VAHTI

LUONNOSVERSIO

VAHTI 2/2016

Toiminnan jatkuvuuden hallinta

Sisällysluettelo

Johdanto

Valtiovarainministeriön asettaman VAHTI-johtoryhmän tuottaman Toiminnan jatkuvuuden hallinta -ohjeen tavoitteena on tehostaa ja yhdenmukaistaa jatkuvuuden hallintaa valtioneuvostossa, hallinnonalojen organisaatioissa sekä julkisessa hallinnossa.

Valtioneuvoston tietoturvallisuutta koskevan periaatepäätöksen 26.11.2009 mukaan yksi kehittämisen painopisteistä on häiriötilanteiden ennaltaehkäisy ja varautuminen. Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) tuli voimaan 1.10.2010 ja sen mukaan valtion virastojen oli toteutettava tietoturvallisuuden perustaso 30.9.2013 mennessä. Siihen sisältyvät menettelyt toiminnan jatkamiseksi poikkeuksellisissa tilanteissa. Toiminnan jatkuvuuden hallinta -ohje edistää myös yhteiskunnan turvallisuusstrategian ja Suomen kyberturvallisuusstrategian toimeenpanoa.

Ohje on suunnattu julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille niiden tuottaman palvelun osalta. Ohjeella pyritään sekä julkishallinnon että talouselämän toiminnan jatkuvuuden kannalta keskeisten toimintojen yhtenäistämiseen ja jatkuvuuden hallinnan saattamiseen kiinteäksi osaksi toimintaa. Tämä parantaa verkostomaisesti tuotettujen ja käytettyjen palvelujen jatkuvuutta ja toipumista häiriötilanteissa. Ohjeella parannetaan organisaatioiden varautumista tietoturva- ja kyberuhkiin parantamalla toimintojen, tietojärjestelmien ja verkkojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja palautumiskykyä.

Valtionhallinnon organisaatioiden ja julkisen hallinnon tulee toiminnassaan ottaa huomioon tämän ohjeen lisäksi ohjeessa VAHTI 2/2012 kuvatut ICT-varautumisen vaatimukset. Vaatimukset tulee ulottaa myös sisäisiin ja ulkoisiin palvelutoimittajiin. Yksittäisten järjestelmien osalta varautumisen vaatimukset tulee ottaa huomioon muun muassa vaatimusmäärittelyissä hankintoja valmisteltaessa sekä tarjouspyynnöissä.

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

Tämän ohjeen on laatinut VAHTIn Ohje-jaoston alainen työryhmä, jossa ovat toimineet seuraavat jäsenet:

Riitta Gröhn, Aalto-yliopisto, puheenjohtaja
Juhani Ahvenainen, Verohallinto
Matti Aitta, oikeusministeriö
Aarne Hummelholm, valtiovarainministeriö
Erja Kinnunen, Valtori
Paul Kinnunen, Liikennevirasto
Kai Knape, puolustusministeriö
Päivö Lappalainen, ELY-keskus
Sonja Marjamäki-Ruuskanen, Haltik
Juha Pietarinen, Valtiokonttori
Minna Romppanen, Maanmittauslaitos
Esko Vainio, valtiovarainministeriö
Mika Iivari, KPMG Oy Ab, ulkopuolinen sihteeri
Ari-Martti Pohtola, KPMG Oy Ab, ulkopuolinen sihteeri

1 Ohjeen soveltamisala, tavoitteet ja rajaukset

Tämän ohjeen soveltamisala on ensisijaisesti valtionhallinnon organisaatioiden ja soveltaen muun julkisen hallinnon toiminnan jatkuvuuden hallinta. Ohjeen avulla mikä tahansa organisaatio voi kehittää jatkuvuuden hallintaansa hyödyntäen annettuja ohjeita ja tarjolla olevia työvälineitä.

Ohjeen tavoitteena on antaa erityisesti julkiselle hallinnolle konkreettisia apuvälineitä toiminnan jatkuvuuden turvaamiseen sekä yhtenäistää ja selkeyttää käsitteistöä ja terminologiaa. Ohjeessa huomioidaan ja kootaan myös yhteen käytössä olevia hyviä käytäntöjä ja standardien menettelyjä. Lisäksi tavoitteena on selkeyttää hankintojen vastuurajauksia jatkuvuuden suhteen.

Toiminnan jatkuvuuden turvaamisessa avainasemassa on toiminnan prosessien jatkuvuus, johon tämä ohje pyrkii antamaan apuvälineitä. Operatiivisen jatkuvuuden hallinnassa merkittävässä roolissa ovat teknologiset korkean käytettävyyden toteutustavat ja niiden mahdollinen ulkoistaminen. Ohje keskittyy jatkuvuuden turvaamiseen yksittäisen organisaation näkökulmasta.

Ohjeessa käsitellään myös ICT-varautumisen vaatimusten (VAHTI 2/2012) soveltamista (erityisesti sopimuksissa) sekä poikkeusolojen valmiussuunnittelua, mutta ohjeen pääpaino on edellä mainittu operatiivisen toiminnan jatkuvuuden varmistaminen normaalioloissa ja normaaliolojen häiriötilanteissa. Ohje ei korvaa muita olemassa olevia ohjeita tai hallinnonalojen vaatimuksia (esim. valmiussuunnitteluun liittyen). Ohjeen kappaleissa 1-7 ja 9-10 kuvataan jatkuvuuden hallintaa ja sen johtamista, kappale 8 keskittyy jatkuvuussuunnittelun käytännön toteuttamiseen.

Ohjeessa annetaan organisaatioille suosituksia ja apuvälineitä jatkuvuuden hallinnan suunnitteluun, käyttöönottoon, dokumentointiin, operointiin, ylläpitoon sekä jatkuvaan parantamiseen ja mahdolliseen sertifiointiin. Ohje noudattaa päätasolla ISO 22301:2012 -standardin rakennetta. Tavoitteena on saada aikaan dokumentoitu jatkuvuuden hallintajärjestelmä, jonka avulla suojaudutaan ennakoivasti toiminnan jatkuvuutta uhkaavilta tapahtumilta, vähennetään häiriöiden mahdollisuutta, valmistaudutaan korjaamaan häiriöitä sekä palautumaan niistä.

Muistilista onnistumiseen

Jatkuvuuden hallinta on ydintoimintojen varmistamista ennalta määriteltyjen mallien mukaan normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa.

2 Jatkuvuuden hallinnan säädösympäristö

Varautuminen normaaliolojen häiriötilanteisiin on osa jokaisen organisaation hyvän tiedonhallintatavan mukaista toimintaa sekä lakisääteisten tehtävien hoitamisen varmistamista. Poikkeusoloihin varautumisen normipohjan muodostavat valmiuslaki (1552/2011) sekä valtioneuvoston päätös huoltovarmuuden tavoitteista (857/2013), jotka velvoittavat viranomaisia varautumiseen. Niiden lisäksi varautumisen ohjauksessa ja vaatimusten muodostamisessa keskeisiä ovat valtioneuvoston periaatepäätökset valtionhallinnon tietoturvallisuuden kehittämisestä (2009), yhteiskunnan turvallisuusstrategiasta (YTS2010) sekä Suomen kyberturvallisuusstrategiasta (2013).

Puolustustilalaki (1083/1991) viittaa useassa kohdassa valmiuslakiin. Valmiuslaki kuvaa viranomaisten velvoitteet, joiden tarkoituksena on poikkeusoloissa suojata väestöä sekä turvata sen toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys. Valmiuslain 3 luku 12§ määrittelee varautumisvelvoitteen:

> ”Valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa.”

Lisäksi Valmiuslain 15 luku 105§ määrittelee valtionvarainministeriön roolin poikkeusoloissa:

> ”Valtiovarainministeriö voi määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä.”

Asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) 5§:ssä säädetään:

> ”Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että … tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi …”

Laissa Valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (1226/2013) 15§:ssä säädetään varautumisesta palvelutuotannon häiriötilanteisiin:

> ”Tässä laissa tarkoitettujen palvelujen tuottajien on valmiussuunnitelmin ja normaaliolojen häiriötilanteissa tai poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava siitä, että toiminta ja palvelujen tuotanto jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa.
>
> Ellei muussa laissa toisin säädetä, normaalioloissa ja niiden häiriötilanteissa noudatetaan tässä laissa tarkoitettujen palvelujen tuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muussa tärkeysmäärittelyssä valtiovarainministeriön ennalta määrittelemiä periaatteita. Valtiovarainministeriön on ennen periaatteiden vahvistamista kuultava asianomaisia palvelujen tuottajia, asiakkaita ja ministeriöitä. Valtioneuvosto päättää merkitykseltään laajakantoisista ja yhteiskunnallisesti merkittävistä periaatteista.”

Myös laissa julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) säädetään palvelujen jatkuvuuden turvaamisesta normaalioloissa, niiden häiriötilanteissa sekä poikkeusoloissa. Suurin osa näistä vaatimuksista on suoraan hyödynnettävissä myös yleiseen jatkuvuussuunnitte-

luun. Laissa mm. annetaan vaatimuksia verkko- ja infrastruktuuripalvelun tuottajille jatkuvuuden turvaamiseksi sekä säädetään palveluntuottajien varautumisvelvollisuudesta.

Yhteiskunnan turvallisuusstrategiassa (2010) ministeriöt sekä muut yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeät viranomaiset velvoitetaan varmistamaan toimintojensa jatkuvuus kaikissa oloissa hallinnollisilla, rakenteellisilla ja teknisillä toimenpiteillä. Lisäksi siinä määritetään yhteiskunnan elintärkeät toiminnot, jotka tulee varmistaa niin normaaliajan häiriötilanteissa kuin poikkeusoloissa. Niiden hoitamiseksi hallinnonaloille on määritetty strategiset tehtävät. Kullakin organisaatiolla voi näiden lisäksi olla myös muita oman toimintansa kannalta kriittisiä palveluja ja tehtäviä.

Yhteiskunnan elintärkeät toiminnot sekä niitä tukevat palvelut ja järjestelmät muodostavat toisistaan riippuvia verkostoja. Palvelujen käyttäjistä ja ylläpitäjistä koostuviin palveluverkostoihin osallistuu hallinnon eri osapuolia, kansalaisia, yhteisöjä, yrityksiä sekä tieto- ja viestintäteknisten palvelujen tuottajia. Palvelut ovat riippuvaisia yhteiskunnan tieto- ja viestintäinfrastruktuurin toimivuudesta. Tiedonhallinnan palvelujen jatkuvuutta pyritään varmistamaan viranomaisten, asiakasorganisaatioiden ja palveluiden tuottajien yhteistyöllä sekä yhteisillä toimintaperiaatteilla ja menettelytavoilla.

Keskeistä on varmistaa, että koko palveluverkosto kykenee erilaisissa normaaliajan häiriötilanteissa sekä yhteiskunnan turvallisuusstrategian mukaisissa uhkatilanteissa jatkamaan toimintaansa asetettujen vaatimusten mukaisesti. Tämä edellyttää kaikilta verkoston osilta yhtenäistä, sovitun tasoista tiedon turvaamista sekä toiminnan ja palvelun jatkamisen valmiutta. Keskeisessä roolissa laajavaikutteisten häiriöiden hallinnassa ovat viestintä sekä tilannekuvan tuottaminen ja johtaminen. Tämä edellyttää osapuolilta entistä tiiviimpää, laaja-alaista yhteistyötä.

Suomen kyberturvallisuusstrategian (2013) strategisten linjausten yhtenä päämääränä on huolehtia tärkeiden toimintojen häiriöttömästä ja turvallisesta jatkumisesta arjessa ja häiriötilanteissa. Kyberturvallisuus perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöön sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden häiriötilanteita.

Kokonaisuudessaan kyberturvallisuusstrategian strategisten linjausten kohdassa 3 määritetään:

> ”Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.
>
> Yhteiskunnan elintärkeiden toimintojen kannalta keskeiset yritykset ja organisaatiot ottavat turvallisuus- ja valmiussuunnittelussaan sekä niihin liittyvissä palvelurakenteissa kattavasti huomioon yhteiskunnan elintärkeisiin toimintoihin liittyvät kyberuhkatekijät ja pitävät yllä tarvittavaa suojautumiskykyä. Tavoitteena on, että riskiarvioissa esiin tulleet elintärkeiden toimintojen mahdolliset häiriöt tunnistetaan ja havaitaan, ja niihin reagoidaan tavalla, joka minimoi häiriöiden haitalliset vaikutukset. Keskeiset toimijat kehittävät sietokykyään, mukaan lukien varamenetelmien suunnittelu ja harjoittelu niin, että ne voivat toimia kyberhyökkäysten alaisena. Huoltovarmuusorganisaatio tukee toimintaa selvityksin, ohjeistuksin ja koulutuksella.”

Tässä yhteydessä kybertoimintaympäristöllä käsitetään kyberturvallisuusstrategian liitteen mukaisesti: ”Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) kä-

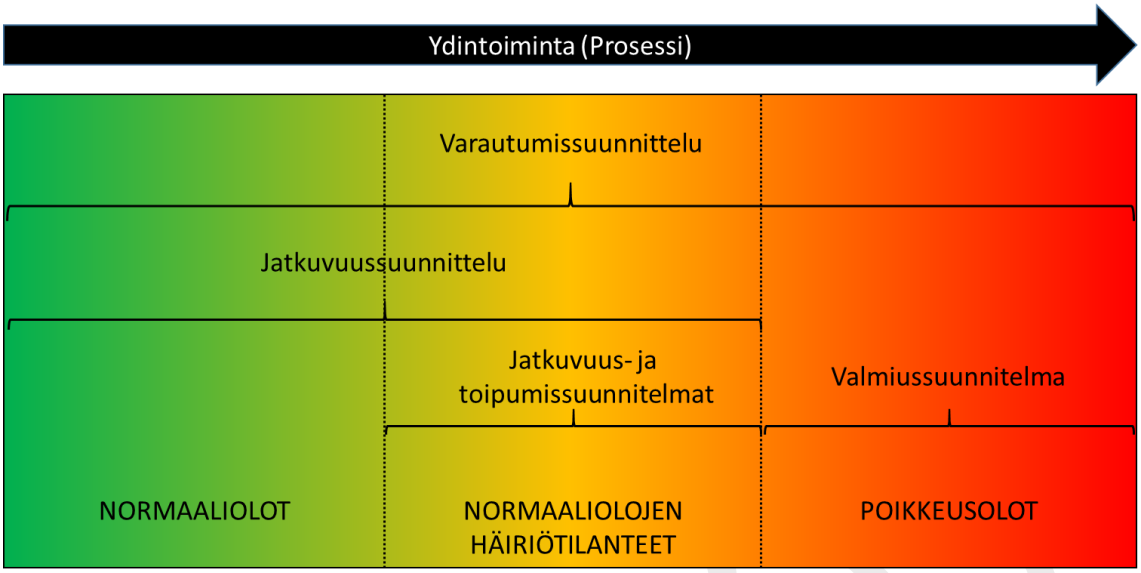
sittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö.”

Samassa yhteydessä on määritetty kyberuhka: ” Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan.”

Muistilista onnistumiseen

- **Huomioi jatkuvuuden hallinnan säädösympäristö sekä siihen liittyvät organisaation toimintaa säätelevät lait, asetukset ja määräykset**
- **Jatkuvuuden hallinnan kehittäminen on merkittävä kyberturvallisuuden osa-alue**

3 Jatkuvuussuunnittelun käsitteet ja määritelmät



Jatkuvuussuunnittelun termien ja määritelmien suhde toisiinsa. (Lähde: Jatkuvuussuunnittelu ja ICT-varautuminen, Iivari & Laaksonen 2009)

3.1 Varautuminen

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 tiedon saatavuuden ja toiminnan jatkuvuuden hallintaa ja tiedon turvaamista niin normaaliolojen häiriötilanteissa kuin poikkeusoloissa.

Lisäksi varautuminen tarkoittaa sitä kokonaisvaltaista toimintaa, jossa määritetään toiminnan ja sen johtamisen sisältö ja puitteet erilaisissa häiriötilanteissa ja poikkeusoloissa, arvioidaan niihin kohdistuvat uhat, määritetään toiminnan jatkuvuuden varmistamiseksi tarvittavat resurssit ja yhteistoimintamenettelyt sekä huolehditaan tilanteen aikana tarpeellisten tehtävien tarkoituksenmukaisesta hoitamisesta. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun.

3.2 Toipumissuunnittelu

Toipumissuunnittelu liittyy yleensä tietojärjestelmiin ja niiden toipumiseen häiriötilanteissa, ja on tärkeä osa jatkuvuussuunnittelua. Yksittäinen toipumissuunnitelma määrittelee ja dokumentoi suunnitelman piirissä oleviin toimintoihin liittyville tietojärjestelmille käytännön toimenpiteet ja toipumisohjeet normaalitilaan palaamiseksi, sisältäen mahdolliset laitteisto-, ohjelmisto- ja varajärjestelmävaatimukset. Lisäksi toipumissuunnitelmassa kuvataan teknisesti korkean käytettävyyden vaatimat toteutustavat sekä miten häiriötilanteessa viestitään toipumista ohjaavalle taholle.

