

Teknoliateollisuus ry:n
jäsenyritysten resilienssin
kehittäminen -
Resilienssimanuaali



Resilienssimanuaali

teknologiateollisuuden jäsenyrityksille

*Auttaa yrityksiä rakentamaan
toimintasuunnitelman, joka tukee
toiminnan jatkuvuutta häiriötilanteissa*

Aihenaamme on tänään kolme kokonaisuutta

Esityksen sisältö

01 LÄHTÖKOHTA
Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

02 RESILIENSSIMANUAALI
Mikä on resilienssimanuaali ja miten sitä käytetään

03 ESIMERKKEJÄ RESILIENSSIMANUAALIN SOVELTAMISESTA
Miltä resilienssimanuaali voisi näyttää eri toimialoilla?

Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

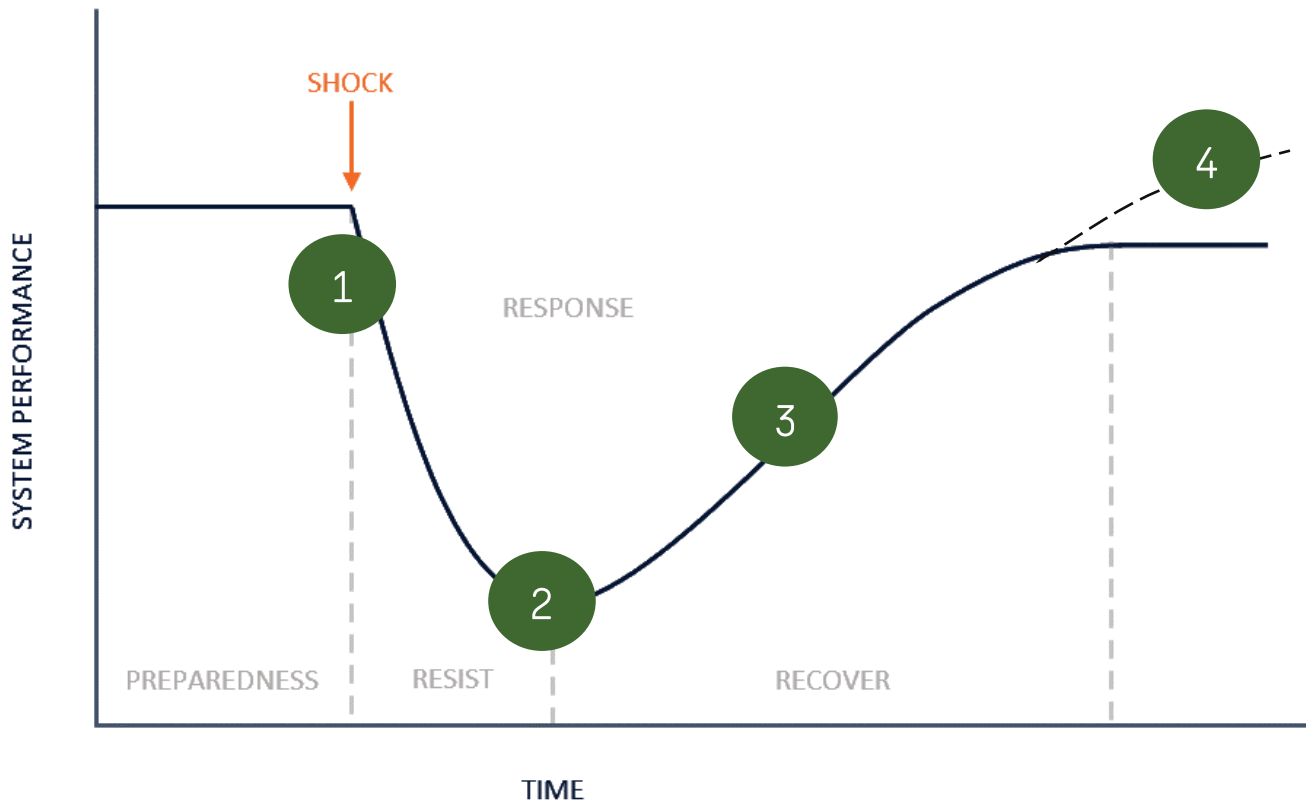
01

—
LÄHTÖKOHTA

Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

Resilienssi on organisaation kykyä varautua, palautua nopeasti ja oppia häiriöistä



1. Resilientti organisaatio on **varautunut**
2. Shokissa sen suorituskyky laskee **vähän**
3. Se palautuu **nopeasti**
4. Se **oppii** tapahtuneesta ja muusta

Kasvavan epävarmuuden maailmassa resilienssi tukee riskienhallinnan ennakointityötä

Monimutkaisuus ja epävarmuus kasvavat

- Monimutkaiset järjestelmät luovat uusia, **odottamattomia riskejä**
- Epävarmuus ja **ennakoimattomuus** lisääntyvät jatkuvasti

Perinteinen riskienhallinta kohdistuu uhkiin

- Riskianalyysi on usein kertaluonteista ja **keskittyy tunnettuihin riskeihin**
- Tarkoituksellinen vaikuttaminen muuttaa riskimaisemaa radikaalisti
- **Riskeihin varautuminen erillisin keinoin on tehotonta**

Tarvitaan kokonaisvaltaista varautumista

- Turvallisuus ja riskienhallinta on mentaalisesti ulkoistettavissa, vaikka sen pitäisi olla **koko organisaation vastuulla**
- Fokuksen tulisi olla **pitkän aikavälin kehittämisessä** ja strategisessa suunnittelussa

Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

Riskienhallinta vastaa tunnistettuihin riskeihin – resilienssi täydentää tätä rakentamalla kyvyn selvittää myös tuntemattomista

Lähtökohta: tunnistetut riskit ja skenaariot
→ fokus uhkissa, jotka voidaan nimetä ja arvioida



Menetelmä: todennäköisyys x vaikuttavuus
→ arvioidaan shokkien todennäköisyyksiä



Tavoite: riskien pienentäminen ja kontrollit
→ estetään tai vähennetään haittaa



Luonne: ennakoiva ja riskikohtainen
→ toimii hyvin tunnetussa toimintaympäristössä

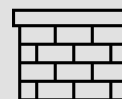


RISKIENHALLINTA



Mitä voi tapahtua ja kuinka todennäköisesti?

RESILIENSSI



Minkä pitää aina toimia ja miten se taataan?

Lähtökohta: kriittiset toimintaedellytykset
→ fokus siinä, mikä mahdollistaa jatkuvuuden



Menetelmä: kyvykkyyksien ja joustavuuden arviointi
→ vaihtoehdot, reagointikyky, sopeutuminen



Tavoite: toimintakyvyn säilyttäminen muutoksessa
→ yrityksellä on kapasiteettia toimia myös yllättävissä tilanteissa



Luonne: kokonaisvaltainen ja adaptiivinen
→ valmistaa myös ennakoimattomiin häiriöihin



Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

Tutustuimme resilienssin johtamisen nykytilaan suomalaisissa pk-yrityksissä

Havaintomme **resilienssin johtamisen nykytilasta**

-  **Resilienssin johtaminen ei tällä hetkellä muodosta yhtenäistä kokonaisuutta**
Riskienhallintaa tehdään, mutta se jää usein irralleen strategiasta. Resilienssille ei usein ole omistajaa eikä rakennetta
-  **Työkalut ovat kevyitä ja itse rakennettuja**
Excel-pohjaiset riskimatriisit ja satunnaiset ISO-auditoinnit. Toimialakohtaista valmista viitekehystä ei ole.
-  **Yritykset toivovat konkretiaa**
Valmiita toimenpide-ehdotuksia, minimivaatimustasoa, mittareita maturiteetin arviointiin — ja matalaa aloituskynnystä.

