



VALTIOVARAINMINISTERIÖ



Toiminnan jatkuvuuden hallinta

13.9.2016 VAHTI-seminaari
Riitta Gröhn, Aalto-yliopisto



Tavoitteena

- Toiminnan jatkuvuuden kannalta keskeisten toimintojen yhtenäistäminen.
 - Konkreettisia apuvälineitä toiminnan jatkuvuuden turvaamiseen.
 - Keskeistä ydintoimintojen prosessien jatkuvuus, ydintoimintojen häiriötön toiminta
- Toiminnan jatkuvuuden hallinta kiinteä osa organisaation toimintaa.
- Dokumentoitu jatkuvuuden hallintajärjestelmä:
 - Suojaudutaan ennakoivasti
 - Vähennetään häiriöiden mahdollisuutta
 - Valmistaudutaan korjaamaan häiriöitä
 - Valmistaudutaan palautumaan häiriöistä.

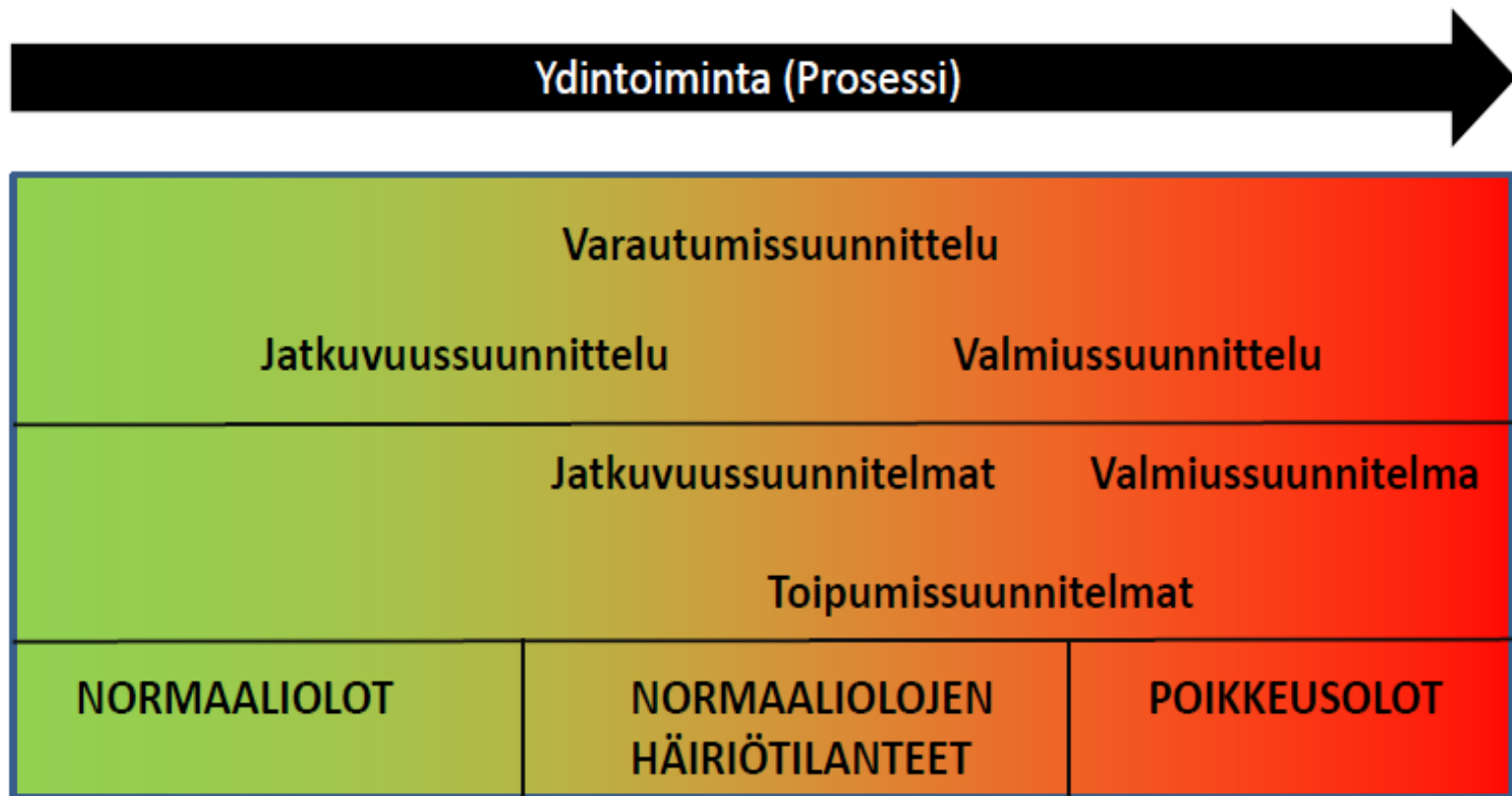


Jatkuvuuden hallinnan johtaminen

- Mahdollista vain kun johto sitoutunut ja tukee jatkuvuuden hallintaa => Jatkuvuuden hallintajärjestelmän suunnittelu ja toteutus
- Johdon sitouttaminen kertomalla ydintoiminnan jatkuvuuteen liittyvistä riskeistä
- Varmista resursointi
- Varmista budjetti
- Dokumentoi periaatteet
- Sisällytä tehtävät vuosikelloon
- Määrittele roolit ja vastuut



Jatkuvuussuunnittelun termien ja määritelmien suhde toisiinsa



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

Jatkuvuussuunnittelun käsitteet ja määritelmät