Toipumissuunnitelmat kuvaavat operatiivisella tasolla ja konkreettisesti järjestelmien palauttamisen häiriötilanteista. Ne sisältävät ohjeet vakavasta häiriöstä toipumiseen, normaaliin toimintaan paluusta ja toiminnan jatkamisesta. Jatkuvuussuunnitelma ohjaa toipumissuunnitelmien toteutusta.

Ostetuissa palveluissa toipumissuunnitelmat tulee vaatia palvelun tuottajalta tai alihankkijoilta sekä samalla sopia niiden säännöllisestä ylläpidosta, katselmoinnista ja mahdollisesti tarvittavasta harjoittelusta.

3.3 Toiminnan vaikutusanalyysi (BIA)

Business Impact Analysis eli (liike)toiminnan vaikutusanalyysi pyrkii selvittämään ja kuvaamaan erilaisten haitallisten tekijöiden vaikutukset tarkastelun alla olevaan liiketoimintaprosessiin. Vaikutusanalyysi on pohjana toiminnan jatkuvuutta uhkaavien riskien arvioinnille sekä toimintojen väliselle priorisoinnille ja niiden välisten riippuvuuksien tunnistamiselle.

3.4 Toipumisaika (RTO)

RTO = Recovery Time Objective tarkoittaa tavoitellun toipumisajan määrittelyä. Toipumisaika määrittelee sen ajan, sekunteina, tunteina tai päivinä, jonka kuluessa kyseessä oleva asia tai toiminto tulee saada palautettua takaisin toimintaan häiriötilanteessa

3.5 Toipumispiste (RPO)

RPO = Recovery Point Objective tarkoittaa tavoitellun toipumispisteen määrittelyä. Toipumispiste määrittelee sen tilan, johon toiminta, tiedot tai järjestelmät tulee saada palautettua häiriön jälkeen. Toipumispiste ei välttämättä ole sama kuin vakavan häiriön alkamishetki, joten toiminnasta vastaavien tahojen on varauduttava siihen erilaisin järjestelyin.

3.6 Vapautus aseellisesta palveluksesta (VAP)

Asevelvollisuuslain 89 §:ssä (1438/2007) on määritelty palvelukseen kutsumatta jättäminen yleisen tai sotilaallisen edun vuoksi. Asianomaisen viraston, laitoksen, yhteisön tai muun työnantajan hakemuksesta liikekannallepanon varalta palvelukseen voidaan jättää määräajaksi tai toistaiseksi kutsumatta julkisoikeudellisessa palvelussuhteessa tai siihen rinnastettavassa tehtävässä olevia, erityisen ammatin harjoittajia sekä muita, joiden palvelukseen kutsuminen saattaisi vaarantaa puolustusvoimien varustamista tai ylläpitoa, yleistä taloutta tai muita yleisiä etuja. Toimenpidettä, jolla tämä toteutetaan, kutsutaan henkilövaraamiseksi (VAP, Vapautettu aseellisesta palvelusta sodan aikana). Yhteiskunnan häiriöttömän toiminnan kannalta kriittiset organisaatiot sekä niille kriittisiä palveluita toimittavat tahot voivat varata henkilöstöään jatkuvuuden varmistamista varten poikkeusoloissa.

3.7 Häiriötilanne

Häiriötilanteella ja häiriöllä tässä ohjeessa tarkoitetaan normaalioloissa palvelussa tai toiminnassa tapahtuvaa merkittävää tai vakavaa häiriötä, joka voi johtaa toiminnan keskeytymiseen tai merkittävään alenemiseen. Häiriöllä ei tässä ohjeessa tarkoiteta normaalissa toiminnassa tapahtunutta pienivaikutteista ongelmaa tai vianselvitystä. Yleisesti palvelutuotannossa käytetty kansainvälinen termi merkittävän tai vakavan häiriötilanteen hallintaprosessille on Major Incident Management (MIM).

Valtionhallinnossa vastaavaa käsitettä kutsutaan laajavaikutteisen häiriötilanteen ratkaisumenettelyksi. Laajavaikutteinen häiriö tarkoittaa kriittisen toiminnon, palvelun tai prosessin laajaa häiriötä, joka voi aiheutua laajasta käyttökatkosta, palveluiden toimimattomuudesta tai inhimillisestä virheestä. Laajavaikutteinen häiriö aiheuttaa vahinkoa suurelle joukolle toiminnon, palvelun tai prosessin käyttäjiä ja edellyttää aina välittömiä toimenpiteitä, jotta tarvittavat korjaus-

toimenpiteet saadaan liikkeelle mahdollisimman nopeasti. Ohjeen liitteessä 2 on esimerkki laajavaikutteisen häiriön ratkaisuprosessista.

3.8 Jatkuvuuden hallinnan vuosikello

Jatkuvuuden hallinnan vuosikello on vuoden aikana tapahtuvien toimenpiteiden aikataulu ja muistilista, joka voidaan esittää sanallisesti tai kuvana. Vuosikelloa käytetään pidemmän aikajakson tapahtumien hahmottamiseen kokonaisuutena. Ohjeen liitteessä 1 on esimerkkikuva jatkuvuuden hallinnan vuosikellosta. Vastaavanlaista vuosikelloa suositellaan käytettäväksi esimerkiksi riskienhallinnassa sekä tieto- ja kyberturvallisuuden hallinnassa.

Muistilista onnistumiseen

Tunnista jatkuvuuden hallinnan eri osa-alueet ja varmista että suunnitelmat kattavat normaaliolot, normaaliolojen häiriötilanteet ja poikkeusolot, mikäli organisaatiolla siihen liittyviä velvoitteita.

4 Organisaation toimintaympäristö

4.1 Organisaation ja sen toimintaympäristön tunteminen

Jokaisen valtionhallinnon organisaation tulee kuvata oma toimintaympäristönsä riittävällä tasolla, jotta jatkuvuutta voidaan suunnitella ja toteuttaa kattavasti ja onnistuneesti.

Organisaatioiden tulee kuvata ja dokumentoida toimintonsa, palvelunsa ja prosessinsa sekä määritellä niiden keskinäiset riippuvuudet ja kriittisyys jatkuvuussuunnittelun pohjaksi. Jatkuvuuden hallinnan tulee tukea organisaation päätehtävien ja strategian toteuttamista.

Kriittisten prosessien tunnistaminen sekä niiden toiminnan ja sisällön tuntemus on jatkuvuussuunnittelun onnistumisen kannalta erittäin tärkeää. Suunnittelun tavoitteena on turvata organisaation kriittisten prosessien toiminta erilaisissa vakavissa häiriötilanteissa. Ilman kriittisten prosessien tuntemusta saatetaan keskittyä turvaamaan vääriä asioita tai oikeita asioita väärällä tavalla.

4.2 Sisäinen toimintaympäristö

Sisäinen toimintaympäristö kattaa kaikki organisaation sisäiset tekijät, jotka voivat vaikuttaa toimintaan tai tulostavoitteiden saavuttamiseen.

Sisäistä toimintaympäristöä kuvattaessa tulee huomioida mm. seuraavia tekijöitä:

- hallintotapa, organisaatiorakenne, roolit ja vastuut
- toimintaperiaatteet, tavoitteet ja niiden saavuttamiseen tarvittavat strategiat
- resursseihin ja tietämykseen liittyvät voimavarat (esim. määrärahat, aika, henkilöt, prosessit, järjestelmät ja teknologia)
- suhteet sisäisiin sidosryhmiin sekä näiden näkemykset ja arvot
- organisaation kulttuuri
- tietojärjestelmät, tiedonkulku ja päätöksentekoprosessit (sekä muodolliset että epämuodolliset)
- viraston käyttöön ottamat standardit, ohjeet ja mallit
- sopimussuhteiden muoto ja laajuus.

4.3 Ulkoinen toimintaympäristö

Ulkoisen toimintaympäristön tunnistaminen on tärkeää, jotta voidaan varmistaa, että kansalaisten, asiakkaiden ja muiden ulkoisten sidosryhmien tarpeet ja huolenaiheet otetaan huomioon tavoitteiden asettamisessa ja riskien arvioinnissa.
Ulkoista toimintaympäristöä kuvattaessa tulee huomioida mm. seuraavia tekijöitä:

- Hallitusohjelma, Suomen poliittinen ja taloudellinen tilanne
- EU ja globaali ulottuvuus sekä muu kansainvälinen, kansallinen, alueellinen tai paikallinen, yhteiskuntaan, kulttuuriin, politiikkaan, lainsäädäntöön, viranomaismääräyksiin, rahoitukseen, teknologiaan, talouteen, luontoon tai kilpailukykyyn liittyvä toimintaympäristö
- Tietoyhteiskuntaan ja digitalisaatioon liittyvä toimintaympäristö
- Keskeiset organisaation tavoitteisiin vaikuttavat kehityssuunnat yhteiskunnassa; kuten rikollisuustilanne, sabotaasit, terrorismi, onnettomuudet, epidemiat, arvojen muutokset ja polarisoituminen

- Muiden hallinnonalojen toimenpiteet, kuten lainsäädäntöön ja hallintorakenteisiin liittyvät muutokset
- Suhteet kansalaisiin, asiakkaisiin, rekrytoitavaan henkilöstöön ja kilpaileviin työnantajiin sekä muihin ulkoisiin sidosryhmiin

4.4 Sidosryhmien tarpeet ja vaatimukset

Tässä kappaleessa sidosryhmillä tarkoitetaan lähinnä organisaation ulkopuolisia tahoja, kuten alihankkijoita, viranomaisia, asiakkaita ja mediaa. Nykyaikana eri sidosryhmillä on merkittävä rooli organisaatioiden toimintaan tai palvelujen tuottamiseen. Ne tulee huomioida ja ottaa mukaan myös jatkuvuussuunnitteluun. Lisäksi tulee turvata jatkuva keskustelu ja tiedonvaihto sidosryhmien kanssa, jotta jatkuvuus varmistetaan myös sidosryhmien toiminnassa ja jotta organisaatioiden jatkuvuussuunnitelmat ovat keskenään yhteensopivia. Sidosryhmät voivat myös esittää vaatimuksia, jotka tulee huomioida jatkuvuussuunnittelussa.

Organisaatiolla on oltava menettelyt, joilla se seuraa lakien ja viranomaisten vaatimusten muutoksia, sekä olennaisten sidosryhmien intressien vaikutuksia toimintoihinsa tai palveluihinsa.

Esimerkki sidosryhmistä:

4.5 Jatkuvuuden hallintajärjestelmän osa-alueet ja järjestelmän piirissä olevan toiminnan määrittäminen

Jatkuvuuden hallintajärjestelmän muodostavat kaikki ne prosessit, toimenpiteet, työkalut ja suunnitelmat, joiden avulla varmistetaan organisaation toiminnan jatkuvuus. Hallintajärjestelmä perustuu jatkuvaan kehittämiseen, vaatimusten seuraamiseen ja päivittämiseen. Siihen rakennetaan mekanismit, joilla tunnistetaan uusien sidosryhmien vaatimukset ja pystytään vastaamaan muuttuneeseen toimintaympäristöön. Jatkuva kehittäminen ja toiminnan optimointi perustuvat suunnittelulle asetettuihin tavoitteisiin ja mittareihin, joita tarkastellaan säännöllisesti.

Jatkuvuuden hallinnan onnistumiseksi organisaation tulee määritellä ja tunnistaa kriittiset toimintonsa. Kun ne on tunnistettu, niihin voidaan kohdistaa suunnittelun kannalta tärkeitä toimenpiteitä, kuten riskienhallinta ja toiminnan keskeytysvaikutusanalyysi. Ei ole mielekästä tai

kustannustehokasta toteuttaa jatkuvuussuunnittelua kaikelle toiminnalle tai komponenteille, jotka eivät ole kriittisiä tai toteuta organisaation ydintehtäviä.

Muistilista onnistumiseen

- **Tunnista organisaation ydinprosessit ja toiminnot**
- **Valitse kriittiset toiminnot**
- **Tunnista sidosryhmät ja niiden vaatimukset**
- **Huomioi sidosryhmien vaatimukset, lait, asetukset ja määräykset jotka vaikuttavat toimintaympäristöön**
- **Dokumentoi määrämuotoisesti**

5 Jatkuvuuden hallinnan johtaminen

Jatkuvuuden hallinnan onnistumisen edellytys on johdon sitoutuminen ja tuki. Johto nimeää jatkuvuuden hallinnan vastuuhenkilön. Toimintojen, palvelujen ja prosessien omistajat vastaavat siitä, että toiminnassa huomioidaan jatkuvuuden vaatimat toimenpiteet. Vastuuhenkilö esittelee jatkuvuuden hallinnan keskeisimmät suunnitelmat johdolle, joka hyväksyy ne mahdollisten muutosten jälkeen. Toimintojen omistajat myös nimeävät ja valtuuttavat jatkuvuuden hallinnan käytännön toimenpiteistä vastaavat.

5.1 Jatkuvuuden hallinnan periaatteet

Ylimmän johdon tulee hyväksyä jatkuvuuden hallinnan periaatteet tai linjaukset, jotka ovat organisaation ydintehtävien mukaiset ja varmistavat jatkuvan kehittämisen. Periaatteet tulee dokumentoida ja niiden tulee olla selkeitä ja helposti ymmärrettäviä. Niissä määritellään jatkuvuuden hallintajärjestelmä, jatkuvuussuunnittelun vastuut sekä jatkuvuuden hallinnan raportointi ja viestintä. Periaatteiden tulee perustua voimassa olevaan lainsäädäntöön, valtioneuvoston periaatepäätöksiin sekä Valtiovarainministeriön antamiin määräyksiin ja ohjeisiin. Ne tulee katselmoida säännöllisesti ja tarvittaessa päivittää vastaamaan toimintaympäristön muutoksia.

Jatkuvuuden hallinnan periaatteissa tulee huomioida:

- Johdon sitoumus
- Linkitys organisaation strategiaan
- Vaatimukset (ml. säätely) jatkuvuuden hallinnalle
- Jatkuvuuden hallinnan tavoitteet
- Sitoutuminen jatkuvuuden hallinnan jatkuvaan parantamiseen
- Roolit ja vastuut jatkuvuuden hallinnan johtamisessa
- Viittaukset tarkentaviin periaatteisiin tai ohjeisiin.

5.2 Organisointi

Jatkuvuuden hallinta pohjautuu työjärjestyksiin, tehtäväkuvauksiin ja vuosikellon toimenpiteisiin. Se on organisoitava osaksi normaalia toimintaa siten, että ohjausvastuut ja toimintamallit pysyvät mahdollisimman muuttumattomina häiriötilanteissa ja poikkeusoloissa. Organisaation ylin johto hyväksyy ja priorisoi jatkuvuuden hallinnan toimenpiteet häiriötilanteiden varalta vastuuhenkilöiden suunnitelmien ja esitysten pohjalta.

Jatkuvuudenhallinnan lähtökohtana ovat organisaation prosessikuvaukset ja riskianalyysit. Prosessit tulee suunnitella, johtaa ja toteuttaa siten, että mahdollisia häiriö- ja poikkeamatilanteita voidaan riittävästi ennalta ehkäistä, ottaen huomioon ennalta ehkäisevistä toimenpiteistä aiheutuvat kustannukset sekä prosessien tärkeysluokittelu. Myös riippuvuudet muista organisaation prosesseista ja toiminnoista tulee ottaa suunnittelussa huomioon.

5.3 Jatkuvuuden hallinnan roolit, vastuut ja sidosryhmät

Roolit ja sidosryhmät, jotka ovat vastuussa toiminnan ja palveluiden jatkuvuudesta sekä tietoturvallisuudesta, tulee tunnistaa ja kuvata esimerkiksi toiminnan ja prosessien kuvaamisen yhteydessä. Myös keskeisiin ulkoisiin sidosryhmiin vaikuttavista palveluista, niiden jatkuvuuden hallinnasta ja tietoturvallisuudesta raportoiminen sekä poikkeamista tiedottaminen tulee organisoida ja vastuuttaa.

5.3.1 Johto

Johdon tehtävä on luoda tarkoituksenmukaiset edellytykset organisaation toiminnan jatkamiseksi kaikissa häiriötilanteissa. Johto asettaa jatkuvuussuunnittelulle tavoitteet ja linjaukset sekä hyväksyy resurssit ja rahoituksen laaditun kehittämissuunnitelman pohjalta. Johto seuraa johtamisjärjestelmän mukaisesti jatkuvuuden hallinnan tavoitteiden toteutumista sekä hyväksyy parannustoimenpiteet.

5.3.2 Toimintojen, prosessien, palvelujen ja tietojärjestelmien omistajat ja vastuuhenkilöt

Toimintojen, prosessien, palvelujen ja tietojärjestelmien omistajilla on paras tuntemus oman alueensa toiminnasta, suojattavasta tiedosta, suojattavista kohteista ja järjestelmistä. Heidän vastuullaan on kartoittaa toimintojen jatkuvuutta uhkaavat riskit ja arvioida palvelua tuottaville yksiköille toimintojen, prosessien ja palveluiden tärkeys organisaation muuhun toimintaan nähden. Omistajat asettavat palvelua tuottaville yksiköille vaatimukset (keskeytyksen sietoaika, tiedon menetys jne.) jatkuvuudelle ja toipumiselle. Omistajat vastaavat siitä, että jatkuvuuden hallinnan suunnitellut toimenpiteet ovat tarkoituksenmukaisia ja tehokkaasti toteutettuja.

