LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Riskienarviointimenetelmän kehittäminen osana tietoturvallisuuden vaatimustenmukaisuuden arviointia

Halttunen, Seppo

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Riskienarviointimenetelmän kehittäminen osana tieto-turvallisuuden vaatimustenmukaisuuden arviointia

Seppo Halttunen
Turvallisuusosaaminen
Opinnäytetyö
Maaliskuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusosaamisen koulutusohjelma

Seppo Halttunen

Riskienarviointimenetelmän kehittäminen osana tietoturvallisuuden vaatimustenmukaisuuden arviointia

Vuosi 2015 Sivumäärä 67

Nyky-yhteiskunta on riippuvainen tietoverkkojen ja –järjestelmien toiminnasta ja tämän myötä myös niihin kohdistuvat uhkat ja riskit ovat kasvaneet ja muuttuneet vaikutuksiltaan vaarallisemmiksi. Riskienhallinnan merkitys tietoturvallisuuden hallinnassa ja toteuttamisessa on tästä johtuen kasvanut. Tietoturvallisuuteen liittyvät lakien mukaan valtionhallinnon viranomaisten tulee huolehtia siitä, että viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan ja että tietoturvallisuuden vaatimustenmukaisuutta arvioidaan. Vaatimustenmukaisuuden ja riskienhallinnan avulla tehtyjen riskinottopäätösten suhde asettaa arviointitoiminnalle haasteita.

Tämän tutkimuksen tavoitteena oli luoda työkalu, jonka avulla voidaan arvioida tietojärjestelmien tietoturva-arvioinneissa havaittujen poikkeamien aiheuttamien riskien vaikutuksia. Turvallisuustoimenpiteistä ja –kontrolleista huolimatta tietojärjestelmiin kohdistuu aina riskejä, eikä täydellistä tietoturvallisuutta voida käytännössä saavuttaa. Tämän vuoksi on tarpeellista luoda menetelmä, jonka avulla voidaan arvioida jäännösriskien vaikutuksia ja mikä niiden suhde on asetettuihin tietoturvallisuusvaatimuksiin.

Tutkimuksessa on perehdytty riskienhallintaan ja arviointitiedon tuottamiseen liittyviin prosesseihin ja metodologiaan. Arvioinnin kannalta on tärkeää, että siitä saatavat tulokset ovat riittävän kattavia ja oikeellisia, ja että niiden perusteella tehtävät johtopäätökset ovat objektiivisia. Tutkimuksen aikana kehitetyn työkalun suunnittelussa on otettu nämä seikat huomioon.

Työn lopputuloksena on arviointityötä tukeva työkalu, jonka avulla voidaan systemaattista ja rakenteista menetelmää käyttäen tuottaa analyyttisempaa tietoa olemassa olevien tietoturvapoikkeamien aiheuttamista riskeistä. Menetelmän tarkoituksenmukainen käyttäminen vaatii syvällistä tuntemusta arvioitavasta kohteesta ja systemaattisen analyysin tekeminen saattaa olla työmäärältään suuri.

Riskienhallinta on turvallisuustoiminnan tukemiseen käytettävä apuväline, jonka avulla voidaan tehostaa ja kehittää organisaatioiden turvallisuustoimintaa. Tässä työssä kehitetty työkalu on riskienhallintaan tarkoitettu apuväline, jonka avulla riskienhallinnan tavoitetta voidaan edistää.

Asiasanat: Riski, riskienhallinta, tietoturvallisuus, arviointi

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security Competence

Seppo Halttunen

Development of a risk assessment tool as part of an information security audit

Year 2015 Pages 67

The importance of information systems and networks to modern society has grown substantially. Alongside the technological development threats, risks and their potential impact related to the systems have grown and become more hazardous. Because of this the importance of risk management and risk assessment has become more relevant. Finnish laws related to information security require that governmental bodies assess risks related to their activities and that their compliancy to information security requirements are assessed. Assessing risks and the risks' relationship to requirements and compliancy is problematic.

The purpose of this thesis was to develop a tool which enables the assessment of effects of risks based on deviations from given requirements found during an information security audit. Security measures and controls cannot remove risks completely and because of this it is meaningful to create a method which allows assessing the impact of residual risks and their relationship to given information security requirements.

This thesis covers methodologies and processes related to risk management and assessment from a theoretical viewpoint. When doing an assessments it is important that the results are comprehensive and based on correct information and context in order to form an objective opinion or assessment. These principles have been applied in the process of developing the tool in this thesis.

The end result of this thesis is a risk assessment tool that enables a systematic and structured method to provide more analytic information of the risks caused by deviations found in the audited information system. Using the method requires in depth knowledge about the system and the assessment process might be complex and time consuming.

Risk management is a tool among others to support management, planning and development of security in an organization. The tool developed in this thesis is another mean to support risk management and give another perspective to the field.

Keywords: Risk, risk management, information security, assessment

Sisällys

1 Johdanto

Suomen kyberturvallisuusstrategiassa todetaan, että nyky-yhteiskunta on riippuvainen tietoverkkojen ja –järjestelmien toiminnasta ja tämän myötä myös niihin kohdistuvat uhkat ja riskit ovat kasvaneet ja muuttuneet vaikutuksiltaan vaarallisemmiksi. (Turvallisuuskomitea 2013, 1) Riskienhallinnan merkitys tietoturvallisuuden hallinnassa ja toteuttamisessa on tästä johtuen kasvanut.

Tietoturvallisuuteen liittyvät lakien mukaan valtionhallinnon viranomaisten tulee huolehtia siitä, että viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan ja että tietoturvallisuuden vaatimustenmukaisuutta arvioidaan. Yhtenäistä tai velvoittavaa menettelyä riskienhallinnan toteuttamiselle ei ole, jonka vuoksi organisaatioissa käytettävät riskienhallinnan menetelmät vaihtelevat.

Tarkastustoiminnassa riskienhallinnallisten menettelyjen suhdetta vaatimuksiin arvioidaan usein tapauskohtaisesti perustuen kohdeorganisaation itsearvioon, menetelmiin ja niiden kuvauksiin. Arvio on aina hyvin subjektiivinen eikä varsinaista työkalua riskienhallinnallisten menettelyjen arviointiin ole olemassa.

Tarkastusten kohdeorganisaatiot toteuttavat riskienhallintaa standardin tai jonkin muun yleisen hallintamenettelyn mukaisesti. Standardit ja ohjeet antavat hyvät lähtökohdat, mutta lopputuloksen arviointiin tietoturvavaatimuksia vasten näistä ei varsinaisesti ole apua. Olemassa olevien riskienhallintamallien (esim. ISO 31010) avulla pyritään tunnistamaan organisaation toimintaan liittyvät uhat, niiden potentiaaliset vaikutukset ja tarvittavat toimenpiteet. Malleissa ei lähtökohtaisesti arvioida käytettävän menetelmän tuottamia lopputuloksia, vaan ne keskittyvät tehostamaan olemassa olevaa toimintaa. Vaihtelevista käytännöistä johtuen olisi hyvä olla olemassa riippumaton työkalu, jonka avulla voidaan tunnistaa ja arvioida olemassa olevia riskejä ja niiden vaikutuksia ottamatta kantaa alkuperäisiin kohdeorganisaatioiden itsensä tuottamiin riskiarvioihin, joiden laajuus ja taso vaihtelevat.

Työn tavoitteena on luoda työkalu, jonka avulla toteutetut tietoturvakontrollit analysoidaan, arvioidaan jäljelle jäävää jäännösriskiä ja lopputulosta verrataan annettuihin vaatimuksiin. Ideaalitilanteessa tulosten perusteella voidaan tehdä parempi arvio siitä, onko riskinotto perusteltua vaatimuksiin nähden. Olemassa oleviin malleihin tuodaan mukaan uusi elementti, jonka avulla riskiarvion tuloksia verrataan riskienhallinnan ulkopuolelta tuotaviin vaatimuksiin. Olemassa olevat riskit kartoitetaan osana arviointia, jolloin arviointi on objektiivisempi kuin kohdeorganisaation itsearvio.

Työn lopputulosta voidaan pitää onnistuneena, mikäli toteutetun työkalun avulla voidaan saada tuloksia, jotka ovat johdonmukaisempia, objektiivisempia ja paremmin perusteltavissa kuin nykyinen arviointimalli, joka perustuu pitkälti tapauskohtaiseen arviointiin.

2 Tutkimusongelma

Tietoturva-asetuksessa ja laissa tietoturvallisuuden arvioinnista arviointiperusteiksi määritellyissä ohjeissa, standardeissa ja säännöksissä edellytetään, että toimintaan liittyvät tietoturvallisuusriskit kartoitetaan ja turvatoimet riskien vähentämiseksi saatetaan hyväksyttävälle tasolle.

Kun tietoturvallisuuden toteuttaminen perustuu arvioinnin kohteena olevan organisaation tietoturvariskien kartoitukseen ja siitä tehtyihin johtopäätöksiin, miten voidaan arvioida laissakin määriteltyä tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimustenmukaisuutta? Vaikka arviointiperusteina käytettävät ohjeet ja säännökset sisältävät konkreettisia toimintamalleja ja vaatimuksia, ne eivät ole kaikilta osin velvoittavia tai ehdottomia kriteeristöjä. Mikäli arvioitavassa tietojärjestelmässä on esimerkiksi toiminnallisista vaatimuksista johtuen jouduttu jättämään osa turvamekanismeista tai -kontrolleista toteuttamatta ja riskienhallinnallinen päätös tästä on tehty, kuinka tällaisen tietojärjestelmän vaatimustenmukaisuutta voidaan luotettavasti arvioida?

3 Tutkimussuunnitelma

Tutkimuksen tarkoituksena on luoda työkalu riskienhallinnallisten menetelmien ja kontrollien analysoimiseksi ja arvioimiseksi. Apuna työssä käytetään KATAKRI:n (versio II) I-osion vaatimuksia, joiden rinnalla työkalu rakennetaan.

Työkalun avulla pyritään luomaan menettely, jolla voidaan tunnistaa ja analysoida kuhunkin kriteeristössä esitettyyn vaatimukseen liittyviä uhkia sekä niiden mahdollisia vaikutuksia tietoturvallisuuteen. Työkalun pohjalta tehdyn analyysin jälkeen tuloksia voidaan verrata olemassa oleviin kontrolleihin ja näin arvioida kontrollien suhdetta vaatimuksiin. Tavoitteena on työkalun avulla luoda johdonmukaisuutta ja yhteismitallisuutta arviointeihin ja arviointimenettelyihin osana tietojärjestelmien tarkastusprosessia.

Työn tuotoksena syntynyttä arviointityökalua testataan asiantuntijaryhmän avulla. Käytännön testauksella saatuja tuloksia analysoidaan reliabiliteetin ja validiteetin kannalta.

Työn lähtökohtainen oletus on, että organisaatioissa toteutetaan riskienhallintaa ja riskianalyyseja tehdään tietojärjestelmille. On mahdollista, että riskiarvioinneissa uhka-analyysia ei tehdä riittävällä tarkkuudella. Työn tavoitteille asetetaan oletus, että lopputuloksena syntyvän työkalun avulla voidaan saada parempi varmuus siitä, että vaatimustenmukaisten kontrollien puutteiden aiheuttamat jäännösriskit on arvioitu riittävällä tarkkuudella.

4 Kirjallisuuskatsaus ja lähdeaineisto

Tässä luvussa kuvataan työn lähdeaineistoa, joka voidaan jakaa kolmeen eri osa-alueeseen. Ensimmäiseksi käsitellään tutkimusaiheeseen liittyvää lainsäädäntöä, asetuksia ja säädöksiä, jotka ensisijaisesti velvoittavat ja ohjaavat viranomaistoimintaa. Toiseksi käsitellään erilaisia ohjeita ja kriteeristöjä, kuten kansallista turvallisuusauditointikriteeristöä (KATAKRI), Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) tietoturvaohjeita sekä Euroopan Unionin neuvoston turvallisuussääntöjä. Kolmanneksi käsitellään standardeja, menetelmäoppaita ja muuta tutkimusaiheeseen liittyvää kirjallisuutta.

Työssä käytetyt lähteet ovat valtaosin lakeja, asetuksia, ohjeita ja julkaistuja standardeja. Päätös tämänkaltaisen materiaalin käyttämiseen työn lähtökohtina perustuu viranomaistoiminnan luonteeseen ja lakien tuomiin velvoitteisiin. Edellä mainitut lähdemateriaalit eivät tutkimuksen kannalta tuo tutkimusaiheeseen uutta teoriapohjaa, mutta työn konstruktiivisen luonteen vuoksi tämä ei ole merkityksellistä.

4.1 Tutkimusaiheeseen liittyvä keskeinen lainsäädäntö

Tutkimuksen kannalta oleellinen lainsäädäntö koskee viranomaisen toiminnan julkisuutta, tietoturvallisuutta ja tietojärjestelmien tietoturvallisuuden arviointia. Kappaleeseen on poimittu työn kannalta merkittävimpiä pykäliä ja momentteja, jotka antavat perusteita työlle.

4.1.1 Laki viranomaisten toiminnan julkisuudesta

Lain yhtenä tarkoituksena on ”toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa”. (21.5.1999/621, 3§)

Hyvää tiedonhallintatapaa käsittelevässä 18§:ssä on säädetty, että

> ”viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä”.

18§:n 3 momentin mukaan viranomaisen tulee

> ”selvittää tietojärjestelmien käyttöönottoa sekä hallinnollisia ja lainsäädännöllisiä uudistuksia valmisteltaessa suunniteltujen toimenpiteiden vaikutus asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun samoin kuin ryhtyä tarpeellisiin

toimenpiteisiin tietoon liittyvien oikeuksien ja tiedon laadun turvaamiseksi sekä asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan järjestämiseksi" (21.5.1999/621, 18§)

4.1.2 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Viranomaisten turvallisuusluokitellun tietoaineiston käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista on säädetty Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (jäljempänä tietoturva-asetus). (1.7.2010/681. 1 §)

Tietoturva-asetuksen 4§:ssä on säädetty tietoturvallisuuden suunnittelun perusteet ja sen mukaan "tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset." (1.7.2010/681, 4§)

Asetuksen 5§:n mukaan "Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että: 1) viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan". (1.7.2010/681, 5§)

4.1.3 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

Laissa on säädetty, että

> "Viestintäviraston tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi:
>
> 1) arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta;
>
> 3) tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta." (1406/2011, 4§)

Tietoturvallisuuden arviointiperusteina voidaan käyttää:

> ”1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
>
> 2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
>
> 3) Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;
>
> 4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;
>
> 5) vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.” (1406/2011, 7§)

Vaikka lainsäädännössä ei varsinaisesti velvoiteta tietojärjestelmille viranomaishyväksyntää, edellytetään että tietojärjestelmien hallinta ja tietoturvallisuuden suunnittelu on hyvän tiedonhallintatavan mukaista.

4.2 Ohjeet, säännöstöt ja kriteeristöt

Valtioneuvoston periaatepäätöksessä valtionhallinnon tietoturvallisuuden kehittämisestä ohjataan tietoturvallisuuden kehittämistä valtionhallinnossa osana hallinnon toimintaa, johtamista ja riskienhallintaa. (VAHTI 7/2009, 7)

Valtiovarainministeriön asettama VAHTI johtoryhmän tavoitteena on kehittää valtionhallinnon tietoturvallisuutta. VAHTI kehittää ja ylläpitää julkisen hallinnon tietoturvallisuuden normeja, ohjeita ja suosituksia.

Puolustusministeriön 2011 julkaiseman kansallisen turvallisuusauditointikriteeristön (KATAKRI) päätavoitteena on ollut viranomaistoimintojen yhtenäistäminen turvallisuustason todentavien tarkastusten tekemisessä. KATAKRI:ssa on huomioitu sen rinnakkaisuus muiden olemassa olevien turvallisuuteen liittyvien dokumenttien kuten VAHTI-ohjeet ja Euroopan Unionin turvallisuussäännöstö. (Puolustusministeriö, 2011, 3)

Euroopan Unionin turvallisuussäännöstöä (2013/488/EU) tulee noudattaa kun käsitellään EU:n turvaluokiteltua tietoa. Säännöstössä on määritelty tietojen suojaamista koskevat periaatteet ja vähimmäisvaatimukset. Turvallisuusriskien hallintaan liittyvän 5 artiklan mukaan ”on pyrittävä määrittelemään tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle”. (2013/488/EU, 2)

Edellä kuvatut dokumentit liittyvät olennaisesti tietoturvallisuuden arviointiin ja laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista mahdollistaa niiden käyttämisen arviointiperusteina. (1406/2011, 7 §)

Kaikissa työn taustamateriaaleiksi valituissa ohjeistuksissa on tunnistettu riskienhallinnan osuus oleelliseksi osaksi tietoturvallisuuden hallinnan kokonaisuutta. Turvallisuustoimenpiteet tulee ohjeiden mukaan suhteuttaa ja määritellä toimintojen edellyttämällä tavalla.