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**.

Toipumisaika (RTO)

- RTO = Recovery Time Objective tarkoittaa tavoitellun toipumisajan määrittelyä.
- Toipumisaika määrittelee sen ajan, jonka kuluessa kyseessä oleva asia tai toiminto tulee saada **palautettua toimintaan**.

Toipumispiste (RPO)

- RPO = Recovery Point Objective tarkoittaa tavoitellun toipumispisteen määrittelyä.
- Toipumispiste määrittelee sen **tilan, johon toiminta, tieto tai järjestelmä tulee saada palautettua**. Palautushetki ei välttämättä ole juuri sama kuin vakavan häiriön alkamishetki.

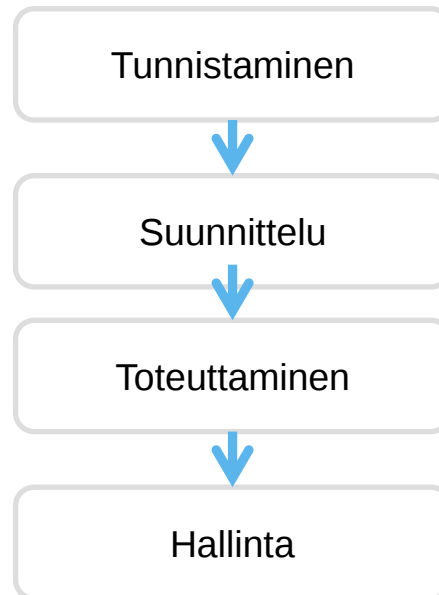
Tehtävälistaa...

- Tunnista organisaation **ydinprosessit** ja toiminnot
- Valitse kohteeksi **kriittiset toiminnot**
 - Tunnista kriittisiin toimintoihin liittyvät prosessit, palvelut, tietojärjestelmät ja tietovarannot sekä niiden väliset riippuvuudet
- Tunnista **sidosryhmät** ja niiden vaatimukset
- Ota huomioon **toimintaympäristöön** vaikuttavat lait, asetukset ja määräykset sekä sidosryhmien vaatimukset
- **Dokumentoi** määrämuotoisesti
- **HUOM!** Ilman kriittisten prosessien tuntemusta saatetaan turvata vääriä asioita tai väärällä tavalla oikeita asioita!