Riskien tunnistaminen **ei automaattisesti johda käytännön toimiin.**
Yritysten on vaikea arvioida oman resilienssinsä tasoa tai suunnitella toimintaansa resilienssin suhteen ilman selkeitä malleja

Miksi resilienssiin tulisi keskittyä — ja miksi resilienssimanuaali

02

RESILIENSSIMANUAALI

Mikä on resilienssimanuaali ja miten sitä käytetään?

Resilienssimanuaalin tarkoitus on auttaa yrityksiä muodostamaan toimenpidesuunnitelma jatkuvuuden varmistamiseksi

Resilienssimanuaalin pohjaksi on luotu kattava lista – noin tuhat – toimenpidettä, jotka toimivat lähtökohtana toimenpidesuunnitelman laatimisessa

Toimenpiteen vaihe	Toimenpiteen maturaiteittaso	Toimenpide
Suunnittelu ja varautuminen	Oletusarvoinen	Ajantasaisen listan ylläpito kaikista suorista toimittajista ja hankintasopimuksista
Suunnittelu ja varautuminen	Oletusarvoinen	Kriittisimpien raaka-aineiden ja niiden korvaavuusmahdollisuuksien tunnistaminen
Suunnittelu ja varautuminen	Oletusarvoinen	Force majeure -ehtojen ja toimitushäiriölausekkeiden varmistaminen hankintasopimuksissa
Suunnittelu ja varautuminen	Oletusarvoinen	Lakisääteisten ja sääntelyvaatimusten tunnistaminen ja dokumentointi hankintaketjulle
Suunnittelu ja varautuminen	Oletusarvoinen	Liiketoiminnan vaikutusanalyysin (BIA) toteuttaminen suorien hankintojen osalta
Suunnittelu ja varautuminen	Keskitason toimenpide	Vaihtoehtoisten toimittajien rekisterin kehittäminen (vähintään 2 vaihtoehtoa kullekin kriittiselle nimikkeelle)
Suunnittelu ja varautuminen	Keskitason toimenpide	Säännöllisen toimittajarisikanalyysin toteuttaminen (taloudellinen vakaus, maantieteellinen sijainti, kapasiteetti)
Suunnittelu ja varautuminen	Keskitason toimenpide	Varastointiasioista ja puskurivarastojen ylläpidosta sopiminen ennakkoon
Suunnittelu ja varautuminen	Keskitason toimenpide	Henkilöstön osaamisen ja tietoisuuden varmistaminen hankintaketjun jatkuvuusmenettelyistä
Suunnittelu ja varautuminen	Keskitason toimenpide	Toimittajien tietoturvarisikien arviointi osana hankintaprosessia
Suunnittelu ja varautuminen	Kehittynyt toimenpide	Reaaliaikaisen toimitusketjun riskimonitoroinnin käyttöönotto (geopolittiset riskit, luonnonkatastrofien seuranta)
Suunnittelu ja varautuminen	Kehittynyt toimenpide	Toimitusketjun kriittisten linkkeiden mallinnus simulatioilla

Kaikki toimenpiteet eivät kuitenkaan ole relevantteja kaikille yrityksille. Resilienssimanuaali tarjoaa ohjeet yrityksille omaan toimintaympäristöön sopivien toimenpiteiden valitsemiseksi

Sisäiset toimintaedellytykset						
Tuotantotilat	IT-infrastruktuuri	Tuotantolaitteet	Data	Ihmiset	Rahoitus	Henkinen pääoma
<ul style="list-style-type: none"> Omat ja vuokratilat Tiloihin liittyvät peruspalvelut (sähkö, vesi) 	<ul style="list-style-type: none"> Oma IT-infrastruktuuri (serverit ja tietokoneet) Ulkoinen IT-infrastruktuuri (pilvipalvelut) 	<ul style="list-style-type: none"> Tuotantolaitteet 	<ul style="list-style-type: none"> Data 	<ul style="list-style-type: none"> Tuotantohenkilöstö Asiantuntijat Johto ja esihenkilöt Tukitoiminnot 	<ul style="list-style-type: none"> Käyttöpääoma Oma pääoma Vieras pääoma 	<ul style="list-style-type: none"> Prosessit (hiljainen ja tallennettu tieto) Kulttuuri Osaaminen
Ulkoiset toimintaedellytykset						
Raaka-aineet ja toimittajat	Tuotantokumppanit	Sijoittajat	Asiakkaat ja myyntikanavat			
<ul style="list-style-type: none"> Suorat hankinnat Epäsuorat hankinnat Strategiset toimittajat Muut toimittajat 	<ul style="list-style-type: none"> Sopimusvalmistajat Yhteisyritykset ja liittoumat Kriittiset kumppanit 	<ul style="list-style-type: none"> Sijoittajat 	<ul style="list-style-type: none"> Avainasiakkaat Pienet ja keskiuuret asiakkaat Suorat myyntikanavat Jakelukumppanit ja jälleenmyyjät 			



Toimenpidesuunnitelma jatkuvuuden varmistamiseksi

- Määrittelee ne oleelliset toimenpiteet, jotka yrityksen tulisi tehdä jatkuvuutensa varmistamiseksi
- Toimenpiteet pohjautuvat yrityksen toimintaedellytysten ja toimintaympäristön erityispiirteisiin
- Toimenpiteet ottavat huomioon yrityksen käytössä olevat resurssit ja osaamisen
- Toimenpiteet jakautuvat neljään luokkaan: varautuminen & havaitseminen, vastustaminen, toipuminen, oppiminen

Toimenpidesuunnitelman lähtökohtana on ydinajatus yrityksen toimintaedellytysten takaamisesta riippumatta ulkoisista shokeista



Toimenpidesuunnitelma jatkuvuuden varmistamiseksi

Ydinkysymys: Minkä pitää aina toimia ja miten se taataan?

➤ Toimenpidesuunnitelma **ei keskity** kysymykseen, ”mitä ulkoisia häiriöitä voi tapahtua ja kuinka todennäköisesti?”



Lähtökohta: kriittiset toimintaedellytykset

→ fokus siinä, mikä mahdollistaa jatkuvuuden



Tavoite: toimintakyvyn säilyttäminen muutoksessa

→ yrityksellä on kapasiteettia toimia myös yllättävissä tilanteissa



Menetelmä: kyvykkyyksien ja joustavuuden arviointi

→ vaihtoehdot, reagointikyky, sopeutuminen



Luonne: kokonaisvaltainen ja adaptiivinen

→ valmistaa myös ennakoimattomiin häiriöihin

Toimenpidesuunnitelman rakentamisessa on kolme vaihetta – oleellista on ymmärtää yrityksen toimintaedellytykset ja maturiteetti

Tavoitteena ei ole ennustaa häiriöitä, vaan varmistaa, että yrityksen keskeiset toiminnot säilyvät, mukautuvat ja toipuvat riippumatta häiriön luonteesta.