Vastuuhenkilöiden rooli on toimia omien toimintojensa substanssiosaajina. Heidän tehtävänään on myös jatkuvuussuunnitelmien dokumentointi ja muiden käytännön toimenpiteiden läpivienti toimintojen, prosessien, palveluiden ja tietojärjestelmien jatkuvuuden turvaamisessa.

5.3.3 Tietohallinto

Tietohallinto tuottaa palvelua toimintojen, prosessien ja palvelujen asettamien vaatimusten mukaisesti sekä vastaa omalta osaltaan siitä, että jatkuvuuden hallinnan ja toipumissuunnittelun tekniset toimenpiteet on dokumentoitu ja testattu. Tietohallinnon rooli on ohjata ja seurata palvelutuottajille asetettujen vaatimusten toteutumista sekä teknisen toteutuksen laadunvalvonta.

5.3.4 Viestintätoiminto

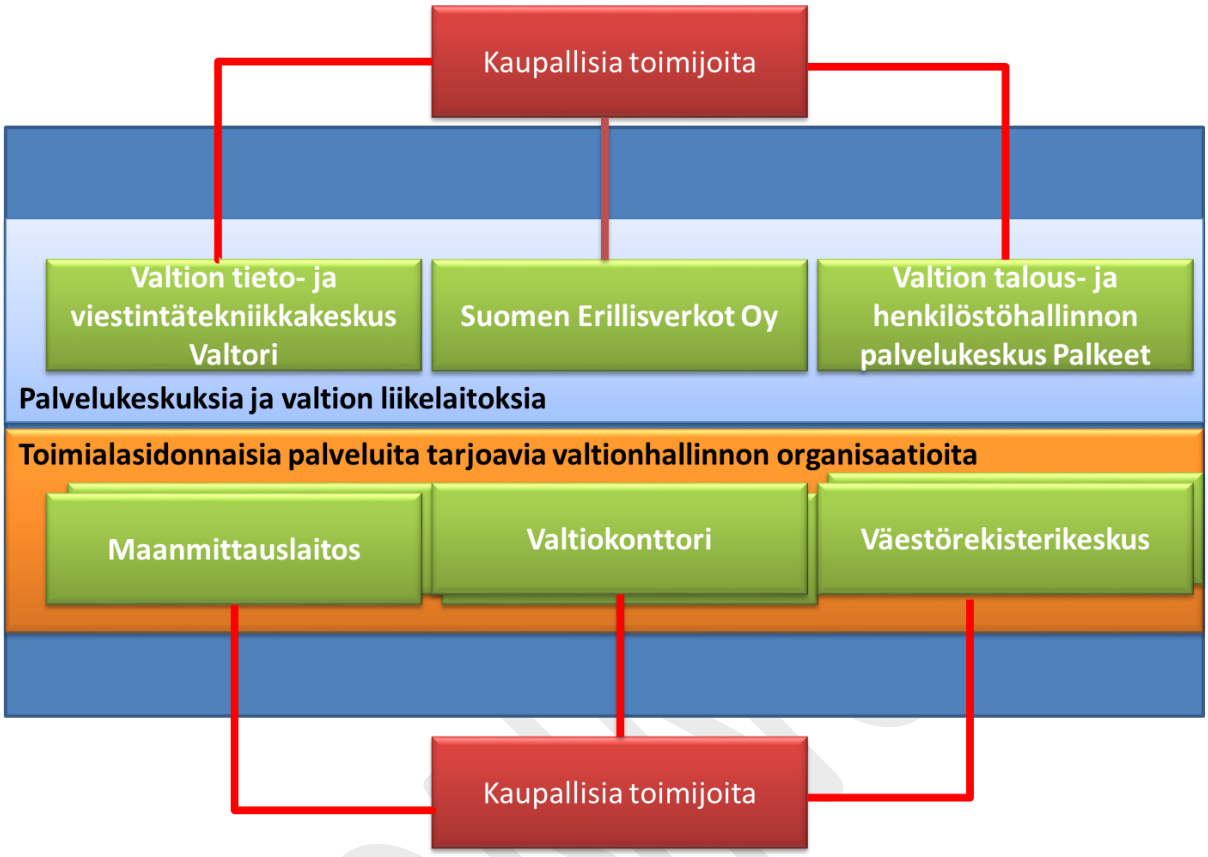
Sisäinen ja ulkoinen viestintä on kriittisessä roolissa häiriötilanteiden johtamisen tukemisessa. Organisaation on linjattava työnjako sekä vastuutettava ja kuvattava nopean sisäisen ja ulkoisen viestinnän toteuttaminen häiriötilanteissa osana operatiivisen toiminnan jatkuvuuden turvaamista.

Viestinnän merkitys korostuu erityistilanteissa, joissa on kyettävä vastaamaan nopeasti, luotettavasti ja mahdollisimman avoimesti eri sidosryhmien tiedontarpeisiin. Yleensä organisaation viestintäyksikkö hoitaa häiriötilanteen aikaisen ulkoisen viestinnän perustuen organisaation johdolta ja asiantuntijoilta saatuihin tilannetietoihin. Sen sijaan organisaatioiden välinen viestintä tapahtuu yleensä määrämuotoisesti omistajien, vastuuhenkilöiden ja palvelutuottajien toimesta.

5.3.5 Sisäiset ja ulkoiset palvelutuottajat ja niiden alihankkijat

Palvelutuottaja vastaa asiakkaan asettamien tavoitteiden teknisestä toteuttamisesta sopimuksen mukaisesti. Se vastaa myös omien alihankkijoidensa prosessien toiminnasta asiakasorganisaation jatkuvuuden hallinnan vaatimusten mukaisesti. Palvelutuottaja toimii teknisten toipumissuunnitelmien päävastuullisena tuottajana sekä vastaa siitä, että palvelutuotannon asiakastuen, muutoshallinnan ja häiriönhallinnan (ml. tietoturvapoikkeamat) prosessit tukevat jatkuvuuden hallintaa ja toipumista. Palvelutuottaja vastaa myös viestinnästä asiakasorganisaatiolle sekä tilannekuvan ylläpitämisestä.

Valtion sisäisinä palvelutuottajina toimivat esimerkiksi Valtori, Senaatti, Palkeet sekä korkean varautumisen ja korkean tietoturvan vaatimusten mukaiset turvallisuusverkon (TUVE) toimijat.



Esimerkkejä keskeisistä valtionhallinnon sisäisistä palvelutuottajista.

5.3.6 Integraatiopalvelut

Integraatiopalvelujen tuottaja vastaa palvelusuunnitteluun ja palvelujen tuotantoon liittyvien integraatioiden toiminnasta ja varmistaa muutoksenhallintaan, häiriönhallintaan ja tietoturvauhkilta suojautumiseen liittyvän yhteistyön palvelutuottajien, palveluiden käyttäjien ja toimintaa ohjaavien tahojen välille.

Integraatiopalvelujen tuottajan tulee tiedottaa muutostöiden aiheuttamista vaikutuksista jatkuvuuteen. Lisäksi sen tulee varmistaa, että suunnittelemattomissa palveluhäiriöissä toiminnasta vastaavat tahot saavat tietoonsa häiriön vaikutukset jatkuvuuteen sekä tiedot palvelujen palauttamisen etenemisestä.

Valtion tieto- ja viestintätekniikkakeskus Valtori toimii valtionhallinnon keskeisimpänä integraatiopalvelujen tuottajana. Se ohjaa ulkoisten palvelutuottajien toimintaa asiakasorganisaatioiden asettamien tavoitteiden mukaisesti.

Muistilista onnistumiseen

- **Sitouta johto kertomalla ydintoiminnan jatkuvuuteen liittyvistä riskeistä**
- **Varmista resursointi johdolta**
- **Varmista budjetti**
- **Dokumentoi periaatteet**
- **Sisällytä tehtävät vuosikelloon**
- **Määrittele roolit ja vastuut**

6 Jatkuvuuden hallinnan suunnittelu

Jatkuvuuden hallinnan suunnittelussa on erityisesti huomioitava palvelujen riippuvuus muista palveluista ja toimijoista sekä näin muodostuvasta toimintaketjusta ja -verkostosta.

6.1 Riskien tunnistaminen ja arviointi

Jatkuvuutta uhkaavien riskien hallinta tulee sisältyä organisaation kokonaisvaltaiseen riskienhallintaan. Niiden tunnistamisessa ja analysoinnissa huomioidaan sisäinen ja ulkoinen toimintaympäristö. Kriittisten toimintojen osalta analysoidaan oman ja sidosryhmien toiminnan riskit. Riskien priorisoinnilla ohjataan varautumisen ja jatkuvuudenhallinnan kehittämistä.

Riskienhallinnan avulla tunnistetaan kriittiset riskit, joita voidaan pienentää jatkuvuutta parantavilla toimenpiteillä. Toimenpiteet ja resurssit mitoitetaan ja kohdennetaan tarkoituksenmukaisesti edistämään organisaation häiriötöntä toimintaa.

On tunnistettava palveluiden ja järjestelmien merkitys organisaation toiminnalle sekä arvioitava uhkien (ml. tietoturva- ja kyberturvallisuusuhkat) vaikutus palveluiden ja järjestelmien toimintakykyyn.

Riskianalyysien tekoon ja riskienhallintaan löytyy paljon erilaisia työkaluja. Valtionhallinnossa on yleisesti käytössä Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003. Siinä käsitellään ensisijaisesti tietoturvallisuutta ja siihen kohdistuvien riskien merkitystä, mutta sen menetelmät ja arviointikriteerit soveltuvat myös jatkuvuuteen vaikuttavien riskien arviointiin. Lisäksi Huoltovarmuuskeskus tarjoaa huoltovarmuuskriittisille toimijoille työkaluja ja ohjeita riskienhallinnan ja jatkuvuudenhallinnan kehittämiseen.

6.2 Jatkuvuussuunnittelun tavoitteet

Jatkuvuussuunnittelun tavoitteena on varmistaa organisaation ydintoimintojen mahdollisimman häiriötön toiminta. Sen tulee noudattaa johdon hyväksymiä jatkuvuuden hallinnan periaatteita, toteuttaa tarvittavat toimenpiteet toiminnan jatkuvuuden varmistamiseksi sekä ottaa huomioon toimintaympäristön ja sidosryhmien vaatimukset. Jatkuvuuden hallinnan toimenpiteet tulee aikatauluttaa ja vaiheistaa, dokumentoida määrämuotoisesti ja niitä tulee mitata, testata, päivittää ja kouluttaa henkilöstölle säännöllisesti. Suunnitellut toimenpiteet on hyvä sisällyttää niistä vastaavien henkilöiden tehtävänkuviin ja tavoitteisiin.

Muistilista onnistumiseen

- **Tunnista riskit esimerkiksi valtionhallinnossa käytössä olevien riskienhallintatyökalujen avulla**
- **Määrittele jatkuvuuden hallinnan tavoitteet ja sisällytä toimenpiteet vastuuhenkilöiden tavoitteisiin**

7 Jatkuvuuden hallinnan tukitoiminnot

Tässä kappaleessa kuvataan jatkuvuuden hallinnan onnistumisen varmistamiseksi tarvittavat organisaation resurssit ja komponentit.

7.1 Henkilöstö ja osaaminen

Organisaation ydintoimintojen kriittiset erityisosaamisalueet on huomioitava henkilöstön osaamisvaatimuksissa, koulutuksessa, palvelujen hankinnassa ja resursoinnissa. Kriittisistä tehtävistä vastuulliset avainhenkilöt koulutetaan toimimaan häiriötilanteissa. Jatkuvuuden hallinnan resursointi tulee tarkistaa säännöllisesti sekä varmistaa henkilöresurssien ja osaamisen saatavuus häiriötilanteiden ja poikkeusolojen varalle. Oleellinen tehtävä on myös henkilövarausten (VAP) ylläpito omassa organisaatiossa sekä palveluja tuottavassa yritysverkostossa alihankintaketjuineen.

7.2 Osaamisen ja tietoisuuden kehittäminen

Organisaation jatkuvuuden hallinnan periaatteissa tulee olla määriteltynä osaamisen ja tietoisuuden kehittämisen konkreettiset toimenpiteet. Näitä ovat:

- Osaamisen kartoitus ja säännöllinen koulutus
- Henkilökohtaiset kehityssuunnitelmat ja niiden seuranta
- Työtehtävien jakaminen
- Osaamisen ja tiedon jakaminen
- Jatkuvuuden hallinnan periaatteiden, hyötyjen ja mahdollisten riskien seurausten selkeä kommunikointi
- Jatkuvuuden hallinnan sitominen osaksi jokapäiväistä tekemistä (esim. osaksi säännöllisiä tiimien kokouksia, näkyvyys sisäisissä viestintäkanavissa jne.)
- Henkilöstön ja sidosryhmien roolien ja vastuiden huomioiminen ja muutokset niissä
- Toimintaympäristön muutosten huomioiminen

Osaamisen ja tietoisuuden kehittämisessä tulee huomioida oman henkilöstön lisäksi avainresurssit myös yhteistyökumppaneiden ja palvelutuottajien organisaatioissa.

7.3 Viestintä ja yhteistyömallit

Viestintämenettelyt ja yhteistyömallit sekä kohderyhmät tulee määritellä ja kuvata jatkuvuussuunnitelmissa siten, että ne tukevat jatkuvuuden hallintaa erityisesti häiriötilanteissa. Kun viestintä- ja yhteistyömallit määritellään etukäteen, taataan täsmällinen, nopea ja oikea viestintä kohderyhmille häiriötilanteessa. Yhteistyössä tulee hyödyntää myös kansallisia toimintamalleja uhkien tunnistamiseen ja havainnointiin, kuten esimerkiksi Kyberturvallisuuskeskuksen CERT-FI-varoitukset ja HAVARO-raportointi.

7.4 Jatkuvuuden hallinnan dokumentointi

Jatkuvuuden hallinnan periaatteiden lisäksi sekä tekniset että hallinnolliset toimenpiteet tulee olla dokumentoitu. Kokonaisuuden hallinnan kannalta on tärkeää että eri jatkuvuussuunnitelmat ja asiakirjakokonaisuus olisivat määrämuotoisia ja noudattaisivat samaa rakennetta. Sama pätee toipumissuunnitelmiin.

Jatkuvuussuunnitelmat laaditaan kaikille organisaation kriittisiksi luokitelluille prosesseille ja toiminnoille sekä niiden toiminnan kannalta merkittäville tukiprosesseille. Toimintojen ja pro-

sessien kannalta kriittisille tietojärjestelmille laaditaan toipumissuunnitelmat. Ohjeen liitteinä 3 ja 4 on esitetty esimerkit jatkuvuus- ja toipumissuunnitelmien sisällysluetteloista ylätasolla.

7.5 Tuotannontekijät

Organisaation toiminnan jatkuvuuden tai toipumisen avainresurssina voi olla myös jokin tuotannontekijä tai resurssi. Mikäli toiminnan riippuvuutta eri tuotannon tekijöistä ei ole tunnistettu, ja niiden jatkuvaan saamiseen tai ylläpitoon ei ole varauduttu, voi koko toipumisprosessi pysähtyä.

Tuotantoresurssien saatavuus tulee huomioida prosessien kuvaamisessa ja riskien analysoinnissa. Toimintaa ja prosesseja tyypillisesti haittaavia asioita ovat muun muassa sähkön, fyysisen tele- ja tietoliikenneverkon, polttoaineiden, kuljetusvälineiden, vara-osien tai raaka-aineiden saatavuuden keskeytyminen.

7.6 Organisaatioiden väliset palvelut ja sopimukset

Organisaation tulee huomioida myös muiden organisaatioiden kanssa sovitut palvelu- tai muut sopimukset. Merkittävässä häiriötilanteessa myös toisen organisaation jatkuvuus- ja toipumisprosessien tulee pystyä kommunikoimaan organisaation jatkuvuusprosessin kanssa. Sopimuksiin sisältyvät palvelutasosopimukset ja sanktiot tulee huomioida jatkuvuusriskejä tunnistettaessa ja toiminnan keskeytysvaikutusanalyysia tehtäessä.

