VALTIOVARAINMINISTERIÖ

Valtionhallinnon ICT-varautuminen

Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset

LUONNOS

15.12.2009

versio 3.0

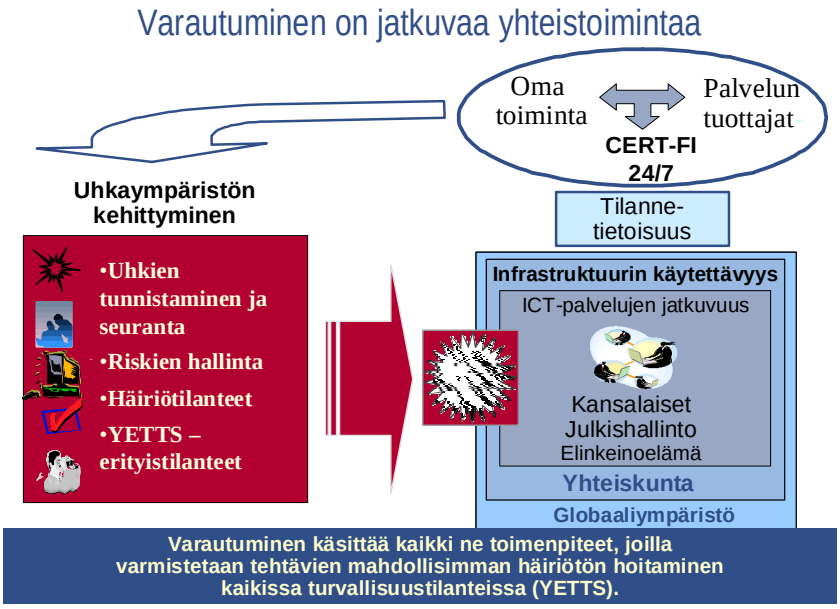
Sisällysluettelo

1. JOHDANTO

1.1 Perusteet

Yhteiskunnan verkostoitunut toiminta edellyttää kaikilta verkoston osilta yhtenäistä, sovitun tasoista tiedon turvaamista sekä toiminnan ja palvelun jatkamisen kykyä normaaliajan häiriö-tilanteissa, erityistilanteissa ja poikkeusoloissa.

Palvelujen käyttäjistä ja ylläpitäjistä koostuviin palveluverkostoihin osallistuu hallinnon eri osapuolia, kansalaisia, yhteisöjä, yrityksiä ja ICT-palveluntuottajia. Keskeistä on varmistaa, että koko palveluverkosto kykenee erilaisissa normaaliajan häiriötilanteissa ja YETTS:n mukaisissa erityistilanteissa jatkamaan toimintaansa asetettujen vaatimusten mukaisesti.



Kuva 1. ICT-varautuminen on jatkuvaa yhteistoimintaa

ICT-varautumisen perusvaatimukset on suunnattu kaikille valtion organisaatioille ja toiminnoille sekä yrityksille, jotka tuottavat valtiolle ICT-palveluja tai ovat yleisesti huoltovarmuuden kannalta merkityksellisiä. Vaatimuksia voidaan soveltaa myös kuntien tarpeisiin.

Vuoden 2011 loppuun mennessä ministeriöiden ohjaamina hallinnonalojen ja virastojen tulee:

- kuvata keskeisimmät toiminta- ja palveluverkostonsa
- määrittää kullekin organisaatiolle ja sen osille sekä palveluille ja järjestelmille tavoiteltava vaatimustaso
- määrittää osaamistarpeet ja käynnistää järjestelmällinen johdon ja muun avainhenkilöstön kouluttaminen
- määrittää aikataulu palveluiden toteuttamiseksi vaatimustasojen mukaisesti
- resursoida toteutus osana normaalia toiminnan ja talouden suunnitteluaan.

Vuoden 2012 loppuun mennessä kriittisimpien palveluiden tulee saavuttaa vähintään perustaso, ja hankinnoissa sekä tarkastustoiminnassa tulee ottaa huomioon jatkuvuuden hallinta ja tiedon turvaaminen.

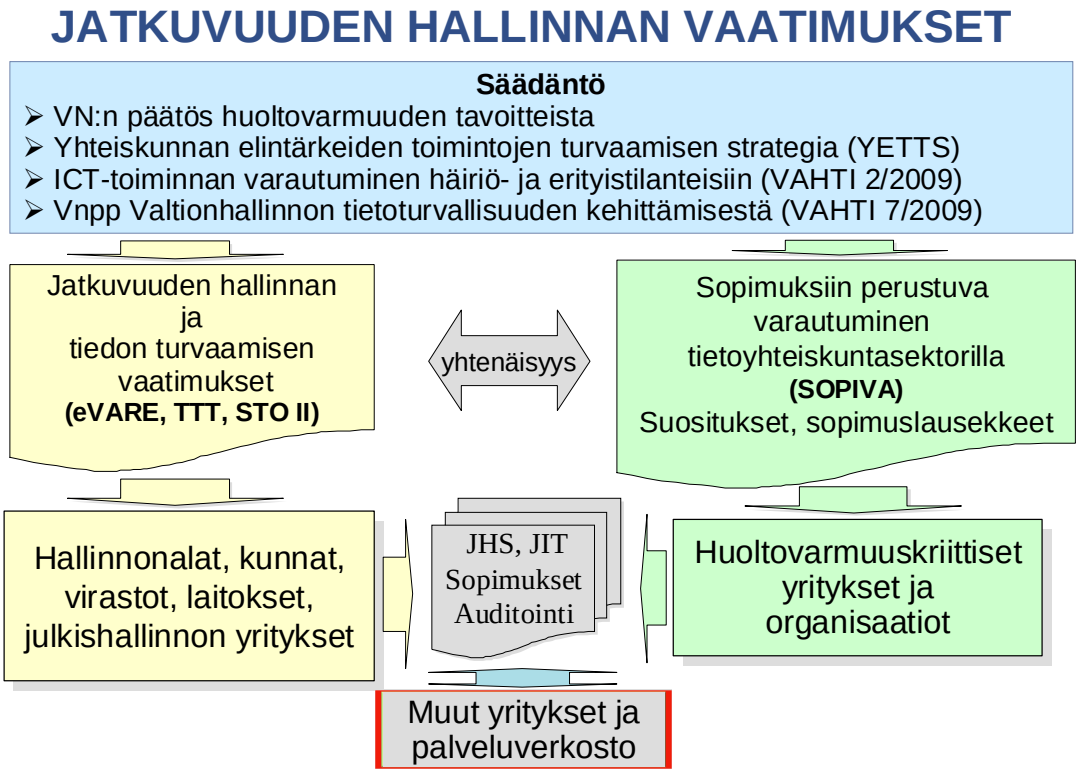
Vuoden 2016 loppuun mennessä valtionhallinnon organisaatioiden, palveluiden ja järjestelmien tulee saavuttaa niille asetettu tavoitetaso.

1.2 Vaatimustasojen muodostuminen ja rakenne

Varautumisen normipohjan muodostavat Valmiuslaki sekä Valtioneuvoston päätös huoltovarmuuden tavoitteista. Valmiuslaki velvoittaa viranomaisia varautumiseen. Normien lisäksi ICT-varautumisen ohjauksessa ja vaatimusten muodostamisessa keskeinen asiakirja on YETT-strategia, jota täydentää VAHTI-yleisohje ”ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin”.

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä[1] ohjaa valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Periaatepäätöksen mukaisesti säädösten ja organisaatiokohtaisten tavoitteiden, toimintojen ja tietojen lisäksi tietoturvallisuuden, varautumisen ja suojauksen tason määrittämisen ja toteuttamisen lähtökohtia ovat valtiovarainministeriön antamat tietoturvallisuuden ja varautumisen tasot ja ohjeet.

Yhtenäisten vaatimusten avulla pyritään sekä julkishallinnon että talouselämän toimintojen yhtenäistämiseen. Samalla edesautetaan palvelujen jatkuvuuden ennakointia häiriö- ja erityistilanteissa. Julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille suunnataan VM:n johdolla laadittu ohje: ”Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset”. Huoltovarmuusorganisaation johdolla on laadittu yritysten keskinäistä toimintaa varten ohje ”Sopimuksiin perustuva varautuminen tietoyhteiskuntasektorilla”. Näiden ohjeiden avulla pyritään saamaan yhtenäiset vaatimukset koko tietoyhteiskunnan käyttöön seuraavan kuvan mukaisesti.

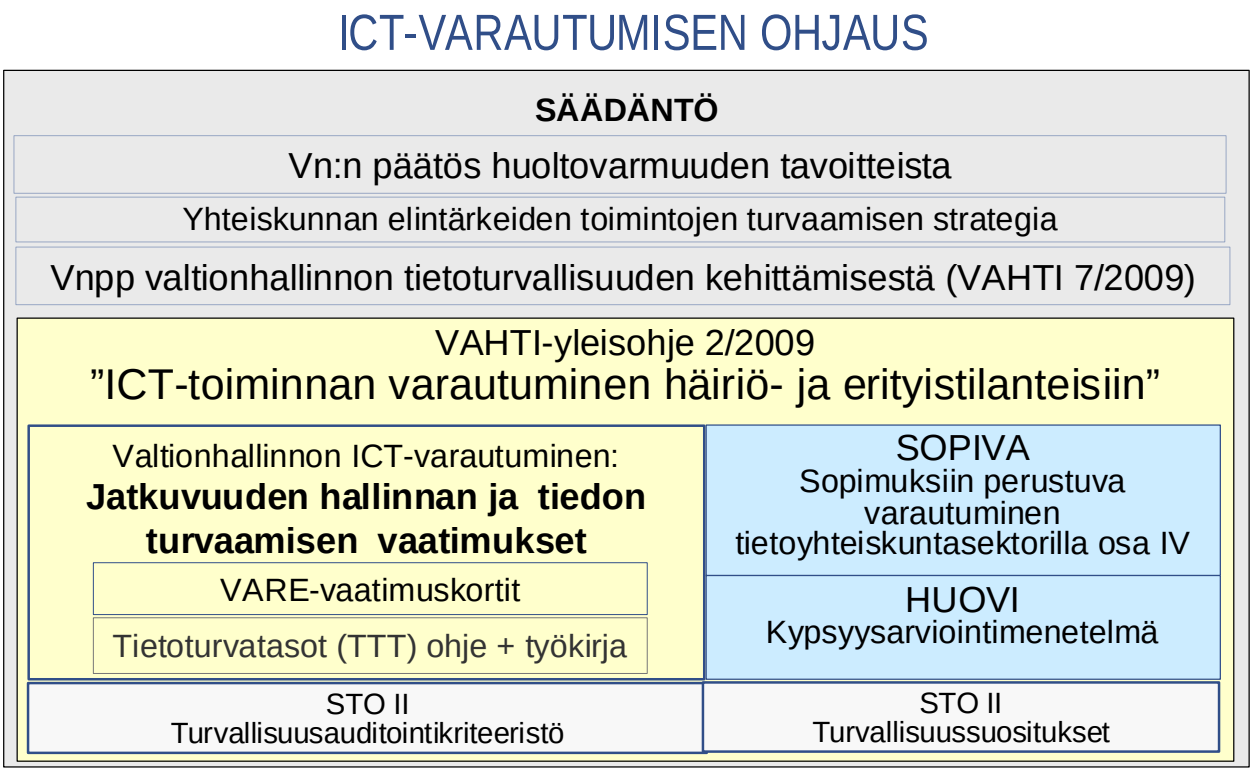


Kuva 2. Vaatimusten ulottaminen julkishallinnon ja talouselämän toimijoihin.

ICT-varautumisen, jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset on määritelty

[1] VAHTI 7/2009, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus

yhteistyössä Huoltovarmuuskeskuksen HUOVI- ja SOPIVA[1]-hankkeiden kanssa. Vaatimuksiin on linkitetty myös STO II -ohjelmassa tuotettu turvallisuusauditointikriteeristö. Eri ohjeista ja vaatimuksista muodostuu toisiaan täydentävä kokonaisuus seuraavan kuvan mukaisesti.



Kuva 3. ICT-varautumiseen liittyvä kokonaisuus toisiaan täydentäviä ohjeita ja linjauksia

Vaatimuksia asetetaan organisaation toiminnalle, palveluille ja ICT:n toteuttamiselle. Vaatimukset on ryhmitetty kuuteen osaan. Osissa 1 – 4 on organisaation ja toiminnan kypsyyteen liittyviä vaatimuksia strategisen johtamisen, toiminnan ohjauksen, henkilöstö-hallinnon ja kumppanuusverkoston hallinnan näkökulmista. Osa 5 asettaa vaatimuksia erilaisille teknisille järjestelmille, prosesseille ja ratkaisuille. Kuudennessa osassa on esitetty vaatimukset mittaamiselle ja auditoinnille.

Julkishallinnon organisaatiot ja toiminnot sekä sen käyttämät ja tuottamat palvelut, järjestelmät ja tekniset ratkaisut määritetään jatkuvuuden hallinnan ja tiedon turvaamisen näkökulmasta pääsääntöisesti perus- korotetulle tai korkealle tasolle.

Kunkin tason saavuttamiseksi on toteutettava kaikki kyseisen tason sekä sitä alempien tasojen vaatimukset. Valittua tasoa ylemmiltä tasoilta voidaan kuitenkin tarvittaessa toteuttaa yksittäisiä lisäkontrolleja, joilla parannetaan esimerkiksi järjestelmän käytettävyyttä määritellyissä erityistilanteissa. Järjestelmän käytettävyys voidaan myös tilapäisesti nostaa korkeammalle tasolle esimerkiksi ennalta tiedettyjen, ajallisesti rajoitettujen maksutapahtumien ajaksi.

[1] SOPIVA: Sopimuksiin perustuva varautuminen tietoyhteiskuntasektorilla. Vaihe 4 : Varautumiseen liittyvien sopimusehtoluonnosten laatiminen. www.huoltovarmuus.fi/julkaisut/julkaisuarkisto

Kuva 4. Vaatimustasot ja esimerkki eri palvelujen ja järjestelmien sijoittumisesta vaatimustasoille.

Lähtötaso on organisaatiolle ensimmäisen vaiheen tila, josta pyritään vähintään jatkuvuuden hallinnan ja tiedon turvaamisen minimitasona olevalle perustasolle**.**

Perustaso mahdollistaa turvallisesti hallinnon normaalin, voimakkaasti verkostoituneen toiminnan. Normaaliolojen häiriötilanteista selviydytään toiminnan vaatimuksia vastaavasti yhtenäistetyillä, normaaleilla palvelusopimuksilla. Taso vastaa normaalin liikeyrityksen laadukasta toimintaa. Perustasolle sijoittuu tyypillisesti suurin osa hallintoa tukevista järjestelmistä, kuten matkahallintajärjestelmät. Perustason vaatimusten täyttäminen ei aiheuta merkittäviä lisäkustannuksia, kun ne otetaan huomioon organisaation, toiminnan, palvelujen ja järjestelmien kehittämisessä alusta alkaen. Jo käytössä olevat palvelut ja järjestelmät siirretään perustasolle järjestelmämuutosten ja päivitysten yhteydessä.

Korotettu taso on tarkoitettu organisaation kriittisille toiminnoille. Perustasoon verrattuna korotetun tason vaatimuksia on tiukennettu vastaamaan verkostoitumisen ja yhteiskunnan elintärkeiden toimintojen hoitamisen asettamia tarpeita. Vain osa organisaation toiminnasta, palveluista ja järjestelmistä on tarkoituksenmukaista toteuttaa tällä tasolla. Korotetun tason järjestelmiä ovat esimerkiksi potilastietojärjestelmät ja perusrekisterit. Myös sähköposti tai organisaation muu keskeinen sanomanvälitysjärjestelmä on hyvä sijoittaa korotetulle tasolle erityistilanteiden toimintaa varmistamaan.

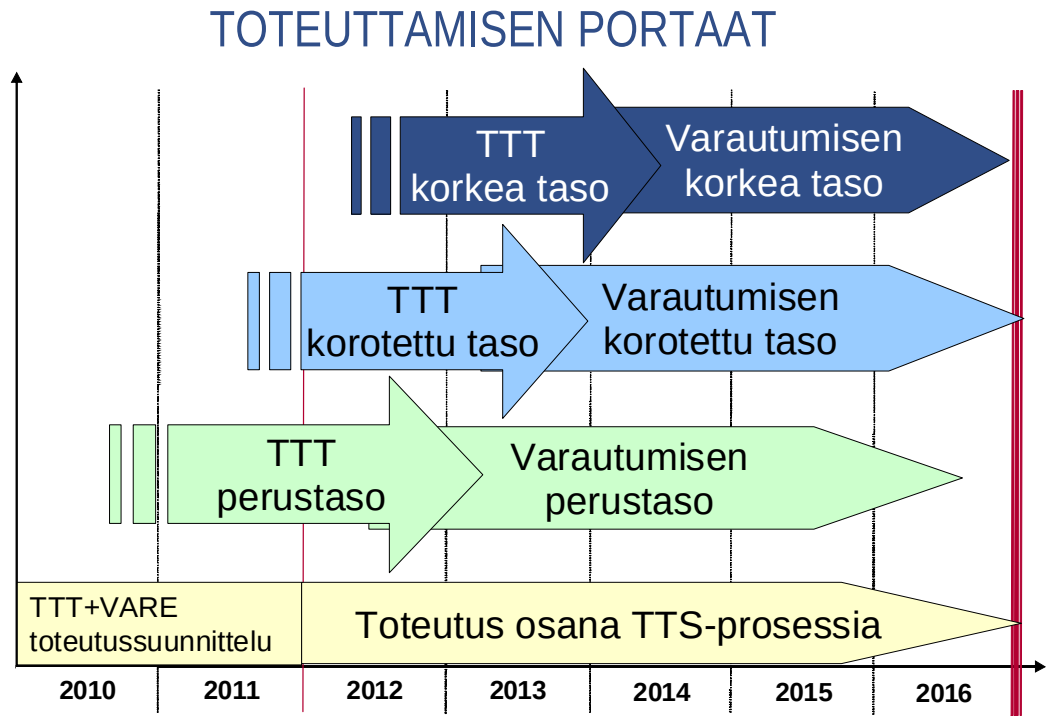
Korkea taso vastaa YETTS:n erityistilanteiden hoitamisen ja poikkeusolojen tarpeita. Korkean vaatimustason järjestelmiä ovat esimerkiksi turvallisuusviranomaisten operatiiviset järjestelmät. Korkea taso asettaa merkittäviä lisävaatimuksia organisaation toiminnalle, osaamiselle ja järjestelmien toteutukselle.

Erityistaso on korkean tason vaatimukset ylittävä tila, jossa on toiminnan luonteen vuoksi jouduttu ottamaan käyttöön yhteisistä menetelmistä ja ratkaisuista poikkeavia, korkean tason vaatimukset ylittäviä ratkaisuja. Näitä vaatimuksia ja ratkaisuja hallinnoi kukin hallinnonala itsenäisesti.

1.3 Vaatimusten käyttö valtionhallinnossa

Valtionhallinnossa käytettävien yhtenäisten jatkuvuuden ja tiedon turvaamisen vaatimusten tulee kattaa koko verkostoitunut toimintaprosessi, myös hallintoalojen rajat ylittäen. Vähintään perustason vaatimusten ja kontrollien noudattaminen, arviointi ja raportointi ovat velvoittavia. Osa kontrolleista on luonteeltaan toimintaa ja toteutusta ohjaavia ja osa selkeästi mitattavia ja raportoitavia.

Ministeriöillä on merkittävä rooli oman hallinnonalansa varautumisen ohjaamisessa tulosohjauksen keinoin. Kunkin viraston on arvioitava mitkä sen palveluista ja järjestelmistä edellyttävät korotetun tai korkean tason varautumista. Tässä arvioinnissa on otettava huomioon myös palvelua käyttävien sidosryhmien tarpeet. Järjestelmät ja palvelut siirretään valitulle tasolle ensisijassa elinkaarenhallinnan luonnollisessa vaiheessa, kuten järjestelmäpäivityksen yhteydessä.



Kuva 5. Vaatimukset kannattaa toteuttaa vaiheittain normaalin TTS-prosessin yhteydessä.

Ministeriöt vahvistavat virastojensa esitysten perusteella hallinnonalansa korkealle tasolle sijoitettavat järjestelmät toiminnan ja talouden suunnitteluun, tulosohjaukseen sekä seurantaan liittyen.

Vaatimukset, kontrollit sekä osa-alueilla tavoiteltavat vaatimustasot vaiheistuksineen kirjataan viimeistään vuodesta 2012 alkaen hallinnonalojen ja tilivirastojen toiminnan ja talouden suunnitteluun, tulosohjaukseen ja raportointiin.

Valtionhallinnon yhteisten palvelujen ja järjestelmien sijoittaminen korkealle ja korotetulle tasolle määritetään yhteistyössä ministeriöiden kesken VM:n koordinoimana, kuten myös hallinnonalarajat ylittävien tietovirtojen ja prosessien koordinointi.

Vuodesta 2012 lähtien virastoilla on oltava kyky yhteistyössä Valtion IT-palvelukeskuksen kanssa arvioida vaatimustasojen täyttymistä omassa ja palveluntoimittajiensa toiminnassa.

1.4 Vaatimusten soveltaminen yrityksissä ja palveluyksiköissä

Yritysten varautuminen normaaliolojen häiriöihin ja poikkeusoloihin perustuu pääsääntöisesti niiden liiketoiminnan tarpeisiin, lakisääteisiin velvoitteisiin ja sopimuksissa määriteltyihin vaatimuksiin. Yritykset voivat ottaa omaehtoisesti käyttöönsä SOPIVA-suosituksia tukeakseen liiketoimintansa tarpeita.

Yritykset voivat myös ryhtyä soveltamaan näitä jatkuvuuden hallinnan ja tiedon turvaamisen vaatimuksia omassa toiminnassaan ja kumppanuusverkostojensa sopimusjärjestelyissä.

Julkishallinnolle palvelua tuottavien yritysten voidaan edellyttää täyttävän palvelutuotantoonsa liittyvät vaatimukset hyödyntäen yrityskohtaisia keinoja. Yritysten tulee silloin osoittaa täyttävänsä asetettu vaatimustaso luotettavasti omien yrityiskohtaisten kontrolliensa avulla.

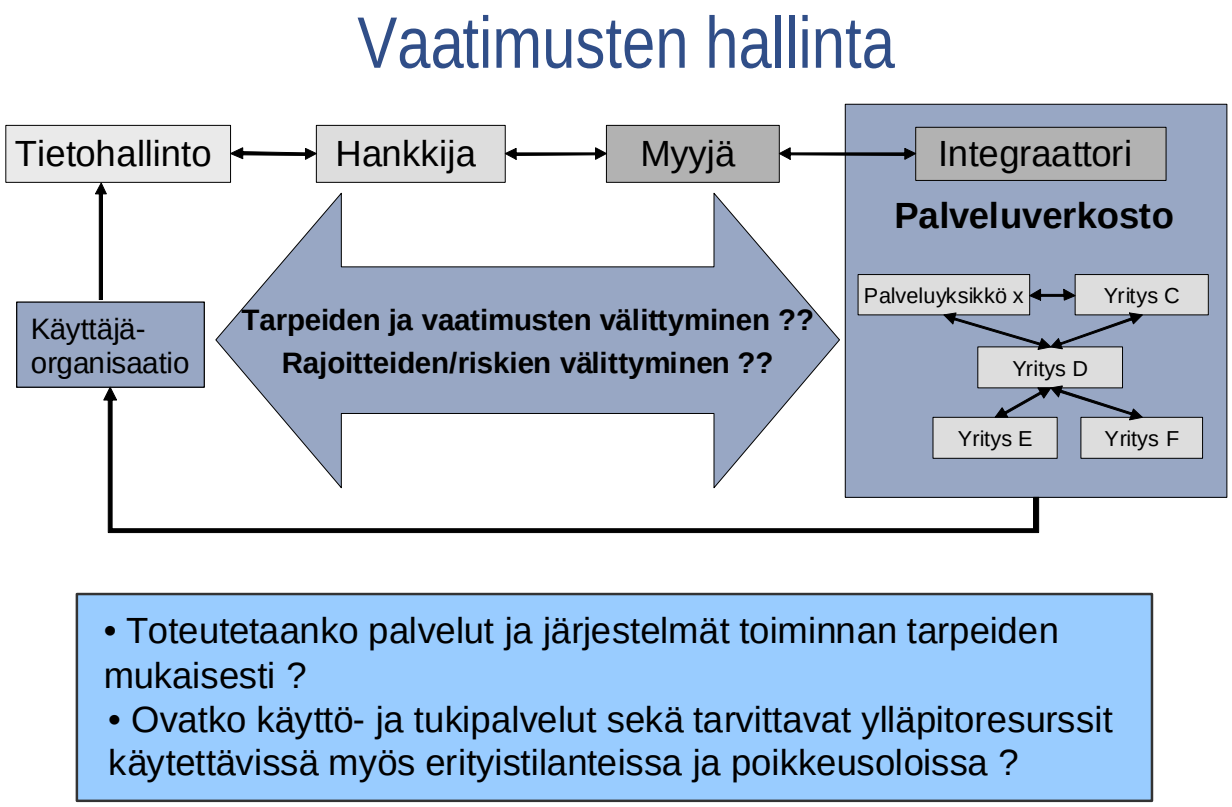
Yritysten näkökulmasta yhtenäinen valtionhallinnon toimijoiden vaatimusasettelu yksinkertaistaa ja yhtenäistää asiakasvaatimusten täyttämistä sekä antaa hyvän työkalun yrityksen oman alihankkija- ja kumppanuusverkoston hallintaan.

Korotetun ja korkean tason vaatimusten toteuttaminen voidaan tarvittaessa rajata vain siihen yksikköön, joka tuottaa tai ylläpitää ko. tason palveluja.

1.5 Soveltaminen hankinnoissa ja palvelusopimuksissa

Jokainen organisaatio vastaa vaatimusten sisällyttämisestä tekemiinsä tarjouspyyntöihin ja sopimuksiin. Tarjouspyyntöjä ja sopimuksia laadittaessa tulee huomioida, että osa tässä hankkeessa määritellyistä jatkuvuuden hallinnan ja tiedon turvaamisen vaatimuksista ei sellaisinaan sovellu hankinnoissa käytettäviksi ja palvelutoimittajia velvoittaviksi. Hankintojen helpottamiseksi VM määrittää alkuvaiheessa hankinnoissa sovellettavat yhteiset vaatimukset. Virastot voivat laajentaa omien tarpeidensa mukaisesti hankinnan kohteeseen liittyvien velvoittavien vaatimusten joukkoa.

Jokaisen organisaation tulee varmistua, että palvelulle asetettu vaatimustaso välittyy hankintaketjussa palvelun toimittajalta edelleen palvelun tuottamiseen osallistuvalle verkostolle. Samoin on varmistuttava, että palveluun jääneet rajoitteet ja jäännösriskit tiedotetaan palvelun tilaajalle ja käyttäjäorganisaatioille seuraavan kuvan mukaisesti.



Kuva 6. Vaatimusten hallinta palveluverkostossa

Kilpailutuksissa palvelun tarjoajan kyvykkyys toimia erilaisissa häiriötilanteissa ja poikkeusoloissa tulee ottaa huomioon omana kriteerinään. Viraston tulee varmistua, että vaatimukset asetetaan ulkoiselle tai sisäiselle sopimuskumppanille ja että nämä huolehtivat niiden asettamisesta edelleen alihankkijoilleen.

Viimeistään vuonna 2011 uusiin palvelusopimuksiin kirjataan perustason ja tarvittaessa korkeampien tasojen vaatimusten noudattaminen.

Perustason noudattamisvelvoite tulee ulottaa myös alihankintaehtoihin ja kumppanuusverkostoon. Menettelyllä edesautetaan keskeisen yritysverkoston toiminnan jatkuvuuden parantamista. Voimassa oleviin sopimuksiin ei vaatimuksia lisätä kesken sopimuskauden muutoin kuin erityisen painavista perusteista.

Hankintojen yhteydessä tarjoavaa organisaatiota koskevat vaatimukset (esim. Johtajuus-osion vaatimukset) tulee määritellä osana sopimusmallia, joka liitetään tarjouspyyntöön. Hyväksytyn tarjoajan on sitouduttava siihen, että nämä vaatimukset täyttyvät sopimuskauden alussa tai viimeistään siihen mennessä kun palvelu otetaan käyttöön. Hankinnan kohdetta koskevat vaatimukset (esim. Prosessit: ICT-jatkuvuuden hallinta -osion vaatimukset soveltuvin osin) ovat arvioitavia vertailuperusteita. Arvioinnissa on huolehdittava, että tarjouskilpailun voittaja täyttää hankinnan kohteelta vaaditun tason vaatimukset. Hankkivalla organisaatiolla tai sen valtuuttamana esimerkiksi Valtion IT-palvelukeskuksella tulee olla oikeus auditoida vaatimusten toteutuminen tarvittaessa.

2. VAATIMUKSET

2.1 Johtajuus

Organisaation johdon panos on ratkaiseva kehitettäessä organisaation ja sen palvelujen toimintavarmuutta myös häiriötilanteissa. Johdon tehtävä on luoda tarkoituksenmukaiset edellytykset organisaation toiminnan jatkamiseksi kaikissa turvallisuustilanteissa[1].

Johto päättää jatkuvuussuunnittelun tavoitteet. Tavoitteet määritellään analysoimalla toiminnan tarpeet, mittaamisen ja raportoinnin kautta toiminnasta saadut palautteet sekä asiakkaiden ja muiden sidosryhmien tarpeet. Tavoitteiden määrittelyssä on huomioitava lakisääteiset velvoitteet.

Sisäisen viestinnän avulla edistetään henkilöstön tietoisuutta jatkuvuuden hallinnan tavoitteista ja merkityksestä organisaation toiminnalle ja yksittäisille työntekijöille kaikissa turvallisuustilanteissa.

JOHTAJUUS: STRATEGINEN OHJAUS	
Yleisvaatimus	Yleisvaatimuksen perusta
1A: Organisaatio on tunnistanut ydintoimintoihinsa liittyvät jatkuvuuden ja erityistilanteiden hallintaa sekä tiedon turvaamista ohjaavat keskeiset tekijät, velvoitteet ja riippuvuudet.	Velvoitteistaan huolehtiakseen organisaation on ensin tiedostettava niiden olemassaolo. Toimintojen riippuvuussuhteiden ymmärtäminen on myös jatkuvuuden johtamisen perusedellytys.
1B: Jatkuvuuden hallinnan ja tiedon turvaamisen linjaukset on määritelty ydintoiminnan asettamien vaatimusten perusteella.	Jatkuvuuden hallinnan ja tietoturvan on tarkoitus tukea ydintoimintaa, ja siksi ne eivät voi toimia irrallaan ilman ydintoiminnan vaatimuksiin perustuvaa ohjausta.