1

Hahmota toimintaedellytyksesi

Minkä varassa yritys toimii? Mitä ilman se ei voisi toimia?

Resilienssi lähtee siitä, että hahmotetaan omat toimintaedellytykset

Yrityksestä ja toimialasta riippuen edellytykset ja niiden merkitys ja kriittisyys organisaatiolle vaihtelevat. **Yleisesti ottaen toimintaedellytykset jakaantuvat sisäisiin ja ulkoisiin.**

2

Tunnista mahdolliset toimenpiteet

Mitä voimme tehdä mitä yleisesti ottaen voidaan tehdä toimintaedellytysten varmistamiseksi?

Toimenpiteet jakautuvat neljään luokkaan: varautuminen & havaitseminen, vastustaminen, toipuminen, oppiminen.

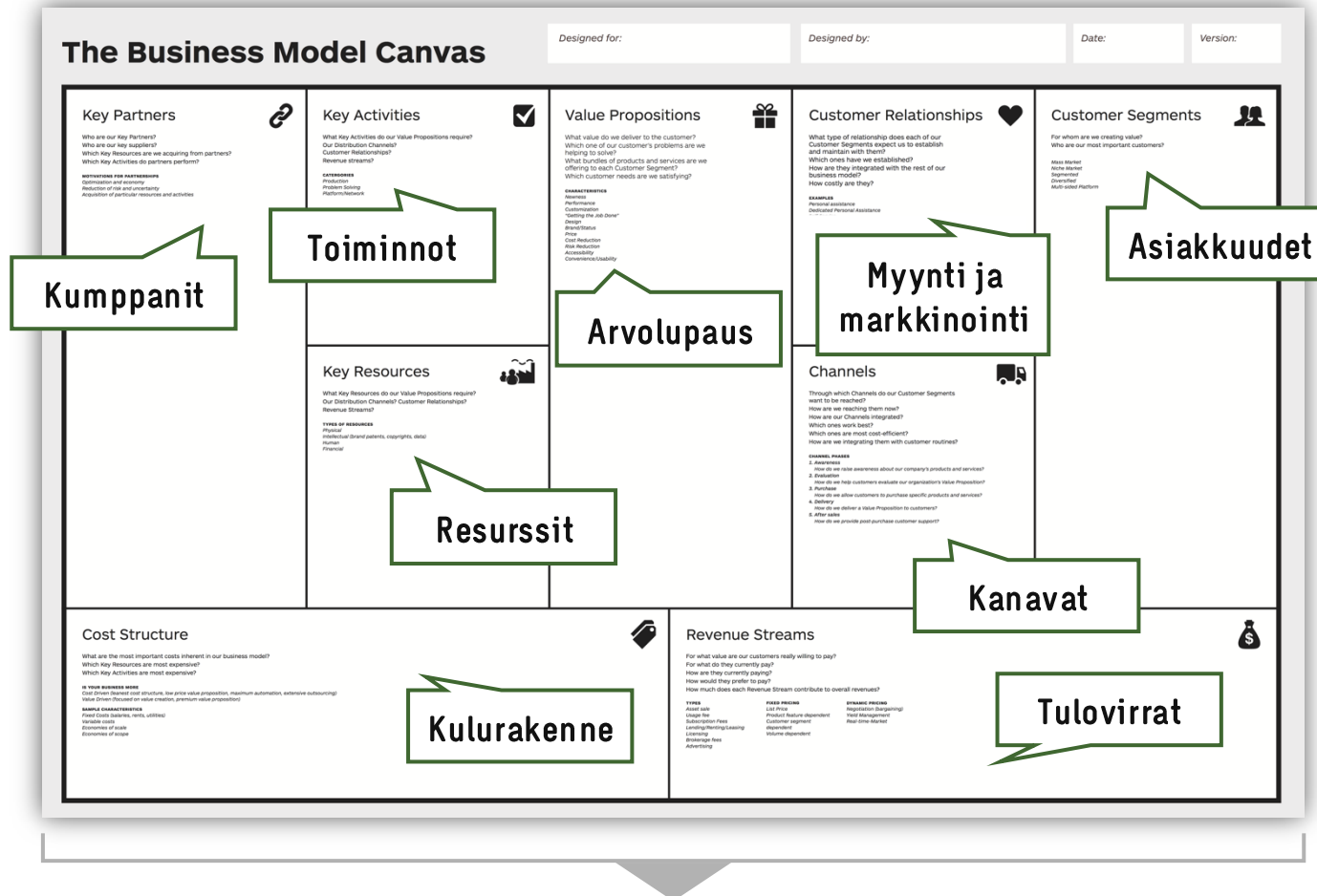
3

Priorisoi toimenpiteet kyvykkyyksiesi mukaan

Mitä oman yritykseni kannattaa tehdä?

Priorisoinnissa on hyödynnettävä toimintaedellytysten kriittisyysarvioinnin lisäksi toimenpiteiden arvioituja hyötyjä ja toimenpiteen vaatimia resursseja .

Resilienssin kehittämisen lähtökohtana on yrityksen toimintaedellytysten ja niiden kriittisyyden hahmottaminen



Sisäiset toimintaedellytykset

Ulkoiset toimintaedellytykset

- Tuotantotilat
- IT-infrastruktuuuri
- Tuotantolaitteet
- Data
- Ihmiset
- Rahoitus
- Henkinen pääoma

- Raaka-aineet ja toimittajat
- Tuotantokumppanit
- Sijoittajat
- Asiakkaat ja myyntikanavat

Resilienssin kannalta oleelliset toimintaedellytykset muodostavat ns. "Resilience Model Canvasin"

Toimintaedellytykset on rakennettu pohjautuen Alexander Osterwalderin Business Model Canvasiin, joka kuvaa yrityksen toimintaa

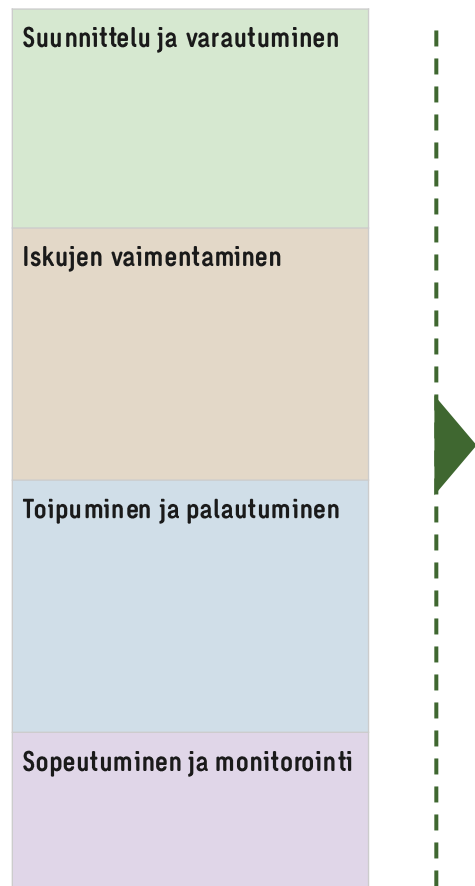
Toimintaedellytyksiä suojaavat toimenpiteet jaetaan neljään ajalliseen vaiheeseen suhteessa ulkoiseen häiriöön

Hyvä toimenpidesuunnitelma ottaa huomioon neljä ajallista vaihetta häiriön tapahtumisen suhteen!