Muistilista onnistumiseen

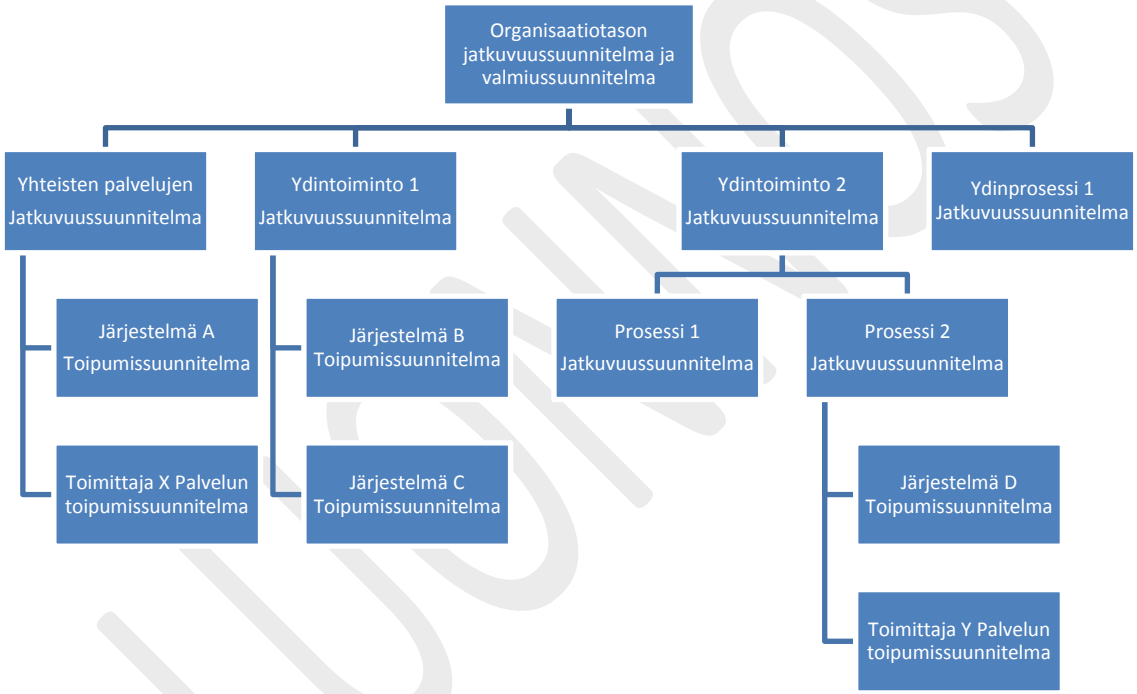
- **Nimeä henkilöt ja varmista osaaminen**
- **Kouluta periaatteet ja varmista tiedon ajantasaisuus**
- **Mieti viestintämallit eri kohderyhmille**
- **Laadi määrämuotoiset mallipohjat jatkuvuus- ja toipumissuunnitelmille**

8 Toiminnan jatkuvuus käytännössä

8.1 Toiminnan suunnittelu ja ohjaus

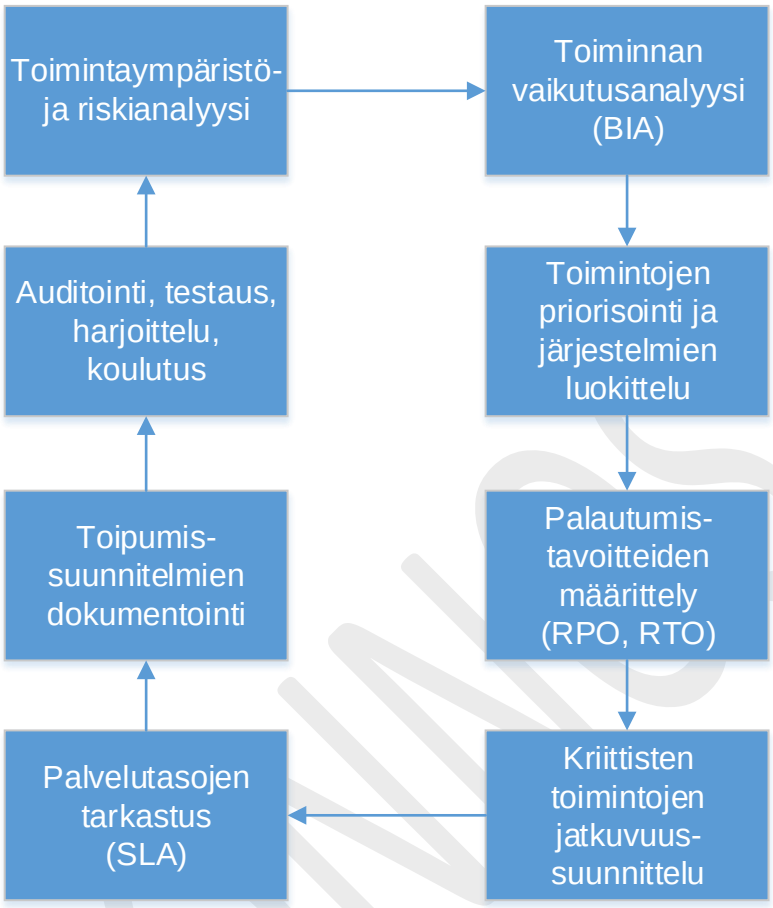
Tässä luvussa käsitellään ensisijaisesti jatkuvuus- ja toipumissuunnitteluun liittyviä käytännön toimenpiteitä. Organisaation tulee tunnistaa, suunnitella, toteuttaa ja hallita menettelyjä, joita tarvitaan jatkuvuuden hallinnan toteuttamiseksi periaatteiden ja vaatimusten mukaisesti. Jatkuvuussuunnittelun prosessissa tulee huomioida sekä yksikkö-/toimintotaso että organisaation taso. Toimintayksiköiden näkemykset tulee lopuksi yhdenmukaistaa koko organisaation tasolla, jotta toimintojen keskinäinen kriittisyys ja tavoitetasot ovat yhteismitallisia. Jatkuvuus- ja toipumissuunnitelmat muodostavat hierarkkisen kokonaisuuden, jossa eri tasoiset jatkuvuus- ja toipumissuunnitelmat muodostavat jatkuvuuden hallinnan kokonaisuuden.

Alla olevassa kuvassa on esitetty esimerkinomaisesti eri suunnitelmien välinen hierarkia ja vaihtoehtojen kirjo.



Tärkeintä on suunnitella ja toteuttaa jatkuvuuden hallinnan suunnitelmien rakenne ja hierarkia heijastamaan oman organisaation toimintaa.

Alla olevassa kuvassa on esitetty keskeiset jatkuvuussuunnittelun prosessit ja vaiheet.



Muistilista onnistumiseen

- **Suorita jatkuvuussuunnittelu kaikissa kriittisissä toiminnoissa**
- **Yhdenmukaista toimintojen suunnitelmat**
- **Yhteismitallista kriittisyys- ja tavoitetasot**

8.2 Toimintaympäristön riskianalyysit ja skenaariot

Organisaation toimintaympäristöön kohdistuu riskejä, jotka tulee huomioida esimerkiksi toimintaympäristöanalyysillä. Toimintaympäristönsä määrittelyllä organisaatio kirkastaa ne ulkoiset ja sisäiset muuttujat, jotka on otettava huomioon tavoitteiden asettamisessa ja riskien hallinnassa. Riskianalyysissä tarkastellaan sisäisen ja ulkoisen toimintaympäristön muutoksia, niiden vaikutusta toimintaan ja toimintaedellytyksiin lyhyellä (esim. 1 vuosi) ja pitkällä (esim. 5 vuotta) aikavälillä. Analyysillä pyritään selvittämään mm. sosiaalisia, yhteiskunnallisia, taloudellisia, poliittisia ja lainsäädännöllisiä - samoin kuin ympäristöön, teknologiaan ja turvallisuuteen liittyviä riskejä nykytilanteessa ja tulevaisuudessa. Tarkoituksena on pyrkiä arvioi-

maan, mihin suuntaan edellä mainitut tekijät ovat muuttumassa ja kuinka nopeasti. Toimintaympäristöanalyysin pohjalta organisaatio hahmottaa seikat, jotka on otettava huomioon jatkuvuuden hallinnan tavoitteiden asettamisessa sekä riskien hallinnassa.

Jatkuvuuden riskit ovat suurilta osin samoja kuin riskit, jotka muutenkin uhkaavat organisaation toimintaa, joten monia jatkuvuussuunnittelun kannalta keskeisiä riskejä on jo mahdollisesti tunnistettu aiemmissa riskianalyyseissä. Jatkuvuussuunnitteluun ja -suunnitelmaan liittyvä riskien kartoitus on järkevää sijoittaa organisaation yleisen riskienhallinnan ja riskianalyysien yhteyteen ja pyrkiä vähentämään päällekkäisen työn määrää.

Jatkuvuussuunnitelmissa kannattaa varautua ainakin seuraavien skenaarioiden varalle. Niiden valinnassa on otettu huomioon yhteiskunnan turvallisuusstrategiassa kuvatut uhkamallit:

1 Organisaation toimitilat tai merkittävä osa niistä ei ole käytössä (voimahuollon tai yhdyskuntatekniikan vakavat häiriöt, onnettomuudet, luonnon ääri-ilmiöt, ympäristöuhkat, terrorismi, sotilaallisen voiman käyttö)

2 Organisaation henkilöstö, merkittävä osa siitä, ylin johto tai avainhenkilöt eivät ole käytettävissä (kuljetuslogistiikan vakavat häiriöt, elintarvikehuollon vakavat häiriöt, väestön terveyden ja hyvinvoinnin vakavat häiriöt, suuronnettomuudet, luonnon ääri-ilmiöt, ympäristöuhkat, terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus, sotilaallisen voiman käyttö)

3 Tietovarantojen, tietojärjestelmien tai tietoliikenteen vakavat häiriöt (kyberuhkat, sovellusvika, ohjelmistovika, voimahuollon tai yhdyskuntatekniikan vakavat häiriöt, onnettomuudet, luonnon ääri-ilmiöt, terrorismi, sotilaallisen voiman käyttö)

4 Merkittävä palveluntoimittaja, vastapuoli, sidosryhmä tms. ei ole käytettävissä (rahoitus- ja maksujärjestelmän vakavat häiriöt, julkisen talouden rahoituksen saatavuuden häiriintyminen, voimahuollon tai yhdyskuntatekniikan vakavat häiriöt, onnettomuudet, luonnon ääri-ilmiöt, ympäristöuhkat, terrorismi, sotilaallisen voiman käyttö)

Yleensä kaikki organisaation toiminnan jatkuvuutta uhkaavat riskit voidaan sijoittaa näiden pääryhmien alle. Näihin skenaarioihin varautumalla voidaan toipua useimmista häiriöistä.

Muistilista onnistumiseen

- **Tunnista jatkuvuutta uhkaavat riskit**
- **Valitse todennäköiset skenaariot**
- **Kohdista jatkuvuutta parantavat toimenpiteet merkittävimpiin riskeihin**

8.3 Toiminnan vaikutusanalyysi (BIA)

Toiminnan vaikutusanalyysissä kerätään tietoa toimintaympäristöstä haastattelemalla toiminnasta vastaavia henkilöitä ja käymällä läpi dokumentaatiota. Toiminnan tuntemus on keskeistä vaikutusanalyysin kannalta. Kun toimintaympäristö, suojattavat kohteet ja niihin liittyvät ydinprosessit ja -toiminnot tunnetaan, voidaan ne luokitella kerättyjen tietojen perusteella kriittisyysluokkiin.

Vaikutusanalyysissä on kyse siitä, että pyritään selvittämään erilaisten riskien toteutumisen toiminnalliset vaikutukset. Niiden perusteella voidaan valita jatkuvuuden turvaamiseen ja toipumistilanteisiin oikeat ja riittävät toimenpiteet.

Vaikutusanalyysissä arvioidaan keskeytysten vaikutuksia toiminnalle, ja siinä voidaan käyttää esimerkiksi seuraavia rahallisia tai laadullisia tekijöitä:

- Toiminnalliset / palvelun saatavuusvaikutukset (laadullinen)
- Kansalaisen luottamus viranomaiseen (laadullinen)
- Julkisuuskuva, uskottavuus, brändi (laadullinen)
- Organisaation lakisääteiset tehtävät (rahallinen / laadullinen)
- Mahdolliset sanktiot jotka tulevat palvelun toimimattomuuden seurauksena (rahallinen)
- Korjaustyöt ja toimintojen palauttaminen normaalitilaan (rahallinen)
- Työpanoksen menetys keskeytyksen vuoksi (rahallinen)
- Asiakastuen kuormittuminen (rahallinen / laadullinen)
- Taloudelliset vaikutukset (rahallinen)
- Tulonmenetys palvelun toimimattomuuden vuoksi, kuten tulonmenetys/liikevaihdon menetys, ei voida tilata, ostaa, prosessoida, toimittaa, laskuttaa (rahallinen).

Koska yllä mainittuja tekijöitä on vaikea vertailla keskenään, voidaan vertailun helpottamiseksi ja kriittisyysluokan arvioimiseksi käyttää erilaisia työkaluja ja malleja.

Valtionhallinnossa vaikutusanalyysien tekemiseen on laadittu erilaisia työkaluja. Vaikutusanalyysityökalu (Jatkuvuus-BIA-tyokalu.xlsx) on kehitetty ja toteutettu Valtion tieto- ja viestintätekniikkakeskuksen (Valtori) toimesta valtionhallinnon korotetun tietoturvatason ja varautumisen yhteishankkeen (KoTVa) aikana. Työkalu on tarkoitettu järjestelmään tai palveluun kohdistuvien odottamattomien häiriöiden vaikutusten arviointiin.

Lisäksi on olemassa vanhempi Prosessin vaikutusanalyysi/jatkuvuustyökalu (VIP-jatkuvuustyokalu.xlsx), joka on kehitetty ja tuotettu Valtion IT-palvelukeskuksen (VIP) aikana ja se soveltuu apuvälineeksi organisaation toimintojen jatkuvuussuunnitteluun. Työkalu soveltuu prosessien ja laajempien palvelukokonaisuuksien odottamattomien häiriöiden vaikutusten arviointiin.

Työkalut ovat saatavissa Valtorilta (tietoturva@valtori.fi) sekä www.vahtiohje.fi –sivustolta tämän ohjeen tukimateriaalina.

Liitteessä 5 on esimerkkejä valtionhallinnossa käytössä olevista häiriöiden kustannusten laskentatavoista.

Muistilista onnistumiseen

- **Tunnista tärkeimmät palvelut ja toiminnot**
- **Määrittele keskeytysten laadulliset ja rahalliset vaikutukset toiminnalle**
- **Yhdenmukaista riskien vaikutusten arviointitapa eri toimintojen välillä**

8.4 Toimintojen priorisointi

Ydin- ja tukitoimintojen priorisointi ohjaa varautumisen ja jatkuvuudenhallinnan kehittämistä. Keskeistä on määrittää kullekin toiminnolle tavoiteltu palvelutaso (SLA). Viranomaisten täytyy jo toimintaa suunnitellessaan huomioida sille asetettavat palvelutaso- ja toipumisaikavaatimukset. Toiminnan jatkuvuuden suunnittelussa tulee huomioida myös julkishallinnon kokonaisarkkitehtuuri.

Organisaation on määritettävä alin hyväksyttävä palvelutaso, jonka alapuolella palvelu ei ole enää sitä hyödyntävän organisaation toiminnan kannalta käyttökelpoinen. Tärkeimmille toiminnoille on määriteltävä toimenpiteet ja ratkaisut, joilla häiriötilanteiden vaikutus minimoidaan ja toiminta saadaan mahdollisimman nopeasti palvelutasovaatimusten mukaiseksi.

Toiminnot, tuotannon tekijät ja suojattavat kohteet tulee luokitella niiden kriittisyyden mukaan, jotta häiriötilanteissa korjaavat toimenpiteet kyetään priorisoimaan ja kohdentamaan oikein. Kriittisyysluokittelu ja toiminnan vaikutusanalyysi (BIA) ovat tärkeitä ja pakollisia osia jatkuvuuden hallinnan suunnittelun onnistumiseksi. Kriittisten tuotannon tekijöiden ja suojattavien kohteiden palautusjärjestys tulee sopia vaikutusanalyysin perusteella. Palautusjärjestystä laadittaessa on huomioitava myös toimintaa tukevien infrastruktuuripalvelujen kriittisyys.

Muistilista onnistumiseen

- **Määrittele toiminnan jatkuvuuden strategia toteuttamaan jatkuvuuden hallinnalle asetettuja tavoitteita**
- **Priorisoi toiminnot vaikutusanalyysin pohjalta**
- **Määrittele alimmat hyväksyttävät käytettävyystasot**
- **Kriittisyysluokittele toiminnot ja suojattavat kohteet**
- **Älä unohda tuki- ja infrastruktuuripalveluiden kriittisyyttä**

8.5 Järjestelmien ja palvelujen luokittelu

Perustan jatkuvuuden hallinnalle luovat toiminnan vaikutusanalyysin tulokset sekä toimintojen, palveluiden ja järjestelmien tärkeysluokittelu. Järjestelmien luokittelussa on otettava huomioon muun muassa niiden käytön laajuus, kriittisyys, käyttökatkojen vaikutukset tuotettaviin palveluihin, järjestelmien käyttötarkoitus, tietosisältö ja niiden välisen tietoliikenteen sisältö.

Järjestelmiä luokiteltaessa voidaan käyttää VAHTI 2/2012 -ohjeen liite 4:n työkalua, joka tuottaa luokittelun perusteella myös JHS 174 mukaiset palvelutasot. Työkalun avulla järjestelmät luokitellaan elintärkeisiin, erittäin tärkeisiin, tärkeisiin, jonkin verran tärkeisiin ja merkityksettään vähäisiin.