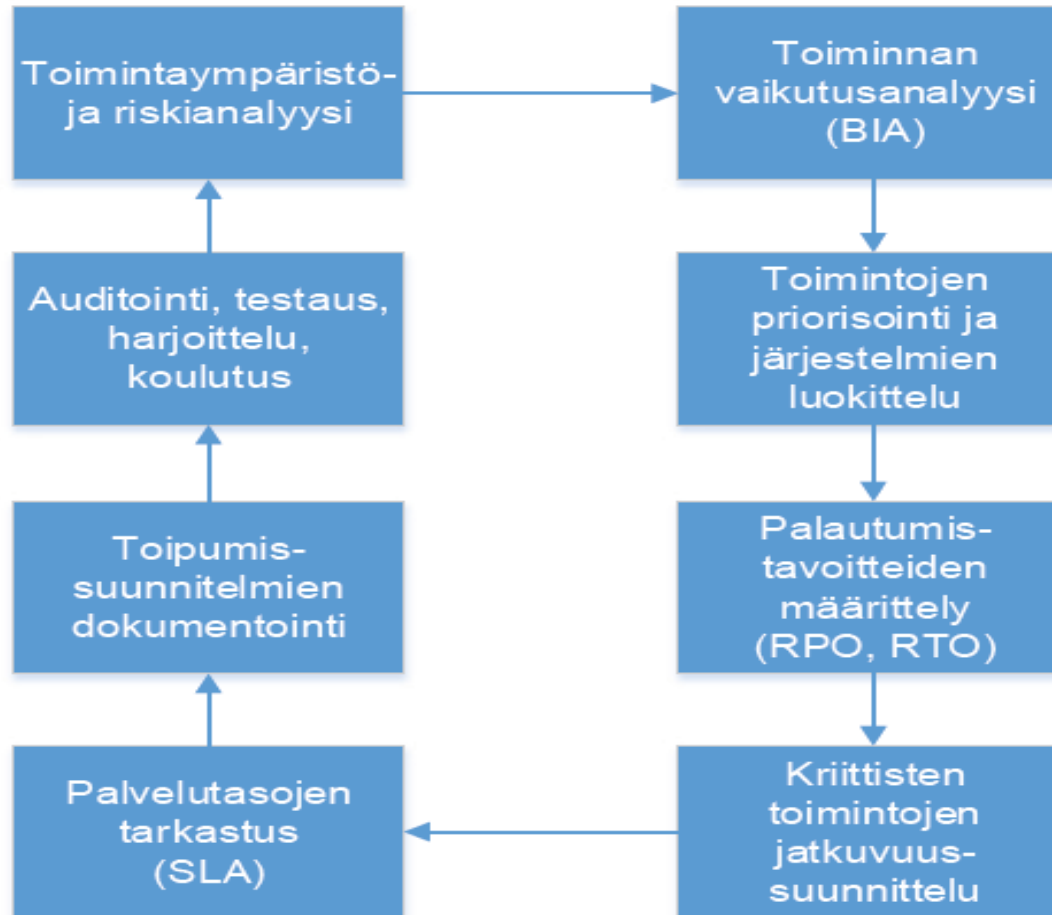


1. Toiminnan suunnittelu ja ohjaus

- Eri toimintayksiköiden näkemykset tulee yhdenmukaistaa koko organisaation tasolla
 - Toimintojen keskinäinen kriittisyys ja tavoitetasot yhteismitallisia.
- Jatkuvuus- ja toipumissuunnitelmat muodostavat hierarkkisen kokonaisuuden = jatkuvuuden hallinnan kokonaisuus
- Suunnittele ja toteuta jatkuvuuden hallinnan suunnitelmien rakenne ja hierarkia vastaamaan oman organisaatiosi toimintaa (sisältö tärkein).



Keskeiset jatkuvuussuunnittelun prosessit ja vaiheet



2. Toimintaympäristön riskianalyysit ja skenaariot

- Toiminnan jatkuvuutta uhkaa suurelta osin samat riskit kuin muutenkin organisaation toimintaa
 - => riskien kartoitus järkevintä osana yleistä riskienhallintaa
- Jatkuvuussuunnittelussa syytä varautua ainakin seuraavien skenaarioiden varalle:
 - 1. Organisaation **toimitilat** tai merkittävä osa niistä ei ole käytössä
 - 2. Organisaation **henkilöstö**, merkittävä osa siitä, ylin johto tai avainhenkilöt eivät ole käytettävissä
 - 3. Tietovarantojen, **tietojärjestelmien** tai tietoliikenteen vakavat häiriöt
 - 4. Merkittävä **palveluntoimittaja, vastapuoli, sidosryhmä** tms. ei ole käytettävissä
- Yleensä kaikki organisaation toiminnan jatkuvuutta uhkaavat riskit näiden pääryhmien alla
- Näihin skenaarioihin varautumalla voidaan toipua useimmista häiriöistä



3. Toiminnan vaikutusanalyysi (BIA)

- Tunne toimintaympäristö, suojattavat kohteet ja niihin liittyvät ydinprosessit ja –toiminnot
 - => Luokittelu kriittisyysluokkiin
- BIA = kartoitetaan erilaisten riskien toteutumisen toiminnalliset vaikutukset
 - => Jatkuvuuden turvaamiseen ja toipumistilanteisiin oikeat ja riittävät toimenpiteet
- Vaikutusanalyysityökalu kriittisyysluokan määrittämiseksi:
 - **Jatkuvuus-BIA-työkalu**
 - Tarkoitettu järjestelmään tai palveluun kohdistuvien häiriöiden vaikutusten arviointiin
 - Yhdenmukaistaa vaikutusten arviointia eri toimintojen välillä