	Ajallinen vaihe	Kuvaus	Esimerkkejä eri toimintaedellytysten suhteen
1	Suunnittelu ja varautuminen	Ennen häiriötä. Toimintaedellytysten tunnistaminen, riippuvuuksien kartoittaminen, riskien arviointi, vaihtoehtojen ennakkosopiminen ja jatkuvuussuunnitelmien laatiminen. Tavoite: organisaatio tietää mistä on riippuvainen, mitä voi mennä pieleen ja mitä silloin tehdään. Toimenpiteet ovat luonteeltaan kartoittavia, dokumentoivia ja sopimuksellisia.	Toimittajille tunnistetaan vaihtoehtoja ja sovitaan varatoimittajasopimuksista. Laitteille laaditaan huolto-ohjelmia ja kartoitetaan varaosien saatavuutta. Henkilöstölle rakennetaan varahenkilöjärjestelmiä ja cross-training-ohjelmia. IT-järjestelmille kehitetään disaster recovery -suunnitelmia ja datalle varmuuskopiointipolitiikkoja. Rahoitukselle määritetään kassareservien minimitasoja ja diversifioidaan rahoituslähteitä.
2	Iskujen vaimentaminen	Häiriön aikana. Välittömät toimenpiteet vaikutusten rajoittamiseksi: varakapasiteetin aktivointi, kriittisten toimintojen priorisointi, viestintä sidosryhmille ja kriisijohtamisen käynnistäminen. Tavoite: minimoida häiriön laajuus ja kesto, turvata kriittisimmät toiminnot. Toimenpiteet ovat luonteeltaan aktivoivia, priorisoivia ja viestinnällisiä.	Toimittajahäiriössä aktivoidaan varatoimittajasopimukset ja priorisoidaan kriittiset tuotantolinjat. Tilahäiriössä evakuoidaan henkilöstö ja siirrytään varatilaan tai etätyöhön. IT-häiriössä käynnistetään failover varajärjestelmiin ja eristetään vaurioitunut ympäristö. Henkilöstövajeessa aktivoidaan vuokratyövoima ja priorisoidaan tehtävät osaamisen mukaan. Rahoitushäiriössä nostetaan luottolimiittejä ja neuvotellaan kovenanttijoustoja.
3	Toipuminen ja palautuminen	Häiriön jälkeen. Normaalin toiminnan palauttaminen, häiriön dokumentointi, juurisyyanalyysi ja suunnitelmien päivittäminen oppien perusteella. Tavoite: palata normaalitilaan ja varmistaa, ettei sama häiriö toistu samalla tavalla. Toimenpiteet ovat luonteeltaan analyysoivia, korjaavia ja päivittäviä.	Toimittajasuhteissa arvioidaan toimittajan suorituskyky häiriön aikana ja päivitetään sopimusehdot. Laitteille tehdään juurisyyanalyysi ja päivitetään kunnossapidon parametrit. IT-häiriöstä laaditaan incident-raportti ja paikataan havaitut haavoittuvuudet. Datahäiriössä varmistetaan eheys ja täytetään tietosuojailmoitusvelvollisuudet. Osaamisvajeista tunnistetaan puutteet ja vahvistetaan cross-training-ohjelmaa. Rahoituksessa täydennetään kassareservit ja arvioidaan rahoitusrakenteen kestävyys.
4	Sopeutuminen ja monitorointi	Jatkuva. Toimintaedellytysten ja riskiympäristön systemaattinen seuranta, harjoitukset, auditoinnit ja strategian päivittäminen. Tavoite: tunnistaa muutokset ja heikot signaalit ennen kuin ne realisoituvat häiriöiksi. Toimenpiteet ovat luonteeltaan mittaavia, testaavia ja ennakoivia.	Toimittajille ylläpidetään scorecard-järjestelmää ja seurataan taloudellista tilaa. Tiloille tehdään vuosittaisia riskiarviointeja ja testataan varavoimajärjestelmiä. IT-ympäristölle toteutetaan penetraatiotestauksia ja DRP-harjoituksia. Henkilöstölle seurataan vaihtuvuutta ja osaamisriskejä.

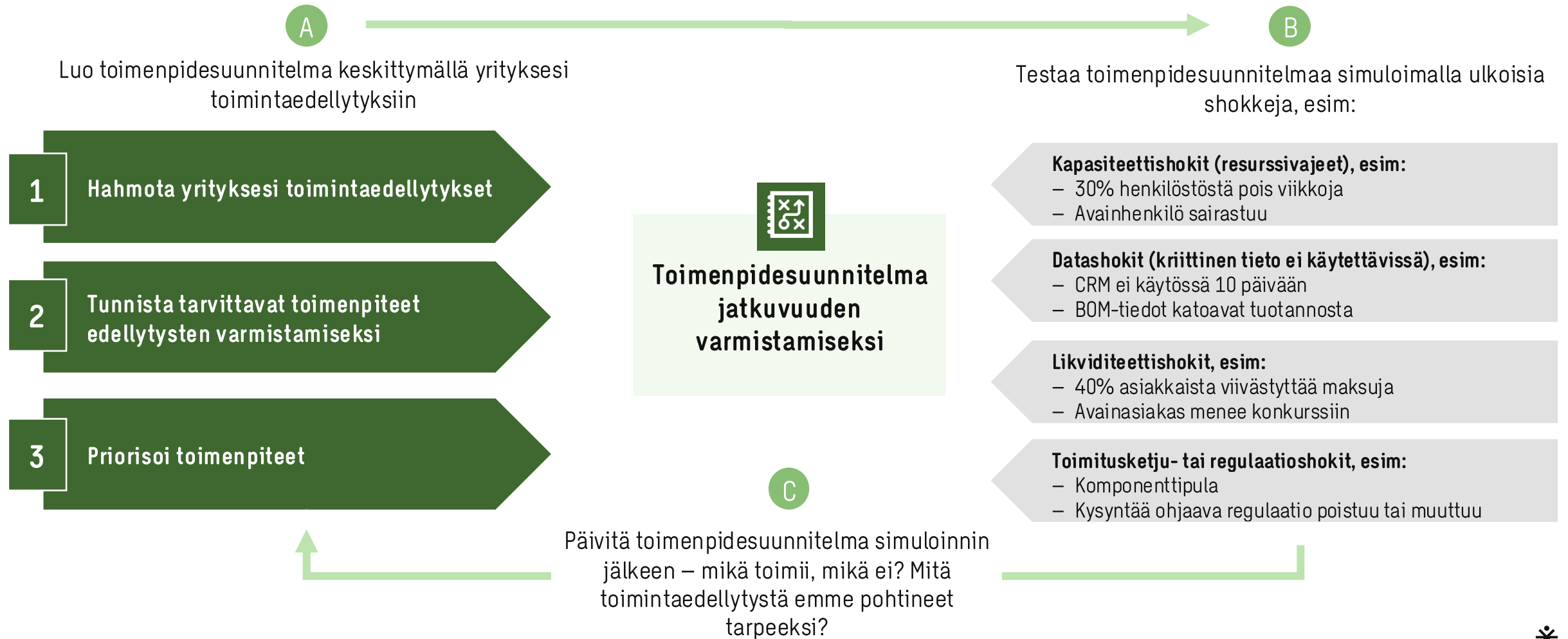
Toimenpiteitä tulee lopuksi arvioida vaikuttavuuden ja kypsyyden mukaan - laajempi toimenpidekattavuus takaa yrityksen resilienssin