Luokittelussa tulee erottaa toisaalta tiedon suojaaminen (luottamuksellisuus ja eheys) ja toisaalta käytettävyydestä johdettavat vaatimukset. Organisaation toiminnan kannalta elintärkeät toiminnot tulee ylläpitää keskeytyksistä huolimatta mahdollisimman korkeatasoisesti. Yhdessä tietojärjestelmän osassa toteutuneen riskin vaikutusten leviäminen muualle tietojärjestelmään tulee voida estää.

JHS 174 mukainen SLA-palvelutaso voidaan johtaa tietojärjestelmän käytettävyysvaatimuksesta alla kuvatulla tavalla:

Käytettävyys:	**SLA-palvelutaso:**
Elintärkeä	Erittäin kriittinen
Erittäin tärkeä	Kriittinen
Tärkeä	Laajennettu
Jonkin verran tärkeä	Normaali
Ei lainkaan tärkeä	Normaali

Linjaorganisaation johto hyväksyy työkalun avulla saadut luokittelut, jonka jälkeen lopullisen keskinäisen tärkeysjärjestyksen päättää organisaation ylin johto. Luokittelussa on huomioitava, että yliluokiteltu palvelu johtaa liian koviin jatkuvuusvaateisiin ja korkeampiin kustannuksiin. Aliluokittelu vastaavasti johtaa liian huonoihin SLA-tasoihin, jotka eivät vastaa toiminnan tarpeita.

Esimerkki valtionhallinnossa käytössä olevasta mallista tietojärjestelmien priorisointiin:

Kohde	Prioriteetti	Palautumistavoite
Infrastruktuuri	1	1 h
Kriittinen sovellus	2	4 h
Toimintaa tukeva sovellus	3	8 h
Muut sovellukset	4	5 vrk

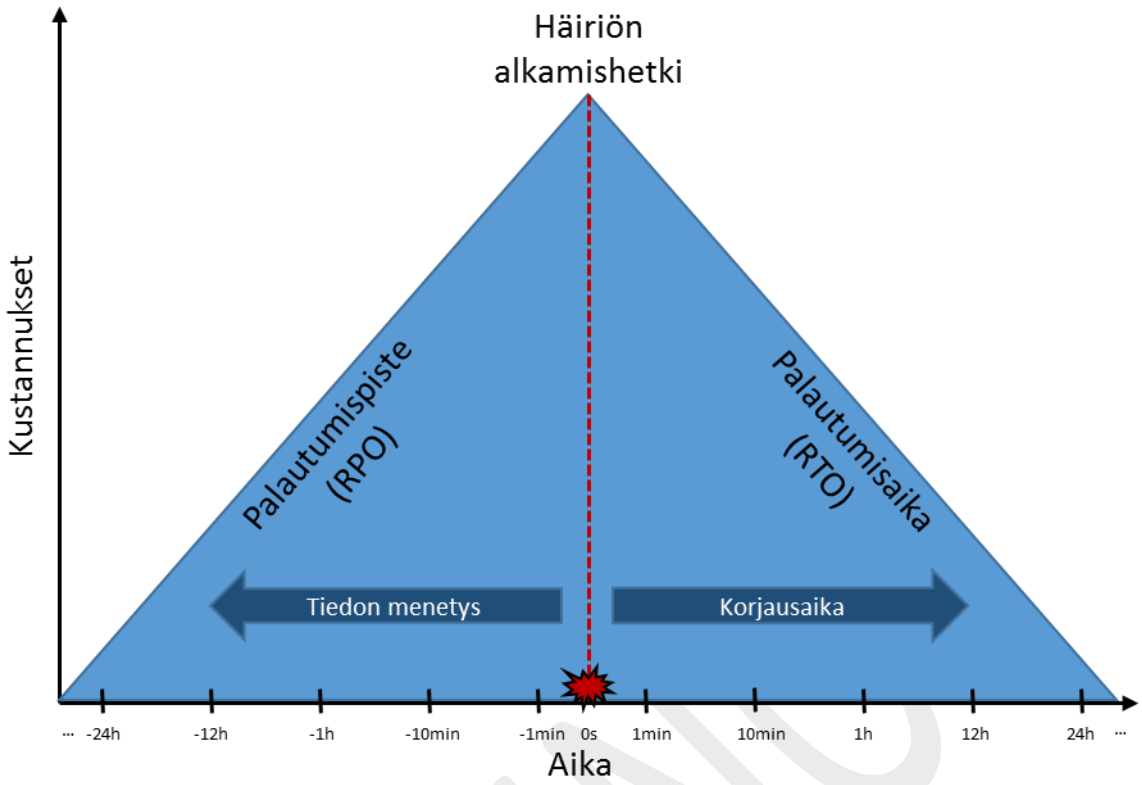
Muistilista onnistumiseen

- **Luokittele järjestelmät niiden kriittisyyden mukaan**
- **Määrittele järjestelmien keskinäinen tärkeysjärjestys**
- **Älä yli- tai aliluokittele järjestelmiä**

8.6 Palautumistavoitteiden määrittely

Toiminnon, prosessin tai palvelun omistaja määrittelee sen palautumistavoitteet. Jos niitä ei ole määritetty, toipumissuunnitelmat eivät välttämättä vastaa toiminnan tarpeita. Palvelutuottajilla palautumistavoitteina käytetään yleisesti RTO- ja RPO-arvoja. Toiminnan keskeytysvaikutusanalyysin perusteella saadaan käsitys pisimmästä toiminnan sietämästä käyttökatkosta (RTO, toipumisaika) sekä siitä, kuinka pitkältä ajalta tietoa voidaan menettää (RPO, toipumispiste). Toipumispistettä määritettäessä on varauduttava siihen, että häiriön alkamisaika ei välttämättä ole oikea tiedon palautumispiste, vaan saatetaan joutua palaamaan aikaisempaan palautuspisteeseen.

Palvelua tuottavan tahon pitää pystyä osoittamaan miten palautumistavoitteet saavutetaan käytännössä.



Yllä oleva kuva havainnollistaa kustannusten ja ajan suhdetta palautumistavoitteita määriteltäessä. Lyhyet palautumistavoitteet johtavat korkeisiin kustannuksiin. Esimerkkinä tästä ovat korkean käytettävyyden ratkaisut, kuten kahdennetut ympäristöt, hajautetut fyysiset ja loogiset komponentit sekä maantieteellisesti toisiaan peilaavat ratkaisut elintärkeissä järjestelmissä.

Kun RTO ja RPO arvot on määritelty, suunnitellaan tekniset ratkaisut, joilla määritettyihin tavoitteisiin on mahdollista päästä. Mitä lyhempää toipumisaikaa tai palautumispistettä tavoitellaan, sitä suuremmaksi kustannukset yleensä nousevat.

Konkreettinen esimerkki RPO:n määrittelystä on, että tietyn järjestelmän pitää pystyä palautumaan siten, että tietoa ei menetetä yli kahden minuutin ajalta (paljon tapahtumia minuutissa). Toisissa järjestelmissä RPO voi olla 24 tuntia (vähemmän tapahtumia, käyttäjiä tai muutoksia). Pitkästä palautumistavoitteesta esimerkkinä on järjestelmän rakentaminen uudelleen ja tiedon palautus viikkovarmistuksista jonkin verran tai ei lainkaan tärkeissä järjestelmissä.

RTO vastaavasti valitaan järjestelmän luokittelun mukaisesti; elintärkeällä järjestelmällä RTO voi olla 1 tunti ja ei lainkaan tärkeällä voi riittää viikon RTO. Palvelutuottajia käytettäessä tulee huomioida RTO:n suhde kuvattuihin palvelutasoihin ja niihin sisältyviin vaateisiin. Ei lainkaan tärkeälle, jonkin verran tärkeälle tai tärkeälle järjestelmälle asetetaan yleensä vasteaika-

Muistilista onnistumiseen

- **Määrittele järjestelmien toipumispisteet ja toipumisajat**
- **Optimoi kustannukset: Lyhyet palautumistavoitteet voivat johtaa korkeisiin kustannuksiin**
- **Huomioi SLA:t ja mahdolliset vasteaika- ja ratkaisuaikavaateet**
- **Sisällytä nämä vaatimusmäärittelyyn hankittavissa palveluissa**

vaade, erittäin tärkeälle tai elintärkeälle järjestelmälle voidaan asettaa tämän sijaan ratkaisuaikavaade. Ratkaisuaikavaade eroaa vasteaikavaateesta siten, että se sisältää palautumislupauksen siitä kuinka nopeasti järjestelmän toiminta palautuu takaisin normaalitilaan.

8.7 Ohjelmistojen ja lisenssien hallinta

Ohjelmisto-omaisuuden hallinnalla viitataan niihin prosesseihin, työrooleihin ja työkaluihin, joilla hallitaan organisaation käytössä olevia ohjelmistoja ja niiden lisenssejä. Ohjelmisto-omaisuuden hallinta tukee IT-omaisuuden hallinnan kokonaisuutta, ja on olennainen osa organisaation IT-ympäristön kontrolleja. Ohjelmisto-omaisuuden hallinta ei kuitenkaan rajoitu IT-osaston toiminnaksi, vaan sillä on vahva linkitys mm. hankintatoimintaan ja taloushallintoon.

Jatkuvuuden hallinnan piirissä olevissa järjestelmissä tulee olla tiedossa mitä ohjelmistoja ja versioita kyseinen järjestelmä tarvitsee. Tämä voi olla dokumentoituna esimerkiksi palvelutuottajan omaisuudenhallintajärjestelmässä. Järjestelmän toipumissuunnitelmaan tulee dokumentoida miten eri komponentit ja ohjelmistot on määritelty ja konfiguroitu.

Asianmukaisen ylläpidon kannalta on tärkeää että organisaation käyttämät lisenssit on dokumentoitu ja niiden ylläpitovastuut on sovittu. Häiriötilanteista toipumista nopeuttaa kun lisenssiavaimet ja koodit ovat helposti ja nopeasti saatavilla. Tämän vuoksi lisenssien ylläpitäjät ja tarvittavien lisenssiavaimien sijainti on dokumentoitava toipumissuunnitelmiin. Tärkeää on myös sopimusten ja lisenssiasiakirjojen hallinta, sekä näistä syntyvien käyttöoikeuksien linkittäminen ohjelmistojen asennus- ja käyttötietoihin.

Jatkuvuuden hallinnassa unohdetaan usein varautuminen lisenssitarkastuksiin. Jos lisenssit eivät ole kunnossa, saattaa toiminto häiriintyä tai pysähtyä. Tarkastusten tuloksena voi syntyä yllättävän suuria, budjetoimattomia kustannuksia, joilla voi pahimmillaan olla vaikutus myös organisaation toiminnan jatkuvuuteen.

Muistilista onnistumiseen

- **Varmista omaisuuden hallinnan ajantasaisuus**
- **Määrittele lisenssien ylläpitovastuut**
- **Väärin lisensoitu järjestelmä on myös itsessään jatkuvuusriski**

8.8 Järjestelmien toipumistoimenpiteet

Toipumissuunnitelmia dokumentoitaessa tulee huomioida ja kuvata mm. seuraavia asioita:

- korjaus- ja palautustoimenpiteet yleisimmistä virhetilanteista,
- järjestelmän hallittu alasajo / pakotettu alasajo,
- järjestelmän hallittuun ja priorisoitu uudelleen käynnistäminen,
- ympäristön toimivuuden testaaminen ennen tuotannon palauttamista,
- kuvaus huolto- ja ylläpitosopimuksista ja niiden kattavuudesta,
- integraatiot ja riippuvuudet muista järjestelmistä sekä
- varajärjestelmät ja korvaavat menettelyt.

Varajärjestelmien osalta kuvataan järjestelmien hankinta, käynnistys ja testaaminen sekä varajärjestelmän käyttöön siirtyminen. Toipumissuunnitelmissa tulee ottaa huomioon myös poikkeamatilanteissa tarvittavat käyttöoikeudet sekä käyttöoikeuksien rajoittaminen häiriötilanteen aikana.

Muistilista onnistumiseen

- **Järjestelmän yleisimpien vikatilanteiden korjaus- ja palautustoimenpiteiden dokumentointi**
- **Järjestelmän alasajon ja uudelleen käynnistämisen liittyvien toimien ja järjestyksen dokumentointi**
- **Määrittele varajärjestelmät ja niihin siirtyminen**

8.9 Häiriötilanteen johtaminen ja ohjaus

Häiriötilanteessa jatkuvuuden hallinnan toimenpiteet ja toipumisen käynnistää tilannejohtoryhmä. Johto kuitenkin vastaa toimenpiteiden hyväksymisestä. Yleensä ne, jotka vastaavat toiminnasta normaalioloissa, vastaavat siitä myös häiriötilanteissa ja poikkeusoloissa.

Organisaation koosta tai toiminnasta riippuen voi olla myös erillinen operatiivista toipumista edistävä ryhmä. Operatiivinen toipumisryhmä vastaa teknisestä toipumisesta toipumissuunnitelmien mukaisesti. Ryhmien kokoonpanot, yhteystiedot ja tavoitettavuustiedot määritellään jatkuvuus- ja toipumissuunnitelmissa sekä kerrotaan etukäteen osallisille. Niiden työnjako ja keskinäinen viestintä tulee myös määritellä etukäteen. Tilannetta johtaa ja koordinoi tilanne-

johtoryhmä, joka ohjaa mahdollista operatiivista toipumisryhmää. Lisäksi tulee ennalta sopia toimintamallit ja päätöksentekijät huomattavia kustannuksia aiheuttaville korjaustoimenpiteille.

Johtamistyövälineiden käytön jatkuvuus tulee aina huomioida toipumissuunnitelmissa. Häiriö voi vaikuttaa myös johtamistyövälineisiin, jolloin jatkuvuuden palauttamista (häiriön korjaamista) ei voida johtaa kokonaisvaltaisesti. Esimerkkejä työvälineistä ovat viestintäkanavat, kuten matkapuhelimet, tekstiviestit/pikaviestit, sähköposti, videoneuvottelulaitteet, konferenssipuhelimet, sähköiset jakelulistat sekä tilannekuvaa luovat järjestelmät, kuten monitorointijärjestelmä tai käytettävyysmittarointi. Toipumisprosessin johtamisen työvälineet luovat osaltaan tilannekuvaa.

Käytäntö on osoittanut, että tilannejohtoryhmällä on hyvä olla nimetty assistentti, joka vastaa esimerkiksi toimenpiteiden kirjaamisesta, yleisistä käytännön järjestelyistä ja raportoinnista.

Muistilista onnistumiseen

- **Määrittele ja vastuuta tilannejohtoryhmä ja mahdolliset operatiiviset toipumisryhmät**
- **Varmista johtamistyövälineiden toiminta häiriötilanteessa**
- **Nimeä tilannejohtoryhmälle assistentti**

8.10 Tilannekuvan luominen ja ylläpito

Tilannekuva muodostuu kaikesta toiminnan kannalta relevantista informaatiosta. Sitä tulee ylläpitää ja seurata, jotta voidaan ennakoida ja pienentää mahdollisten häiriöiden vaikutuksia. Esimerkkejä toimintaan mahdollisesti vaikuttavista tekijöistä ovat ulkoiseen toimintaympäristöön kohdistuvat myrskyt, lakot, epidemiat ja mielenosoitukset.

Häiriötilanteessa teknisen tilannekuvan muodostamiselle hyödyllisiä tietoja ovat esimerkiksi seuraavat:

- verkon tilannetieto
- palveluiden käytettävyyden tilannetieto
- suunnitellut huoltokatkot
- havainnot kyberuhista ja niiden mahdollisista vaikutuksista
- tilannetieto käyttö- ja palvelukeskusten sekä kenttätoiminnan valmiustason muutoksista
- muu merkittävä, palvelun tuottamiseen vaikuttava tapahtuma, esim. jakeluhäiriö sähköverkossa.

Organisaatiolla ja sen palvelutuottajilla tulee olla käytettävissään ennalta määritelty prosessi tietojen luontevaan, turvalliseen vaihtamiseen ja kommunikaatioyhteyden nopeaan avaamiseen. Lisäksi kaikilla tilannekuvaa tarvitsevilla organisaatioilla tulee olla keskenään jaettavissa tarvittavat tilannetiedot sellaisessa muodossa ja sellaisilla riittävillä tiedoilla ja toimenpide-ehdotuksilla varustettuna, että niiden perusteella nopeiden, oikeiden ja tarkoituksenmukaisten päätösten tekeminen on mahdollista.

Muistilista onnistumiseen

- **Kerää ja muodosta ajantasainen tilannekuva**
- **Varmista että kaikilla osapuolilla on sama tieto tilanteesta**
- **Vain ajantasainen tilannekuva mahdollistaa häiriötilanteen onnistuneen johtamisen**

8.11 Toipumisen edellyttämät tilat ja varatilat

Toipumisen johtamiseen, tekniseen toipumiseen ja palvelun tuottamiseen tarvittavat tilat tulee etukäteen määritellä ja kuvata jatkuvuus- ja toipumissuunnitelmissa.