4. Toimintojen priorisointi

- Kunkin toiminnon tavoiteltu palvelutaso ja toipumisaikavaade huomioitava jo suunnitteluvaiheessa
- Toimintojen luokittelu kriittisyyden mukaan ohjaa häiriötilanteissa korjaavien toimenpiteiden priorisointia
- Tuotantoon palautusjärjestys
- Jatkuvuus- tai toipumissuunnitelma ei auta jos palvelua tai järjestelmää suunniteltaessa ja rakentaessa ei ole otettu huomioon sen kriittisyyden vaatimia asioita.
- Kokonaisarkkitehtuurin huomioiminen



Palvelukerrokset – palvelutoimittajien hallinta?



tekninen palvelukerros	Tarkenne
Sovellus/järjestelmät	Liiketoimintasovellus
Sovellustietokannat	Tietokannat
Hakemisto/konfiguraatio	Varusohjelmat, middleware, hakemistot
Käyttöjärjestelmät	Käyttöjärjestelmä: HP-UX, Windows, klusterointi
Palvelinrauta	Palvelinlaitteistot
Ulkoiset tietoliikenneliittymät	Varmennusverkko, palomuuripalvelut
Verkkopalvelut	Toimistoverkko, hallintayhteydet, palvelutoimittajan toimistoverkko, nimipalvelut DNS, Active Directory
Storage/SAN	Levyjärjestelmät, kytkennät
Konesalien välinen siirtoyhteys	Kahdennettu tekniikka
Fyysinen konesali	Salien rakenne, tilaturvallisuus, varmennettu sähkönsyöttö, jäähdytys

5. Järjestelmien ja palvelujen luokittelu



- Järjestelmän luokittelu:
 - Käytön laajuus
 - Kriittisyys
 - Käyttökatkon vaikutukset
 - Järjestelmien käyttötarkoitus
 - Tietosisältö....
- JHS 174 mukainen SLA-palvelutaso:

Käytettävyys:

Elintärkeä

Erittäin tärkeä

Tärkeä

Jonkin verran tärkeä

Ei lainkaan tärkeä

SLA-palvelutaso:

Erittäin kriittinen

Kriittinen

Laajennettu

Normaali

Normaali

- Lopullisen keskinäisen tärkeysjärjestyksen päättää organisaation ylin johto

6. Palautumistavoitteiden määrittely

- BIA -> RTO -> RPO!
- Toiminnan keskeytysvaikutusanalyysi
- => pisin toiminnan sietämä käyttökatko (RTO, toipumisaika)
 - = **Järjestelmä takaisin ylhäällä**
- => kuinka pitkältä ajalta tietoa voidaan menettää (RPO, toipumispiste)
 - = **Mihin dataan palataan ts. mistä datasta jatketaan**
- RTO ja RPO määritely:
 - Suunnitellaan tekniset ratkaisut
 - Mitä lyhempää toipumisaikaa tai palautumispistettä halutaan, sitä suuremmat kustannukset
- HUOM! Vasteaika vs. Ratkaisuaika



7. Ohjelmistojen ja lisenssien hallinta

- Mikäli järjestelmä/palvelu joudutaan asentamaan uudestaan, toipumista nopeuttaa kun lisenssiavaimet ja koodit helposti saatavilla => kirjaa suunnitelmiin
- Lisenssiepäselvyydet, lisenssitarkastukset?
- Toiminto voi häiriintyä tai pysähtyä
- Tarkastuksen tuloksena suuria budjetoimattomia kustannuksia, joilla voi olla vaikutusta organisaation toiminnan jatkuvuuteen
- Varmista:
 - Omaisuuden hallinnan ajantasaisuus
 - Lisenssien ylläpitovastuut



8. Järjestelmien toipumistoimenpiteet

- Toipumissuunnitelmat kuvaavat operatiivisella tasolla järjestelmien palauttamisen häiriötilanteista
 - Korjaus- ja palautustoimet käytännössä
 - Hallittu alasajo/pakotettu alasajo
 - Hallittu uudelleen käynnistäminen
 - Toimivuuden testaaminen ennen käyttäjien pääsyä järjestelmään
 - Huolto- ja ylläpitosopimukset
 - Integraatiot ja riippuvuudet
 - Varajärjestelmät ja korvaavat menettelyt
 -