Toimenpiteet jakautuvat ajallisen vaiheen lisäksi maturiteettiltaan kolmeen luokkaan



Maturiteettitaso	Kuvaus	Esimerkkejä eri ajallisten vaiheiden suhteen
Oletusarvoinen	Perustason toimenpiteet, jotka jokaisen organisaation tulisi vähintään toteuttaa. Vaativat suhteellisen vähän resursseja ja erikoisosaamista. Keskittyvät tunnistamiseen, dokumentointiin, perusvarajärjestelyihin ja manuaalisiin prosesseihin.	Suunnittelussa: toimittajarekisterin ylläpito, kriittisten laitteiden tunnistaminen, varahenkilöjärjestelmän toteuttaminen, varmuuskopiointipolitiikan dokumentointi. Iskujen vaimentamisessa: puskurivarastojen aktivointi, varakanavaan siirtyminen, sidosryhmien informointi, kassareservien aktivointi. Toipumisessa: häiriön dokumentointi, normaalin toiminnan palauttaminen, vakuutuskorvausprosessin käynnistäminen. Monitoroinnissa: sopimusten vuosittainen tarkistaminen, palvelutason seuranta, varajärjestelmien testaaminen.
Keskitaso	Systemaattisemmat ja rakenteellisemmat toimenpiteet, jotka edellyttävät analyttistä osaamista, poikkifunktionaalista yhteistyötä ja strategisempaa otetta. Keskittyvät riskianalyyseihin, scorecard-järjestelmiin, auditointeihin ja vaihtoehtoisten ratkaisujen kvalifointiin.	Suunnittelussa: toimittajariskianalyysin toteuttaminen, IT disaster recovery -suunnitelman kehittäminen, kriisijohtamiskoulutuksen järjestäminen, data governance -mallin kehittäminen. Iskujen vaimentamisessa: ennalta sovittujen varatoimittajasopimusten aktivointi, kriisiviestintäsuunnitelman käynnistäminen, kovenanttijoustoista neuvottelu, forensiikkatoimenpiteiden käynnistäminen. Toipumisessa: juurisyyanalyysin tekeminen, sopimusehtojen päivittäminen oppien perusteella, cross-training-ohjelman vahvistaminen, rahoitusrakenteen kestävyuden arviointi. Monitoroinnissa: vuosittaiset stressitestit ja auditoinnit, toimittajien scorecard-järjestelmä, henkilöstöriskien vuosittainen arviointi, DRP-harjoitukset.
Kehittynyt	Edistyneisimmät toimenpiteet, jotka hyödyntävät reaaliaikaista analytiikkaa, automaatiota, simulaatioita ja adaptiivisia malleja. Vaativat merkittäviä investointeja teknologiaan ja osaamiseen. Keskittyvät ennakointiin, dynaamiseen optimointiin ja jatkuvaan sopeutumiseen.	Suunnittelussa: toimitusketjun simulaatiot, digital twin -mallinnus, kyberresilienssin zero trust -arkkitehtuuri, ilmatoriskien skenaariopohjainen mallinnus. Iskujen vaimentamisessa: automatisoidut failover-mekanismit, reaaliaikainen data-analytiikka resurssien ohjaamiseksi, dynaaminen tuotantosuunnittelu, multi-cloud-failoverin automaattinen aktivointi. Toipumisessa: häiriödatan integrointi riskimalleihin, automatisoidun palautumisprotokollan kehittäminen, resilienssipisteityksen kehittäminen kumppaneille. Monitoroinnissa: tekoälypohjainen ennusteanalytiikka, jatkuva kyberuhka-analytiikka, adaptiiviset strategiat jotka mukautuvat automaattisesti riskiympäristön muutoksiin.

Resilienssin rakentaminen on iteratiivinen prosessi, jossa toimintasuunnitelmaa testataan ulkoisia shokkeja simuloimalla



Lopullinen toimenpidesuunnitelma kokoaa priorisoidut toimenpiteet, vastuut ja aikataulun yhteen näkymään

ESIMERKKI LOPULLISESTA TOIMENPIDESUUNNITELMASTA

Toiminta- edellytys	Toimenpide	Nykytila	Prioriteetti	Vaikutus	Vastuu	Aika- taulu	Status
Asiantuntijat	Varahenkilömalli kriittisiin rooleihin	Osittainen	Korkea	Korkea	HR	Q3/2026	Käynnissä
Asiantuntijat	Asiantuntijoiden osaamiskartoitus	Ei käytössä	Korkea	Korkea	HR	Q2/2026	Ei aloitettu
Data	Kriittisten datatyyppeiden ja varantojen tunnistaminen ja luokittelu	Ei käytössä	Korkea	Korkea	IT	Q2/2026	Ei aloitettu
Strategiset toimittajat	Toimittaja-diversifiointi	Osittainen	Keskitaso	Korkea	Hankinta	Q4/2026	Käynnissä
Oma pääoma	Kassapuskurin kasvattaminen	Käytössä	Keskitaso	Keskitaso	CFO	Jatkuva	OK

”Nykytila” kuvaa, missä määrin toimenpide on yrityksessä käytössä. ”Ei käytössä” tarkoittaa, että toimenpide on tarkoitus ottaa käyttöön, mutta kartoitusvaiheessa sitä ei ole toteutettu yrityksessä.

Toimenpidesuunnitelma kokoaa yhteen yrityksen resilienssin kehittämisen kannalta kriittisimmät toimenpiteet, niiden prioriteetit ja vastuut, toimien johdon käytännön työkaluna, **joka varmistaa että tunnistetut riskit kääntyvät systemaattiseksi kehitystoimiksi ja konkreettisiksi päätöksiksi.**

Se **ei ole staattinen lista**, vaan jatkuvasti kehittyvä kokonaisuus, jota päivitetään simulointien ja muuttuvan toimintaympäristön perusteella varmistaen sen ajantasaisuus ja vaikuttavuus.

Resilienssityökalu tuottaa arvoa vain systemaattisella ja laajasti organisaatiota osallistavalla käytöllä

Kenelle tarkoitettu?

Liikkeenjohdolle pääasiassa pk-yrityksessä, mutta hyödynnettävissä myös isommissa.

Milloin hyödynnetään?

Vuosittain laajempaan arvion strategia-prosessin yhteydessä sekä häiriötilanteissa tai isommissa muutostilanteissa.

Mihin tarkoitukseen?

Strategia- ja vuosisuunnittelu, riskienhallinta ja jatkuvuussuunnittelu sekä kehitystoimenpiteiden priorisointi.

Tehtäväjako?