Johtamistiloille asetettavat vähimmäisvaatimukset ovat:

- Tilannejohtoryhmän on helppo siirtyä tilaan
- Tilaan on rajoitettu pääsy
- Ääni- ja näköeristys (myös tilaan johtavilla kulkureiteillä)
- Käyttövalmiit ja etukäteen valitut viestintä- ja kommunikaatiovälineet, jotka mahdollistavat tilannetta johtavien henkilöiden osallistumisen työskentelyyn myös etänä
- Käytettävien palveluiden edellyttämät tietoliikenneyhteydet, mahdollisesti myös varayhteydet
- AV-välineet sovitinkaapeleineen, tulostin ja verkkoyhteydet (tulostinta varten sovitinkaapelit jotta se saadaan tarvittaessa toimimaan paikallisena)
- Laitteiden virtalähteitä ja latureita sekä jatkojohtoja
- Muistiinpanovälineitä, paperia ja fläppitaulu
- Ajan tasalla olevat jatkuvuus- ja toipumissuunnitelmat joko paperisina kassa- tai paloturvakaapissa tai sähköisinä esimerkiksi muistitikulla

Tiloille tulee etukäteen valita myös varatilat, jotka on voitava helposti varustaa vastaavilla työvälineillä kuin varsinaiset tilat. Tiloina voi toimia myös poikkeusolo

varatilan tulee olla riippumattomia suojattavien kohteiden sijainnista. Häiriötilanteen pitkittyessä on tärkeää, että kriisiä hoitaville henkilöille on myös ravintoa, juotavaa ja virkistäytymistiloja, ja että he pystyvät tarvittaessa lepäämään tilan läheisyydessä.

Muistilista onnistumiseen

- **Määrittele ja varusta toipumistilat etukäteen**
- **Valitse tilat, joihin toipumisryhmien on helppo siirtyä**
- **Suojaa tilat ja kulku tiloihin**
- **Muista ravinto, virkistäytymis- ja lepotilat**

8.12 Toiminta toipumistilanteessa

Tehokkaan palautumisprosessin ja jatkuvuussuunnitelman aktivoinnin tavoitteena on helpottaa ja nopeuttaa toiminnan palautumista sekä vähentää toiminnoille ja järjestelmille aiheutuvia vahinkoja tai muita vaikutuksia.

Merkittävän häiriötilanteen sattuessa tärkeintä on:

- estää ja minimoida ihmisiin kohdistuvat vahingot
- minimoida häiriötilanteen vaikutukset organisaation toimintaan, sen tuottamiin palveluihin ja sidosryhmiin
- minimoida vaikutukset toimintaa tukeviin järjestelmiin ja niissä olevaan tietoon
- varmistaa kriittisten järjestelmien palautuminen ilman tarpeetonta viivytystä
- palauttaa normaali toiminta lyhimmässä mahdollisessa ajassa mahdollisimman kustannustehokkaasti
- rajoittaa keskeytyksen vaikutuksia organisaation maineeseen, toimintaan ja talouteen.

Jatkuvuus- ja toipumissuunnitelmien käyttöönottoon liittyy useita eri vaiheita ja tehtäviä, joita ovat:

- vakavan häiriötilanteen tunnistaminen ja häiriön prioriteetin määrittäminen
- päätös jatkuvuussuunnitelman piiriin kuuluvien toimenpiteiden aloittamisesta
- tilannejohtoryhmän informointi ja koolle kutsuminen (fyysinen paikallaolo / etäneuvottelu)
- vahinkojen rajoittaminen sekä häiriövaikutusten kartoitus ja minimointi
- operatiivisen toipumisryhmän ohjaaminen ja toipumistoimenpiteiden etenemisen valvonta
- ajantasainen viestintä eri kohderyhmille ennalta määritettyjen mallien mukaan
- toimenpiteiden ja päätösten kirjaaminen (”tapahtumaloki”)
- tehtyjen toimien ja tilanteen analysointi sekä suunnitelmien päivittäminen.

Häiriön prioriteetti määräytyy häiriön vakavuuden ja laajuuden perusteella.

Esimerkki häiriön vakavuuden määrittelystä:

Vakavuusluokka	Kuvaus
Estävä	Häiriö **estää tai pysäyttää** asiakkaan toiminnan
Vaikeuttava	Häiriö **vaikeuttaa** asiakkaan toimintaa
Haittaava	Häiriö **haittaa/häiritsee** asiakkaan toimintaa

Esimerkki häiriön laajuuden määrittelystä:

Laajuusluokka	Kuvaus
Laaja	Häiriö koskee useita asiakkuuksia tai tuhansia käyttäjiä
Paikallinen	Häiriö koskee käyttäjäryhmää tai asiakkuutta
Rajoitettu	Häiriö koskee yksittäisiä käyttäjiä

Esimerkki häiriön prioriteetin luokittelusta:

Prioriteetti

Vakavuus → ↓ Laajuus	**Estävä**	**Vaikeuttava**	**Haittaava**
Laaja	Kriittinen	Keskitaso	Matala
Paikallinen	Korkea	Keskitaso	Matala
Rajoitettu	Korkea	Matala	Matala

Häiriötilanteen ratkaisumenettely käynnistetään aina kun häiriö kriittinen, tarvittaessa se käynnistetään myös silloin kun häiriö on prioriteetiltaan korkea. Prioriteettiluokittelu tehdään etukäteen osana häiriönhallintaprosessia.

Muistilista onnistumiseen

- **Estä ja minimoi ihmisiin kohdistuvat vahingot**
- **Minimoi häiriötilanteen vaikutukset toimintaan, palveluihin ja sidosryhmiin**
- **Varmista kriittisten järjestelmien palautuminen ilman tarpeetonta viivytystä**

8.13 Palvelutuottajan tehtävät, vastuut ja velvollisuudet

Palvelutuottajan jatkuvuus- ja toipumissuunnitelmien tulee olla linjassa sekä tukea organisaation omaa jatkuvuussuunnittelua. Näin varmistetaan toimintojen mahdollisimman nopea ja organisaation suunnitelmien mukainen toipuminen häiriötilanteista.

Ostetuissa palveluissa palvelutuottajat vastaavat ylläpitämiensä palvelujen ja järjestelmien toimivuudesta sovitun palvelutason mukaisesti. Jatkuvuus- ja varautumisvaatimukset tulee määritellä jo tarjouskilpailuvaiheessa, jolloin niiden kustannusvaikutukset ovat tiedossa alusta lähtien. Lisäksi on erittäin tärkeää, että osapuolilla on yhtenevä käsitys sopimuksen sisällöstä, pätemisjärjestyksestä ja mahdollisista sanktioista jatkuvuuteen vaikuttavissa häiriötilanteissa. Sanktioiden tulee olla oikeassa suhteessa häiriöiden toiminnalle aiheuttamiin vahinkoihin. Väärin määritellyt sanktiot voivat ohjata palvelutuottajan toimintaa organisaation toiminnan jatkuvuuden kannalta väärään suuntaan.

Jatkuvuus- ja toipumissuunnitelmat kuvataan, toteutetaan, koulutetaan ja testataan myös palvelutuottajien toiminnan osalta. Vaatimuksia arvioidaan ja toteutetaan kaikissa järjestelmän elinkaaren vaiheissa.

Priorisoitujen toimintojen palvelutuottajien tulee kuvata jatkuvuuden ja toipumisen osalta vähintään seuraavat asiat:

- varautumisen sisäiset henkilöjärjestelyt ja vastuut

- häiriötilanteiden ja poikkeusolojen vaikutukset palveluun (ml. toipumisskenaarioiden kuvaaminen)
- toimet, joilla estetään tai minimoidaan teknisten häiriöiden haitat
    - sähkönsyötön ongelmat
    - laite- ja kaapeliviat
    - tietojärjestelmäviat
    - palveluohjelmien häiriöt
    - palvelukeskustiloihin kohdistuvat häiriöt
    - tietoliikenneverkkojen häiriöt (verkonhallinta-, palvelinhallinta-, valvonta-, tuotanto-, varmistus- jne. verkot)
    - ohjelmistotuen tai ohjelmistopäivitysten loppuminen
- toimet, joilla minimoidaan verkkohyökkäysten vaikutukset
- toimet, joilla varmistetaan avainhenkilöiden käytettävyys
- toimet, joilla varmistetaan henkilöresurssien saatavuus kaikissa tilanteissa
- toimet, joilla varmistetaan korvaavien laiteresurssien saatavuus kaikissa tilanteissa.

Lisäksi palvelutuottajan tulee laatia kirjalliset järjestelmien tekniset toipumissuunnitelmat, jotka perustuvat riskiarvioinnissa kuvattuihin uhkaskenaarioihin.

Muistilista onnistumiseen

- **Määrittele selkeät jatkuvuusvaatimukset jo tarjouskilpailuvaiheessa**
- **Määrittele selkeät ja mahdollisia vahinkoja vastaavat sanktiot häiriöistä**
- **Vaadi palvelutoimittajalta kuvaus organisaation toimintaa tukevista toipumisjärjestelyistä**

8.14 Toimittajien ja alihankkijoiden ohjaus ja hallinta

Priorisoitujen toimintojen kumppani- ja palvelutoimittajaverkostoa on vaadittava osaltaan kuvaamaan kyseiseen palveluun tai toimintoon liittyvät toimintamallit ja vastuut häiriötilanteissa. Palvelutuottajalla tulee tämän lisäksi olla oma jatkuvuuden hallintamallinsa ja tarvittavat jatkuvuussuunnitelmat.

Palvelua tuottavien valtionhallinnon sisäisten ja ulkoisten kumppanien on täytettävä palvelutuotantoonsa liittyen palvelulle asetetut toiminnan jatkuvuuden ja varautumisen vaatimukset. Palvelua hankkiva organisaatio hyväksyy menettelytavat ja tekniset ratkaisut, joilla palvelulle tarjouspyynnössä asetetut ja sopimusneuvotteluissa tarkennetut jatkuvuus- ja varautumisvaatimukset toteutetaan sekä valvoo niiden toteutumisen todentamista ja raportointia. Kullekin palvelulle tulee määrittää vastuuhenkilö, joka vastaa sen hallinnasta, toiminnan jatkuvuudesta sekä toipumisen koordinoinnista poikkeus- ja häiriötilanteissa. Vastuuhenkilö voi olla palvelua ostavan organisaation oma henkilö tai nimetty kumppani.

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

Muistilista onnistumiseen

- **Vaadi toimittajilta ja alihankkijoilta toimintamallit organisaatioon kohdistuvien häiriötilanteiden varalta**
- **Valvo vaatimusten toteutumista**
- **Nimeä vastuuhenkilöt**

8.15 Sopimukset ja palvelutasot

Toiminnan jatkuvuuteen liittyvät velvoitteet ulotetaan sopimuksissa koko alihankintaketjuun ja palvelutuottajaverkostoon ottaen huomioon tuotettavan palvelun luonne ja sopijaosapuolten rooli sen tuottamisessa.

ICT-varautumisen vaatimusten mukaan uusiin ja uusittaviin palvelusopimuksiin kirjataan perustason ja tarvittaessa korkeampien tasojen vaatimukset. Vaatimusten noudattamisvelvoite tulee ulottaa myös alihankkijoihin ja kumppanuusverkostoon. Menettelyllä edesautetaan keskeisen yritysverkoston toiminnan jatkuvuuden parantamista. Organisaation tulee varmistua, että vaatimukset asetetaan ulkoisille tai sisäisille sopimuskumppaneille, ja että nämä huolehtivat niiden asettamisesta edelleen alihankkijoilleen.

SLA:lla tarkoitetaan palvelutasosopimusta, jolla sovitaan tuotettavien palvelujen taso, sen mittaaminen ja poikkeamien seuraamukset. Ne voivat olla joko sanktioita tai kannustimia. SLA on asiakkaan ja tieto- ja viestintäteknologisten palvelujen tuottajan välinen sopimus palvelun sisällöstä ja palvelutasosta (=palvelutasotavoite). SLA kuvaa palvelun, dokumentoi palvelutasotavoitteet sekä yksilöi palvelutuottajan ja asiakkaan vastuut. Käytännössä se toteutetaan usein palvelusopimuksella, jonka liitteinä ovat palvelukuvaukset sekä määritellyt palvelutasoluokat ja kohteittain sovitut palvelutasotavoitteet.

JHS 174:n mukaiset palvelutasot ovat:

Palvelutaso	**Palveluaika, häiriöselvitys**	**Käytettävyys**	**Palveluvaste**
A (Lähtötaso)	P1 arkisin 8-16	K1 97%	V1 reag:4h, ratk: 2tp
B (Normaali)	P2 arkisin 7-19	K2 99%	V2 reag:2h, ratk: 1tp
C (Laajennettu)	P3 arkisin 7-21, la,su 9-18	K2 99%	V2 reag:2h, ratk: 1tp
D (Kriittinen)	P4 24/7	K3 99,5%	V3 reag 30 min, ratk: 4h
E (Erittäin kriittinen)	P4 24/7	K4 99,9%	V4 reag:15min,

ratk: 3h

Muistilista onnistumiseen

- **Ulota vaatimukset koko palveluketjuun**
- **Määrittele SLA:t vastaamaan palvelun kriittisyysluokitusta**

8.16 Sisäinen ja ulkoinen viestintä häiriötilanteessa

Organisaatiolla tulee olla viestintäperiaatteet ja -ohjeet sisäiseen ja ulkoiseen tiedottamiseen. Niissä kuvataan myös häiriöviestinnän toteuttaminen, sekä siihen liittyvät roolit ja vastuut. Sidosryhmät ja kontaktipisteet, joille organisaatio on vastuussa palvelujen jatkuvuudesta ja tietoturvallisuudesta, tulee tunnistaa esimerkiksi toimintojen kuvaamisen yhteydessä. Viestinnän sisältöä suunniteltaessa huomioidaan esimerkiksi pitkät käyttökatkot, suunnitellut korjaustoimenpiteet, haittaohjelmien aiheuttamat katkot tai isojen tietomäärien varmistusten palautuksen vaatima aika-arvio.

ICT-varautumisen vaatimuksissa tiedottamiseen liittyy vaatimuksia jo perustasolla. Sidosryhmiin vaikuttavista tietoturva-asioista raportointi sekä tietoturvapoikkeamista tiedottaminen tulee organisoida ja vastuuttaa. Myös ulkoisen ja sisäisen tiedottamisen tulee olla suunniteltua, vastuutettua ja ohjeistettua.

Viestinnän työvälineiden saatavuus tulee huomioida jatkuvuussuunnittelussa. Häiriö voi vaikuttaa myös viestinnän onnistumiseen. Mikäli viestinnän työvälineet kuten sähköposti, internet-julkaisujärjestelmä tai puhelimet eivät ole käytettävissä, viestinnän kohderyhmää ei aina tavoiteta oikea-aikaisesti tai oikealla viestillä.

Kommunikointi organisaatioiden sekä palvelutuottajien ja alihankkijoiden välillä korostuu erityisesti hajautetussa tieto- ja viestintäteknologisten palvelujen tuotannossa. Häiriötilanneviestintä tulee suunnitella osana organisaation viestintäperiaatteita ja kuvata jatkuvuussuunnitelmassa.

Organisaatio voi osallistua esimerkiksi valtionhallinnon jatkuvuus- ja kyberturvallisuusharjoituksiin, joissa yhtenä osa-alueena on tiedottaminen eri tilanteissa. Kriisitilanteessa on erittäin tärkeää, että viestintä perustuu oikeisiin tilannetietoihin ja niistä tehtyihin johtopäätöksiin. Viestintää erityistilanteissa hoidetaan samoilla välineillä kuin normaalioloissakin eli median, verkkosivujen, sähköpostin ja puhelimen välityksellä.

Kriisitilanteen viestinnän käynnistymisen ja onnistumisen kannalta on tärkeää, että viestinnästä vastaavat saavat viipymättä realistiset ja ajantasaiset tilannetiedot tapahtumista. Viestintäryhmällä tulee olla toimiva varallaolo- tai päivystysmenettely, jolla taataan laadukas ja jatkuva viestintä kaikissa vakavissa häiriötilanteissa.

Käytännön esimerkki vakavan häiriötilanteen viestinnästä
Laajavaikutteisen häiriötilanteen ratkaisumenettely viedään läpi ennalta määriteltyjen toimintatapojen mukaisesti. Häiriötilanteen aikana asianomaisia tiedotetaan säännöllisesti esimerkiksi tunnin välein prosessin etenemisestä, kunnes häiriö on ratkaistu. Ulkoistetun palvelun tuottajan nimetty vastuuhenkilö tai hänen varahenkilönsä vastaa tiedottamisesta etukäteen sovitun ohjeen mukaisesti organisaation toipumista ohjaaville ryhmille (tilannejohtoryhmä ja operatiivinen toipumisryhmä). Viestinnän tulee aina olla oikea-aikaista, jatkuvaa ja avointa.