JOHTAJUUS: ORGANISOINTI	
Yleisvaatimus	Yleisvaatimuksen perusta
1C: Häiriö- ja erityistilanteiden hallinta on linjattu, organisoitu ja huomioitu ohjausmalleissa.	Häiriö- ja erityistilanteissa on tärkeää pystyä toimimaan nopeasti ja tehokkaasti. Se saattaa vaatia normaalista poikkeavaa päätöksentekoa ja toimintatapaa, jota tulee myös harjoitella.
1D: Jatkuvuuden hallinta ja tiedon turvaaminen on organisoitu ja vastuutettu osaksi normaalia johtamista, toimintaa sekä kumppanuusverkoston hallintaa.	Jatkuvuuden hallinta ja tiedon turvaaminen eivät voi olla erillisiä siiloja tai saarekkeita, vaan ne toteutuvat vain osana itse toimintaa, hankehallintaa ja tiedon käsittelyä.
1E: Jatkuvuuden hallinnalle ja tiedon turvaamiselle on osoitettu tavoitteisiin nähden riittävät resurssit.	Tavoitetason tulee olla realistinen ja sen saavuttamiseksi tulee varata riittävät resurssit. Tavoitteiden ja resurssien määrittely tulee sitoa toiminnan ja talouden suunnitteluun.
1F: Jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä.	Yhteistyö on tarpeen, jotta ydintoimintojen kannalta välttämättömät tukitoiminnot voidaan myös huomioida jatkuvuussuunnittelussa, ja jotta toteutetut toimenpiteet ovat linjassa keskenään.

[1] Turvallisuustilanteella tarkoitetaan uhkan tasosta johtuvaa ajallista yhteiskunnan tilaa, joka jakautuu normaalioloihin, häiriötilaan ja poikkeusoloihin. Ks. sanasto

JOHTAJUUS: YHTEISTYÖ, VIESTINTÄ JA RAPORTOINTI	
Yleisvaatimus	Yleisvaatimuksen perusta
1G: Organisaation johto seuraa jatkuvuuden hallinnan ja tiedon turvaamisen kehittämistä, jatkuvuussuunnittelua sekä toimenpiteiden vaikutuksia ja kustannuksia.	Organisaation johdon tulee vaatia riittävät ja ymmärrettävät tiedot jatkuvuuden hallinnan ja tiedon turvaamisen tilasta päätöksenteon tueksi.
1H: Viestinnän ja raportoinnin vastuut ja toimintamalli keskeisimpien sidosryhmien kanssa on määritetty ja organisoitu.	Ulkoistusten ja verkottuneen toimintatavan vuoksi useimmat organisaatiot ovat riippuvaisia keskeisistä sidosryhmistään toimintansa jatkuvuuden varmistamiseksi ja siksi tiedonkulun tulee toimia myös näiden organisaatiorajojen yli.

Vaatimukset 1A, 1C, 1D, 1E, 1F, 1G ja 1H ovat SOPIVA-suosituksia 1,3,4,6,7,9 ja 8.

Tarkemmat johtamiselle asetettavat vaatimukset ovat liitteessä 2.1.

2.2 Strategiat ja toiminnan suunnittelu

Organisaation strateginen suunnittelu kattaa myös häiriöiden ennakoimisen ja varautumisen erityistilanteisiin ja poikkeusoloihin. Organisaation riskien analysointi kohdistuu sisäiseen ja ulkoiseen toimintaympäristöön. Kriittisten tehtävien osalta analysoidaan oman toiminnan ja sidosryhmien toiminnan riskit. Ydin- ja tukitoimintojen riskien priorisointi ohjaa jatkuvuudenhallinnan kehittämistä.

Jatkuvuudenhallinnan ja poikkeusoloihin varautumisen kehittämisessä huomioidaan lakisääteiset velvoitteet. Johto arvioi tapahtuneiden häiriötilanteiden seurauksia ja päättää toimintakyvyn parantamisesta.

STRATEGIAT JA TOIMINNAN SUUNNITTELU: **TOIMINNAN SUUNNITTELU RISKIENHALLINNAN AVULLA**	
Yleisvaatimus	Yleisvaatimuksen perusta
2A: Organisaation ja toimintaympäristön vuorovaikutus otetaan toiminnassa huomioon.	Mikään organisaatio ei toimi tyhjiössä, vaan toimintaympäristössä tapahtuvat muutokset voivat vaikuttaa merkittävästi organisaation toimintakykyyn.
2B: Riskienhallinnan tulokset ohjaavat jatkuvuuden hallinnan ja tiedon turvaamisen kehittämistä.	Riskienhallinnan avulla kehittämistoimenpiteet voidaan kohdistaa sinne missä niistä saatava hyöty on suurin.
2C: Toiminnan jatkuvuuden hallinnan ja tiedon turvaamisen toimenpiteet tukevat organisaation ydintoiminnan tavoitteita.	Jatkuvuuden hallinta ja tiedon turvaaminen ei ole itsetarkoitus, vaan niiden täytyy palvella organisaation tehtävää. (Ks. myös 1B)

STRATEGIAT JA TOIMINNAN SUUNNITTELU: **PALVELUJEN JATKUVUUDEN SUUNNITTELU**	
Yleisvaatimus	Yleisvaatimuksen perusta
2D: Erityistilanteiden hallinnan menettelyt on dokumentoitu, koulutettu ja harjoiteltu.	Selkeät ohjeet ja harjoittelu luovat edellytykset erityistilanteissa toiminnalle. (Ks. myös 1C)
2E: 24/7 toiminta ja CERT-FI -yhteistoiminta vastaa organisaation tavoitteita ja velvoitteita.	Tärkeiden kohteiden ympärivuorokautinen valvonta sekä CERT-FI -yhteistoiminta ovat tärkeitä valtionhallinnon yleisen tilannekuvan ylläpitämiseksi ja riittävän nopean uhkiin reagoinnin varmistamiseksi.

Vaatimukset 2A ja 2B ovat SOPIVA-suosituksia 11 ja 14.

Vaatimukseen 2D on yhdistetty SOPIVA-suositukset 16 ja 18.

Tarkemmat toiminnan ohjaukselle asetettavat vaatimukset ovat liitteessä 2.2.

2.3 Henkilöstö

Jatkuvuuden hallinta on ydintoimintojen ja niiden tarvitsemien tukitoimintojen yhteistoimintaa. Organisaation tulee luoda henkilöstölle mahdollisuus jatkuvasti kehittää osaamistaan, ottaa vastuuta ja olla aloitteellinen. Organisaatiossa on varmistettava että henkilöstöllä on kyky ja taito toimia sovitulla tavalla häiriö- ja erityistilanteissa sekä poikkeusoloissa.

HENKILÖSTÖ: OSAAMISEN JA TIETOISUUDEN KEHITTÄMINEN	
Yleisvaatimus	Yleisvaatimuksen perusta
3A: Jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään.	Henkilöstön riittävä tehtäviensä ja vastuidensa mukainen osaaminen on välttämätön edellytys jatkuvuuden hallinnalle ja tiedon turvaamiselle. Osaamisvaje heikentää työn tuottavuutta.
3B: Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia.	Motivoitunut henkilöstö tuottaa hyviä tuloksia tehokkaasti, vähällä ohjauksella ja valvonnalla.
3C: Organisaatiossa on sovittu menettely valvonnalle, sekä turvallisuuspoikkeamissa ja väärinkäytöstilanteissa toimimiseen.	Selvät pelisäännöt ennaltaehkäisevät väärinkäytöksiä ja varmistavat henkilöstön ja muiden osapuolten oikeuksien toteutumisen myös väärinkäytöstilanteissa/-epäilyissä.

HENKILÖSTÖ: HENKILÖSTÖRESURSSIEN JA TEHTÄVIEN HALLINTA	
Yleisvaatimus	Yleisvaatimuksen perusta
3D: Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt suunniteltu.	Varajärjestelyt ovat välttämättömiä, jotta toiminta voisi jatkua myös silloin kun avainhenkilöt eivät syystä tai toisesta ole käytettävissä.
3E: Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla.	Jos henkilöstöä on liian vähän, osa tehtävistä tehdään huonosti tai jää kokonaan tekemättä. Ydintoimintojen jatkuvuus ei kuitenkaan saa vaarantua.

Vaatimukset 3A, 3B, 3C, 3D ja 3E ovat SOPIVA-suosituksia 19, 20, 21, 22 ja 23.

Tarkemmat henkilöstöresurssien hallinnalle asetettavat vaatimukset ovat liitteessä 2.3.

2.4 Kumppanuudet ja resurssit

Organisaatioiden toiminta ja tuotanto tarvitsevat sisäisiä ja ulkoisia kumppanuuksia ja resursseja. Palvelua hankkiva organisaatio[1] luo yhdessä pääkumppanien kanssa menettelytavat häiriöiden varalle.

Jatkuvuudenhallinnan kehittäminen on yhteistoimintaa kumppaniverkoston ja tilaajan ydin- ja tukitoimintojen välillä.

Kumppanitoiminnan johtamisella on suuri vaikutus häiriöttömyydestä vastaavien tahojen toimintaan.

KUMPPANUUDET JA RESURSSIT: SOPIMUSTEN HALLINTA	
Yleisvaatimus	Yleisvaatimuksen perusta
4A: Organisaation toiminnalle välttämättömät kumppanit, alihankkijat ja resurssit on tunnistettu.	Keskeiset tahot täytyy tunnistaa, jotta kustannuksia aiheuttavat vaatimukset voidaan kohdistaa vain niille sopimuskumppaneille joista toiminta todella on riippuvainen.
4B: Sopimuksissa on vaatimukset toiminnan jatkuvuuden hallinnalle ja tiedon turvaamiselle sekä niiden toteuttamiselle.	Ellei näistä asioista ole sovittu selkeästi esim. palvelutasosopimuksessa (SLA), ne eivät todennäköisesti toteudu käytännössä.

KUMPPANUUDET JA RESURSSIT: TOIMINNAN VARMISTAMINEN ERITYISTILANTEISSA	
Yleisvaatimus	Yleisvaatimuksen perusta
4C: Kriittisen toiminnan jatkuvuuden ja tiedon turvaamisen hallintavelvoite on ulotettu keskeiseen toimittajaverkostoon.	Ei riitä että palvelua tuottavan ketjun yksittäinen osa huolehtii jatkuvuuden varmistamisesta, sillä ketju on vain niin vahva kuin sen heikoin lenkki.
4D: Yhteistoiminta kumppanien kanssa häiriö- ja erityistilanteiden hallitsemiseksi on organisoitu ja vastuutettu.	Organisaatiorajat ylittävä yhteistoiminta voi olla vaikeaa jo normaalioloissa – tiukan paikan tullen pitää pystyä toimimaan nopeasti eikä yhteistyön ongelmiin ole varaa.

Vaatimukset 4A, 4B, 4C ja 4D ovat SOPIVA-suosituksia 24, 25, 26 ja 27.

Tarkemmat kumppanuusverkostolle asetettavat vaatimukset ovat liitteessä 2.4.

[1] Palvelutuotannosta vastaava ja sopimuksen tekevä organisaatio.

2.5 Prosessit: ICT-jatkuvuuden hallinta

Jatkuvuudenhallinnan keinoina kehitetään ja ylläpidetään toiminta- ja toipumismenettelyjä sekä tarvittavia teknisiä ratkaisuja häiriö- ja erityistilanteiden hallitsemiseksi.

ICT-JATKUVUUDEN HALLINTA : ICT-JOHTAMINEN	
Yleisvaatimus	Yleisvaatimuksen perusta
5A: ICT-hankkeen jokaisessa vaiheessa sekä sen johtamisessa otetaan huomioon keskeiset jatkuvuuden tekijät.	Mitä aikaisemmassa elinkaaren vaiheessa nämä huomioidaan, sitä kustannustehokkaammaksi se tulee. Yksikin huono päätös missä tahansa vaiheessa voi vaarantaa toiminnan jatkuvuuden ja tiedon turvaamisen.
5B: Tietojärjestelmäkehityksessä ja -hankinnoissa huomioidaan tietoturva- ja jatkuvuusvaatimukset.	Turvallisten ja toimintavarmojen järjestelmien kehittäminen tai hankkiminen on kustannustehokkaampaa ja tuottavampaa kuin järjestelmien korjailu jälkikäteen.

ICT-JATKUVUUDEN HALLINTA : TIETOJENKÄSITTELY-YMPÄRISTÖN HALLINTA	
Yleisvaatimus	Yleisvaatimuksen perusta
5C: Ydintoimintojen palvelutuotanto ja hallinnan prosessit on varmistettu ja niillä on varamenettelyt.	Varmistusten ja varamenettelyjen avulla minimoidaan katkot ja yllättävät lisäkustannukset erilaisissa häiriö- ja erityistilanteissa sekä mahdollistetaan palvelujen nopea toipuminen.
5D: Kriittisten toimintojen vaatimat tietoaineistot on turvattu häiriö- ja erityistilanteissa.	Perusrekisterien ja muiden toiminnan kannalta välttämättömien tietoaineistojen suojaamiseen tulee kiinnittää erityistä huomiota, koska niiden uudelleenluonti ei ole kohtuullisin ponnistuksin mahdollista.
5E: Tietoturvallisuuden ja jatkuvuudenhallinnan tilasta tiedotetaan ja raportoidaan yhteistyö- ja palveluketjussa.	Eri tahot/roolit tarvitsevat tietoa heille sopivassa muodossa tilanteen hahmottamiseksi ja kehittämistoimia koskevan päätöksenteon perustaksi.

ICT-JATKUVUUDEN HALLINTA : TIETOJENKÄSITTELY-YMPÄRISTÖN HALLINTA	
Yleisvaatimus	Yleisvaatimuksen perusta
5F: Organisaation vastuulla oleva ICT-kokonaisuus on tunnistettu ja sen hallinta järjestetty.	Sellaisen omaisuuden suojaamisesta ei voi huolehtia, jonka olemassaolosta ei ole tietoinen.
5G: Tietojenkäsittely-ympäristöt otetaan käyttöön, päivitetään ja poistetaan käytöstä hallitusti.	Huolimattomasti ja suunnittelematta tehdyt muutokset aiheuttavat usein toimintahäiriöitä, tietojen katoamista ja tietoturva-aukkoja.

ICT-JATKUVUUDEN HALLINTA : TIEDON TURVAAMINEN	
Yleisvaatimus	Yleisvaatimuksen perusta
5H: Tietoverkkojen eriyttämisellä ja suodatuksella rajataan turva-alueiden välistä liikennettä.	Verkkoliikenteen suodatus torjuu osan verkkohyökkäyksistä. Turva-alueiden avulla voidaan myös rajoittaa ongelmien leviämistä organisaation sisällä.
5I: Pääsynvalvonnalla varmistetaan, että tietoon pääsevät käsiksi vain valtuutetut käyttäjät.	Oikein määritellyt käyttövaltuudet parantavat toiminnan tehokkuutta. Liian laajat käyttövaltuudet lisäävät riskiä että tietoa käytetään luvatta tai joku muuttaa tai tuhoaa tietoa vahingossa.
5J: Käyttäjätunnukset ja käyttövaltuudet ovat yhdistettävissä niitä käyttävään henkilöön tai rooliin.	Tavoitteena on, että väärinkäytöstilanteessa tekijä voidaan jäljittää. Tieto jäljitysmahdollisuudesta ennaltaehkäisee väärinkäytöksiä.
5K: Organisaation ICT-ratkaisut on suojattu haittaohjelmilta.	Kattava ja ajantasainen haittaohjelmien torjuntajärjestelmä on välttämätön yleisimmiltä hyökkäyksiltä suojautumiseksi.
5L: Turvallisuusriskien realisoituminen estetään käyttämällä fyysisen turvallisuuden menetelmiä ICT-ympäristön suojaamiseen.	Sähköisten hyökkäysten lisäksi järjestelmät tulee suojata mm. vesivahingoilta ja ilkivallalta.
5M: Varmuuskopioinnilla estetään tiedon katoaminen organisaatiosta ja vähennetään erilaisten häiriötilanteiden vaikutusta organisaation toimintaan.	Tieto voi tuhoutua esim. laiterikon tai inhimillisen virheen vuoksi, ellei siitä ole kopioita eri paikoissa. Ajantasaiset suojakopiot mahdollistavat nopean palautumisen järjestelmän rikkouduttua tai tuhouduttua.

ICT-JATKUVUUDEN HALLINTA : HÄIRIÖTILANTEIDEN HALLINTA	
Yleisvaatimus	Yleisvaatimuksen perusta
5N: Tapahtumien valvonnalla havaitaan tietoturvapoikkeamat ja mahdollistetaan niiden selvittäminen.	Tietoturvapoikkeamien nopealla havaitsemisella ja reagoinnilla pienennetään aiheutuvia haittavaikutuksia ja kustannuksia.
5O: Tietojärjestelmiä kohtaaviin häiriöihin on varauduttu nopean palautumisen varmistamiseksi.	Moni toipumista nopeuttava toimenpide vaatii ennakkovalmisteluja, joiden puuttuminen aiheuttaa merkittävästi lisätyötä ja kustannuksia.

Vaatimukseen 5B on yhdistetty SOPIVA-suositukset 2 ja 10.

Tarkemmat ICT-jatkuvuudelle asetettavat vaatimukset ovat liitteessä 2.5.

2.6 Mittaaminen

Jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen toteutumista ja tuloksellisuutta on seurattava säännöllisesti erilaisten arviointien avulla. Arviointeja voidaan joko tehdä itse tai antaa ulkopuolisen toteutettavaksi.

Mittaaminen, raportointi ja auditointi tuottavat johtamiselle, strategioille ja toiminnan suunnittelulle perusteita toiminnan kehittämiseksi. Perustason vaatimusten mukaisen seurannan toteuttamisen kustannukset sisältyvät normaaliin toimintakyvyn kehittämiseen.

MITTAAMINEN	
Yleisvaatimus	Yleisvaatimuksen perusta
6A: Jatkuvuuden hallinnan ja tiedon turvaamisen toteutumista ja tarkoituksenmukaisuutta seurataan ja arvioidaan.	Mittarit auttavat kuvaamaan kehitystä ja luovat pohjaa päätöksenteolle. Seuranta ja arviointi on tärkeää, jotta mahdolliset puutteet havaitaan ja niihin voidaan puuttua ajoissa.

Vaatimus 6A on SOPIVA-suositus 28.

Tarkemmat mittaamiselle asetettavat vaatimukset ovat liitteessä 2.6.

LIITTEET:

Liite 1: Keskeiset termit ja lyhenteet
Liite 2: Vaatimuskortit
Liite 2.1: Johtajuus
Liite 2.2: Strategiat ja toiminnan suunnittelu
Liite 2.3: Henkilöstö
Liite 2.4: Kumppanit ja resurssit
Liite 2.5: Prosessit: ICT-jatkuvuuden hallinta
Liite 2.6: Mittaaminen

LIITE 1: KÄYTETYT KESKEISET TERMIT JA LYHENTEET

Arviointi	Arviointi on tilanteen tarkastelua arvioitsijan omasta näkökulmasta, lähtökohtaisesti subjektiivista toimintaa. Toiminta ei perustu vertailuun mihinkään ennalta asetettuun kriteeriin. Jos tällainen kuitenkin on, toiminta lähestyy auditointia.
Auditointi	Valmiussuunnittelun auditoinnilla tarkoitetaan tärkeimpien yritysten valmiussuunnitelmien läpikäymistä niin, että riskikartoituksessa huomioidaan myös ns. yhteiskunnalliset uhkatekijät (esim. laajalla alueella vaikuttava sähkönjakeluhäiriö). Keskustelun kautta pyritään löytämään yrityksen kannalta sopivat varmennustoimenpiteet. - *HVK*
BCMS	Business Continuity Management System. Liiketoiminnan jatkuvuuden hallintajärjestelmä.
BS	British Standard. Esimerkiksi BS 25999 – Business Continuity Management, on jatkuvuudenhallinnan standardi.
CERT-FI	CERT-FI on Viestintävirastossa toimiva kansallinen tietoturvaviranomainen, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen.
CIS	Center for Internet Security. Voittoa tavoittelematon yhteisö, joka tukee neuvontatoiminnallaan turvallisten tietojärjestelmien rakentamista.
Eheys	1) (tietojen tai tietojärjestelmän) aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus 2) ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta – *VAHTI*
Elintärkeä toiminto	Yhteiskunnan toiminnalle välttämätön toimintokokonaisuus. Elintärkeiden toimintojen turvaamisella osaltaan ylläpidetään valtiollinen itsenäisyys, yhteiskunnan turvallisuus sekä väestön elinmahdollisuudet. Elintärkeitä asioita uhkaavat vaarat esitetään YETTS:ssä uhkamalleina. - *YETTS*
eVARE	Valtionhallinnon ICT-varautumisen kehittämis- ja koordinointihanke. - *VM*
HALTIK	Hallinnon tietotekniikkakeskus HALTIK tuottaa sisäasiainministeriön hallinnonalalle tieto- ja viestintäteknisiä palveluita.
Huoltoikkuna	Etukäteen varattu mahdollinen katko laitteen tai järjestelmän palvelun käytettävyydessä, esim. kuukauden ensimmäinen sunnuntai klo 02.00-04.00. Huoltoikkunan aikanakin palvelu/laite saattaa olla käytettävissä mutta saatavuutta ei taata.
Huoltovarmuuskeskus HVK	Huoltovarmuuskeskus (HVK), engl. National Emergency Supply Agency (NESA), on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuuskeskuksen toimintaa johtaa sen hallitus.
HUOVI	Huoltovarmuuskeskuksen hanke yritysten varautumistilanteen kartoittamiseksi -*HVK*.
Häiriötilanne	1) tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti 2) toiminnan jonkin osatekijän haitallinen vaihtelu, josta huolimatta toiminta voi silti pääosin jatkua -*HVK, VAHTI*
ICT	Information and Communications Technology, Informaatio ja Kommunikaatiotekniikka. Yleiskäsite tietohallinnolle ja tietotekniikalle.
IDS	Intrusion Detection System. Tunkeutumisen havainnointijärjestelmä
IEC	International Electrotechnical Commission, standardointi-organisaatio

IPS	Intrusion Prevention System. Tunkeutumisen estojärjestelmä
ISO	International Organization for Standardization, standardointi-organisaatio. ISO/IEC 27001 on tietoturvallisuuden hallintajärjestelmän (ISMS) vaatimusmäärittely, jota vastaan tietoturvallisuuden sertifiointi toteutetaan. ISO/IEC 27002 on tietoturvallisuuden hallintajärjestelmän (ISMS) rakentamisen hyvät käytännöt esittävä standardi.
ITIL	Information Technology Infrastructure Library. ITIL-malli on prosessikeskeinen laadunhallintakehikko, joka soveltuu kaikenkokoisten organisaatioiden jatkuvien IT-palvelujen tuottamisen ja osin johtamisen prosessikehykseksi. - *VAHTI*
Jatkuvuuden hallinta	Jatkuvuuden hallinnalla tarkoitetaan kaikkia toimia, joiden päämääränä on toiminnan jatkuvuus. Jatkuvuuden hallinnan tärkein osa on jatkuvuussuunnittelu. Jatkuvuuden hallinta on organisaation ylimmän johdon hyväksymää strategista ja taktista toimintaa, jolla organisaatio varautuu hallitsemaan toimintaa häiritsevät tilanteet jatkaakseen toimintaa hyväksyttävällä ennalta määritellyllä tasolla.
Jatkuvuussuunnittelu	Toiminnan jatkuvuussuunnittelulla (varautumissuunnittelulla) tarkoitetaan varautumista toiminnan keskeytyksiin siten, että organisaatio pystyy jatkamaan toimintaansa ja rajoittamaan haittavaikutuksia erilaisissa toimintaa kohtaavissa häiriötilanteissa. -*VAHTI*
JHS	Julkisen Hallinnon Suositukset. JHS-järjestelmän mukaiset suositukset koskevat valtion- ja kunnallishallinnon tietohallintoa.
JIT	Julkisten IT-hankintojen yleiset sopimusehdot
Jäännösriski	Kaikkien varautumistoimenpiteiden jälkeen jäävä tiedostettu ja hyväksytty riski.
Kiistämättömyys	Tietoverkossa eri menetelmin saatava varmuus siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi – *VAHTI*
Kirjausketju	Alkutositteiden, syöttötietojen ja tulosteiden aukoton ketju, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet.
Koventaminen	Järjestelmän asetusten muuttaminen niin, että järjestelmän tietoturvallisuuden tekninen taso paranee.
Kriittinen	Ydintoimintoja tukevat ICT-rakenteet, jotka ovat välttämättömiä YETTS:n mukaisen erityistilanteen hoitamisessa ja joiden toimimattomuus estää usean keskeisen organisaation, järjestelmän tai palvelun toiminnan. Kriittisyyttä tarkastellaan yhteiskunnan, valtionhallinnon, hallinnonalan ja viraston näkökulmista.
Käytettävyys	Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla – *VAHTI*
Käyttäjähallinta	Käyttäjähallinta koostuu käytännöistä ja prosesseista, työkaluista, sopimuksista sekä valvonnasta. Käyttäjähallinta määrittelee, miten, kenelle, missä tapauksissa ja millä ehdoilla ICT-järjestelmien ja –palvelujen käyttöoikeuksia luodaan, ylläpidetään ja poistetaan.
Käyttöpalvelu	Käyttöpalvelut kattavat muun muassa palvelujen ja sovellusten ylläpidon ja päivitykset, tietojen varmennus- ja palautuspalvelut, valvonnan ja viankorjauksen sekä tietoturvavalvonnan ja häiriötilanteiden hallinnan.
Luottamuksellisuus	1) tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta 2) se, missä määrin luottamuksellisuutta pidetään tärkeänä – *VAHTI*
NFPA	National Fire Protection Association. Kansainvälinen palontorjuntayhteisö,

	joka neuvoo ja opastaa palontorjunta-asioissa.
Osaaminen	Organisaation tehtävänsä suorittamiseksi tarvitsema voimavara. Organisaatiossa oleva osaaminen rakentuu muun muassa henkilöstön ammattitaidosta ja kokemuksesta, osaamista tukevasta dokumentaatiosta ja tapahtumatiedosta sekä muista osaamista tukevista palveluista ja järjestelmistä. Organisaatio käyttää yleensä oman osaamisensa lisäksi ulkoisia osaamisresursseja.
Palautuminen	Toimintakyvyn palautuminen häiriötilanteen tai seisokin jälkeen. Vrt. toipuminen – *VAHTI*
Palveluketju	Sellaisten palvelujen joukko, jotka ovat välttämättömiä asiakkaan saaman palvelun tuottamiselle
Palvelutasosopimus	Palvelutasosopimus eli SLA (Service Level Agreement) on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. Sitä mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio.
Palveluverkosto	Palvelutuottajien ja palvelujen kokonaisuus, jossa palvelut ovat kytkeytyneet välttämättöminä resursseina toisiinsa.
Poikkeusolot	1) Poikkeusoloilla tarkoitetaan kansainvälisestä tilanteesta, suuronnetto-muudesta tai muista vastaavista syistä johtuvaa vakavaa vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle. -HVK 2) Turvallisuustilanne, jonka hallitseminen ei ole mahdollista viranomaisten säännönmukaisin toimivaltuuksin ja resurssein. -*VVS*
PTS	Puolustustaloudellinen Suunnittelukunta, 2008 lopetettu huoltovarmuuden suunnitteluorganisaatio
PVJJK	Puolustusvoimien johtamisjärjestelmäkeskus.
Riskienhallinta	Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa. Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, -V*AHTI*
RTF	Rich Text Format. Tekstitiedostomuoto.
Service Desk, Help Desk	Palvelupiste, tukikeskus. Yleensä keskitetty yhteydenottopiste, jonka tehtävänä on ottaa vastaan asiakkaan palvelupyynnöt ja käynnistää näiden käsittely.
SLA - Service Level Agreement, palvelutasosopimus	Sopimus IT-palvelutuottajan ja asiakkaan välillä tietyn IT-palvelun sisällöstä ja sen palvelutasosta (=palvelutasotavoite). SLA kuvaa IT-palvelun, dokumentoi palvelutasotavoitteet ja yksilöi IT-palvelutuottajan ja asiakkaan vastuut. - *JHS*
SOPIVA	Sopimuksiin perustuva varautuminen, Huoltovarmuuskeskuksen elektroniikka-, tietoyhteiskunta- ja tietotekniikkapoolien varautumiseen liittyvä nelivaiheinen hanke vuosina 2006 – 2009.
STO II	Sisäisen turvallisuuden ohjelma 2. Hallituksen periaatepäätös, jossa määritetään poikkihallinnollisesti sisäisen turvallisuuden kehittämisen painopisteet, tavoitteet ja toimenpiteet.
Suojakopio	Turvalliseen paikkaan sijoitettu varmuuskopio, joka on käytettävissä, jos alkuperäistä tiedostoa tai varmuuskopiota ei voida käyttää. Suojakopio on tyypillisesti pitkäaikaistalletukseen soveltuva järjestelmän täysvarmistus. -*VAHTI*
TELA	Työeläkevakuuttajat Ry.
TIETO-harjoitus	Kahden vuoden välein järjestettävä tietotekniikka-alan keskeinen

	valmiusharjoitus. Harjoituksen päämääränä on tehostaa viranomaisten ja hallinnon yhteistyökykyä tietojärjestelmiin kohdistuvien ongelmien hoitamisessa.
Tietojärjestelmä information system	1) Ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi 2) abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.
Tietoturvapoikkeama	Tahallinen tai tahaton olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palveluiden eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyys on tai saattaa olla vaarantunut. ISO 27001 –standardissa tästä tilanteesta puolestaan käytetään nimitystä tietoturvatapahtuma ja poikkeama-termillä käsitetään eroa ISO27001-hallintajärjestelmän vaatimuksiin (engl. nonconformity).
Toimintaympäristö	Se toiminnallinen ympäristö, jossa organisaatio toteuttaa tehtäväänsä. Tietoturvatasojen näkökulmasta tällä tarkoitetaan paitsi fyysistä ympäristöä (esim. rakennukset eri toimipisteissä), myös loogista toiminnallisen ympäristön jaottelua. Jälkimmäisestä loogisesta jaottelusta ovat esimerkkeinä organisaation sisäisten osastorajojen tai tietojärjestelmän elinkaaren (kehitys, testaus, tuotanto) mukaiset ympäristöt. Tarkoitus on tunnistaa erilaiset ympäristöt, jotta niiden erilaiset tietoturvallisuuspiirteet ja -vaatimukset voidaan ottaa huomioon.
Toipuminen	1) toimintakyvyn palautuminen kriisin, häiriö- tai erityistilanteen tai poikkeusolojen jälkeen -*VVS* 2) toimet ja hankkeet joiden tarkoituksena mahdollistaa toiminnan paluu hyväksyttävälle tasolle. (Activities and programs designed to return conditions to a level that is acceptable to the entity). *NFPA1600*
TTS	Toiminta- ja taloussuunnitelma. Keskipitkän aikavälin vuosittain päivitettävä toiminnan ja talouden suunnitelma, joka muodostaa perustan valtionhallinnon suunnittelulle ja vuosittaiselle budjetille.
TTT	Tietoturvatasot (TTT) tarjoaa yhteisen käsitemallin tietoturvallisuudelle. Tasojen avulla voidaan asettaa tietoturvallisuuden hallinnalle ja kehittämiselle mitattavat tavoitteet (mittarit). Valtion IT-strategian mukainen kärkihanke. -*VM*
Tuki-infrastruktuuri	Palvelun tuottamiseen tarvittavat tukitoiminnot (esimerkiksi vartiointi, huoltotoiminta, tilat, valvomotoiminta), joita ilman kyseistä ydintoimintaa ei voida tehdä tai suorittaa.
Turvallisuustilanne	Uhkan tasosta johtuva ajallinen yhteiskunnan tila, joka jakautuu normaalioloihin, häiriötilaan ja poikkeusoloihin. Normaaliolot on jokapäiväinen tila, jossa esiintyvät uhkat voidaan ehkäistä ennalta, torjua ja niiden vaikutuksista toipua olemassa olevilla säädöksillä ja voimavaroilla. Normaaliolojen järjestelyt luovat perustan toiminnalle häiriötilassa ja poikkeusoloissa. Häiriötila on normaalioloissa tapahtuva poikkeava, äkillinen turvallisuustilan muutos, joka aiheuttaa vaaraa yhteiskunnan toimivuudelle ja väestön turvallisuudelle. Tilanne edellyttää valtionjohdon ja viranomaisten erityisiä toimia. Normaaliolojen häiriötila saattaa edellyttää myös säädösten tarkistamista. Poikkeusoloja ovat valmiuslaissa ja puolustustilalaissa tilanteet, joiden hallitseminen ei ole mahdollista säännönmukaisin toimivaltuuksin tai voimavaroin. - *YETTS*
Uhkamalli	Uhkamalli tarkoittaa yleisellä tasolla olevaa kuvausta turvallisuusympäristön häiriöistä, jotka toteutuessaan voivat vaarantaa turvallisuuden. -*YETTS*
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä - *VAHTI*
VALHA	Valtionhallinnon säännöllisesti järjestämä laaja valmiusharjoitus.

