VALTIOVARAINMINISTERIÖ

ICT -varautumisen vaatimukset

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2012 VAHTI

VALTIOVARAINMINISTERIÖ

ICT-varautumisen vaatimukset

Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2012 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Taina Ståhl

ISSN 1455-2566 (nid.)
ISBN 978-952-251-374-8 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-375-5 (PDF)

YMPÄRISTÖMERKKI
MILJÖMÄRKT
441 729
Painotuote

Suomen Yliopistopaino Oy
Juvenes Print, 2012

VALTIOVARAINMINISTERIÖ **Ohje** VM/1619/00.00.00/2012

25.9.2012

Ministeriöille, virastoille ja laitoksille

ICT-VARAUTUMISEN VAATIMUKSET -OHJE

Valtiovarainministeriön *ICT-varautumisen vaatimukset -ohjeen* tavoitteena on tehostaa ja yhdenmukaistaa ICT-varautumista ministeriöissä ja hallinnonalojen organisaatioissa. Valtioneuvoston tietoturvallisuutta koskevan periaatepäätöksen 26.11.2009 mukaan yksi kehittämisen painopisteistä on *ennaltaehkäisy ja varautuminen*. Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) tuli voimaan 1.10.2010 ja sen mukaan valtion virastojen on toteutettava tietoturvallisuuden perustaso 30.9.2013 mennessä. Tietoturvallisuuden perustasoon sisältyvät menettelyt poikkeuksellisten tilanteiden varalle.

Ohje on suunnattu julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille näiden tuottaman palvelun osalta. Vaatimusten avulla pyritään sekä julkishallinnon että talouselämän varautumisen kannalta keskeisten toimintojen yhtenäistämiseen. Tällä parannetaan verkostomaisesti tuotettujen ja käytettyjen palvelujen häiriönsietokykyä ja edesautetaan palvelujen jatkuvuutta ja toipumista häiriötilanteissa. Ohjeella parannetaan organisaatioiden varautumista tietoturva- ja kyberuhkiin.

Valtionhallinnon organisaatioiden tulee toiminnassaan ottaa huomioon ohjeessa kuvatut ICT-varautumisen vaatimukset. Vaatimukset tulee ulottaa valtionhallinnon sisäisiin ja ulkoisiin palvelutoimittajiin. Yksittäisten järjestelmien osalta keskeistä on huomioida varautumisen vaatimukset muun muassa hankintojen valmisteluissa ja tarjouspyynnöissä.

Ministeriöiden ohjaamina hallinnonalojen ja virastojen tulee määrittää kullekin organisaatiolle, palveluille ja järjestelmille niiltä edellytettävä varautumisen taso. Organisaatioiden on määritettävä aikataulu palveluiden toteuttamiseksi varautumistasojen mukaisesti sekä resurssoitava toteutus osana normaalia toiminnan ja talouden suunnittelua.

Hallinto- ja kuntaministeri — Henna Virkkunen

Yksikön päällikkö — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: ICT-varautumisen vaatimukset –ohje (VAHTI 2/2012)

TIEDOKSI: Kunnat

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0986674-0 SUOMEN VALTIO

Lyhyesti VAHTIsta

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTI edistää hallitusohjelman, valtionhallinnon tietoturvallisuusasetuksen (681/2010), Yhteiskunnan turvallisuusstrategian (YTS), valtion IT-strategian, valtioneuvoston huoltovarmuuspäätöksen, kansallisen tietoturvastrategian, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös korostaa VAHTIn asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Periaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta astaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu yksi maailman kattavimmista yleisistä tietoturvaohjeistoista (www.vm.fi/vahti ja www.vahtiohje.fi). VM:n ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma.

VAHTI on saanut kolme kertaa tunnustuspalkinnon esimerkillisestä toiminnastaan Suomen tietoturvallisuuden parantamisessa.

Sisältö

Virastojen johdolle 5
Lyhyesti Vahtista 7

1 Johdanto 11
1.1 Lukuohje 12
1.2 Perusteet 12
1.3 Turvallisuusympäristö ICT-varautumisen kannalta 13

2 Varautumisvaatimusten rakenne 17
2.1 Vaatimusten muodostuminen 17
2.2 ICT-varautumisen vaatimustasot 19
2.2.1 Vaatimustasojen muodostuminen 19
2.2.2 Vaatimustasot 20

3 Varautumisen vaatimusten käyttö 25
3.1 Vaatimusten käyttö julkishallinnossa 25
3.2 Soveltaminen hankinnoissa ja palvelusopimuksissa 26
3.3 Vaatimusten soveltaminen hallinnon palveluyksiköissä ja yrityksissä 27

4 Varautumisen vaatimukset 29
4.1 Johtajuus 29
4.1.1 Strateginen ohjaus 30
4.1.2 Organisointi 31
4.1.3 Yhteistyö, viestintä ja raportointi 32
4.2 Strategiat ja toiminnan suunnittelu 32
4.2.1 Toiminnan suunnittelu riskienhallinnan avulla 33
4.2.2 Palvelujen jatkuvuuden suunnittelu 34
4.3 Henkilöstö 35
4.3.1 Osaamisen ja tietoisuuden kehittäminen 35
4.3.2 Henkilöstöresurssien ja tehtävien hallinta 36

4.4 Kumppanuudet ja resurssit 37
4.4.1 Sopimusten hallinta 37
4.4.2 Toiminnan varmistaminen erityistilanteissa 38
4.5 ICT-jatkuvuuden hallinta 38
4.5.1 ICT-palvelujen ja järjestelmien elinkaaren hallinta 39
4.5.2 ICT-palvelujen jatkuvuuden turvaaminen 40
4.6 Mittaaminen ja raportointi 41

Liite 1 ICT-varautumisen vaatimuskortit 43

1 Johtajuus 43
2 Strategiat ja toiminnan suunnittelu 53
3 Henkilöstö 61
4 Kumppanuudet ja resurssit 67
5 ICT-jatkuvuuden hallinta 73
6 Mittaaminen ja raportointi 81

Liite 2 Keskeisimmät ICT-varautumista ohjaavat säädökset ja ohjeet 83

1 Lait ja asetukset 83
2 Valtioneuvoston päätökset ja periaatepäätökset 84
3 Viranomaisten määräyskokoelmat 84

Voimassa olevat VAHTI julkaisut 87

1 Johdanto

Varautumisella ymmärretään kaikki ne hallinnolliset, toiminnalliset ja tekniset toimenpiteet ja ratkaisut, joilla varmistetaan tiedon saatavuus ja palveluiden mahdollisimman häiriötön toiminta kaikissa tilanteissa sekä mahdollistetaan palvelujen sopimusten mukainen, palvelutasojen avulla määritetty toipuminen häiriöistä.

ICT-varautuminen on riskienhallintaan pohjautuvaa ICT-toiminnan jatkuvuuden hallintaa ja tiedon turvaamista niin normaaliolojen häiriötilanteissa kuin poikkeusoloissa.

Tämä ohje on suunnattu julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille tuottamaansa palveluun liittyen. Yhtenäisten vaatimusten avulla pyritään sekä julkishallinnon että talouselämän varautumisen kannalta keskeisten toimintojen yhtenäistämiseen. Tällä parannetaan verkostomaisesti tuotettujen ja käytettyjen palvelujen häiriönsietokykyä ja edesautetaan palvelujen jatkuvuutta ja toipumista häiriötilanteissa. Ohjeella parannetaan organisaatioiden varautumista tietoturva- ja kyberuhkiin.

Ministeriöiden ohjaamina hallinnonalojen ja virastojen tulee:

- määrittää kullekin organisaatiolle sekä palveluille ja järjestelmille niiltä edellytettävä varautumisen taso
- määrittää aikataulu palveluiden toteuttamiseksi määritetyn varautumistason mukaisesti
- resursoida toteutus osana normaalia toiminnan ja talouden suunnitteluaan.

1.1 Lukuohje

Tässä ohjeessa on kuvattu ICT-varautumisen johtamisen ja toteuttamisen kannalta keskeisimmät periaatteet. ”ICT-varautumisen vaatimukset” -ohje korvaa VAHTI -yleisohjeen ”ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin” (VAHTI 2/2009).

Ylimmän johdon kannalta tärkeimmät asiat on esitetty tekstilaatikoissa. Toiminnan suunnittelusta vastaavalle johdolle tärkeät asiat ovat runkoasiakirjassa. Luvussa neljä on osakokonaisuuksittain esitetty yleisvaatimukset, joiden toteuttaminen on organisaation toiminnassa ja sitä tukevissa palveluissa täytettävä. Vaatimuksen jälkeen on esitetty, mitä vaatimuksella tarkoitetaan ja mitä asiaa se varautumisen näkökulmasta parantaa.

Liitteessä 1 olevat vaatimuskortit on tarkoitettu palvelun ja järjestelmän toteutuksesta ja ICT-varautumisesta vastaaville toimijoille. Vaatimuskorteissa on kuvattu tarkemmin perustason, korotetun tason ja korkean tason vaatimukset kutakin yleisvaatimusta tarkentamaan. Korteissa on myös näille vaatimuksille esimerkkejä, joilla kuvataan yhtä mahdollisuutta toteuttaa vaatimus tai selvennetään mitä vaatimuksella haetaan.

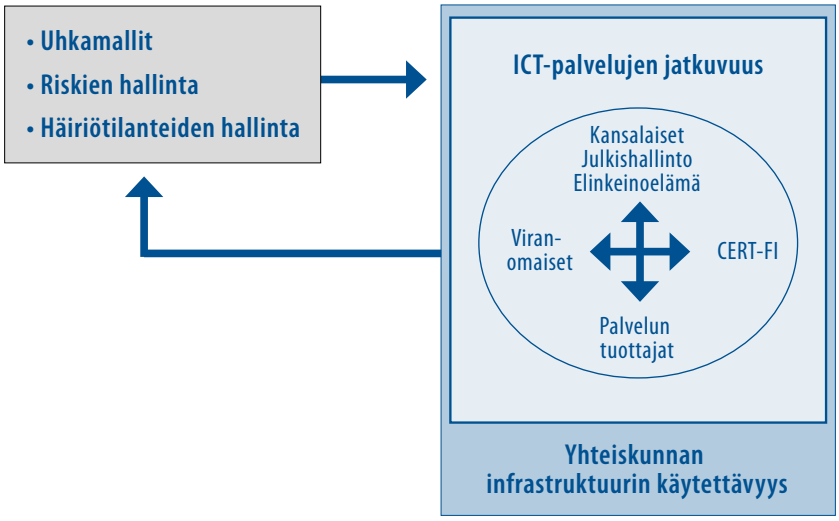
1.2 Perusteet

Varautuminen normaaliolojen häiriötilanteisiin on osa jokaisen organisaation hyvän tiedonhallintatavan mukaista toimintaa. Poikkeusoloihin varautumisen normipohjan muodostavat valmiuslaki sekä valtioneuvoston päätös 539/2008 huoltovarmuuden tavoitteista. Valmiuslaki velvoittaa viranomaisia varautumiseen. Normien lisäksi varautumisen ohjauksessa ja vaatimusten muodostamisessa keskeisessä osassa ovat valtioneuvoston periaatepäätökset valtionhallinnon tietoturvallisuuden kehittämisestä (2009) ja yhteiskunnan turvallisuusstrategiasta (YTS 2010).

Strategiassa määritetään yhteiskunnan elintärkeät toiminnot, jotka tulee varmistaa niin normaaliajan kuin poikkeusolojen häiriötilanteissa. Elintärkeiden toimintojen hoitamiseksi hallinnonaloille on määritetty strategiset tehtävät. Kullakin virastolla ja organisaatiolla voi näiden lisäksi myös olla muita oman toimintansa kannalta kriittisiä palveluja ja tehtäviä.

Yhteiskunnan elintärkeät toiminnot sekä niitä tukevat palvelut ja järjestelmät muodostavat toisistaan riippuvaisia verkostoja. Palvelujen käyttäjistä ja ylläpitäjistä koostuviin palveluverkostoihin osallistuu hallinnon eri osapuolia, kansalaisia, yhteisöjä, yrityksiä sekä tieto- ja viestintäteknisten palvelujen tuottajia. Palvelut ovat riippuvaisia yhteiskunnan ICT-infrastruktuurin toimivuudesta. ICT-palvelujen jatkuvuutta varmistetaan viranomaisten, asiakasorganisaatioiden ja palvelun tuottajien vuorovaikutuksella sekä yhteisillä toimintaperiaatteilla ja menettelytavoilla.

Kuva 1: ICT-varautuminen on koko yhteiskunnan yhteistoimintaa



Keskeistä on varmistaa, että koko palveluverkosto kykenee erilaisissa normaaliajan häiriötilanteissa ja yhteiskunnan turvallisuusstrategian mukaisissa uhkamalleissa jatkamaan toimintaansa asetettujen vaatimusten mukaisesti.

Tämä edellyttää kaikilta verkoston osilta yhtenäistä, sovitun tasoista tiedon turvaamista sekä toiminnan ja palvelun jatkamisen kykyä normaaliajan ja poikkeusolojen häiriötilanteissa.

Yhteiskunnan elintärkeät toiminnot:

- Valtion johtaminen
- Kansainvälinen toiminta
- Suomen puolustuskyky
- Sisäinen turvallisuus
- Talouden ja infrastruktuurin toimivuus
- Väestön toimeentuloturva ja toimintakyky
- Henkinen kriisinkestävyys

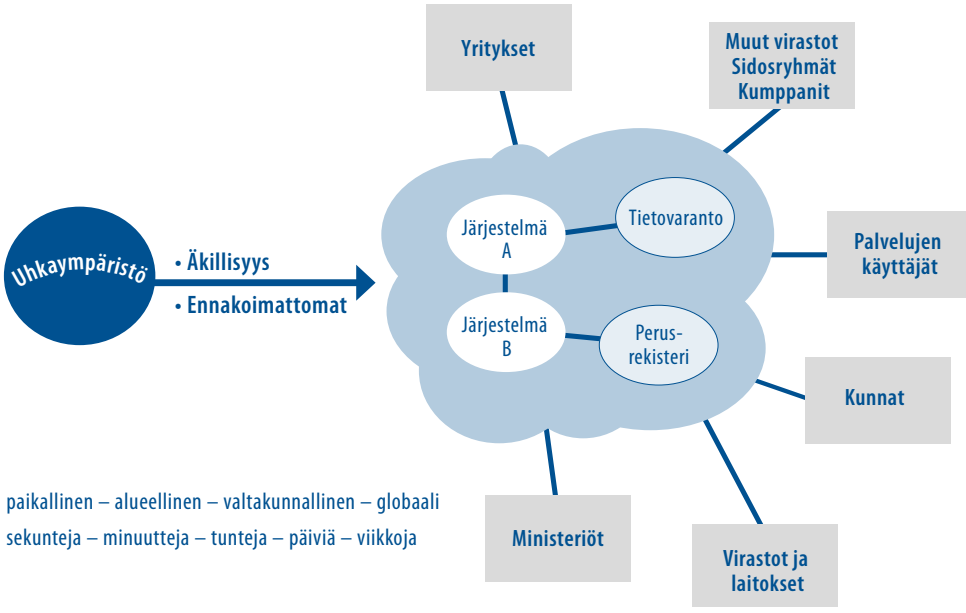
1.3 Turvallisuusympäristö ICT-varautumisen kannalta

Yhteiskunnan elintärkeät toiminnot ovat poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintakokonaisuuksia, joiden on oltava turvattuna kaikissa tilanteissa. Ympäröivän yhteiskunnan, julkishallinnon ja uhkaympäristön kehitys vaikuttavat mahdollisuuksiin tuottaa elintärkeiden toimintojen edellyttämiä palveluja ja ne pitää huomioida myös palveluiden varautumistarpeissa.

Tieto- ja viestintäteknisten palveluiden näkökulmasta keskeisimmät yhteiskunnan muutostrendit ovat:

- Palvelut, prosessit, tuotantoketjut ja järjestelmät automatisoituvat, monimutkaistuvat, integroituvat ja verkottuvat voimakkaasti.
- Tietojen yhteiskäyttö laajenee ja automatisoituu.
- Palvelukokonaisuudet hankitaan usean toimittajan palveluverkostolta.
- ICT-palveluketjujen omistus- ja sopimussuhteissa tapahtuu jatkuvasti muutoksia.
- Kansainvälisen yhteistoiminnan ja ohjauksen merkitys kasvaa voimakkaasti.
- Uhkaympäristö ja uhat muuttuvat yllätyksellisemmiksi, ammattimaisemmiksi ja vakavammiksi.

Kuva 2: Palveluverkoston ja järjestelmien yhteentoimivuus on ratkaisevaa häiriötilanteiden hallinnassa



Häiriötilanteita voi esiintyä sekä normaali- että poikkeusoloissa. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa.

Yhteiskunnan turvallisuusstrategian uhkamallit muodostavat yhteismitallisen ja palveluverkoston toimintaa yhtenäistävän suunnitteluperustan julkishallinnon toimijoiden, elinkeinoelämän ja järjestöjen yhteistyölle. Eri toimijat voivat hyödyntää yhdenmukaista aineistoa laatiessaan toimialojensa yksityiskohtaisia uhka-arvioita ja arvioidessaan uhkien aiheuttamia vaikutuksia palveluihin.

Tämän päivän yhteiskunta tietotekniikkaan pohjautuvine palveluineen on osa kyberympäristöä ja alttiina myös siihen liittyville uhille. Tietotekniselle toimintaympäristölle on tyypillistä uhkien äkillinen realisoituminen sekä niistä aiheutuneiden häiriöiden vaikutusten nopea ja ennalta arvaamaton laajentuminen. Häiriötilanteet voivat vaikuttaa suoraan tietotekniseen kokonaisuuteen tai välillisesti tukirakenteisiin (esimerkiksi henkilöstöön). Häiriö voi syntyä luonnonilmiöstä, onnettomuudesta, sähkökatkosta, tietojärjestelmävirheestä, laatuvirheestä, tietoliikennekatkosta, laiteviasta, toiminta- tai käyttövirheestä, tietokatkosta tai väärinymmärryksestä.

Häiriö voidaan aiheuttaa myös tahallisesti, kuten tietoverkkoon (ml. laitteisiin, järjestelmiin) kohdistettu vahingonteko, ilkivalta tai tietoverkkohyökkäys.

Organisaation tehtävien, toiminnan ja toimintaympäristön analysointi suhteessa uhkamalleihin tuottaa vaatimukset varautumiselle sekä toimenpiteet häiriötilanteiden ennaltaehkäisyyn ja hallintaan sekä näihin liittyvien suorituskykyjen kehittämiseen. Erityisesti kyberympäristön voimakas kehittyminen jatkuvasti muuntuvine uhkineen aiheuttaa tarpeen jatkuvaan varautumisen toteutumisen arviointiin ja kehittämiseen.