8.17 Testaaminen, harjoittelu ja koulutus

Testaamisen, harjoittelun ja koulutuksen tarkoituksena on perehdyttää jatkuvuutta ja toipumista ohjaavat ryhmät sekä kaikki muut suunnitelmien kanssa tekemisissä olevat tahot tietoisiksi toimenpiteistään, vastuistaan sekä rooleistaan jatkuvuuden hallinnassa ja laajavaikutteisen häiriötilanteen ratkaisemisessa.

Testauksella varmistetaan, että suunnitelmissa on otettu huomioon kaikkien ydintoimintojen jatkuvuus ja toipuminen muuttuvassa toimintaympäristössä. Suunnitelmien ylläpito ja päivitys tulee aikatauluttaa jatkuvuuden hallinnan vuosikelloon. Testaamisen ja harjoittelun tulokset tulee raportoida aina jatkuvuuden hallintaa ohjaaville tahoille, jotta prosessista mahdollisesti löydetyt puutteet tai virheellisyydet saadaan resursoitua ja korjattua. Myös häiriötilanneviestinnän harjoittelu on sidottava toipumisharjoituksiin.

Säännöllinen harjoittelu kehittää valmiuksia ja antaa varmuutta toimia oikealla tavalla nopeasti ja tehokkaasti, kun suunnitelma otetaan käyttöön tositilanteessa. Harjoittelu kehittää osallistujien kykyä tehdä toiminnan kannalta järkeviä päätöksiä myös sellaisissa tilanteissa, joihin suunnitelmissa ei ole varauduttu. Säännöllisellä harjoittelulla organisaatio voi osoittaa sidosryhmilleen ja yhteistyökumppaneilleen olevansa kykenevä hallitsemaan organisaatiota mahdollisesti kohtaavat ongelmat ja näin lisätä niiden luottamusta toimintaansa kohtaan. Olennaista on myös, että jatkuvuutta ohjaavat ja toipumista operoivat tahot tuntevat suunnitelmien sisällön jo ennalta eikä niihin tutustuta vasta tositilanteessa.

Suoritettujen harjoitusten on tarkoitus kehittää myös jatkuvuuden hallinnan prosessia. Harjoitusten jälkeen tulee arvioida:

- kuinka hyvin harjoitus vastasi tavoitteita
- saatiinko halutut asiat testattua
- toimiko harjoitus suunnitellulla tavalla
- kuinka tilannejohtoryhmä ja toipumisryhmä toimivat
- havaittiinko harjoituksessa ennalta tuntemattomia riskejä.

Harjoituksen esille tuomista kehityskohteista tulee laatia toimenpideluettelo aikatauluineen.

Jatkuvuussuunnitelman toteuttamiseen liittyvästä koulutuksesta, sen suunnittelusta, kohdentamisesta ja tavoitteista vastaa yleensä jatkuvuussuunnittelua ohjaava taho. Koulutusten tulee olla jatkuvaa sekä kohdennettua eri ryhmien ja roolien mukaisesti. Koulutukset tulee sitoa organisaation jatkuvuuden hallinnan vuosikelloon osaksi muuta säännöllistä toimintaa.

Vuosittaisessa koulutuksessa ja suunnitelmien harjoittelussa on hyvä huomioida ainakin seuraavat asiat ja kohderyhmät:

- johdolle perehdytys ja päivitys jatkuvuussuunnittelusta
- häiriötilanteen viestintää ja toipumista ohjaavien ryhmien (tilannejohtoryhmä ja operatiiviset toipumisryhmät) koulutus
- toipumissuunnitelmien harjoittelu varavoimalaitteiden ja generaattoreiden testauksen yhteydessä
- suunnitellun käyttökatkon yhteydessä suoritetut jatkuvuusharjoitukset
- poistumisharjoitukset koko henkilökunnalle hälytysten yhteydessä
- uusien jatkuvuussuunnittelun vastuuhenkilöiden perehdytys.

ICT-varautumisen korotetun tason vaatimuksissa toiminnan jatkuvuuden harjoittelu ja testaus tulee ulottaa myös toimintaverkostoon eli jatkuvuutta tulee testata yhdessä yhteistyökumppaneiden, palvelutuottajien ja muiden toimijoiden kanssa, jolloin oppiminen ylittää organisaatiorajat.

Valtorissa on laadittu ohje harjoitusten läpiviennistä ja erilaisista harjoitustyypeistä. Se on saatavissa Valtorilta (tietoturva@valtori.fi) sekä www.vahtiohje.fi –sivustolta tämän ohjeen tukimateriaalina.

Muistilista onnistumiseen

- **Testaamaton jatkuvuus- tai toipumissuunnitelma on riski palautumiselle ja prosessin kehittymiselle**
- **Testaus ja harjoittelu kehittävät varmuutta ja kykyä toimia oikein, myös ennakoimattomissa tilanteissa**
- **Laajenna testaus myös toimintaverkostoon**

8.18 Suunnitelmien säilytys

Suunnitelmien versionhallinta, asianmukainen säilytys ja saatavuus tilanteessa, jossa toiminnan jatkuvuus on uhattuna, on tärkeä osa jatkuvuuden hallintaprosessia. Suunnitelmien saatavuus on varmistettava myös siinä tilanteessa että tietoliikenneyhteydet eivät toimi. Ajantasaisia jatkuvuus- ja toipumissuunnitelmia tulee säilyttää vähintään seuraavissa, fyysisesti erillisissä paikoissa:

- Tilannejohdon tila
- Tilannejohdon varatila
- Operatiivisen toipumisryhmän tilat

Kaikissa säilytyspaikoissa suunnitelmista tulee säilyttää kopio sekä paperilla että sähköisessä muodossa. Suunnitelmien päivityksen yhteydessä tulee luonnollisesti päivittää kaikki kopiot ajantasaisiksi. Suunnitelmissa tulee luetella fyysisten kopioiden sijaintipaikat sekä vastuuhenkilö joka vastaa suunnitelmien toimittamisesta ko. tiloihin.

Käytännön esimerkki suunnitelmien säilytyksestä
Jatkuvuus- ja toipumissuunnitelmien sähköiset versiot sijaitsevat dokumentinhallintajärjestelmässä sekä vastuuhenkilöiden työasemissa. Dokumentinhallintajärjestelmästä ajantasaiset versiot tiedostoista synkronoituvat työasemille (offline-kopiot). Fyysiset paperikopiot ajantasaisista suunnitelmista sijaitsevat tilannejohdon ja operatiivisten toipumisryhmien tiloissa lukituissa säilytyskaapeissa. Fyysinen ja looginen pääsynhallinta tiloihin ja säilytyskaappeihin on etukäteen määritelty ja kuvattu suunnitelmiin.

9 Jatkuvuuden hallinnan mittaaminen ja arviointi

Mittaaminen, raportointi ja auditoinnit tuottavat johtamisessa sekä strategioiden ja toiminnan suunnittelussa tarvittavaa tietoa häiriötilanteita sietävän toiminnan kustannustehokkaaksi kehittämiseksi.

Suunnitelmien ajantasaisuutta ja jatkuvuuteen liittyvää toimintaa seurataan organisaation johdon hyväksymän jatkuvuuden hallinnan 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.

9.1 Seuranta, mittaaminen ja arviointi

Jatkuvuuden hallinnan prosessin mittaamisen ja parantamisen mahdollistamiseksi organisaatiolla tulee olla keinot, kyvykkyydet ja työkalut mittaamiseen. Jo jatkuvuuden hallintaa käynnistettäessä tulee miettiä mitä, milloin, millä työkaluilla mittausta tehdään ja miten tuloksia arvioidaan.

Jotta tuloksia ja toimenpiteiden vaikuttavuutta voidaan luotettavasti arvioida, on historiatieto säilytettävä ja varmistettava tulosten yhteismitallisuus. Pidemmän aikavälin seurannalla varmistetaan myös se, että jatkuvuuden hallinnan toimenpiteet ja valitut mittarit vastaavat muuttuvaa toimintaympäristöä. Esimerkkinä toimintaympäristön muutoksesta jatkuvuuden hallinnan seurantaan on ulkoistuksen lisääntyminen, joka vaatii painopisteen siirtämisen palvelutuottajien jatkuvuus- ja toipumissuunnittelun sekä sen mittareiden seurantaan.

Käytännössä jatkuvuuden hallinnan seuranta ja mittaaminen tehdään yleensä harjoitusten ja testien yhteydessä, sekä toteutuneita häiriötilanteita jälkikäteen arvioimalla. Niistä saadut tulokset analysoidaan, dokumentoidaan ja raportoidaan. Raportointiin tulee lisäksi sisällyttää välittömät häiriö- ja poikkeamailmoitukset sekä vuosikelloon sidotut, analysoidut yhteenvetoraportit.

Valittujen mittarien tulee liittyä organisaation ydintoimintoihin ja mitata asetettujen tavoitteiden täyttymistä. Seuranta ja mittaaminen tulee sitoa jatkuvuuden hallinnan vuosikelloon. Mittaamiseen tulee sisällyttää myös merkittävät häiriötilanteet ja niistä toipuminen. Seuranta ja mittaustulokset eivät kuitenkaan saa perustua vain toteutuneisiin häiriötilanteisiin vaan pääasiassa erilliseen mittaristoon.

Esimerkkejä mitattavista kohteista:

- Toteutuneet palautusajat ja -pisteet vs. toipumisskenaarioissa arvioidut tavoitteet (RTO ja RPO)
- Riskianalyysin onnistuminen (BIA vs. toteutunut vahinko, SLA:n vastaavuus)
- Reagointi-, vaste- ja läpimenoajat (oma henkilöstö, palvelutarjoaja, jne.) vs. luvatut
- Suunnittelemattomien käyttökatkojen pituus
- Jatkuvuus- ja toipumissuunnitelmien sisällön ajantasaisuus (Vastaavatko suoritetut toipumistoimenpiteet suunniteltuja; vastaavatko toiminnan prosessit kuvattuja)
- Viestinnän onnistuminen; saavatko oikeat tahot oikean tiedon oikeaan aikaan
- Tapahtuneet merkittävät virhe- ja häiriötilanteet vs. skenaariot joihin on varauduttu
- Hallintajärjestelmän vuosikellon mukaisten toimenpiteiden toteutuminen
- Dokumenttien ajantasaisuus
- Koulutusten järjestäminen ja kohdentaminen
- Hallintajärjestelmän auditoinnit ja standardinmukaisuus
- Omien seurantajärjestelmien havainnointikyky.

Organisaation jatkuvuuden hallinnan tilaa voi mitata myös erilaisilla kypsyysmalleilla ja työkaluilla, esimerkiksi Kuntaliiton ja Huoltovarmuuskeskuksen laatiman KUJA-arviointimallin avulla.

9.2 Sisäinen ja ulkoinen auditointi

Jatkuvuuden hallintajärjestelmän sekä jatkuvuus- ja toipumissuunnitelmien säännölliset sisäiset ja ulkoiset auditoinnit (auditointisuunnitelman mukaan) ovat välttämättömiä jatkuvuuden hallinnan jatkuvalle kehittämiselle. Auditointien tuloksena saadaan raportti, jossa on selkeät havainnot ja korjausehdotukset toiminnan sekä suunnitelmien parantamiseksi. Auditoinneissa tarkastetaan suunnitelmien olemassaolo, kattavuus, ajantasaisuus sekä niiden harjoittelu, testaus, päivitys ja näiden toimien dokumentointi. Auditoinnin tuloksena saadaan sen hetkinen kuva jatkuvuussuunnittelun todellisesta tasosta organisaatiossa. Hyödyt korostuvat silloin kun auditointeja tehdään säännöllisesti, ja ne kirjataan osaksi jatkuvuuden hallinnan vuosikelloa.

Sisäinen auditointi tulee aina toteuttaa eri henkilöiden kuin jatkuvuuden hallintaa toteuttavan henkilöstön toimesta, esimerkiksi sisäisen tarkastuksen toimesta. Sisäisen tarkastuksen suorittamissa auditoinneissa käydään yleensä vuosittain läpi organisaation eri toimintoja tai prosesseja, jolloin niiden jatkuvuus- ja toipumissuunnitelmien auditointi voidaan sisällyttää sisäisen tarkastuksen vuosisuunnitelmiin. Auditointi voidaan toteuttaa myös ulkopuolisen, riippumattoman ja luotettavan osapuolen toimesta.

Jatkuvuuden hallinnan ja johtamisjärjestelmän kokonaisvaltaisessa auditoinnissa kannattaa käyttää tunnettua viitekehystä tai standardia, kuten ISO 22301. Jatkuvuuden hallinnan kontrollien varmentamisessa palveluntarjoajilla voidaan käyttää myös yleistä ISAE 3000 (International Standard on Assurance Engagements) varmennuslausuntoa, joka antaa luotettavan ulkopuolisen näkemyksen minkä tahansa kontrolliympäristön suunnittelusta, toteutuksesta ja toimivuudesta. ISAE 3000 -lausunto voidaan laatia esimerkiksi perustuen ISO 22301 mukaiseen jatkuvuuden hallintajärjestelmään ja sen kontrolleihin.

9.3 Johdon katselmointi

Johdon pitää pystyä varmistamaan jatkuvuuden hallinnan kehitys ja sen vaatimien toimenpiteiden resursointi. Tämän vuoksi sen tulee saada ajantasaista tietoa toimintaympäristön muutoksista, toiminnan riskeistä, jatkuvuuden hallintajärjestelmän toiminnasta ja nykytilasta. Johdon katselmointi tulee sitoa normaaliin toiminnan seurantaan ja jatkuvuuden hallinnan vuosikelloon. Tavoitteena on varmistua siitä, että jatkuvuuden hallinnan prosessi on asianmukainen, tehokas ja että sen toimenpiteet kohdentuvat oikeisiin asioihin.

Johdolle raportoidaan jatkuvuuden hallinnan osalta ainakin seuraavista asioista:

- Yhteenveto toteutuneista, jatkuvuustoimenpiteitä edellyttäneistä häiriöistä
- Aiempien kehitystoimenpiteiden tilanne
- Muutokset jatkuvuuden hallinnan toimintaympäristössä
- Jatkuvuuden hallinnan seurannan ja mittaamisen trendit
- Auditointien tulokset
- Uudet tarvittavat kehitystoimenpiteet.

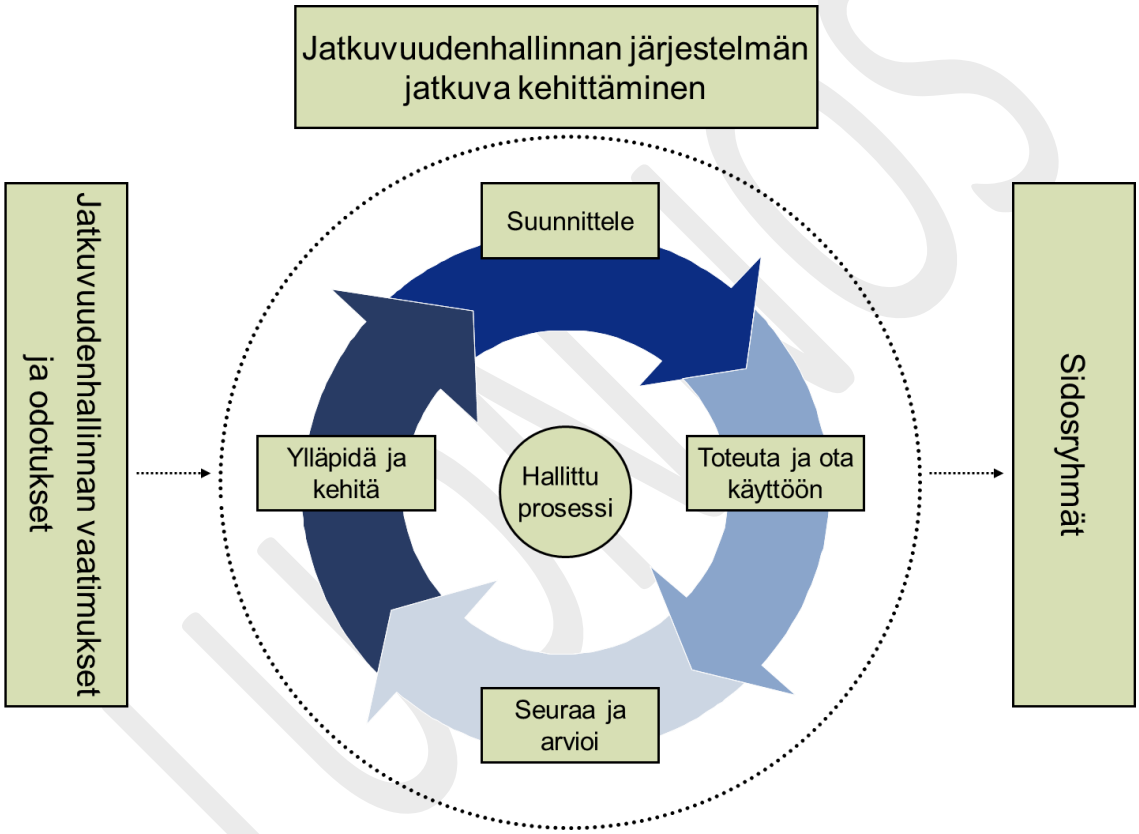
Muistilista onnistumiseen

- **Valitse ymmärrettävät ja selkeät mittarit**
- **Raportoi ja seuraa säännöllisesti, dokumentoi tulokset**
- **Pyydä säännöllisesti riippumattoman osapuolen auditointi tai varmennus**
- **Suorita säännöllinen johdon katselmointi**

10 Jatkuvuuden hallinnan kehittäminen

Jatkuvuussuunnittelu on prosessi, ei kertaluonteinen tehtävä. Jatkuvuuden hallinnan standardit esittelevät jatkuvuuden hallintajärjestelmän (BCMS, Business Continuity Management System), joka perustuu prosessien jatkuvaan parantamiseen. Ensin suunnitellaan (plan), sitten toteutetaan (do), tarkistetaan (check) ja tehdään tarvittaessa korjaukset ja kehitystoimet (act). PDCA-sykli tunnetaan myös Demingin laatuympyränä tai kehänä. Korjausten jälkeen ympyrässä palataan alkuun eli suunnitteluun. Kehittäminen nähdään spiraalina, päättymättömänä prosessina – jokaisen ympyrän kierroksen jälkeen ollaan kierros lähempänä kulloistakin tavoitetta.