Valmiuslainsäädäntö	Lainsäädäntö, jolla säädellään poikkeusoloihin varautumista ja viranomaisten erityistoimivaltuuksien käyttöä laissa määritellyissä poikkeusoloissa. -*YETTS ja Puolustusvoimien Kenttäohjesääntö, yleinen osa*
Valmiuslaki	Laki (1080/1991), joka määrittelee poikkeusolot ja viranomaisten erityistoimivaltuudet poikkeusoloissa.
Valmiuspäällikkö	Organisaation varautumisasioista vastaava henkilö. -*HVK*
VAP-varaus	Henkilö, joka on vapautettu työtehtävänsä vuoksi aseellisesta palvelusta sodan aikana.
Varautuminen	Laaja käsite, jonka osa-alueita ovat muun muassa uhka-arvio, riskienhallinta, suojaamistoimet ja jatkuvuuden hallinta, häiriötilanteiden hallinta, valmius, palautuminen ja toipuminen -*HVK*
VARE	Valtion ICT-varautumisen jo päättynyt esitutkimusselvityshanke. Yleisnimitys VM:n koordinoimalle valtionhallinnon ICT-varautumiselle.
VIP	Valtion IT-palvelukeskus
VIRTU	Virkamiehen tunnistaminen, tietoturvahanke
VITKO	Valtion IT-koordinaatioryhmä, ministeriöiden tietohallintojohdosta koostuva yhteistoimintaryhmä
YETTS	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETT-strategia). Valtioneuvoston periaatepäätöksessä määritetään yhteiskunnan elintärkeät toiminnot sekä asetetaan niiden turvaamiselle tavoitetila ja kehittämislinjaukset. Linjaukset ohjaavat hallinnonaloja niiden vastuulla olevien strategisten tehtävien hoitamisessa kaikissa turvallisuustilanteissa. Yhteiskunnan elintärkeiden toimintojen turvaamista johtaa, valvoo ja sovittaa yhteen valtioneuvosto sekä toimivaltainen ministeriö hallinnonalallaan. -*Puolustushallinnon keskeisiä käsitteitä.*

Sanasto on koottu seuraavista lähteistä (esitetty pätemisjärjestyksessä):

1. YETT, Yhteiskunnan elintärkeidentoimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 23.11.2006 (http://www.yett.fi/content/common/yett_strategiadokumentti.pdf)
2. ICT-Varautumisen käsitteitä ja määritelmiä. Varautumisen esitutkimus. (www.vm.fi/varautuminen)
3. HVK, Huoltovarmuuskeskuksen sanasto (http://www.huoltovarmuus.fi/sanasto/)
4. SOPIVA, Sopimuksiin perustuva varautuminen (http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf)
5. TTT Tietoturvatasot, Käsikirjan liite 3, Sanasto
6. Valtionhallinnon tietoturvasanasto VAHTI 08/2008 (www.vm.fi/vahti)
7. VVS Varautumisen ja väestönsuojelun sanasto, Tekniikan sanastokeskus, 2007

ICT-varautumiseen keskeisesti liittyviä käsitteitä ja määritelmiä löytyy seuraavista julkaisuista:

- Valtionhallinnon ICT-varautuminen. Esitutkimusraportti 2008 (www.vm.fi/varautuminen)

Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimuskortit

LUONNOS

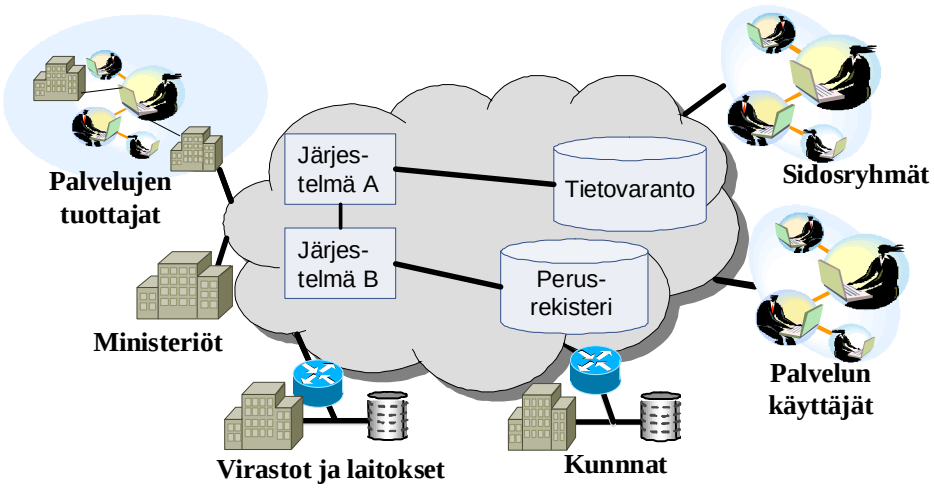
15.12.2009

versio 3.0

JOHDANTO

Yhteiskunnan verkostoitunut toiminta edellyttää kaikilta verkoston osilta yhtenäistä, sovitun tasoista tiedon turvaamista sekä toiminnan ja palvelun jatkamisen kykyä normaaliajan häiriötilanteissa, erityistilanteissa ja poikkeusoloissa.

Palvelujen käyttäjistä ja ylläpitäjistä koostuviin palveluverkostoihin osallistuu hallinnon osapuolia, kansalaisia, yhteisöjä, yrityksiä ja ICT-palveluntuottajia seuraavan kuvan mukaisesti.



Kuva 1. Sähköiset palvelut toteutuvat usean toimijan ja järjestelmän muodostamassa palveluverkostossa.

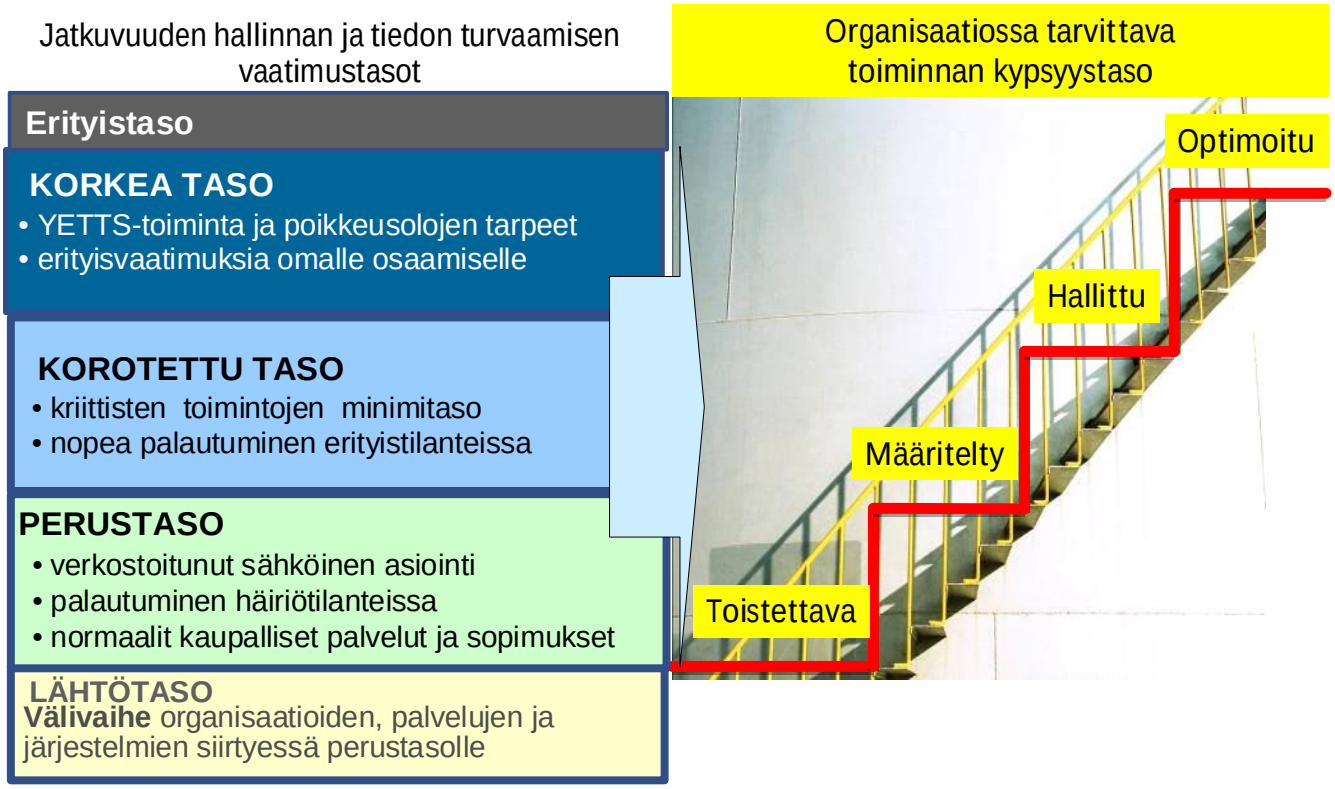
ICT-varautumisen vaatimukset on suunnattu valtion organisaatioille sekä yrityksille, jotka tuottavat valtiolle ICT-palveluja tai ovat huoltovarmuuden kannalta tärkeitä toimittajia. Valtionhallinnossa käytettävien yhtenäisten jatkuvuuden ja tiedon turvaamisen vaatimusten tulee kattaa koko verkostoitunut toimintaprosessi, myös yli hallinnonalarajojen. Keskeistä on varmistua, että koko palveluverkosto kykenee normaaliajan häiriötilanteissa ja YETTS:n mukaisissa erityistilanteissa jatkamaan toimintaansa asetettujen vaatimusten mukaisesti.

Vaatimuksiin on linkitetty SOPIVA:n ja tietoturvatasojen vaatimukset sekä STO II -ohjelman 20.11.2009 valmistunut turvallisuusauditointikriteeristö. Ohjeista ja vaatimuksista muodostuu yksi, toisiaan täydentävä ja tarkentava kokonaisuus.

Vaatimusten jäsentelyssä ja vaatimustasojen muodostamisessa on otettu huomioon keskeisimmät jatkuvuuden hallinnan, tietoturvallisuuden ja laadun hallinnan standardit. ICT-varautumisen vaatimukset koostuvat kolmen eri tason vaatimuksista (perustaso, korotettu taso ja korkea taso) sekä näiden kontrolleista ja vaatimuksia tukevista mittareista.

Vaatimukset on ryhmitetty kuuteen osaan. Osissa 1 – 4 on organisaation ja toiminnan kypsyyteen liittyviä vaatimuksia strategisen johtamisen, toiminnan ohjauksen, henkilöstöhallinnon ja kumppanuusverkoston hallinnan näkökulmista. Osa 5 asettaa vaatimuksia erilaisille teknisille järjestelmille, prosesseille ja ratkaisuille. Kuudennessa osassa on esitetty vaatimukset mittaamiselle ja auditoinnille.

Vaatimukset kohdistuvat organisaation toimintaan, palveluihin ja ICT:n toteuttamiseen seuraavan kuvan mukaisesti.



Kuva 2. Vaatimustasot koskevat sekä organisaation toimintaa että palvelujen ja ICT:n toteuttamista.

Kunkin tason saavuttamiseksi on toteutettava kaikki vaaditun tason sekä sitä alempien tasojen vaatimukset. Vaadittua tasoa ylempää voidaan kuitenkin tarvittaessa toteuttaa yksittäisiä vaatimuksia.

Valtionhallinnossa jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen perustason vaatimusten ja kontrollien noudattaminen, arviointi ja raportointi ovat velvoittavia. Osa kontrolleista on luonteeltaan toimintaa ja toteutusta ohjaavia sekä osa selkeästi mitattavia ja raportoitavia.

HUOMAUTUS

Vaatimuskorteissa viitataan TTT- ja SOPIVA-hankkeiden vaatimuksiin

= TTT 1.1: Vaatimus on sama TTT-hankkeen vaatimuksen 1.1:n kanssa.

~ SOPIVA 1: Vaatimus on lähes tai osittain sama SOPIVA-suositus 1:n kanssa.

~ STO I: 304.0: Vaatimusta käsitellään STO II-kriteeristön luvussa 4.4 kohdassa I 304.

Vaatimuskorteissa toistuva ISO/IEC 27002 on Tietoturvallisuuden hallintajärjestelmää käsittelevä kansainvälinen standardi. BS 25999/2007 on Jatkuvuudenhallintajärjestelmää käsittelevä kansainvälinen standardi. ISO/IEC 27005 on Tietoturvariskien hallintaa käsittelevä kansainvälinen standardi. Standardit ovat maksullisia.

LIITE 2.1 JOHTAJUUS

JOHTAJUUS: STRATEGINEN OHJAUS	
1 A **Organisaatio on tunnistanut ydintoimintoihin liittyvät jatkuvuuden ja erityistilanteiden hallintaa sekä tiedon turvaamista ohjaavat keskeiset tekijät, velvoitteet ja riippuvuudet.** (~TTT 1.1,=SOPIVA 1)	
Perustaso	1. Organisaatiolla on tiedossa toimintaansa koskeva lainsäädäntö sekä muut normit ja nämä on huomioitu linjauksissa ja toiminnassa. (~TTT 1.1.1) 2. Virastolla on jatkuvuuden hallinnan ja varautumisen huomioiva kehittämisohjelma sekä säännöllisesti päivittyvä toiminnan suunnitteluun kytketty toteuttamissuunnitelma. (~TTT 1.1.5, ~STO I:701.0)
Korotettu taso	3. Organisaatiolla on menettely ulkoisten vaatimusten tunnistamiseksi ja näiden muutosten viemiseksi toiminnan suunnitteluun. 4. Virastolla on valmiussuunnitelmassaan valmius erityistilanteissa esittää ja ottaa käyttöön toimintansa jatkuvuuden edellyttämiä lainsäädännön mahdollistamia erityisvaltuuksia. 5. Organisaatio on tunnistanut ja kuvannut ydintoimintojen riippuvuudet muista toiminnoista, palveluista, järjestelmistä ja toimijoista (=toimintaympäristö).
Korkea taso	6. Organisaatio arvioi ja kehittää järjestelmällisesti ydintoimintojaan ja -prosessejaan sekä näiden välisten riippuvuuksien hallintaa erityistilanteiden hallinnan näkökulmasta.
Tausta-aineisto	Suomen lainsäädäntö • Valmiuslaki (1080/1991) • Laki huoltovarmuuden turvaamisesta (/1390/1992) • Valtioneuvoston päätös huoltovarmuuden tavoitteista (539/2008) Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETTS) 2006 • Uhkamallit, varautumisvelvoitteet Kansallinen turvallisuusauditointikriteeristö • Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2 Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004 • Luku 4.1 Tietoturva-asiat osana tulosohjausprosessia Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 2.4 Kytkeytyminen tulosohjaukseen, vuosikello • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta ISO/IEC 27002 • Luku 15.1.1 Identification of applicable legislation Muut vaatimukset ja määräykset Finanssivalvonnan standardi 4.4b Operatiivisten riskien hallinta • Luku 6.4 Jatkuvuussuunnittelu • Luku 6.5 Varautuminen poikkeusoloihin

Esimerkki

Vaatimus 1: Perustasolla julkishallinnossa huomioidaan lainsäädäntö, hallinnonalan määräykset, hallinnon ohjeet, standardit ja sopimukset sekä mahdolliset kansainväliset velvoitteet. Yrityksissä huomioitavia asioita ovat lainsäädäntö, sopimuksissa määritellyt velvoitteet sekä mahdolliset toimialakohtaiset suositukset.

Viraston toimintaa ohjaava lainsäädäntö ja muut ohjaavat asiakirjat on useimmiten tunnistettu ja listattu tietoturva- ja riskienhallintapolitiikan perusteissa. Vaatimusta täydentävä kriteeri (STO I:108.0).

Virastojen strategioissa, periaatteissa ja toiminnan suunnittelussa on huomioitu valtioneuvostotason ohjausasiakirjoissa asetetut ICT-varautumista ohjaavat linjaukset.

Vaatimus 2: Organisaation tietoturvallisuuden ja jatkuvuuden kehittäminen perustuu riskien arviointiin ja jatkuvan kehittämisen malliin, joka on standardien mukainen lähtökohta. Toiminnan ja talouden suunnitteluprosessin (TTS) kautta seurataan toteutumisen edistymistä ja asetetaan uusia tavoitteita asteittaiselle toiminnan parantamiselle. Vaatimusta täydentävä kriteeri (STO I:104.0) .

Vaatimus 3: Organisaatiolla on vastuutettu toimija (henkilö tai ryhmä), jonka tehtävä on seurata muutoksia ja huolehtia, että muutoksista saatava tieto on organisaation käytettävissä ja muutokset huomioidaan toiminnan suunnittelussa ja kehittämisohjelmissa sekä kirjataan näihin. Johto hyväksyy muutokset ja valvoo, että ne viedään täytäntöön. Vaatimusta täydentävä kriteeri (STO I:101.0).

Vaatimus 4: Virastolla on valmius ottaa käyttöön eli tehdä esityksiä ministeriölle etukäteen valmistelluista tarpeista muuttaa normeja jotka antavat edellytykset organisaation ydintoiminnan turvaamiseksi.

Etukäteen valmistellut esitykset mahdollistavat lainsäädännön kautta tulevat lisävaltuudet toimia erityistilanteissa ja poikkeusoloissa. Normit sitovat palvelun tilaajaa ja velvoitteet ulotetaan sopimuksen kautta palvelun toimittajille. Toimittajien on noudatettava voimassaolevia normeja.

Vaatimus 5: Jatkuvuussuunnittelu edellyttää organisaation ydinprosessien kuvauksen. Riippuvuudet (strategiset kumppanit, oman organisaation tukiprosessit) on tunnistettava ja kuvattava. Kuvaamisessa käytetään organisaation käyttämää kuvausmenetelmää.

Vaatimus 6: Kehittäminen perustuu vuosittaiseen ydintoimintojen prosessien katselmointiin ja toiminnan riskienarviointiin. Katselmoinnin perusteella päätetään, mitä prosesseja asteittain parannetaan toiminnan laadun varmistamiseksi ja jatkuvuudenhallinnan edistämiseksi. Vaatimusta täydentävä kriteeri (STO I:105.0).

Palveluprosessissa on kuvattava vastuiden muutokset toimijalta toiselle, rajapinnat jossa vastuu siirtyy sekä miten vastuun ja tiedon siirto varmistetaan.

JOHTAJUUS: STRATEGINEN OHJAUS	
1 B **Jatkuvuuden hallinnan ja tiedon turvaamisen linjaukset on määritetty ydintoiminnan asettamien vaatimusten perusteella**	
Perustaso	1. Johto on päättänyt linjauksista ja tavoitteista toiminnan jatkuvuudelle, tiedon turvaamiselle ja varautumiselle. (~TTT 1.1.3, ~STO I:101.0) 2. Jatkuvuuden hallinnan vastuut toiminnallisessa ja ICT-johdossa on määritetty.
Korotettu taso	3. Linjaukset, tavoitteet ja resurssit toiminnan jatkuvuudelle, tiedon turvaamiselle ja varautumiselle tarkistetaan toiminnan suunnittelurytmin mukaisesti.
Korkea taso	4. Viraston poikkeusolojen ydintoiminnot ja niiden jatkuvuuden hallinnan toteutustavat on määritelty ja dokumentoitu ja niitä testataan.
Tausta-aineisto	Kansallinen turvallisuusauditointikriteeristö • Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2 Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta • Luku 11 Kuva 12 Toimintojen turvaamisen kokonaisuus Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 2.3 Tietoturvallisuuden johtamis- ja hallintajärjestelmä ja sen kehittäminen • Luku 3.2 Tietoturvatavoitteiden asettaminen ja seuranta Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004 • Luku 4.1 Tietoturva-asiat osana tulosohjausprosessia • Luku 4.2 Tietoturva-asiat organisaation sisäisessä ohjauksessa ISO/IEC 27002 • 14.1.3 Developing and implementing continuity plans including information security • 14.1.4 Business continuity planning framework

Esimerkki

Vaatimus 1: Linjaukset ja tavoitteet on kuvattu esimerkiksi tietoturva- ja riskienhallintapolitiikoissa sekä jatkuvuussuunnitelmassa. Suunnitelmien ja muiden asiakirjojen rungot ovat VAHTI 3/2007 -ohjeen liittessä 1.

Ministeriön johdon linjauksia ovat heidän päätöksensä esimerkiksi toiminnan periaatteista ja tavoitteista. Näiden pohjalta ministeriö antaa hallinnonalalle tarkemmat määräykset ja ohjeet tulosohjauksen avulla. Viraston johto päättää toiminnan linjaukset ja antaa tähän liittyvät ohjeet ja velvoitteet toimialoilleen tulostavoitteina. Vaatimusta täydentävä kriteeri (STO I:101.0)

Myös yrityksissä johto päättää yrityksen yleisistä toiminnan periaatteista ja tavoitteista liiketoiminnan jatkuvuuden ja tiedon turvaamisen suhteen. Linjauspäätöksiä voivat olla esim. hyväksytty tietoturvapolitiikka, riskienhallintapolitiikka ja liiketoiminnan jatkuvuuden strategia. Vaatimusta täydentävä kriteeri (STO I:102.0).

Vaatimus 2: Eri toimijoiden roolit ja vastuut on kuvattu riskienhallinta- ja tietoturvaperiaatteissa ja -ohjeissa sekä viestitetty organisaatiolle.

Vaatimus 3: Viraston johto määrittää jatkuvuuden hallinnan linjaukset riskiarvioinnin pohjalta ja huomioiden toiminnan tavoitteet.

Osavuosiraportoinnin yhteydessä käsitellään kehittämissuunnitelman mukaiset tehdyt toimenpiteet ja niiden vaikuttavuus arvioidaan. Vuosiraportissa on yhteenveto toimenpiteiden vaikuttavuuden arvioista. Kehittämissuunnitelma on viraston johtoryhmän syksyn asialistalla oleva vakioaihe. Esittelijänä toimivat turvallisuusjohto ja tietohallintojohto.

Vaatimus 4: Ydintoiminnot on määritelty strategiassa ja niitä tukevat jatkuvuus- ja valmiussuunnitelmat ovat olemassa. Suunnitelmien toimivuutta testataan säännöllisesti esimerkiksi VALHA- ja muiden varautumisharjoitusten yhteydessä. Erityistilanteiden ja poikkeusolojen raportointi- ja auditointimenettelyt on suunniteltu, ohjeistettu ja harjoiteltu.

JOHTAJUUS: ORGANISOINTI	
1 C **Häiriö- ja erityistilanteiden hallinta on linjattu, organisoitu ja huomioitu ohjausmalleissa** (~TTT 1.5)	
Perustaso	1. Häiriötilanteisiin liittyvä päätöksenteko ja tietoturvapoikkeamien käsittely on ohjeistettu ja vastuutettu. (~TTT 1.5.1) 2. Organisaatiossa on keskeisten palveluiden jatkuvuuden yleisohjeet häiriötilanteiden varalta.
Korotettu taso	3. Toiminta- ja johtamismallit sekä toipumissuunnitelmat todennäköisimmistä häiriö- ja erityistilanteista palautumiseen on määritetty ja ovat otettavissa käyttöön. 4. Erityistilanteiden yhtenäinen perusohjeistus on koulutettu ja ulotettu sopimusvelvoittein palveluverkostoon. 5. Organisaatiorakenteet ja toimintamallit edesauttavat häiriö- ja erityistilanteiden johtamista, hallintaa ja palautumista.
Korkea taso	6. Kriittisten järjestelmien ja palvelujen erityisohjeiden saatavuus erityistilanteissa ja poikkeusoloissa on varmistettu.
Tausta-aineisto	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2006 • Uhkamallit, varautumisvelvoitteet Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Luku 2.2.4: Reagoinnin organisointi ja toimivaltuudet Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta ISO/IEC 27002 • 13.2 Management Of Information Security Incidents And Improvements

Esimerkki

Vaatimus 1: Päätöksenteon vastuut ja valtuudet on sovittu. Sijaisuudet on määritelty ja henkilöstö tietää miten tilannetta johdetaan. On olemassa taho, joka käsittelee tietoturvapoikkeamat. Tietoturvapoikkeamasta ilmoittaminen tehdään vakioidulla lomakkeella tai intranetissä sähköisesti, josta se on helppo liittää riskiraporttiin. Hyödynnetään VAHTI 3/2005 –ohjetta, luku 2.

Vaatimus 2: Yleisohjeet liittyvät esim. tilojen käyttöön (ei päästä rakennukseen), varatilojen käyttöönottoon, etätyön mahdollisuuksien hyödyntämiseen ja tehtävien priorisointiin useiden henkilöiden ollessa poissa työstä. Yleisohjeilla ei tarkoiteta tarkkoja järjestelmäkohtaisia ohjeita ja suunnitelmia.

Vaatimus 3: Jatkuvuussuunnitelmassa on tapahtumamallien kautta kuvattuina tarvittavat toipumisjärjestelyt ja niiden johtaminen. Toipuminen sovitaan palvelukohtaisesti järjestelmän käyttöpalveluntoimittajan kanssa.

Vaatimus 4: Omalle henkilöstölle järjestetään säännöllisesti koulutusta erityistilanteissa toimimisesta. Myös palvelua toimittavan organisaation henkilöstölle on koulutettu palveluun liittyvien turvaohjeiden sisältö. Sopimuksissa on liitteenä turvallisuussopimus, jossa on velvoitteita palvelun turvallisuuden ja saatavuuden suhteen. Turvallisuussopimusmallit ovat VAHTI 3/2007 –ohjeen liitteessä 1.

Vaatimus 5: Organisaatiorakenteiden muodostamisessa on huomioitu YETTS-erityistilanteiden hallinnan asettamat vaatimukset. Turvallisuusjohtajan tai valmiusasioista vastaavan henkilön olisi hyvä kuulua johtoryhmään.

Vaatimus 6: Ohjeet on jaettu avainhenkilöille sähköisesti ja paperilla. Erityisohjeet voivat olla salaisia asiakirjoja ja vain nimettyjen henkilöiden käyttöön tarkoitettuja, mutta niitä tulee säilyttää siten että niihin päästään tarvittaessa käsiksi silloinkin jos varsinaiset toimitilat ja normaalit tietojärjestelmät eivät ole käytössä.

JOHTAJUUS: ORGANISOINTI	
1 D **Jatkuvuuden hallinta ja tiedon turvaaminen on organisoitu ja vastuutettu osaksi normaalia johtamista, toimintaa sekä kumppanuusverkoston hallintaa.** (~SOPIVA 4)	
Perustaso	1. Jatkuvuuden hallinta, tiedon turvaaminen ja varautuminen sisältyvät organisaation tehtäviin ja henkilöiden tehtävänkuvauksiin. (~TTT 1.2.2 & 1.2.3) 2. Jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen johtamisen roolit ja vastuut on määritetty. (~TTT 1.2.1)
Korotettu taso	3. Organisaation johto on määritellyt tehtävien ja resurssien käytön priorisoinnin häiriö- ja erityistilanteissa. 4. Organisaatiossa on määritetty erityistilanteiden hallinnan ja poikkeusolojen toiminnan roolit ja vastuut.
Korkea taso	5. Resurssien lisääminen erityistilanteissa on sovittu.
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Liite 2 Tietoturvavastuut rooleittain Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 2 Tietoturvallisuuden johtamisen malli ISO/IEC 27002 • 6.1.1 Management commitment to information security • 6.1.3 Allocation of information security responsibilities Muut vaatimukset ja määräykset Finanssivalvonta 4.4b, Operatiivisten riskien hallinta • 6.4 Jatkuvuussuunnittelu • 6.5 Varautuminen poikkeusoloihin
Esimerkki	**Vaatimus 1**: Organisaation tehtävät varautumisen osalta määräytyvät mm. valmiuslain perusteella. Organisaatiossa käytetään henkilökohtaisia työnkuvia tai tehtävien roolikuvauksia. Kuvauksia on mallina VAHTI 3/2007 -ohjeen liitteessä 2. **Vaatimus 2**: Johtaminen ei muutu häiriötilanteissa. Organisaation johto tekee päätökset huomioiden ydintehtävän suorittamisen. Jatkuvuuden hallinnan keskeisiä rooleja ovat yleensä organisaation johtoryhmä, valmiuspäällikkö, tietoturvapäällikkö, turvallisuuspuolen riskienhallintapäällikkö, suojelujohtaja, IT-johto ja tietoturva-asiantuntija. **Vaatimus 3**: Jatkuvuussuunnitelmassa on huomioitu tehtävien priorisointi. Suunnitelman liitteenä voi olla tähän liittyvä vuosittain päivitettävä lista. **Vaatimus 4**: Roolit ja vastuut on kuvattu ja tiedotettu. Asiat esitellään perehdyttämiskoulutuksessa ja tiedotetaan sisäisesti esimerkiksi intranetissä ja henkilöstölehdessä. Jatkuvuussuunnittelu on koordinoitu yhteistyössä eri toimintayksikköjen tai toimialojen kanssa. Määriteltyjä resursseja ja rooleja ovat esimerkiksi turvallisuusjohtaja, valmiuspäällikkö, tietoturvapäällikkö, riskienhallintapäällikkö ja turvallisuusasiantuntija. **Vaatimus 5**: Jatkuvuussuunnitelmassa on huomioitua ydintoiminnan tukemiseksi tarvittavat lisähenkilöt organisaation sisällä ja palveluntoimittajilla tai kumppaneilla. Häiriöiden aiheuttamien riskien, niiden vaikutuksien ja kustannuksien seurantaan on nimetty järjestelmä-, palvelu- ja/tai asiakaskohtaiset vastuutahot tukemaan jatkuvuussuunnittelua.