4.3 Standardit, menetelmäoppaat ja muu kirjallisuus

Työn lähdemateriaalina on käytetty useita kansainvälisen standardoimisjärjestön (International Organization of Standardization, ISO) määrittelemiä standardeja. Standardien lisäksi työn teoreettisia lähtökohtia varten on käytetty useita riskienhallintaan, tietoturvallisuuteen ja arvioitiin liittyviä teoksia.

4.3.1 ISO/IEC standardit

Tutkimusaiheeseen liittyvistä standardeista lähdemateriaaliksi on valittu tietoturvallisuuden hallintajärjestelmiä käsittelevä ISO 27000 –sarja sekä riskienhallintaa käsittelevä ISO 31000 –sarja.

ISO koostuu kansallisista standardoimisjärjestöistä jotka osallistuvat kansainvälisten standardien laadintaan. ISO:n julkaisemat standardit ovat laajalti hyväksyttyjä, sillä julkaiseminen edellyttää vähintään 75 %:n kannatuksen organisaation jäsenmäärästä. ISO standardit ovat ohjeita.

ISO standardien valinta työn lähdemateriaaliksi on perusteltua niiden laajan hyväksynnän johdosta. Standardeissa määriteltyjen menetelmien ja prosessien käyttäminen on linjassa myös tietoturvallisuuden arviointiin liittyvän lain (1406/2011) 7§:n 4 ja 5 momentin kanssa.

4.3.2 Riskienhallintaan liittyvä kirjallisuus ja menetelmäoppaat

Tietoturvallisuuteen ja riskienhallintaan liittyvää kirjallisuutta on käytetty työssä konstruktion luomisen ja ideoinnin taustalla. Käytetyissä teoksissa ei varsinaisesti ole standardeihin verrattuna työn teoreettiselta kannalta merkittävää lisäystä, vaan niissä on käsitelty samoja malleja ja teemoja hieman eri näkökulmista.

Menetelmäoppaita on käytetty tietoperustan, teoreettisen viitekehyksen ja metodologian määrittelemisessä.

4.4 Lähdekritiikki

Menetelmiin liittyvän kirjallisuuden osalta työssä on tukeuduttu vain muutamiin lähteisiin. Konstruktiiviseen tutkimukseen liittyvä taustamateriaali pohjautuu pääosin Kari Lukan (2001) menetelmäartikkeliin, johon on koostettu tiivistelmä tutkimusotteeseen liittyvästä aikaisemmasta tutkimuksesta ja julkaisuista. Lähdeluettelossa mainitut konstruktiiviseen tutkimukseen liittyvät artikkelit on kirjoitettu liiketaloustieteen näkökulmasta. Artikkeleissa ei käsitellä konstruktiivista tutkimusta teoreettisesta näkökulmasta, eikä artikkeleita ole tästä johtuen voitu työn kannalta oleellisesti hyödyntää. Konstruktiivista tutkimusta on käsitelty kehittämistyön menetelmäoppaissa tapaustutkimuksen ja toimintatutkimuksen yhteydessä, mutta ei laajasti omana tutkimusmenetelmänään.

Arviointitietoon liittyvä osuus työstä perustuu Petri Virtasen 2007 kirjoittamaan teokseen. Yhteen lähdeteokseen perustuvaa tietoa tulee arvioida kriittisesti. Virtanen viittaa teoksessaan suoraan lukuisiin alan tutkimuksiin ja aiheen kirjallisuuteen. Viittausten, teoksen lähdeluettelon ja muutamien lähteiden tarkistamisen perusteella voidaan teosta pitää luotettavana lähdeaineistona.

5 Teoreettinen viitekehys

Työn tutkimusmenetelmäksi on valittu konstruktiivinen tutkimusote. Työ on konstruktiivinen, normatiivinen tutkimus joka sisältää kvalitatiivisia ja kvantitatiivisia elementtejä. Ohjaava, eli normatiivinen tutkimus pyrkii parantamaan valitun kohteen tilaa.

Konstruktiivinen tutkimusote soveltuu työn tarkoitusperiin paremmin kuin tapaustutkimusta ja toimintatutkimus. Tapaustutkimus ja toimintatutkimus soveltuisivat yksittäisen organisaation riskienhallintamenetelmien tutkimiseen ja kehittämiseen, mutta työn tarkoitus on luoda yleisempi malli jolloin konstruktiivinen tutkimusote on perusteltua.

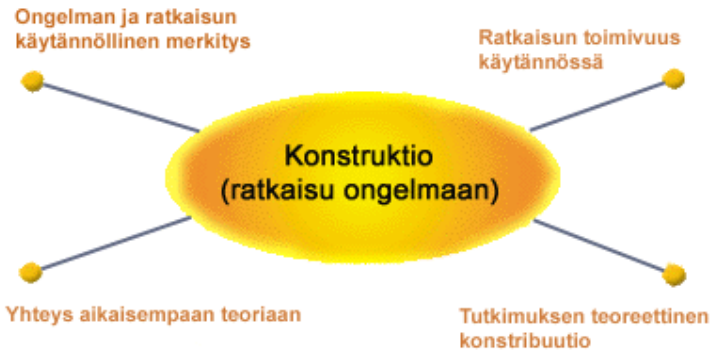
5.1 Konstruktiivinen tutkimus

Konstruktiivinen tutkimusote on eräs tapaustutkimuksen muoto, joka on kehitetty ensisijaisesti liiketaloustieteen tarpeisiin. Tutkimustapa on saanut huomiota tekniikan alan tutkimuksessa ja sitä on sovellettu myös tietojärjestelmätieteiden alalla. Metodologian avulla pyritään ratkaisemaan reaalimaailman ongelmia. Tärkein metodologiaan liittyvä abstrakti käsite on konstruktio, jolla tarkoitetaan keksittyä tai kehitettyä mallia, diagrammia, tuotetta tai muuta vastaavaa. Matemaattiset algoritmit ja ohjelmointikielet ovat esimerkkeinä teoreettisten konstruktioiden kehittämisestä. (Lukka, 2001)

Konstruktiivinen tutkimusote edellyttää, että tutkimus

- keskittyy tosielämän ongelmaan, joka nähdään tarpeelliseksi ratkaista,
- tuottaa uuden konstruktion, jonka avulla pyritään ratkaisemaan alkuperäinen ongelma,
- sisältää konstruktion testaamisen tai toteuttamisen, jolla testataan konstruktion soveltumista käytäntöön,
- on kytketty olemassa olevaan teoreettiseen viitekehykseen ja tietämykseen, ja
- kiinnittää huomiota empiiristen havaintojen ja löydösten reflektoimiseen takaisin teoriaan

(Lukka, 2001)



Kuvio 1: Konstruktiivinen tutkimusote (Lukka, 2001)

Kari Lukan mukaan ”konstruktiivisen tutkimusotteen ideaalinen tulos on, että tosielämän ongelma ratkaistaan implementoidulla uudella konstruktiolla”. (Lukka, 2001)

Ojasalo, Moilanen ja Ritalahti (2009) toteavat, että konstruktiivisen tutkimuksen avulla pyritään ratkaisemaan käytännön ongelma luomalla uusi rakenne. Tutkimuksen pyrkimyksenä on löytää uudenlainen teoreettisesti perusteltu ratkaisu ongelmaan. Näin ollen on oleellista luoda yhteys ongelman, sen ratkaisun ja teoreettisen tiedon välille. Kirjoittajat määrittelevät konstruktiivisen tutkimuksen olevan suunniteltua mallintamista sekä mallien toteutusta ja testaamista. (Ojasalo ym. 2009, 65)

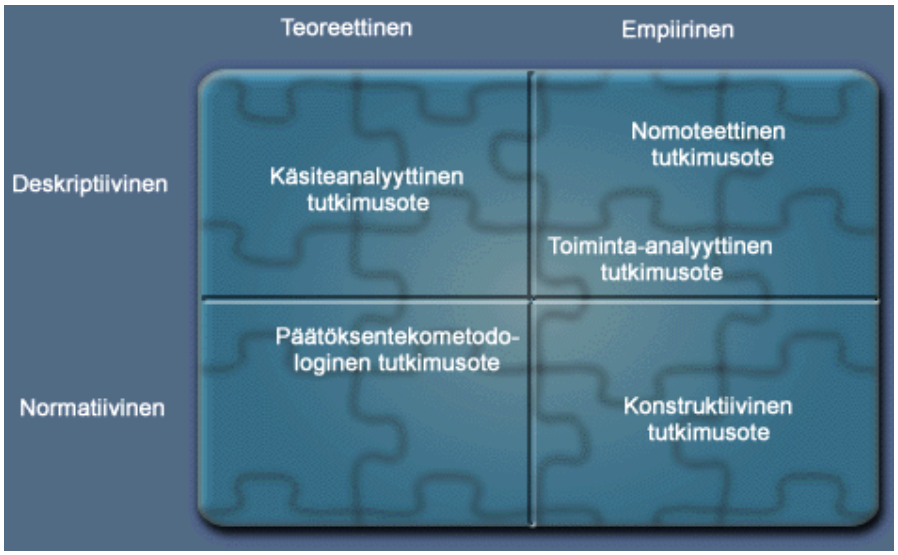
Lukan mukaan hyvä konstruktiivisen tutkimuksen aihe on sellainen, johon voidaan yhdistää käytännön merkitys ja samalla aihetta ei ole juurikaan analysoitu aikaisemmassa kirjallisuudessa. (Lukka, 2001)

5.2 Konstruktiivisen tutkimuksen metodologia

Tutkimuksen aikana kehitetyn konstruktion toimivuutta tulee testata ja arvioida käytännössä. Tutkimusmenetelmä tukeutuu pragmatistiseen totuuskäsitykseen, jonka argumenttina on ”se mikä toimii, on totta”. Konstruktiivisen tutkimusotteen ero tyypilliseen analyyttiseen mallinnukseen on konstruktion empiirinen testaaminen. Mikäli tutkimuksessa edetään testausvaiheeseen, voidaan kyseisen tutkimusprosessin olettaa kokonaisuudessaan onnistuneen teoreettisesta näkökulmasta katsottuna. (Lukka, 2001)

Konstruktiivisen tutkimusotteen metodologiaa voidaan rinnastaa nomoteettiseen ja päätöksentekometodologiseen tutkimusotteeseen. Nomoteettinen tutkimusote perustuu kausaaliseen selitysmalliin ja sen avulla pyritään löytämään säännönmukaisuuksia. Päätöksentekometodologisessa tutkimusotteessa keskitytään analyyttiseen mallintamiseen ja se perustuu oletta-

muksiin kuten nomoteettinenkin tutkimusote. Päätöksentekometodologiseen tutkimusotteeseen kuuluu myös normatiivisuus, eli sillä pyritään ohjaamaan toimintaa. Edellä kuvattuihin tutkimusotteisiin nähden konstruktiivinen tutkimusote lisää metodologiseen lähestymistapaan normatiivisia ja empiirisiä elementtejä. (Lukka, 2001)



Kuvio 2: Konstruktiivinen tutkimusote metodologiana (Lukka, 2001)

6 Tutkimusaiheeseen liittyvät prosessit

Työkalun käyttäminen edellyttää riskienhallintaan ja arviointiin liittyvien prosessien ymmärtämistä, jotta sen käyttö johtaa työn kontekstina olevaan haluttuun lopputulokseen. Riskienhallinta on lähtökohtaisesti eräänlainen arviointiprosessi, jolloin lopputuloksen kannalta on oleellista ymmärtää arviointiin liittyvää metodologiaa.

Tietojärjestelmien tietoturvallisuuden takaaminen teknisin keinoin on rajallista ja tietoturvallisuuden hallintaa tulee tukea johtamisen ja prosessien avulla. (ISO/IEC 17799:2005, viii)

Yleisten käytäntöjen noudattaminen, vaatimusten- tai sääntöjenmukaisuus ja tarkistuslistojen käyttäminen eivät itsessään takaa turvallisuutta. Riskienhallintaan perustuva malli tietoturvallisuuden toteuttamisessa voi tarjota dynaamisempia ja joustavampia toimintatapoja.

Riskienhallinnan tarkoitus on tehostaa toimintoja ja samalla minimoida odottamattomia tapahtumia kohdeympäristössä. Täydellinen riskien poistaminen saattaa olla käytännön tasolla erittäin kallista ja jopa mahdotonta, jolloin toimintatapojen tulee pyrkiä määrittelemään, kontrolloimaan ja ennakoimaan riskitekijöitä.

Tietoturvallisuuden kuvataan yleisesti koostuvan luottamuksellisuudesta, eheydestä ja saatavuudesta. Vastuullisuuden lisääminen osaksi tietoturvaan liittyvää hallintamallia ja riskienarviointia tuo uuden ulottuvuuden kokonaisuuteen. Vastuullisuudella tarkoitetaan tässä yhteydessä tarvetta jäljittää tapahtumien kulkua (Wheeler, 2011, 30 – 31). Lähestymistapaa on alettu soveltamaan esimerkiksi NIST:n riskienhallintamallissa (NIST, 2010).

Tässä luvussa kuvataan yleisesti riskienhallintaa, siihen liittyviä osatekijöitä ja prosessia sekä arviointia ja arviointitiedon tuottamiseen liittyvää teoriaa. Luvun lopussa käsitellään konstruktion lähtökohtana käytettävää Hazard and Operability Study (HAZOP) -mallia.

6.1 Riskienhallinta

Kaikkiin organisaatioihin ja niiden toimintoihin kohdistuu sisäisiä ja ulkoisia epävarmuustekijöitä, joiden vaikutuksia kuvataan riskeinä. Riskejä voidaan hallita riskejä tunnistamalla ja analysoimalla sekä näiden pohjalta tehtävän riskiarvion ja riskien käsittelyyn tähtäävien toimenpiteiden määrittelyn pohjalta. (ISO 31000 2009, v)

Riskienhallinta on tärkeä osa organisaation tietoturvallisuutta ja riskienhallinnan merkitys on tunnistettu kaikissa työn lähdemateriaaleissa. Tietoturva-asetus edellyttää, että toimintaan liittyvät tietoturvariskit kartoitetaan. (1.7.2010/681, 5§) VAHTI:n teknisen ICT-ympäristön

tietoturvataso-ohjeessa (VAHTI 3/2012) viitataan tietoturva-asetukseen ja riskienhallinta on otettu ohjeessa huomioon lain edellyttämällä tavalla. Riskienhallinnan prosessia kuvataan työssä ISO standardeissa esitettyihin malleihin tukeutuen.