2 Varautumisvaatimusten rakenne

2.1 Vaatimusten muodostuminen

Tietohallintolaki (634/2011) velvoittaa julkisen hallinnon viranomaisia suunnittelemaan ja kuvaamaan kokonaisarkkitehtuurinsa julkishallinnon tietojärjestelmien yhteentoimivuuden mahdollistamiseksi ja varmistamiseksi. Laki myös velvoittaa julkishallinnon organisaatioita noudattamaan yhteentoimivuuden kuvauksia ja määrityksiä sekä asettaa valtiovarainministeriölle ohjaus- ja koordinaatiovelvoitteen.

Valtioneuvoston periaatepäätös (26.11.2009) valtionhallinnon tietoturvallisuuden kehittämisestä ohjaa valtionhallintoa kehittämään tietoturvallisuutta ja alan osaamista tärkeänä osana johtamista, riskienhallintaa sekä hallinnon toimintaa ja kehittämistä. 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 varmistamista erilaisissa häiriötilanteissa.

Varautumisvaatimuksia laadittaessa on otettu huomioon EU:n ja valtionhallinnon jatkuvuuden hallintaa ja tiedon turvaamista koskevat ohjeet ja määräykset. Nämä määräykset myös yksilöivät toimenpiteitä, joilla ICT-varautumisen vaatimukset voidaan toteuttaa. ICT-varautumisen kannalta keskeisimmät ohjeet on lueteltu liitteessä 2.

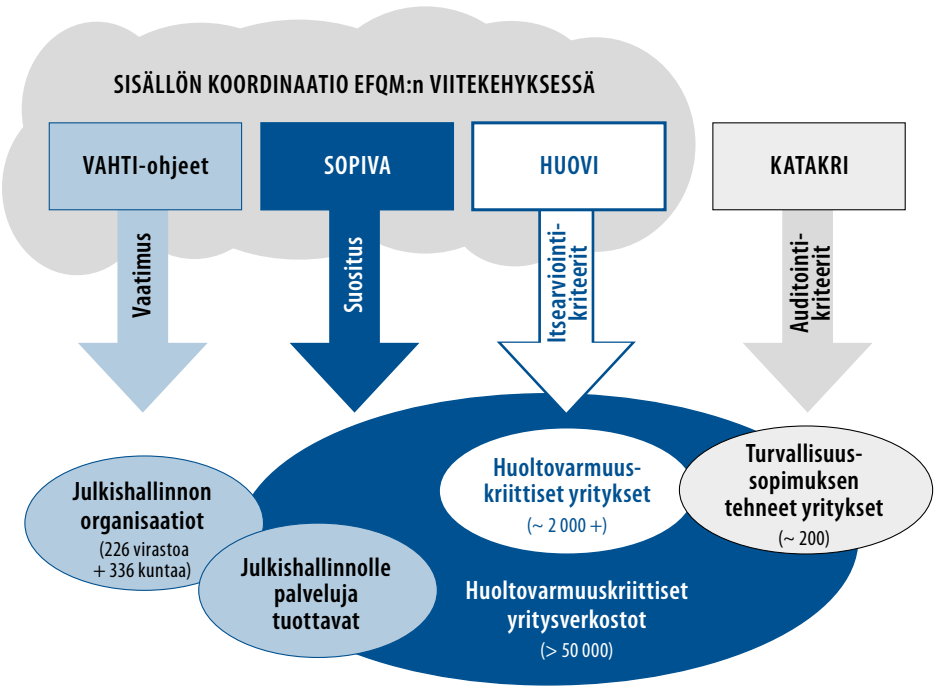
Varautumisen vaatimukset (VARE) ja tietoturva-asetuksen vaatimukset ohjaavat ensisijassa julkishallinnon organisaatioita. SOPIVA-suositukset ja HUOVI-itsearviointityökalu on tehty ensisijaisesti huoltovarmuuskriittisten yritysten käyttöön.

Kansallisen turvallisuusauditointikriteeristön (KATAKRI) ensisijainen kohderyhmä on ne julkishallinnon ja elinkeinoelämän organisaatiot tai niiden tietojärjestelmät ja tietoliikennejärjestelyt, jotka ovat olleet yritysturvallisuusselvityksen kohteena ja jotka käsittelevät kansainvälistä, turvallisuusluokiteltua tietoaineistoa.

KATAKRI:n turvallisuusauditointikriteeristöä voidaan soveltuvin osin käyttää erityisesti ICT-varautumisen korotetun, korkean ja erityistason palveluissa todentamaan tiedon ja palvelujen saatavuuteen sekä tilaturvallisuuteen liittyvien vaatimusten täyttymistä.

Kuva 3: ICT-varautumista ohjaavaa säädäntöä ja ohjeistusta

Kuva 4: ICT-varautumista ja tiedon turvaamista ohjaavat kriteeristöt



2.2 ICT-varautumisen vaatimustasot

2.2.1 Vaatimustasojen muodostuminen

ICT-varautumisen vaatimuksia asetetaan organisaation toiminnalle, palveluille sekä tietoja viestintäteknisten järjestelmien ja palveluiden toteuttamiselle. Vaatimusten muodostamisessa viitekehyksenä on hyödynnetty yleisesti käytettyjä EFQM[1] ja CAF[2] laadunarviointimalleja sekä vaatimuksissa ISO standardeja 27001 ja 22301.

Vaatimusten rungon muodostavat perusvaatimukset ovat yhteensopivia huoltovarmuusorganisaation johdolla laadittujen SOPIVA-suositusten ja HUOVI-kypsyysarviointimallin sekä tietoturva-asetuksen soveltamisohjeen (VAHTI 2/2010) kanssa. Tietoturva-asetus määrittää ensisijassa tiedon luottamuksellisuuden näkökulmasta vaatimuksia viranomaisten tiedonkäsittelyyn liittyen. ICT-varautumisen vaatimusten kohde on tiedon ja palvelujen saatavuus.

ICT-varautumisen vaatimukset on ryhmitetty kuuteen osaan. Osat 1–4 sisältävät organisaation ja toiminnan kypsyyteen liittyviä vaatimuksia strategisen johtamisen, toiminnan ohjauksen, henkilöstöhallinnon ja kumppanuusverkoston hallinnan näkökulmista. Näiden vaatimusten tarkoituksena on saada ICT-varautumisen hallinta osaksi organisaation normaalia toimintaa. Tämä edistää toiminnan ja palvelujen jatkuvuuden ja tiedon saatavuuden turvaamista osana palveluverkostoa myös häiriötilanteissa.

Osa 5 asettaa vaatimuksia erilaisille teknisille järjestelmille, prosesseille ja ratkaisuille. Kuudennessa osassa on esitetty vaatimuksia toiminnan sisäiselle ja ulkoiselle mittaamiselle.

Varautumisvaatimukset ovat yleisvaatimuksia, jotka kuvaavat toteutettavan, varautumista tukevan toimenpiteen. Yleisvaatimuksia täsmentävät toteuttamista ohjaavat perustason, korotetun tason ja korkean tason vaatimukset.

Tasojen tarkoituksena on ohjata organisaatioita kehittämään toimintaansa, tuottamiaan palveluja ja omistamiaan järjestelmiä tarkoituksenmukaisella tavalla sekä varautumaan erilaisiin uhkatilanteisiin ja ennalta ehkäisemään häiriöiden syntyä.

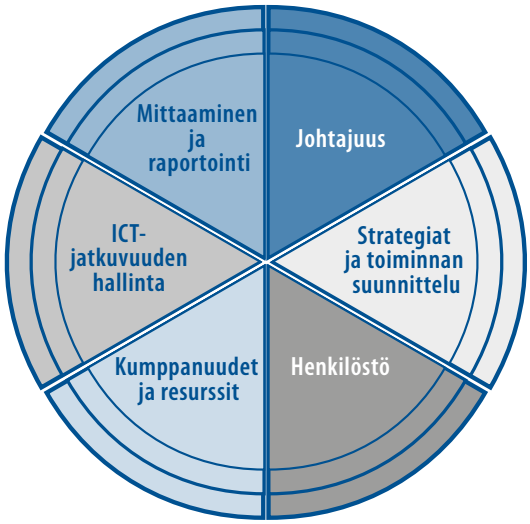
Järjestelmän tai palvelun ostajan velvollisuus on varmistua, että hankinnan kohde täyttää sille asetetut varautumisen vaatimukset.

---

1 EFQM (European Foundation for Quality Management) muodostaa viitekehyksen kilpailukyvyn ja erinomaisuuden kehittämiselle pyrkimättä silti tarkasti ohjailemaan, millaisia toimintatapoja organisaatioiden tulisi soveltaa. Mallia käytetään Euroopan laatupalkinnon ja Suomen laatupalkinnon arviointiperustana.

2 CAF (Common Assessment Framework) on EU-jäsenmaiden yhteistyönä kehitetty julkisen sektorin organisaatioiden laadunarviointimalli.

Kuva 5: ICT-varautumisen vaatimukset ryhmitellään kuuteen luokkaan ja kolmelle tasolle



2.2.2 Vaatimustasot

ICT-varautumisen tasojen avulla myös yhtenäistetään varautumistoimenpiteitä, jotta kumppanuuteen ja luottamukseen pohjautuvassa verkostoituneessa toiminnassa tunnettaisiin kunkin osan edellytykset kestää häiriötilanteita.

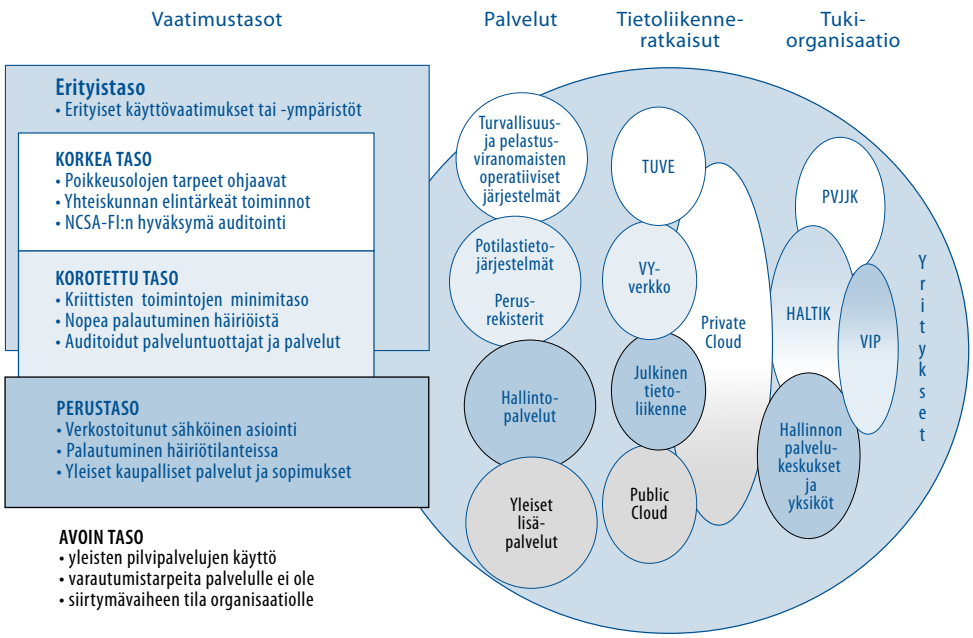
Organisaation toiminnot ja palvelut sijoitetaan tietoturva- ja varautumistasoille niiden tarpeiden mukaisesti. Jokin palvelu voi olla tietoturvan perustasolla ja varautumisen korkealla tasolla tai päin vastoin. ICT-varautumisen korotetun ja korkean tason saavuttaminen edellyttää kuitenkin minimissään myös tietoturvan perustason täyttymistä.

Viranomainen voi riskianalyysinsä pohjalta päätyä myös ratkaisuun, jossa valitussa palvelussa tavoitellaan vain tiettyjen vaatimusten täyttymistä. Valittua tasoa ylemmiltä tasoilta voidaan myös toteuttaa yksittäisiä lisävaatimuksia, joilla halutaan esimerkiksi parantaa järjestelmän käytettävyyttä arvioiduissa uhkatilanteissa. Järjestelmän käytettävyysvaatimus voidaan myös tilapäisesti nostaa korkeammalle palvelutasolle ennalta tiedettyjen, ajallisesti rajoitettujen tapahtumien ajaksi, kuten maksutapahtumat. Tämä edellyttää asian kuvaamista palvelusopimuksissa ja -prosesseissa.

Kaikilla ICT-varautumisen tasoilla julkishallinnon palvelua voivat toteuttaa joko organisaatio itse, julkishallinnon palvelutuottajat tai yksityiset palvelutuottajat. Korkealla tasolla on erikseen varmistuttava, että palveluntuottajan viankorjauksen resurssit ovat osaamistasoltaan ja saatavuudeltaan riittävät kaikissa uhkamallien mukaisissa häiriötilanteissa.

Julkishallinnon palvelut sijoitetaan ICT-varautumisen vaatimustasoille pääpiirteissään seuraavan sivun kuvan mukaisesti.

Kuva 6: ICT-varautumisen vaatimustasot



Avoin taso

Avoin taso on organisaation varautumisen kehittymisessä lähtötaso, jossa organisaation varautumistarpeiden tunnistaminen ja palvelujen luokittelu ICT-varautumisen eri tasoille on kesken.

Organisaatio voi myös harkitusti toteuttaa joitakin palvelujaan ja järjestelmiään avoimella tasolla, jolloin nämä eivät täytä ICT-varautumisen vaatimuksia. Tällaisia palveluja voivat olla esimerkiksi yleisistä pilvipalveluista tuotettavat palvelut. Palvelu voi tässä tapauksessa olla esimerkiksi sellainen lisäarvopalvelu kansalaisille, että se voi olla pitkiäkin aikoja poissa toiminnasta ilman, että organisaation perustehtävät jäävät täyttymättä ja kansalainen saa vastaavan palvelun myös muun palvelun kautta. Tällaisiin palveluihin ei voida kohdistaa tilaajan kautta erityisvaatimuksia ICT-varautumisen osalta.

Jokaisen julkishallinnon viranomaisorganisaation on kuitenkin saavutettava ICT-varautumisen perustaso, vaikka jotkut palvelut eivät suunnitellusti täyttäisikään perustason vaatimuksia ja toteutetaan siten avoimella tasolla.

Perustaso

Perustaso mahdollistaa turvallisesti organisaation normaalin, voimakkaasti verkostoituneen toiminnan. Perustasolle sijoittuu tyypillisesti suurin osa hallintoa tukevista järjestelmistä, kuten matkahallintajärjestelmät. Perustasolle sijoitetaan palvelut ja järjestelmät, joiden hetkellinen lamautuminen häiriötilanteissa ei keskeytä organisaation ydintoimin-

toja. Häiriötilanteista selviydytään toiminnan vaatimuksia vastaavilla yhtenäistetyillä, normaaleilla palvelusopimuksilla. Tyypillisesti perustasolle sijoitetaan järjestelmiä, joiden käytön pääpaino on virka-aikana, joiden viankorjaus voidaan aloittaa havaintoa seuraavana arkipäivänä tai joiden tavoitteellinen toipumisaika häiriöstä voi olla seuraavan työpäivän aikana.

ICT-varautumisen perustason vaatimusten täyttäminen ei aiheuta merkittäviä lisäkustannuksia, kun vaatimukset otetaan huomioon organisaation, toiminnan, palvelujen ja järjestelmien kehittämisessä alusta alkaen. Jo käytössä olevat palvelut ja järjestelmät siirretään perustasolle uudelleen kilpailutusten, järjestelmämuutosten ja päivitysten yhteydessä.

Perustason todentaminen voidaan tehdä itsearviointina tai ulkopuolisia palveluja käyttäen.

Korotettu taso

Korotettu taso on tarkoitettu organisaation kriittisille toiminnoille. Vain osa organisaation toiminnasta, palveluista ja järjestelmistä on tarkoituksenmukaista toteuttaa tällä tasolla. Korotetulle tasolle voidaan sijoittaa myös yhteiskunnan elintärkeitä toimintoja tukevia tai kansalaiselle häiriötilanteissa keskeisiä palveluja ja järjestelmiä. Korotetun tason järjestelmiä ovat esimerkiksi potilastietojärjestelmät ja perusrekisterit niiltä osin, kuin viranomaisten korotetun ja korkean ICT-varautumisen tason palvelut ovat niistä riippuvaisia. Yhteiskunnan elintärkeiden toimintojen kannalta keskeisten organisaatioiden tulisi sijoittaa myös joku kriisitilanteiden johtamisen mahdollistava viestitysjärjestelmä minimissään korotetulle tasolle.

Korotetulla tasolla on tehostettu häiriöitä ennaltaehkäiseviä varautumisen toimenpiteitä ja otettu käyttöön häiriön sietäviä ratkaisuja. Korotetun tason järjestelmissä on ympärivuorokautinen valvonta ja kyky aloittaa viankorjaus viivytyksettä. Korotetulla tasolla voidaan myös edellyttää käyttäjäorganisaatioilta päivystysjärjestelyjä, joilla varmistetaan kyky häiriötilanteiden hoitamisen toimenpiteistä päättämiseen.

Jos palvelut ja järjestelmät ovat merkityksellisiä yhteiskunnan elintärkeille toiminnoille ja poikkeusolojen toiminnalle, on huolehdittava niiden toimintaedellytyksistä myös tilanteissa, joissa tietoliikenneyhteydet Suomesta ulkomaille ovat lamautuneet. Tällöin on perusteltua asettaa korotetun tason palvelutuottajille joitakin erityisvaatimuksia muun muassa ulkomailla tuotettaviin palveluihin ja niiden ulkoisiin tarkastuksiin liittyen.

Korotetun tason todentamiseen on hyvä käyttää myös organisaation ulkopuolista toimijaa.

Korkea taso

Korkea taso täyttää yhteiskunnan turvallisuusstrategian uhkamallien mukaisiin laajoihin häiriötilanteisiin ja poikkeusoloihin varautumisen tarpeet erityisturvallisuutta vaativissa toiminnoissa. Korkean vaatimustason järjestelmiä ovat esimerkiksi hallinnon turvallisuusverkko ja turvallisuusviranomaisten operatiiviset järjestelmät. Korkealle tasolle sijoitetaan palveluja ja järjestelmiä, joiden tulee toimia ympärivuorokautisesti ja joiden pienetkin palvelukatkokset aiheuttavat vakavia toiminnallisia häiriöitä tai erittäin huomattavia taloudellisia vaikutuksia.