Liikkeenjohto: vastaa priorisoinnista ja päätöksistä

Riskienhallinta: fasilitoi prosessia ja ylläpitää työkalua

Muut funktiot: tukevat analyysin teossa

YKSINKERTAISTETTU PROSESSIKUVAUS TYÖKALUN KÄYDÖSTÄ YRITYKSESSÄ



1. Kriittisten toimintaedellytysten tunnistus johtoryhmässä



2. Nykytilan arviointi funktioissa työkalufasilitoijan johtamana



3. Tulosten tiivistäminen ja priorisointilistaehdotuksen luominen (fasilitoija)



4. Priorisoitavien toimenpiteiden valinta johtoryhmässä sekä omistajuus ja aikataulumääritykset



5. Kehitystoimenpiteiden seuranta, häiriösimulointi ja mahdolliset muutokset



Onnistumisen edellytykset

1. Selkeä prosessiomistajuus (esim. riskienhallinta)
2. Johdon sitoutuminen
3. Poikkifunktionaalinen osallistuminen
4. Realistinen priorisointi
5. Linkitys budjetointiin ja tiekarttoihin



Yleisimmät sudenkuopat

1. Työkalua käytetään vain kerran > ei jatkuvuutta
2. Liian teoreettinen käyttö, joka ei johda toimenpiteisiin
3. Ei omistajuutta > ei toteutusta
4. Liikaa valittuja toimenpiteitä > ei fokuointia

03

ESIMERKKEJÄ RESILIESSIMANUAALIN SOVELTAMISESTA

Miltä resilienssimanuaali voisi näyttää eri toimialoilla?

Yritykset eri toimialoilla luovat toimenpidesuunnitelman perustuen oman toiminnan kriittisimpiin toimintoihin

Viisi esimerkkitapausta –
**toimintapidesuunnitelmat
eroavat, koska kriittiset
toimintaedellytykset
eroavat!**

1. **Kone- ja metallituoteteollisuus** – toimenpidesuunnitelma painottaa fyysisen tuotantoympäristön, kriittisten laitteiden ja toimituskyvyn turvaamista teollisen tuotannon jatkuvuuden takaamiseksi.
2. **Elektroniikka- ja sähköteollisuus** – toimenpidesuunnitelma painottaa ennen kaikkea teknisten järjestelmien, datan ja kriittisen osaamisen suojaamista liiketoiminnan jatkuvuuden varmistamiseksi.
3. **Tietotekniikka** – toimenpidesuunnitelma painottaa data-intensiivisen liiketoiminnan turvaamiseksi erityisesti IT-järjestelmien, asiakasdatan ja kriittisen asiantuntijaosaamisen suojaamista.
4. **Metallin jalostus** - toimenpidesuunnitelma painottaa ennen kaikkea fyysisen tuotantoympäristön, laitteiden ja kriittisen henkilöstön suojaamista tuotannon keskeytymättömyyden varmistamiseksi.
5. **Suunnittelu- ja konsultointi** – toimenpidesuunnitelma painottaa IT-ympäristön ja kriittisen asiantuntijaosaamisen turvaamista

Ensimmäinen esimerkki koskee kuvitteellista kone- ja metallituote-teollisuuden toimialan yritystä

Esimerkkiyritys 1: Kone- ja metallituote-teollisuus

- Keskisuuri perheyriety, 180 työntekijää
- Erikoistunut vaativien koneenosien ja -komponenttien valmistukseen energia- ja laivanrakennusteollisuudelle
- Liikevaihto 45 M€
- Tuotantolaitokset Suomessa (päälaitos) ja Virossa (tytäryhtiö)
- 85% tuotannosta menee vientiin
- Pitkäaikaiset toimitussopimukset 3-4 globaalin pääasiakkaan kanssa
- Investoinut voimakkaasti automaatioon ja robotiikkaan viimeisen 5 vuoden aikana

Esimerkkiyritys 1:n kriittisimmät toimintaedellytykset

- Omat tilat - Erikoisvarusteltu oma tuotantolaitos
- Tiloihin liittyvät peruspalvelut - Teollisuussähkön saatavuus kriittistä
- Tuotantolaitteet - Erittäin kalliit CNC-koneet ja robottijärjestelmät
- Tuotantohenkilöstö - Erikoisosaamista vaativat hitsaajat ja koneistajat
- Osaaminen - Vuosien aikana kehittynyt erikoisosaaminen
- Avainasiakkaat - 75% liikevaihdosta 3-4 asiakkaalta
- Strategiset toimittajat - Erikoisterästen ja -metallien toimittajat

Toimintasuunnitelma rakentuu näiden toimintaedellytysten ympärille!

Case-esimerkit toimialoittain

Toimenpidesuunnitelmassa korostetaan fyysisten toimintojen, tuotantolaitteiden ja toimituskyvyn varmistamista

Yritys on keskisuuri ja sillä on suhteellisen paljon resursseja, joten suunnitelmassa on myös kehittyneitä toimenpiteitä kriittisimmille toiminnoille.

Kone- ja metallituoteteollisuuden esimerkkiyrityksen toimintaedellytykset ja niitä suojelevat toimenpiteet (ESIMERKKI)