JOHTAMINEN: ORGANISOINTI	
1 E **Jatkuvuuden hallinnalle ja tiedon turvaamiselle on asetettu tavoitteisiin nähden riittävät resurssit** (=TTT 1.2, ~SOPIVA 6)	
Perustaso	1. Tulosohjauksessa on osoitettu tavoitteet ja talousarviossa riittävät resurssit jatkuvuuden hallinnalle, tiedon turvaamiselle ja varautumiselle. (~TTT 1.2.4)
Korotettu taso	2. Jatkuvuuden hallinnan ja tiedon turvaamisen resursointi erityistilanteita ja poikkeusoloja varten on huomioitu viraston budjetissa sekä toiminta- ja taloussuunnittelussa. (~TTT 1.2.6)
Korkea taso	3. Resurssien riittävyys on todennettu.
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Kuva 1 Tulosprisma • Kuva 4 Esimerkki Tietoturvallisuuden vuosikello Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004 • Luku 4 Tietoturva-asiat osana tulosohjausprosessia Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 3 Tietoturvan tavoitteiden kytkeminen resurssiallokointiin ISO/IEC 27002 • 6.1.1 Management commitment to information security
Esimerkki	**Vaatimus 1**: Johto on osana tulosohjausta sekä toiminnan ja talouden suunnittelua päättänyt mikä taso organisaation eri osien jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen tulee saavuttaa tai ylläpitää. Budjetoinnin yhteydessä on varmistettu, että näihin liittyviin tehtäviin on osoitettu henkilö- ja muut resurssit. **Vaatimus 2**: Ministeriö päättää hallinnonalan kehyksen rahoittajana jatkuvuuden hallintaan annettavat mahdolliset lisäresurssit (lisäbudjetti). ICT-varautumisen resurssit varataan TTS-prosessin yhteydessä jatkuvuuden hallinnan kehittämissuunnitelman hyväksymisen myötä. Organisaation johto seuraa jatkuvuuden hallintaan tehtyjen panostusten toteumaa vuosiraportoinnin avulla ja antaa hyväksymänsä riskitason mukaiset tulostavoitteet resursseineen. **Vaatimus 3**: Resurssien tarve on arvioitu YETTS-erityistilanteita vasten. Resurssien riittävyys testataan esim. varautumisharjoituksissa. Kumppanuussopimuksissa varmistetaan, että kriittisten toimintojen ylläpitoon on riittävä määrä henkilöstöä käytettävissä.

JOHTAJUUS: YHTEISTYÖ, VIESTINTÄ JA RAPORTOINTI	
1 F **Jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä** (=TTT 1.3, =SOPIVA 7)	
Perustaso	1. Virastossa on säännöllisesti kokoontuva turvallisuus-, jatkuvuus-, tietoturva-asioita käsittelevä yhteistyöryhmä (vast.). (=TTT 1.3.2) 2. Organisaation johto käsittelee säännöllisesti jatkuvuuden ja tiedon turvaamisen tilannetta, linjauksia ja periaatteita sekä toteutumista ja koordinaatiota. (~TTT 1.3.1)
Korotettu taso	3. Ydintoimintojen palvelujen hallinta häiriö- ja erityistilanteiden varalta suunnitellaan yhdessä tukitoimintojen, keskeisten sidosryhmien ja palveluntuottajien kanssa.
Korkea taso	4. Suunnitelmien toimivuus palveluverkostossa on todennettu.
Tausta-aineisto	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Taulukko 1 Tietoturvatavoitteet ja aika • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta Tietoturvallisuuden hallintajärjestelmän arviointisuositus VAHTI 3/2003 • Liite 6 Arviointityökalu ISO/IEC 27002 • 6.1.2 Information security co-ordination • 6.2 External parties • 14.1.3 Developing and implementing continuity plans including information security
Esimerkki	**Vaatimus 1**: Yhteistyöryhmässä käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia. (~TTT 1.3.5) Yhteistyöryhmä kokoontuu vähintään kolme kertaa vuodessa. (~TTT 1.3.4). Sovitut toimenpiteet kirjataan pöytäkirjaan ja niiden toteutumista seurataan. (~TTT 1.3.6) Palvelun toimittajien kanssa asioita käsitellään esimerkiksi palvelun seurantaryhmässä. **Vaatimus 2**: Jatkuvuus- ja varautumisasioita voidaan suunnitella ja käsitellä yksiköiden johtoryhmissä, palvelujen ohjausryhmissä ja organisaation johtoryhmässä omana asiakohtanaan, esim. yhteistyöryhmän esityksestä. ISO 27001 ja ISO 27002-standardien mukaista tietoturvallisuuden hallintamallia noudattava organisaatio järjestää puolivuosittain johdon katselmointitilaisuuden. **Vaatimus 3**: Keskeisten tukitoimintojen, kuten tietohallinnon, henkilöstöhallinnon ja kiinteistöhuollon edustajat osallistuvat myös organisaation jatkuvuussuunnitteluun. Toimialan henkilöstö osallistuu jatkuvuuden hallinnan käsittelyyn osa-alueensa näkökulmasta. Palveluntuottajien kanssa koordinoidaan vuosittain heidän tilanteensa ja se, miten he toteuttavat turvallisuussopimuksen mukaista jatkuvuudenhallintaa. **Vaatimus 4**: Todentaminen voidaan toteuttaa varautumisharjoituksissa skenaarioharjoittelun avulla.

JOHTAJUUS: YHTEISTYÖ, VIESTINTÄ JA RAPORTOINTI	
1 G **Organisaation johto seuraa jatkuvuuden hallinnan ja tiedon turvaamisen kehittämistä, jatkuvuussuunnittelua sekä toimenpiteiden vaikutuksia ja kustannuksia.** (~TTT 1.6, ~SOPIVA 9)	
Perustaso	1. Organisaation johdolle raportoidaan riskianalyysin perusteella päätettyjen kehittämistoimenpiteiden edistymisestä normaalin raportoinnin osana. (~TTT 1.6.1)
Korotettu taso	2. Organisaation johdolle raportoidaan toimintaympäristön muutosten vaikutuksesta sekä häiriö- ja erityistilanteiden hallintaan liittyvistä kehittämistarpeista ja -toimenpiteistä.
Korkea taso	3. Säännöllinen raportointi johdolle perustuu päätettyihin jatkuvuuden hallinnan mittareihin ja tuloksia hyödynnetään toiminnan kehittämisessä. (~TTT 1.6.5)
Tausta-aineisto	Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 5.6 Esimerkki raportointimenettelyistä ja raportin sisällöstä Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Kuva 1 Tulosprisma • Kuva 4 Esimerkki Tietoturvallisuuden vuosikello ISO/IEC 27002 • 6.2.3 Addressing security in third party agreements • 13.1.1 Reporting information security events • 13.1.2 Reporting security weaknesses
Esimerkki	**Vaatimus 1**: Organisaation johdolle annettava raportti tietoturvallisuuteen ja jatkuvuuden hallintaan liittyvistä kehitystoimista sisältää arvion niiden vaikutuksista organisaatioon kohdistuviin riskeihin. Raportointi toteutetaan organisaation normaalin raportointirytmin mukaisesti, esimerkiksi kerran kuukaudessa. Vuosittainen arvio turvallisuusasioista ja jatkuvuudenhallinnasta tehdään osa-alueittain ja sitä verrataan aiempien vuosien tilanteeseen jotta voidaan seurata muutosta. **Vaatimus 2**: Raportin sisältöön kuuluu tietoa resurssien käytöstä, jatkuvuuden hallinnan ja tiedon turvaamisen tavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyistä toimenpiteistä sekä muista merkittävimmistä tietoturvamuutoksista. (~TTT 1.6.6). Raporttien pohjalta kerätään seurantatietoa koulutuksen ja ohjeistuksen perusteiksi sekä toimintaprosessien muuttamiseksi turvallisemmiksi. **Vaatimus 3**: TTS:ssä sovitut jatkuvuuden hallinnan mittarit ovat käytössä. Valtionhallinnossa suositellaan käytettäväksi mittareita, joilla voidaan tuottaa aineistoa valtionhallinnon seurantakyselyihin.

JOHTAJUUS: YHTEISTYÖ, VIESTINTÄ JA RAPORTOINTI	
1 H **Viestinnän ja raportoinnin vastuut ja toimintamalli keskeisimpien sidosryhmien kanssa on määritetty ja organisoitu** (~TTT 1.4, =SOPIVA 8)	
Perustaso	1. Sisäisen ja ulkoisen kriisiviestinnän periaatteet ja vastuut sekä menetelmät on määritetty.
Korotettu taso	2. Viestintäkäytännöt ja -vastuut sekä varmentavat viestintävälineet ja menetelmät häiriötilanteessa on sovittu. 3. Sidosryhmille viestitään jatkuvuuden hallinnasta ja tietoturvallisuudesta vuosittain tai erikseen sovitulla aikataululla ja tavalla. (~TTT 1.4.3, ~TTT 1.4.4)
Korkea taso	4. Viestintää ja raportointia harjoitellaan ja kehitetään sidosryhmien palautteen perusteella erityistilanteiden ja poikkeusolojen näkökulmasta. (~TTT 1.4.6)
Tausta-aineisto	Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 5.6 Esimerkki raportointimenettelyistä ja raportin sisällöstä Tietoturvapoikkeamatilanteiden hallinta VAHTI 3/2005 • Luku 2.2.6 Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti • Luku 3.8 Sisäinen ja ulkoinen viestintä reagoinnin aikana • Liite 3 Esimerkkejä tiedotteiden sisällön perusrungosta • Liite 4 Poikkeaman dokumentaatioon kirjattavia asioita • Liite 5 Esimerkki poikkeaman dokumentoinnista Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 3.4.4 Viestintä ISO/IEC 27002 • 13 Information security incident management
Esimerkki	**Vaatimus 1**: Organisaatiolla on viestintäperiaatteet ja -ohjeet sisäiseen sekä ulkoiseen tiedottamiseen. Näissä periaatteissa on kuvattu myös kriisiviestinnän toteuttaminen. Viestintävastuut on kuvattu ja -roolit ovat olemassa. Sidosryhmät ja kontaktipisteet, joille organisaatio on vastuussa palvelujen jatkuvuudesta ja tietoturvallisuudesta, on tunnistettu esimerkiksi prosessien kuvaamisen yhteydessä, ja tiedottaminen suunnataan näille tahoille. (~TTT 1.4.1) Viestintä sisältää esimerkiksi pitkät käyttökatkot, suunnitellut korjaustoimenpiteet, haittaohjelmien aiheuttamat katkot tai tarkastustoimet, isojen tietomäärien varmistuksien palautukset jne. **Vaatimus 2**: Varmentavat menetelmät on etukäteen valmisteltu ja kaikki osapuolet ovat näistä tietoisia. Välineiden käyttöä on harjoiteltu. Sähköpostin lisäksi on käytettävissä puhelin, telefax, lähetti tai tapaamisyhteys. **Vaatimus 3**: Keskeisiin sidosryhmiin vaikuttavista palvelujen jatkuvuuden hallinnasta ja tietoturvallisuudesta raportointi sekä poikkeamista tiedottaminen on organisoitu ja vastuutettu. (~TTT 1.4.2) Sidosryhmäraportilla ja häiriötilannetiedotteilla on mallipohjat yhtenäistämään tiedon keräämistä, analysointia ja välittämistä. VAHTI 6/2006-ohjeessa on luvussa 5.6 esimerkki hallinnonalan sisäisestä raportoinnista. Sidosryhmiä ovat esimerkiksi toimintaa ohjaava ministeriö, henkilöstö, hallinnonalan yhteistyöryhmät (esim. VAHTI, VITKO), organisaation toimialat, CERT-FI, jne. **Vaatimus 4**: Viestinnän varamenettelyjä harjoitellaan osana varautumisharjoitustoimintaa. Viestinnän nopeuttamista voidaan auttaa kehittämällä toiminnan rakenteita. Viestinnän onnistumisesta kerätään palautetta osana riskiraportointia.

LIITE 2.2 STRATEGIAT JA TOIMINNAN SUUNNITTELU

STRATEGIAT JA TOIMINNAN SUUNNITTELU: TOIMINNAN SUUNNITTELU RISKIENHALLINNAN AVULLA	
2 A **Organisaation ja toimintaympäristön vuorovaikutus otetaan toiminnassa huomioon.** (~TTT 2.1, =SOPIVA 11)	
Perustaso	1. YETTS:n erityistilanteiden vaikutus tärkeimpiin palveluihin ja tietojen käsittelyyn on tunnistettu ja arvioitu. (~STO I:104.0) 2. Tietojenkäsittelyn toimintaympäristöt ja niihin liittyvät toiminnot sekä niissä käytettävät järjestelmät on tunnistettu. (~TTT 2.1.1)
Korotettu taso	3. Organisaation toiminnan kannalta keskeisistä toimintaympäristöistä sekä niihin liittyvistä palveluista, järjestelmistä ja toimijoista on ajantasainen dokumentaatio. (~TTT 2.1.3, ~STO I:702.0) 4. Organisaation johto käsittelee ja arvioi ydintoimintojen ICT-riippuvuuksia vähintään kerran vuodessa. (~TTT 1.3.3)
Korkea taso	5. Turvallisuus- ja toimintaympäristön muutostilanteet tunnistetaan ja niiden asettamat erityisvaatimukset otetaan toiminnassa huomioon. (~TTT 2.1.5)
Tausta-aineisto	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia YETTS 2006 Viestintä- ja sähkönjakeluverkkojen keskinäiset riippuvuudet, HVK 1/2006 Uhkakuva-analyysi 2005, PTS 2005 Viestintäverkkojen ja viestintäpalveluiden varmistaminen. Opas käyttäjille, PTS 2/2005 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, työryhmämuistio 18.12.2008 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 5.1 Tietoturvallisuuden johtaminen
Esimerkki	**Vaatimus 1**: Organisaation jatkuvuussuunnittelussa on tarkasteltu miten eri tapahtumat vaikuttavat toimintaan ja organisaation tehtävän hoitamiseen, ja miten näihin on suunnitelmassa varauduttu. Tämä edellyttää, että tärkeimpien ICT-palveluiden osalta on olemassa riittävät dokumentaatiot. **Vaatimus 2**: Organisaatio on tunnistanut, että sillä on päätoimipaikka ja mahdollisia alueellisia yksiköitä. Henkilöstö voi myös tehdä etätyötä. Alueelliset yksiköt käsittelevät lupa-asioita, muut toiminnot tapahtuvat päätoimipaikassa. Lupa-asioihin liittyvät tietojärjestelmät on myös sijoitettu alueellisten yksiköiden tiloihin. Päätoimipaikan keskeiset tietojärjestelmät on sijoitettu palvelutoimittajan tiloihin. Tilojen, toimintojen ja järjestelmien tunnistaminen luo pohjan tarkemmalle turvallisuus- ja jatkuvuussuunnittelulle. **Vaatimus 3**: Dokumentaation taso ja tarkkuus on sovittu osapuolten kanssa ja ajantasaisuus varmistetaan vuosittain. Dokumentaation tulee olla niin yksityiskohtaista, että ulkopuolinen auditoija voi muodostaa sen perusteella oikean kuvan vallitsevasta tilanteesta. **Vaatimus 4**: Viraston tilaa ja riippuvuuksia arvioidaan osana TTS-prosessia ja arvioinnin tulosten perusteella sovitaan tarvittavista kehittämistoimista. Riippuvuuksien arviointi on osa viraston riskienhallintaa. **Vaatimus 5**: Hallinnonalan ylin johto (esimerkiksi ministeriö) tekee yleensä arvion tilanteen muuttumisesta ja ohjeistaa valmistaviin toimenpiteisiin ryhtymisen. Näitä tilanteita harjoitellaan esimerkiksi VALHA-harjoituksissa. Turvallisuustilanteen muuttuessa kyseeseen voi esimerkiksi tulla ministeriölle laadittava esitys saada käyttöön joitain valmiuslain mahdollistamia toimivaltuuksia. Keskeisen palvelutoimittajan taloudelliset vaikeudet tai omistajamuutokset voivat edellyttää nopeata reagointia.

STRATEGIAT JA TOIMINNAN SUUNNITTELU: TOIMINNAN SUUNNITTELU RISKIENHALLINNAN AVULLA	
2 B **Riskienhallinnan tulokset ohjaavat jatkuvuuden hallinnan ja tiedon turvaamisen kehittämistä.** (~TTT 2.3, =SOPIVA 13)	
Perustaso	1. Ydintoimintojen ja -prosessien omistajat arvioivat vuosittain ja suurten toiminnallisten muutosten yhteydessä ydintoimintojen tietoturvallisuuteen ja toiminnan jatkuvuuteen liittyviä riskejä. (~TTT 2.3.1,~ TTT 2.3.4 & ~TTT 2.3.7) 2. Johto päättää riskienarvioinnin periaatteista ja arvioinnin perusteella tehtävistä riskien hallinnan toimenpiteistä sekä hyväksyy jäännösriskit. (~TTT 2.3.2 & ~TTT 2.3.3)
Korotettu taso	3. Riskienhallinnan tulosten ja toimenpiteiden vaikuttavuusarvioinnin tuloksena määritetään ja dokumentoidaan jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen toteutustavat häiriö- ja erityistilanteiden varalle. (~TTT 2.3.6, ~STO I:104.0)
Korkea taso	4. Riskejä arvioidaan yhdessä sidosryhmien ja palveluntoimittajien kanssa käyttäen yhteismitallisia riskienhallintamenetelmiä. (~STO I:104.0)
Tausta-aineisto	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003 • Luku 1.3 Johdon rooli riskienhallinnassa • Luku 3 Riskien arvioinnin merkitys ja organisointi • Luku 5 Uhkien määrittely ja tunnistaminen • Luku 6 Riskien suuruuden arviointi • Luku 7 Toimenpiteiden määrittely • Luku 8 Jatkokehitys- ja seurantasuunnitelmat ISO/IEC 27005/2008 Information technology — Security techniques — Information security risk management • Liite B: Identification and valuation of assets and impact assessment • Liite C: Examples of typical threats • Liite D: Vulnerabilities and methods for vulnerability assessment • Liite E: Information security risk assessment approaches ISO/IEC 27002 • 4. Risk assessment and treatment Muut määräykset ja ohjeet Finanssivalvonta 4.4b, Operatiivisten riskien hallinta

Esimerkki

Vaatimus 1: Riskienhallinta valtionhallinnossa on osa TTS-prosessia. Talousarvioasetus edellyttää riskienhallinnan toteuttamista ja arviointia. Riskit käsitellään tunnistamalla uhat, arvioimalla riskien suuruudet, priorisoimalla riskit, määrittelemällä toimenpiteet joilla tunnistetut riskit hallitaan, sekä seuraamalla ja arvioimalla esim. tulosraportoinnin yhteydessä toimenpiteiden riittävyyttä.

Apuna voidaan käyttää: VAHTI 7/2003 –ohjeen liite 2. Saman ohjeen tietoturvauhkien tunnistamisen tarkistuslistoja, liite 3. Potentiaalisten ongelmien analyysi ja liite 4. Esimerkkejä toteutuneista riskeistä.

Riskienhallinnan välineenä voidaan käyttää myös Kaiku-Luotain-työkalua.

Vaatimus 2: Virastolla on johdon hyväksymät riskien arviointiin ja hallintaan liittyvät periaatteet, menetelmä ja ohjeistus. Vaatimusta täydentävät kriteerit (~TTT 2.3.2, ~ TTT 2.3.5 & ~ TTT 2.3.8, ~STO I:104.0).

Suurimmista riskeistä pidetään koko viraston ja palveluverkoston tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan. (=TTT 2.3.9) Jäännösriskien hyväksymisperusteet kirjataan ja niiden kehittymistä seurataan. Vaatimusta täydentävä kriteeri (STO I:104.0).

Vaatimus 3: Riskienhallintatoimenpiteiden tuomat hyödyt riskien pienentämiseksi sekä niiden kustannukset arvioidaan ja toteutettavat toimenpiteet valitaan arvion perusteella. Jatkuvuus-, tietoturva- ja valmiussuunnitelmat päivitetään sisältämään toteutettavaksi valitut toimenpiteet.

Vaatimus 4: Hallinnonalalla on yhtenäiset riskienhallintamenetelmät ja -ohjeet, ja riskienhallintaa kehitetään yhdessä. Palveluntoimittajat osallistuvat tuottamiensa palvelujen riskien arviointiin tai välittävät oman riskianalyysinsä tulokset palvelun asiakkaalle. Palveluntoimittajilla ei kuitenkaan tarvitse olla käytössään täysin samoja riskienhallintavälineitä ja -ohjeita kuin hallinnolla, vaan riittää että osapuolet pystyvät hyödyntämään toistensa tuloksia ja ymmärtävät saadut tulokset samalla tavalla.

STRATEGIAT JA TOIMINNAN SUUNNITTELU: PALVELUIDEN JATKUVUUDEN SUUNNITTELU	
2 C **Toiminnan jatkuvuuden hallinnan ja tiedon turvaamisen toimenpiteet tukevat organisaation ydintoiminnan tavoitteita.** (~TTT 2.2, =SOPIVA 14)	
Perustaso	1. Ydintoimintojen ja -prosessien suojattavat palvelut ja järjestelmät on tunnistettu ja sijoitettu perus-, korotetulle tai korkealle tasolle ydintoimintojen tai -prosessien vaatimusten mukaisesti. (~TTT 2.2.1 & ~TTT 2.2.2, ~STO I:103.0)
Korotettu taso	2. Virasto kykenee priorisoimaan kriittiset palvelut YETTS:n erityistilanteissa muiden palveluiden edelle. 3. Ydintoiminnoista ja -prosesseista on toiminta- ja prosessikuvaukset. (~TTT 2.2.4)
Korkea taso	4. Ydintoimintojen prosessikuvauksiin on liitetty jatkuvuuden hallinnan ja tiedon turvaamisen kannalta oleelliset toimet. (~TTT 2.2.5) 5. Ydintoimintojen tavoitteisiin on liitetty jatkuvuuden hallinnan ja tiedon turvaamisen toteutumista kuvaavia mittareita. (~TTT 2.2.6)
Tausta-aineisto	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2006 • Uhkamallit BS 25999/2007 – Business Continuity Management – Osa 2 • 3.3 Embedding BCM in the Organization's Culture • 4.1 Understanding the Organization ISO/IEC 27002 • 4 Risk assessment and treatment • 14.1.2 Business continuity and risk assessment
Esimerkki	**Vaatimus 1**: Organisaation tulee tunnistaa ydintoimintansa. Ensimmäisessä vaiheessa tulee tunnistaa toiminnot, jotka ovat keskeisiä YETTS:ssä määritettyjen strategisten tehtävien toteuttamisen kannalta. Toisessa vaiheessa on tunnistettava toiminnot, jotka ovat tärkeitä YETTS:ssä kuvattujen erityistilanteiden hoitamisen kannalta. Jatkuvuuden hallinnan ja tiedon turvaamisen tavoitteiden määrittelyssä otetaan huomioon sekä luottamuksellisuus, eheys että saatavuus. (~TTT 2.2.3). **Vaatimus 2:** Organisaation jatkuvuussuunnitelma sisältää periaatteet siitä miten toiminta järjestetään suunnitelmallisesti eri tilanteissa ja miten muutokset toteutetaan. Hankittavien palvelujen aikakriittisyydestä, prioriteeteista ja niiden toteuttamisesta on sovittava myös palvelutoimittajien kanssa. Organisaatio on etukäteen käynyt läpi ja kuvannut tapaukset, joissa tähän tilanteeseen voidaan joutua. Organisaatio tunnistaa palvelun merkityksen toiminnalle. **Vaatimus 3:** Kukin organisaatio voi valita omalle toiminnalleen sopivan kuvaustavan, -välineen ja tarkkuustason. **Vaatimus 4:** Organisaation yksi ydintoiminto on asiointiprosessi. Prosessiin on kuvattu, miten asioijan henkilöllisyys tarkistetaan, miten asiointitietoja säilytetään ja miten tiedot suojataan jos tietoja siirretään toisille viranomaisille. **Vaatimus 5**: Mittarien tulee olla sellaisia, että ne tukevat TTS-raportointia, hallinnossa sovittua tulosohjausta ja VAHTI:n tekemää tietoturvakyselyä valtionhallinnon tietoturvallisuuden kehittymisestä.

STRATEGIAT JA TOIMINNAN SUUNNITTELU: PALVELUIDEN JATKUVUUDEN SUUNNITTELU	
2 D **Erityistilanteiden hallinnan menettelyt on dokumentoitu, koulutettu ja harjoiteltu** (=TTT 2.5 & ~TTT 3.3, =SOPIVA 16+18)	
Perustaso	1. Ydin- ja tukitoimintojen toimintamalleissa ja suunnitelmissa on otettu huomioon erityistilanteissa heikentyvät ICT-palvelut ja -resurssit. 2. Toiminnan jatkuvuuden, tiedon turvaamisen ja varautumisen linjausten päivitys on vastuutettu sekä organisoitu. (~TTT 2.5.2 & ~TTT 2.5.3)
Korotettu taso	3. Kriittisimmille palveluille on laadittu yksityiskohtaiset järjestelmäkohtaiset ohjeet ja koulutettu toiminta avainhenkilöille keskeisimpien häiriötilanteiden varalta. 4. Häiriötilanteiden toimintaohjeita kehitetään häiriö- ja erityistilanteista kerätyn aineiston ja saatujen kokemusten perusteella.
Korkea taso	5. Kriittisten ICT-palvelujen kapasiteetti ja resurssit on varmistettu sovitun minimitarpeen tasolle. 6. Jatkuvuus- ja valmiussuunnitelmia ohjeineen testataan ja harjoitellaan säännöllisesti käytännön tasolla erityistilanteiden ja poikkeusolojen hallitsemiseksi. (~TTT 2.5.4)
Tausta-aineisto	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2006 • Uhkamallit, erityistilanteet Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta • Jatkuvuussuunnitelman runko s. 90 Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, VN periaatepäätös 2006 • Luku 3.3. Ministeriöiden strategiset tehtävät toimintojen turvaamiseksi • Liite 2. Varautuminen erityistilanteisiin ISO/IEC 27002 • 14.1.5 Testing, maintaining and re-assessing business continuity plans BS 25999/2007 – Business Continuity Management – Osa 2 • 4.4 Excercising, maintaining and reviewing BCM arrangements BS 25999/2006 – Business Continuity Management – Osa 1 • Taulukko 1 – Types and methods of exercising BCM strategies

Esimerkki

Vaatimus 1: Organisaatio ymmärtää, että erityistilanteissa käytössä olevien ICT-palveluiden taso heikkenee ja toiminta pitää sopeuttaa siihen esimerkiksi lopettamalla tilapäisesti vähemmän tärkeitä toimintoja. Sopeuttamistoimet on suunniteltu ennalta.

Organisaatiolla on kirjalliset toimintaohjeet mm. sähkökatkon, tietoliikennekatkon, järjestelmävian, keskeistä henkilöstöryhmää tai toimittajaa koskevan lakon, pandemian, tulipalon, myrskyn tai tulvan varalta. YETTS:n erityistilanteiden hallinta perustuu hyvään jatkuvuussuunnitteluun. Jatkuvuussuunnitelmaan on kirjattu käytettävissä oleva henkilöstö, avainhenkilöt ja varahenkilöt sekä arvio heidän saatavuudestaan.

Vaatimus 2: Tietoturva- ja riskienhallintapolitiikan sekä tietoturvan kehittämissuunnitelman päivityksen valmistelu on vastuutettu tietoturvapäällikölle ja jatkuvuussuunnitelman päivityksen valmistelu valmiuspäällikölle. Päivitysrytmiksi on sovittu kerran vuodessa, ja päivitys on vuosikellossa sidottu tehtäväksi riskien arvioinnin ja jatkuvuussuunnitelman testauksen yhteyteen. Vaatimusta täydentävä kriteeri (STO I:104.0).

Vaatimus 3: Organisaation järjestelmäkohtaisissa ohjeistuksissa kuvataan mm. järjestelmän riippuvuudet muista järjestelmistä, kuinka järjestelmä asennetaan uudelleen, kuinka tiedot palautetaan ja kuinka testataan että järjestelmä on saatu jälleen toimimaan normaalisti.

Vaatimus 4: Häiriötilanteen aikana vastuuhenkilö pitää lokia tapahtumien kulusta. Jokainen häiriötilanne käydään jälkikäteen läpi ja pyritään selvittämään miten tapahtuma syntyi, miten se vaikutti ja olisiko tilanteen aiheuttava tekijä voinut aiheuttaa jotain muuta. Lisäksi arvioidaan kuinka henkilöstö hallitsi tilanteen ja onko tarpeen tehdä ohjeistukseen muutoksia tai järjestää koulutusta vastaisuuden varalta.

Vaatimus 5: ICT-palveluita ovat esimerkiksi tietoliikenne- ja käyttöpalvelut, tietoteknisten laitteiden huolto ja järjestelmien kehitystyö sekä muutosten hallinta. ICT-palveluiden tarvitsemat minimitasot määritellään SLA-sopimuksessa tai palvelusta laaditussa jatkuvuus- ja toipumissuunnitelmassa. Minimitasot voidaan asettaa aikavaatimuksina, laitteistoalustana tai tietoliikennekapasiteettina, joka vähintään tarvitaan.

Vaatimus 6: Jatkuvuussuunnitelma on hyvä pöytätestata parin vuoden välein. Mikäli suunnitelma sisältää varatoimipaikkojen käyttöönoton, tulisi tämä harjoitella pöytätestauksen välivuosina henkilöstön kouluttamiseksi ja totuttamiseksi toimimaan häiriötilanteiden aikana.

Korkean tason organisaatio sekä sen keskeiset toimittajat osallistuvat TIETO-harjoituksiin tai soveltavat TIETO-harjoituksien tilannekuvauksia organisaatiokohtaisessa harjoittelussa. Toimintaohjeita kehitetään harjoitusten oppien perusteella.