Korkea taso asettaa merkittäviä lisävaatimuksia organisaation toiminnalle, osaamiselle ja järjestelmien toteutukselle. Korkean tason järjestelmät ovat jatkuvan ympärivuorokautisen valvonnan, hallinnan ja viankorjauksen piirissä. Korkean tason järjestelmät edellyttävät myös tilaaja- ja käyttäjäorganisaatioilta järjestelyjä, joilla taataan kyky nopeaan päätöksentekoon häiriötilanteissa. Korkealla tasolla on erityisesti varmistettava tietoliikenteen toimivuus, tiedon, palvelujen, ylläpidon ja osaamisen saatavuus ja toiminta Suomen lainsäädännön alaisuudessa poikkeusolot huomioon ottaen. Korkealle tasolle sijoitettavien palvelujen tulee toimia, vaikka tietoliikenneyhteydet ulkomaille olisivat poikki. Korkean tason palveluissa on erikseen määritettävä, mitkä tiedot on säilytettävä ja mitkä hallintatoimet on toiminnan kriittisyyden tai poikkeusoloihin varautumisen kannalta toteutettava Suomessa.

Korkean varautumistason järjestelmät tulee rakentaa siten, ettei yhden konesalin tai tietoliikenneyhteyden tuhoutuminen lamauta järjestelmän toimintaa.

Korkean tason ICT-varautumisen todentamiseen tulee käyttää NCSA-FI:n hyväksymää toimijaa.

Erityistaso

Erityistasolle sijoitetaan kriittisiä toimintoja, palveluja ja järjestelmiä, joissa on toiminnan luonteen ja sen edellyttämän palvelun saatavuuden varmistamiseksi jouduttu soveltamaan korotetun ja korkean tason vaatimuksia ja ottamaan käyttöön yhteisistä menetelmistä ja ratkaisuista poikkeavia ratkaisuja.

Järjestelmän sijoittumisen erityistasolle päättää ohjaava ministeriö ja hyväksyy valtiovarainministeriö. Palvelun ja järjestelmän auditoinnin toteuttaa kansallinen tietoturvaviranomainen (NCSA-FI) tai sen hyväksymä toimija.

3 Varautumisen vaatimusten käyttö

3.1 Vaatimusten käyttö julkishallinnossa

Valtiovarainministeriö vastaa ICT-varautumiseen liittyvien varautumistarpeiden kokoamisesta, varautumisvaatimusten asettamisesta, ohjeistuksesta ja toteutuksen ohjauksesta.

Julkishallinnossa käytettävien varautumisen vaatimusten tulee kattaa koko verkostoitunut toimintaprosessi, myös hallinnonalojen rajat ylittäen. Poikkihallinnollisissa prosesseissa tulee kunkin prosessin osan täyttää hyväksytyt vaatimukset. Mahdolliset erityisen painavasta syystä sallitut poikkeamat tulee hyväksyä erikseen ja käsitellä kaikkien prosessista riippuvaisten organisaatioiden kanssa. Varautumisen lähtökohtana on, että jokainen prosessiin kuuluva organisaatio on täyttänyt tietoturva-asetuksen mukaisen tietoturvallisuuden perustason.

Kunkin julkishallinnon organisaation on arvioitava mille sen palveluista ja järjestelmistä riittää varautumisen perustaso ja mitkä edellyttävät korotetun tai korkean tason varautumista. Tässä arvioinnissa korostuu palvelua käyttävien sidosryhmien tarpeet. Järjestelmät ja palvelut siirretään valitulle tasolle ensisijassa elinkaarenhallinnan luonnollisessa vaiheessa, kuten järjestelmäpäivityksen tai uudelleen kilpailutuksen yhteydessä.

> Viranomaisten on kirjattava omille toiminnoille, palveluille ja järjestelmille tavoiteltavat varautumisen tasot ja liitettävä tasojen saavuttamisen aikataulu ja resurssit tulosohjaukseen, toiminnan ja talouden suunnitteluun sekä raportointiin.

Valtionhallinnon yhteisten palvelujen ja järjestelmien sijoittaminen korkealle ja korotetulle tasolle sekä hallinnonalojen rajat ylittävien tietovirtojen ja prosessien koordinointi määritetään yhteistyössä ministeriöiden kesken VM:n koordinoimana.

Ministeriöillä on merkittävä rooli oman hallinnonalansa varautumisen ohjaamisessa tulosohjauksen keinoin. Ministeriöt vahvistavat virastojensa esitysten perusteella hallinnonalansa korkealle tasolle sijoitettavat järjestelmät toiminnan ja talouden suunnitteluun, tulosohjaukseen sekä seurantaan liittyen.

> Julkishallinnon organisaatioiden on toteutettava palvelujensa ja järjestelmiensä arviointi ja tarvittaessa akkreditointi valtiovarainministeriön ohjeiden mukaisesti.

3.2 Soveltaminen hankinnoissa ja palvelusopimuksissa

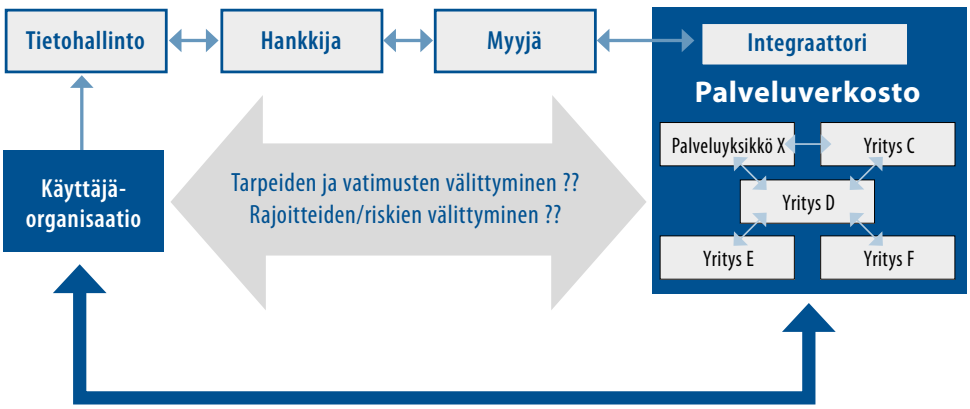
Jokainen organisaatio vastaa vaatimusten sisällyttämisestä tekemiinsä tarjouspyyntöihin ja sopimuksiin. Tarjouspyyntöjä ja sopimuksia laadittaessa tulee huomioida, että kussakin hankittavassa palvelussa on arvioitava, mitkä vaatimukset sopivat sellaisenaan ja mitä vaatimuksia tulee hankinnan luonteen vuoksi muokata, jotta niitä voidaan käyttää palvelutoimittajia velvoittavina.

Valtiovarainministeriö määrittää alkuvaiheessa hankinnoissa sovellettavat yhteiset velvoittavat vaatimukset. Nämä sisällytetään mahdollisuuksien mukaan myös julkishallinnon yhteisiin puitesopimuksiin. Kukin organisaatio voi omissa kilpailutuksissaan ja puitesopimuksissaan täsmentää hankittavan palvelun ja oman toiminnan erityisluonteen edellyttämällä tavalla hankinnan kohteeseen liittyviä velvoittavia vaatimuksia.

Jokaisen organisaation tulee palvelusopimuksissaan 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.

Perustason noudattamisvelvoite tulee ulottaa myös alihankintaehtoihin ja kumppanuusverkostoon. Menettelyllä edesautetaan keskeisen yritysverkoston toiminnan jatkuvuuden parantamista. Viraston tulee varmistua, että vaatimukset asetetaan ulkoisille tai sisäisille sopimuskumppaneille ja että nämä huolehtivat niiden asettamisesta edelleen alihankkijoilleen.

Kuva 7: Varautumisen vaatimusten on välityttävä läpi palvelun hankintaketjun



- Toteutetaanko palvelut ja järjestelmät toiminnan tarpeiden mukaisesti?
- Ovatko käyttö- ja tukipalvelut sekä tarvittavat ylläpitoresurssit käytetävissä myös häiriötilanteissa ja poikkeusoloissa?

Uusiin puitesopimuksiin ja palvelusopimuksiin kirjataan perustason ja tarvittaessa korkeampien tasojen varautumisen vaatimusten noudattaminen.

Voimassa oleviin sopimuksiin ei vaatimuksia lisätä kesken sopimuskauden muutoin kuin erityisen painavista perusteista.

3.3 Vaatimusten soveltaminen hallinnon palveluyksiköissä ja yrityksissä

Varautumisen vaatimukset tulee ulottaa sekä julkishallinnon sisäisiin että ulkoisiin palvelutoimittajiin. Vaatimusten toteutustapa voi eri toimijoilla poiketa toisistaan, kunhan vaatimuksella tavoiteltu asia kyseessä olevassa palvelussa ja hankinnan kohteessa täyttyy ja yhteentoimivuus verkostoituneessa toiminnassa säilyy.

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 varautumisen vaatimuksia omassa toiminnassaan ja kumppanuusverkostojensa sopimusjärjestelyissä. Yritysten näkökulmasta yhtenäinen valtionhallinnon toimijoiden vaatimusasettelu yksinkertaistaa ja yhtenäistää asiakasvaatimusten täyttämistä sekä antaa hyvän työkalun yrityksen oman alihankkija- ja kumppanuusverkoston hallintaan.

Julkishallinnolle palvelua tuottavien yritysten voidaan edellyttää täyttävän tarjouspyynnössä ja sopimuksissa edellytetyt varautumisen vaatimukset koskien myymäänsä palvelua ja siihen liittyvää palvelutuotantoa. Korotetun ja korkean tason vaatimusten toteuttaminen voidaan tarvittaessa rajata vain siihen yksikköön, joka tuottaa tai ylläpitää ko. tason palveluja.

Ellei tarjouspyynnössä ole erityisestä syystä edellytetty jotain tiettyä vaatimusten toteutustapaa, voi yritys halutessaan hyödyntää myös yrityskohtaisia menetelmiä. Tällöin yrityksen tulee kuvata miten edellytetty vaatimus täyttyy yrityksen käyttämillä keinoilla ja esittää ratkaisu tilaajan hyväksyttäväksi.

4 Varautumisen vaatimukset

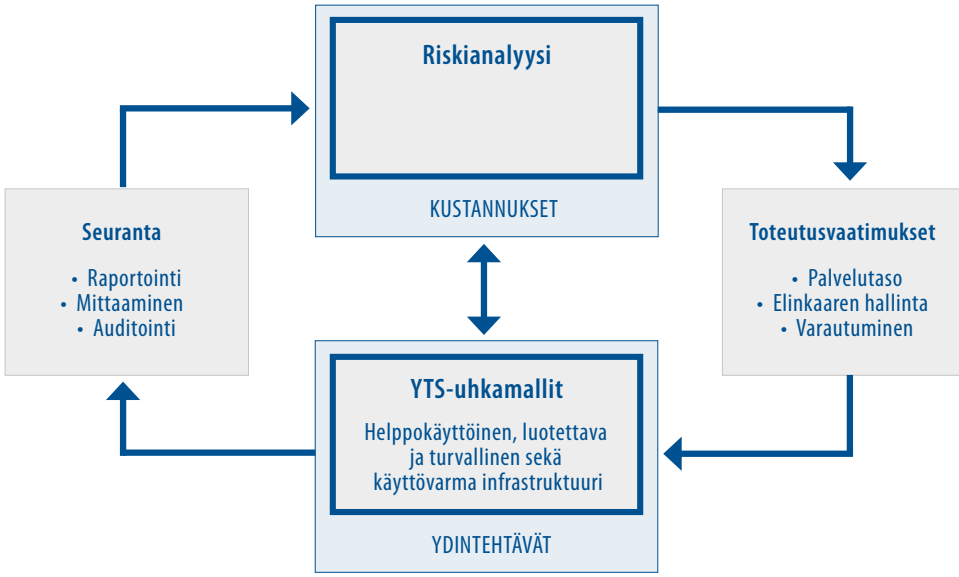
4.1 Johtajuus

Yhteiskunnan elintärkeitä toimintoja uhkaavat häiriötilanteet johdetaan useimmiten normaaliolojen johtamissäännöstöjen mukaisesti. Vakavissa häiriötilanteissa otetaan käyttöön yhteiskunnan turvallisuusstrategian mukaiset kriisijohtamismallit.

Organisaation johdon tuki on ratkaisevaa kehitettäessä organisaation ja sen palvelujen toimintavarmuutta häiriötilanteissa. Johdon tehtävä on luoda tarkoituksenmukaiset edellytykset organisaation toiminnan jatkamiseksi kaikissa häiriötilanteissa.

Johto päättää varautumis- ja jatkuvuussuunnittelun tavoitteet, linjaukset ja hyväksyy resurssit laaditun kehittämissuunnitelman pohjalta. Organisaation ydintehtävien tulee hoitua kaikissa yhteiskunnan turvallisuusstrategian uhkamallien häiriötilanteissa.

Kuva 8: ICT-varautumisen suunnittelun ja toteutuksen prosessi



Tätä tukemaan organisaatio tarvitsee helppokäyttöiset, luotettavat ja turvalliset palvelut ja käyttövarman ICT-infrastruktuurin. Toiminnan tarpeiden ja vaatimusten arvioinnilla suhteessa riski- ja kustannushyötyanalyyseihin voidaan muodostaa vaatimukset ICT-palveluille ja ICT-varautumisen kehityssuunnitelma. Mittaamisen ja raportoinnin kautta toiminnasta saadut palautteet hyödynnetään palvelua ja ICT-varautumista kehitettäessä osana normaalia toiminnan ja talouden suunnittelua.

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

4.1.1 Strateginen ohjaus

Strategisen ohjauksen keskeinen tehtävä on määrittää organisaation ja palveluiden varautumistarpeet ja viedä varautuminen yhtenäisesti tulosohjaukseen sidottuna osaksi kunkin organisaation johtamista sekä toiminnan ja talouden suunnittelua ja toteutusta.

Vaatimus 1.1:
Organisaatiolla on tiedossa toimintaansa ja palveluihinsa liittyvä ICT-varautumista ohjaava lainsäädäntö ja muut normit ja nämä on huomioitu varautumisen linjauksissa ja toiminnassa.

- Velvoitteistaan huolehtiakseen on ensin tiedostettava niiden olemassaolo. Lainsäädäntö ja normit määrittävät minimitason ICT-varautumisen toteuttamiselle. Tämän lisäksi organisaation on huomioitava oman toimintansa erityispiirteistä nousevat tarpeet. Toimintojen sisäisten ja ulkoisten riippuvuussuhteiden ymmärtäminen on perusedellytys varautumisen kustannustehokkaalle johtamiselle. Johdon on huolehdittava, että alaisille organisaatioille ja yksiköille on selkeästi määritetty ja kerrottu niiden poikkeusolojen tehtävät.

Vaatimus 1.2:
ICT-varautumisen linjaukset on määritetty toiminnan asettamien vaatimusten perusteella.

- Ydintoimintojen ja niitä tukevien järjestelmien on toimittava häiriötilanteissa mahdollisimman häiriöttömästi. Varautumistoimenpiteet tulee mitoittaa ja kohdentaa toiminnan tarpeiden mukaisesti. Hyvänä työmenetelmänä on toiminnan vaikuttavuusanalyysi (BIA=Business Impact Analysis).

4.1.2 Organisointi

Varautuminen on organisoitava osaksi normaalia toimintaa pohjautuen työjärjestyksiin ja tehtäväkuvauksiin siten, että ohjausvastuut ja toimintamallit pysyvät mahdollisimman muuttumattomina häiriötilanteissa ja poikkeusoloissa. Organisaation ylin johto priorisoi tehtävät toimenpiteet.

Vaatimus 1.3:
Häiriötilanteiden hallinta on linjattu, organisoitu ja huomioitu ohjausmalleissa.

- Häiriötilanteissa on tärkeää pystyä päättämään ja toimimaan nopeasti ja tehokkaasti. Tämän mahdollistaa selkeät ja kaikkien osapuolten tiedossa olevat ohjausvastuut.

Vaatimus 1.4:
ICT-varautuminen on organisoitu ja vastuutettu osaksi normaalia johtamista, toimintaa sekä kumppanuusverkoston hallintaa.

- Kustannustehokas toiminta edellyttää, että kaikki osapuolet huolehtivat oman toimintansa varautumisesta häiriötilanteisiin yhteisten linjausten mukaisesti.

Vaatimus 1.5:
Varautumiselle ja jatkuvuuden hallinnalle on asetettu tavoitteisiin nähden riittävät resurssit.

- Tavoitetason tulee olla realistinen ja sen saavuttamiseksi tulee varata riittävät resurssit. Vain sovitut ja testatut varautumistoimenpiteet auttavat häiriötilanteiden ehkäisyssä ja niistä toipumisessa. Tavoitteiden ja resurssien määrittely tulee sitoa toiminnan ja talouden suunnitteluun.

Vaatimus 1.6:
Varautumisen ja jatkuvuuden hallinnan suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä.

- Ylin johto nimeää tarvittavat henkilöt yhteistyön toteuttamiseen. Yhteistyö on tarpeen, jotta ydintoimintojen kannalta välttämättömät tukitoiminnot voidaan huomioida myös jatkuvuussuunnittelussa, ja jotta toteutetut toimenpiteet ovat linjassa keskenään.

4.1.3 Yhteistyö, viestintä ja raportointi

> Organisaation johdon on vietävä ICT-varautumisen raportointi osaksi johtoryhmätyöskentelyn ja yhteistyötapaamisten vuosikelloa. Johdon on myös linjattava ja vastuutettava nopean sisäisen ja ulkoisen viestinnän toteuttaminen häiriötilanteissa osana operatiivisen toiminnan jatkuvuuden toteuttamista.

Vaatimus 1.7:
Organisaation johto seuraa varautumisen ja kyberturvallisuuden kehittämistä ja jatkuvuussuunnittelua sekä näihin liittyvien toimenpiteiden vaikutuksia ja kustannuksia.

- Organisaation johto on vastuussa palvelujen toimintakyvystä häiriötilanteissa. Johdon on ohjattava varautumista osana johtoryhmätyöskentelyään sekä vaadittava riittävät ja ymmärrettävät tiedot ICT-varautumisen tilasta päätöksenteon tueksi. Jatkuvuuden hallintaa ei voida menestyksellisesti toteuttaa ilman johdon sitoutumista.

Vaatimus 1.8:
Viestinnän ja raportoinnin vastuut ja toimintamalli keskeisimpien sidosryhmien kanssa on määritetty ja organisoitu.

