omavalvontaan. Päivitysohjelmassa tulee asettaa toimialakohtaisesti aikamääreet sisältöjen tarkistamiselle sekä keinot näissä aikamääreissä pysymiseksi. On myös syytä huomioida järjestelmän sisältöihin liittyvät muut prosessit tai projektit, joiden tulokset voivat vaikuttaa tietojärjestelmän sisältämään informaation. Lisäksi päivitysohjelmaan tulee sisältyä käytännön menettelyohjeet siitä, miten sisältö päivitetään.

Poikkeamien kuittausmahdollisuus

Järjestelmän tulee mahdollistaa kommenttien kirjaamisen poikkeamailmoituksiin ja turvallisuuden omavalvontaan liittyviin dokumentteihin jälkikäteen. Kommenttien lisäämismahdollisuus tulee olla niillä käyttäjillä, joiden vastuualueille poikkeamailmoituksen tai omavalvonnan suorittanut yksikkö kuuluu.

Omavalvonnan toimenpide-muistutukset

Turvallisuuden omavalvonta–työkaluun tulee lisätä ominaisuus, joka muistuttaa omavalvonnan suorittajaa korjaavien toimenpiteiden määräaikojen umpeutumisesta.

Sähköposti-ilmoitukset

Sähköposti-ilmoituksien sisältämän informaation lisäämistä tulee arvioida. Pelkkä poikkeaman otsikko ei välttämättä riitä, vaan sähköposti-ilmoituksen tulisi sisältää tarkempia tietoja tapahtumasta, jolloin erillistä kirjautumista tietojärjestelmään ei tarvita näiden tietojen saamiseksi.

Käyttäjäkoulutukset

Järjestelmän käytön laajentuessa tulisi arvioida eri käyttäjätasojen tarpeet tietojärjestelmään liittyvälle koulutukselle. Koulutus voisi olla tarpeellinen erityisesti niille käyttäjille, jotka hyödyntävät järjestelmästä saatavaa tietoa riskienhallintatoimenpiteiden suunnittelutyössä, eli käytännössä toimialojen keskijohdolle ja riskienhallinnan asiantuntijoille.

Omavalvonnan yhteenvetosivu

Järjestelmästä tulisi pystyä tulostamaan raportti, jolla on eroteltu valitun yksikön turvallisuuden omavalvonnan vastaukset. Raportissa tulisi näkyä suoritetut kohdat sekä avointen kohtien toimenpiteet ja määräajat, vastuuhenkilöt sekä tieto siitä, milloin mikäkin omavalvonnan kohta on suoritettu.

Järjestelmän uusiminen

Nykyinen tietojärjestelmän käyttöliittymä on vanhanaikainen ja se tulee saattaa nykyaikaiseksi. Myös tietojärjestelmän tekninen kokonaisuus tulee arvioida sen hetkisen käytön laajuuden ja muiden mahdollisten tekijöiden näkökulmasta. On myös syytä arvioida mahdollinen tarve järjestelmäympäristön korvaamiseksi uudella ratkaisulla, jos nykyisen päivittäminen tarpeita vastaavaksi ei ole kohtuullisin ajallisin ja rahallisin panostuksin mahdollista.

8 Onnistumisen arviointi

Esitin toimenpide-ehdotukset SOK Riskienhallinta –yksikön asiantuntijoille saadakseni kommentteja ja palautetta ehdotusten työstämiseksi. Paikalla oli riskienhallintayksikön päällikkö Mikko Koskinen, riskienhallintapäällikkö Anna Koskenniemi, hävikinhallintapäällikkö

Anna-Liisa Flink sekä yritysturvallisuuspäällikkö Jari Takki. Esitin toimenpide-ehdotukset ja niille asettamani tärkeysluokituksen. Esitys herätti paljon keskustelua tietojärjestelmän heikkouksista ja puutteista sekä korjaavien toimenpiteiden tärkeysjärjestyksestä. Toimeksiantajan näkökulmasta tärkeimmiksi nousivat raportoinnin sekä käyttäjätasojen määrittäminen ja samalla käyttäjähallinnan kehittäminen. Konkreettisena kehityskohteena toimeksiantaja nosti käyttäjätunnusten yhdistämisen henkilökunnan järjestelmän käyttäjätunnukseen, jolloin erillisiä tunnuksia tietojärjestelmään ei tarvittaisi.