STRATEGIAT JA TOIMINNAN SUUNNITTELU: PALVELUIDEN JATKUVUUDEN SUUNNITTELU	
2 E **24/7-toiminta ja CERT-FI-yhteistoiminta vastaa organisaation tavoitteita ja velvoitteita**	
Perustaso	1. Organisaatio on järjestänyt CERT-FI:n ilmoitusten vastaanoton. (~STO I:706.0) 2. Organisaatio ilmoittaa CERT-FI:lle vakavista tietoturvaloukkauksista ja niiden epäilyistä. 3. Tarpeet ympärivuorokautiselle palveluiden, järjestelmien ja verkkojen valvonnalle on määritelty.
Korotettu taso	4. CERT-FI ilmoitusten seuranta, sisäinen välitys ja käsittely palveluissa on järjestetty. 5. Organisaatiolla on käytössä laite- ja ohjelmistorekisteri helpottamaan CERT-FI ilmoitusten kohdentamista. 6. Keskeiset palvelut ja niiden edellyttämä ICT ovat tarvittavassa laajuudessa 24/7-valvonnan ja siihen liittyvän raportoinnin piirissä.
Korkea taso	7. Organisaation ydintoiminnoissa on käytössä 24/7-toiminta, joka toimii kiinteässä yhteistyössä CERT-FI:n ja palveluverkoston kanssa.
Tausta-aineisto	CERT-FI -ohjeet Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Luku 2 Tietoturvapoikkeamiin varautuminen • Luku 2.2.6 Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti • Luku 3.8.1 Yhteydenpito omaan verkkopalvelujen tarjoajaan ja CERT-toimijoihin ISO/IEC 27002 • 13 Information security incident management

Esimerkki

Vaatimus 1:Organisaatiossa on määrätty henkilöt, jotka ottavat vastaan CERT-FI:n lähettämiä varoituksia ja ilmoituksia.

Vaatimus 2: Organisaatiolla on ohjeistettu ja koulutettu menettely ilmoituksien tekemiseen. Vakavia tietoturvaloukkauksia ovat mm. henkilötietojen varkaudet sekä laajat palvelunestohyökkäykset.

Vaatimus 3: Ympärivuorokautinen valvonta on tarvepohjaista, ja määriteltävä kullekin kohteelle erikseen. Perustason järjestelmiä ei yleensä tarvitse valvoa ympäri vuorokauden, elleivät ne ole myös ympärivuorokautisessa käytössä. ICT-järjestelmien valvonnan, hallinnan ja ylläpitämisen yhteistoimintamallit keskeisessä palveluntuottajaverkostossa on organisoitu ja sovittu.

Vaatimus 4: Organisaation Service Desk tai Help Desk -palvelu tarkastaa CERT-FI:n sivuilta ajankohtaiset asiat ja ilmoittaa varoituksista tietoturvaryhmälle. Muitakin tietoturvallisuuden tilanteen seurantapalveluita voidaan käyttää. Palveluntoimittajalla on menettely ilmoitusten seurantaan ja niihin reagointiin. Seurantavelvoite ulotetaan sopimuksissa palveluntoimittajiin ko. palvelun kriittisyysluokituksen mukaisesti. Palvelussa voidaan seurata muitakin kuin CERT-FI:n ilmoituksia.

Vaatimus 5: Organisaation Help Desk ylläpitää rekisteriä tai luetteloa toimintaympäristön laitteista ja ohjelmistoista ja vertaa ilmoituksia näihin. Laajemmissa ympäristöissä voidaan rekisterin ylläpitoa helpottamaan käyttää ratkaisua, joka automaattisesti kartoittaa ympäristön laitteet ja ohjelmistot. Palveluntoimittajan kanssa sovitaan seurantavelvoitteesta ja ilmoituksien aiheuttamista toimenpiteistä.

Vaatimus 6: Valvonnan havaitsemiin ongelmiin reagoinnissa voi olla pitempi vaste-aika virka-ajan ulkopuolella, jos itse palvelukin on käytössä vain virka-aikaan. Jotkin palvelut voivat olla aikakriittisiä tiettyyn aikaan vuodesta, jolloin niiden valvonnankin tulee olla ympärivuorokautista, ja muina aikoina voi riittää esim. 12/7 valvonta.

Vaatimus 7: Ympärivuorokautinen valvonta ja uhkiin reagointi voidaan toteuttaa organisaation omin voimin, useiden hallinnon organisaatioiden yhteistyönä, tai palveluntarjoajalta ostettuna palveluna. Kriittisissä ja keskeisissä ympäristöissä on käytössä tunkeutumisenhavaitsemisjärjestelmä.

Palveluverkoston muodostavat esimerkiksi käyttöpalvelun toimittaja ja verkko-operaattori ja näiden alihankkijat, jotka tarvitaan ydintoiminnon tuottamisessa.

LIITE 2.3 HENKILÖSTÖ

HENKILÖSTÖ: OSAAMISEN JA TIETOISUUDEN KEHITTÄMINEN	
3 A **Jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään.** (~TTT 3.1, =SOPIVA 19)	
Perustaso	1. Henkilöstön roolit ja vastuut jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelussa ja toteuttamisessa on määritetty myös häiriötilanteet huomioiden. 2. Tietoturvaohjeet ja -käytännöt sekä niiden muutokset koulutetaan kaikille organisaatiossa toimiville. (~TTT 3.1.3 & ~TTT 3.1.4, ~STO I:204.0)
Korotettu taso	3. Osaamisen johtamisessa seurataan tietoturvallisuuden ja ICT-varautumisen koulutuksien toteutumista. (~TTT 3.1.6 & ~TTT 3.1.8)
Korkea taso	4. Erityistilanteiden ja poikkeusolojen asettamat vaatimukset on otettu huomioon henkilösuunnittelussa, tehtävänkuvauksissa ja koulutuksessa. 5. Palveluverkoston osaamisen varmistaminen ja kehittäminen on organisoitu ja ydintoiminnan kannalta keskeinen osaaminen on kartoitettu. (~TTT 3.2.6)
Tausta-aineisto	Tietoturvakouluttajan opas, VAHTI 11/2006 • Luku 4 Koulutussuunnittelu Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 3.4.3 Koulutus • Kuva 8. Koulutus osana tietoturvallisuuden hallintajärjestelmää • Kuva 9. Koulutus osana organisaation kypsyyttä • Liite 2. Tietoturvavastuut rooleittain Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 6 Henkilöstöturvallisuus • Luku 6.1 Henkilöstön toimenkuvat • Luku 6.2 Henkilöstön soveltuvuus • Luku 6.3 Henkilöstön osaamisen varmistaminen ENISA tietoturvatietoisuusohje • Liitteet 1-4, Tietoturvatietoisuusprojektin suunnittelupohjia • Liite 5: Kansalaisten tietoturvatietoisuuskyselyn pohja ISO/IEC 27002 • 8.1.1 Roles and responsibilities • 8.2.2 Information security awareness, education, and training

Esimerkki

Vaatimus 1: Organisaatiossa on määritelty VAHTI 3/2007 -ohjeen liitteen 2 mukaiset roolitja yleisellä tasolla tehtävän edellyttämä osaaminen.

Vaatimus 2: Perehdytykseen sisältyy varautumiseen, jatkuvuuden hallintaan ja tiedon turvaamiseen liittyvä osuus, jossa käsiteltäviä asioita ovat mm. tietoturvapolitiikan sekä henkilön työtehtävien kannalta tärkeimpien ohjeiden ja jatkuvuuden hallinnan suunnitelmien sisältö. Perehdyttäjällä on käsiteltävistä asioista kirjallinen aineisto. Vaatimusta täydentävät kriteerit (~TTT 3.1.7, ~STO I:204.0).

Muuttuneista ohjeista järjestetään info-tilaisuus sekä tiedotetaan sähköisiä kanavia käyttäen. Henkilöstön koulutuksessa otetaan huomioon myös organisaatiossa ja toiminataympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat. (=TTT 3.1.10) Vaatimusta täydentävä kriteeri (~STO I:204.0).

Vaatimus 3: Perehdytyksen päätteeksi on lyhyt sähköinen testi ja kaikkien perehdytysosuuksien läpikäynti on tulosmittari. Sähköistä testiä käytetään myös muuttuneiden ohjeiden koulutuksen seurantaan.

Vaatimus 4: Henkilöstöä rekrytoitaessa huomioidaan organisaation tarpeet jatkuvuuden ja valmiusasioiden osaamisessa. Kehityskeskusteluissa tai osaamiskartoituksilla selvitetään henkilöstön osaamisen riittävyyttä suhteessa heidän työnkuvaansa. Tarvittavaan koulutukseen varataan suunnitelmallisesti resurssit ja työkuormituksessa huomioidaan henkilöiden koulutuksessa olo.

Vaatimus 5: Hankintojen yhteydessä edellytetään palvelun tuottamiseen osallistuvilta avainhenkilöiltä riittävää osaamista ja sen ylläpitoa. Palveluverkoston osaamista kehitetään yhteisillä harjoituksilla. Osaamiskartoitusten avulla valvotaan osaamistason toteutumista.

HENKILÖSTÖ: OSAAMISEN JA TIETOISUUDEN KEHITTÄMINEN	
3 B **Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia.** (~TTT 3.1, =SOPIVA 20)	
Perustaso	1. Henkilöstön turvallisuustietoisuutta ja motivaatiota kehitetään. (~TTT 3.1.2) 2. Avainhenkilöt ja heidän esimiehensä käsittelevät vuosittain kehityskeskustelun yhteydessä jatkuvuuden hallintaan ja tiedon turvaamiseen liittyviä vastuita ja osaamisen kehittämisen tarpeita. (~TTT 3.1.11)
Korotettu taso	3. Henkilöstö osallistuu häiriö- ja erityistilanteiden vaikutuksien arviointiin ja hallintakeinojen kehittämiseen.
Korkea taso	4. Henkilöstön tietoturvatietoisuuden tasoa ja kehittymistä mitataan. (=TTT 3.1.12)
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 3.4.3 Koulutus • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta • Liite 2 Tietoturvaroolit Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008 • Luku 3. Henkilöstöriskienriskien hallinnan perusteet • Luku 3.5 Keskeiset lainsäädännön velvoitteet • Luku 4. Henkilöstöturvallisuuden järjestelyt virastossa. ISO/IEC 27002 • 8.2.2 Information security awareness, education, and training
Esimerkki	**Vaatimus 1**: Henkilöstölle järjestetään säännöllisesti info-tilaisuuksia joissa käsitellään tietoturvan, jatkuvuuden hallinnan ja varautumisen perusasiat, sekä ajankohtaisia teemoja kuten erilaisten huijausten ja urkinnan (social engineering, phishing) torjumista. Vaatimusta täydentävät kriteerit (~TTT 3.1.2, ~STO I:204.0). Työhyvinvointiohjelman avulla vältetään kuormitusta ja huolehditaan työssä jaksamisen edellytyksistä. Hyvistä tietoturvateoista annetaan positiivista huomiota esimerkiksi palkitsemalla kuukauden tietoturvateosta ja arpomalla palkintoja tietoturvakyselyyn vastanneiden kesken. (~TTT 3.1.13) **Vaatimus 2**: Vastuista ja niihin liittyvistä osaamisen kehittämisen tarpeista keskustellaan osana kehityskeskustelua, tai erikseen jossain muussa yhteydessä. Opiskelua tuetaan ja se huomioidaan koulutussuunnitelmassa. Koulutussuunnitelma mahdollistaa sekä kotimaassa että ulkomailla tapahtuvan osallistumisen alan asiantuntijaseminaareihin. **Vaatimus 3**: Jatkuvuusharjoituksiin ja niiden purkuun sekä jatkotoimenpiteiden suunnitteluun osallistuu edustajia organisaation kaikilta tasoilta. **Vaatimus 4**: Henkilöstölle tehdään säännöllisesti tietoturvakysely, jossa selvitetään, onko koulutus lisännyt ymmärrystä ja tietoisuutta. Organisaatiossa käytetään tietoturvakoulutukseen esimerkiksi tietokoneavusteista koulutuspakettia, joka sisältää myös koulutuksen aiheeseen liittyvän testin ja pitää kirjaa koulutuksen läpikäyneistä sekä heidän testituloksistaan. Hallinnonalan virastojen välillä seurataan turvallisuustietoisuuden tasoa yhdenmukaisella mittaristolla ja tehdään vertailuja pidemmällä ajanjaksolla. Tulosten perusteella kehitetään toimintaa.

HENKILÖSTÖ: OSAAMISEN JA TIETOISUUDEN KEHITTÄMINEN	
3 C **Organisaatiossa on sovittu menettely valvonnalle, sekä turvallisuuspoikkeamissa ja väärinkäytöstilanteissa toimimiseen.** (~TTT 3.1, ~SOPIVA 21)	
Perustaso	1. Sääntöjen noudattamista seurataan ja poikkeamiin puututaan. (=TTT 3.1.5, ~STO I:107.0) 2. Sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuus ja oikea käsittely on ohjeistettu. (~TTT 3.3.1, ~STO I:108.0) 3. Henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapauksista tai niiden uhkista tulee ilmoittaa. (=TTT 3.3.2, ~STO I:107.0) 4. Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu. (=TTT 3.2.5, ~STO P: 404.0)
Korotettu taso	5. Tietoturvapoikkeamien raportointimenettely on kuvattu kirjallisesti ja siihen on määrämuotoinen pohja. (~TTT 1.6.3, ~TTT 1.6.4)
Korkea taso	6. Poikkeusolojen tarpeet ja mahdollisuudet tarvittaessa rajoittaa ja valvoa työntekijän toimintaa (yksityisyyden suojaa) työpaikalla on kartoitettu. 7. Organisaatiossa tai sen tukena on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti. (~TTT 3.3.4)
Tausta-aineisto	Laki yksityisyydensuojasta työelämässä (759/2004) • 6 luku Työnantajalle kuuluvien sähköpostiviestien hakeminen ja avaaminen Sähköisen viestinnän tietosuojalaki (516/2004) • 4 § ja 5 § Viestintäviraston CERT-FI:n ohjeita Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Luku 2.1 Ennaltaehkäisevät toimenpiteet • Luku 3 Reagoiminen poikkeaman ilmettyä Valtionhallinnon sähköpostin käsittelyohje, VAHTI 2/2005 • Liite 2 Sähköpostin käsittelysäännöt • Liite 5 Malli sähköpostilaatikon avauslomakkeeseen ISO/IEC 27002 • 8.2.3 Disciplinary process • 13 Information security incident management

Esimerkki

Vaatimus 1: Riskiraportoinnissa kirjataan tapahtumat ja esimiesten tehtävä on puuttua laiminlyönteihin. Tietoturvamääräysten ja -ohjeiden noudattamatta jättämisen mahdolliset seuraukset on kuvattu tietoturvapolitiikassa ja tiedotettu kaikille organisaatiossa työskenteleville. Vaatimusta täydentävät kriteerit (~TTT 3.1.9, ~STO I:107.0, ~STO I: 108.0).

Vaatimus 2: Tekninen valvonta on käsitelty henkilöstön kanssa YT-menettelyn mukaisesti. (~TTT 3.1.1). Teknistä valvontaa ovat mm. tilojen kameravalvonta, kulunvalvonta, sekä sähköpostiliikenteen ja muun verkkoliikenteen haittaohjelmasuodatus. Valvonnassa ja tietoturvapoikkeamia selvitettäessä tulee noudattaa ”Laki yksityisyydensuojasta työelämässä , 6 luku: Työnantajalle kuuluvien sähköpostiviestien hakeminen ja avaaminen” sekä Sähköisen viestinnän tietosuojalain 4 § ja 5 §.

Valvonta- ja selvitystehtäviä suorittavilla on ohjeet siitä, mitkä ovat heidän lailliset toimintavaltuutensa ja miten rikkomustilanteissa tulee menetellä.

Vaatimus 3: Henkilöstöä on neuvottu ilmoittamaan turvallisuuteen ja jatkuvuuden hallintaan liittyvistä havainnoistaan esimiehelleen tai verkkolomakkeen avulla suoraan aihealueen vastuuhenkilölle. Esimiehet on ohjeistettu ja koulutettu välittämään saamansa tiedot edelleen oikealle vastuuhenkilölle.

Vaatimus 4: Turvallisuusselvitys voidaan tehdä vain, jos organisaatio on sen piirissä. Valtionhallinnon avainhenkilöiden lisäksi kyseeseen tulevat tärkeysluokitellut yritykset ja niiden henkilöstö sen mukaan kuin organisaatio on päättänyt selvityksiä hakea. Tähän vaikuttaa mm. se, mihin tietoon henkilöllä on työssään pääsy. Tarvittaessa tehdään erikseen salassapito- tai vaitiolositoumukset. Vaatimusta täydentävät kriteerit (~STO I:202.0, STO I:204.0).

Vaatimus 5: Tietoturvapoikkeaminen ilmoittaminen on ohjeistettu ja tarvittava aineisto on esimerkiksi organisaation intranetissä. Raportoinnin helpottamiseksi voidaan käyttää valmista lomaketta.

Vaatimus 6: Organisaatio on valmistellut menettelyt esimerkiksi viestiliikenteen rajoittamiseksi.

Vaatimus 7: Ryhmä voi koostua organisaation omasta henkilöstöstä tai voidaan käyttää hallinnonalan tai palveluntarjoajan kokoamaa ryhmää. Poikkeamien selvittely edellyttää riittävän osaamisen sekä teknisesti että laillisesti. Rikosepäilyissä poliisi on tutkiva viranomainen. Tietoturvaryhmän täydennyskoulutus sisältää erilaisten häiriötilanteiden selvittelyn harjoittelua ja yhteistoimintaan poliisin kanssa.

HENKILÖSTÖ: HENKILÖRESURSSIEN JA TEHTÄVIEN HALLINTA	
3 D **Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt suunniteltu.** (~TTT 3.2, =SOPIVA 22)	
Perustaso	1. Avaintehtävät on tunnistettu ja niihin on nimetty varahenkilö tai -henkilöt. (~TTT 3.2.2, = STO I:203.0) 2. Kriittisistä tehtävistä vastuulliset avainhenkilöt on koulutettu toimimaan häiriötilanteissa. (~TTT 3.2.4)
Korotettu taso	3. Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön varajärjestelyt. 4. Avainhenkilöstö harjoittelee säännöllisesti ylläpitämään kriittisiä toimintoja erityistilanteissa.
Korkea taso	5. Kriittisten tehtävien toteuttamisen edellyttämät varajärjestelyt poikkeusoloissa on testattu ja harjoiteltu.
Tausta-aineisto	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 6 Henkilöstöturvallisuus • Luku 6.4 Avainhenkilöstö • Luku 6.7 Sijais- ja väliaikaisjärjestelyt • Luk 6.8 Työnkierto ja lomat Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Liite 2 Tietoturvavastuut rooleittain ISO/IEC 27002 • 10.2 Third Party Service Delivery Management
Esimerkki	**Vaatimus 1**: Varahenkilö voi olla myös organisaation ulkopuolinen henkilö, mutta tällöin asiasta sovittaessa tulee kiinnittää erityistä huomiota varahenkilön kouluttamiseen sekä siihen että varahenkilö on tarvittaessa käytettävissä. **Vaatimus 2**: Järjestelmien asiantuntijoilla on riittävä häiriötilanteiden hallintaan liittyvien ohjeiden osaaminen ja ohjeet ovat helposti saatavilla. Tietoturvapoikkeamia selvittävät henkilöt on nimetty ja koulutettu. (~TTT 3.3.3) **Vaatimus 3**: Vaihtoehtoinen toimintatapa on suunniteltu jatkuvuussuunnitelmassa. **Vaatimus 4**: Organisaatio järjestää vuosittain vähintään pöytätestauksen johonkin erityistilanteeseen liittyvästä skenaariosta. Mikäli mahdollista, avainhenkilöt osallistuvat myös valtionhallinnon yhteisiin harjoituksiin (esim. VALHA, TIETO). **Vaatimus 5**: Testaaminen ja harjoittelu sovitaan organisaation TTS-prosessissa. Avainhenkilöt ja näiden varahenkilöt osallistuvat säännöllisesti häiriö- ja erityistilanteita koskevien tilanteiden harjoitteluun ja heidän toimintakykyään poikkeusoloissa arvioidaan. Harjoituksien tulosten perusteella järjestetään tarvittaessa lisäkoulutusta tai harjoituksia joilla parannetaan kykyä toimia oikein näissä tilanteissa.

HENKILÖSTÖ: HENKILÖRESURSSIEN JA TEHTÄVIEN HALLINTA	
3 E **Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla.** (~TTT 3.2, =SOPIVA 23)	
Perustaso	1. Poikkeusolojen varalle on tehty ja ylläpidetty henkilövaraukset (VAP). 2. Toteutettavaksi valitut jatkuvuuden hallinnan toimenpiteet ja -prosessit on organisoitu ja vastuut on dokumentoitu. (=TTT 3.2.1 & ~TTT 3.2.3)
Korotettu taso	3. Palveluverkoston kriittiset erityisosaamisalueet on kartoitettu ja ne on huomioitu palvelujen hankinnassa ja henkilöstön käytössä sekä muussa resursoinnissa.
Korkea taso	4. Henkilövarauksia (VAP) ylläpidetään myös palveluketjuissa, ja varatut henkilöt perehdytetään vuosittain tehtävään.
Tausta-aineisto	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2006 • Uhkamallit, varautumisvelvoitteet Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 6 Henkilöstöturvallisuus • Luku 6.1 Henkilöstön toimenkuvat • Luku 6.2 Henkilöstön soveltuvuus • Luku 6.3 Henkilöstön osaamisen varmistaminen • Luku 6.4 Avainhenkilöstö • Luku 6.5 Työhöntuloprosessi • Luku 6.6 Prosessi työsuhteen päättyessä (tai keskeytyessä pitkäksi ajaksi) • Luku 6.7 Sijais- ja väliaikaisjärjestelyt • Luku 6.8 Työnkierto ja lomat • Luku 6.9 Ulkopuolinen työvoima • Luku 6.10 Varautuminen poikkeusoloihin Pandemiaan varautuminen tietoverkko-/tietotekniikka-alan yrityksessä, PTS 2007
Esimerkki	**Vaatimus 1**: Henkilöiden VAP-varaukset tarkastetaan vähintään kahden vuoden välein ja silloin kun henkilöstö vaihtuu. Virasto esittää varaukset organisaation alueen sotilaslääänin esikuntaan. **Vaatimus 2**: Ydintoiminnot on kuvattu prosesseineen ja niihin liittyvät turvakontrollit määritelty ja toteutettu. Henkilöt varahenkilöineen on määrätty ja tietävät tehtävänsä. **Vaatimus 3**: Palveluverkoston henkilöstön osaaminen ja kyky toimittaa palvelua erilaisissa häiriötilanteissa tunnetaan, eikä kriittisiä palveluja hankita toimittajalta jonka toimituskyky ei ole riittävällä tasolla. **Vaatimus 4**: Korkean tason palvelun VAP-henkilöiden luettelo päivitetään aina kun palvelua tuottava henkilöstö muuttuu, riippumatta siitä onko kyse viraston omasta vai palveluntarjoajan henkilöstöstä. Kaikki VAP-luettelon henkilöt osallistuvat vuosittaiseen jatkuvuusharjoitukseen. Jos henkilövarauksiin sisältyy henkilöitä jotka normaalisti tekevät jotain toista työtä, heille järjestetään vuosittain perehdytyskoulutus, lomasijaisuus tai muu kertaus siitä, mitä tehtävän hoitamiseen sisältyy, jotta he pystyvät suoriutumaan tehtävästä tarvittaessa. Tehtävää normaalisti hoitavat henkilöt perehtyvät tehtävään jatkuvasti, eivätkä tarvitse erillistä vuosittaista perehdytystä.

LIITE 2.4 KUMPPANUUDET JA RESURSSIT

KUMPPANUUDET JA RESURSSIT: SOPIMUSTEN HALLINTA	
4 A **Organisaation toiminnalle välttämättömät kumppanit, alihankkijat ja resurssit on tunnistettu.** (=SOPIVA 24, ~STO II: 106.0)	
Perustaso	1. Palveluverkoston eri toimijoiden merkitys ICT-palveluille on tunnistettu. 2. Kumppanuus- ja ICT-hankintatoiminta on vastuutettu ja organisoitu. (~TTT 4.1.1)
Korotettu taso	3. Palveluverkosto on tärkeimmiltä osiltaan kuvattu ja jatkuvuudenhallinnan toimintaperiaatteet on sovittu ja koulutettu. 4. Ydintoiminnan ja sen jatkuvuuden edellyttämien verkoston palvelujen ja muiden resurssien käytettävyys häiriö- ja erityistilanteissa on selvitetty.
Korkea taso	5. Palveluverkosto on kokonaisuudessaan kuvattu ja jatkuvuudenhallinnan toimintaperiaatteet on sovittu, koulutettu ja harjoiteltu. 6. Ydintoiminnan ja sen jatkuvuuden edellyttämien verkoston palvelujen ja muiden resurssien käytettävyys erityistilanteissa ja poikkeusoloissa varmistetaan suurien muutosten yhteydessä ja vuosittain. 7. Palveluntarjoajaksi voidaan valita vain sellainen palveluntarjoaja, jolla on mahdollisuus suojata asiakirjojen luottamuksellisuus ja tarvittaessa selvittää luottamuksellisuuden loukkaukset sähköisen viestinnän tietosuojalina (516/2004) 13a-13k§:ssä tarkoitetulla tavalla
Tausta-aineisto	Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006 • Luku 4. Muutoksen johtaminen ja tietoturvallisuus • Luku 6 Prosessien kehittäminen ja muutos Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Luku 2.2.5 Poikkeamatilanneharjoitukset • Luku 3.8 Sisäinen ja ulkoinen viestintä reagoinnin aikana Hankkeen tietoturvaohje VAHTI 9/2008 • Luku 3 Tietoturvallisuus hankkeen eri vaiheissa ISO/IEC 27002 • 6.2 External Parties • 6.2.1 Identification of risks related to external parties • 6.2.2 Addressing security when dealing with customers • 6.2.3 Addressing security in third party agreements BS 25999/2006 – Business Continuity Management – Osa 1 • 4.5 Outsourced activities

Esimerkki

Vaatimus 1: Organisaation jatkuvuussuunnittelussa tunnistetaan ne palvelut, joista organisaation ydintoiminnot ovat riippuvaisia, arvioidaan mitä vaikutuksia eripituisilla ICT-palvelujen katkoilla on organisaation ydintoimintoihin, sekä selvitetään kuka näitä palveluja organisaatiolle tuottaa ja mitkä ovat palvelutoimittajien tärkeimmät alihankkijat ja heidän roolinsa palvelun tuottamisessa.

Vaatimus 2: Hankintatoimi on keskitetty organisaatiossa yhteen yksikköön, joka ylläpitää riittävää hankintatoimen osaamista ja avustaa muita yksikköjä tarvittavien hankintojen toteuttamisessa sekä sopimusasioissa. Kumppanuussuhteiden hoitoon on nimetty yhteyshenkilöt kullekin kumppanille.

Vaatimus 3: ICT-palveluketjun rakenne eli palvelutoimittajan tärkeimmät alihankkijat ja heidän merkityksensä palvelun jatkuvuudelle (varaosat, huoltohenkilöstö, ICT-asiantuntijat, tukitoimet, laitetilat, jne.) on kuvattu yhteistyössä palvelutoimittajan kanssa tarkoituksenmukaista työkalua käyttäen. Palveluverkoston kuvaukset katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain.

Vaatimukset ja tavoitteet palveluverkoston jatkuvuudenhallinnan ja tietoturvallisuuden osalta on sovittu yhdessä palveluntoimittajien kanssa ja koulutettu avainhenkilöille.

Vaatimus 4: Palveluverkoston toimintakykyä voidaan arvioida palveluntarjoajille suunnattujen kyselyjen, häiriötilanteista saatujen kokemusten, yhteisten harjoitusten sekä auditointien avulla. Palveluverkostoa hallitaan ja siinä tapahtuvia omistajamuutoksia seurataan ja arvioidaan niiden vaikutusta omaan toimintaan. Tavoitteena on, että organisaatiolla on riittävän hyvä tilannekuva palvelua tuottavasta verkostosta, jotta se voi arvioida mitä riskejä verkostossa voi olla ja varautua niiden hallintaan.

Vaatimus 5: Palveluverkoston kuvauksissa huomioidaan myös alihankkijoiden alihankkijat, joilla on merkitystä palvelun jatkuvuuden ja turvallisuuden kannalta.

Vaatimus 6: Toiminnan muutosten yhteydessä osana muutostenhallintaprosessia arvioidaan muutoksien vaikutus ICT-toiminnan jatkuvuuden ylläpitoon esimerkiksi pöytätestien avulla tai riskienhallinnan välineitä käyttäen. Auditoinneilla ja palvelun seurantakokouksilla varmistetaan sovittu taso vuosittain.

KUMPPANUUDET JA RESURSSIT: SOPIMUSTEN HALLINTA	
4 B **Sopimuksissa on vaatimukset toiminnan jatkuvuuden hallinnalle ja tiedon turvaamiselle sekä niiden toteuttamiselle.** (~TTT 4.1, =SOPIVA 25)	
Perustaso	1. Kumppanin kanssa on tehty kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset, sekä niiden auditointi, raportointi ja sanktiointi. (=TTT 4.1.2) 2. Palvelusopimuksessa määritellään, mitä tietoturvallisuuden tasoa palvelun, palvelutoimittajan ja tämän mahdollisen alihankintaverkoston on noudatettava. (~TTT 4.1.4)
Korotettu taso	3. Sopimusosapuolten kanssa tarkastellaan sopimuksen toteutumista ja jatkuvuudenhallinnan tarpeita vuosittain. 4. Kumppanille asetetaan tietoturva- ja jatkuvuudenhallintavaatimukset jo tarjouspyyntö- tai kumppanuusneuvotteluvaiheessa. (=TTT 4.1.3)
Korkea taso	5. Jatkuvuudenhallintamenettelyt on otettu käyttöön koko palveluverkostossa ja niiden toimintaa testataan ja harjoitellaan säännöllisesti. 6. Palveluverkoston palvelu- ja turvallisuussopimuksia ylläpidetään ja niiden noudattamista auditoidaan säännöllisesti.
Tausta-aineisto	JHS 166 Julkisen hallinnon IT-hankintojen yleiset sopimusehdot (JIT 2007) • Luku 27 Yleiset ehdot • Luku 10 Sovellushankinnan mallisopimus • Luku 7 ja 11 Palveluiden mallisopimus • Luku 8 Konsultoinnin mallisopimus Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006 • Liite 3 Tietoturvallisuuden hallintajärjestelmä Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006 • Liitteet 1 ja 2 Turvallisuussopimusmalleja • Liite 6 Kumppanin tietoturvamenettelyiden tarkistuslista Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, työryhmämuistio 18.12.2008 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 5.2 Suhteet sidosryhmiin ja asiakkaisiin BS 25999/2006 – Business Continuity Management – Osa 1 • Kuva 1 – Incident timeline • 4.5 Outsourced activities

Esimerkki

Vaatimus 1: Sopimuksessa tai sen liitteessä luetellaan ne jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset, jotka osapuolten vastuut huomioiden ovat sovellettavissa hankinnan kohteeseen. Esimerkiksi tilojen suojaamista koskevia vaatimuksia ei kohdisteta palveluntoimittajaan, mikäli palvelun toimitus tapahtuu ostavan organisaation omissa tiloissa.