9. Häiriötilanteiden johtaminen ja ohjaus

- Tilannejohtoryhmä
- Operatiivinen toipumisryhmä
- Johto vastaa toimenpiteiden hyväksymisestä
- Toiminnasta normaalioloissa vastaavat toimivat myös häiriötilanteissa ja poikkeusoloissa (jos käytettävissä)
- Kaikki suunniteltava ja dokumentoitava etukäteen
- Ihmisten oltava tietoisia ja sitoutuneita rooliinsa
- Huomioi johtamistyövälineiden ja viestintävälineiden käytön jatkuvuus -> korvaavat menetelmät



10. Tilannekuvan luominen ja ylläpito

- Tilannekuva = kaikki toiminnan kannalta relevantti informaatio
- Tilannekuvaa tarvitaan ilman häiriöitäkin
- Häiriötilanteessa tarvitaan teknistä tilannekuvaa
 - Verkko
 - Palveluiden käytettävyys
 - Kyberuhkat
 - Palvelutoimittajat
 - Jne.
- Luo ennalta määritelty prosessi tietojen turvalliseen vaihtamiseen ja kommunikaatioyhteyden avaamiseen eri tahojen kanssa
- Kaikille osapuolille sama tieto tilanteesta
- Ajantasainen tilannekuva => johtaminen häiriötilanteessa mahdollista



11. Toipumisen edellyttämät tilat ja varatilat

- Määritettävä etukäteen tilat:
 - Toipumisen johtamiseen
 - Tekniseen toipumiseen
 - Palvelun tuottamiseen
 - Ja näiden varatilat
- Varusta toipumistilat etukäteen



12. Toiminta toipumistilanteessa

- Vakavan häiriötilanteen tunnistaminen
- Häiriön prioriteetin määrittäminen
- Minimoi tai estä ihmisiin, organisaation toimintaan, palveluihin, järjestelmiin, tietoon kohdistuvat vahingot
- Varmista kriittisten järjestelmien palautuminen ilman tarpeetonta viivytystä

13. Palvelutuottajan tehtävät, vastuut ja velvollisuudet

- Palvelutuottajan jatkuvuus- ja toipumissuunnitelmien tulee olla linjassa organisaation oman jatkuvuussuunnittelun kanssa
- Palvelutason mukaisesti -> huomioi jo kilpailutusvaiheessa kustannukset
- Varmista yhteinen käsitys sopimuksen sisällöstä, pätemisjärjestyksestä, sanktioista
- Harjoitukset koko järjestelmän elinkaaren ajan

14. Toimittajien ja alihankkijoiden ohjaus ja hallinta, sopimukset ja palvelutasot

- Kriittisten toimintojen palvelutoimittajaverkostolta vaadittava toimintamallit ko. organisaatioon kohdistuvien häiriötilanteiden varalta
- Velvoitteet ulotettava sopimuksissa koko alihankintaketjuun ja palvelutuottajaverkostoon
- Palvelua hankkiva organisaatio hyväksyy menettelytavat -> valvo vaatimusten toteutumista



15. Viestintä

- Sisäisen ja ulkoisen viestinnän periaatteet ja ohjeet, joihin sisältyy myös häiriötilanneviestinnän toteuttaminen
- Oikea tilannetieto ja tehdyt johtopäätökset
- Oikea-aikaista, jatkuvaa, avointa



16. Testaaminen, harjoittelu, koulutus

- Laajavaikutteisen häiriötilanteen harjoittelu kokonaisuudessaan kerran vuodessa
- Jatkuvuus- ja toipumissuunnitelmien ns. pöytätestaukset jos ei mahdollista harjoitella käytännössä laajoissa järjestelmissä
- Testaamisen ja harjoittelun avulla kehittyminen ja ongelmakohtien löytäminen -> kyky toimia oikein myös ennakoimattomissa tilanteissa
- Suunnitelmien säilytys eri muodoissa ja eri paikoissa

Jatkuvuuden hallinnan mittaaminen ja kehittäminen



- Jatkuvuuden hallinnan **vuosikello**
- Käytännössä **seuranta** ja **mittaaminen** tehdään yleensä harjoitusten yhteydessä ja toteutuneita häiriötilanteita arvioimalla
- **Raportoi** johdolle säännöllisesti
- **Auditoi** säännöllisesti
- **Jatkuvuussuunnittelu on prosessi, joka saatava kiinteäksi osaksi organisaation muuta toimintaa ja prosesseja**

Kiitos!