Ollakseen tehokasta, riskienhallintaa tulee toteuttaa kokonaisvaltaisesti kaikilla organisaation tasoilla. ISO 31000 –standardin periaatteiden mukaan riskienhallinnan tulee:

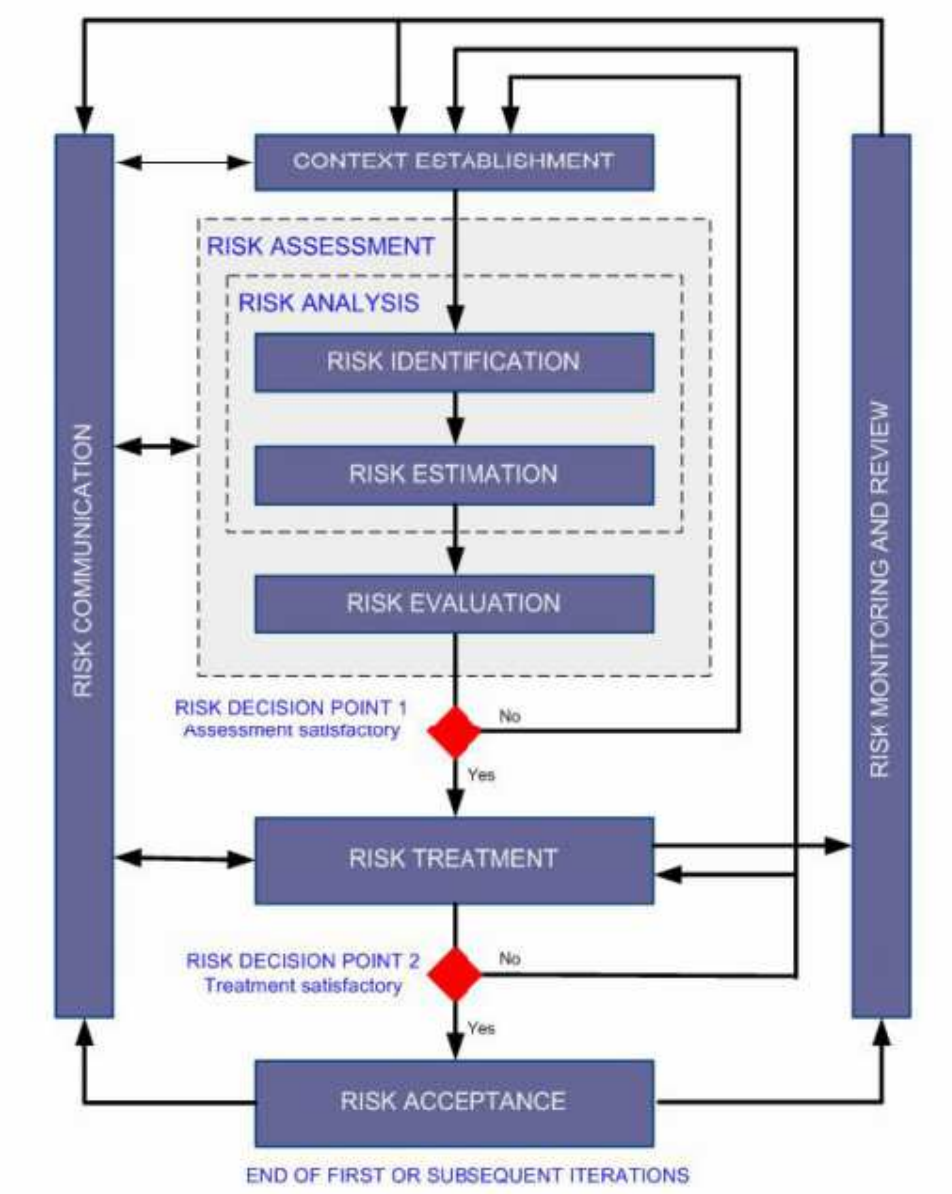
- tuottaa lisäarvoa organisaatiolle
- olla olennainen osa kaikkia toimintoja
- olla osa päätöksentekoa
- ottaa huomioon epävarmuustekijät
- olla systemaattista, jäsenneltyä ja oikea-aikaista
- perustua parhaaseen mahdolliseen taustatietoon
- olla organisaation tarpeisiin kohdennettua
- ottaa inhimilliset ja kulttuurilliset tekijät huomioon
- olla läpinäkyvää
- olla dynaaminen, iteroitava prosessi
- parantaa ja kehittää organisaation toimintaa
  (ISO 31000, 2009, 7 – 8)

Työssä tuotettavan työkalun eräänä tarkoituksena on mahdollistaa organisaatioissa tehdyn riskienhallinnallisten menettelyjen arviointia, kun toimintaympäristön tietoturvallisuuden vaatimustenmukaisuutta tarkastetaan tai arvioidaan. Työkalun tavoitteena on mahdollistaa systemaattisen, kattavan, jäsennellyn ja läpinäkyvän menetelmän käyttäminen osana arviointiprosessia sekä tuottaa lisäarvoa ja arviointitietoa arvioinnin kohteesta. Edellä mainittujen tekijöiden täyttyessä työkalun voidaan katsoa soveltuvan työn kontekstin mukaiseen käyttöön.

6.1.1 Hallintamalli

Hallintamallissa määritellään lähtökohdat riskienhallinnalle sekä kuvataan mitä, miksi ja ketä varten riskienhallintaa tehdään ja mikä riskienhallintaprosessin konteksti on toimintaan nähden. Hallintamalli ei ole yksityiskohtainen kuvaus varsinaisesta prosessista ja menettelytavoista, vaan yleinen pohja riskienhallinnan toteuttamiselle organisaatiossa.

Riskienhallinnan prosessien ja hallintamallien kehittämisessä tulee kartoittaa toimintaympäristön erityispiirteet, erilaiset vaikutteet ja toiminnan suhteet sidosryhmien kanssa. Lisäksi tulee ottaa huomioon organisaation sisäiset vaikuttimet kuten rakenne, roolit, tavoitteet ja toimintatavat. Edellä mainittujen tekijöiden tunnistaminen on edellytys sille, että organisaatio osaa suhteuttaa riskienhallintamallinsa toimintaansa oikein. (ISO 31000 2009, 10)



Kuvio 3: Riskienhallintaprosessi (ISO/IEC 27005 2008, 5)

Erilaisiin uhkamalleihin, analyyseihin ja tilannekuvaan perustuva riskien kartoittaminen ja hallinta tulee tehdä organisaatiokohtaisesti ja sitä tulee kehittää kunkin organisaation tarpeisiin mukautuvasti. (ISO 31000 2009, 10 - 11)

Työn lopputuloksena syntyvän työkalun tarkoituksenmukainen käyttäminen edellyttää, että arviointi toteutetaan yllä kuvatun riskienhallintamallin mukaisesti. Riskienhallinnan kontekstisidonnaisuus on merkittävässä osassa riskienarviointia tehtäessä. Työkalun avulla tuotettujen tulosten ja tiedon oikeellisuus liittyvät vahvasti oikean kontekstin määrittelyyn. Järjestelmällisen mallin avulla saavutetaan kokonaisvaltainen arvio, joka on yksi työn tavoitteista.

6.1.2 Riskien tunnistaminen ja analysointi

Tietoturvallisuuden hallintajärjestelmästandardien sarja (ISO 27000) määrittelee tietoturvariskin olevan mahdollisuus siihen, että uhka hyödyntää turvattavan kohteen tai turvamekanismin heikkoutta ja siten aiheuttaa organisaatiolle haittaa. (SFS-ISO/IEC 27000, 14 - 18)

Tietojärjestelmien riskien arvioinnilla pyritään yleisesti määrittämään suojattava kohde, tunnistamaan siihen liittyvät olemassa olevat ja mahdolliset uhkat ja haavoittuvuudet, tunnistamaan olemassa olevat havaittuja riskejä pienentävät kontrollit, määrittää potentiaaliset seuraukset sekä priorisoimaan riskien tärkeysjärjestys. (ISO/IEC 27005 2008, 10 - 13) Tietojärjestelmien tietoturvallisuuden arviointi tai vaatimustenmukaisuuden tarkastaminen keskittyvät riskejä pienentävien kontrollien arviointiin. Vaatimukset ja kriteeristöt ovat melko yksiselitteisiä, eikä niissä oteta kantaa riskienhallinnan merkitykseen vaatimuksen täyttämisessä. Työn avulla pyritään helpottamaan riskienhallinnan vaikutusten analysointia osana tarkastus- tai arviointiprosessia.

Riskien tunnistamisen tulee olla riskienhallinnan kohdeorganisaation tavoitteisiin ja toimintaan perustuva. Riskien aiheuttajat ja seuraukset, todennäköisyydet, omistajat ja sietokyky pitää arvioida toimintaympäristöstä riippuen. (ISO 31000 2009, 17)

Tämän työn kannalta edellä mainitut kontrollien vaikutukset, seuraukset ja priorisointi tullaan huomioimaan työkalun riskien tunnistamiseen liittyvässä osassa. Tunnistamisvaiheessa seurauksien ja todennäköisyyksien arvioinnin avulla kartoitetaan riskien suhdetta toisiinsa ja niiden mahdollisia yhteisvaikutuksia.

Uhka-analyysissä tulee arvioida tiedon käsittelyä siirron, prosessoinnin ja tallennuksen aikana. Kaikissa vaiheissa tietoon kohdistuu uhkia kuten oikeudeton käsittely, korruptoituminen, tiedon tavoittamattomuus tai kyvyttömyys todistaa hyökkäyksen lähdettä. Kaikki luetellut uhkat voidaan kategorisoida johonkin tietoturvallisuuden osa-alueeseen. (Wheeler, 2011, 31 – 40) Kategorisointi huomioidaan työssä siten, että työkalu mahdollistaa vain tiettyyn tietoturvallisuuden osa-alueeseen liittyvien riskien arvioinnin.

6.1.3 Riskienarviointi

Riskienarvioinnin tarkoituksena on tunnistaa, priorisoida ja ennakoida riskien vaikuttavuutta organisaation toimintaan liittyen sekä auttaa analyysin avulla tunnistettuihin riskeihin liittyvässä päätöksenteossa. Jatkotoimenpiteet ja riskien hoitamisen priorisointi sekä riskien sietokyky tulee arvioida. Päätöksenteossa tulee huolehtia lakisääteisten velvoitteiden ja muiden vaatimusten täyttyminen riskien osalta. (ISO 31000 2009, 18)

Riskienarviointi tukee organisaation toimintaa monella eri tasolla ja sen avulla pyritään mm. kehittämään tietoturva-arkkitehtuuria, määrittelemään vaadittavia turvallisuuskontrolleja, muokkaamaan prosesseja sekä toteuttamaan ja ylläpitämään turvallisuusjärjestelyjä.

Arvioinnilla pyritään määrittelemään taso, kuinka tietoturvakontrollien oikeellinen toteutus ja toiminta sekä niiden tuottamat tulokset ovat suhteessa tavoiteltuun tietoturvatasoon tai vaatimuskriteereihin. Tunnistettujen riskien mahdolliset kumulatiiviset vaikutukset tulee huomioida, arvioida ja käsitellä toimintaympäristö, tarpeet ja mahdolliset sidosryhmät huomioon ottaen. (ISO/IEC 27005 2008, 17)

Työ keskittyy juuri riskien arviointiin ja tästä syystä toteutettavaa työkalua luotaessa ja käytettäessä tulee ottaa kappaleessa määritellyt periaatteet erityisesti huomioon. Monitahoinen ja analyyttinen riskienarviointi ja tätä kautta saatava kattavampi ymmärrys olemassa olevista riskeistä sekä niiden syistä ja seurauksista edesauttaa turvallisuusjärjestelyjen toteuttamista ja suunnittelua. Tarkemman vaatimuksiin ja poikkeamiin pohjautuvan riskianalyysin avulla tietoturvakontrollien toteutuksesta saatetaan havaita puutteita, jotka eivät näkyisi yleisemmällä tasolla tehdyn riskianalyysin tuloksissa.

6.1.4 Riskien käsittely

Riskien käsittelyn aikana riskit tunnistetaan, arvioidaan niiden mahdolliset vaikutukset ja päätetään toimenpiteistä.

ISO/IEC 27005 standardi määrittelee neljä eri vaihtoehtoa riskien käsittelyyn, jotka ovat

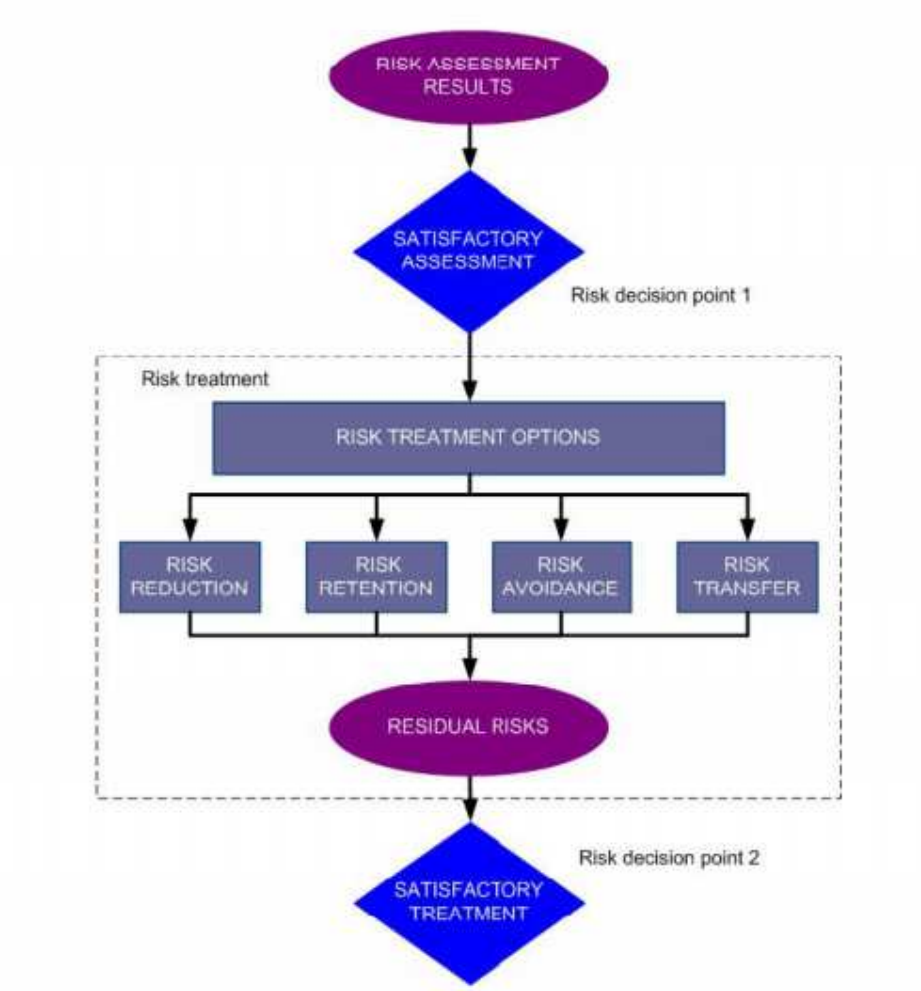
- **Riskien vähentäminen** pyrkii vähentämään riskin todennäköisyyttä tai vaikuttavuutta. Toimenpiteitä voivat olla esimerkiksi teknisten tietoturvakontrollien kompensoiminen fyysisen turvallisuuden kontrolleilla.

- **Riskien säilyttäminen** perustuu organisaation riskinsietokykyyn. Päätöksessä riskin hyväksymisestä tulee huomioida toiminnan luonne, sille asetetut toiminnalliset vaatimukset ja riskin vaikutukset.

- **Riskien välttäminen** soveltuu tilanteisiin, joissa riskinsietokyky ylittyy. Organisaatio voi pyrkiä välttämään riskin esimerkiksi vaihtamalla käytössä olevaa tekniikkaa. Tällä pyritään poistamaan riskin aiheuttama tekijä toimintaympäristöstä.

- **Riskien siirtämisellä ja jakamisella** pyritään vastuun jakamiseen muiden toimijoiden kanssa. Riskin siirtäminen ei vähennä riskin todennäköisyyttä tai vaikuttavuutta. Riskin siirtämistä voi olla esimerkiksi vartioinnin ostaminen ulkopuoliselta kumppanilta.

Riskien käsittelyyn valittavien menettelyjen tulisi perustua riskien arviointiin ja kustannustehokkuuteen. (ISO/IEC 27005 2008, 17 – 18)



Kuvio 4: Riskien käsittelyn vaiheet (ISO/IEC 27005 2008, 18)

Riskien käsittelemiseksi tehtävien toimenpiteiden määrittelyssä tulisi erityisesti huomioida, miten eri riskin vaikutuspiiriin kuuluvat tahot näkevät riskin ja kuinka kommunikointi riskin osalta tulee järjestää. (ISO/IEC 27005 2008, 19)

Työkalun avulla tuotetun analyysin lopputulosten perusteella pyritään antamaan perusteltu toimenpidesuositus riskien käsittelylle. Vaatimustenmukaisuuden arvioinnin tarkoituksena on havaita olemassa oleva poikkeama ja tuottaa arvioinnin kohteelle riittävästi tietoa siitä, mihin toimenpiteisiin sen tulee ryhtyä. Päätös tehtävistä toimenpiteistä jätetään arvioinnin kohteelle, joka voi hyödyntää arviointitietoa omassa päätöksenteossaan saavuttaakseen haluamansa asianmukaisen lopputuloksen.