	Omat tilat	Tiloihin liittyvät peruspalvelut	Tuotantolaitteet	Tuotantohenkilöstö	Strategiset toimittajat	Osaaminen	Avainasiakkaat
1. SUUNNITTELU JA VARAUTUMINEN	Toimitilojen rekisterin ylläpito	Kriittisten peruspalvelujen (esim. sähkö) riippuvuuksien tunnistaminen ja dokumentointi	Kaikkien tuotantolaitteiden rekisterin ylläpito	Kriittisten tuotantoroolien ja avainhenkilöiden tunnistaminen	Strategisten toimittajien tunnistaminen ja dokumentointi	Kriittisten osaamisten tunnistaminen ja osaamiskartan laatiminen	Suurimpien asiakkaiden tunnistaminen ja sopimussuhteiden dokumentointi
	Kriittisten toimitilojen tunnistaminen ja BIA:n toteuttaminen	Peruspalvelujen toimittajien ja sopimusten dokumentointi	Kriittisten laitteiden tunnistaminen ja niiden palautumisajan ja maksimikeskeytysajan arviointi	Varahenkilöjärjestelmän toteuttaminen kriittisiin tuotantotehtäviin	Strategisten toimittajien vähintään perustason jatkuvuus-suunnitelman varmistaminen	Osaamisvajaiden tunnistaminen suhteessa jatkuvuustarpeisiin	Asiakaskeskittymäriskin arviointi: top 5 asiakkaiden liikevaihto-osuuden analyysi
	Toimitilojen pelastussuunnitelman laatiminen ja ylläpito	Varavoimaratkaisujen perustason varmistaminen	Huolto- ja kunnossapito-ohjelman ylläpito kriittisille laitteille	Työterveys- ja turvallisuusohjelman ylläpito	Säännölliset yhteistyöpalaverit ja häiriötilanteiden viestintäprotokolla	Koulutussuunnitelman kehittäminen kriittisten osaamisten varmistamiseksi	Selkeiden toimitushäiriöehtojen varmistaminen myyntisopimuksissa
	Toimitilojen riskiarvioinnin toteuttaminen	BIA:n (toiminnan keskeytymisen vaikutusten arviointi) toteuttaminen peruspalvelujen katkon vaikutusten arvioimiseksi	Varaosien saatavuuden varmistaminen kriittisille laitteille	Moniosaajuusohjelman (cross-training) kehittäminen tuotantohenkilöstölle	Lakisääteisten, sääntelyyn ja sopimukseen perustuvien vaatimusten tunnistaminen strategisille toimittajasuhteille	Osaamisen hajautuksen varmistaminen	Asiakaskohtaisten jatkuvuussuunnitelmien kehittäminen avainasiakkaille
	Vaihtoehtoisten toimitilojen kartoittaminen ja ennakkosopiminen	Varmistetaan kriittisiin tiloihin varayhteydet ja varasyöttö (esim. kahdennettu sähkönsyöttö)	Varalaitteiston ja varakapasiteetin kartoittaminen (oma, vuokra, kolmas osapuoli)	Työvoiman saatavuusriskianalyysin toteuttaminen	Perusteellisen riippuvuusanalyysin tekeminen	Osaamisriskianalyysin toteuttaminen	Avainasiakkaiden omien riskien ja heijastusvaikutusten kartoittaminen
	Toimitilojen riskiarvioinnin toteuttaminen	Varavoimakapasiteetin riittävyden arviointi suhteessa kriittisten toimintojen tarpeeseen	Laittekohtaisen riskiarvioinnin toteuttaminen (vikaantumistodennäköisyys, seurausten vakavuus)	Henkilöstön kouluttaminen häiriötilanteiden varalle ja harjoitusten järjestäminen	Yhteisen jatkuvuussuunnitelman (joint BCP) kehittäminen toimittajan kanssa	Koulutuksen ja osaamisen kehittämisen vaikuttavuuden mittaaminen	Asiakaskunnan hajauttaminen yksittäisiin asiakkaisiin kohdistuvan riippuvuuden vähentämiseksi
	Toimitilojen vakuutusturvan riittävyden arviointi ja päivittäminen	Peruspalveluhäiriöiden varasuunnitelmien kehittäminen	Ennakoivan kunnossapito-ohjelman kehittäminen (predictive maintenance)	Etätyö- ja joustavien työjärjestelyiden mahdollisuuksien kartoittaminen tuotantotehtäville	Strategisten toimittajien alihankintaketjujen kartoitus (tier 2 ja tier 3)	Osaamisen ennustemallin kehittäminen teknologiamurrosten ja markkinamuutosten varalle	
		Kriittisten tilojen teknisten järjestelmien	Peruspalveluntarjoajien	Laitteiden vakuutusturvan	Henkilöstön selviytymiskyvyn	Yhteisen riskienhallintafoorumin	Strategisen osaamisen riskimallin

Toinen esimerkki koskee kuvitteellista elektroniikka- ja sähköteollisuuden yritystä

Esimerkkiyritys 2: Elektroniikka- ja sähköteollisuus

- Kasvuvaiheessa oleva teknologiayritys, 65 työntekijää
- Valmistaa IoT-antureita ja mittausjärjestelmiä teollisuuden kunnossapitoon
- Liikevaihto 12 M€, kasvu 30% vuodessa
- Oma tuotekehitys Suomessa, valmistus osittain ulkoistettu Aasiaan
- Riippuvainen kriittisistä komponenteista (mikropiirien saatavuus)
- Patentoitua teknologiaa ja merkittävää dataa asiakasprosesseista
- Pilvipalveluihin perustuva SaaS-liiketoimintamalli
- Rahoitus: VC-sijoittajat mukana, seuraava rahoituskierros suunnitteilla

Esimerkkiyritys 2:n kriittisimmät toimintaedellytykset

- Ulkoinen IT-infrastrukturi - AWS-pilvipalvelut SaaS-alustalle
- Data - Asiakkaiden prosessidata ja algoritmit
- Asiantuntijat - R&D-tiimi ja ohjelmistokehittäjät
- Prosessit - IPR ja patentit
- Strategiset toimittajat – Mikropiiritoimittajat
- Kriittiset kumppanit - Teknologiakumppanit (Microsoft, AWS)
- Sijoittajat - VC-rahoitus kasvun mahdollistajana

Toimintasuunnitelma rakentuu näiden toimintaedellytysten ympärille!

Toimenpidesuunnitelmassa painotetaan teknisten järjestelmien, datan ja osaamisen suojaamista

Yritys on hiljattain perustettu, joten suunnitelmassa keskitytään aluksi enimmäkseen perus- ja keskitason toimenpiteisiin.

Elektroniikka- ja sähköteollisuuden esimerkkiyrityksen toimintaedellytykset ja niitä suojelevat toimenpiteet (ESIMERKKI)

	Ulkoinen IT-infrastruktuuri	Data	Asiantuntijat	Prosessit	Strategiset toimittajat	Kriittiset kumppanit	Sijoittajat
	Kaikkien pilvipalveluiden ja ulkoisten IT-palveluntarjoajien dokumentointi	Kriittisten datatyyppien ja -varantojen tunnistaminen ja luokittelu	Kriittisten asiantuntijaroolien tunnistaminen ja dokumentointi	Kriittisten liiketoimintaprosessien tunnistaminen ja dokumentointi	Strategisten toimittajien tunnistaminen ja dokumentointi	Kriittisten kumppanien tunnistaminen ja riippuvuuksien dokumentointi	Keskeisten sijoittajien sekä niiden sitoumusten ja ehtojen tunnistaminen
	Pilvipalveluiden kriittisyyden arviointi ja riippuvuusanalyysin toteuttaminen	Datan vamuuskopiointipolitiikan ja -menettelyiden dokumentointi	Varahenkilöjärjestelmän toteuttaminen avainasiantuntijoille	Prosessien omistajuuden ja vastuuden selkeä määrittely	Strategisten toimittajien vähintään perustason jatkuvuus-suunnitelman varmistaminen	IP-suojan, tietoturvalausekkeiden ja häiriömenettelyiden sisällyttämisen varmistaminen sopimuksissa	Luotettavan talousraportoinnin ja avoimen sijoittajaviestinnän ylläpito
	Palvelutasosopimusten (SLA) saatavuusehtojen ja tietoturvastuuden varmistaminen	Tietosuojalainsäädännön (GDPR) vaatimusten huomiointi datan hallinnassa	Asiantuntijoiden hiljaisen tiedon tallentamisen perusprosessin luominen	Kriittisten prosessien varatoimintatapojen kirjaaminen häiriötilanteiden varalle	Säännölliset yhteistyöpalaverit ja häiriötilanteiden viestintäprotokolla	Kriisitilanteiden viestintäprotokollasta sopiminen	Sijoittajasuhteiden hallintasuunnitelman (IR) kehittäminen häiriötilanteisiin
	Datan sijainnin, omistajuuden ja siirrettävyyden selvittäminen ja dokumentointi	Datan saatavuuden, eheyden ja luottamuksellisuuden perusvaatimusten määrittely	Asiantuntijoiden osaamiskartoitus ja osaamisen hajauttamisen toteuttaminen	Hiljaisen tiedon taltiointiprosessin luominen avainprosesseille	Lakisääteisten, sääntelyyn ja sopimukseen perustuvien vaatimusten tunnistaminen strategisille toimittajasuhteille	Riippuvuusanalyysin tekeminen: kumppanin kokonaan menettämisen seurausten arviointi	Kriisiviestintäsuunnitelman kehittäminen erikseen rahoittajia ja sijoittajia varten
	Pilvipalveluntarjoajien tietoturva-auditoinnin toteuttaminen (SOC 2, ISO 27001 -sertifikaatti)	Datan hallintamallin (data governance) kehittäminen: omistajuus, vastuut, elinkaari	Asiantuntijoiden pysyvyyteen vaikuttavien tekijöiden analysointi ja retention-ohjelman kehittäminen	Prosessien yhtenäistäminen ja toimintaohjeiden kirjaaminen (vakioidut työskentelytavat)	Perusteellisen riippuvuusanalyysin tekeminen	Kumppanikohtaisen jatkuvuussuunnitelman kehittäminen vaihtoehtoisten kumppanien kartoituksella	Maksuvalmiussuunnitelman laatiminen vähintään 3–6 kuukauden kassavirran kattamiseksi ilman uutta rahoitusta
	Exit-suunnitelman kehittäminen pilvipalveluntarjoajan vaihtamista varten	3-2-1-varmuuskopiointisäännön toteuttaminen (3 kopiota, 2 mediaa, 1 off-site)	Ulkoisten asiantuntijaverkostojen ja konsulttisopimusten kehittäminen varakapasiteetiksi	Tiedonhallintajärjestelmän käyttöönotto	Yhteisen jatkuvuussuunnitelman (joint BCP) kehittäminen toimittajan kanssa	Kumppanin tietoturva-auditoinnin toteuttaminen ja kyberriskien arviointi	
	Datan palautustestauksen säännöllinen toteuttaminen ja RTO/RPO-tavoitteiden validointi	Tekoäly- ja automaattoratkaisujen hyödyntäminen asiantuntijatehtävien tukemiseksi ja riippuvuuden	Prosessien haavoittuvuusanalyysin toteuttaminen	Strategisten toimittajien alihankintaketjujen kartoitus (tier 2 ja tier 3)			