- Ulkoistusten ja verkottuneen toimintatavan vuoksi organisaatiot ovat riippuvaisia keskeisistä sidosryhmistään toimintansa jatkuvuuden varmistamisessa. Tiedonkulun tulee toimia organisaatiorajojen yli. Keskeistä on huolehtia palveluihin vaikuttavien poikkeamien ja häiriöiden välittömästä viestittämisestä.

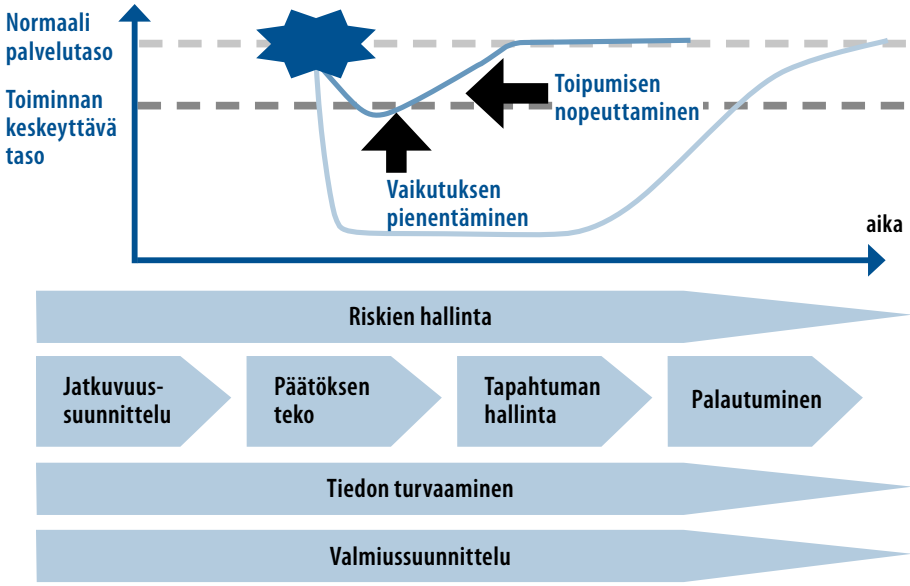
4.2 Strategiat ja toiminnan suunnittelu

ICT-varautumisen kehittämisessä on huomioitava lakisääteiset velvoitteet. Toiminnan ja palveluiden jatkuvuuden varmistamisen suunnittelu toteutetaan osana toiminnan ja talouden suunnittelua. Toiminnan suunnittelussa on erityisesti huomioitava palvelujen riippuvuus muista palveluista ja toisista toimijoista sekä näin muodostuvasta toimintaketjusta ja -verkostosta.

Riskienhallinta on integroitava toiminnan suunnitteluun. Riskienhallintaan liittyvissä uhka-arvoissa tulee hyödyntää yhteiskunnan turvallisuusstrategian mukaisia uhkamalleja. Organisaation riskien analysointi kohdistuu sisäiseen ja ulkoiseen toimintaympäristöön. Kriittisten tehtävien osalta analysoidaan oman ja sidosryhmien toiminnan riskit. Ydin- ja tukitoimintojen riskien priorisointi ohjaa varautumisen ja jatkuvuudenhallinnan kehittämistä.

Keskeistä on määrittää kullekin palvelulle tavoiteltu palvelutaso. On myös tunnettava taso, minkä alapuolella palvelu ei ole palvelua käyttävän organisaation toiminnan kannalta enää käyttökelpoinen. Jokaiselle palvelulle määritetään hyväksyttävät toimenpiteet, joilla häiriötilanteiden vaikutus minimoidaan ja palvelujen toipuminen nopeutetaan palvelutasovaatimusten mukaiseksi.

Kuva 9: Jatkuvuuden hallinta on ICT-varautumista toteuttava prosessi



Organisaatiolla tulee olla kirjattuna varautumisperiaatteet, joiden mukaisesti ICT-varautuminen, jatkuvuuden hallinta ja tiedon turvaaminen toteutetaan. Varautumissuunnittelu voi myös olla osa organisaation valmiussuunnittelua, joka toteutetaan valmiuslain ja pelastuslain prosessein. Jatkuvuussuunnittelu sisältää varautumis- ja toipumissuunnittelun. Suunnittelussa on oleellista tunnistaa toimenpiteiden oikea järjestys vaikuttavuuden näkökulmasta. Varautumisen lähtökohtana on, että viranomaisorganisaatiot, palvelua käyttävät ja tuottavat yksiköt sekä itse palvelut täyttävät minimissään tietoturva-asetuksen mukaisen tietoturvallisuuden perustason.

Jatkuvuussuunnittelu tulee tehdä yhteistyössä palvelutuottajien kanssa. Jokainen palvelutuottaja sitoutetaan sopimuksin yhdessä sovittuihin toimenpiteisiin. Poikkeusolojen toiminnan erityispiirteet huomioidaan valmiussuunnittelussa, joka voidaan toteuttaa yhtenä osana normaaliajan jatkuvuussuunnittelua.

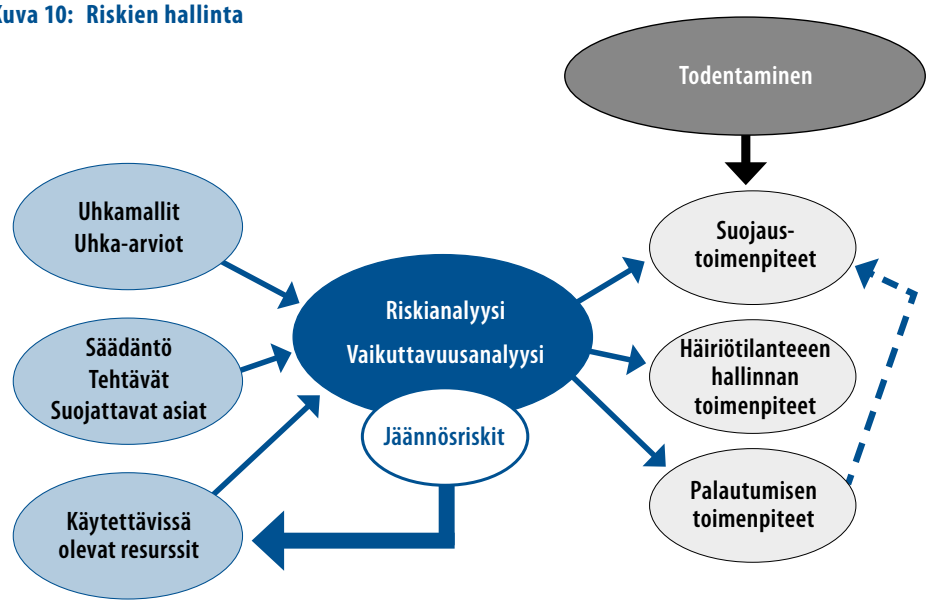
4.2.1 Toiminnan suunnittelu riskienhallinnan avulla

Riskienhallinnan avulla varautumistoimenpiteet ja resurssit mitoitetaan ja kohdennetaan tarkoituksenmukaisesti edistämään organisaation toimintaa ja toiminnan häiriönsietoa.

Riskienhallintaan liittyen on palveluittain ja järjestelmittäin tunnistettava niiden merkitys organisaation omalle toiminnalle ja yhteiskunnan elintärkeille toiminnoille sekä arvioitava malleissa kuvattujen uhkien (ml. tietoturva- ja kyberturvallisuusuhkat) vaikutus palveluiden ja järjestelmien toimintakykyyn. Palvelut ja järjestelmät tulee myös luokitella niiden kriittisyyden mukaan, jotta korjaavat toimenpiteet kyetään priorisoimaan ja kohdentamaan häiriötilanteissa.

Riskienhallinnassa keskeistä on systemaattisesti arvioida uhkia, organisaatiolle asetettuja tehtäviä ja vaatimuksia sekä käytettävissä olevia resursseja ja määrittää näiden pohjalta ne toteutettavat toimenpiteet, joiden vaikuttavuus on ICT-varautumisen kannalta suurin (kuva 10).

Kuva 10: Riskien hallinta



Vaatimus 2.1:

Organisaation ja toimintaympäristön vuorovaikutus otetaan toiminnassa huomioon.

- Organisaation toimintamahdollisuuksiin vaikuttaa toimintaympäristö ja siellä tapahtuvat muutokset. Vuorovaikutuksella voidaan ennakoida omaan toimintaan kosketta-via tekijöitä ja vaikuttaa niihin.

Vaatimus 2.2:

Riskienhallinnan tulokset ohjaavat varautumisen kehittämistä.

- Riskienhallinnan avulla kehittämistoimenpiteet voidaan kohdistaa sinne missä niistä saatava hyöty on suurin.

4.2.2 Palvelujen jatkuvuuden suunnittelu

Organisaatioiden on tunnistettava varautumistoimenpiteitä tarvitsevat palvelut ja järjestelmät sekä suunnitella tarvittavat toimenpiteet ja järjestää tärkeiden järjestelmien ympärivuorokautinen valvonta.

Vaatimus 2.3:
Varautumistoimenpiteet tukevat organisaation ydintoiminnan tavoitteita.

- Jatkuvuuden hallinta ja tiedon turvaaminen ei ole itsetarkoitus, vaan niiden täytyy palvella organisaation tehtävää.

Vaatimus 2.4:
Häiriötilanteiden hallinnan ja poikkeusolojen menettelyt on dokumentoitu, koulutettu ja harjoiteltu.

- Selkeät ohjeet ja harjoittelu luovat edellytykset häiriötilanteissa toimimiselle ja mahdollistavat tarvittaessa toimintamallien nopean soveltamisen uuden tyyppisessä tilanteessa. Normaaliajan häiriötilanteisiin varautuminen luo pohjan myös toiminnalle poikkeusoloissa. Mikäli poikkeusolot edellyttävät organisaatiolta muutoksia toimintamalleihin ja palveluihin, tulisi nämä valmistella jo normaaliaikana.

Vaatimus 2.5:
24/7 toiminta ja CERT-FI -yhteistoiminta vastaavat organisaation tavoitteita ja velvoitteita.

- Tärkeiden kohteiden ympärivuorokautista valvontaa sekä CERT-FI -yhteistoimintaa tarvitaan varmistamaan riittävän nopea uhkiin reagointi. Nämä ovat tärkeitä myös valtionhallinnon yleisen tilannekuvan mahdollistamiseksi.

4.3 Henkilöstö

Organisaation ydintoimintojen kriittiset erityisosaamisalueet on huomioitava henkilöstön osaamisvaatimuksissa, koulutuksessa, palvelujen hankinnassa ja resursoinnissa. Kriittisistä tehtävistä vastuulliset avainhenkilöt koulutetaan häiriötilanteissa toimimiseen. Henkilöresurssien ja osaamisen saatavuus häiriötilanteiden ja poikkeusolojen varalle on varmistettava. Oleellinen tekijä on henkilövarausten (VAP) ylläpito omassa organisaatiossa ja palveluja tuottavassa yritysverkostossa alihankintaketjuineen.

Strategiseen suunnitteluun tulee sisältyä myös häiriöiden ennakoiminen sekä varautuminen erityistilanteisiin ja poikkeusoloihin. Riskien analysointi kohdistetaan 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 toteutuneiden häiriötilanteiden seurauksia ja päättää toimintakyvyn parantamisesta.

4.3.1 Osaamisen ja tietoisuuden kehittäminen

> Organisaation on määritettävä varautumisen, jatkuvuuden hallinnan ja tiedon turvaamisen keskeisten tehtävien osaamisvaatimukset ja kehitettävä osaamista järjestelmällisesti.

Vaatimus 3.1:
ICT-varautumisen 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.

Vaatimus 3.2:
Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia.

- Motivoitunut henkilöstö tuottaa hyviä tuloksia tehokkaasti pienemmällä ohjauksella ja valvonnalla.

Vaatimus 3.3:
Organisaatiossa on määritetty menettelyt valvonnan toteuttamiseen ja toimintaan turvallisuuspoikkeamissa ja väärinkäytöstilanteissa.

- Selvät pelisäännöt ennaltaehkäisevät väärinkäytöksiä ja varmistavat henkilöstön ja muiden osapuolten oikeuksien toteutumisen myös väärinkäytöstilanteissa/-epäilyissä.

4.3.2 Henkilöstöresurssien ja tehtävien hallinta

> Organisaation toiminnassa on systemaattisesti pienennettävä avainhenkilöriskiä ja varmistettava osaamisen saatavuus myös häiriötilanteissa.

Vaatimus 3.4:
Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt on suunniteltu.

- Varajärjestelyt ovat välttämättömiä, jotta toiminta voisi jatkua myös silloin kun avainhenkilöt eivät ole käytettävissä.

Vaatimus 3.5:
Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla.

- Jos henkilöstöä on liian vähän tai sen osaamistaso ei täytä vaatimuksia, osa tehtävistä tehdään huonosti tai jää kokonaan tekemättä. Ydintoimintojen jatkuvuus ei saa vaarantua missään tilanteessa.

4.4 Kumppanuudet ja resurssit

Palvelua tuottavien valtionhallinnon sisäisten organisaatioiden ja ulkoisten kumppanien on täytettävä palvelutuotantoonsa liittyen palvelulle asetetut varautumisen vaatimukset. Palvelua hankkiva organisaatio hyväksyy menettelytavat ja tekniset ratkaisut, joilla palvelulle tarjouspyynnössä asetetut ja sopimusneuvotteluissa tarkennetut varautumisvaatimukset toteutetaan sekä valvoo niiden toteutumisen todentamista ja raportointia. Kullekin palvelulle tulee määrittää vastuuhenkilö, joka vastaa kyseessä olevaan palvelun kumppani- ja palveluntuottajaverkoston hallinnasta varautumiseen sekä poikkeus- ja häiriötilanteista toipumiseen liittyen. Koordinoija voi olla palvelun ostavan organisaation oma tai nimetty kumppani.

Valtiovarainministeriön koordinoimana laaditaan ja ylläpidetään listaa hankintoihin sisällytettävistä julkishallinnon yhteisistä ICT-varautumisen vaatimuksista. Kuhunkin hankintaan sovelletaan listalta niitä vaatimuksia, jotka liittyvät hankinnan kohteeseen ja ovat hankinnan kohteeseen liittyvän lainsäädännön mukaisia.

Palvelujen toimittaja- ja teknologiavalinnoissa on otettava huomioon ylläpitopalvelujen ja -resurssien sekä varaosien saatavuus häiriötilanteissa ja poikkeusoloissa hankittavien palvelujen luonteen edellyttämässä laajuudessa.

4.4.1 Sopimusten hallinta

Varautumisen velvoitteet ulotetaan sopimuksissa koko alihankintaketjuun ja palvelutuottajaverkostoon ottaen huomioon kunkin tuotettavan palvelun luonne ja sopijaosapuolten rooli palvelun tuottamisessa.

Vaatimus 4.1:
Organisaation toiminnalle välttämättömät kumppanit, alihankkijat ja resurssit on tunnistettu.

- Verkostoituneessa toiminnassa jokaisella toimijalla on merkityksensä ja sen mukaiset velvoitteet yhteistoiminnan suhteen. Keskeisetta hottäytyytunnistaa, jotta kustannuksia aiheuttavat vaatimukset voidaan kohdistaa vain niille sopimuskumppaneille joista toiminta on riippuvainen.

Vaatimus 4.2:
Sopimuksissa on vaatimukset toiminnan varautumiselle, jatkuvuuden hallinnalle ja tiedon turvaamiselle sekä niiden toteuttamiselle.

- Vaatimuksilla varmistetaan, että sopimuskumppani on ymmärtänyt palvelun tarpeet ja tuottaa palvelut sovitusti. Kriittisissä palveluissa tarjouspyynnössä on määritettävä varautumisvaatimukset ja mahdollinen erityistarve toiminnalle ”Force Majeure”-tilanteissa. Sopimusvaiheessa kumppanien on yhdessä sovittava, mitkä ovat hyväksyttävät varautumistoimenpiteet, joilla vaatimukset täyttyvät ja millä palvelu saadaan ylläpidettyä olosuhteiden mahdollistamalla tavalla myös ”Force Majeure” tilanteissa.

4.4.2 Toiminnan varmistaminen erityistilanteissa

Kumppani- ja palvelutoimittajaverkoston kanssa sovitaan toimintamallit ja vastuut häiriötilanteiden varalle.

Vaatimus 4.3:
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.

Vaatimus 4.4:
Yhteistoiminta kumppanien kanssa häiriötilanteiden 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.

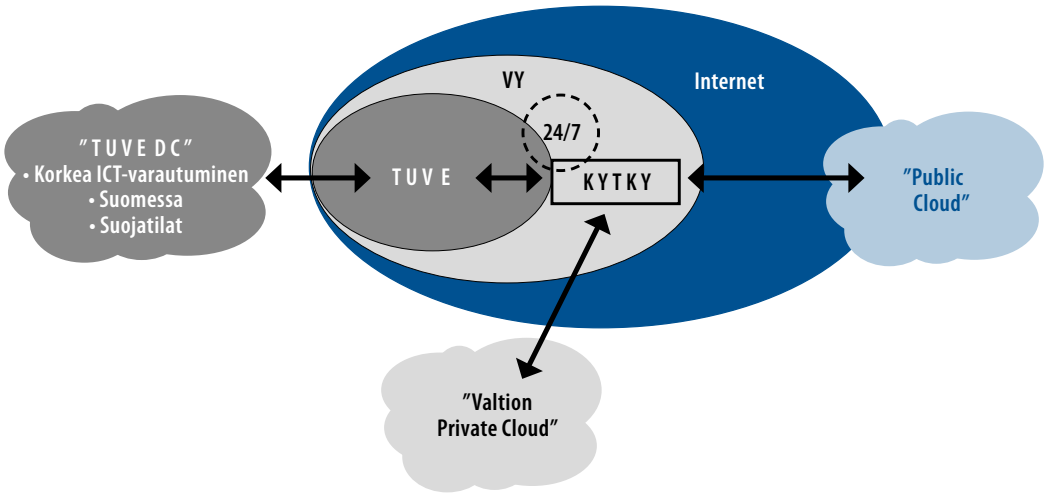
4.5 ICT-jatkuvuuden hallinta

Julkishallinnon palveluissa on varauduttava yhteiskunnan turvallisuusstrategian uhkamallien mukaisiin tapahtumiin ja varmistettava häiriötilanteissa toiminnan luonteen edellyttämä jatkuvuus.

Yhteiskunnan tietojärjestelmäratkaisuissa tasapainoilevat tietoturvallisuus (luottamuksellisuus – eheys – saatavuus), varautuminen ja kustannustehokkuus. ICT-varautumisen ja yhteentoimivuuden kannalta tulisi pyrkiä muodostamaan palvelukokonaisuuksia, joissa ylläpitäjinä ja tuottajina voivat olla julkishallinnon organisaatiot ja yritykset joko yhdessä tai erikseen. Esimerkki eritasoisten palvelujen hankkimisesta on kuvassa 11.