Lisäksi sopimuksessa määritellään ostavan organisaation tai sen edustajan oikeus auditoida vaatimusten toteutuminen, palvelutoimittajan velvollisuus raportoida havaituista poikkeamista, sekä sanktiot mikäli palveluntoimittaja ei täytä vaatimuksia sovitusti eikä huomautuksesta huolimatta kykene korjaamaan tilannetta palvelun kohteeseen nähden kohtuullisen ajan kuluessa.

Vaatimus 2: Palvelun hankinnasta solmittavassa sopimuksessa tai sen liitteessä määritellään palvelulta ja palveluntoimittajalta edellytettävä turvallisuustaso (perus-, korotettu tai korkea taso), velvoitetaan toimittaja edellyttämään vastaavaa tasoa palvelun kannalta keskeisiltä alihankkijoiltaan.

Palveluun liittyen voidaan myös solmia turvallisuussopimus, joka sisältää vaadittavan turvallisuustason, yritysturvallisuuden osa-alueiden mukaiset asiat ja osapuolten vastuutaulukon rooleittain. Turvallisuussopimus tehdään valtionhallintoon vakiintunutta mallia soveltaen ja se määrittelee palvelulle asetettavat turvallisuusvaatimukset. Turvallisuussopimuksen edellytyksenä on palvelutoimittajan laatima kuvaus tämän turvallisuustoiminnan järjestelyistä.

Vaatimus 3: Palveluntarjoajan kanssa käsitellään palvelutasosopimuksen toteutumista ja kehittämistä säännöllisissä seurantapalavereissa. Toimintaan liittyvä sopimuksen mukaisuus ja raportoinnin toimivuus voidaan myös auditoida vuosittain.

Vaatimus 4: Mallisopimus sekä sen liitteenä oleva turvallisuussopimus, joka sisältää jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset, liitetään tarjouspyyntöön. Sitoutuminen vaatimusten täyttämiseen palvelun käyttöönottoon mennessä on toimittajan kelpoisuusvaatimus, eli ehtona tarjouskilpailuun osallistumiselle. Ennen sopimuksen solmimista organisaatio auditoi tai pyytää kirjallisen selvityksen siitä, miten kumppani toteuttaa tarjouspyynnössä esitetyt tietoturva- ja muut vaatimukset. (~TTT 4.1.5)

Vaatimus 5: Jatkuvuussuunnitelmien toimivuutta arvioidaan säännöllisesti pöytätesteillä ja palveluverkoston yhteisillä harjoituksilla sekä auditoimalla.

Vaatimus 6: Palvelutasosopimuksen päivitys voi olla tarpeen, mikäli palvelun merkitys organisaation toiminnalle muuttuu oleellisesti. Turvallisuussopimusta päivitetään esimerkiksi silloin, kun palvelutoimittaja muuttaa uusiin tiloihin tai päivittää turvallisuuskäytäntöjään. Päivitys voi olla tarpeen myös, mikäli harjoituksissa paljastuu sovittuihin käytäntöihin liittyviä puutteita.

Auditointi perustuu vuosisuunnitteluun ja kulloinkin kohteiksi valittavien osa-alueiden arviointiin. Auditointisuunnitelmat laaditaan yhteistyössä palveluntoimittajan kanssa välttäen päällekkäistä auditointia. Palveluntoimittajan turvallisuuden hallintajärjestelmän toimivuuteen luotetaan ilman erillistä auditointia, jos se on sertifioitu esimerkiksi ISO/IEC 27001ja ISO 27002 tai muiden vastaavanlaisten standardien mukaisesti.

KUMPPANUUDET JA RESURSSIT: TOIMINNAN VARMISTAMINEN ERITYISTILANTEISSA	
4 C **Kriittisen toiminnan jatkuvuuden ja tiedon turvaamisen hallintavelvoite on ulotettu keskeiseen toimittajaverkostoon.** (~ TTT 4.1, =SOPIVA 26)	
Perustaso	1. Sopimusosapuolten vastuut resurssien hallinnasta ja saatavuudesta on sovittu. 2. Keskeisen toimittajaverkoston kyky tuottaa ostajan toiminnan kannalta keskeisiä palveluja häiriötilanteissa tunnetaan**.**
Korotettu taso	3. Tärkeimpien palvelujen tuotanto ja ylläpito kyetään priorisoimaan palveluverkostossa. 4. ICT-järjestelmien valvonnan, hallinnan ja ylläpitämisen yhteistoimintamallit keskeisessä toimittajaverkostossa on organisoitu ja sovittu.
Korkea taso	5. ICT-toiminnan, varautumisen ja tiedon turvaamisen säännöllinen ja palveluverkoston kattava auditointi on toteutettu yhteistyö- ja palvelusopimuksiin kirjattujen menettelyjen mukaisesti.
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006 • Liite 3 Tietoturvallisuuden hallintajärjestelmä ISO/IEC 27002 • 6.2 External Parties • 6.2.1 Identification of risks related to external parties • 6.2.3 Addressing security in third party agreements • 10.2.1 Service delivery • 10.2.2 Monitoring and review of third party services • 14.1.5 Testing, maintaining and re-assessing business continuity plans BS 25999/2007 – Business Continuity Management – Osa 2 • 4.1 Understanding the organization • 5 Monitoring and reviewing the BCMS • 5.1 Internal audit BS 25999/2006 – Business Continuity Management – Osa 1 • 4.5 Outsourced activities

Esimerkki

Vaatimus 1: Sopimuksessa palveluntoimittajaa velvoitetaan edellyttämään riittävää jatkuvuuden hallintaa ja tiedon turvaamista myös palvelun kannalta keskeisiltä alihankkijoiltaan. Vastuista sovittaessa määritellään sekä ostajan että palvelutoimittajan vastuut.

Vaatimus 2: Tarjouspyynnössä ja tarjoajan soveltuvuutta arvioitaessa huomioidaan sen kyky vastata toimintansa jatkuvuudesta. Ostaja selvittää miten toimittaja kykenee toimimaan häiriötilanteissa ja sopii toiminnasta osana turvallisuussopimusta.

Vaatimus 3: Palvelutoimittajilla on tieto siitä, mitkä heidän toimittamistaan palveluista ovat perus-, korotetun ja korkean tason palveluita, ja mikäli valtionhallinnon palvelutasoa on joltain osin erityistilanteen tai poikkeusolojen takia pakko laskea, se tehdään tässä järjestyksessä.

Vaatimus 4: Menettelyistä on sovittu turvallisuussopimuksessa. Yhteistyön osapuolilla on nimetyt vastuuhenkilöt, jotka koordinoivat yhteistyötä. Yhteistyön toimintaa käsitellään ostajan ja toimittajan kesken palvelun seurantaryhmissä.

Vaatimus 5: Organisaatiolla on palvelujen raportointi- ja auditointimenettelyt. Auditoinnit on sovittu osana turvallisuussopimusta ja niiden toimeenpanoon on suunnitelma, jossa on vuosittain auditoitavat kohteet. Auditoinnit voidaan toteuttaa esimerkiksi Valtion IT-palvelukeskuksen auditointipalvelua käyttäen. Vaatimusta täydentävä kriteeri (STO I : 106.0).

KUMPPANUUDET JA RESURSSIT: TOIMINNAN VARMISTAMINEN ERITYISTILANTEISSA	
4 D **Yhteistoiminta kumppanien kanssa häiriö- ja erityistilanteiden hallitsemiseksi on organisoitu ja vastuutettu.** (=SOPIVA 27)	
Perustaso	1. Häiriötilanteista ja niiden syistä kerätään tietoa, jota käytetään sopimusten ja toiminnan parantamiseen. (~TTT 4.2.3 & ~TTT 4.2.6) 2. Havaituista tietoturvapoikkeamista ja häiriöistä tiedotetaan välittömästi ja korjaustoimet aloitetaan sovitusti. (~TTT 4.2.2) 3. Häiriötilanteiden yhteistoimintaperiaatteet viranomaisten ja muiden sidosryhmien kanssa on suunniteltu ja keskeisimmiltä osiltaan koulutettu avainhenkilöille.
Korotettu taso	4. Kumppanuusverkostossa tietoturvapoikkeamista ja häiriöistä saatuja kokemuksia käytetään keskitetysti hyväksi toiminnan kehittämisessä. 5. Sidosryhmien ja palveluntuottajien kanssa arvioidaan säännöllisesti palvelun jatkuvuutta ja siihen kohdistuvia uhkia YETTS:n erityistilanteissa. 6. Erityistilanteiden yhteistoiminta ja kriisitiedottaminen viranomaisten sekä muiden sidosryhmien kanssa on suunniteltu, toteutettu ja keskeisimmiltä osiltaan harjoiteltu.
Korkea taso	7. Poikkeusolojen yhteistoiminta viranomaisten ja muiden sidosryhmien kanssa on todennettu ja harjoiteltu. 8. Yhteistoimintaa toimittajaverkostossa testataan ja harjoitellaan säännöllisesti.
Tausta-aineisto	Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Luku 2.2.5 Poikkeamien jälkiraportointi ja todisteaineiston kerääminen • Luku 3.8 Sisäinen ja ulkoinen viestintä reagoinnin aikana Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006 • Luku 6 Prosessien kehittäminen ja muutos ISO/IEC 27002 • 6.2 External Parties • 6.2.1 Identification of risks related to external parties • 6.2.2 Addressing security when dealing with customers • 6.2.3 Addressing security in third party agreements • 13.1 Reporting Information Security Events And Weaknesses • 13.2 Management Of Information Security Incidents And Improvements BS 25999/2007 – Business Continuity Management – Osa 2 • 4.3 Developing and implementing a BCM response BS 25999/2006 – Business Continuity Management – Osa 1 • Kuva 1 – Incident timeline • 4.5 Outsourced activities

Esimerkki **Vaatimus 1**: Sopimusten liitteenä on kuvattu menettelyt tiedon keräämiseksi.

Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen. (=TTT 4.2.1).

Palvelutaso- ja tietoturvapoikkeamista ja niiden syistä laaditaan toimittajan kanssa yhteistyössä kirjallinen raportti. (~TTT 4.2.4).

Raportin pohjalta käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi. Organisaation häiriötilanteista kerätään tilasto- ja historiatietoja.

Vaatimus 2: Sopimuksissa on määritelty osapuolten velvollisuus tiedottaa välittömästi yhteistyön kohteeseen liittyvistä tietoturvapoikkeamista ja häiriöistä, sekä menettelyt kuinka tiedottaminen tehdään. Tiedottaminen tukee onnistunutta yhteistoimintaa ja tuottaa mahdollisesti apua häiriön ratkaisuun. Palvelutasosopimuksessa on määritelty kuinka nopeasti korjaustoimet tulee aloittaa.

Vaatimus 3: Yhteistoimintakäytännöt on kuvattu jatkuvuussuunnitelmassa ja niitä käsitellään avainhenkilöstön koulutuksessa ja harjoittelussa.

Vaatimus 4: Organisaatiossa osallistutaan aktiivisesti tietoturvatilanteen seuranta- tai yhteistyöryhmiin. (=TTT 5.D.9) Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto ja analyysi niiden vaikutuksesta toimintaan. (~TTT 1.5.5)

Havaintotietoa jaetaan esimerkiksi VAHTI-työryhmässä valtionhallinnon sisäiseen käyttöön. Tapauksista opitaan ja muutetaan toimintaa niin, että riskiä pienennetään.

Vaatimus 5: YETTS osaltaan vaatii tätä tarkastelua, sillä valtionhallinnon organisaatioiden pitää tehdä tätä oman riskienhallintapolitiikkansa mukaisesti ja valmiuslain velvoitteiden täyttämiseksi. Tarkastelu voidaan tehdä esimerkiksi riskien arvioinnin yhteydessä.

Vaatimus 6: Kriisiviestintä on suunniteltu osana organisaation viestintäperiaatteita ja kuvattu jatkuvuussuunnitelmassa. Organisaatio voi osallistua esimerkiksi VALHA- tai TIETO-harjoituksiin, joissa yhtenä osa-alueena on myös tiedottaminen eri tilanteissa.

Vaatimus 7: Organisaatio harjoittelee viranomaisten ja muiden sidosryhmien kanssa.

Vaatimus 8: Yhteistoimintaa harjoitellaan TIETO- ja VALHA-harjoituksissa sekä organisaatioiden omissa varautumisharjoituksissa.

LIITE 2.5 PROSESSIT: ICT-JATKUVUUDEN HALLINTA

ICT-JATKUVUUDEN HALLINTA: ICT-JOHTAMINEN	
5 A **ICT-hankkeen jokaisessa vaiheessa sekä sen johtamisessa otetaan huomioon keskeiset jatkuvuuden tekijät.**	
Perustaso	1. ICT-järjestelmien omistajat tietävät ICT-varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti. (=TTT 5.L.1) 2. Jatkuvuuden hallinnan prosessille, tiedon turvaamiselle ja varautumiselle on kuvattu ja toteutettu toteutustapa. 3. ICT-hankkeiden ja projektien eri vaiheissa kontrolloidaan jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen vaatimusten toteutumista. (~STO I:103.0)
Korotettu taso	4. Tiedon turvaamiselle ja varautumiselle on kuvattu, toteutettu, koulutettu ja testattu keskeisimmät häiriö- ja erityistilanteet huomioon ottava toteutustapa ja jatkuvuuden hallinnan prosessi.
Korkea taso	5. Tiedon turvaamiselle ja varautumiselle on kuvattu, toteutettu, koulutettu ja säännöllisesti harjoiteltu erityistilanteet ja poikkeusolot huomioon ottava toteutustapa sekä jatkuvuuden hallinnan prosessi.
Tausta-aineisto	Tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000 • Luku 5 Järjestelmäkehityksen tietoturvallisuuden hallinnointi • Luku 6 Tietoturvallisuusvaatimukset järjestelmän elinkaaren eri vaiheissa • Luku 7 Järjestelmäkehityksen tietoturvallisuuden erityiskysymyksiä Hankkeen tietoturvaohje VAHTI 9/2008 • Luku 2 Tietoturvallisuuden toteuttaminen hankkeiden elinkaaren aikana.. Tietoturvaopas sähköisen palvelun tarjoajalle, Luoti -julkaisu 8/2006, LVM • Kuva 1, sivu 10 ISO/IEC 27002 • 12.1 Security Requirements Of Information Systems • 12.1.1 Security requirements analysis and specification. • 12.5.5 Outsourced software development BS 25999/2006 – Business Continuity Management – Osa 1 • 6.4 Determining continuity requirements

Esimerkki

Vaatimus 1: Organisaation johto tietää tähän liittyvät vastuunsa ja resursoi jatkuvuudenhallinnan.

Vaatimus 2: ICT-hanke on kuvattu tietojärjestelmäkehityksen vaiheistuksen mukaisesti prosessiksi, jossa on mukana turvallisuusasioiden tarkastelupisteet. Kussakin pisteessä arvioidaan tulokset ja päätetään siirtymisestä seuraavaan kehitysvaiheeseen.

Vaatimus 3: Arkkitehtuurivalinnoissa, projektihallinta- ja systeemityömenetelmissä sekä -ohjeissa on huomioitu jatkuvuuden hallinta, tiedon turvaamisen ja varautumisen vaatimukset. Hankkeen johtoryhmä päättää toimenpiteiden riittävyyden riskiarvioinnin perusteella.

Hankkeissa voidaan käyttää apuna tausta-aineistoissa mainittuja VAHTI-ohjeiden tarkastuslistoja ja esimerkiksi standardeja, NFPA 1600, ISO 27005.

Vaatimus 4: Arkkitehtuurivalinnoissa, projektihallinta- ja systeemityömenetelmissä sekä -ohjeissa painotetaan jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen vaatimusten huomioon ottamista. Hankkeen projektihallinta pitää auditoida ulkopuolisen toimesta. Ohjeistuksessa hyödynnetään tarkastuslistoja, joita on tausta- aineistoissa mainituissa VAHTI-ohjeissa.

Vaatimus 5: ICT-hankkeiden ja projektien eri vaiheissa testataan (esim. vaatimusmäärittelyä vastaan, käyttöönottotestaus tulokset verrattuna vaatimusmäärittelyyn) ja arvioidaan sekä auditoidaan jatkuvuuden hallinnan, tiedon turvaamisen ja varautumisen vaatimusten toteutumista.

ICT-JATKUVUUDEN HALLINTA: ICT-JOHTAMINEN	
5 B **Tietojärjestelmäkehityksessä ja -hankinnoissa huomioidaan tietoturva- ja jatkuvuusvaatimukset.** (~TTT 5.M)	
Perustaso	1. Järjestelmän omistaja hyväksyy, mitä tietoturvatasoa järjestelmän tulee valmiina tai muutosten jälkeen noudattaa. (=TTT 5.M.1, ~STO I:109.0) 2. Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan. (=TTT 5.M.2) 3. Kriittiset tietojärjestelmäpalveluiden ja ICT-infrastruktuurin tukitoiminnot on tunnistettu ja kuvattu.
Korotettu taso	4. Hankkivalla organisaatiolla on tietoturvallisuusvaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittaville järjestelmille asetettavien vaatimuksien tulee olla. (=TTT 5.M.4) 5. Jos organisaatio hankkii räätälöityjä tietojärjestelmiä, on organisaatiolla oltava dokumentoitu tietojärjestelmän hankintaprosessi, jonka eri vaiheissa on otettu tietoturvallisuus ja järjestelmään kohdistuva jatkuvuuden hallinta huomioon. (=TTT 5.M.5) 6. Osana hankintaprojektia järjestelmästä valmistuu kirjallinen turvallisuuskuvaus ja käyttäjän ohje, joissa kerrotaan miten järjestelmä suojataan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat tietoturvatoimenpiteet. (=TTT 5.M.6)
Korkea taso	7. Tietoturvavastaava tarkastaa järjestelmän tietoturvakuvaukset. (=TTT 5.M.7) 8. Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja. (=TTT 5.M.8) 9. Järjestelmään tehdään tietoturvatestaus tai -auditointi ennen kuin se otetaan käyttöön. (=TTT 5.M.9)
Tausta-aineisto	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 4 Keskeisten tietojärjestelmien erityishaasteita • Luku 10 Ohjelmistoturvallisuus • Luku 12.4 Muutoshallinta Valtiohallinnon salauskäytäntöjen tietoturvaohje VAHTI 3/2008 • Luku 4.7 Ohjaavat arkkitehtuurit Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001 • Luku 4 Valmisohjelmistohankinnat • Luku 5 Sovelluskehitys Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus VAHTI 3/2000 • Luku 6 Tietoturvallisuusvaatimukset järjestelmän elinkaaren eri vaiheissa

Tausta-aineisto	BS 25999/2006 – Business Continuity Management – Osa 1 • 6.3 Identification of critical activities ISO/IEC 27002 • 12.5 Security In Development And Support Processes • 12.5.1 Change Control Procedures • 12.5.2 Technical Review Of Applications After Operating System Changes • 12.5.3 Restrictions On Changes To Software Packages • 12.5.4 Information Leakage • 12.5.5 Outsourced Software Development • 12.6 Technical Vulnerability Management • 12.6.1 Control Of Technical Vulnerabilities ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
Esimerkki	**Vaatimus 1**: Organisaatiossa on järjestelmien omistajien hyväksymä järjestelmien tärkeysluokitus, jonka perusteella vaadittava tietoturvataso määräytyy. **Vaatimus 2**: Riskianalyysin lisäksi VAHTI 5/2004 -ohjeen luvun 10.3 sisältöä käytetään tarkistuslistana hankittavan ohjelmiston tietoturvavaatimusten laadinnassa. Järjestelmäkehitystä ja jatkuvuudenhallintaa varten on olemassa järjestelmien tärkeysluokitus sekä palvelujen priorisointimenettely. **Vaatimus 3**: Jatkuvuussuunnittelu edellyttää tämän toimenpiteen suorittamisen. **Vaatimus 4**: Vaatimuksia on listattu VAHTI 6/2001 (luku 4) ja VAHTI 3/2000 –ohjeessa (luku 6). **Vaatimus 5**: Sovellus- ja versiohallinta on määritelty, poikkeamat estetty sekä ympäristö dokumentoitu ja valvottu. Ohjelmistohankinnoissa suositellaan tuotteen tietoturva-auditointia ennen käyttöönottoa. **Vaatimus 6**: Liitteeksi tuotetaan hankittavan kohteen mukainen tietoturvakuvaus. **Vaatimus 7**: Kehitysprosessin eri vaiheissa tuotetaan tarvittava aineisto kuvaukseen ja eri roolit käyvät läpi tehtäväkuvauksensa (esim. kehityspäällikkö, tietoturvavastaava, tuotannosta vastaava, ohjelmistosta vastaava) mukaiset osa-alueet kuvauksesta. **Vaatimus 8**: Katselmointeja järjestetään esimerkiksi työparikatselmointeina, projektiryhmän tai ohjelmointitiimin kokouksissa tai ulkopuolisen auditoijan tekeminä. **Vaatimus 9**: Esimerkkejä eri testi- tai auditointitavoista ovat ei-haluttujen ominaisuuksien ja käyttötapausten testaus sekä penetraatiotestaus ilman ennakkotietoja (ns. black-box testaus) tai ennakkotietojen kera (ns. white-box testaus). **Vaatimus 10**: Organisaatio voi hyödyntää VAHTI 3/2000 -ohjeen liitteen 3 tarkastuslistaa.

ICT-JATKUVUUDEN HALLINTA: ICT-PALVELUJEN TURVAAMINEN	
5 C **Ydintoimintojen palvelutuotanto ja hallinnan prosessit on varmistettu ja niillä on varamenettelyt.** (~SOPIVA 2 &10)	
Perustaso	1. Ydintoimintojen järjestelmissä on määritelty mitattavat perustason hallinnolliset ja tekniset vaatimukset. 2. Ydintoimintojen tarvitsemien käyttöpalveluiden ja tuotanto-operoinnin häiriö- ja erityistilanteiden hallinta on huomioitu sopimuksissa. 3. Ydintoimintojen tuotantomuutokset ja varajärjestelyihin siirtyminen ja häiriöistä toipumisen prosessit on suunniteltu ja dokumentoitu.
Korotettu taso	4. Järjestelmittäin on todennettu keskeiset mitattavat tekniset vaatimukset. 5. Ydintoimintojen palvelutuotannon ja hallinnan prosesseissa on sovittu, ohjeistettu ja koulutettu häiriö- ja erityistilanteiden hallinta sekä varamenettelyt. 6. Ydintoimintojen tuotantomuutokset ja varajärjestelyihin siirtymisen ja toipumisen prosessit häiriö- ja erityistilanteissa on suunniteltu, sovittu, ohjeistettu ja koulutettu.
Korkea taso	7. Ydintoimintojen järjestelmissä on todennettu ja testattu teknisten vaatimusten toteutuminen. 8. Ydintoimintojen palvelu tuotannon ja hallinnan prosesseissa on todennettu ja harjoiteltu erityistilanteiden ja poikkeusolojen hallinta ja varamenettelyt. 9. Ydintoimintojen järjestelmien käyttöpalveluiden ja tuotanto-operoinnin poikkeusolojen toteutus on huomioitu ja todennettu sopimuksissa ja toiminta on harjoiteltu.
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 11 Jatkuvuuden ja erityistilanteiden hallinta Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • 2.2.5 Poikkeamatilanneharjoitukset Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 6.7 Sijais- ja väliaikaisjärjestelyt • Luku 6.8 Työnkierto ja lomat • Luku 6.9 Ulkopuolinen työvoima • Luvut 5 -12 Tietoturvallisuuden eri osa-alueiden mukainen varautuminen poikkeusoloihin • Luku 13 Tietoturvallisuuden arviointi Viestintä- ja sähkönjakeluverkkojen keskinäiset riippuvuudet, HVK 1/2006 BS 25999/2006 – Business Continuity Management – Osa 1 • Taulukko 1 – Types and methods of exercising BCM strategies

Esimerkki

Vaatimus 1: Laadittavassa SLA-sopimuksessa kuvataan mittarit. Ne voivat olla määrällisiä tai laadullisia. Perustasolla hyödynnetään JHS-suosituksen mittareita.

Mittarien asettamisessa ja arvioinnissa käytetään apuna VAHTI 5/2004 -ohjeen lukujen 5-12 tarkastuslistoja. Arvioinnin kautta saadulla tiedolla kehitetään järjestelmien tarvitsemaa suojausta. VAHTI 5/2004 –ohjeen kuva 4 Kerätyn tiedon arvo.

Vaatimus 2: Palvelun toimittajan jatkuvuussuunnitelmaa arvioidaan tästä näkökulmasta. Palvelukohtaisesti on määritelty normaali- ja minimipalvelutaso sekä aikavaatimukset ja palautumispisteet.

Vaatimus 3: Palvelun toimittajalla pitää olla kuvattuna toimintansa näiden tapahtumien varalta ja testattuna niiden toimivuus.

Varajärjestelmät palvelun tuottamiseen on sovittava sopimuksissa.

Vaatimus 4: Laaditaan järjestelmäkohtainen SLA. Tarvitaan palveluluetteloa, jossa on kaikki eri hallinnonalojen kriittiset palvelut. Tämän pohjalta vaatimukset koordinoidaan tietoturvatasojen ja kokonaisarkkitehtuurin näkökulmasta keskistetysti johdettavaksi kustannustehokkaaksi kokonaisuudeksi. Vaatimusta täydentävä kriteeri (STO I:106.0)

Vaatimus 5: Kriittisten ja keskeisten toimintojen sähköiset palvelut ja niiden väliset riippuvuudet on kuvattu sekä arvioitu riippuvuuksista muodostuvia riskejä. Käyttöpalveluiden ICT-infrastruktuurin ja sen vaatimiin tukitoimintoihin liittyviä kuvauksia ja jatkuvuussuunnitelmia ylläpidetään säännöllisesti.

Vaatimus 6: Palvelukohtaisesti on määritelty normaali- ja minimipalvelutaso sekä palautumisen aikavaatimukset häiriötilanteissa, sekä varmistettu niiden toteutumista keskeisiltä osiltaan. Siirtymisen järjestelyt suositellaan auditoitavaksi.

Vaatimus 7: Palvelutasosopimukset (SLA) on laadittu ja auditoitu kattavasti korkean tason järjestelmien palveluverkostoissa. Testaaminen aikaisessa elinkaaren vaiheessa vähentää kustannuksia ja erityisesti käyttöönottotestaus tuotantoon oton jälkeisiä muutoksia. ICT-järjestelmien valvonnan, hallinnan ja ylläpitämisen yhteistoimintamallit palveluntuottajaverkostossa on testattu ja harjoiteltu säännöllisesti yhteistyö- ja palvelusopimuksiin kirjatuin aikavälein.

Vaatimus 8: Palvelukohtaisesti on määritelty normaali- ja minimipalvelutaso sekä palautumisen aikavaatimukset erityistilanteissa ja poikkeusoloissa, sekä varmistettu palvelutason toteutuminen.

Vaatimus 9: Tuotantomuutokset, tarvittava osaaminen ja resurssit sekä varajärjestelyihin siirtyminen ja toipuminen poikkeusoloissa on suunniteltu, varmistettu, dokumentoitu ja säännöllisesti harjoiteltu.

ICT-JATKUVUUDEN HALLINTA: ICT-PALVELUJEN TURVAAMINEN	
5 D **Kriittisten toimintojen vaatimat tietoaineistot on turvattu häiriö- ja erityistilanteissa.**	
Perustaso	1. Tietoaineistojen turvallisuudelle on asetettu vaatimukset luottamuksellisuuden, eheyden ja käytettävyyden suhteen. (~STO I:505.0) 2. Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään. (=TTT 5.1.3 & ~STO I:601.0)
Korotettu taso	3. Tietoaineistojen käyttö erityistilanteissa (yhteiskunnallinen häiriö) on suunniteltu, dokumentoitu, toteutettu ja testattu. 4. Kriittisten toimintojen tietoaineistot on hajautettu maantieteellisesti vähintään kahteen eri paikkaan, joista vähintään yksi on Suomessa.
Korkea taso	5. Tietoaineistojen käyttö poikkeusoloissa on suunniteltu, dokumentoitu, toteutettu ja testattu. 6. Kriittisten toimintojen tietoaineistojen sijainti ja hallinta ovat Suomessa korkean suojaustason paikassa.
Tausta-aineisto	Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002 • Luku 4.1 Varakeskus Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 8.8 Varautuminen poikkeusoloihin Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 4. Tietoaineistoturvallisuus – tietopääoman hallinta ISO/IEC 27002 • 7.2 Information Classification

Esimerkki

Vaatimus 1: Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä tiedonhallinta- tai tiedonohjaussuunnitelma. Vaatimusta täydentävä kriteeri (STO I:607.0).

Organisaation käytössä olevat tietoaineiston hallinnan ohjeet ja välineet tukevat aineistojen luokittelua ja arkistointia (=TTT 5.1.7) Vaatimusta täydentävä kriteeri (~ STO I:601.0)

Ohje sisältää eri suojaus- ja turvaluokkiin kuuluvien aineistojen hallinnan sen elinkaaren eri vaiheissa. Tietojen varmistukset on hoidettu huomioiden niiden tärkeys toiminnalle. Vaatimusta täydentävät kriteerit (STO I:602.0, STO I:604.0, STO I:605.0, STO I:606.0, STO I :607.0)

Vaatimus 2: Tietoaineiston käsittely on ohjeistettu ja hävitettäväksi tarkoitettavat asiakirjat tuhotaan niin, että luottamuksellisuus ja tietosuoja on varmistettu. (=TTT 5.1.4, =TTT 5.1.5) Vaatimusta täydentävät kriteerit (STO I:603.0). Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§) (=TTT 5.1.3). Auditoinneilla ja itsearvioinneilla varmistutaan toimintatapojen turvallisuudesta.

Vaatimus 3: Jatkuvuudenhallinnan suunnitelmassa kuvataan tietoaineistojen käsittelyn osuus. Suunnitelmia testataan ja niiden toimivuutta arvioidaan säännöllisesti. Vaatimusta täydentävä kriteeri (STO I:701.0).

Vaatimus 4: Toiminnan hajautus perustuu valtionhallinnon toimijan tärkeysluokkaan ja sen ydintoimintojen (tuottamien palveluiden) tärkeyteen valtionhallinnolle.