6.2 Arviointi

Arviointia toimintona voidaan lähestyä järjestelmäteoreettiselta kannalta. Arviointitoimintaan liittyy olennaisesti näyttövaatimus ja todistusvoima (evidence-based evaluation). Tällä tarkoitetaan, että arviointi perustuu arvioinnin aikana kerättyyn aineistoon ja että johtopäätökset perustuvat tähän. Näyttövaatimuksilla ja todistusvoimaisella arvioinnilla pyritään poistamaan mielivaltaisuus arvioinnin johtopäätöksistä. Arviointitoimintaan liittyy olennaisesti myös tulosten hyödynnettävyys. (Virtanen, 2007, 14 – 16, 54) Näyttövaatimuksen ja todistusvoiman periaatteiden noudattaminen viranomaisen toiminnassa tulee huomioida, jotta toiminnan läpinäkyvyydestä voidaan varmistua. Työssä luotavan työkalun avulla pyritään vahvistamaan näitä periaatteita arviointitoiminnassa.

Arviointi tulee kohdistaa tarvelähtöisyyteen, tarkoituksenmukaisuuteen ja yhtenäisyyteen. Esimerkiksi organisaation arvioinnissa kartoitetaan ensin lähtökohdat, jonka jälkeen tutkitaan käytännön toimintaa tai toiminnan sisältöä lähtökohtiin perustuen. Arvioinnin viimeinen osio tutkii toiminnasta seuraavia vaikutuksia. (Virtanen, 2007, 18 – 19)

Arviointitoiminnan määrä on kasvanut huomattavasti vuosituhannen vaihteen jälkeen. Kasvun eräitä selittäviä tekijöitä ovat hallintojärjestelmiin vakiintunut arviointikulttuuri sekä muutokset hallinnon ohjausjärjestelmissä. Arviointitoiminnan kysyntä on kasvanut, kun normiohjauksesta on siirrytty tiedolla ohjaamiseen. Informaatio-ohjauksen tuloksena syntyneet käytännöt voidaan kokea sekavina ja merkitys kyseenalaistaa. (Virtanen, 2007, 28).

Arvioinnin lähestymismallit voivat olla joko preskriptiivisiä tai deskriptiivisiä. Preskriptiivisissä malleissa pyritään kuvaamaan hyvää arviointitoimintaa ja oikeaoppista toimintaa erilaisten ohjeiden, määritelmien ja viitekehysten avulla. Deskriptiiviset mallit ovat arvioinnin kulun yksinkertaistavia yleistyksiä. Teorialähtöisessä arvioinnissa arvioinnin kohde tulee purkaa

osiin. Tämäntyyppistä teorialähtöistä arviointimallia on pidetty hyvänä lähtökohtana kompleksisia, monitasoisia ja useista eri osista koostuvia kokonaisuuksia. (Virtanen, 2007, 35 – 36) Tämän työn näkökulmasta arviointitoiminta noudattaa lähinnä teorialähtöistä arviointimallia. Tietojärjestelmien tarkastuksissa arviointia suoritetaan sekä teknisen, hallinnollisen että fyysisen turvallisuuden kannalta, jonka vuoksi osakokonaisuuksia saattaa olla paljon ja niiden vaikutukset toisiinsa tulee huomioida monella eri tasolla.

Arviointityön tavoitteena on tuotettavan tiedon tarkoituksenmukainen hyödyntäminen. Arvioinnin johtopäätökset tulee tästä syystä aina suhteuttaa kohteen kontekstiin. Arvioinnissa tulee pohtia arvioinnin kohteen kontekstin, toiminnan ja tulosten suhdetta toisiinsa. (Virtanen, 2007, 76) Myös itse arviointimalli tulee suhteuttaa kohteeseen. Kontingentin tulkintatavan mukaan arvioitavaan kohteeseen tulee hahmottaa ja kehittää tilanteeseen sopiva joustava malli, joka on arvioinnin kohdetta tarkastellessa tarkoituksenmukaisin. (Virtanen, 2007, 104) Tehtäessä arviointia annettuja vaatimuksia tai kriteeristöä vasten, on vaatimusten valinta ja tulkinta tehtävä arvioinnin kohteeseen soveltuvin osin. Työn kannalta on oleellista, että kontingenttia tulkintatapaa noudatetaan työkalua käytettäessä jotta sen avulla saatavat tulokset ovat hyödynnettävissä.

Arvioinneista saatavaa tietoa ei voi sellaisenaan yleistää tai siirtää muihin arviointitilanteisiin. Arviointien pohjalta saadun tiedon hyödyntäminen muissa samantyyppisissä konteksteissa (ekstrapolointi) edellyttää tarkkaa aineistojen ja kontekstin tulkintaa. (Virtanen, 2007, 155)

6.3 Hazard and operability study (HAZOP)

Hazard and operability study –menetelmää (HAZOP) voisi vapaasti käännettyä kutsua toiminnallisuuteen kohdistuvien uhkien riskienarviointimenetelmäksi. Menetelmä on arvioinnin kohteelle tehtävä rakenteinen ja systemaattinen analyysi. HAZOP on kvalitatiivinen menetelmä, joka perustuu avainsanojen käyttämiseen. Avainsanojen avulla pyritään löytämään arvioitavan kohteen suunnitellun toiminnallisuuden vaarantavia tekijöitä. (ISO 31010, 32) Valinta menetelmän käyttämiseksi työn eräänä pohjana perustuu sen rakenteisuuden ja systemaattisuuden tuomiin etuihin työn kontekstin mukaista arviointitoimintaa tehtäessä, vaikka menetelmä ei sellaisenaan sovellu pohjaksi työssä luotavalle konstruktiolle.

Menetelmä on alun perin kehitetty analysoimaan kemiallisia prosessiteollisuuden järjestelmiä, mutta sen käyttö on laajentunut mm. prosessien ja ohjelmistojen arviointiin. Menetelmää käytetään yleisesti myös ohjelmistosuunnittelun katselmoinneissa. (ISO 31010, 32)

Menetelmässä arvioinnin kohteena oleva prosessi tai järjestelmä jaetaan osatekijöihin. Osatekijöitä kutakin arvioidaan erikseen ja arvion avulla pyritään löytämään poikkeamia halutusta

toiminnallisuudesta, mahdollisia syitä ja todennäköisiä seurauksia. Menetelmässä muutetaan osatekijöiden toiminnallisia parametrejä avainsanojen avulla ja arvioidaan mitä vaikutuksia muutoksilla on alkuperäiseen haluttuun toiminnallisuuteen. Alla olevassa taulukossa on kuvattu esimerkkejä avainsanoista, joiden avulla toiminnallisuuden muutoksia voidaan tarkastella. Arviointia varten kootaan ryhmä henkilöitä, jotka suorittavat arvioinnin. Arviointiryhmään ei tulisi kuulua henkilöitä, jotka ovat osallisena arvioinnin kohteen suunnittelussa. (ISO 31010, 33)

Guide word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN	Complete substitution

Taulukko 1: Esimerkkejä avainsanoista (BS IEC 61882, 2001, 10)

HAZOP:n avulla pyritään löytämään järjestelmäkohtaisia kontrolleja ja niiden vaikutuksia kyseessä olevaan tarkastuksen kohteeseen. Mallin vahvuuksiin kuuluu soveltuvuus monenlaisiin käyttöympäristöihin sekä systemaattisuus ja laajuus. Toisaalta systemaattinen analyysi vaatii erittäin tarkan kuvauksen ja ymmärryksen arvioinnin kohteena olevasta järjestelmästä ja prosessi saattaa olla aikaa vievää. (ISO 31010, 2009, 34) Lisäksi monet järjestelmien osat usein vaikuttavat toisiinsa, jolloin yksittäisen havaitun poikkeaman korjaaminen ei välttämättä auta todellisen ongelman löytämisessä. (BSC IEC 61882, 2001, 14)

STUDY TITLE: AUTOMATIC TRAIN PROTECTION SYSTEM								**SHEET:** 1 of 2		
REFERENCE DRAWING No.: ATP BLOCK DIAGRAM				**REVISION No.:** 1				**DATE:**		
TEAM COMPOSITION: DJ, JB, BA								**MEETING DATE:**		
PART CONSIDERED:				INPUT FROM TRACKSIDE EQUIPMENT						
DESIGN INTENT:				TO PROVIDE SIGNAL TO PES VIA ANTENNAE GIVING INFORMATION ON SAFE SPEEDS AND STOPPING POINTS						
No.	**Element**	**Characteristic**	**Guide word**	**Deviation**	**Possible causes**	**Consequences**	**Safeguards**	**Comments**	**Actions required**	**Action allocated to**
1	Input signal	Amplitude	NO	No signal detected	Transmitter failure	Considered in separate study of trackside equipment			Review output from trackside equipment study	DJ
2	Input signal	Amplitude	MORE	Greater than design amplitude	Transmitter mounted too close to rail	May damage equipment	Checks to be carried out during installation		Add check to installation procedure	DJ
3	Input signal	Amplitude	LESS	Smaller than design amplitude	Transmitter mounted too far from rail	Signal may be missed	As above		Add check to installation procedure	DJ
4	Input signal	Frequency	OTHER THAN	Different frequency detected	Pick up of a signal from adjacent track	Incorrect value passed to processor	Currently none		Check if action is needed to protect against this	DJ
5	Antennae	Position	OTHER THAN	Antennae is in other than the correct location	Failure of mountings	Could hit track and be destroyed	Cable should provide secondary support		Ensure that cable will keep antennae clear of track	JB
6	Antennae	Voltage	MORE	Greater voltage than expected	Antennae short to live rail	Antennae and other equipment become electrically live			Check if there is any protection against this occurring	DJ

Taulukko 2: Esimerkki standardinmukaisesta HAZOP:ista (BSC IEC 61882, 2001, 39)

Tässä työssä arviointityökalun luomiseen käytetään sovellettua HAZOP-mallia. HAZOP:lla tarkoitetaan tässä työssä uhkien ja toiminnallisuuden vertailuun käytettävää riskienarviointimenetelmää.

HAZOP menetelmänä sopii tutkimuskohteeseen hyvin rajoitteistaan huolimatta. Työn kontekstissa tehtävät arvioinnit edellyttävät arvioinnin kohteen tarkkaa tuntemusta ja yksityiskohtaista systemaattista analysointia.

7 Konstruktio

Työkalun käytön lähtökohtana on, että tietojärjestelmätarkastuksessa arvioinnin kohteesta on havaittu poikkeama tai poikkeamia asetetuista tietoturvallisuusvaatimuksista. Arvioinnin kohteena oleva organisaatio on tehnyt poikkeamista riskianalyysin, jonka perusteella on tehty päätös jättää vaatimustenmukaiset kontrollit toteuttamatta. Riskinoton perusteena voi olla esimerkiksi tilanteet joissa tietojärjestelmän operatiivinen toiminnallinen käytettävyys on erittäin tärkeää. Tietojärjestelmässä tai sen osassa saattaa olla myös tietoteknisiä toiminnallisia rajoitteita, joiden vuoksi asetettua vaatimusta ei teknisesti voida täysin täyttää.

Arvioinnin lopputulosten hyödynnettävyyden ja työkalun tarkoituksenmukaisen käyttämisen kannalta on oleellista, että arviointiryhmän jäsenet tuntevat riskienhallintaan ja arviointiin liittyvät prosessit ja metodologian.

Työkalun käyttäminen voidaan jakaa kolmeen eri vaiheeseen. Ensimmäisessä vaiheessa arvioinnin kohteena olevaan riskiin liittyvät havaitut poikkeamat tunnistetaan ja listataan sekä pohditaan niistä aiheutuvia mahdollisia seurauksia tai vaikutusalueita. Toisessa vaiheessa arvioidaan poikkeamasta aiheutuvan riskin mahdollisen realisoitumisen vaikuttavuutta ja todennäköisyyttä. Kahden ensimmäisen vaiheen tulokset yhdistetään riskimatriisiin. Matriisin avulla lasketaan arvo poikkeamien kumulatiivisista vaikutuksista ja suhteutetaan arvoa annettuun suojaustasoon. Tuloksen perusteella tehdään päätelmiä toimenpidesuosituksista ja arvio siitä, ovatko arvioinnin lähtökohtina olleet riskit hyväksyttävissä suhteessa annettuihin vaatimuksiin. Suojaustasoilla tarkoitetaan tietoturva-asetuksen 9§:n mukaista asiakirjojen, tietoaineistojen tai tietojenkäsittely-ympäristöjen luokittelua.

Työkalussa yhdistetään kvalitatiivista ja kvantitatiivista riskienarviointia. Kvantitatiivisen arvioinnin vahvuuksia ovat mm. yleiskuvan luominen, vertailuarvojen tuottaminen ja muutosten mittaaminen. Kvalitatiivisen arvioinnin etuja ovat mm. kausaalisuhteiden, kontekstin ja kategorisoinnin luominen osana arviointiprosessia. (Evalsed, 2013, 74 – 76)

Työkalun käytännön toiminnallisuutta käydään konkreettisemmin läpi luvussa 7.5 ja työkalu kokonaisuudessaan on kuvattu liitteessä 1.

7.1 Poikkeamien tunnistaminen ja riskianalyysi

Poikkeamien tunnistamisessa käytetään avainsanoja, joiden avulla poikkeaman luonnetta voidaan tulkita tarkemmin. Avainsanojen käyttämisen pyrkimyksenä on luoda tietoa, jonka avulla voidaan tarkemmin arvioida mitkä tekijät ovat aiheuttaneet tunnistetun poikkeaman. Tekijöiden tunnistaminen on oleellista poikkeaman seurausten ja vaikutusten arvioinnin kannalta. Avainsanoja käyttäessä tulee huomioida, että ne eivät ole välttämättä tarkasti määriteltyjä tai sidottuja vaan niiden tarkoitus on olla apuna arvioitaessa poikkeamaa sen kontekstissa.

Esimerkeissä on käytetty HAZOP-mallin mukaisia avainsanoja ja vaatimuskriteeristönä KATAKRI:n versiota II.

Avainsanat:	Selite:
NO or NOT	Negation of intention (ei kontrollia)
MORE	Quantitative increase (enemmän kuin vaadittu)
LESS	Quantitative decrease (riittämätön kontrolli)
AS WELL AS	Quantitative increase (vaaditun lisäksi)
PART OF	Quantitative decrease (osittainen kontrolli)
REVERSE	Logical opposite of intention (päinvastainen toiminto)
OTHER THAN	Complete substitution (kompensointi)

ID	Vaatimus	Poikkeama	Uhka	Seuraus
1	I 501.0	Ei vahvaa käyttäjäntunnistusta (osittainen/PART OF)		
2	I 501.0	Ei henk.koht. tunnuksia (riittämätön/LESS)		
3	I 504.0	Puutteelliset lokimenettelyt (osittainen/PART OF)		
4				

Taulukko 3: Poikkeamien ja riskien tunnistaminen

Kun arviointia tehdään avainsanojen avulla, on syytä kiinnittää huomiota käytettävään terminologiaan. Riittämätön ei työkalun kontekstissa tarkoita välttämättä sitä että kontrollilla ei olisi merkitystä, vaan että kontrolli ei täytä kaikkia sille annettuja vaatimuksia. Yksinkertaistettuna esimerkkinä voidaan ottaa salasanan pituudelle asetettu vaatimus. Jos pituudelle on asetettu vaatimuksessa minimiarvo 16 ja toteutuksessa tämä arvo on 12, niin kontrolli on tällöin riittämätön. Kaikkia käytettäviä avainsanoja tulee käsitellä vastaavalla tavalla suhteutettuna arvioinnin kohteeseen.

Poikkeamien kirjaamisen tulee tapahtua siten, että kukin poikkeamasta johtuva tai aiheutuva riski määritellään erikseen riittävällä tarkkuudella. Tällöin esimerkiksi yhtä kriteeristön vaa-

timusta koskevaa poikkeamaa vasten voi olla lukuisia taulukkoon määriteltäviä ja arvioitavia riskejä.

7.2 Vaikuttavuuden ja todennäköisyyden arviointi

Työkalussa vaikuttavuudella ja todennäköisyydellä viitataan havaittuun poikkeamaan, poikkeamasta aiheutuvaan riskiin ja tämän tunnistetun riskin realisoitumisen todennäköisyyttä ja vaikutuksia. Vaikuttavuuden ja todennäköisyyden arviointia ei siis tule työkalun kontekstissa tehdä koko arvioitavan tietojärjestelmän, vaan yksittäisen riskin näkökulmasta.