Palvelutuottajat vastaavat ylläpitämiensä palvelujen ja järjestelmien toimivuudesta sovitun palvelutason mukaisesti. Palvelutasoissa otetaan huomioon omistajien asettamat toiminnalliset vaatimukset. ICT-varautumiselle kuvataan, toteutetaan, koulutetaan ja testataan toteutustapa ja prosessi huomioiden uhkatekijät.

Kuva 11: Palveluiden hankinnassa ja toteuttamisessa on huomioitava varautuminen ja erilaiset verkkorakenteet



4.5.1 ICT-palvelujen ja järjestelmien elinkaaren hallinta

> Häiriösietoisten palvelujen kustannustehokas toteuttaminen edellyttää, että ICT-varautumisen vaatimuksia arvioidaan ja toteutetaan kaikissa järjestelmän elinkaaren vaiheissa.

Palveluiden arkkitehtuurissa sekä elinkaaren hallinnan kaikissa vaiheissa tulee huomioida yhteiskunnan turvallisuusstrategian uhkamallit ja varautuminen. Julkishallinnon viranomaisten täytyy palveluja rakentaessaan ottaa huomioon palvelulle asetettavat palvelutaso- ja toipumisaikavaatimukset sekä tarve vakavissa yhteiskunnallisissa häiriötilanteissa ja poikkeusoloissa säädellä ja priorisoida palvelujensa käyttöä ja ylläpitoa. Julkishallinnon kokonaisarkkitehtuureissa tulee huomioida ICT-varautuminen.

Vaatimus 5.1:
ICT-palvelun elinkaaren vaiheissa otetaan huomioon ICT-varautumisen vaatimukset.

- Turvallisten ja toimintavarmojen järjestelmien kehittäminen tai hankkiminen on kustannustehokkaampaa ja tuottavampaa kuin järjestelmien korjaaminen jälkikäteen. Mitä aikaisemmassa elinkaaren vaiheessa ICT-varautumisen vaatimukset huomioidaan, sitä kustannustehokkaammaksi palvelu kokonaiskustannuksiltaan tulee.
- Erityisesti korkean tason järjestelmissä voidaan arkkitehtuuri- ja teknologiaratkaisuilla pienentää uhkamallien toteutumisen aiheuttamia häiriöitä ja niistä aiheutuvia kustannuksia sekä varmistaa palvelujen jatkuvuutta ja nopeaa palautumista vakavissa häiriötilanteissa.

4.5.2 ICT-palvelujen jatkuvuuden turvaaminen

Tärkeimpien palvelujen tietojärjestelmät, tietokannat ja tietoliikenne tulee varmistaa häiriötilanteiden ja verkkohyökkäysten varalta.

Vaatimus 5.2:
Ydintoimintojen palvelutuotanto on varmistettu ja ydintoiminnoilla on varamenettelyt.

- Organisaation ydintoiminnat mahdollistaville tietojärjestelmille on määritetty sallitut keskeytysrajat, jonka perusteella palvelutuotanto pitää toteuttaa. Varamenettelyillä huolehditaan toiminnan jatkuvuudesta häiriötilanteissa.

Vaatimus 5.3:
Kriittisten toimintojen tarvitsemat tiedot on turvattu häiriötilanteissa.

- Tietojen saatavuus on organisaatioille keskeinen tarve. Tämän varmistamiseksi tarvitaan esimerkiksi kahdennusratkaisuja sekä ajallisia vaatimuksia toiminnalle tietynlaatuisissa häiriötilanteissa. Tämä saattaa rajoittaa joissakin palveluissa tai palvelun osissa pelkästään ulkomailta tapahtuvaa palvelutuotantoa.

Vaatimus 5.4:
Uhkien realisoituminen estetään käyttämällä fyysisen turvallisuuden menetelmiä ICT-ympäristön suojaamiseen.

- Toimi- ja laitetilojen sijoittamisella ja rakenteellisilla ratkaisuilla voidaan merkittävästi pienentää ulkoisen uhan riskiä ja vaikutuksia.

Vaatimus 5.5:
Tietoliikenteen toimivuudesta huolehditaan palvelujen kriittisyysluokittelun edellyttämällä tavalla.

- Tiedon ja palvelujen saatavuuden kannalta kriittinen elementti on tietoliikenteen toimivuus. Erityisesti korotetun ja korkean tason järjestelmissä tämä edellyttää erityistoimenpiteitä.

Vaatimus 5.6:
Tietojärjestelmien häiriöihin on varauduttu nopean palautumisen varmistamiseksi.

- Tämän päivän toimintaympäristölle on tyypillistä yllättävät ulkoisten tekijöiden ja teknisten haavoittuvuuksien yhteisvaikutuksesta syntyvät häiriötilanteet. Näiden vaikutusten pienentämisestä ja nopeaa toipumista edistävät merkittävästi ennalta suunnitellut ja keskeisiltä osin harjoitellut menettelyt, tekniset varajärjestelyt sekä johtamis- ja viestintätoimenpiteet.

4.6 Mittaaminen ja raportointi

Mittaaminen, raportointi ja auditoinnit tuottavat johtamiselle, strategioille ja toiminnan suunnittelulle tarvittavaa tietoa häiriötilanteita sietävän toiminnan kustannustehokkaalle kehittämiselle.

Palveluiden rakentamista, ylläpitämistä ja toimintaa seurataan organisaation johtoryhmän hyväksymän vuosikellon ja vastuujaon mukaisesti.

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

Raportointi muodostuu välittömistä häiriö- ja poikkeamailmoituksista sekä vuosikelloon sidotusta, analysoidusta yhteenvetoraportoinnista. Raportointi sidotaan myös normaaliin toiminnan ja talouden seurantaan, kuten tietotilinpäätös.

Vaatimus 6.1:
ICT-varautumisen 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.

Liite 1 ICT-varautumisen vaatimuskortit

1 Johtajuus

1.1 Organisaatiolla on tiedossa toimintaansa ja palveluihinsa liittyvä ICT-varautumista ohjaava lainsäädäntö ja muut normit ja nämä on huomioitu varautumisen linjauksissa ja toiminnassa

Perustaso

1.1-1: Organisaatiolla on tiedossa toimintaansa ja palveluihinsa liittyvä ICT-varautumista ohjaava lainsäädäntö ja muut normit ja nämä on huomioitu varautumisen linjauksissa ja toiminnassa.

Korotettu taso

1.1-2: Organisaatiolla on menettely ICT-varautumisen vaatimusten tunnistamiseksi ja näiden muutosten viemiseksi toiminnan suunnitteluun.

Korkea taso

1.1-3: Organisaation johto on varmistanut, että sen valtuudet a) vakavissa häiriötilanteissa ja b) poikkeusoloissa ovat tarkoituksenmukaiset ja organisaatiolla on kyky ottaa ne käyttöön.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.1-1: 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. Erityisen tärkeää on, että sekä palvelua hankkiva että palvelua tuottava organisaatio tuntee palveluun vaikuttavat määräykset ja pitävät toisensa näistä tietoisina.

Viraston toimintaa ohjaava lainsäädäntö ja muut ohjaavat asiakirjat on useimmiten tunnistettu ja listattu tietoturva- ja riskienhallintapolitiikan perusteissa. Virastojen strategioissa, periaatteissa ja toiminnan suunnittelussa on huomioitu valtioneuvostotason ohjausasiakirjoissa asetetut ICT-varautumista ohjaavat linjaukset.

1.1-2: Varautumiseen liittyvän vaatimuskokonaisuuden (ml. pakottavat ja suosittavat vaatimukset) seuranta ja siinä tapahtuvien muutosten kanavointi tietoturvan ja jatkuvuuden hallintaan on olennaista vastuuttaa tarkoituksenmukaiselle taholle. Vastuutetun toimijan (henkilö tai ryhmä) tehtävänä 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. Vastaavalla tavalla toimitaan palvelujen kohdalla, jossa palvelun eri osapuolten palvelupäälliköt (vast) arvioivat vaatimuksia ja vievät palvelua koskevia esityksiä palvelun johtoryhmään.

1.1-3: 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.

1.2 ICT-varautumisen linjaukset on määritetty toiminnan asettamien vaatimusten perusteella

Perustaso

1.2-1: Johto on päättänyt linjauksista ja tavoitteista toiminnan jatkuvuudelle ja ICT-varautumiselle.

1.2-2: ICT-varautumisen vastuut on määritetty prosessien omistajille.

Korotettu taso

1.2-3 Linjaukset, tavoitteet ja resurssit ICT-varautumiselle tarkistetaan toiminnan suunnittelun vuosikellon mukaisesti.

Korkea taso

1.2-4 Organisaation johto on varmistanut, että poikkeusolojen ydintoiminnot ja niiden jatkuvuuden hallinnan toteutustavat on määritelty ja dokumentoitu ja niitä testataan.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.2-1: Linjaukset ja tavoitteet on kuvattu esimerkiksi organisaation tietoturva- ja riskienhallintapolitiikoissa sekä jatkuvuussuunnitelmassa. Esimerkkejä suunnitelmista ja muiden asiakirjojen rungoista on 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. 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. Palveluihin kohdistuvat linjaukset kirjataan palvelusopimuksiin tai erillisiin asiakirjoihin.

1.2-2: Eri toimijoiden roolit ja vastuut kuvataan esim. palvelukuvauksissa, riskienhallinta- ja tietoturvaperiaatteissa erillisiin asiakirjoihin.

1.2-3: 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 vuosikellossa.

1.2-4: 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. Nämä menettelyt siirretään kuhunkin hankittavaan palveluun.

1.3 Häiriötilanteiden hallinta on linjattu, organisoitu ja huomioitu ohjausmalleissa

Perustaso

1.3-1 Häiriötilanteisiin liittyvä päätöksenteko ja poikkeamien käsittely on ohjeistettu ja vastuutettu.

Korotettu taso

1.3-2 Organisaation johto varmistaa, että toiminta- ja johtamismallit sekä toipumissuunnitelmat on määritetty riskiarvioiden perusteella todennäköisimmistä häiriötilanteista palautumiseen.

1.3-3 Häiriötilanteiden yhtenäinen perusohjeistus on koulutettu ja ulotettu sopimusvelvoittein palveluverkostoon.

Korkea taso

1.3-4: Organisaatiorakenteet ja toimintamallit tukevat häiriötilanteiden ja poikkeusolojen johtamista, hallintaa ja palautumista.

1.3-5: Organisaatiolla on prosessi koetuista häiriötilanteista oppimiseen.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.3-1: Päätöksenteon vastuut ja valtuudet on sovittu. Sijaisuudet on määritelty ja henkilöstö tietää miten tilannetta johdetaan. Nämä voidaan kuvata esimerkiksi organisaation jatkuvuudenhallintapolitiikassa ja hallintomalliasiakirjassa. On olemassa taho, joka käsittelee poikkeamat. Poikkeamasta ilmoittaminen tehdään vakioidulla lomakkeella tai intranetissä sähköisesti, josta se on helppo liittää riskiraporttiin. Hyödynnetään VAHTI 3/2005 –ohjetta, luku 2.

1.3-2: Jatkuvuussuunnitelmassa on esim. tapahtumamallien kautta kuvattuina tarvittavat toipumisjärjestelyt ja niiden johtaminen. Toipuminen sovitaan palvelukohtaisesti järjestelmän käyttöpalveluntoimittajan kanssa.

1.3-3: Jatkuvuussuunnittelu tulee ulottaa myös kolmansien osapuolien ylläpitämiin järjestelmiin. 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. Ohjeet on jaettu avainhenkilöille sähköisesti ja paperilla. Erityisohjeet voivat olla salaisia asiakirjoja ja vain nimettyjen henkilöiden käyttöön tarkoitettuja, mutta salassapidettäviä tulee säilyttää siten että niihin päästään tarvittaessa käsiksi silloinkin jos varsinaiset toimitilat ja normaalit tietojärjestelmät eivät ole käytössä.

1.3-4: Organisaatiorakenteiden muodostamisessa on huomioitu YTS-uhkamallit.

1.3-5: Häiriötilanteista kerätään systemaattisesti kokemukset ja viedään toimintaan, palveluihin ja järjestelmiin liittyvät kehittämistarpeet osaksi vuosikellon mukaista toiminnan ja talouden kehittämistä.

1.4 ICT-varautuminen on organisoitu ja vastuutettu osaksi normaalia johtamista, toimintaa sekä kumppanuusverkoston hallintaa

Perustaso

1.4-1: ICT-varautumisen johtamisen roolit ja vastuut on määritetty ja ne sisältyvät henkilöiden tehtäväkuvauksiin.

Korotettu taso

1.4-2: Organisaation johto on määritellyt organisaation tehtävien, palvelujen ja resurssien käytön priorisoinnin häiriötilanteissa.

Korkea taso

1.4-3: Resurssien lisääminen häiriötilanteissa ja poikkeusoloissa on sovittu palvelukohtaisesti palveluverkosto huomioon ottaen.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.4-1: Organisaation tehtävät varautumisen osalta määräytyvät mm. valmiuslain perusteella. Organisaatiossa käytetään henkilökohtaisia työnkuvia tai tehtävien roolikuvauksia. Kuvauksia on mallina VAHTI 3/2007 -ohjeen liitteessä 2. Toteuttamistapa voidaan kuvata hallintomallissa.

1.4-2: Jatkuvuussuunnitelmassa on huomioitu tehtävien ja priorisointi. Suunnitelman liitteenä voi olla tähän liittyvä vuosittain päivitettävä lista. Tehtävien, palvelujen ja resurssien käytön priorisoinnin tulee perustua realistisiin oletuksiin esimerkiksi hyödyntäen perusteellista liiketoiminnan vaikuttavuusanalyysia (BIA).

1.4-3: 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.

1.5 Varautumiselle ja jatkuvuuden hallinnalle on asetettu tavoitteisiin nähden riittävät resurssit

Perustaso

1.5-1: Tulosohjauksessa on osoitettu jatkuvuuden hallinnan ja tiedon turvaamisen tavoitteet ja resurssit.

Korotettu taso

1.5-2: ICT-varautumisen resursointi häiriötilanteita ja poikkeusoloja varten on huomioitu viraston budjetissa sekä toiminta- ja taloussuunnittelussa.

Korkea taso

1.5-3: Resurssien saatavuus ja riittävyys poikkeusoloissa on varmistettu.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.5-1: 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.

1.5-2: Riittävät henkilöresurssit arvioidaan jatkuvuussuunnitelmia laadittaessa. Tarvittavat hankinnat ym. lisäkustannukset on huomioitava budjetissa. Ministeriö päättää hallinnonalan kehyksen rahoittajana on huomioitava ICT-varautumiseen ja jatkuvuuden hallintaan annettavat. 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.

1.5-3: Resurssien tarve on arvioitu YTS-uhkamalleja vasten. Resurssien riittävyys testataan esim. varautumisharjoituksissa. Kumppanuussopimuksissa varmistetaan, että kriittsten toimintojen ylläpitoon on riittävä määrä henkilöstöä käytettävissä.

1.6 Varautumisen ja jatkuvuuden hallinnan suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä

Perustaso

1.6-1: Organisaation turvallisuuden yhteistyöryhmä käsittelee myös ICT-varautumiseen liittyviä asioita.

1.6-2: Organisaation johto käsittelee säännöllisesti jatkuvuuden ja tiedon turvaamisen tilannetta, linjauksia ja periaatteita sekä toteutumista ja koordinaatiota.

Korotettu taso

1.6-3: Ydintoimintojen palvelujen hallinta häiriö- ja erityistilanteiden varalta suunnitellaan yhdessä tukitoimintojen, keskeisten sidosryhmien ja palveluntuottajien kanssa.

Korkea taso

1.6-4: Suunnitelmien toimivuus palveluverkostossa on todennettu.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.6-1: Virastossa/organisaatiossa on eri toimialojen henkilöistä muodostettu yhteistyöryhmässä. Osa henkilöstöistä on turvallisuus, tietoturva ja valmiusihmisiä. Ryhmässä käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia. Yhteistyöryhmä on hyvä kokoontua vähintään kolme kertaa vuodessa. Sovitut toimenpiteet kirjataan pöytäkirjaan ja niiden toteutumista seurataan. Palvelun toimittajien kanssa asioita käsitellään esimerkiksi palvelun seurantaryhmässä.

1.6-2: 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.

1.6-3: Jatkuvuudenhallinta on toteutettava niin, että kaikki tarvittavat ydin- ja tukitoiminnot ovat mukana. 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.

1.6-4: Todentaminen voidaan toteuttaa varautumisharjoituksissa skenaarioharjoittelun avulla.

1.7 Organisaation johto seuraa varautumisen ja kyberturvallisuuden kehittämistä ja jatkuvuussuunnittelua sekä näihin liittyvien toimenpiteiden vaikutuksia ja kustannuksia

Perustaso

1.7-1 Organisaation johdolle raportoidaan riskianalyysin perusteella päätettyjen kehittämistoimenpiteiden edistymisestä normaalin raportoinnin osana.

Korotettu taso

1.7-2 Organisaation johdolle raportoidaan toimintaympäristön muutosten vaikutuksesta sekä varautumiseen ja häiriötilanteiden hallintaan liittyvistä kehittämistarpeista ja -toimenpiteistä.

Korkea taso

1.7-3 Säännöllinen raportointi johdolle perustuu päätettyihin jatkuvuuden hallinnan mittareihin ja tuloksia hyödynnetään toiminnan kehittämisessä.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.7-1: Organisaation johdolle annettava raportti 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.

1.7-2: Raportin sisältöön kuuluu tietoa resurssien käytöstä, ICT-varautumisen, jatkuvuuden hallinnan ja tiedon turvaamisen tavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyistä toimenpiteistä sekä muista merkittävimmistä tietoturvamuutoksista. Raporttien pohjalta kerätään seurantatietoa koulutuksen ja ohjeistuksen perusteiksi sekä toimintaprosessien kehittämiseksi ja turvallisemmiksi.

1.7-3: Toiminnan ja talouden suunnittelussa sovitut jatkuvuuden hallinnan mittarit ovat käytössä. Valtionhallinnossa suositellaan käytettäväksi mittareita, joilla voidaan tuottaa aineistoa valtionhallinnon seurantakyselyihin.

1.8 Viestinnän ja raportoinnin vastuut ja toimintamalli keskeisimpien sidosryhmien kanssa on määritetty ja organisoitu

Perustaso

1.8-1: Sisäisen ja ulkoisen kriisiviestinnän periaatteet, vastuut ja menetelmät on määritetty.