Vaatimus 5: Palvelusopimus sisältää varautumiseen liittyvät vaatimukset palveluntoimittajalle. Valmiussuunnitelmassa kuvataan tietoaineistojen suojaaminen. Suunnitelmaa testataan ja sen toimivuutta arvioidaan säännöllisesti.

Vaatimus 6: Vaatimus koskee valtion turvallisuuden kannalta tärkeitä tietojärjestelmiä. Esimerkkinä ovat sähkönjakelun ohjausjärjestelmät ja tietoliikenneverkon solmujen kytkentäpisteet. Kriittisten toimintojen järjestelmät tietoineen on hajautettu reaaliaikaisesti ja maantieteellisesti vähintään kahteen eri korkean suojaustason paikkaan.

ICT-JATKUVUUDEN HALLINTA: ICT-PALVELUJEN TURVAAMINEN	
5 E **Tietoturvallisuuden ja jatkuvuudenhallinnan tilasta tiedotetaan ja raportoidaan yhteistyö- ja palveluketjussa.** (~TTT 5.A)	
Perustaso	1. Säännöllinen kirjallinen sisäinen raportointi tietoturvallisuuden tilasta ja jatkuvuuden hallinnasta on organisoitu ja vastuutettu. (~TTT 5.A.1, ~TTT 5.A.3) 2. Tietoturvatapahtumista ilmoitetaan tietoturvavastaavalle viivytyksettä. (~TTT 5.A.2) 3. Raportoinnin perusteella tehdään turvaamisen kehitystoimia, joiden toteutumista seurataan.
Korotettu taso	4. Valtionhallinnon palvelujen toiminnan kannalta kriittiset poikkeamat käsitellään palvelutoimittajan johtoryhmässä ja hallinnonalan ministeriössä sekä raportoidaan merkittävien havaintojen osalta VM:lle. 5. VAHTI:ssa ja harjoitukseen osallistuneissa organisaatioissa käsitellään VALHA ja TIETO harjoituksien havainnot ja kehittämiskohteet.
Korkea taso	6. VALHA- ja TIETO- harjoituksien tuloksia seurataan ja kehitetään toimintaa havaintojen perusteella.
Tausta-aineisto	Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 5.6: Esimerkki raportointimenettelyistä ja raportin sisällöstä Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 • Sivu 7 Yleiskuvaus toimintaprosessista • Luku 2.2.6 Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti Tietoturvallisuuden hallintajärjestelmän arviointisuositus VAHTI 3/2003 • Liite 8 Esimerkki tietoturvallisuuden arviointiraportista ISO/IEC 27002 • 13 Information security incident management • 13.1 Reporting Information Security Events And Weaknesses • 13.1.1 Reporting information security events • 13.1.2 Reporting security weaknesses

Esimerkki

Vaatimus 1: Tietoturvapäällikkö (tai vastaava) tapaa kuukausittain tietohallinnon edustajia. Tapaamisessa käsitellään tehtyjä tietoturvallisuuden kehitystoimia, päivityksiä ja käsitellään mahdollisia uusia havaittuja uhkia ja riskejä. Vaatimusta täydentävä kriteeri (STO I:104.0).

Tietoturvapäällikkö kerää tiedot palvelun toimittajien tietoturvallisuuden ja jatkuvuudenhallinnan tilanteesta palveluiden toiminnasta vastaavien palvelupäälliköiden avulla.

Raportti laaditaan kirjallisena osana viraston omaa riskienhallinnan raportointia (=TTT 5.A.3).

Kirjallinen raportti dokumentoidaan ja kirjataan asiakirjahallintajärjestelmään. Raportit ovat luottamuksellisia.

Vaatimus 2: Palvelun toimittajiin liittyvä raportointi on sovittu palveluun liittyvässä turvallisuussopimuksessa. Vakavana tapahtumana voidaan pitää tilannetta, jossa palvelu joudutaan sulkemaan tietoaineistoon kohdistuvan vaaran välttämiseksi tai haitallisen ohjelman leviämisen estämiseksi.

Vaatimus 3: Normaali raportointi palvelun tilasta noudattaa SLA:n mukaisia asioita. Siihen kirjataan esimerkiksi suojakopioinnit, palautuksien harjoittelu, tietoturvapäivityksien suoritus, järjestelmän huoltokatkot, välittömät järjestelmään tehdyt korjaustoimien määrä syineen, jne.

Kaikki raportointi perustuu sovittuihin tietoturvatavoitteisiin ja niiden mittareihin. (=TTT 5.A.4)

Raportti on mittari jolla seurataan palveluprosessien ja järjestelmien toimintaa. Havaintojen perusteella tehdään sovitusti muutoksia toimintatapoihin tai työohjeisiin tai jatkuvuussuunnitelmiin. Raportoinnissa seurataan järjestelmiin kohdistuvien riskien hallintaa.

Kehitystoimet kuuluvat riskienhallinnan mukaan seurattaviin asioihin PDCA-mallin (Plan-Do-Check-Act) mukaisesti.

Vaatimus 4: Kokemukset käsitellään ja tuleviin sopimuksiin tehdään muutoksia. Sopimuspohjia päivitetään, etteivät asiakohdat jää unohduksiin.

Raportointi on osana TTS-prosessia ja organisaation riskienhallintaa. Jaetaan yhteenvetotietoa harjoituksien havainnoista.

Vaatimus 5: Harjoituksissa mitataan suoriutumista annetuista YETTS:n mukaisissa pelitilanteissa.

ICT-JATKUVUUDEN HALLINTA: TIETOJENKÄSITTELY-YMPÄRISTÖN HALLINTA	
5 F **Organisaation vastuulla oleva ICT-kokonaisuus on tunnistettu ja sen hallinta on järjestetty** (~TTT 5.B)	
Perustaso	1. Organisaation henkilörekistereistä ja tietojärjestelmistä on laadittu lainsäädännön mukaiset rekisteriselosteet ja järjestelmäkuvaukset sekä -selosteet. Virastossa on saatavilla luettelot viraston omistamista ja käyttämistä fyysisistä tai virtuaalisista tietoteknisistä laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä. (=TTT 5.B.3 ja TTT 5.B.1 ja TTT 5.B.2) 2. Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu. (=TTT 5.B.4, ~STO I:508.0) 3. Laite-, tietojärjestelmä-, palvelu- ja ohjelmistoluettelojen sekä lain mukaisten selosteiden ja kuvausten päivitys on organisoitu ja vastuutettu. (=TTT 5.B.5)
Korotettu taso	4. Omistaja on dokumentoinut laitteiden, tietojärjestelmien ja rekistereiden tietosisällön. (=TTT 5.B.6) 5. Omistaja on luokitellut omaisuuden tarvittavan tietoturvatason mukaisesti. (=TTT 5.B.7) 6. Omistajat katselmoivat laite-, rekisteri-, palvelu- ja ohjelmistoluetteloiden sekä lain mukaisten selosteiden ja kuvausten sisällön vuosittain. (=TTT 5.B.8)
Korkea taso	
Tausta-aineisto	Henkilörekisteriselosteen RTF-lomakepohja Tietosuojavaltuutetun toimistosta Tietojärjestelmäselosteen RTF-lomakepohja Tietosuojavaltuutetun toimistosta. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Liite 2. Tietoturvavastuut rooleittain ISO/IEC 27002 • 7.1 Responsibility For Assets • 7.1.1 Inventory of assets

Esimerkki

Vaatimus 1: Organisaation sähköisessä asiointipalvelussa rekisteriseloste on palvelun käyttäjien nähtävissä. Henkilötietolain 10 § mukainen rekisteriseloste on asetettu rekisteröityjen nähtäville. (=TTT 5.B.1).

Kustakin tietojärjestelmästä on Julkisuuslain18 § mukainen tietojärjestelmäkuvaus. (=TTT 5.B.2) ASP ja SaaS -palveluiden osalta on huolehdittava tietojen varmistuksien käsittelystä alustojen muuttuessa. Asiakohta on käsiteltävä sopimuksissa ja yhdessä palveluntoimittajan kanssa selvitettävä miten näissä tilanteissa toimitaan.

Vaatimus 2: Tietohallinto ylläpitää laiterekisteriä yhteistyössä palveluntoimittajien kanssa. Sopimuksissa on sovittava menettelyt ja vuosittain tehtävä tarkastus jossa varmistutaan sovittujen toimenpiteiden suorittamisesta.

Vaatimus 3: Organisaation asianhallintajärjestelmän omistaa hallintopalveluyksikkö ja tietoverkkoinfrastruktuurin tietohallinto. Yksiköt nimeävät sisältään henkilöt, joille omistajarooli kuuluu.

Vaatimus 4: Kun uusi työasema tai ohjelmisto otetaan käyttöön, työasematuen vastuulla on kirjata laite tietoineen työasemien laiteluettelona toimivaan tietokantaan tai Excel-taulukkoon.

Vaatimus 5: Tietojärjestelmät on luokiteltu sekä tietoturvatason mukaisesti, että sen mukaan kuinka välttämättömiä ne ovat organisaation toiminnalle.
Organisaatiossa on kaksi tietojärjestelmää: matkahallintajärjestelmä korotetulla tietoturvatasolla ja asiointijärjestelmä korkealla tietoturvatasolla. Kummankin järjestelmän taustalla olevat tietokannat toimivat resurssien maksimaalisen käytön vuoksi samalla fyysisellä tietokantapalvelimella. Tietokantapalvelimen tietoturvatason tulee tällöin olla korkealla tasolla.

Vaatimus 6: Säännöllisenä pidetään vuosittain tapahtuvaa inventointia. Tämä on standardien lähtökohta ja perustuu vuosittain tehtävään hallintajärjestelmän katselmointiin ja kehittämis-suunnitelman päivittämiseen.

Tavoitteena on PDCA-mallin mukainen toiminta prosesseissa.

ICT-JATKUVUUDEN HALLINTA: TIETOJENKÄSITTELY-YMPÄRISTÖN HALLINTA	
5 G **Tietojenkäsittely-ympäristöt otetaan käyttöön, päivitetään ja poistetaan käytöstä hallitusti.** (~TTT 5.C)	
Perustaso	1. Tietojärjestelmän ja työasemien käyttöönottoasennuksessa, päivityksissä, muutoksissa ja käytöstä poistamisessa otetaan huomioon järjestelmän tietosisällön tietoturvavaatimukset. (=TTT 5.C.1, =TTT 5.D.2, =TTT 5.D.6, =TTT 5.D.1, ~STO I:109.0) 2. Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu, kontrolloitu ja organisoitu. (=TTT 5.C.2, =TTT 5.D.2, =TTT 5.D.6, =TTT 5.D.1) 3. Tietojärjestelmät ja työasemat huolletaan niin, että tiedot eivät joudu ulkopuolisten haltuun riippumatta niiden tallennusmuodosta. (~TTT 5.C.6)
Korotettu taso	4. Tietojärjestelmien ja työasemien ensiasennuksesta ja käytöstä poistosta on kirjallinen ohjeisto, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturva-asetukset sekä laitteiden käsittelyn ja massamuistien tyhjennyksen ohjeet kun ne siirtyvät ympäristöstä toiseen tai kun ne poistuvat organisaation hallinnasta. (~TTT 5.C.3) 5. Ohjeiden päivitys on vastuutettu ja organisoitu. (=TTT 5.C.4) 6. Muut kuin päivitys- ja muutoshallintaperiaatteiden perusteella kiireellisinä toteutettavat päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana (ns. huoltoikkuna). (=TTT 5.D.4)
Korkea taso	7. Korkean tietoturvatason tietojärjestelmät ja työasemat kovennetaan mm. poistamalla niistä sellaiset palvelut ja toiminnot joita järjestelmän käytössä ei tarvita. (~TTT 5.C.5) 8. Päivitysten ajantasaisuutta ja onnistumista mitataan ja seurataan. (=TTT 5.D.7) 9. Päivitykset ja muutokset testataan ennen kuin ne otetaan tuotantokäyttöön. (=TTT 5.D.8)
Tausta-aineisto	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 12 Käyttöturvallisuus Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004 • Luku 5.1 Työaseman turvalliset asetukset NIST:in teknisiä järjestelmien ylläpito- ja konfigurointiohjeita NIST:in teknisiä järjestelmien tietoturvallisuuden tarkistuslistoja Center for Internet Security CIS: eri järjestelmien koventamisohjeita ISO/IEC 27002 • 9.2.6 Secure disposal or re-use of equipment • 9.2.7 Removal of property • 1 0.7 Media Handling • 10.7.1 Management of removable media • 10.7.2 Disposal of media • 10.7.3 Information handling procedures

Esimerkki

Vaatimukset 1-2: Organisaatiossa työasemapalvelut on hankittu ulkopuoliselta palveluntarjoajalta, joka vastaa ensiasennuksista ja käytöstä poistamisesta sopimuksen tietoturvaliitteessä olevien teknisten ohjeiden mukaisesti. Käytöstä poistamisen yhteydessä on sovittava menettely järjestelmästä otettujen varmistusten osalta. Mitkä tiedot siirretään uuteen järjestelmään ja mitkä tiedot pitää säilyttää, mikäli niihin pitää palata tietojen eheyden varmistamiseksi.

Järjestelmän toimivuus testataan ennen tuotantokäyttöön ottamista. (=TTT 5.M.3) Käyttöjärjestelmien, varusohjelmistojen ja sovellusten käyttö ja versionhallinta on kontrolloitu ja dokumentoitu.

Tietoverkkoon ja -järjestelmään voidaan asentaa tai liittää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita. (=TTT 5.D.5) Vaatimusta täydentävät kriteerit (STO I: 110.0, STO I:508.0, STO I:703.0)

Vaatimus 3: Huoltoprosessissa on oltava kuvattuna menettely miten tiedot suojataan huoltotilanteissa ja miten ne poistetaan. (~STO I: 507.0)

Luvan asentamiseen antaa verkkoympäristöstä vastaava tietohallintopäällikkö sen jälkeen kun liittämisen riskiarvio on tehty ja uuden laitteen tai ohjelmiston riittävistä turvaominaisuuksista on varmistuttu. Ohjelmisto ei saa olla sellainen, että sen toimivuuden varmistamiseksi pitäisi purkaa palomuurisääntöjä siten, että verkon riskitaso nousee. Hallittu ympäristön ylläpito edellyttää dokumentaatiota ja riittävää ajantasaista ohjeistusta. Vaatimusta täydentävä kriteeri (STO I:703.0).

Vaatimus 4: Organisaatiossa on sovittu, että Solaris-käyttöjärjestelmän tietoturva-asetukset kovennetaan käyttämällä Solaris security toolkit -työkalua ja Windows Server 2003 -järjestelmät käyttämällä CIS:n ohjeiden perusteella tehtyä Group Policyä. Kovennuksilla vähennetään eri mahdollisesti eri palveluihin liittyvien haavoituksien hyväksikäyttöä järjestelmään murtautumisessa. Vaatimusta täydentävä kriteeri (STO I:502.0).

Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset voidaan ja tulee asentaa välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa. (~TTT 5.D.3).

Käyttöjärjestelmien, varusohjelmistojen ja sovellusten käyttö ja versiohallinta on analysoitu, kuvattu, testattu ja kontrolloitu.

Vaatimus 6: Tietohallinto vastaa ohjeistuksesta. Ratkaisu pitää laiteympäristön vakaana ja dokumentaation hallittuna. Palvelusopimuksissa on sovittava menettelytavat. Tämä tarkoittaa käytännössä, että muilla kuin valmisohjelmistoilla on testiympäristö tai kehitysympäristö, jossa testi voidaan suorittaa.

Ohjelmistojen hankinnoissa on huomioitava, ettei hankita sellaisia järjestelmiä, jotka ovat riippuvaisia alustan tietystä versiosta. Tällainen ratkaisu saattaa estää tietoturvatuotteiden päivitykset ja lisätä ICT-järjestelmien haavoittuvuutta. Tämä edellyttää hyvin kuvattua ja kontrolloitua prosessia, jonka mukaan toiminta tapahtuu.

Vaatimus 7: Korkeaa turvatasoa vaativissa järjestelmissä tämä on ehdoton vaatimus ja jatkuvasti seurattava asia turvapäivityksien yhteydessä. Järjestelmän päivityksien yhteydessä ei saa tapahtua niin, että jo muutettu kovennus jää pois patch:n asennuksen seurauksena. Vaatimusta täydentävä kriteeri (~STO I:502.0)

Vaatimus 8:Työasematuki käyttää ohjelmistoa, jolla se voi seurata, monellako prosentilla organisaation työasemista tietty päivitys on.

Vaatimus 9: Palvelusopimuksissa on sovittava menettelytavat. Tämä edellyttää hyvin kuvattua ja kontrolloitua prosessia, jonka mukaan toiminta tapahtuu.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 H **Tietoverkkojen eriyttämisellä ja suodatuksella rajataan turva-alueiden välistä liikennettä** (~TTT 5.E & ~STO I:401.0)	
Perustaso	1. Organisaatiossa on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä eriytetään ja suodatetaan. (~TTT 5.E.1) 2. Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. (~TTT 5.E.2, ~STO I:402.0) 3. Organisaatiossa on kirjalliset etäkäyttöperiaatteet. (=TTT 5.E.5, ~STO I:704.0)
Korotettu taso	4. Organisaatiossa on kirjallinen palomuuri- ja liikenteensuodatuspolitiikka sekä kirjallinen sääntöjen päivitysprosessi. (=TTT 5.E.6) 5. Palomuurien tai muiden suodatuslaitteiden säännöstöjen ajantasaisuutta katselmoidaan säännöllisesti. (=TTT 5.E.7)
Korkea	6. Tietoverkkoja valvotaan tietoturvapoikkeamien ja -loukkausten varalta ja havaittuihin poikkeamiin puututaan ja ne selvitetään. (=TTT 5.E.10) 7. Tietoverkon turvallisuuden varmistamiseksi edellytetään erillinen hallintaverkko jonka kautta tehdään etänä muutoksia tietoverkon aktiivilaitteisiin. (~STO I:404.0)
Tausta-aineisto	Valtionhallinnon lähiverkkojen turvallisuussuositus VAHTI 2/2001 (päivitys julkaistaan 2009) • Luku 4 Turvaperiaatteet osa-alueittain • Luku 5 Poikkeusoloihin varautuminen Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003 • Luku 3.2 Yhteys Internetiin Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003 • Luku 5 Turvallisen etäkäytön arkkitehtuurin toteuttaminen Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004 • Luku 5.4 Organisaation verkon suojaaminen • Luku 5.5 Työskentely organisaation ulkopuolella Tietoturvallisuuden arviointi valtionhallinnossa. VAHTI 8/2006 • Luku 5 Arviointialueet ISO/IEC 27002 • 11.4.5 Segregation in networks • 11.4.6 Network connection control • 11.4.7 Network routing control • 11.7 Mobile Computing And Teleworking • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking

Esimerkki

Vaatimus 1: Organisaatiolla on eriytetty kolme loogisesti erillistä tietoverkkosegmenttiä: julkisia palveluita sisältävä puoliluotettu verkko (ns. DMZ), työasemat sisältävä työasemaverkko sekä tietovarastoja ja palvelimia sisältävä palvelinverkko, jotka on eristetty palomuurilla. Vaatimusta täydentävä kriteeri (STO I:110.0).

Julkisesta verkosta organisaatioon sisäänpäin tulevaa liikennettä valvotaan, rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” -periaatteella. Myös organisaatiosta julkiseen verkkoon lähtevää liikennettä valvotaan, rajoitetetaan ja suodatetaan. (=TTT 5.E.4)

Liikenteen suodatus on tiedotettu YT-menettelyn mukaan. Siinä on kerrottu mihin pääsyä on rajoitettu sekä perustelu. Työntekijöiden ja asiakkaiden käyttöön voidaan antaa työasemapisteitä, jotka eivät ole organisaation verkossa. Ratkaisu mahdollistaa häiriötilanteita varten toimivan varayhteyden eri tietoliikenneoperaattorin kautta ja yhteys voidaan ottaa tarvittaessa organisaation käyttöön.

Vaatimus 2: Organisaatiossa on sovittu, että ainoastaan tietoturvapäällikkö saa lähettää tietoliikenteen palveluntarjoajalle muutospyyntöjä julkisen verkon palomuuriin. Jokaisesta ulkoisen palomuurin avaussäännöstä on kirjattu palomuurin hallintakäyttöliittymän sääntökohtaiseen kommenttikenttään avauspyynnön tekijä, pyynnön syy sekä voimassaoloaika. Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu ja niistä käy ilmi säännön tarkoitus, voimassaolo ja hyväksyjä. (~TTT 5.E.3)

Vaatimus 3: Etäkäytöstä sovitaan ja se rajoitetaan käytön tarpeen mukaan. Etäkäyttöperiaatteet ovat kirjalliset ja niissä kerrotaan minkälaisilla laitteilla ja mistä verkoista yhteyttä voidaan ottaa sekä mitä järjestelmiä käyttää ja ylläpitää. (=TTT 5.E.9) Etäkäyttöratkaisu ei saa vaarantaa organisaation verkkoympäristöä ja yhteys on suojattava päästä päähän unohtamatta työaseman suojausta. Etäkäyttö edellyttää vahvan käyttäjän tunnistuksen. VIP:n työkalupakissa on kuvattu esimerkkiratkaisu turvallisesta etäkäyttöratkaisusta.

Vaatimus 4: Selkeät ohjeet ja kuvattu prosessi varmistaa hallitun toiminnan.

Vaatimus 5: Säännöllisin välein tehdään katselmointi dokumenttien ja asetuksien paikkansa pitävyyden varmistamiseksi. Havainnot kirjataan ja tarkastus dokumentoidaan. Laitteiden asetukset kovennetaan poistamalla tarpeettomat protokollat ja toiminnallisuudet. Vaatimusta täydentävä kriteeri (~STO I:405.0)

Vaatimus 6: Havaitut poikkeamat selvitetään ja virheelliseen, prosessista poikkeavaan toimintaan puututaan.

Vaatimus 7: Korkean suojaustason tietoverkossa käytetään loukkausten havaitsemiseen ja torjuntaan IPS- tai IDS-järjestelmää.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 I **Pääsynvalvonnalla varmistetaan, että tietoon pääsevät käsiksi vain valtuutetut käyttäjät.** (~TTT 5.F & ~STO I: 501.0)	
Perustaso	1. Tiedon omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan (=TTT 5.F.1, ~STO I:501.0) 2. Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset tunnistamista vaativaan järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. (=TTT 5.F.2) 3. Huonolaatuisten salasanojen käyttö estetään järjestelmäasetuksilla. (=TTT 5.F.3)
Korotettu taso	4. Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. tiedon eri suojatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet. (=TTT 5.F.4) 5. Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan. (=TTT 5.F.5, ~STO I:504.0) 6. Kriittisten palvelujen ja sovellusten käyttöoikeudet hallintaan ja valvotaan keskitetysti.
Korkea taso	7. Jos virastossa käytetään vahvaa käyttäjän tunnistamista, niiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista hyväksytyistä tunnistamismenetelmistä ajantasainen lista. (~TTT 5.F.7) 8. Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti. (=TTT 5.F.8) 9. Tunnistuksen epäonnistumista sekä muita valtuuksien puutteeseen kariutuvia toimenpideyrityksiä tilastoidaan. (=TTT 5.F.9) 10. Kriittisten palvelujen ja sovellusten käyttöoikeudet hallitaan ja valvotaan Suomessa.
Tausta-aineisto	Käyttövaltuushallinnan periaatteet ja hyvät käytännöt, VAHTI 9/2006 • Luku 3 Hyvän käyttövaltuushallinnon edellytysten luominen Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006 • Luku 4.2 Käyttäjien tunnistamisen luotettavuus • Luku 4.3 Palvelutyyppien edellyttämä käyttäjän tunnistamisen luotettavuus. Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008 • Luku 4.12 Pääsyn hallinta ja tunnistaminen Lokiohje, VAHTI 3/2009 • Luku 6 Lokien säilytys, kerääminen ja suojaaminen. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 12.5 Järjestelmien tärkeysluokitus ISO/IEC 27002 • 11.1 Business requirement for access control • 11.1.1 Access control policy • 11.2 User access management • 11.2.1 User registration • 11.2.2 Privilege management • 11.2.3 User password management • 11.2.4 Review of user access rights

Esimerkki

Vaatimus 1: Organisaatiossa on riskianalyysin avulla todettu, että WLAN-vierailijaverkon käyttöön ei tarvita tunnistusta, koska siitä ei pääse organisaation sisäverkkoon.

Organisaatiossa on järjestelmien omistajien hyväksymä järjestelmien tärkeysluokitus, jonka perusteella vaadittava tunnistuksen vahvuus määräytyy. Vaatimusta täydentävä kriteeri (STO I:501.0)

Organisaation verkkopalveluille on määritelty eri tunnistustavat VAHTI 12/2006-ohjeen luvun 4.2 mukaisesti. Tietohallinto esittelee ehdotuksen järjestelmien omistajayksiköille, joka hyväksyy ehdotuksen, jos se on linjassa järjestelmien sisältämien tietojen asettamien vaatimusten kanssa. Uusissa tietojärjestelmissä suositellaan Virtu-luottamuusverkoston tunnistautumisen hyödyntämistä.

Vaatimus 2: Lokit kerätään tiedon omistajan päätöksen mukaisesti järjestelmäkohtaisesti järjestelmän tärkeyden mukaan huomioiden siinä käsiteltävien tietojen asettama suojausvaatimus.

Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen. (=TTT 5.F.6)

Vaatimus 3: Organisaatiossa on kirjallisesti ohjeistettu hyvä salasanakäytäntö salasanan vähimmäispituuksineen. Sen lisäksi niissä tietojärjestelmissä, joissa se on mahdollista, on otettu salasanan laatutarkistus käyttöön (pakolliset erikoismerkit, salasanan pituus).

Vaatimus 4: Organisaatiossa on kirjallinen ohje, jossa kerrotaan periaatteet miten kirjaudutaan verkkopalveluihin ja operatiivisiin järjestelmiin. Näissä ohjeistetaan sallittavien tunnusten ja salasanojen periaatteet sekä lokien tuottamis- ja valvontapolitiikka.

Vaatimus 5: Lokit siirretään toiseen ympäristöön ja ne allekirjoitetaan sähköisesti tiivistefunktiolla.

Vaatimus 6: Noudatetaan ohjeistusta valtionhallinnon käyttövaltuushallinnasta.

Vaatimus 7: Omistaja antaa oikeudet ja myönnetyt oikeudet kirjataan organisaation Service Desk:ssä.

Vaatimus 8: Ohje sisältää kortin hakuprosessin ja sulkemisen. Organisaation henkilöstöhallinto huolehtii korttien hankinnan, jakelun ja sulkemisen sekä pois keräämisen.

Vaatimus 9: Terveystietojärjestelmä ja väestötietojärjestelmä lokittavat myös sen, kuka on käynyt katsomassa sairauskertomuksia tai arkaluontoisia henkilötietoja, jotta tarvittaessa voidaan selvittää, onko henkilöllä ollut peruste nähdä tiedot.

Vaatimus 10: Nämä palvelut ovat YETTS:n näkökulmasta kriittisiä.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 J **Käyttäjätunnukset ja käyttövaltuudet ovat yhdistettävissä niitä käyttävään henkilöön tai rooliin.** (~TTT 5.G)	
Perustaso	1. Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. (~TTT 5.G.1) 2. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu hallintaperiaatteiden mukaisesti. (~TTT 5.G.1) 3. Yksittäisen käyttäjän ja ylläpitäjien käyttövaltuudet on voitava selvittää. (~TTT 5.G.4) 4. Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään. (=TTT 5.G.10) (~STO I:709.0)
Korotettu taso	5. Organisaatiossa on kirjallinen käyttövaltuuspolitiikka ja hallintaprosessi. (=TTT 5.G.6) 6. Jokaisella käyttövaltuudella on omistaja. (=TTT 5.G.7) 7. Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet poistetaan. (~TTT 5.G.8) 8. Myöntöprosessista jää jälki, millä perusteella ja kenen toimesta käyttäjälle on myönnetty käyttövaltuus. (~TTT 5.G.9)
Korkea taso	9. Ylläpito- ja pääkäyttäjäoikeuksien käyttöä ja määrää seurataan ja tilastoidaan. (=TTT 5.G.11) 10. Käyttövaltuuksien myöntämiseen ja poistoon kuluvaa aikaa seurataan ja tilastoidaan. (=TTT 5.G.12) 11. Organisaatiossa on dokumentoitu menettely käyttäjätunnuksen tai käyttövaltuuksien välittömään poistoon tai passivointiin. (=TTT 5.G.13)
Tausta-aineisto	Käyttövaltuushallinnan periaatteet ja hyvät käytännöt, VAHTI 9/2006. • Luku 2.2 Käyttövaltuusrekisterin suunnitteluvaatimus. • Luku 3 Hyvän käyttövaltuushallinnon edellytysten luominen. • Luku 4 Hyvää hallintokäytäntöä tukevan käyttövaltuuksien hallintaympäristön arkkitehtuuri • Liite 1 Organisaatiorajat ylittävät käyttövaltuudet Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008 • Luku 4.5 Valtuuttaminen Lokiohje, VAHTI 3/2009 • Luku 3 Lokit ja lokityypit ISO/IEC 27002 • 11.1 Business Requirement For Access Control • 11.1.1 Access control policy • 11.2 User access management • 11.2.1 User registration • 11.2.2 Privilege management • 11.2.3 User password management • 11.2.4 Review of user access rights

Esimerkki

Vaatimus 1: Käyttövaltuuksien on perustuttava palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö on teknisesti estettävä ilman tarpeetonta viivytystä perusteen päätyttyä. Uuden henkilön tullessa viraston palvelukseen ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta ja sähköiseen vahvaa tunnistamista vaativaan palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää. (=TTT 5.G.5)

Organisaatiossa on sovittu, että kaikki virka- tai työsopimussuhteessa olevat saavat automaattisesti käyttöönsä työasematunnuksen, mutta tunnuksia sovelluksiin tai palvelimiin annetaan vain esimiehen katsoessa sen työtehtävien osalta tarpeelliseksi. Käyttövaltuudet ovat henkilö- tai roolikohtaisia. (=TTT 5.G.2)

Vaatimus 2: Virtu-luottamusverkostoon kytketyt käyttäjätunnukset ovat henkilökohtaisia.

Vaatimus 3: Organisaatiossa on käytössä identiteetinhallintajärjestelmä, jonka avulla henkilön käyttäjätunnukset poistetaan automaattisesti kun henkilön työ- tai virkasuhde päättyy.

Vaatimus 4: Organisaatio ylläpitää oikeuksien myöntämiseen liittyvää kirjanpitoa tai ”tikettejä” Service Desk –järjestelmässä, josta asia voidaan selvittää. Tunnuksien hakeminen pitää arkistoida ja arkistoituun kappaleeseen pitää liittää merkintä kun tunnus aikanaan poistetaan tai passivoidaan.