Vaikuttavuutta ja todennäköisyyttä arvioidaan viisiportaisen asteikon mukaan, jossa vaihtoehdot ovat:

- Pieni (low)
- Melko pieni (low to medium)
- Kohtalainen (medium)
- Melko suuri (medium to high)
- Suuri (high)

Vaikuttavuuden ja todennäköisyyden arvioinnissa on hyvin oleellista arvioida kontekstia. Lisäksi ensimmäisessä vaiheessa tehty poikkeamien analysointi ja jaottelu tulee huomioida. Esimerkiksi avainsanojen avulla määritellyllä osittaisella tai riittämättömällä kontrollilla on alentava vaikutus riskin realisoitumisen todennäköisyyteen kuin jos kontrollia ei ole lainkaan. Vaikuttavuuden ja todennäköisyyden arvioinnissa tulee myös huomioida kompensoivat kontrollit ja eri kontrollien mahdolliset kumulatiiviset vaikutukset.

Työkaluun on määritelty myös tietoturvallisuuden kannalta keskeiset osa-alueet mikäli poikkeaman vaikutusaluetta halutaan käsitellä arviointia tehtäessä. Jaottelun käyttäminen soveltuu tilanteisiin, joissa kohteena olevaa järjestelmää arvioidaan esimerkiksi pelkän luottamuksellisuuden näkökulmasta. Tällöin eheyteen ja saatavuuteen liittyvien poikkeamien vaikutukset voidaan jättää huomioimatta, mikäli tällainen menettely sopii järjestelmän ja sen arvioinnin kontekstiin.

Kompensaatio	Luottamuksellisuus	Vaikutusalue: Eheys	Saatavuus	Vaikuttavuus	Todennäköisyys

Pieni
Melko pieni
Kohtalainen
Melko suuri
Suuri

Taulukko 4: Vaikuttavuus ja todennäköisyys

7.3 Riskimatriisi

Tunnistetut ja luokitellut poikkeamat lisätään riskimatriisiin määriteltyjen vaikuttavuuden ja todennäköisyyden perusteella. Matriisin soluihin lisätään numeerinen arvo, joka kuvastaa kuinka monta kyseisen vaikuttavuuden ja todennäköisyyden omaavaa poikkeamaa arvioinnissa on löydetty.

Todennäköisyys							
	1	Suuri					
	0,8	Melko suuri					
	0,6	Kohtalainen			1		
	0,4	Melko pieni					
	0,2	Pieni	3		1		
			Pieni	Melko pieni	Kohtalainen	Melko suuri	Suuri
			0,2	0,4	0,6	0,8	1
					Vaikuttavuus		

Taulukko 5: Riskimatriisi

Matriisin jokainen solu saa arvon perustuen todennäköisyyden ja vaikuttavuuden tuloon. Mikäli poikkeaman vaikuttavuuden ja todennäköisyyden on arvioitu olevan kohtalaisia, solu saa

yhteenlasketun arvon 0,36. Arvot on valittu siten, että niitä voi ohjeellisesti ajatella prosentuaalisina arvoina. Tämän karkean jaottelun mukaan 0 – 20% todennäköisyys on luokiteltu pieneksi jne. Tämänkaltainen jaottelu on kuitenkin hyvin karkea ja erittäin tulkinnanvarainen.

Taulukossa 5 on kuvattu tilannetta, jossa viisi poikkeamaa on analysoitu ja ne on viety matriisiin luokitustensa perusteella. Kolme poikkeamista on arvioitu vaikuttavuuksiltaan ja todennäköisyyksiltään pieniksi, yksi poikkeama vaikuttavuudeltaan ja todennäköisyydeltään kohtalaiseksi ja yksi poikkeama vaikuttavuudeltaan kohtalaiseksi, mutta todennäköisyydeltään pieneksi.

Poikkeamien sijoittuminen matriisiin antaa niille numeerisen arvon, joka on todennäköisyyden ja vaikuttavuuden tulo. Arvojen summa kuvastaa poikkeamien yhteisvaikutusten riskilukua. Saatua riskilukua verrataan raja-arvoon, joka kuvastaa analysoitujen poikkeamien yhteenlaskettua vaikutusta tai riskiluokitusta. Taulukkoon on määritelty toimenpidesuositus riskien vähentämiseksi ja poikkeamien korjaamiseksi sekä suuntaa antava vastaus sille, onko riskinotto hyväksyttävissä vaatimuksiin ja tavoiteltuun suojaustasoon nähden. Suositukset on jaoteltu tietoturva-asetuksen mukaisten suojaustasojen mukaan. Taulukon 5 esimerkin tulos saavuttaa raja-arvon 0,6 ja saa siten korkean riskiluokituksen.

Raja-arvo	Riskiluokitus	Toimenpidesuositus:	ST IV	ST III
> 0,8	Erittäin korkea	Vaatii välittömiä toimenpiteitä	Ei hyväksyttävissä	Ei hyväksyttävissä
0,6	Korkea	Huomattava tarve toimenpiteille	Hyväksyttävissä, tarve toimenpiteille	Ei hyväksyttävissä
0,4	Kohtalainen	Tarve toimenpiteille	Hyväksyttävissä	Hyväksyttävissä, tarve toimenpiteille
0,2	Matala	Ei välitöntä tarvetta toimenpiteille	Hyväksyttävissä	Hyväksyttävissä

Taulukko 6: Riskiluokitus

Esimerkissä toimenpidesuositus olisi siis ryhtyä toimenpiteisiin, joilla uhkan realisoitumisen todennäköisyyttä tai vaikuttavuutta voidaan pienentää. Korjaavien tai kompensoivien toimenpiteiden avulla riskinotto voisi olla hyväksyttävää suojaustason IV vaatimuksiin nähden.

7.4 Huomioita

Lopputuloksen analysoinnissa on kiinnitettävä erityistä huomiota arvioinnin kohteeseen ja kontekstiin. Työkalun tuloksia ei voi pitää varsinaisena mittarina, eikä niitä voi tulkita yksiselitteisesti. Työkalun ja siitä saatavien tulosten tarkoitus on auttaa ymmärtämään paremmin poikkeamien vaikutuksia kokonaisuutena ja arvioida, onko riskienhallinnan tuloksena syntynyt päätös riskinotosta perusteltua. Työkalun käyttö vaatii vahvaa ymmärrystä arvioitavasta kohteesta kokonaisuutena, arviointiin ja riskienhallintaan liittyvien prosessien ymmärtämistä sekä arvioinnin tarpeen, tarkoituksen ja kontekstin hahmottamista. Työkaluun määritetyt raja-arvot on alustavasti suunniteltu melko konservatiivisiksi. Syy tälle on se, ettei riskienhallintaa

ja sen avulla saatujen tulosten tulkittaisi oikeuttavan riskien hyväksymistä välttämättä sellaisenaan.

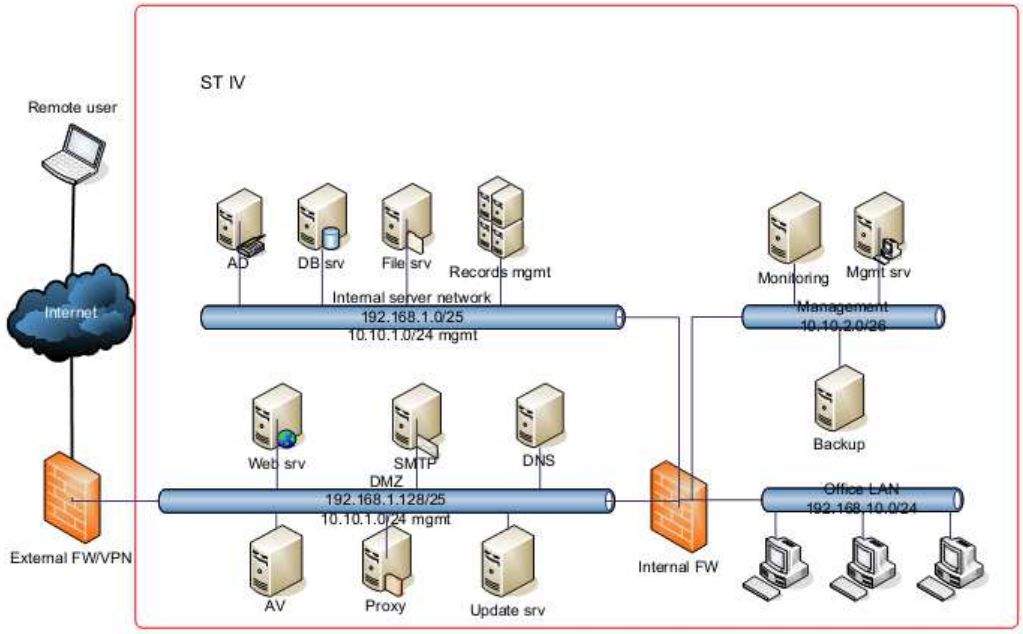
7.5 Esimerkki: Suojaustason IV järjestelmä

Työkalun käyttöä esittelevää esimerkkiä varten on kuvattu järjestelmäratkaisu jonka osaa arvioidaan työssä kuvattuja menetelmiä käyttäen. Esimerkissä järjestelmää varten ei ole luotu yksityiskohtaisia konfiguraatioita, asetuksia tai muita vastaavia määrityksiä. Järjestelmien toiminnallisuus, käyttötapaukset ja keskeiset tietoturvakontrollit kuvataan yleisellä tasolla siten, että poikkeamien arvioiminen työkalun avulla on mahdollista.

7.5.1 Ympäristön kuvaus

Organisaation verkkoympäristö koostuu työasemaverkosta, DMZ-verkosta, palvelinverkosta ja hallintaverkosta. Hallintaverkkoa käytetään palvelinten ylläpitoon ja valvontaan. Palvelin- ja DMZ-verkot sisältävät tietojärjestelmän sovellukset ja palvelut. DMZ-alueelle on sijoitettu sisäiset ja ulkoiset web-sivustot, sähköposti-, välitys-, antivirus- ja päivityspalvelimet. Active Directory (AD), tiedosto-, sovellus- ja tietokantapalvelimet on sijoitettu sisäiseen palvelinverkkoon.

Sovelluspalvelimella sijaitsevaa asianhallintajärjestelmää käytetään organisaation turvaluokiteltujen dokumenttien ja tiedostojen hallintaan. Sovelluksessa on selainpohjainen käyttöliittymä (https). Sovelluksen toimittaja on kaupallinen yritys. Tietojärjestelmälle ei ole asetettu käytettävyysvaatimuksia ja sovelluksen ylläpito tapahtuu virka-aikana. Palvelinten ja verkkolaitteiden ylläpito on järjestetty virka-ajan ulkopuolella päivystysluonteisesti. Organisaatio käsittelee ympäristössään korkeintaan suojaustason IV tietoja ja on luokitellut koko käyttöympäristön tälle tasolle.



Kuvio 5: Esimerkki 1

7.5.2 Keskeiset kontrollit

Liikenteen suodatus:

DMZ-verkon palvelinten ja Internetin välinen liikenne on rajattu toiminnallisten tarpeiden mukaisesti sisäänpäin ja ulospäin internet-palomuurissa. Toimistoverkon liikenne Internetin suuntaan kulkee välityspalvelimen kautta. Palvelin-, DMZ- ja toimistoverkkojen välistä liikennettä rajoitetaan sisäverkon palomuurissa toiminnallisten tarpeiden mukaan.

Työasemat:

Organisaatiossa käytetään Windows 7 työasemia, jotka ovat keskitetyn hallinnan piirissä. Toimistokäyttäjillä ei ole pääkäyttäjäoikeuksia työasemiin. Työasemiin on asennettu antivirus- ja palomuuriohjelmistot ja kiintolevyt on salattu käyttöjärjestelmän tarjoamalla salausratkaisulla. Kirjautumiseen käytetään toimikorttia ja PIN-koodia tai vaihtoehtoisesti käyttäjätunnusta ja vahvaa salasanaa. Etäyhteyden muodostamiseen VPN ohjelmiston avulla käytetään lisäksi vahvaa käyttäjätunnistusta. Käyttöjärjestelmän ja ohjelmistojen päivitykset tehdään keskitetysti. Ylläpitohenkilöstöllä on toimistokäyttäjistä poiketen pääkäyttäjäoikeudet työasemiin. Käyttäjätilit lukittuvat viiden virheellisen kirjautumisyrityksen jälkeen. Sovellustoimittajalla on käytössään työasemat, jotka eivät ole organisaation hallinnassa.

Käyttöoikeudet:
Käyttöoikeudet palvelimille on rajattu käyttäjäryhmien mukaisesti. Ylläpitoa varten on luotu erilliset ryhmät eri toimintoja varten ja ylläpitäjät voivat kuulua vain yhteen ryhmään kerrallaan. Ryhmät on jaoteltu tietokantojen, käyttöjärjestelmien, verkkolaitteiden ja sovelluksen ylläpitoa varten. Kaikilla ylläpitäjillä on rooliensa mukaisesti pääkäyttäjäoikeudet hallinnoimiinsa laitteisiin tai ohjelmistoihin. Toimistokäyttäjillä on asianhallintajärjestelmään luku- ja kirjoitusoikeudet käyttöliittymän kautta.

Ylläpito:
Palvelinten (Windows 2008 server R2) ylläpito tapahtuu hallintaverkossa sijaitsevalta hallintapalvelimelta. Hallintapalvelimelle on sallittu RDP yhteydet toimistoverkosta ja VPN ohjelmistolle varatusta osoiteavaruudesta. Oletetaan, että VPN-ratkaisu täyttää suojaustason IV salausvaatimukset. Ylläpitäjillä on hallintapalvelimelle henkilökohtaiset tunnukset. Muilla palvelimilla on käytössä yhteiskäyttöiset tunnukset ylläpitoa varten. Ylläpitoyhteydet palvelimille ja verkkolaitteille muodostetaan SSH ja RDP protokollia käyttäen. Palvelinten tietoturvan koventamisen periaatteina on käytetty Microsoftin perustason ohjetta (baseline server hardening).

Sovellustoimittaja ylläpitää ja tekee muutokset asianhallintajärjestelmään omilla työasemillaan omasta toimipisteestään. Ylläpitoyhteyksiin käytetään organisaation tarjoamaa client VPN -ratkaisua.

Päivitykset:
Käyttöjärjestelmä- ja ohjelmistopäivitykset haetaan valmistajien web-palvelimilta keskitetysti DMZ-verkossa sijaitseville päivitys- ja antiviruspalvelimille. Antivirus- ja päivityspalvelimet liikennöivät ulospäin välityspalvelimen kautta. Välityspalvelimelle on määritelty domainpohjainen pääsylista päivitysten hakemista varten.

Antivirusohjelmistojen tunnistetiedot päivitetään kerran vuorokaudessa ja ne jaellaan automaattisesti palvelimille ja työasemille. Palvelinten ja verkkolaitteiden käyttöjärjestelmä- ja ohjelmistopäivitykset tehdään kuukausittain huoltoikkunan aikana virka-ajan ulkopuolella.

Valvonta:
Työasemille ja palvelimille asennetut antivirusohjelmistot muodostavat hälytyksen virus- tai haittaohjelmatartuntatapaus havaittaessa ja hälytys lähetetään ylläpidolle sähköpostitse. Hallintaverkon valvontapalvelin tekee kyselyitä (polling) verkkolaitteiden ja palvelinten tilasta verkkotasolla. Valvontapalvelin luo kyselyiden perusteella havaituista virhetilanteista hälytyksen, joka lähetetään sähköpostitse ylläpidolle.

Varmistukset:
Tietokannasta ja palvelimista otetaan päivittäin inkrementaaliset varmistukset. Verkkolaitteiden konfiguraatioiden varmistukset otetaan aina kun konfiguraatioihin tehdään muutoksia. Kaikkia varmistuksia säilytetään 6kk.