Korotettu taso

1.8-2: Viestintäkäytännöt ja -vastuut sekä varmentavat viestintävälineet ja menetelmät häiriötilanteessa on sovittu.

1.8-3: Sidosryhmille viestitään jatkuvuuden hallinnasta ja tietoturvallisuudesta vuosittain tai erikseen sovitulla aikataululla ja tavalla.

Korkea taso

1.8-4: Viestintää ja raportointia harjoitellaan ja kehitetään sidosryhmien palautteen perusteella erityistilanteiden ja poikkeusolojen näkökulmasta.

Esimerkkejä vaatimusten soveltamisen tueksi:

1.8-1: 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. Viestintä sisältää esimerkiksi pitkät käyttökatkot, suunnitellut korjaustoimenpiteet, haittaohjelmien aiheuttamat katkot tai tarkastustoimet, isojen tietomäärien varmistuksien palautukset jne.

1.8-2: Varmentavat menetelmät on etukäteen valmisteltu ja kaikki osapuolet ovat näistä tietoisia. Välineiden käyttöä on harjoiteltu. Sähköpostin lisäksi on käytettävissä esimerkiksi puhelin, telefax, lähetti tai tapaamisyhteys.

1.8-3: Keskeisiin sidosryhmiin vaikuttavista palvelujen jatkuvuuden hallinnasta ja tietoturvallisuudesta raportointi sekä poikkeamista tiedottaminen on organisoitu ja vastuutettu. 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.

1.8-4: Viestinnän varamenettelyjä harjoitellaan osana varautumisharjoitustoimintaa. Viestinnän nopeuttamista voidaan auttaa kehittämällä toiminnan rakenteita. Viestinnän onnistumisesta kerätään palautetta osana riskiraportointia.

2 Strategiat ja toiminnan suunnittelu

2.1 Organisaation ja toimintaympäristön vuorovaikutus otetaan toiminnassa huomioon

Perustaso

2.1-1: Yhteiskunnan turvallisuusstrategian uhkamallien mukaisten häiriöiden vaikutus tärkeimpiin palveluihin ja tietojen käsittelyyn on tunnistettu ja arvioitu.

Korotettu taso

2.1-2: Organisaation toiminnan kannalta keskeisistä toimintaympäristöistä sekä niihin liittyvistä palveluista, järjestelmistä ja toimijoista on ajantasainen dokumentaatio.

2.1-3: Organisaation johto käsittelee ja arvioi ydintoimintojen ICT-riippuvuuksia vähintään kerran vuodessa.

Korkea taso

2.1-4: Turvallisuus- ja toimintaympäristön muutostilanteet tunnistetaan ja niiden asettamat erityisvaatimukset otetaan toiminnassa huomioon.

Esimerkkejä vaatimusten soveltamisen tueksi:

2.1-1: 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.

2.1-2: 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.

2.1-3: Viraston tilaa ja riippuvuuksia arvioidaan osana toiminnan ja talouden suunnitteluprosessia (TTS) ja arvioinnin tulosten perusteella sovitaan tarvittavista kehittämistoimista. Riippuvuuksien arviointi on osa viraston riskienhallintaa.

2.1-4: Hallinnonalan ylin johto (esimerkiksi ministeriö) tekee yleensä arvion tilanteen muuttumisesta ja ohjeistaa valmistaviin toimenpiteisiin ryhtymisen. Näitä tilanteita harjoitellaan valmiusharjoituksissa, kuten VALHA. 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.

2.2 Riskienhallinnan tulokset ohjaavat varautumisen kehittämistä

Perustaso

2.2-1: Johto päättää riskienarvioinnin periaatteista ja arvioinnin perusteella tehtävistä riskien hallinnan toimenpiteistä sekä hyväksyy jäännösriskit.

Korotettu taso

2.2-2: Riskienhallinnan tulosten ja toimenpiteiden vaikuttavuusarvioinnin tuloksena määritetään ja dokumentoidaan ICT-varautumisen, jatkuvuuden hallinnan ja tiedon turvaamisen toteutustavat häiriötilanteiden, kyberuhkien ja poikkeusolojen varalle.

Korkea taso

2.2-3: Riskejä arvioidaan yhdessä sidosryhmien ja palveluntoimittajien kanssa käyttäen yhteismitallisia riskienhallintamenetelmiä.

Esimerkkejä vaatimusten soveltamisen tueksi:

2.2-1: Organisaatiolla on johdon hyväksymät riskien arviointiin ja hallintaan liittyvät periaatteet, menetelmä ja ohjeistus. Suurimmista riskeistä pidetään koko viraston ja palveluverkoston tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan. Jäännösriskien hyväksymisperusteet kirjataan ja niiden kehittymistä seurataan.

2.2-2: 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.

2.2-3: 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.

2.3 Varautumistoimenpiteet tukevat organisaation ydintoiminnan tavoitteita

Perustaso

2.3-1: Ydintoimintojen ja -prosessien suojattavat palvelut ja järjestelmät on tunnistettu ja sijoitettu perus-, korotetulle tai korkealle tasolle ydintoimintojen tai -prosessien vaatimusten mukaisesti.

Korotettu taso

2.3-2: Organisaatio kykenee priorisoimaan kriittiset palvelut häiriötilanteissa muiden palveluiden edelle.

Korkea taso

2.3-3: Ydintoimintojen prosessikuvauksiin on liitetty ICT-varautumisen kannalta oleelliset toimet.

2.3-4: Ydintoimintojen tavoitteisiin on liitetty ICT-varautumisen toteutumista kuvaavia mittareita.

Esimerkkejä vaatimusten soveltamisen tueksi:

2.3-1: Organisaation tulee tunnistaa ydintoimintansa. Ensimmäisessä vaiheessa tulee tunnistaa toiminnot, jotka ovat keskeisiä YTS:ssä määritettyjen strategisten tehtävien toteuttamisen kannalta. Toisessa vaiheessa on tunnistettava toiminnot, jotka ovat tärkeitä YTS:ssä kuvattujen uhkamallien mukaisien häiriötilanteiden hoitamisen kannalta. Varautumistoimenpiteet tulee suunnitella ydintoiminnan/ydinprosessien/ ydinpalveluiden tavoitteiden näkökulmasta, ei ainoastaan yksittäisen tukifunktion/tukipalvelun näkökulmasta.

2.3-2: 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.

2.3-3: Organisaation yksi ydintoiminto on asiointiprosessi. Prosessiin on kuvattu, miten asioijan henkilöllisyys tarkistetaan, miten asiointitietoja säilytetään ja miten tiedot suojataan jos tietoja siirretään toisille viranomaisille.

2.3-4: Mittarien tulee olla sellaisia, että ne tukevat toiminnan ja talouden raportointia, hallinnossa sovittua tulosohjausta ja VAHTI:n tekemää tietoturvakyselyä valtionhallinnon tietoturvallisuuden kehittymisestä.

2.4 Häiriötilanteiden hallinnan ja poikkeusolojen menettelyt on dokumentoitu, koulutettu ja harjoiteltu

Perustaso

2.4-1: Ydin- ja tukitoimintojen häiriötilanteiden toimintamalleissa ja suunnitelmissa on otettu huomioon ICT-palveluiden käytettävyys resurssien määrän mahdollisesti heikentyessä.

2.4-2: Toiminnan jatkuvuuden, tiedon turvaamisen ja varautumisen linjausten päivitys on vastuutettu sekä organisoitu.

Korotettu taso

2.4-3: Kriittisimmille palveluille on laadittu järjestelmäkohtaiset toipumisohjeet ja avainhenkilöille on koulutettu toiminta keskeisimmissä häiriötilanteissa.

2.4-4: Häiriötilanteiden toimintaohjeita kehitetään häiriö- ja erityistilanteista kerätyn aineiston ja saatujen kokemusten perusteella.

Korkea taso

2.4-5: Kriittisten ICT-palvelujen kapasiteetti ja resurssit on varmistettu sovitun minimitarpeen tasolle.

2.4-6: Jatkuvuus- ja valmiussuunnitelmia ohjeineen testataan ja harjoitellaan säännöllisesti käytännön tasolla erityistilanteiden ja poikkeusolojen hallitsemiseksi.

Esimerkkejä vaatimusten soveltamisen tueksi:

2.4-1: Organisaatio ymmärtää, että erityistilanteissa käytössä olevien ICT-palveluiden taso heikkenee ja toiminta pitää sopeuttaa siihen esimerkiksi keskeyttämällä tilapäisesti vähemmän tärkeitä toimintoja. Sopeuttamistoimet on suunniteltu ennalta.

2.4-2: Tietoturva- ja riskienhallintapolitiikan sekä tietoturvan kehittämissuunnitelman päivityksen valmistelu on vastuutettu esimerkiksi tietoturvapäällikölle ja jatkuvuussuunnitelman päivityksen valmistelu valmiuspäällikölle. Päivitysrytmiksi on sovittu kerran vuodessa, ja päivitys on vuosikellossa sidottu tehtäväksi riskien arvioinnin ja jatkuvuussuunnitelman testauksen yhteyteen.

2.4-3: Organisaation järjestelmäkohtaisissa ohjeistuksissa kuvataan mm: järjestelmän riippuvuudet muista järjestelmistä, kuinka järjestelmä asennetaan uudelleen, kuinka tiedot palautetaan, kuinka testataan että järjestelmä on saatu jälleen toimimaan normaalisti.

2.4-4: Organisaatiolla on kirjalliset toimintaohjeet mm. sähkökatkon, tietoliikennekatkon, järjestelmävian, keskeistä henkilöstöryhmää tai toimittajaa koskevan lakon, pandemian, tulipalon, myrskyn tai tulvan varalta. YTS:n uhkamallien hallinta pohjautuu hyvään jatkuvuussuunnitteluun. Jatkuvuussuunnitelmaan on kirjattu käytettävissä oleva henkilöstö, avainhenkilöt ja varahenkilöt sekä arvio heidän saatavuudestaan.

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.

2.4-5: 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.

2.4-6: Jatkuvuussuunnitelma on hyvä pöytätestata parin vuoden välein. Mikäli suunnitelma sisältää varatoimipaikkojen käyttöönoton, tulisi tämä harjoitella 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.

2.5 24/7-toiminta ja CERT-FI-yhteistoiminta vastaavat organisaation tavoitteita ja velvoitteita

Perustaso

2.5-1: Organisaatio on järjestänyt CERT-FI:n ilmoitusten vastaanoton.

2.5-2: Organisaatio ilmoittaa CERT-FI:lle vakavista tietoturvaloukkauksista ja niiden epäilyistä.

2.5-3: Tarpeet ympärivuorokautiselle palveluiden, järjestelmien ja verkkojen valvonnalle on määritelty.

Korotettu taso

2.5-4: Keskeiset palvelut ja niiden edellyttämä ICT ovat tarvittavassa laajuudessa 24/7-valvonnan ja siihen liittyvän raportoinnin piirissä.

Korkea taso

2.5-5: Organisaation ydintoiminnoissa on käytössä 24/7-toiminta, joka toimii kiinteässä yhteistyössä CERT-FI:n ja palveluverkoston kanssa.

Esimerkkejä vaatimusten soveltamisen tueksi:

2.5-1: Organisaatiossa on määrätty henkilöt, jotka ottavat vastaan CERT-FI:n lähettämiä varoituksia ja ilmoituksia.

2.5-2: Organisaatiolla on ohjeistettu ja koulutettu menettely ilmoituksien tekemiseen. Vakavia tietoturvaloukkauksia ovat mm. henkilötietojen varkaudet sekä laajat palvelunestohyökkäykset.

2.5-3: 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.

2.5-4: Organisaation Service Desk tai Help Desk -palvelu tarkastaa CERT-FI:n sivuilta ajankohtaiset 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. Laajemmissa ympäristöissä voidaan rekisterin ylläpitoa helpottamaan käyttää ratkaisua, joka automaattisesti kartoittaa ympäristön laitteet ja ohjelmistot. Palveluntoimittajan kanssa sovitaan seurantavelvoitteesta ja ilmoituksien aiheuttamista toimenpiteistä.

2.5-5: 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. 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

Palveluverkoston muodostavat esimerkiksi käyttöpalvelun toimittaja ja verkkooperaattori ja näiden alihankkijat, jotka tarvitaan ydintoiminnon tuottamisessa.

3 Henkilöstö

3.1 ICT-varautumisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään

Perustaso

3.1-1: Henkilöstön roolit ja vastuut jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelussa ja toteuttamisessa on määritetty myös häiriötilanteet huomioiden.

Korotettu taso

3.1-2: Osaamisen johtamisessa seurataan tietoturvallisuuden ja ICT-varautumisen koulutuksien toteutumista.

Korkea taso

3.1-3: Häiriötilanteiden ja poikkeusolojen asettamat vaatimukset on otettu huomioon henkilösuunnittelussa, tehtävänkuvauksissa ja koulutuksessa.

3.1-4: Palveluverkoston osaamisen varmistaminen ja kehittäminen on organisoitu ja ydintoiminnan kannalta keskeinen osaaminen on kartoitettu.

Esimerkkejä vaatimusten soveltamisen tueksi:

3.1-1: Organisaatiossa on määritelty VAHTI 3/2007 -ohjeen liitteen 2 mukaiset roolit ja yleisellä tasolla tehtävän edellyttämä osaaminen.

3.1-2: 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. Muuttuneista ohjeista järjestetään info-tilaisuus sekä tiedotetaan sähköisiä kanavia käyttäen. Henkilöstön koulutuksessa otetaan huomioon myös organisaatiossa ja toimintaympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat.

3.1-3: 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.

3.1-4: Hankintojen yhteydessä edellytetään palvelun tuottamiseen osallistuvilta avainhenkilöiltä riittävää osaamista ja sen ylläpitoa. Palveluverkoston osaamista kehitetään yhteisillä harjoituksilla. Osaamiskartoitusten avulla valvotaan osaamistason toteutumista.

3.2 Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia

Perustaso

3.2-1: Henkilöstön turvallisuustietoisuutta ja -osaamista kehitetään.

Korotettu taso

3.2-2: Tietoturva- ja varautumisasioiden koulutus on integroitu osaksi organisaation muuta koulutusta ja toimintaa.

3.2.3: Henkilöstö osallistuu häiriö- ja erityistilanteiden vaikutuksien arviointiin ja hallintakeinojen kehittämiseen.

Korkea taso

3.2-4: Henkilöstöä kannustetaan osallistumaan erilaisiin varautumista tukeviin yhteistyöryhmiin.

Esimerkkejä vaatimusten soveltamisen tueksi:

3.2-1: 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.

3.2-2: Kaikkeen koulutukseen olisi hyvä integroida vaikka pari lausetta koulutettavaan asiaan oleellisimmin liittyvistä tietoturva- ja varautumisasioiden toimintatavoista organisaatiossa ja koulutettavassa palvelussa.

3.2-3: Jatkuvuusharjoituksiin ja niiden purkuun sekä jatkotoimenpiteiden suunnitteluun osallistuu edustajia organisaation kaikilta tasoilta. Keskeisimmät henkilöt ydinpalveluista otetaan mukaan suunnitteluun. Kokonaiskuvan varmistamiseksi tulee varmistaa harjoituksen heterogeeninen kokoonpano.

3.2-4: Organisaatio nimeää asiantuntijoita yhteistyöryhmiin.

3.3 Organisaatiossa on määritetty menettelyt valvonnan toteuttamiseen ja toimintaan turvallisuuspoikkeamissa ja väärinkäytöstilanteissa

Perustaso

3.3-1: Henkilöstö tietää, kenelle väärinkäytöksistä ja turvallisuuspoikkeamista tai niiden uhkista tulee ilmoittaa.

3.3-2: Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu.

Korotettu taso

Korkea taso

3.3-3: Poikkeusolojen tarpeet ja mahdollisuudet tarvittaessa rajoittaa ja valvoa työntekijän toimintaa (yksityisyyden suojaa) työpaikalla on kartoitettu.

3.3-4: Organisaatiossa tai sen tukena on turvallisuuspoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.

Esimerkkejä vaatimusten soveltamisen tueksi:

3.3-1: Riskiraportoinnissa kirjataan tapahtumat ja esimiesten tehtävä on puuttua laiminlyönteihin. Tietoturvamääräysten ja -ohjeiden noudattamatta jättämisen mahdolliset seuraukset on kuvattu tietoturvapolitiikassa ja tiedotettu kaikille organisaatiossa työskenteleville. Vastaa TTT 1.3.3.2-vaatimusta.

3.3-2: 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. Vastaa TTT 1.3.2.5-vaatimusta.

3.3-3: Organisaatio on valmistellut menettelyt esimerkiksi viestiliikenteen rajoittamiseksi.

3.3-4: Ryhmä voi koostua organisaation omasta henkilöstöstä tai voidaan käyttää hallinnonalan tai palveluntarjoajan kokoamaa ryhmää. Poikkeamien selvittely edellyttää riittävän teknisen ja juridisen osaamisen. Rikosepäilyissä poliisi on tutkiva viranomainen. Tietoturvaryhmän täydennyskoulutus sisältää erilaisten häiriötilanteiden selvittelyn harjoittelua ja yhteistoimintaa poliisin kanssa. Vastaa TTT 1.3.3.4-vaatimusta.

3.4 Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt on suunniteltu

Perustaso

3.4-1: Avaintehtävät on tunnistettu ja niihin on nimetty varahenkilö tai -henkilöt.

3.4-2: Kriittisistä tehtävistä vastuulliset avainhenkilöt on koulutettu toimimaan häiriötilanteissa.

Korotettu taso

3.4-3: Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön varajärjestelyt.

3.4-4: Avainhenkilöstö harjoittelee säännöllisesti ylläpitämään kriittisiä toimintoja erityistilanteissa.

Korkea taso

3.4-5 Kriittisten tehtävien toteuttamisen edellyttämät varajärjestelyt poikkeusoloissa on testattu ja harjoiteltu.

Esimerkkejä vaatimusten soveltamisen tueksi:

3.4-1: Varahenkilö voi olla myös organisaation ulkopuolinen henkilö, mutta tällöin asiasta sovittaessa tulee kiinnittää erityistä huomiota varahenkilön kouluttamiseen sekä siihen että varahenkilö on tarvittaessa käytettävissä.

3.4-2: Järjestelmien asiantuntijoilla on riittävä häiriötilanteiden hallintaan liittyvien ohjeiden osaaminen ja ohjeet ovat helposti saatavilla. Tietoturvapoikkeamia selvittävät henkilöt on nimetty ja koulutettu.

3.4-3: Vaihtoehtoinen toimintatapa on suunniteltu jatkuvuussuunnitelmassa.