Vaatimus 5: Potentiaalisen työntekijän henkilöllisyys tarkastetaan jo haastatteluvaiheessa valokuvallisesta henkilöllisyystodistuksesta. Sähköisessä asioinnissa käyttäjäksi voi rekisteröityä verkkopankkitunnuksien avulla.

Vaatimus 6: Periaatteet ja prosessi on kuvattu organisaation käyttämällä prosessinkuvausmenetelmällä.

Vaatimus 7: Organisaatiossa on sovittu, että järjestelmän omistaja omistaa myös siihen järjestelmään tehdyt valtuudet, on ne henkilö- tai roolikohtaisia tai teknisten järjestelmien välisiä tunnuksia.

Vaatimus 8: Tietojärjestelmän omistaja käy vuosittain läpi järjestelmän tunnukset ja valtuudet, ja esimerkiksi työtehtävien vaihtumisen vuoksi vanhentuneet valtuudet poistetaan.

Vaatimus 9: Myöntäminen kirjataan Service Desk tai Help Desk -järjestelmään.

Vaatimus 10: Myöntämisen yhteydessä tarkastetaan asia. Prosessi sisältää tähän liittyvän kontrollin.

Vaatimus 11: Seurannalla vältetään turhia tunnuksia ja seuranta on hallintaprosessin yksi kontrolli.

Seurataan läpimenoaikaa. Pitkä aika voi olla riski henkilön lähtiessä pois työsuhteen päättyessä. Service Desk- tai Help Desk -toimintojen sekä henkilöstöhallinnon (HR) välisen yhteistyön on oltava saumatonta, etteivät tarpeettomasti voimassaolevat käyttöoikeudet ja -tunnukset muodosta riskiä organisaatiolle.

Organisaatiossa on hyväksytty menettely, jossa henkilöstöhallinnosta vastaava voi puhelinsoitolla pyytää välittömästi käyttötuelta henkilön etäkäyttö- ,työasema- ja tietojärjestelmien tunnusten passivointia.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 K **Organisaation ICT-ratkaisut on suojattu haittaohjelmilta.** (~TTT 5.H & ~STO I:503.0)	
Perustaso	1. Organisaatiossa suodatetaan haittaohjelmia sekä työasematasolla, palvelimilla että kaikissa sähköpostin ja www-liikenteen sisääntulo- ja ulosmenopisteissä. (=TTT 5.H.1, ~STO I:110.0) 2. Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti. (=TTT 5.H.2)
Korotettu taso	3. Käyttäjiä on ohjeistettu huoneentauluna, miten haittaohjelmia levittäviä sähköposteja voidaan yrittää tunnistaa ja mitä tehdä epäiltäessä haittaohjelman tarttuneen työasemaan. (=TTT 5.H.3) 4. Haittaohjelmakuvausten ajantasaisuutta valvotaan. (=TTT 5.H.4)
Korkea	5. Työasema tai palvelin ei saa kytkeytyä korkean turvallisuustason verkkoihin, ellei niiden puhtautta haittaohjelmista ole varmistettu. (=TTT 5.H.5) 6. Haittaohjelmasuodatuksen kattavuutta mitataan ja seurataan. (=TTT 5.H.6)
Tausta-aineisto	Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004 • Luku 5 Kuinka välttää tartunta • Liite 3 Käyttäjän pikaopas ISO/IEC 27002 • 10.4 Protection Against Malicious And Mobile Code 10.6 Network Security Management
Esimerkki	**Vaatimus 1**: Tietoverkkoon tuleva ja uloslähtevä tietoliikenne tarkastetaan haittaohjelmien varalta. Keskeisiä sisääntulopisteitä ovat käyttäjän kannalta sähköposti ja internet-selailu. Organisaatiossa on riskianalyysin avulla todettu, että työasematasolla tarvitaan haittaohjelma-suojausta ainoastaan Windows-pohjaisissa työasemissa ja niissä älypuhelimissa, joissa on käytössä organisaation sähköposti- ja kalenteripalvelut. Lisäksi sähköpostipalvelimeen ja www-välityspalvelimeen asennetaan haittaohjelmasuodatus. Haittaohjelmien torjunta suositellaan toteutettavaksi yhdyskäytävätason ratkaisuna, jossa samalla tuotteella voidaan tutkia kaikkien keskeisten tietoliikenneprotokollien läpi kulkeva tietoliikenne. **Vaatimus 2**: Työasemissa on käytössä automaattipäivitys. Mikäli päivitykset eivät ole toimineet esimerkiksi kolmeen päivään, järjestelmä ilmoittaa päivitysten mahdollisesta epäonnistumisesta. Palvelimien haittaohjelmien torjuntajärjestelmien muutokset testataan ennen merkittäviä muutoksia. **Vaatimus 3**: Perehdyttämis- ja täydennyskoulutuksessa valistetaan henkilöstöä suhtautumaan epäilevästi tuntemattomista osoitteista tuleviin viesteihin, jotka eivät näytä liittyvän työtehtäviin, ja poistamaan ne ilman mukana seuraavan liitetiedoston avaamista. **Vaatimus 4**: Verkon työasemia ja palvelimia seurataan automaattisesti, jotta varmistutaan päivitysten onnistumisesta. Ne työasemat, jotka eivät jostain syystä ole automaattisen päivityksen piirissä, päivitetään manuaalisesti. Tätä varten pitää Help Desk:ssä olla lista näistä erikoistyöasemista. Listan ylläpidosta vastaa tietohallintopäällikkö. **Vaatimus 5**: Verkkoon kytkeminen estetään teknisesti ristikytkennässä ja ohjelmallisesti pitämällä kirjaa mitkä verkko-osoitteet saavat liittyä korkean tason verkkoon. **Vaatimus 6**: Ylläpidetään prosenttilukua kuinka moni työasema on automaattipäivityksen piirissä ja kuinka moneen tehdään manuaalinen päivitys.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 L **Tietoturvariskien realisoituminen estetään käyttämällä fyysisen turvallisuuden menetelmiä ICT-ympäristön suojaamiseen.** (~TTT 5.I)	
Perustaso	1. Organisaatiossa on tunnistettu omien tilojen tarvitsema suojausluokka ja eriytetty eri suojausluokkaa vaativat osat rajoittamalla kulkua tilojen välillä. (=TTT 5.I.1, ~STO I: 301.0) 2. Organisaatiossa on sovittu henkilö- tai roolitasolla, kenellä on pääsy ICT-laitetiloihin, ja pääsynvalvonta sekä toiminnan valvonta tiloissa on organisoitu tämän mukaisesti. (=TTT 5.I.2, =TTT 5.I.6, ~STO I:301.0 & STO I:302.0) 3. Tärkeät laitteet ja laitetilat on suojattu ympäristötekijöitä vastaan (murto, palo, lämpö,kosteus, kaasut, vesi ja pöly). (~STO I:304.0)
Korotettu taso	4. Tilojen eriytyksen tekniset ratkaisut suojausluokkiin on dokumentoitu. (=TTT 5.I.3) 5. Tietoliikennelaitteiden, -yhteyksien ja kytkentäpisteiden sijainti on otettu huomioon suojausluokittelussa. (=TTT 5.I.4) Organisaatiolla on testattu suunnitelma ICT-palvelujen tuotannon siirtämisestä toisiin tiloihin mikäli nykyiset tilat muuttuvat käyttökelvottomiksi.
Korkea taso	6. Tiloja ja niissä kulkua seurataan (tilanteen mukaan), valvotaan automaattisesti ja valvontamenettely on dokumentoitu. (=TTT 5.I.5) 7. Toimitilajärjestelyt mahdollistavat korkean tason palveluille fyysisesti riittävän kaukana sijaitsevan varatoimipaikan, jossa ICT-toimintaa voidaan jatkaa jos varsinainen toimipaikka muuttuu käyttökelvottomaksi.
Tausta-aineisto	Sisäasiainministeriön asetus S1-, S3- ja S6-luokan kalliosuojista sekä S3-luokan teräsbetonisesta väestönsuojasta. Pelastuslaki (468/2003) 65 §. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 12.2 Toimitilojen luokitus. Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002 • Luku 3 IT-laitetilojen tietoturvatoimenpiteet osa-alueittain. Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008 • Liite 5 Pääsyn hallinnan toteuttaminen EU määräyksen mukaisesti Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003 • Luku 5 Uhkien määrittely ja tunnistaminen Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Liite 2. Tietoturvavastuut rooleittain BS 25999/2006 – Business Continuity Management – Osa 1 • Identification of critical activities ISO/IEC 27002 • 9.1 Secure Areas • 9.1.1 Physical Security Perimeter • 9.1.2 Physical Entry Controls • 9.1.3 Securing Offices, Rooms, And Facilities

Esimerkki

Vaatimus 1: Jatkuvuus- ja valmiussuunnittelun pohjana on organisaation tärkeysluokka. Siitä johdetaan tarvittavat suojausratkaisut. Toimitilat erotellaan kulkualueiksi siten, että ulkopuoliset eivät pääse työtiloihin ja työtiloista pääsevät ICT-tiloihin vain ne henkilöt, joiden työtehtäviensä vuoksi on niihin päästävä.

Vaatimus 2: Kulunvalvontajärjestelmä perustuu roolien hallinnointiin. Ulkopuolisia tukipalveluja ovat tyypillisesti mm. siivous, vartiointi ja kiinteistöhuolto. Palveluntuottajien liikkumista valvotaan ja se rajoitetaan mahdollisuuksien mukaan työaikana tapahtuvaksi. Tiloissa on tekninen valvonta, jolla seurataan niissä tapahtuvaa toimintaa.

Vaatimus 3: Tärkeät laitteet sijoitetaan laitetilaan, joka on suojattu VAHTI 5/2004 -ohjeen luvussa 7 kuvatulla tavalla.

Tilat suunnitellaan ja rakennetaan siten, että niiden kestävyydessä huomioidaan esimerkiksi ilkivalta, erilaiset aseelliset hyökkäykset sekä terrorismi.

Vaatimus 4: Ratkaisut on dokumentoitu. Ratkaisut kuten muu turvatekniikka ei ole julkista tietoa.

Vaatimus 5: Laitteet sijoitetaan siten, että niitä voidaan valvoa, ja ne ovat lukituissa tiloissa.

Vaatimus 6: Tilat voivat olla esimerkiksi organisaation toinen toimipiste toisella paikkakunnalla. Tämä on huomioitu jatkuvuussuunnitelmassa.

Vaatimus 7: Ratkaisut on dokumentoitu.

Vaatimus 8: Esimerkiksi Suomen Huoltovarmuusdata Oy tarjoaa valtion ja yksityisen sektorin huoltovarmuuskriittisille organisaatioille huipputurvallista konesalitilaa sekä tietoaineistojen tallennus- ja suojakopiopalveluita.

Korkean tason kriittisten palvelujen ylläpitäminen on mahdollista ilman palveluverkoston ulkopuolisia palveluja (tuki-infrastruktuuri) ja resursseja (sulkutila). Vaatimus huomioidaan tilojen suunnittelussa.

Suojarakentamisen yksityiskohtaisia lujuuksia ja materiaalivahvuuksia on lueteltu sisäasiainministeriön antamassa asetuksessa.

ICT-JATKUVUUDEN HALLINTA: TIEDON TURVAAMINEN	
5 M **Varmuuskopioinnilla estetään tiedon katoaminen organisaatiosta ja vähennetään erilaisten häiriötilanteiden vaikutusta organisaation toimintaan.** (~TTT 5.J, ~STO I:710.0)	
Perustaso	1. Organisaatiossa on vastuutettu ja organisoitu varmuuskopioiden ottaminen. (=TTT 5.J.1) 2. Organisaatiossa on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti sekä pidetään kirjaa. Myös varmuuskopioiden palauttaminen on suunniteltu. (=TTT 5.J.2) 3. Järjestelmien varmuuskopioiden palautusta testataan säännöllisesti. (=TTT 5.J.1)
Korotettu taso	4. Organisaatiossa on kirjallinen varmuuskopiointipolitiikka ja -prosessi, jotka on muodostettu ottaen huomioon toiminnan vaatimukset ja jossa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana. (=TTT 5.J.3) 5. Organisaatiossa otetaan tärkeimmistä järjestelmistä suojakopioita, joita säilytetään toisessa rakennuksessa eri palotilassa kun varsinaisia varmuuskopioita. (=TTT 5.J.4)
Korkea taso	6. Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan. (=TTT 5.J.6)
Tausta-aineisto	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 11.8 Tietoaineiston varmuuskopiointi Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000 (Ohje uusittavana) Arkistolaitoksen ohje 62/40/2003 asiakirjojen suojaamisesta poikkeusoloissa ISO/IEC 27002 10.5.1 Information back-up
Esimerkki	**Vaatimus 1**: Järjestelmän omistaja vastaa siitä, että hänen omistamansa järjestelmän tiedot varmistetaan niiden arvon mukaisesti. Varmistamisen tiheys on suunniteltava siten, että riittävän monta varmistussukupolvea on olemassa. Esimerkiksi Työeläkelaitokset ovat julkaisseet tähän liittyvän suosituksen. Vastuu asiakirjojen suojelusuunnitelman valmistelusta ja toimeenpanosta kuuluu organisaation johdolle. **Vaatimus 2**: Organisaation tieto-omaisuus on arvotettu ydintoimintojen näkökulmasta. Jokaisen organisaation tulee laatia oma asiakirjojen suojelusuunnitelma, jonka ajantasaisuus tarkistetaan määräajoin. Suunnitelman tulee olla joko erillisenä tai sisällytettynä organisaation valmius-, pelastus- tai muuhun vastaavaan suunnitelmaan. Myös tietoliikennelaitteiden (reitittimet, runkokytkimet) asetustiedot tulee säännöllisesti varmuuskopioida suurten muutosten jälkeen. **Vaatimus 3**: Kerran puolessa vuodessa testataan jonkin varmistustaltion palautusta testilaitteeseen. **Vaatimus 4**: Korkean tason tietojärjestelmästä otetaan viikottain täysvarmistus ja joka yö varmistetaan muuttuneet tiedot, koska järjestelmän vaatimuksena on kyky palata virheen jälkeen edellisen päivän tilanteeseen. Järjestelmän salaamaton suojakopio voidaan siirtää toiseen rakennukseen vain oman työntekijän saattamana tai kuljettamiseen käytetään arvokuljetuspalvelua. **Vaatimus 5**: Suojakopioinnissa voi hyödyntää TELA:n (Työeläkelaitokset) suositusta suojakopioinnista. **Vaatimus 6**: Osana operatiivista toimintaa seurataan millaisia tietoja yleisimmin palautetaan ja miksi. Organisaation toimintaa ja ohjeistusta kehitetään tilastoinnista kerättävän tiedon perusteella.

ICT-JATKUVUUDEN HALLINTA: HÄIRIÖTILANTEIDEN HALLINTA	
5 N **Tapahtumien valvonnalla havaitaan tietoturvapoikkeamat ja mahdollistetaan niiden selvittäminen.** (~TTT 5.K)	
Perustaso	1. Tietoaineistojen, henkilötietojen, sähköisten viestien, sähköpostien, tunnistamistietojen, lokien sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan säädösten mukaisesti. (=TTT 5.K.1, ~STO I:504.0) 2. Laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan mahdollisen tietoturvapoikkeamien selvittämiseksi. (=TTT 5.K.2)
Korotettu taso	3. Organisaatiossa on kirjallinen lokienkeräys-, hälytys- ja seurantapolitiikka, joka on muodostettu ottaen huomioon toiminnan vaatimukset. (=TTT 5.K.3)
Korkea taso	4. Lokien seurannan perusteella muodostetaan tilannekuvaa, havaitaan tietoturvapoikkeamia ja kehitetään toimintaa. (=TTT 5.K.4)
Tausta-aineisto	Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006 • Luku 5 Loki- ja muutoshistoriatiedot. Lokiohje, VAHTI 3/2009 • Luku 4 Lokien käsittelyn vastuut ja käsittelyprosessi.. ISO/IEC 27002 • 10.10 Monitoring • 10.10.1 Audit logging • 10.10.2 Monitoring system use • 10.10.3 Protection of log information • 10.10.4 Administrator and operator logs • 10.10.5 Fault logging • 10.10.6 Clock synchronization
Esimerkki	**Vaatimus 1**: Teknisen valvonnan periaatteissa kuvataan mitä valvontakeinoja on käytössä ja miksi. Teknisessä valvonnassa noudatetaan voimassa oleviea lakeja. Tekninen valvonta käsitellään YT-menettelyn mukaan. **Vaatimukset 2 ja 3**: Organisaatiossa kaikki laitteet ja tietojärjestelmät kirjoittavat lokinsa keskitettyyn lokipalvelimeen, josta ylläpito tarvittaessa selvittää häiriöiden ja tietoturvapoikkeamien syitä. Tekninen valvonta on käsiteltävä YT-menettelynä. **Vaatimus 4**Järjestelmien lokeista voidaan esimerkiksi käynnistää ongelmanselvitys, selvittää käyttöoikeuksien käyttöä sekä mahdollisia tietoturvapoikkeamia.

ICT-JATKUVUUDEN HALLINTA: HÄIRIÖTILANTEIDEN HALLINTA	
5 O **Tietojärjestelmiä kohtaaviin häiriöihin on varauduttu nopean palautumisen varmistamiseksi.** (~TTT 5.L)	
Perustaso	1. ICT-järjestelmien häiriöiden selvitys ja niistä toipuminen on organisoitu ja vastuutettu. (=TTT 5.L.2) 2. Organisaatiossa on yleinen toipumisstrategia ja -suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille. (=TTT 5.L.3) 3. Palvelinympäristöjen ja tietoliikenneinfrastruktuurin vikasietoisuus vastaa ydintoimintojen ja ympäristön normaaliolojen häiriöiden hallinnan asettamia vaatimuksia.
Korotettu taso	4. Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat. (=TTT 5.L.4) 5. Kriittisten palvelujen verkko-, palvelin- ja laiteympäristöt varmennetaan esimerkiksi kahdentamalla siten, että yksittäinen vika ei voi aiheuttaa palvelutason laskua alle kriittisten toimintojen määrittämän palvelutason. 6. Organisaatio on yhdessä palveluntoimittajan kanssa analysoinut, suunnitellut ja sopinut tietoliikennepalvelujen priorisoinnin ja muutokset erityistilanteissa.
Korkea taso	7. Palvelinympäristöjen vikasietoisuus vastaa erityistilanteiden ja poikkeusolojen vaatimuksia. 8. Verkkoympäristöt ja tietoliikennepalvelut varmennetaan siten, että yhden operaattorin palvelutason lasku ei aiheuta toiminnan määrittämän palveluntason laskua. 9. Organisaatio on suunnitellut, sopinut ja testannut myös palveluverkoston tietoliikennepalvelujen priorisoinnin ja muutokset poikkeusoloissa.
Tausta-aineisto	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Liite 1 Mallipolitiikat ja suunnitelmarungot, • Toipumissuunnitelman runko s. 91 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 • Luku 5.7 Järjestelmäluokkien erityispiirteet • Luku 10.6 Erityyppisten järjestelmien toipumisen erityispiirteitä Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006 • Liite 6 Arviointilomakkeistot Viestintäverkkojen ja viestintäpalveluiden varmistaminen. Opas käyttäjille, PTS 2/2005 ISO/IEC 27002 • 10.2 Third Party Service Delivery Management • 10.6 Network Security Management • 10.1.1 Documented operating procedures
	ISO/IEC 27002 • 13 Information security incident management • 13.2 Management Of Information Security Incidents And Improvements BS 25999/2006 – Business Continuity Management – Osa 1 • Identification of critical activities BS 25999/2007 – Business Continuity Management – Osa 2 • 3.3 Embedding BCM in the Organization's Culture • 4 Implementing and Operating the BCMS

Esimerkki

Vaatimus 1: Organisaatiossa tietohallinnon käyttöpäällikkö vastaa ICT-palveluiden toiminnasta. Käyttöpäällikkö on nimennyt kullekin ICT-palvelulle teknisen vastaavan, jonka tehtävänä on ryhtyä toipumissuunnitelman mukaisiin toimenpiteisiin. Organisaation omassa hallinnassa oleva ICT-infrastruktuuri, laitteet, resurssit ja osaaminen on mitoitettu normaaliolojen häiriöt ja erityistilanteet huomioon ottaen.

Vaatimus 2: Organisaatiossa on valittu yleiseksi toipumisstrategiaksi palveluiden ulkoistus ja riittävät palvelutaso-sopimukset. Järjestelmäkohtaisten toipumissuunnitelmien valmistelusta vastaa tällöin palveluntarjoaja. Tilaaja arvioi toipumissuunnitelman testaamalla sitä.

Vaatimus 3: Järjestelmien tekniset ja toiminnalliset vaatimukset on tunnistettu ja niiden ratkaisut on määritelty ja riskit on arvioitu. Erikseen valittuihin työasemiin on asennettu erillinen tietoliikenneyhteys jonka kautta voi päästä yleiseen tietoverkkoon (varayhteys).

Jos organisaation toimitiloissa on toimintoja, jotka eivät saa pysähtyä sähkön puuttumiseen, on tiloihin suunniteltava varavoima. UPS:n käyttö on realistista alle tunnin katkoja vastaan. Mikäli riskinä on pidempi katko, niin varavoimaratkaisu on huomioitava sähkönsaannin varmistamiseksi. Järjestelmät on kyettävä ajamaan alas hallitusti UPS:n käyttöaikana. Vaatimusta täydentävä kriteeri (STO I:304.0).

Vaatimus 4: Organisaatiossa on valittu yleiseksi ICT-palveluiden toipumisstrategiaksi varalaitteiden käyttö. Tämän vuoksi on olemassa suunnitelmat siitä, miten tärkeimmät palvelut voidaan siirtää olemassa olevaan varalaitteeseen jos tilanne niin vaatii.

Vaatimus 5: Järjestelmän testausympäristö voidaan ottaa tuotantokäyttöön mikäli järjestelmän kriittisyysvaatimus edellyttää erillisen testiympäristön olemassaolon. Tähän liittyen kriittisten palveluympäristöjen sovellushallinta on määritelty, ohjeistettu ja valvottu. Vaatimusta täydentävä kriteeri (STO I:705.0).

Vaatimus 6: Organisaation ydintoimintojen tarvitsemat järjestelmät on tunnistettu.

Vaatimus 7: Palveluntoimittajan kanssa on yhdessä sovittu tietoliikenteen, -laitteiden ja henkilöstön käyttö häiriötilanteissa. Organisaation ICT-arkkitehtuuri edellyttää, että palveluntoimittaja tarjoaa kahdennetut ympäristöt ja palvelusopimuksissa on määritelty palvelun aikakriittisyys. Kriittisten palvelujen tietotekniset ympäristöt varmennetaan katkeamattomalla sähkönsyötöllä vähintään neljän tunnin sähkökatkoa varten.

Vaatimus 8: Tietoliikenne kahdennetaan fyysisesti kahta eri reittiä pitkin kahden eri operaattorin toimesta. Asia edellytetään tarjouskilpailutuksessa. Kriittisten palvelujen tietotekniset ympäristöt varmennetaan varavoimalla tai varavoimaliitännöillä siten, että sähkönjakelu voidaan käynnistää tunnin kuluessa ja ylläpitää sitä viikon ajan.

Vaatimus 9: Organisaation on tunnettava koko palveluketjun toimivuus ja osana omaa jatkuvuus- ja varautumisharjoittelua käytävä läpi sen toimivuus eri tilanteissa.

LIITE 2.6 MITTAAMINEN

MITTAAMINEN	
6 A **Jatkuvuuden hallinnan ja tiedon turvaamisen toteutumista ja tarkoituksenmukaisuutta seurataan ja arvioidaan** (~TTT 6.1, =SOPIVA 28)	
Perustaso	1. Jatkuvuuden, tiedon turvaamisen ja varautumisen tavoitetason saavuttamista seurataan TTS-prosessissa. (~TTT 6.1.1, ~STO I:105.0) 2. Palvelutuottajien tuottamien tietojenkäsittelypalveluiden katselmoinnit kuuluvat toimintatapaan. 3. Auditoinnit tai itsearvioinnit toteutetaan säännöllisesti ja ne ovat suunniteltuja sekä johdon hyväksymiä. (=TTT 6.1.2)
Korotettu taso	4. Sisäinen tarkastus toimintona (tarkastussuunnitelma) ja esimiehet suorittavat säännöllisesti tuotteiden, palvelujen, toimintojen, prosessien ja järjestelmien riskiarvioinnin sekä jatkuvuuden hallinnan tarkastuksia. (~TTT 6.1.1, (~STO I:701.0) 5. Tietoturva-auditointeja tai arviointeja tehdään vuosittain suunnitelmallisesti osana muuta auditointia. (=TTT 6.1.4) 6. Palveluverkoston varautumisen ja tiedon turvaamisen toimenpiteiden katselmointeja ja auditointeja toteutetaan. 7. Virastossa on kirjallinen valtionhallinnon mallin mukainen johdon hyväksymä auditointi- tai arviointiprosessi, jossa on mm. määritelty auditoijien tai arvioijien pätevyysvaatimukset. (=TTT 6.1.5) 8. Auditointien tai arviointien tuottamista suosituksista pidetään koko organisaation tasolla kirjaa ja kehittämistoimenpiteiden toteutumista seurataan. (=TTT 6.1.9, ~STO I:105.0)
Korkea taso	9. Poikkeamahavaintojen pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa kehittämistoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle. (=TTT 6.1.6, ~STO I:104.0) 10. Tietoturva-auditoinneissa tai arvioinneissa edellytetään käytettäväksi myös ulkopuolisia resursseja. (=TTT 6.1.8)
Tausta-aineistoa	Tietoturvallisuuden hallintajärjestelmän arviointisuositus VAHTI 3/2003 • Luku 5 Hallintajärjestelmän arviointiprosessi Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 • Luku 2.7 Arviointi ja seuranta Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006 • Luku 4 Tietoturva-arvioinnin periaatteita Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006 • Luku 4 Tietoturvariskien hallinta sekä tietoturvallisuuden arviointi ja mittaaminen ISO/IEC 27002 • 10.2.1 Service delivery • 10.2.2 Monitoring and review of third party services • 15.3 Information Systems Audit Considerations • 15.3.1 Information systems audit controls BS 25999/2007 – Business Continuity Management – Osa 2 • 5 Monitoring and reviewing the BCMS • 5.1 Internal audit

Esimerkki

Vaatimus 1: Organisaatiossa on auditiontisuunnitelma, jonka mukaisesti esimerkiksi vuonna 2010 auditoidaan organisaatiossa jatkuvuuden hallintaprosessit, vuonna 2011 kaikkien ulkoistus- ja palvelutasosopimusten tietoturvaan ja jatkuvuuteen liittyvät vaatimukset ja vuonna 2012 kriittiset tietojärjestelmät. Organisaatio voi tehdä auditoinnit esimerkiksi vuosikellon mukaisesti.

Vaatimus 2: Asiakaskatselmointi suoritetaan sovittuna aikana ja siinä käsitellään sovittujen toimenpiteiden tilanne ja sovitaan uusista toimenpiteistä, joita jatkuvuudenhallinnan osalta olisi perusteltua ryhtyä tekemään. Asiakaskatselmoinnilla seurataan toimenpiteiden edistymistä.

Vaatimus 3: Organisaation johto on hyväksynyt periaatteet, joiden mukaisesti yksiköt arvioivat joka toinen vuosi oman toimintansa tietoturvallisuutta ja raportoivat tuloksista.

Vaatimus 4: Mittaustulokset on analysoitava, eikä pelkästään seurattava lukumääriä, myös poikkeustilanteiden osalta. Auditoinneista mittareina voi olla negatiivisten löydösten määrä ja vakavuus.

Mittarit: käytettävyysprosentit palvelukohtaisesti. Käyttäjän kokema palvelunlaatu: palveluun vaikuttavat palvelut (esim. sähköposti, mobiilisähköposti ei toimi => 80 %:n saatavuus). Poikkeamien määrät. Suunnittelu on tärkeää mittauksessa: päätetään minkälaista ongelmaa halutaan pienentää ja viritetään mittarit seuraamaan ongelman parantumista.

Mittari käyttöpalvelun osalta: K= (PA-KA+EH)/PA*100 (PA mitattava aika, KA katkojen aika, EH yhteensä katkoihin kulunut aika). Järjestelmillä voi olla riippuvuuksia, joiden takia kaikkia päivityksiä ei voida asentaa. Mittaritieto viedään järjestelmänkehitykseen ja arkkitehtuurisuunnitteluun muutoksen aikaansaamiseksi.

Mittaus prosessina on tärkeä jotta saadaan sisältöä kehittämistoimenpiteiksi. Mittari 1: kuinka suuri osa kehittämisehdotuksista muuttuu toimenpiteiksi. Mittari 2: kuinka suuri osa sovelluskehitystyöstä menee virheiden korjaamiseen.

Mittaamiseen olisi hyvä saada yhteinen kehikko. Mittari: Montako korjauskierrosta toimitettu järjestelmä joutuu käymään ensimmäisen toimituksen jälkeen.

Vaatimus 5: Organisaation päättämä toimija (esim. sisäinen tarkastus) tekee tietoturvallisuuteen liittyvän kokonaisarvioinnin esimerkiksi VAHTI 8/2006 -ohjeen liitteiden avulla.

Vaatimus 6: TTS-kausi sisältää auditointisuunnitelman, joka tehdään yhteistyössä sisäisen tarkastuksen kanssa päällekkäisen työn välttämiseksi. Tietoturvallisuuden resursointia erityistilanteita ja poikkeusoloja varten seurataan organisaation toiminta- ja taloussuunnittelun toteutumassa. (=TTT 1.2.6)

Vaatimus 7: Palveluntoimittajan kanssa sovitaan auditointirytmi ja kirjataan asia TTS-koordinaation varmistamiseksi. Organisaation turvallisuusjohto koordinoi auditoinnit ja tarkastukset.

Vaatimus 8: Organisaation käyttämä arviointiprosessi ja arvioitsijoiden pätevyydet voivat olla VAHTI 8/2006 -ohjeen mukaiset. Organisaatio voi edellyttää esimerkiksi ISACA:n antamia pätevyyttä osoittavia sertifikaatteja.

Vaatimus 9: Riskienhallinnan seurantaraporttiin kirjataan toimenpiteet ja niiden arvioitu vaikutus. Uudet turvakontrollit kirjataan ja niiden toimivuutta toimintaprosessissa seurataan. Vaatimusta täydentävä kriteeri (STO I:104.0).

Vaatimus 10: Ulkopuolisia resursseja tarvitaan teknisen puolen ratkaisujen arviointiin, sillä hallinnossa on liian vähän eri teknisten osa-alueiden auditointikokemuksen omaavia asiantuntijoita.