7.5.3 Riskianalyysi

Riskianalyysin esimerkiksi on valittu organisaation sovellustoimittajan työasemiin kohdistuvat riskit. Taulukoon 7 on listattu osa poikkeamista, joita työasemiin kohdistuu verrattuna KATAKRI:n suojaustason IV vaatimuksiin. Seuraavissa sarakkeissa on kuvattu poikkeamista aiheutuvia uhkia ja niiden seurauksia. Menetelmän mukaisesti poikkeaman aiheuttavaa kontrollin puutetta ja siihen mahdollisesti tehtäviä muutoksia tulisi arvioida monesta eri näkökulmasta (valitut avainsanat), jolloin todennäköisyyksien ja vaikutusten arviointi voitaisiin tehdä tarkemmin. Esimerkkiympäristössä varsinaista kontekstia suojattavan tiedon osalta ei ole, jonka vuoksi analyysin tarkoituksenmukainen tekeminen ei ole kaikilta osin mahdollinen. Etenkin todennäköisyyksien ja vaikutusten arvioiminen on vaikeaa, sillä vaikutukset saattavat riippua pitkälti esim. suojattavan tiedon luonteesta, määrästä ja sisällöstä.

ID	Vaatimus	Poikkeama	Uhka	Seuraus
1	I 503.0	Haittaohjelmien suodatuksesta ei voida varmistua, eikä mahdollisista hälytyksistä välity tietoa organisaatiolle.	Sovellustoimittajan hallintatyöasemalla on haittaohjelma, joka leviää organisaation palvelinverkkoon tai antaa hyökkääjälle pääsyn työasemaan.	Suojattava tieto paljastuu ja/tai altistuu asiattomalle käsittelylle.
2	I 504.0	Työasemien keräämistä lokitiedoista ei ole varmuutta, eikä niihin ole näkyvyyttä.	Lokitietoja käyttäjien toimenpiteistä ei kerätä riittävästi, eikä niitä säilötä riittävän pitkältä aikaväliltä	Mahdollisissa väärinkäytöksissä tai virhetilanteissa tarvittavaa jäljitettävyyttä tapahtumista ei ole. Poikkeaman juurisyyn selvittäminen vaikeutuu.
3	I 507.0	Työasemien huollosta ja elinkaaren hallinnasta ei ole varmuutta.	Työasema ja sen kiintolevy päätyvät kolmannen osapuolen haltuun esim. huollon yhteydessä	Suojattavaa tietoa päätyy kolmannen osapuolen haltuun ja tiedon luottamuksellisuus vaarantuu
4	I 602.0	Tietoaineiston säilytyksestä ja käsittelystä ei voida varmistua	Suojattavaa tietoa ei säilytetä asianmukaisesti	Suojattava tieto paljastuu tahattomasti asiattomille henkilöille
5	I 703.0	Toimittajan henkilöstön käyttöoikeuksien hallinnasta ei voida varmistua.	Toimittajan henkilöstöllä on työasemiin ylläpito-oikeudet, jolloin haittaohjelmiin ym. liittyvät riskit kasvavat.	Organisaation tietojärjestelmiin kohdistuvien riskien todennäköisyys kasvaa.
6	I 706.0	Toimittajan tietoverkkojen ja -järjestelmien turvallisuudesta ei voida varmistua	Suojattavaa tietoa siirretään toimittajan tietoverkossa ja tietojärjestelmissä, jolloin turvallisuuden tulisi vastata organisaation tietoturvallisuuden tasoa. Ylläpitoon käytettävien työasemien ja niiden sisältämään suojattavaan tietoon kohdistuva hyökkäyspinta-ala kasvaa.	Suojattava tieto paljastuu ja/tai altistuu asiattomalle käsittelylle.

Taulukko 7: Uhka-analyysi

Esimerkissä uhkien kompensointia ei ole otettu huomioon puutteellisista lähtötiedoista johtuen. Todennäköisyydet ja vaikutukset on määritetty alustavasti ja sijoitettu riskimatriisiin (Taulukko 8).

Todennäköisyys							
	1	Suuri					
	0,8	Melko suuri					
	0,6	Kohtalainen					
	0,4	Melko pieni			2	1	
	0,2	Pieni		3			
			Pieni	Melko pieni	Kohtalainen	Melko suuri	Suuri
			0,2	0,4	0,6	0,8	1
					Vaikuttavuus		
			Riskiarvo	1,04			

Taulukko 8: Esimerkin riskimatriisi

Yllä kuvatussa esimerkissä on arvioitu vain osittain sovellustoimittajan työasemaratkaisua ja riskiarvo tässä tapauksessa saavuttaa taulukossa 6 asetetun erittäin korkean riskin raja-arvon. Mikäli arvio tehtäisiin kattavasti koko työasemaratkaisuun ja esimerkkiympäristöön kokonaisuudessaan, olisi luku tästä vielä huomattavasti suurempi.

Esimerkin avulla pyritään osoittamaan, että riskin (toimittajan omat työasemat) systemaattinen analysointi ja purkaminen osiin kriteeristöä vasten tuottavat huomattavasti enemmän tietoa, kuin jos toimittajan omien työasemien käyttö käsiteltäisiin yhtenä yksittäisenä riskinä.

Mikäli esimerkissä kuvattua organisaation sisäistä palvelinten hallintamallia sovellettaisiin myös sovelluksen hallintaan, olisivat tulokset hyvin erilaisia. Organisaation työasemat ovat keskitetysti hallittuja, käyttöoikeudet rajattu toiminnallisten tarpeiden mukaisesti ja niiden liikennöintiä valvotaan ja lokeja kerätään organisaation sisällä. Ylläpitomallissa palvelimia hallitaan yhteiskäyttöisillä tunnuksilla, josta voidaan kirjata poikkeama (KATKARI II, I 501.0). Yhteiskäyttöisten tunnusten käyttämistä kompensoidaan edellyttämällä ensin henkilökohtaisilla tunnuksilla kirjautumista hallintapalvelimelle, josta varsinainen ylläpitoyhteys muodostetaan. Tällöin yhteydet ovat jäljitettävissä eri palvelinten kirjautumislokeja yhdistelemällä.

Kompensoinnin voidaan katsoa vaikuttavan alentavasti todennäköisyyteen, jos oletetaan että tiukemmalla kontrollilla voidaan vaikuttaa henkilöiden turvallisuuskäyttäytymiseen. Myös mahdollisen haitta- tai vakoiluohjelman jäljittäminen saattaa helpottua.

ID	Vaatimus	Poikkeama	Uhka	Seuraus	Kompensaatio
1	I 501.0	Ei henkilökohtaisia tunnuksia palvelinten ylläpitoon.	Organisaatio ei tunnista mahdollista väärinkäytösten lähdettä.	Väärinkäytösten mahdollinen lisääntyminen kontrollin puutteesta johtuen.	Jäljitettävyyden parantaminen erillisen hallintapalvelimen käytön seurauksena.

Taulukko 9: Uhka-analyysi

Yllä kuvattujen esimerkkien avulla saatujen lopputulosten perusteella voidaan suositeltaviksi toimenpiteiksi esittää esimerkiksi toimittajan hallinta- ja ylläpitoyhteyksien toteuttamista organisaation hallinnoimilla työasemilla ja menetelmillä tai niitä mukaillen.

8 Konstruktion arviointi

Työkalun rakennetta, toiminnallisuutta ja soveltuvuutta arvioitiin asiantuntijaryhmässä. Työkalun nähtiin pääosin soveltuvan sille tarkoitettuun käyttöön. Hyvinä puolina nähtiin, että tulosten avulla arvioinnin tulokset voivat olla paremmin perusteltavissa ja tarkemman arviointitiedon tuottaminen tuo lisäarvoa. Lisäksi koettiin, että pidemmällä aikavälillä arviointien yhteismitallisuus voi parantua, mikäli menetelmää käytetään säännönmukaisesti ja se koetaan toimivaksi.

Työkalun huonoiksi puoliksi koettiin sen vaatima raskas työkuorma. Työkalun tulosten suhteellinen hyöty työmäärään nähden on saatava tasolle, jolla saadaan tavoiteltu lisäarvo. Mikäli työkalun vaatima työmäärä ylittää siitä saatavan hyödyn, sen käyttö voi jäädä vähäiseksi eikä työlle asetettuja tavoitteita näin ollen saavuteta. Riskianalyysin ja riskimatriisin välinen tulosten automatisointi nähtiin edellytykseksi työkalun käyttämiselle, jotta työkuorma ja tulosten saaminen helpottuisi ja käytettävyys yleisesti parantuisi. Vaikuttavuuden ja todennäköisyyden merkityksen ymmärtäminen työkalun kontekstissa todettiin olevan epäselvä eli työkalua käyttäessä tulisi huomioida ja tuoda selkeästi esille se, että analysoinnissa määreet viittaavat yksittäiseen uhkaan tai riskin eikä arvioinnin kohteeseen kokonaisuutena. Näkemys vahvistaa työssä käsiteltyä työkalun kontekstisidonnaisuutta.

Työkalun käytännön testaaminen tulee tehdä oikeissa ympäristöissä, jotta työkalusta saatavien tulosten lisäarvoa ja työkalun käytettävyyttä voidaan arvioida paremmin. Oikeiden käyttöympäristöjen arviointi ja niiden tulokset on rajattu tästä työstä pois julkisuuslain 6 luvun perusteella.

8.1 Validiteetti

Työkalun validiteettia arvioitaessa on otettava huomioon sen avulla tuotettava tieto ja tulokset. Työn kontekstissa validiteetti perustuu riskienhallintaan ja arviointitiedon tuottamiseen liittyvien menetelmien avulla saatuihin tuloksiin ja niiden hyödynnettävyyteen. Työkalussa käytettävät menetelmät, joiden avulla tuloksiin päädytään, ovat tarkoituksenmukaisia ja ne on valittu riittävän kattavasti perustuen luvussa 6 esiteltyihin prosesseihin.

Uhkien ja riskien arviointi on aina subjektiivista ja asiayhteydestä riippuvaista. Tästä johtuen työkalun tulosten validius on suhteellista ja käyttötapauksesta riippuen lähtötiedot sisältävät epätarkkuuksia ja epävarmuustekijöitä. Edellä mainittujen seikkojen lisäksi arviointiin käytettävien lähde- ja taustamateriaalien määrä ja laatu saattavat vaihdella merkittävästi, jolloin tulosten validiteetti on myös näistä riippuvainen. Työkalun kvantitatiiviseen arviointiin liitty-

vistä mittaristoista ei ole työn aikana saatu empiirisiä tuloksia, jonka vuoksi mittaristojen tuottamien tulosten validiutta ei voida varmistaa.

Työkalun voidaan todeta olevan loogisesti ja sisällöllisesti validi, eli työkalun tulokset näyttävät tukevan lähtökohtaisia oletuksia ja teoriapohja vastaa tarkoituksenmukaisuutta. Ulkoisen ja sisäisen validiteetin arviointi vaatii työkalun käytännön testaamista ja tätä kautta saatavien empiiristen tulosten analysointia, jotta voidaan varmistua siitä tukevatko tulokset todellisuudessa olettamuksia.

8.2 Reliabiliteetti

Työkalun käytön yhdenmukaisuudesta voidaan varmistua sitomalla se tiettyyn arviointikriteeristöön. Tällöin työkalussa käytettävä mittaristo on lähtökohtaisesti sama ja

Tulosten tarkkuus ja yhdenmukaisuus saattavat vaihdella käyttötapauksesta ja arvioitavasta kohteesta riippuen huomattavasti, vaikka käytettävä kriteeristö olisikin sama. Tarkkuutta voidaan mitata paremmin, kun työkalun avulla on arvioitu useita samankaltaisia tai toistuvia ilmiöitä. Tulosten vertailukelpoisuudessa on kuitenkin huomioitava aina havainnon tai arvion asiayhteys ja konteksti.

Työkalun tarkoituksena on tuottaa objektiivisempaa arviointitietoa, vaikka lähtökohtaisesti työkalun ja sen avulla suoritettavan riskienarvioinnin tulokset pohjautuvat aina subjektiiviseen ja tapauskohtaiseen arviointiin. Tulosten objektiivisuus edellyttää myös, että työkalua käytetään tässä työssä kuvatulla tavalla. Objektiivisuutta ja tulkinnanvaraisuutta voidaan arvioida, kun työkalun avulla on saatu riittävästi vertailukelpoisia tuloksia tai teettämällä työkalun mukainen arvio samaan kohteeseen usealla eri arvioijalla.

9 Reflektio ja kritiikki

Työn tutkimusaiheen kannalta oleellinen puute on, että työkalua ei ole testattu käytännössä. Käytännön testaamisen puute vaikuttaa tutkimuksen validiteetin ja reliabiliteetin arviointiin. Validiteetti ja reliabiliteetti ovat työn lopputulosten arvioinnin kannalta tärkeässä osassa ja tutkimus jää tältä osin puutteelliseksi.

Tutkimuksessa luodun konstruktion käyttäminen edellyttää paljon taustatietoa ja syvää ymmärrystä arvioitavasta kohteesta. Systemaattinen analysointiprosessi on raskas ja työmäärältään suuri. Näistä syistä johtuen työkalulle asetettu tavoiteltu käyttö saattaa jäädä tarkoitustaan vähäisemmäksi. Toisaalta työkalun käyttötarkoitus on tuottaa tarkempaa tietoa arvioin-

nin kohteesta, joten valittu menetelmä tukee asetettuja tavoitteita ja on tältä osin perusteltua.

Jotta työkalulla voidaan tuottaa tarkoituksenmukaista arviointitietoa, taustalla vaikuttavat prosessit ja metodologia arviointitiedon tuottamiseen ja riskienhallintaan liittyen tulee ymmärtää riittävällä tarkkuudella. Muutoin työkalun tulokset eivät välttämättä ole luotettavia ja tästä saattaa aiheutua virheellisiä johtopäätöksiä.

Lähdemateriaali perustuu pitkälti standardeihin, lakeihin ja asetuksiin. Riskienhallintaan liittyen on tehty paljon tutkimusta, mutta työssä on tarkoituksellisesti pitäydytty laeissa määritellyissä tietoturvallisuuden arviointiperusteissa. Konstruktio on rakennettu perustuen standardissa esiteltyyn malliin, joka ei ole suoraan sovellettavissa tutkimusaiheeseen. Mallin käyttämistä ja soveltuvuutta tietoriskien hallintaan ja arviointiin tulee arvioida kriittisesti.

Työkalu keskittyy vain tietoriskeihin, eikä siinä ole huomioitu esim. henkilöriskien ja fyysisen turvallisuuden riskeihin kuin välillisesti. Henkilöstöön, turvallisuusjohtamiseen ja fyysiseen turvallisuuteen liittyvät riskit, kontrollit ja menetelmät ovat osa tietoturvallisuuden kokonaisuutta, joten näiden osa-alueiden puuttuminen tutkimuksessa tulee huomioida arvioitaessa lopputulosta.

Tutkimuksen metodologia, työhön valitut prosessit ja menetelmät sekä lähdemateriaali antavat työkalulle perustellun pohjan tutkimuksen puutteista huolimatta.

10 Jatkokehitys

Työkalun jatkokehityksen kannalta on välttämätöntä saada tuloksia todellisista ympäristöistä, jotta työkalun reliabiliteettia ja validiteettia pystytään parantamaan. Työkalun mittaristoja ja raja-arvoja tulee arvioida ja kehittää siten, että ne tukevat tarkoituksenmukaista toimintaa ja että tulosten tulkinta olisi helpompaa. Jatkokehitys tulee tapahtumaan työkalun käytön ohella tapaustutkimuksen kaltaisesti havainnoinnin ja reflektoinnin kautta.

Toisena kehityskohteena on työkalun taulukoiden välinen automatisoiminen, jolloin käsin tehtävä työmäärä vähenee. Automatisointi parantaa työkalun käytettävyyttä ja vähentää virheiden määrää.

Vaikka tässä tutkimuksessa kehittämisessä on käytetty vaatimuskehikkona KATAKRI II:ta, ei työkalua ole sidottu yksittäiseen kriteeristöön. Jatkokehitys tullaan tekemään KATAKRI:n kolmatta versiota ja VAHTI-ohjeistuksia vasten. Kriteeristöjen lisääminen osaksi työkalua osaltaan helpottaisi työkalun käyttämistä.

11 Yhteenveto

Tietoverkkoihin ja –järjestelmiin kohdistuu nykyisin enemmän uhkia ja riskejä ja tästä johtuen riskienhallinnan merkitys tietoturvallisuuden hallinnassa ja toteuttamisessa on kasvanut. Erilaisia riskienhallinnan menetelmiä on laajalti käytössä, mutta useat olemassa olevat mallit keskittyvät operatiiviseen toimintaan ja taloudellisiin vaikutuksiin liittyvien riskien tunnistamiseen ja hallintaan yleisellä tasolla. Toimintaan ja toimintoihin liittyvien riskien syyt, seuraukset ja vaikutukset voivat olla hyvin moniulotteisia ja tästä syystä riskien tarkempi analysointi voi tuoda lisäarvoa organisaatioille.