Samaa jatkuvan kehittämisen mallia suositellaan käytettäväksi myös muissa tieto- ja kyberturvallisuuden osa-alueissa.



Lähde: Jatkuvuussuunnittelu ja ICT-varautuminen (Iivari & Laaksonen 2009).

10.1 Suunnitelmien ylläpito, päivitys ja kehitys

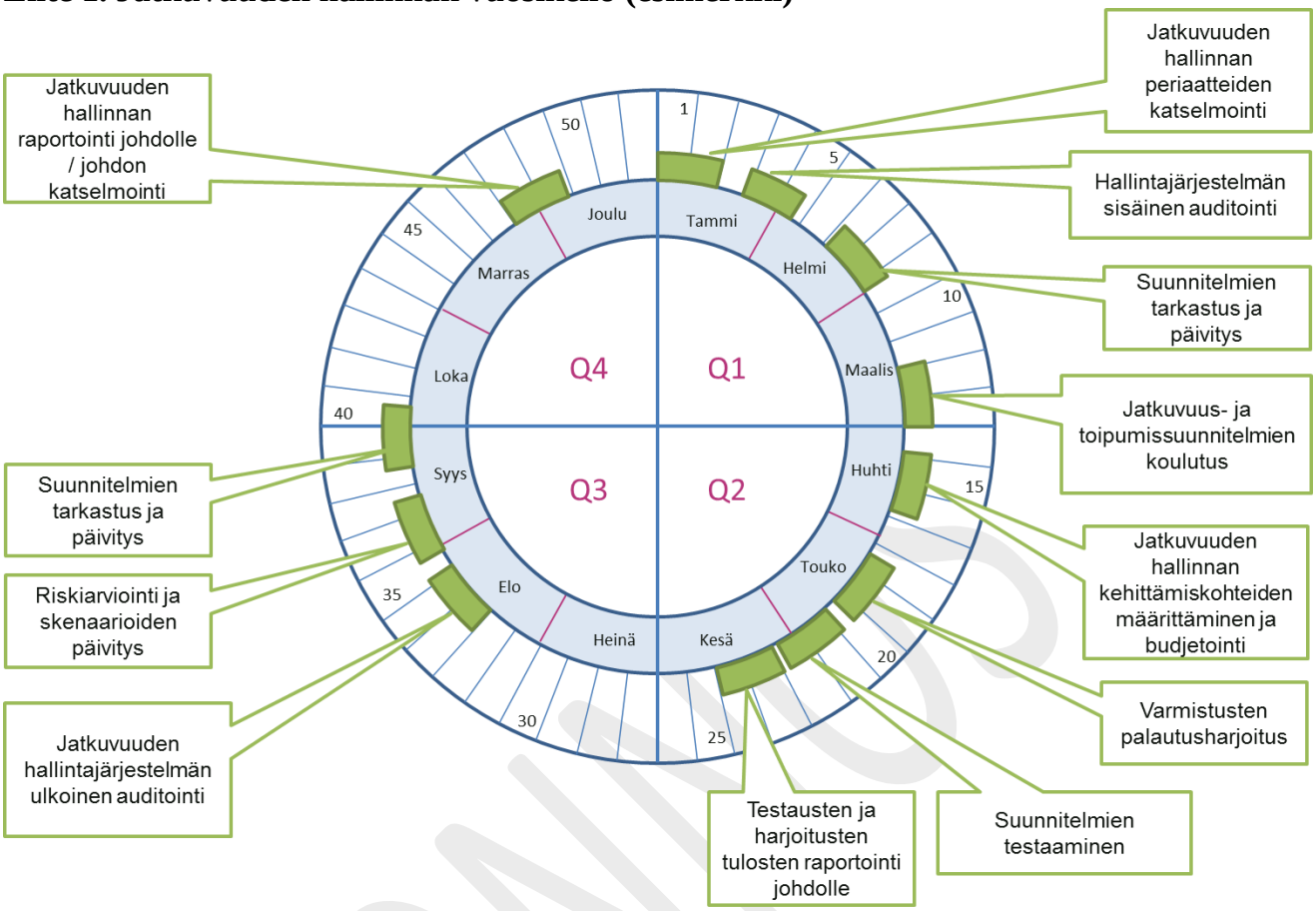
Päivittämättömät jatkuvuus- ja toipumissuunnitelmat kuvaavat vain laatimishetken aikaista tilannetta. Suunnitelmien tarkastus ja päivitys tulee sitoa jatkuvuuden hallinnan vuosikelloon. Lisäksi suunnitelmia tulee päivittää aina kun toimintaympäristössä, riskeissä tai toiminnoissa tunnistetaan merkittäviä muutoksia tai suunnitelmien testauksissa löydetään virheitä tai puutteita. Kun tunnistetaan kehityskohteita, niihin pitää reagoida välittömästi ja päättää niiden korjaamiseen liittyvistä toimenpiteistä.

Suunnitelmien ajantasaisuus varmistetaan säännöllisesti esimerkiksi vuosikellon mukaisissa harjoituksissa ja testauksissa. Suunnitelmiin tulee kirjata niiden päivityksestä, ylläpidosta ja kehityksestä vastaavien henkilöiden roolit ja vastuut.

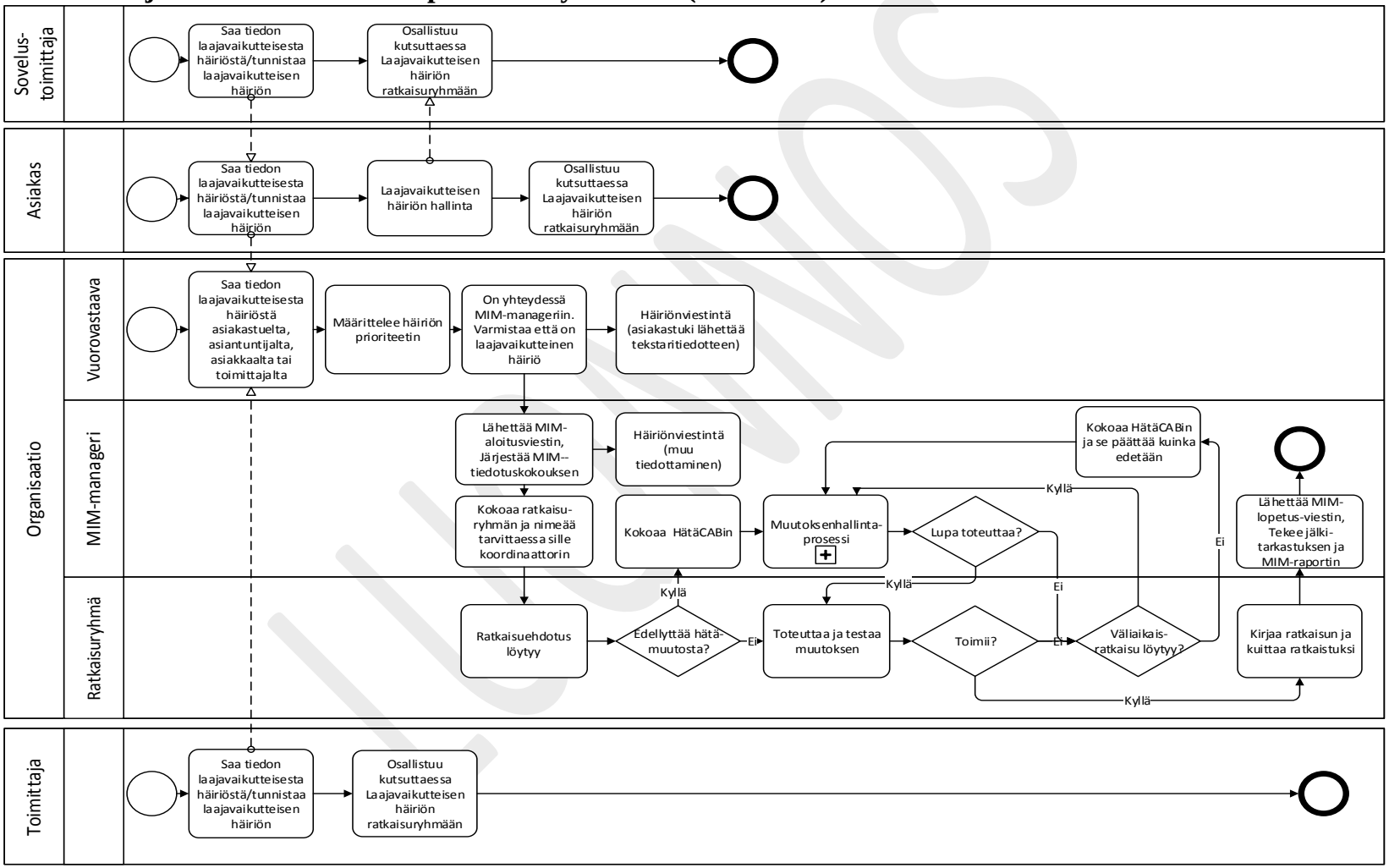
Muistilista onnistumiseen

- **Jatkuvuuden hallinta ei ole kertaluonteinen projekti vaan jatkuva, kehittyvä prosessi**
- **Hyödynnä mittareiden tuottama tieto jatkuvuuden hallinnan prosessin parantamisessa**
- **Varmista johdolta kehitystoimenpiteiden hyväksyntä**
- **Vastuuta suunnitelmien päivitys ja ylläpito**

Liite 1. Jatkuvuuden hallinnan vuosikello (esimerkki)



Liite 2. Laajavaikutteisen häiriön prosessin työnkulku (esimerkki)



Liite 3. Palvelun jatkuvuussuunnitelman sisällysluettelorunko (esimerkki)

Liite 4. Järjestelmän toipumissuunnitelman sisällysluettelorunko (esimerkki)

Liite 5. Esimerkkejä BIA-laskennasta

Tässä liitteessä on yksinkertaistettuja esimerkkejä valtionhallinnossa käytössä olevista häiriöiden kustannusten laskentatavoista, joissa huomioidaan keskeytyksen vaikutus myyntitoimintaan ja työajan menetykseen. Esimerkeissä myyntitoiminta estyy ja puolet organisaation ihmisistä osallistuu sen tuottamiseen. Lisäksi oletuksena on, että myyntitoimintaa harjoitetaan 250 päivänä vuodessa, mutta yksittäisen työntekijän työpäiviä on vain 200 päivää vuodessa (lomat huomioiden):

TULOT JA MENOT	TOTEUMA VUODESSA
Myyntitulot	2 500 000€
Muut tulot	2 500 000€
Tulot yhteensä	**5 000 000€**
Palkkausmenot	4 500 000€
Muut menot	500 000€
Menot yhteensä	**5 000 000€**

Keskeytyksen vaikutus	Työpäiviä vuodessa	Toiminnan tai työsuorituksen alenemisaste	Menetys / htp
Myyntitulojen menetykset	250	100%	10 000€
Menetetyn työajan kustannukset	200	50%	11 250€
Yhteensä			**21 250€**

Toinen esimerkki laskukaavasta, joka huomioi työntekijän keskimääräisen tuntihinnan:

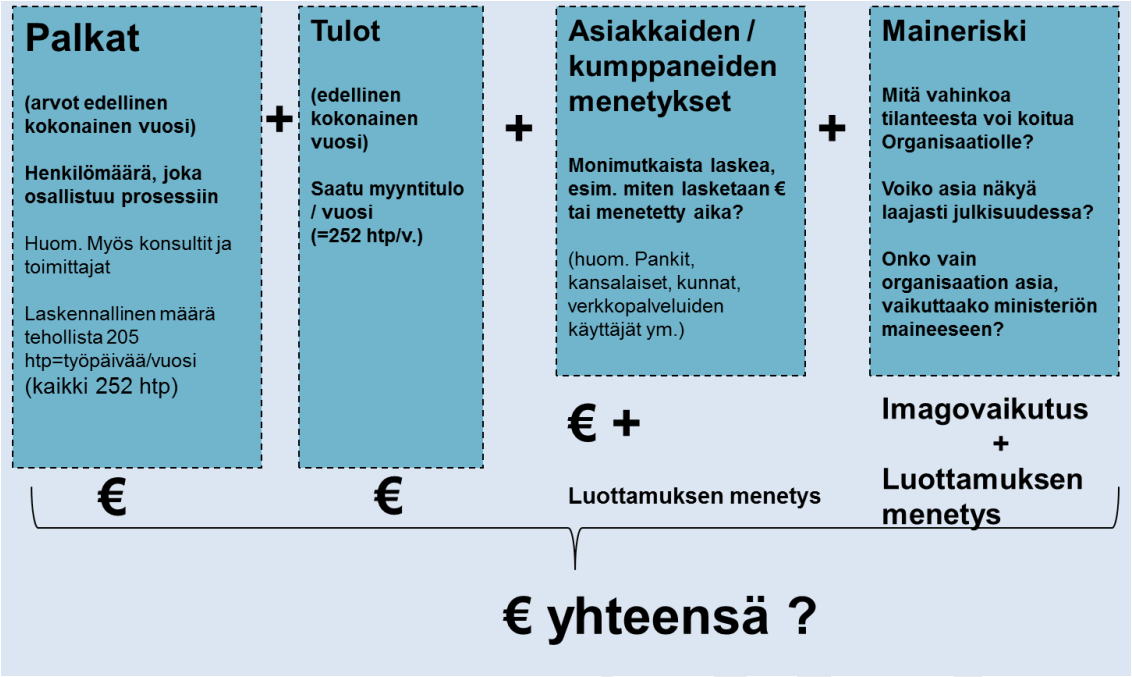
V x K x T x H, jossa

V=Vaikutuksen alaiset henkilöt
K= kerroin siitä kuinka paljon yksittäisen työntekijän työpanos
laskee toimimattomuuden vuoksi (50% = 0,5, 100%=1)
T= työntekijän keskimääräinen tuntihinta
H= häiriön kesto tunteina

Esimerkki laadullisten riskien ja toiminnan estymisestä aiheutuvien vaikutusten määrällistämisestä valtionhallinnossa käytössä olevasta mallista (arvot tulee suhteuttaa omaan toimintaan sopiviksi).

Vaikutus toimintaan	Mainevaikutus	Seuraukset
Yksittäinen lyhytkestoinen häiriö toiminnassa	Yksittäinen pettynyt asiakas	Ei vaikutusta
Toistuvia lyhyitä häiriöitä toiminnassa, jolloin jotain perustehtävää ei voida hoitaa luotettavasti	Useita pettyneitä asiakkaita, mielenilmaisuja sosiaalisessa mediassa	Jonkin verran
Ajoittaisia häiriöitä toiminnassa, jolloin jotain perustehtävää ei voida hoitaa lainkaan	Negatiivinen kansallinen julkisuus yksittäisessä asiassa	Merkittävät
Jaksottaisia pitkäkestoisia häiriöitä toiminnassa, jolloin perustehtäviä ei voida hoitaa lainkaan	Pitkäkestoinen negatiivinen kansallinen julkisuus	Kohtuuttomat
Kyky hoitaa organisaation perustehtäviä on menetetty	Vakava ja pitkäkestoinen vaikutus organisaation uskottavuuteen globaalisti	Sietämättömät

Esimerkki päivän keskeytyksen (useita pettyneitä henkilöitä, mielenilmaisuja sosiaalisessa mediassa, myyntitoimintaa ei ole voitu hoitaa) aiheuttamista kokonaiskustannusten laskennasta:



Menetys	summa
Palkkakustannukset	11 250€
Tulojen menetykset	10 000€
Asiakkaiden / kumppaneiden menetykset, arvio*	10 000€
Maineriskistä johtuva menetys, arvio*	10 000€
Yhteensä	43 250€

* Asiakkaiden ja kumppaneiden menetyksiä on vaikeaa arvioida, koska organisaatiolla ei ole suoraa näkyvyyttä näihin lukuihin ja ne voivat realisoitua esim. vahingonkorvausvaateina ja tulevien tulojen vähenemisenä tai luottamuksen menetyksenä. Maineriskistä johtuva menetys on arvioitu ylempänä olevan taulukon mukaan.