Kehittämistyötä voi pitää onnistuneena, sillä tavoite tietojärjestelmän käytön ja ominaisuuksien nykytilanteen selvittämisestä ja määrittelemisestä toteutui. Ongelmakohdat saatiin järjestelmän käytön kannalta selvitettyä. Myös tavoite keinojen löytämisestä ongelmien selvittämiseksi toteutui, sillä työssä esitellään useita konkreettisia ehdotuksia toimenpiteiksi järjestelmän kehittämiseksi. Toimenpidelista ei kuitenkaan ole tyhjentävä. Kehittämissuunnitelmalle huomattavaa lisäarvoa olisi tuonut toimenpiteiden kokeileminen käytännössä ja niiden edelleen kehittäminen. Nyt suunnitelma antaa vain suunnan kehittämiselle mutta ei ohjaa sen pidemmälle.

Lähteet

Kirjallisuuslähteet

Hovi, A.,Ylinen, J. ja Koistinen, H. 2001. Tietovarastot liiketoiminnan tukena. Jyväskylä: Gummerus.

Hirsjärvi, S. ja Hurme, H. 2000. Tutkimushaastattelu. Teemahaastattelun käytäntö ja teoria. 4. painos. Helsinki: Yliopistopaino Kustannus.

Kerkko, Pertti. 2001. Turvallisuusjohtaminen. Porvoo: WS Bookwell Oy.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Jyväskylä: Talentum.

Ojasalo, K., Moilanen, T. ja Ritalahti, R. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Porvoo: WSOY.

Sähköiset lähteet

ISM3 Consortium. 2009. Glossary. Internet:[http://www.ism3.com/index.php?option=com_content&task=view&id=10&Itemid=13] Luettu 27.3.2009 klo 11.01.

SOK-yhtymä Vuosikertomus 2008. 2009. Internet:[http://www.digipaper.fi/sok-yhtyma/27408/] Luettu 17.10.2009.

Turun yliopisto. 1999. Informaatioteknologian laitos. Tietojärjestelmien peruskurssin kurssimateriaali. Internet:[http://www2.cs.utu.fi/kurssit/tietojarjestelmien_peruskurssi/syksy_1999/tietojar.htm] Luettu 27.3. klo 9.54.

Haastattelut

Koskinen, M. 2009. Haastattelu. SOK. Helsinki.

Laustola, R. 2009. Haastattelu. SOK. Helsinki.

Lindholm, J. 2009. Haastattelu. SOK. Helsinki.

Tupala, V. 2009. Haastattelu. SOK. Helsinki.

Taulukot

LIITE 1. Haastattelukysymykset.

1. Haastateltavan koulutus- ja työuratausta.
2. Mikä käytännön merkitys mielestäsi raportoinnilla, tietojenkeruulla ja tietojen hallinnalla on kokonaisvaltaisen riskienhallinnan / turvallisuuden johtamisen kannalta?
3. Mitä tarpeita turvallisuusjohtamisella (tai riskienhallinnan johtamisella) on tietojen hallinnan suhteen?
4. Mitä hyötyä tietojärjestelmän käytöllä on?
5. Mitä haittaa tietojärjestelmän käytöllä voi olla?
6. Miten kuvailisit S-ryhmän Riskienhallinnan ja turvallisuusjohtamisen tietojärjestelmän käyttöä yleisesti tällä hetkellä S-ryhmässä?
7. Mitkä ovat tietojärjestelmän käytön tavoitteet S-ryhmän tasolla?
   a. Entä toimiala/ketju/yksikkökohtaisesti?
   b. Miten järjestelmän käyttö ja siitä saatavan tiedon soveltaminen onnistuisi hyvin?
   c. Miten tiedon hallinta ja raportointi hoidettaisiin käytännössä?
8. Millä tavalla järjestelmä vastaa tällä hetkellä oman vastuualueesi tarpeisiin ja minkälaista tietoa tarvitset oman työsi kannalta järjestelmästä?
9. Mitä kehittämiskohteita itse tietojärjestelmässä on mielestäsi tällä hetkellä?
10. Minkälaisia eri ominaisuuksia tietojärjestelmässä voisi olla turvallisuuden / riskienhallinnanjohtamisen hallitsemiseksi/avuksi?