Viranomaisten toimintaan liittyy erilaisia lakipohjaisia vaatimuksia. Tässä työssä on tarkasteltu riskienhallintaan liittyvää toimintaa tietoturvallisuudelle asetettujen vaatimusten näkökulmasta ja luotu työkalu, jonka avulla pyritään systemaattisesti analysoimaan olemassa olevia riskejä pohjautuen tietojärjestelmille asetettuihin vaatimuksiin. Arvioitaessa vaatimustenmukaisuutta riskienhallinnan tuloksia verrataan asetettuihin vaatimuksiin. Tässä työssä lähestymistapa on osittain käänteinen ja eroaa edellä mainitusta mallista siten, että analyysi tehdään asetetuista vaatimuksista havaittuihin poikkeamiin pohjautuen ja riskienhallinnan tulokset johdetaan tehdystä analyysista. Systemaattinen ja rakenteinen analyysi poikkeamien

Työssä luodun työkalun tarkoituksenmukainen käyttäminen edellyttää hyvää riskienhallinnallisten menettelyjen ja arviointitiedon tuottamiseen liittyvien periaatteiden tuntemusta. Uhkien ja riskien analysoinnin tulokset ovat aina vahvasti sidottuja tapauskohtaiseen kontekstiin. Tästä syystä yleistettävän mallin ja tulosten vertailukelpoisuutta tulee aina arvioida kriittisesti.

Työssä kehitetyn työkalun avulla voidaan saada tarkempaa ja analyyttisempaa arviointitietoa olemassa olevista riskeistä ja niiden vaikutuksista. Riskienhallintaa tulee kuitenkin käsitellä vain turvallisuustoiminnan tukemiseen käytettävänä apuvälineenä. Mitä tarkempaa tietoa organisaatioiden, niiden järjestelmien ja toimintoihin liittyvistä uhkista ja riskeistä voidaan saada riskienarvioinnin tuloksena, sitä paremmat edellytykset organisaatioilla on riskien hallitsemiselle.

Lähteet

Asetus tietoturvallisuudesta valtionhallinnossa 2010/681.

BSC/IEC 61882. 2001. Hazard and operability studies – Application guide. Lontoo. BSI.

EU neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä. 2013/488/EU.

Evalsed. 2013. The resource for the evaluation of Socio-Economic Development.

Hiltunen, L. 2009. Validiteetti ja reliabiliteetti. Jyväskylän yliopisto. Viitattu 26.2.2015. http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

ISO/IEC 27005. 2008. Information technology – Security techniques - Information security risk management. International Electrotechnical Commission. Sveitsi.

ISO 31000. 2009. Risk management – Principles and guidelines. Sveitsi.

ISO/IEC 31010. 2009. Risk management – Risk assessment techniques. International Electrotechnical Commission. Sveitsi.

Kasanen, E. Lukka, K. Siitonen, A. 1992. The Constructive Approach in Management Accounting Research. Journal of Management Accounting Research.

Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588.

Laki tietoturvallisuuden arviointilaitoksista 22.12.2011/1405.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 1406/2011.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Lukka, K. 2001. Konstruktiivinen tutkimusote. Viitattu 21.1.2015. http://www.metodix.com/fi/sisallys/01_menetelmat/02_metodiartikkelit/lukka_const_research_app/?tree:D=&tree:selres=168562&hrpDelimChar=%3B&parentCount=1

Metsämuuronen, J. 2006. Laadullisen tutkimuksen käsikirja. 1. painos. Jyväskylä. Gummerus.

National Institute of Standards and Technology. 2010. Guide for Applying the Risk Management Framework to Federal Information Systems. 1. revisio. Yhdysvallat.

Ojasalo, K. Moilanen, T. Ritalahti J. 2009. Kehittämistyön menetelmät. WSOYpro Oy.

Oyegoke, A. 2011. The constructive research approach in project management research. International Journal of Managing Projects in Business, Vol. 4.

Peltier, T. 2001. Information security risk analysis. Yhdysvallat. CRC Press LLC.

Puolustusministeriö. 2011. Kansallinen turvallisuusauditointikriteeristö. Helsinki.

SFS-ISO/IEC 27001. 2013. Informaatioteknologia. Turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät, vaatimukset. 2. painos. Suomen standardoimisliitto.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.

Valtiovarainministeriö. 2009. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä VAHTI 7/2009.

Valtiovarainministeriö. 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta VAHTI 2/2010.

Valtiovarainministeriö. 2012. Teknisen ICT-ympäristön tietoturvataso-ohje VAHTI 3/2012.

Vaso, J. 1998. Ammatillisen aikuiskoulutuksen laatu. Tampere. Tampereen yliopisto.

Virtanen, P. 2007. Arviointi. Helsinki. Edita Publishing Oy.

Wheeler, E. 2011. Security Risk Management. Yhdysvallat. Elsevier.

Kuviot

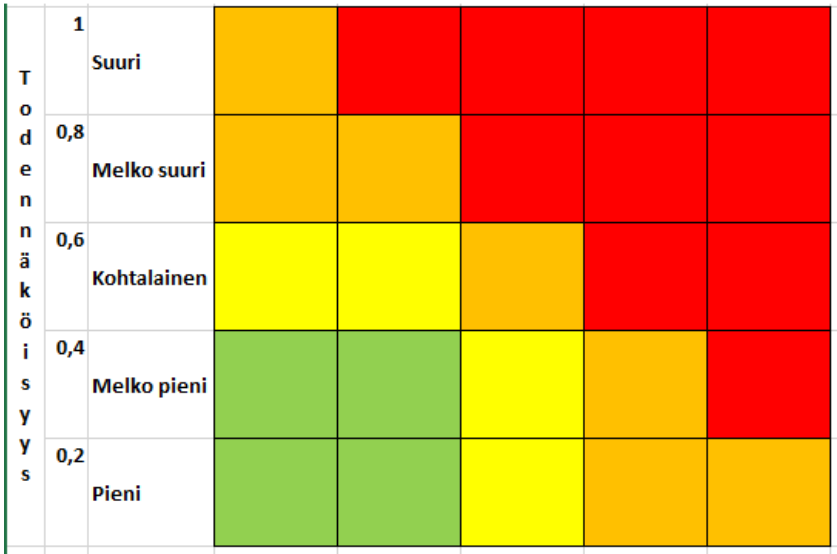
Taulukot

Liitteet

Liite 1 Arviointityökalu

Arvioinnin kohde:				Päivämäärä:							
				Arviointiryhmä:							
ID	Vaatimus	Poikkeama	Uhka	Seuraus	Kompensaatio	Luottamuksellisuus	Vaikutusalue: Eheys	Saatavuus	Vaikuttavuus	Todennäköisyys	
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Avainsanat:	Selite:
NO or NOT	Negation of intention (ei kontrollia)
MORE	Quantitative increase (enemmän kuin vaadittu)
LESS	Quantitative decrease (riittämätön kontrolli)
AS WELL AS	Quantitative increase (vaaditun lisäksi)
PART OF	Quantitative decrease (osittainen kontrolli)
REVERSE	Logical opposite of intention (päinvastainen toiminto)
OTHER THAN	Complete substitution (kompensointi)



Riskiarvo	0

Raja-arvo	Riskiluokitus	Toimenpidesuositus:	ST IV	ST III
> 0,8	Erittäin korkea	Vaatii välittömiä toimenpiteitä	Ei hyväksyttävissä	Ei hyväksyttävissä
0,6	Korkea	Huomattava tarve toimenpiteille	Hyväksyttävissä, tarve toimenpiteille	Ei hyväksyttävissä
0,4	Kohtalainen	Tarve toimenpiteille	Hyväksyttävissä	Hyväksyttävissä, tarve toimenpiteille
0,2	Matala	Ei välitöntä tarvetta toimenpiteille	Hyväksyttävissä	Hyväksyttävissä

Liite 2 KATAKRI II, I-osion vaatimukset

ID	Kysymys	Perustaso (IV)	Korotettu taso (III)
Tietoliikenneturvallisuus			
I 401.0	Onko tietoliikenneverkon rakenne turvallinen?	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internet-verkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja. (Vrt. I 403.0) 3) Tietoliikenneverkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri suojaustarpeen järjestelmät on sijoitettu erillisille verkko-alueille (esim. DMZ-erottelu). 4) Vyöhykkeisiinjakoperusteet on kuvattu. 5) Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain luvallinen liikenne sallitaan. 6) Valvonnan ja rajoitusten periaatteet on kuvattu. 7) Työasemilla, kannettavilla tietokoneilla ja vastaavilla on käytössä (host-based) palomuuriratkaisu, myös organisaatioverkon sisällä. 8) Fyysinen verkko on jaettu turvavyöhykkeisiin. Käytännössä vaaditaan, että hallitun fyysisen tilan ulkopuolelle menevä liikenne salataan siirrettäessä ST IV -tason (turvallisuusluokitusmerkintä KÄYTTÖ RAJOITETTU) mukaisia tietoaineistoja (vrt. I 605.0).	1) Tietojenkäsittely-ympäristö on fyysisesti tai loogisesti erotettu ja valvottu verkko, josta ei ole suoria liittymiä alemman suojaustason verkkoihin. Viranomainen voi tapauskohtaisesti hyväksyä valvotun ja rajatun yhteyden määriteltyihin vastaavan suojaustason järjestelmiin. 2) Tiettyihin viranomaisen suojaustason III tietojärjestelmiin voidaan tuoda tietoa viranomaisen hyväksymän yhdyskäytäväratkaisun (esim. vain yksisuuntaisen liikenteen sallivan datadiodin) kautta. 3) Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri suojaustason järjestelmiin/verkkoihin, se on järjestettävä erillisellä tietokoneella, jota ei kytketä suojaustason III verkkoon. Viranomainen voi tapauskohtaisesti hyväksyä myös tietyt yhdyskäytäväratkaisut eri suojaustason järjestelmien välillä. 4) Tietyt viranomaisen tietojärjestelmät koostuvat suuresta määrästä tietyn suojaustason tietoa ja näissä järjestelmissä asiakokonaisuus nousee luokitukseltaan usein yksittäistä tietoa korkeampaan suojaustasoluokkaan (kasautumisvaikutus, esim. suuri määrä suojaustason IV tietoa voi muodostaa yhdistettynä suojaustason III tietovarannon). Viranomainen voi tapauskohtaisesti hyväksyä rajatun ja valvotun pääsyn osaan tällaisen järjestelmän tietosisällöstä myös luokkaa alemman suojaustason hyväksytyistä järjestelmistä. Hyväksyttävä toteutus edellyttää yleisten suojausmenetelmien lisäksi muun muassa pääsyn rajaamista vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, havainnointi- ja torjuntakykyä poikkeavien/luvattomien käyttötapausten (esim. suuret

			määrät tietohakuja) varalle ja sitä, että järjestelmään tehdyistä tietohauista jää lainmukaisesti säilöttävä tallenne, josta voidaan jälkikäteen yksilöidä mm. tapahtuman (esim. tietohaku) suorittanut henkilö.

I 402.0	Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia? Miten on varauduttu yleisimpiin nykyisiin verkkohyökkäyksiin?	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa. c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisy-	Perustason vaatimukset soveltuen, lähinnä vyöhykkeiden sisällä ja/tai rajoilla, vrt. I 401:n määritykset. 1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa. c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunesto-

		keinot toteutettu.	hyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu.
I 403.0	Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu (vrt. I 401.0). 3) Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan tarkastuksilla.	Perustason vaatimusten 1 ja 2 lisäksi:Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisillä tarkastuksilla.
I 404.0	Onko hallintayhteydet suojattu asianmukaisesti?	1) Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2) Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä. Vrt. etähallintavaatimus I 704.0.	1) Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2) Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä. Vrt. etähallintavaatimus I 704.0.
I 405.0	Miten verkon aktiivilaitteet on kovennettu?	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset, 4) hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista, 5) Laitteistot on konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti. 6) Kytkimen työasemaportit on erotettu toisistaan	Perustason vaatimusten lisäksi: 1) Verkkolaitteiden lokeista on pystyttävä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. 2) Kytkimien käyttämättömät portit on poistettu käytöstä.

		ja työasemat eivät voi suoraan kommunikoida keskenään. Kytkimet eivät saa olla verkkoliikennettä kaiuttavassa toimintatilassa (HUB-toiminnallisuus). 7) Mikäli kytkimissä käytetään VTP-toimialuetta (VLAN Trunking Protocol domain), on VTP-salasana asetettu ja otettu käyttöön. 8) Kytkimissä ei käytetä oletus-VLAN:ia (tyypillisesti VLAN 1) operatiiviselle liikenteelle.	
I 406.0	Miten langattomia verkkoja suojataan?	1) "Vierasverkoille", joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista. 2) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 3) Liikenne salataan luotettavasti.	Langattomat verkot ovat lähtökohtaisesti kiellettyjä. Tapauskohtaisesti voidaan hyväksyä ratkaisu, jossa liikenne on turvatasolle hyväksytyllä menetelmällä salattu päästä-päähän (ei vain radiotie), ts. langatonta verkkoyhteyttä käsitellään kuin julkista verkkoa.
I 407.0	Onko sisäverkon rakenteen näkyminen Internetiin ja muihin ei-luotettuihin verkkoihin estetty? Onko sisäverkon rakenteen ja liikenteen tarpeeton näkyminen sisäverkossa estetty?	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa (ks. I 402.0 ja I 405.0).	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa (ks. I 402.0 ja I 405.0).
I 408.0	Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan? Onko resurssit mitoitettu toimintavaatimusten mukaisiksi?	1) Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa. 2) Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti.	Perustason vaatimusten lisäksi:Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. I 107.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a) merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b) normaalitilaan nähden poikkeavat protokollat, c) luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).

I 409.0	Miten IPv6:n turvallisuuteen vaikuttavat erityispiirteet on huomioitu verkoissa ja järjestelmissä? Onko organisaatiolle ongelmalliset piirteet huomioitu ja tarpeelliset vastatoimet otettu käyttöön?	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperustetta.	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperustetta.
I 410.0	Miten reitityksen turvallisuudesta on huolehdittu?	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.
Tietojärjestelmäturvallisuus			

I 501.0	Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin? Miten tämä on käytännössä järjestetty?	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin: 1) Käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet. 2) Kaikki käyttäjät tunnistetaan ja todennetaan. 3) Pääsyä käyttöjärjestelmään valvotaan turvallisen sisäänkirjausmenettelyn avulla. 4) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. 5) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 6) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. 7) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.	Perustason vaatimusten 1-4, 6, 7 lisäksi: Käyttäjän tunnistamiseen käytetään vahvaa käyttäjäntunnistusta, mikäli samalla tietojärjestelmällä hallinnoidaan useampia kuin yhtä ko. suojaustason hanketta.
I 502.0	Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Katso IV-tason kohdennetut vaatimukset Huom-kentästä.	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Katso IV- ja III-tasojen kohdennetut vaatimukset Huom-kentästä.

I 503.0	Miten on pienennetty haittaohjelmien aiheuttamia riskejä?	1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet). 2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja. 4) Haittaohjelmatunnisteet päivittyvät säännöllisesti. 5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta (vrt. A 806.0). 6) Haittaohjelmahavaintoja seurataan (vrt. A 408.0).	Perustason vaatimusten lisäksi: Tapauskohtaisesti arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. Mikäli liityntöjen käytölle ei ole todellista perustetta, ne poistetaan käytöstä. Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.
I 504.0	Onko organisaation teknisten laitteiden ja palveluiden lokimenettelyt kunnossa? Kerätäänkö verkoista, laitteista ja järjestelmistä keskeiset lokitiedot ja käsitelläänkö niitä asianmukaisesti?	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 2) Keskeisiä tallenteita säilytetään 6 kk tai erillisessä sopimuksessa määrätty aika. 3) Suojattavaa tietoa sisältävät lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).	Perustason vaatimusten 1 ja 3 lisäksi:1) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 2) On käytössä menettely hyökkäyksen/väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan. Menettelyn on sisällettävä vähintään kerran viikossa tapahtuva lokitietojen tarkkailu normaalitilaan nähden poikkeavien tapahtumien havaitsemiseksi. Erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan (vrt. I 408.0 ja A 410.0). 3) Samassa organisaatiossa tai turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun tarkan ajanlähteen kanssa. 4) Lokitiedot ja niiden kirjauspalvelut ovat suojattuja väärentämiseltä ja luvattomalta pääsyltä. On käytössä jokin menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen. 5) Keskeiset lokitiedot varmuuskopioidaan säännöllisesti. 6) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkintä. 7) Kriittisistä ylläpitotoimista tallennetaan kirjausketju (audit trail).