3.4-4: Organisaatio järjestää vuosittain vähintään pöytätestauksen johonkin erityistilanteeseen liittyvästä skenaariosta. Mikäli mahdollista, avainhenkilöt osallistuvat myös valtionhallinnon yhteisiin harjoituksiin (esim. VALHA, TIETO).

3.4-5: 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.

3.5 Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla

Perustaso

3.5-1: Poikkeusolojen varalle on tehty ja ylläpidetty henkilövaraukset (VAP).

Korotettu taso

3.5-2: Palveluverkoston kriittiset erityisosaamisalueet on kartoitettu ja ne on huomioitu palvelujen hankinnassa ja henkilöstön käytössä sekä muussa resursoinnissa.

Korkea taso

3.5-3: Henkilövarausten (VAP) ja niihin liiittyvän ohjeistuksen ajantasaisuus tarkistetaan vuosittain, myös palveluketjuissa.

3.5-4: Kriittisten palvelujen osalta on toteutettu lakko-oikeuksien poistaminen ja valmisteltu hätätöiden käyttö.

Esimerkkejä vaatimusten soveltamisen tueksi:

3.5-1: Henkilöiden VAP-varaukset (Vapautus aseellisesta palvelusta) tarkastetaan vähintään kahden vuoden välein ja silloin kun henkilöstö vaihtuu. Virasto esittää varaukset organisaation alueen sotilaslääninn esikuntaan. Lisätietoja Asevelvollisuuslaki 89 §.

3.5-2: Ydintoiminnot on kuvattu prosesseineen ja niihin liittyvät turvakontrollit määritelty ja toteutettu. Henkilöt varahenkilöineen on määrätty ja tietävät tehtävänsä. Palveluverkoston henkilöstön osaaminen ja kyky toimittaa palvelua erilaisissa häiriötilanteissa tunnetaan, eikä kriittisiä palveluja hankita toimittajalta jonka toimituskyky ei ole riittävällä tasolla.

3.5-3: 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.

4 Kumppanuudet ja resurssit

4.1 Organisaation toiminnalle välttämättömät kumppanit, alihankkijat ja resurssit on tunnistettu

Perustaso

4.1-1: Palveluverkoston eri toimijoiden merkitys ICT-palveluille on tunnistettu.

Korotettu taso

4.1-2: Palveluverkosto on tärkeimmiltä osiltaan kuvattu ja jatkuvuudenhallinnan toimintaperiaatteet on sovittu ja koulutettu.

4.1-3: Ydintoiminnan ja sen jatkuvuuden edellyttämien verkoston palvelujen ja muiden resurssien saatavuus häiriötilanteissa ja poikkeusoloissa on selvitetty.

Korkea taso

4.1-4: Ydintoiminnan ja sen jatkuvuuden edellyttämien verkoston palvelujen ja muiden resurssien käytettävyys erityistilanteissa ja poikkeusoloissa varmistetaan suurien muutosten yhteydessä ja vuosittain.

Esimerkkejä vaatimusten soveltamisen tueksi:

4.1-1: 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. Erityisesti riippuvuus ulkopuolisista toimijoista on selvitettävä kunkin ydinpalvelun osalta ja määriteltävä tarvittavat toimenpiteet.

4.1-2: Palveluverkoston kuvauksissa huomioidaan myös alihankkijoiden alihankkijat, joilla on merkitystä palvelun jatkuvuuden ja turvallisuuden kannalta.

4.1-3: 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.

4.1-4: 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. 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.

4.2 Sopimuksissa on vaatimukset toiminnan varautumiselle, jatkuvuuden hallinnalle ja tiedon turvaamiselle sekä niiden toteuttamiselle

Perustaso

4.2-1: Palvelusopimuksessa määritellään, mitä ICT-varautumisen tasoa palvelun, palvelutoimittajan ja tämän mahdollisen alihankintaverkoston on noudatettava.

Korotettu taso

4.2-2: Sopimusosapuolten kanssa tarkastellaan sopimuksen toteutumista ja jatkuvuudenhallinnan tarpeita vuosittain.

Korkea taso

4.2-3: Palveluverkoston palvelu- ja turvallisuussopimuksia ylläpidetään ja niiden noudattamista auditoidaan säännöllisesti.

Esimerkkejä vaatimusten soveltamisen tueksi:

4.2-1: 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.

4.2-2: Voimassa olevat sopimukset on hyvä käydä läpi ja pyrkiä tekemään niihin tarvittavat lisäykset/muutokset . Jatkuvuuden hallinta on aiheellista ottaa sopimusryhmän agendalle vähintään kerran vuodessa. 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.

4.2-3: Auditointi perustuu vuosisuunnitteluun ja kulloinkin kohteiksi valittavien osa-alueiden arviointiin. Auditointisuunnitelmat laaditaan yhteistyössä palveluntoimittajan kanssa välttäen päällekkäistä auditointia. Palveluntoimittajan turvallisuuden hallintajärjestelmän toimivuuteen voidaan esimerkiksi luottaa ilman erillistä auditointia, jos se on sertifioitu esimerkiksi ISO/IEC 27001ja ISO 27002 tai muiden vastaavanlaisten standardien mukaisesti. Tällöin auditoinnissa voidaan keskittyä ICT-varautumisen vaatimusten toteutumiseen.

4.3 Kriittisen toiminnan jatkuvuuden ja tiedon turvaamisen hallintavelvoite on ulotettu keskeiseen toimittajaverkostoon

Perustaso

4.3-1: Sopimusosapuolten vastuut resurssien hallinnasta ja saatavuudesta on sovittu.

4.3-2: Keskeisen toimittajaverkoston kyky tuottaa tilaajan toiminnan kannalta keskeisiä palveluja häiriötilanteissa tunnetaan.

Korotettu taso

4.3-3: Tärkeimpien palvelujen tuotanto ja ylläpito kyetään priorisoimaan palveluverkostossa.

4.3-4: ICT-järjestelmien valvonnan, hallinnan ja ylläpitämisen yhteistoimintamallit keskeisessä toimittajaverkostossa on organisoitu ja sovittu.

Korkea taso

4.3-5: Jatkuvuudenhallintamenettelyt on otettu käyttöön koko palveluverkostossa ja niiden toimintaa testataan ja harjoitellaan säännöllisesti.

Esimerkkejä vaatimusten soveltamisen tueksi:

4.3-1: Sopimuksessa palveluntoimittajaa velvoitetaan edellyttämään riittävää jatkuvuuden hallintaa ja tiedon turvaamista myös palvelun kannalta keskeisiltä alihankkijoiltaan. Vastuista sovittaessa määritellään sekä tilaajan että palvelutoimittajan vastuut.

4.3-2: Tarjouspyynnössä ja tarjoajan soveltuvuutta arvioitaessa huomioidaan sen kyky vastata toimintansa jatkuvuudesta. Tilaaja selvittää miten toimittaja kykenee toimimaan häiriötilanteissa ja sopii toiminnasta osana turvallisuussopimusta.

4.3-3: 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.

4.3-4: Menettelyistä on sovittu turvallisuussopimuksessa. Ulkoistettujen palveluiden kohdalla priorisointi saattaa edellyttää sopimusmuutoksia. Yhteistyön osapuolilla on nimetyt vastuuhenkilöt, jotka koordinoivat yhteistyötä. Yhteistyön toimintaa käsitellään tilaajan ja toimittajan kesken palvelun seurantaryhmissä.

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.

4.3-5: Jatkuvuussuunnitelmien toimivuutta arvioidaan säännöllisesti pöytätesteillä ja palveluverkoston yhteisillä harjoituksilla sekä auditoimalla.

4.4 Yhteistoiminta kumppanien kanssa häiriötilanteiden hallitsemiseksi on organisoitu ja vastuutettu

Perustaso

4.4-1 Häiriötilanteiden yhteistoimintaperiaatteet viranomaisten ja muiden sidosryhmien kanssa on suunniteltu ja keskeisimmiltä osiltaan koulutettu avainhenkilöille.

Korotettu taso

4.4-2 Sidosryhmien ja palveluntuottajien kanssa arvioidaan säännöllisesti palvelun jatkuvuutta ja siihen kohdistuvia uhkia YTS uhkamallien pohjalta.

4.4-3 Häiriötilanteiden yhteistoiminta ja kriisitiedottaminen viranomaisten sekä keskeisten sidosryhmien kanssa on suunniteltu, toteutettu ja keskeisimmiltä osiltaan harjoiteltu.

Korkea taso

4.4-4 Poikkeusolojen yhteistoiminta viranomaisten ja muiden sidosryhmien kanssa on todennettu ja harjoiteltu.

4.4-5 Poikkeusolojen yhteistoimintaa toimittajaverkostossa testataan ja harjoitellaan säännöllisesti.

Esimerkkejä vaatimusten soveltamisen tueksi:

4.4-1: 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.

4.4-2: Yhteistoimintakäytännöt on kuvattu jatkuvuussuunnitelmassa ja niitä käsitellään avainhenkilöstön koulutuksessa ja harjoittelussa.

4.4-3: 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.

4.4-4: Organisaatio harjoittelee viranomaisten ja muiden sidosryhmien kanssa.

4.4-5: Yhteistoimintaa harjoitellaan esimerkiksi valtionhallinnon TIETO- ja VALHA-harjoituksissa sekä organisaatioiden omissa varautumisharjoituksissa.

5 ICT-jatkuvuuden hallinta

5.1 ICT-palvelun elinkaaren vaiheissa otetaan huomioon ICT-varautumisen vaatimukset

Perustaso

5.1-1 Prosessin/toiminnon omistaja määrää, mitä tietoturva- ja varautumistasoa järjestelmän tulee noudattaa.

5.1-2 ICT-järjestelmien omistajat tietävät ICT-varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti.

5.1-3 Viranomaisten kokonaisarkkitehtuureissa on kuvattu tietojärjestelmien yhteentoimivuuden varmistaminen.

Korotettu taso

5.1-4 ICT-varautuminen sisältyy ICT-hankkeiden elinkaaren kaikkien vaiheiden dokumentaatioon.

5.1-5 Arkkitehtuurivalinnoissa huomioidaan uhka-arviot (YTS) ja ICT-varautumisen vaatimukset.

5.1-6 Järjestelmään tehdään tietoturvatestaukset ennen hyväksyttyä käyttöönottoa.

Korkea taso

5.1-7 Kehitys- tai räätälöintityön aikana järjestetään katselmointeja varautumisen kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.

5.1-8 Järjestelmään tehdään tarvittava auditointi ennen kuin se otetaan tuotannolliseen käyttöön.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.1-1: Ennen jokaista sopimusta, budjetointia ja kehittämistä tulee varmistua, että järjestelmä on luokiteltu tietoturvan ja varautumisen suhteen.

5.1-2: Keskeisiin järjestelmän ylläpitotehtäviin tulee sisällyttää vastuut varautumisen suunnittelusta ja toteuttamisesta.

5.1-3: Tietojärjestelmien yhteentoimivuus on häiriötilanteisiin varautumisen perusedellytys. Tietohallintolaki velvoittaa julkishallinnon viranomaisia kuvaamaan kokonaisarkkitehtuurissaan yhteentoimivuuden toteuttamisen ja varmistamisen sekä noudattamaan järjestelmäkehityksessään tähän liittyviä määrittelyjä.

5.1-4: ICT-hanke on kuvattu tietojärjestelmäkehityksen vaiheistuksen mukaisesti prosessiksi, jossa on mukana turvallisuusasioiden tarkastelupisteet. Kussakin pisteessä arvioidaan tulokset ja päätetään siirtymisestä seuraavaan kehitysvaiheeseen. Arkkitehtuurivalinnoissa, projektihallinta- ja systeemityömenetelmissä sekä -ohjeissa huomioidaan jatkuvuuden hallinta, tiedon turvaamisen ja ICT-varautumisen vaatimukset. Hankkeen johtoryhmä päättää toimenpiteiden riittävyyden riskiarvioinnin perusteella. 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. Hankkeissa voidaan käyttää apuna VAHTI-ohjeiden tarkastuslistoja ja esimerkiksi standardeja, NFPA 1600, ISO 27005.

5.1-5: Arkkitehtuurivalinnoissa, projektihallinta- ja systeemityömenetelmissä sekä -ohjeissa painotetaan jatkuvuuden hallinnan, tiedon turvaamisen ja ICT-varautumisen vaatimusten huomioon ottamista. Hankkeen projektihallinta auditoidaan ulkopuolisen toimesta. Ohjeistuksessa hyödynnetään tarkastuslistoja, joita on tausta- aineistoissa mainituissa VAHTI-ohjeissa.

5.1-6: 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).

5.1-7: Katselmointeja järjestetään esimerkiksi työparikatselmointeina, projektiryhmän tai ohjelmointitiimin kokouksissa tai ulkopuolisen auditoijan tekeminä.

5.1-8: Auditointi toteutetaan ulkoisen auditoijan toimesta, esimerkiksi Kansallisen tietoturvaviranomaisen toimesta tai sen ohjeistuksen mukaisesti esim. KATAKRIa hyödyntäen.

5.2 Ydintoimintojen palvelutuotanto on varmistettu ja ydintoiminnoilla on varamenettelyt

Perustaso

5.2-1 Ydintoimintojen varamenettelyt ja häiriöistä toipumisen prosessit on suunniteltu ja dokumentoitu.

Korotettu taso

5.2-2 Ydintoimintojen palvelutuotannon ja hallinnan prosesseissa on sovittu, ohjeistettu ja koulutettu häiriötilanteiden hallinta sekä varamenettelyt.

5.2-3 Keskeisten palvelujen varavoimansaanti häiriötilanteissa on toteutettu riskianalyysin perusteella päätetyllä tavalla.

Korkea taso

5.2-4 Ydintoimintojen järjestelmien käyttöpalveluiden ja tuotanto-operoinnin poikkeusolojen toteutus on huomioitu ja todennettu sopimuksissa ja toiminta on harjoiteltu.

5.2-5 Saatavuudeltaan aikakriittisiin palveluihin, joiden sallittu keskeytysaika organisaatiossa erikseen määritellään, on mahdollistettava häiriötilanteissa valvottu etäylläpito.

5.2-6 Kriittisten palvelujen ja sovellusten käyttöoikeudet hallitaan ja valvotaan Suomesta.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.2-1: Organisaation tulee tunnistaa tärkeimmät toimintonsa ja niiden tarvitsemat palvelut.

5.2-2: Palvelun toimittajalla pitää olla kuvattuna toimintansa häiriötilanteiden varalta ja testattuna niiden toimivuus. Varajärjestelmät palvelun tuottamiseen on sovittava sopimuksissa.

5.2-3: 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. Otetaan käyttöön esim. viestintäviraston suositukset ja KATAKRI-kriteeristön tätä kohtaa koskevat kriteerit.

5.2-4: 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. Tuotantomuutokset, tarvittava osaaminen ja resurssit sekä varajärjestelyihin siirtyminen ja toipuminen poikkeusoloissa on suunniteltu, varmistettu, dokumentoitu ja säännöllisesti harjoiteltu.

5.2-5: Vakavissa häiriötilanteissa pitää heti käynnistää estävät ja palauttavat ylläpitotoimenpiteet. Tällöin voi olla välttämätöntä avata ylläpitoon etäyhteys. Ulkopuolisen toimijan kohdalla on ennakolta valmisteltava ja akreditoitava prosessit, tilat ja yhteydet.

5.2-6: Laajat, vakavat häiriötilanteet saattavat edellyttää nopeita muutoksia palvelujen käyttöoikeuksiin. Varautumisen kannalta aikakriittisyys edellyttää, että toimenpiteet tehdään Suomesta ja Suomen lainsäädännön alaisena (esim tietoliikennekatkokset, poikkeusolojen toimivaltuudet jne).

5.3 Kriittisten toimintojen tarvitsemat tiedot on turvattu häiriötilanteissa

Perustaso

5.3-1 Tietoaineistojen turvallisuudelle on asetettu vaatimukset luottamuksellisuuden, eheyden ja saatavuuden suhteen.

Korotettu taso

5.3-2 Tietoaineistojen käyttö häiriötilanteissa on suunniteltu, dokumentoitu, toteutettu ja testattu.

5.3-3 Organisaatiossa otetaan kriittisistä järjestelmistä varmistusten lisäksi suojakopioita, joita säilytetään toisessa rakennuksessa eri palotilassa kun varsinaisia tietoja.

Korkea taso

5.3-4 Tietoaineistojen käyttö poikkeusoloissa on suunniteltu, dokumentoitu, toteutettu ja testattu.

5.3-5 Kriittisten toimintojen tietoaineistot on hajautettu maantieteellisesti vähintään kahteen eri paikkaan Suomessa.

5.3-6 Kriittisten toimintojen palvelutuotanto sijaitsee Suomessa.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.3-1: Organisaation käytössä olevat tietoaineiston hallinnan ohjeet ja välineet tukevat aineistojen luokittelua ja arkistointia. Ohje sisältää eri suojaus- ja turvaluokkiin kuuluvien aineistojen hallinnan sen elinkaaren eri vaiheissa. Tietojen varmistukset on hoidettu huomioiden niiden tärkeys toiminnalle.

5.3-2: Jatkuvuudenhallinnan suunnitelmassa kuvataan tietoaineistojen käsittelyn osuus. Suunnitelmia testataan ja niiden toimivuutta arvioidaan säännöllisesti.

5.3-4: Toiminnan hajautus perustuu valtionhallinnon toimijan tärkeysluokkaan ja sen ydintoimintojen (tuottamien palveluiden) tärkeyteen valtionhallinnolle.

5.3-5: Palvelusopimus sisältää varautumiseen liittyvät vaatimukset palveluntoimittajalle. Valmiussuunnitelmassa kuvataan tietoaineistojen suojaaminen. Suunnitelmaa testataan ja sen toimivuutta arvioidaan säännöllisesti.

5.3-6: 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.

5.4 Uhkien realisoituminen estetään käyttämällä fyysisen turvallisuuden menetelmiä ICT-ympäristön suojaamiseen

Perustaso

5.4-1: Organisaatiossa on tunnistettu tilojen tarvitsema suojausluokka.

5.4-2: Tärkeät laitteet ja laitetilat on suojattava ympäristötekijöitä vastaan (murto, palo, lämpö, kosteus, kaasut, vesi ja pöly).

Korotettu taso

5.4-3 Organisaatiolla on suunnitelma ICT-palvelujen tuotannon siirtämisestä toisiin tiloihin mikäli nykyiset tilat muuttuvat käyttökelvottomiksi.

Korkea taso

5.4-4 Keskeiset laitetilat on suojattu toimitiloihin kohdistuvaa ulkoista hyökkäystä vastaan.

5.4-5 Toimitilajärjestelyt mahdollistavat korkean tason palveluille fyysisesti riittävän kaukana sijaitsevan varatoimipaikan, jossa toimintaa voidaan jatkaa jos varsinainen toimipaikka muuttuu käyttökelvottomaksi.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.4-1: 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.

5.4-2: Suojaamisessa sovelletaan tilan käyttötarkoituksen mukaisia yleisiä ohjeita, Esimerkiksi viestintäviraston teletiloja koskeva ohjeistus.

5.4-3: Tilat voivat olla esimerkiksi organisaation toinen toimipiste toisella paikkakunnalla. Tämä on huomioitu jatkuvuussuunnitelmassa. Esimerkiksi KATAKRI:n kriteerien soveltaminen.

5.4-4: 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 ja terrorismi. Esimerkiksi KATAKRI:n kriteerien soveltaminen.

5.4-5: Esimerkiksi Suomen Huoltovarmuusdata Oy tarjoaa valtion ja yksityisen sektorin huoltovarmuuskriittisille organisaatioille turvallista 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 ja riittävä etäisyys päätetään riskianalyysin perusteella. Suojarakentamisen yksityiskohtaisia lujuuksia ja materiaalivahvuuksia on lueteltu sisäasiainministeriön antamassa asetuksessa.

5.5 Tietoliikenteen toimivuudesta huolehditaan palvelujen kriittisyysluokittelun edellyttämällä tavalla

Perustaso

5.5-1 Organisaatio on tunnistanut tietoliikenteen kriittisyyden omassa toiminnassaan ja palveluissaan.

Korotettu taso

5.5-2 Tietoliikennelaitteiden, -yhteyksien ja kytkentäpisteiden sijainti on otettu huomioon suojausluokittelussa.

5.5-3 Valtionhallinnon keskeisimmät palvelut tukeutuvat VY-verkon ratkaisuihin.

5.5-4 Organisaatio on yhdessä palveluntoimittajan kanssa analysoinut, suunnitellut ja sopinut tietoliikennepalvelujen priorisoinnin ja muutokset häiriötilanteissa.

Korkea taso

5.5-5 Julkisen hallinnon kriittisimmät palvelut ja niiden tiedonsiirto toteutetaan mahdollisuuksien mukaan hallinnon turvallisuusverkon vaatimusten mukaisesti.

5.5-6 Verkkoympäristöt ja tietoliikennepalvelut varmennetaan siten, ettei yhden operaattorin palvelutason heikentyminen keskeytä toiminnan edellyttämää palvelua.

5.5-7 Organisaatio on suunnitellut, sopinut ja testannut palveluverkoston tietoliikennepalvelujen priorisoinnin ja muutokset poikkeusoloissa.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.5-4: 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.

5-5-5: Palvelujen riittävän korkeatasoinen toteutuksen varmistamiseksi Valtiovarainministeriö vahvistaa sovellettavat vaatimukset.

5.5-6: 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. Järjestelmien tekniset ja toiminnalliset vaatimukset on tunnistettu ja niiden ratkaisut on määritelty ja riskit on arvioitu. Erikseen valittuihin työasemiin voidaan esimerkiksi asentaa erillinen tietoliikenneyhteys jonka kautta voi päästä yleiseen tietoverkkoon (varayhteys).

5.6 Tietojärjestelmien häiriöihin on varauduttu nopean palautumisen varmistamiseksi

Perustaso

5.6-1 Organisaatiolla on ydintoimintojen varmistamiseksi kuvattu toipumisprosessi.

5.6-2 Palveluittain on määritetty toimenpiteiden käynnistämiskyky.

Korotettu taso

5.6-3 Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat.

5.6-4 Kriittisten palvelujen verkko-, palvelin- ja laiteympäristöt varmennetaan esimerkiksi kahdentamalla.

Korkea taso

5.6-5 Palvelinympäristöjen vikasietoisuus vastaa häiriötilanteiden ja poikkeusolojen vaatimuksia.

5.6-6 Organisaatio harjoittelee palveluketjuittain häiriötilanteiden varalle.

Esimerkkejä vaatimusten soveltamisen tueksi:

5.6-1: Organisaation ydintoimintojen tarvitsemat järjestelmät on tunnistettu.

5.6-2: 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. Ulkoistetuissa palveluissa on oltava riittävät palvelutaso-sopimukset.

5.6-3: Toipumissuunnitelmien olemassaolosta vastaa aina palvelun tilaaja. Ulkoistetussa palvelussa järjestelmäkohtaisten toipumissuunnitelmien valmistelusta vastaa palveluntarjoaja. Tilaaja arvioi toipumissuunnitelman testaamalla sitä.

5.6-4: 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.

5.6-5: Palvelinympäristöjen mitoituksessa ja teknisissä rakenteissa ohjaava tekijä on YTS 2010 uhkamallien mukaisten häiriötilanteiden ja poikkeusolojen olosuhteet.

5.6-6: Organisaation on tunnettava koko palveluketjun toimivuus ja osana omaa jatkuvuus- ja varautumisharjoittelua käytävä läpi sen toimivuus eri tilanteissa.

6 Mittaaminen ja raportointi

6.1 ICT-varautumisen toteutumista ja tarkoituksenmukaisuutta seurataan ja arvioidaan

Perustaso

6.1-1: Jatkuvuuden, tiedon turvaamisen ja varautumisen tavoitetason saavuttamista seurataan toiminnan ja talouden suunnitteluprosessissa.

6.1-2: Palvelutuottajien tuottamien tietojenkäsittelypalveluiden tilaa ja kehittämistoimenpiteitä seurataan säännöllisesti.

6.1-3: Auditoinnit tai itsearvioinnit toteutetaan suunnitelmallisesti ja ne ovat johdon hyväksymiä.

Korotettu taso

6.1-4 Sisäinen tarkastus toimintona (tarkastussuunnitelma) ja esimiehet suorittavat säännöllisesti tuotteiden, palvelujen, toimintojen, prosessien ja järjestelmien riskiarvioinnin sekä jatkuvuuden hallinnan tarkastuksia.

6.1-5 Palveluverkoston varautumisen ja tiedon turvaamisen toimenpiteiden katselmointeja ja auditointeja toteutetaan.

6.1-6 Poikkeamahavaintojen pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa kehittämistoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.

Korkea taso

6.1-7 Varautumis- ja tietoturva-auditoinnit toteutetaan kansallisen tietoturvallisuusviranomaisen ohjeistuksen mukaisesti.

Esimerkkejä vaatimusten soveltamisen tueksi:

6.1-1: Organisaatiossa on auditiontisuunnitelma, jonka pohjalta auditoidaan esimerkiksi ensimmäisenä vuonna organisaatiossa hallintaprosessit, seuraavan vuonna kaikkien ulkoistus- ja palvelutasosopimusten tietoturvaan ja jatkuvuuteen liittyvät vaatimukset ja kolmantena kriittiset tietojärjestelmät. Organisaatio voi tehdä auditoinnit esimerkiksi vuosikellon mukaisesti.

6.1-2: 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.

6.1-3: Organisaation johto on hyväksynyt periaatteet, joiden mukaisesti yksiköt arvioivat joka toinen vuosi oman toimintansa tietoturvallisuutta ja raportoivat tuloksista.

6.1-4: Mittaustulokset on analysoitava, eikä pelkästään seurattava lukumääriä. Auditoinneista mittareina voi olla negatiivisten löydösten määrä ja vakavuus. 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.

6.1-5: Oman toiminnan osalta tehdään yhteistyössä sisäisen tarkastuksen kanssa päällekkäisen työn välttämiseksi. Tietoturvallisuuden resursointia erityistilanteita ja poikkeusoloja varten seurataan organisaation toiminta- ja taloussuunnittelun toteutumassa. Palveluntoimittajan kanssa sovitaan auditointirytmi ja kirjataan asia Toiminnan ja talouden suunnittelun koordinaation varmistamiseksi. Organisaation turvallisuusjohto koordinoi auditoinnit ja tarkastukset.

6.1-6: Riskienhallinnan seurantaraporttiin kirjataan toimenpiteet ja niiden arvioitu vaikutus. Uudet turvakontrollit kirjataan ja niiden toimivuutta toimintaprosessissa seurataan. Korkean tason järjestelmät auditoi kansallinen tietoturvallisuusviranomainen.

6.1-7: Ulkopuolisia resursseja tarvitaan teknisen puolen ratkaisujen arviointiin, sillä hallinnossa on liian vähän eri teknisten osa-alueiden auditointikokemuksen omaavia asiantuntijoita.

Liite 2 Keskeisimmät ICT-varautumista ohjaavat säädökset ja ohjeet

(elokuussa 2012)

1 Lait ja asetukset

Lait ja asetukset		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimaan**
Valmiuslaki 29.12.2011/1552	Valtioneuvoston yhteensovittaminen, hallinnonalojen velvollisuudet	2012
Laki tietoturvallisuuden arviointilaitoksista (1405/2011)	Viestintäviraston rooli tietoturvallisuuden arviointilaitoksen hyväksyjänä. Tietoturvallisuuden arviointilaitoksen vaatimukset.	2012
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista" (1406/2011).	Viranomaisten tietojärjestelmien tai tietoliikenteen tietoturvallisuuden arviointi Viestintäviraston tehtävät viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi	2012
Tietohallintolaki (634/2011)	VM:lle ohjaus ja koordinaatiovelvoite yhteentoimivuuteen liittyen Julkisen hallinnon viranomaisen on julkisen hallinnon tietojärjestelmien yhteentoimivuuden mahdollistamiseksi ja varmistamiseksi suunniteltava ja kuvattava kokonaisarkkitehtuurinsa sekä noudatettava laadittua ja ylläpidettyä kokonaisarkkitehtuuria ja sen edellyttämiä yhteentoimivuuden kuvauksia ja määrityksiä sekä toimialakohtaisia tietojärjestelmien yhteentoimivuuden kuvauksia ja määrityksiä	2011
Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (tietoturvallisuusasetus, TTA) 681/2010	Velvoitteita tiedon suojaamisesta	2010
Asevelvollisuuslaki 28.12.2007/1438 91§ (asevelvollisuusrekisteri):	Asevelvollisten ja siviilipalveluksen suorittaneiden tietojen ylläpitäminen mm. varautumista vasten	2007
Laki vapaaehtoisesta maanpuolustuksesta 11.5.2007/556 7§:	Maanpuolustusyhdistys voi järjestää mm. varautumiskoulutusta Viranomaisella mahdollisuus kutsua jäseniä varautumistyöhön	2007
Asetus valtioneuvoston kansliasta 4.4.2007/393 1§:	VNK:n tehtävä 24) valtioneuvoston turvallisuuspalvelut, turvallisuuteen liittyvän yleisen tilannekuvan kokoaminen ja valtioneuvoston yhteinen poikkeusoloihin varautuminen	2007
Laki Pelastusopistosta 21.7.2006/607 1§:	Tehtävä antaa mm. varautumiseen liittyvää koulutusta	2006
Pelastuslaki 379/2011	Väestönsuojelun varautumisvelvoite	2003
Viestintämarkkinalaki 23.5.2003/393:	Teleyritysten varautumisvelvoite	2003
Valtioneuvoston ohjesääntö 3.4.2003/262:	Kansliapäällikön yleinen tehtävä (huolehtia ministeriön ja sen hallinnonalan yleisestä turvallisuudesta sekä varautumisesta)	2003
Laki turvallisuusselvityksistä 8.3.2002/177:	Turvallisuusselvitysten tekemisen peruste	2002
Laki radiotaajuuksista ja telelaitteista 16.11.2001/1015:	ICT-Varautumisvelvoite	2001

Ympäristönsuojelulaki 4.2.2000/86:	Varautumisvelvoite	2000
Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621:	Asiakirjojen salassapitoperusteet, poikkeusoloihin varautumista koskevat asiakirjat ks. 24 § 1 mom 8 kohta	1999
Laki televisio- ja radiotoiminnasta 9.10.1998/744:	Varautumisvelvoite viranomaistiedotteiden välittämiseen	1998
Laki huoltovarmuuden turvaamisesta 18.12.1992/1390:	HVK:n tehtävä, Johtosuhteet (TEM) Velvoite hallinnonaloille (ValmL)	1992
Rikoslaki 19.12.1889/39, 12 luvun 3 §:	Varautumista koskeva tieto vs. vakoilu	1989

2 Valtioneuvoston päätökset ja periaatepäätökset

Valtioneuvoston päätökset ja periaatepäätökset		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimaan**
VNp Huoltovarmuuden tavoitteista (539/2008)	Määräyksiä/rajoituksia palvelujen tuottamiseen ulkomailta	
Valtioneuvoston periaatepäätös 16.12.2010, Yhteiskunnan turvallisuusstrategia 2010 (YTS 2010)		
Valtioneuvoston periaatepäätös 2009, Valtionhallinnon tietoturvallisuuden kehittäminen	Ennaltaehkäisy ja varautuminen yksi painopiste. Toinen painopiste on tiedon ja sen arvon suojaaminen	2009

3 Viranomaisten määräyskokoelmat

3.1 VAHTI-ohjeisto

Valtiovarainministeriön VAHTI-ohjeisto		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimaan**
3/2010 Sisäverkko-ohje	Sisäverkon uhkien ja jatkuvuussuunnittelun tarkistuslistat, vaatimusluettelo	3.12.2010
2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta	Tiedon saatavuuden vaatimuksia Tietoturvatasot	28.10.2010
6/2009 Kohdistetut hyökkäykset	Ohjeita varautumisesta kohdistettuihin tietoverkkohyökkäyksiin	17.11.2009
3/2009 lokien käsittelyohje	Tietoturvapoikkeamiin reagointi	11.5.2009
2/2009 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin	Yleiset ICT-varautumisen periaatteet	14.4.2009
3/2007 Tietoturvallisuudella tuloksia	Yleisohje tietoturvallisuuden johtamiseen ja hallintaan	30.11.2007
3/2005 Tietoturvapoikkeamatilanteiden hallinta	Tietoturvapoikkeamatilanteiden hallinta	1.1.2005
5/2004 keskeisten tietojärjestelmien turvaaminen	Yleisiä ohjeita järjestelmien toiminnan varmistamiseen	1.12.2004

3.2 Liikenne- ja viestintäministeriön ohjeisto

Liikenne- ja viestintäministeriön ohjeisto		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimassaolo**
Valmiusohje 1/2003, viestintäverkkojen ja palveluiden turvaaminen	Antaa toimijoille ja käyttäjäorganisaatioille perusteet varautumiselle poikkeusoloissa sekä normaaliajan häiriötilanteissa.	2003
EMP-suojausohje (LM 7/ETS/89, 21.6.1989).	Ohjeita sähkömagneettiselta säteilyltä suojautumiseen	21.6.1989

3.3 Viestintäviraston määräykset ja ohjeet

Viestintäviraston määräykset ja ohjeet		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimassaolo**
Viestintävirasto 33 C/2006 M	Määräys : HÄTÄLIIKENTEEN OHJAUKSESTA JA VARMISTAMISESTA	16.10.2006
Viestintävirasto 309/2007 S	Määräys: HÄTÄLIIKENTEEN OHJAUS YRITYSVERKOISTA	5.6.2007
Viestintävirasto 47 C/2009 M	Määräys: TELEYRITYSTEN TIETOTURVALLISUUDEN HALLINNASTA	27.8.2009
Viestintävirasto 54/2008 M	Määräys: VIESTINTÄVERKKOJEN JA -PALVELUJEN VARMISTAMISESTA	14.2.2008
Viestintävirasto 306/2006 S	Määräys: KIINTEISTÖJEN TELETILOJEN LUKITUS	15.11.2006
Viestintävirasto 57/2009 M	Määräys: VIESTINTÄVERKKOJEN JA -PALVELUJEN YLLÄPIDOSTA SEKÄ MENETTELYSTÄ VIKA- JA HÄIRIÖTILANTEISSA	20.10.2009
Viestintävirasto 43 C/2004 M	Määräys: VIESTINTÄVERKON SÄHKÖISESTÄ SUOJAAMISESTA	16.12.2004
Viestintävirasto 53/2008 M	Määräys: TUNNISTAMISTIETOJEN TALLENNUSVELVOLLISUUDESTA	4.6.2008
Viestintävirasto 48 B/2004 M	Määräys: VIESTINTÄVERKON FYYSISESTÄ SUOJAAMISESTA	20.10.2004
Viestintävirasto 30 D/2003 M	Määräys: VIESTINTÄVERKON TEHONSYÖTÖSTÄ	6.6.2003
Viestintävirasto 57/2009 M	Määräys: VIESTINTÄVERKKOJEN JA -PALVELUJEN YLLÄPIDOSTA SEKÄ MENETTELYSTÄ VIKA- JA HÄIRIÖTILANTEISSA	20.10.2009
Viestintävirasto 58/2009 M	Määräys: VIESTINTÄVERKKOJEN JA -PALVELUJEN LAADUSTA JA YLEISPALVELUSTA	20.10. 2009

3.4 Puolustushallinnon määräykset ja ohjeet

Puolustushallinnon määräykset ja ohjeet		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimassaolo**
PEteknark-os:n PAK-asiakirjat 06:01-08	sisältävät asennustöissä käytettävät sähkötyöohjeet ja määräykset EMP, HPM, EMC ja ukkossuojauksesta.	
NATO-suositukset (MIL-STD-461, MIL-STD-188-125 sekä mittaussuositus MIL-STD-462	EMP, HPM, EMC	

3.5 Huoltovarmuusorganisaation ohjeet

Huoltovarmuusorganisaation ohjeet		
Asiakirja	**Sisältö varautumisen kannalta**	**Voimassaolo**
Toiminnan jatkuvuuden hallinta	Suosituksia yrityksille toiminnan jatkuvuuden hallintaan liittyen	15.5.2009

Voimassa olevat VAHTI-julkaisut

VAHTI 1/2012	VAHTIn toimintakertomus vuodelta 2011
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 1/2011	VAHTIn toimintakertomus vuodelta 2010
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 5/2009	Effective Information Security
VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008	Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008	Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008	Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007	Älypuhelimien tietoturvallisuus
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 10/2006	Henkilöstön tietoturvaohje
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006	Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä

VAHTI 3/2006	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2000	Tietojärjestelmäkehityksen tietoturvallisuussuositus

Ohjeisto löytyy VAHTIn Internet-sivuilta
http://www.vm.fi/vahti sekä http://www.vahtiohje.fi

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 0295 160 01
Telefaksi (09) 160 33123
www.vm.fi

2/2012
VAHTI
syyskuu 2012

ISSN 1455-2566 (nid.)
ISBN 978-952-251-374-8 (nid.)
ISSN 1798-0860 (PDF)
ISSN 978-978-952-251-375-5 (PDF)