I 505.0	Miten suojattavat tiedot säilytetään tietojärjestelmissä?	1) Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä. 2) Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti (ks. I 603.0). 3) Suojaustason IV tietoa sisältävät kannettavien tietokoneiden kiintolevyt ovat riittävällä tasolla suojattuja (vrt. I 506).	Perustason vaatimusten 1 ja 2 lisäksi: 1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason III tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 509.0). 2) Mikäli samalla palvelimella/palvelimilla säilytetään useamman kuin yhden ko. turvatason hankkeen/projektin/toiminnon tietoja, palvelimella olevat tiedot säilytetään luotettavasti salakirjoitettuna käyttöoikeusrajoitteisissa hakemistoissa tai alueilla. 3) Suojaustason III tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.
I 506.0	Kuinka varmistutaan siitä, että suojattavaa tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, mobiilipäätteet, ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?	1) Suojattavaa tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. 2) Turvaluokiteltua tietoa sisältävät älypuhelimet:a) Pääsy puhelimen ja muistikortin tietoihin suojataan salasanalla. b) Käytössä puhelimen/SIM-kortin/muistikortin automaattinen lukittuminen. c) Etätyhjennysmahdollisuus käytössä. d) Puhelimen ja muistikortin muisti suojataan. e) Verkko- ja haittaohjelmauhat huomioidaan riskienarvioinnin mukaisesti. f) Bluetooth- ja WLAN-yhteydet ovat oletusarvoisesti kytketty pois päältä ja ne aktivoidaan vain käytön ajaksi. Bluetooth-asetuksissa puhelimen näkyvyys on oletuksena asetettu piilotetuksi.	Perustason vaatimuksen 1 lisäksi:Suojaustason III aineistoa ei lähtökohtaisesti käsitellä älypuhelimilla. Toimivaltainen viranomainen voi kuitenkin tapauskohtaisesti erillishyväksyä tietyt toteutukset, joissa älypuhelin ja kaikki sen kautta kulkeva liikenne suojataan luotettavasti.

I 507.0	Kuinka varmistutaan siitä, etteivät suojattavat tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.
I 508.0	Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä? Miten tiedetään mitä (tietojärjestelmiin liittyviä) laitteita organisaatiossa on käytössä? Miten hallitaan tietoa käytetyistä ohjelmistoista ja niiden versio- ja lisenssitilanteesta? Havaitaanko, jos laite viedään luvatta pois organisaation tiloista? Havaitaanko, jos järjestelmiin on asennettu luvattomia ohjelmistoja? Tarkistetaanko kaikki tilat, joista on mahdollista päästä organisaation verkkoon, säännöllisesti luvattomien laitteistojen ja ohjelmistojen havaitsemiseksi?	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit. 3) Konesalit, kytkentäkaapit ja vastaavat tilat tarkistetaan todennettavaan suunnitelmaan pohjautuen säännöllisesti luvattomien laitteistojen (pakettikaappaimet, key-loggerit, luvattomat langattomat tukiasemat, jne.) löytämiseksi.	Perustason vaatimusten lisäksi: 1) Kaikki tilat, joista on mahdollista päästä suojattuun verkkoon, tarkistetaan todennettavaan suunnitelmaan pohjautuen säännöllisesti luvattomien laitteistojen löytämiseksi. 2) Verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet, jotka eivät ole käytössä, on kytketty fyysisesti kytkentäpisteistä irti. 3) Tuntemattomien laitteiden kytkeminen verkkoon estetään verkkoteknisin keinoin.
I 509.0	Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.

I 510.0	Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä? Ovatko salausavaintenhallinnan prosessit ja käytännöt dokumentoituja? Miten käytännön toteutus on järjestetty?	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.
I 511.0	Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.
I 512.0	Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.
I 513.0	Miten on varmistuttu ajettavan koodin turvallisuudesta?	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	Perustason vaatimuksen lisäksi: 1) Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus). 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaatteiden, esim. Open Web Application Security Project Guide, toteuttamista. Toimittajilta vaaditaan selvitys, miten tietoturvallisuus on otettu huomioon tuotekehityksessa.

I 514.0	Kuinka varmistutaan siitä, että organisaatioon hankittavat laitteistot ovat tietoturvaperiaatteiden mukaisia ja käyttötarkoitukseensa nähden riittävän tietoturvallisia?	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.
Tietoaineistoturvallisuus			
I 601.0	Millainen tiedon luokittelumenettely organisaatiolla on?	Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.
I 602.0	Onko huolehdittu siitä, että suojattavia tietoa sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti?	1) Suojattavalle aineistolle on työtiloissa lukitut kaapit, kassakaapit tai vastaavat. 2) Huonetilasta poistuttaessa selväkielisessä muodossa oleva, mutta suojassa pidettävä aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään kassakaappiin, lukittuun kaappiin tai vastaavaan säilytystilaan. 3) Huonetilasta poistuttaessa työskentelytila tarkistetaan tai tila lukitaan ulkopuolisilta.	Huonetilasta poistuttaessa suojaustason III aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään EURO II -tason kassakaappiin tai vastaavaan tarkoitukseen hyväksyttyyn säilytystilaan, kuten hälytysjärjestelmällä varustettuun holviin (EURO IV).

I 603.0	Hävitetäänkö suojattavia tietoja sisältävät aineistot luotettavasti?	1) Suojattavien sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen). 2) Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti. Vrt. I 505.0. 3) Ei-sähköisten suojattavien aineistojen tuhoaminen on järjestetty luotettavasti. Organisaatiossa on paperinrepijä, jonka silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4), tai jokin muu hyväksytty menetelmä suojaustason IV aineiston hävittämiseksi (esim. polttaminen).	1) Uudet asiakashankkeet (esim. ohjelmistoprojektit) aloitetaan aina "puhtaalla" laitteistolla. Ts. uudet hankkeet aloitetaan aina ympäristössä, jossa ei ole jäännöstietoja edellisistä hankkeista. 2) Eri asiakkaiden tietoja käsitellään erillisillä muisteilla (eri kiintolevyt eri hankkeille). Viranomainen voi tapauskohtaisesti hyväksyä myös ratkaisun, jossa eri hankkeita käsitellään erillisillä loogisilla muistialueilla (esim. virtualisointia hyödyntäen). 3) Organisaatiossa on hyväksytty paperinrepijä suojaustason III aineiston hävittämiseksi. Silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4).
I 604.0	Miten suojattavan aineiston kopiointi ja tulostus on järjestetty?	1) Kopioita käsitellään kuten alkuperäistä asiakirjaa. 2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus aineistoon ja tarve tietosisältöön. 3) Alkuperäiset luokittelumerkinnät säilyvät kopioinnissa ja tulostuksessa (tai vastaavat merkinnät lisätään välittömästi kopioinnin/tulostuksen jälkeen).	Perustason vaatimusten lisäksi: 1) Kopion/tulosteen saa ottaa vain suojaustasolle hyväksytyllä laitteella. 2) Kopiokoneiden ja tulostimien on oltava hyväksytyssä tilassa, eikä niistä saa olla ulkoisia tiedonsiirto- tai huoltoyhteyksiä, ellei niitä ole erikseen viranomaisen toimesta hyväksytty. 3) Tulostimen, kopiokoneen ja vastaavien laitteiden massamuistien tulee olla yksikön turvallisuusvastaavan hallinnassa. 4) Hajasäteilysuojausten on vastattava niille asetettuja vaatimuksia (vrt. F 217.0).

I 605.0	Miten suojattavan aineiston sähköinen välitys on järjestetty? Onko tietoliikenne (ml. sähköinen viestintä) suojattu riskeihin nähden riittävillä mekanismeilla?	1) Organisaatiossa pystytään tunnistamaan suojattavat tiedot ja huolehtimaan siitä, että ne välitetään asianmukaisesti suojaten. 2) Yhteys sähköpostipalvelimen ja -asiakasohjelman välillä on suojattu. 3) Mikäli sähköpostissa, telekopioviestinä, pikaviestimissä, IRC-keskusteluissa, VoIP-puheluissa ja vastaavissa käsitellään suojattavaa tietoa, on liikenne (tai viesti) suojattava siten, että luottamuksellista tietoa ei pääse vuotamaan ulkopuolisille. 4) Aina, kun liikenne kulkee julkisen verkon (Internet, puhelinverkko, GSM-verkko tai muu verkko, mikä ei ole ko. suojaustason vaatimusten mukainen) kautta, on liikenne (tai aineisto) salattava luotettavasti siirrettäessä IV -tason (turvallisuusluokitusmerkintä KÄYTTÖ RAJOITETTU) mukaisia tietoaineistoja. 5) Yhteyden on oltava luotettavasti suojattu päästä-päähän. Tapauskohtaisesti voidaan hyväksyä toteutukset, joissa a) liikenne kulkee salaamattomana vain organisaation luotetun verkon tai verkon osan sisällä, b) liikenne salataan palvelimelta-palvelimelle tai organisaatioiden välillä rajalta-rajalle. 6) Sähköpostia/telekopiolaitetta käytettäessä varmistetaan vastaanottajan osoite/numero. 7) Kun suojattava tieto siirretään tietojärjestelmästä toiseen, se suojataan siirron aikana ja vastaanottavassa järjestelmässä tiedon alkuperäisen tason edellyttämällä tavalla. 8) Tapauskohtaisesti arvioidaan tarve (sähköposti)viestin eheyden tarkistukseen, ja lisäksi arvioidaan onko tarpeen saada tietää, kun viesti on vastaanotettu ja/tai avattu.	1) Telekopiona aineistoa lähetetään vain, jos telekopiokone on a) varustettu viranomaisen hyväksymällä salaamislaitteella ja b) mikäli telekopiolaite on sijoitettu tilaan, johon pääsy on asiattomilta estetty. 2) Puhelimessa suojaustason III aineistosta keskustellaan vain viranomaisen hyväksymän päästä-päähän -salausratkaisun välityksellä (vrt. I 506.0).

I 606.0	Onko suojattavan aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?	1) Lähetykset osoitetaan henkilön nimellä. 2) Pakkaus ei saa ulkoisesti paljastaa sen sisältävän suojattavaa materiaalia. Huom: kirjekuoren tai vastaavan on oltava läpinäkymätön. 3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.	Perustason vaatimuksen 1 lisäksi:1) Suojattavat aineistot lähetetään kirjattuna postina suljetussa, läpinäkymättömässä kaksinkertaisessa kirjekuoressa. Ulommassa kuoressa ei saa olla merkintää suojaustasosta. 2) Organisaation sisäiseen postin käsittelyketjuun saa kuulua vain hyväksyttyä henkilöstöä, jonka perehtymisoikeus ko. tiedon suojaustasoon on hyväksytty ja kirjattu. Henkilöllä on oltava esimiehensä määrittämä, työtehtäviinsä perustuva tarve perehtyä ko. aineistoon. 3) Lähetettäessä aineistoa kuriirin välityksellä, pakkauksen päällä tulee selkeästi ilmoittaa, että pakkauksen saa toimittaa vain kuriirin välityksellä. Kuriiri on koulutettava ja varustettava sekä kuriiritodistuksella, että kuriiripostikirjalla, johon vastaanottaja kuittaa vastaanottamansa lähetyksen.
I 607.0	Pystytäänkö seuraamaan minne ja mistä suojattavat aineistot on välitetty? Kirjataanko suojattavat aineistot?	Ei vaatimuksia.	Ei välityksen seurantavaatimusta. Kirjataan. Huom! EU:n turvaluokiteltu tieto rekisteröidään/diarioidaan.
Käyttöturvallisuus			
I 701.0	Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat? Testataanko toipumisvalmiutta säännöllisesti? Turvataanko suojattavat tiedot myös hätätilanteissa?	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.

I 702.0	Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen? Onnistuuko toipuminen jos järjestelmän tai verkon vastuuhenkilö ei ole käytettävissä? Miten nopeasti toipuminen onnistuu? Seurataanko säännöllisesti, että suojattavaa tietoa käsittelevän ympäristön dokumentaatio on ajan tasalla? Miten menetellään, mikäli tiedoissa on puutteita?	1) Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. 2) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 3) Eroavaisuuksia käsitellään tietoturvapoikkeamina.	1) Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. 2) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 3) Eroavaisuuksia käsitellään tietoturvapoikkeamina.
I 703.0	Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita? Käytetäänkö vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä? Käytetäänkö suojattavan tiedon käsittelyyn vain viranomaisen hyväksymiä tiloja, verkkoja ja järjestelmiä? Miten varmistutaan tietojärjestelmien eheydestä?	1) Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä. 4) Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään (vrt. muutoshallinta: A 608.0). 5) Suojattavan tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä verkkoja ja järjestelmiä.	Perustason vaatimusten lisäksi:Suojattavan tiedon käsittely tapahtuu vain viranomaisen hyväksymässä fyysisessä tilassa.

I 704.0	Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle. 3) Turvallisesta etä- ja matkatyöskentelystä on henkilöstön saatavilla ohje. 4) Laitteita, tietoaineistoja tai ohjelmia ei siirretä pois työpaikalta ilman ennalta saatua valtuutusta. 5) Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja todennusmenettelyjä. 6) Suojattavaa tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle. 7) Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei jätetä valvomatta julkisille paikoille, kannettavat tietokoneet kuljetetaan matkustaessa käsimatkatavarana. 8) Vain luotettavia ja käyttöympäristöön hyväksyttyjä laitteita (esim. työnantajan tarjoama kannettava tietokone) ja etätyöyhteyksiä käytetään.	Suojaustason III järjestelmien etähallinta on lähtökohtaisesti estetty. Etähallinta on sallittu vain viranomaisen erikseen hyväksymällä menettelyllä.
I 705.0	Ovatko kehitys-/testaus- ja tuotantojärjestelmät erilliset?	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.

I 706.0	Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia? Onko tietoturvatiedotteiden seuranta vastuutettu? Onko turvapäivitysten asentamiseen luotu menettelytavat? Valvotaanko niiden toteutumista?	1) Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti. 2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan vuosittain haavoittuvuuksien löytämiseksi.	Perustason vaatimuksen 1 lisäksi: Skannaus suoritetaan vähintään puolivuosittain ja aina merkittävien muutosten jälkeen.
I 707.0	Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?	1) Käyttäjät velvoitetaan seuraavantapaiseen käytäntöön: a) Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. b) Aktiiviset istunnot päätetään työn päättyessä ja pitemmillä tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). c) Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä. 2) Mikäli suojattavaa tietoa sisältävä laite joudutaan jättämään tilaan, jossa siihen on fyysinen pääsy ei-luotetuilla (arvioitava tapauskohtaisesti: esim. organisaation ulkopuolisilla), suojaus on aktivoitava laitteelta poistuttaessa (esim. sammuttamalla kannettava tietokone, jolloin salaus aktivoituu).	Perustason vaatimuksen 1 lisäksi: Suojaustason III aineistoa sisältävää laitetta ei lähtökohtaisesti jätetä tilaan, jossa siihen on pääsy ei-luotetuilla.
I 708.0	Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.

I 709.0	Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä? Onko huolehdittu siitä, että kriittiset ylläpitotoimet vaativat kahden tai useamman henkilön hyväksynnän?	Ei vaatimuksia.	1) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. 2) Vaarallisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, on niitä varten oltava valvontamekanismi. 3) On määritettävä järjestelmäkohtaisesti ne kriittiset toimet, joihin erityisvalvonta kohdistetaan.
I 710.0	Onko riittävästä varmuuskopioinnista huolehdittu?	1) Toimintavaatimuksiin nähden riittävästä varmuuskopioinnista on huolehdittu. 2) Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. 3) Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä. 4) Suojattavaa tietoa sisältävät varmuuskopiot säilytetään tiedon tason edellyttämässä tilassa ja tarvittaessa salakirjoitettuna.	Perustason vaatimusten lisäksi:Varmistusmedioista on olemassa listat.