Kolmas esimerkki koskee kuvitteellista tietotekniikan alan yritystä

Esimerkkiyritys 3: Tietotekniikka

- Ohjelmistoyritys, 120 työntekijää (90% asiantuntijoita)
- Kehittää teollisuuden digitalisaatoratkaisuja ja data-analytiikkaa
- Liikevaihto 18 M€, yrityksellä ollut nopeaa kasvua
- Toimipisteet Helsingissä, Tampereella ja Oulussa
- Hybridityömalli, 60% henkilöstöstä etätyössä
- Asiakkaina 50+ keskisuurta ja suurta teollisuusyritystä
- Jatkuvan palvelukehityksen malli (DevOps)
- Henkilöstön vaihtuvuus IT-alan keskiarvoa korkeampi (18% vuodessa)

Esimerkkiyritys 3:n kriittisimmät toimintaedellytykset

- Oma IT-infrastrukturi - Kehitysympäristöt ja työkalut
- Ulkoinen IT-infrastrukturi - Pilvipalvelut ja kehitysalustat
- Data - Asiakasdata ja kehitetyt algoritmit
- Asiantuntijat - Korkean osaamisen IT-asiantuntijat
- Johto ja esihenkilöt - Osaava johto kasvun hallintaan
- Prosessit - Ketterät kehitysmenetelmät ja IP
- Osaaminen - Teollisuuden toimialaosaaminen + IT

Toimintasuunnitelma rakentuu näiden toimintaedellytysten ympärille!

Case-esimerkit toimialoittain

Toimenpidesuunnitelmassa painotetaan teknologian, datan ja asiantuntijuuden turvaamista

Yritys on kasvanut nopeasti ja resilienssiin halutaan osoittaa paljon resursseja, joten toimintoihin ohjataan myös kehittyneitä toimenpiteitä.

Tietotekniikan toimialan esimerkkiyrityksen toimintaedellytykset ja niitä suojelevat toimenpiteet (ESIMERKKI)

	Oma IT-infrastruktuuri	Ulkoinen IT-infrastruktuuri	Data	Asiantuntijat	Johto ja esihenkilöt	Prosessit	Osaaminen
1. SUUNNITTELU JA VARAUTUMINEN	IT-omaisuusrekisterin (CMDB) ylläpito kaikista laitteista, ohjelmistoista ja lisenssistä	Kaikkien pilvipalveluiden ja ulkoisten IT-palveluntarjoajien dokumentointi	Kriittisten datatyyppejen ja -varantojen tunnistaminen ja luokittelu	Kriittisten asiantuntijaroolien tunnistaminen ja dokumentointi	Avainjohtajien seuraajien suunnittelu ja varmistaminen	Kriittisten liiketoimintaprosessien tunnistaminen ja dokumentointi	Kriittisten osaamisten tunnistaminen ja osaamiskartan laatiminen
	Kriittisten IT-järjestelmien tunnistaminen ja BIA:n toteuttaminen	Pilvipalveluiden kriittisyyden arviointi ja riippuvuusanalyysin toteuttaminen	Datan varmuuskopiointipolitiikan ja -menettelyiden dokumentointi	Varahenkilöjärjestelmän toteuttaminen avainasiantuntijoille	Johdon roolien ja vastuiden selkeä määrittely kriisitilanteissa	Prosessien omistajuuden ja vastuiden selkeä määrittely	Osaamisvajaiden tunnistaminen suhteessa jatkuvustarpeisiin
	Säännöllisen varmuuskopioinnin varmistaminen ja palautustestauksen suorittaminen	Palvelutasosopimusten (SLA) saatavuusehtojen ja tietoturvakäytännöiden varmistaminen	Tietosuoja- ja tietosuojan (GDPR) vaatimusten huomioiminen datan hallinnassa	Asiantuntijoiden hiljaisen tiedon tallentamisen perusprosessin luominen	Johdon sitouttaminen häiriötilanteisiin varautumiseen	Kriittisten prosessien vara-toimintatapojen kirjaaminen häiriötilanteiden varalle	Koulutussuunnitelman kehittäminen kriittisten osaamisten varmistamiseksi
	Tietoturvan perushallinnan toteuttaminen (palomuurit, virusohjelmistot, päivitykset)	Datan sijainnin, omistajuuden ja siirrettävyyden selvittäminen ja dokumentointi	Datan saatavuuden, eheyden ja luottamuksellisuuden perusvaatimusten määrittely	Asiantuntijoiden osaamiskartoitus ja osaamisen hajauttamisen toteuttaminen	Kriisijohtamiskoulutuksen järjestäminen johdolle ja esihenkilöille	Hiljaisen tiedon taltiointiprosessin luominen avainprosesseille	Osaamisen hajaantumisen varmistaminen
	IT-tilojen fyysisen turvallisuuden varmistaminen (kuluvalvonta, paloturvallisuus, jäähdytys)	Multi-cloud- tai hybrid-strategian kehittäminen toimittajalukon välttämiseksi	Datan hallintamallin (data governance) kehittäminen: omistajuus, vastuut, elinkaari	Asiantuntijoiden pysyvyyteen vaikuttavien tekijöiden analysointi ja retention-ohjelman kehittäminen	Kriisijohtamistimien perustaminen ja toimintamallin dokumentointi	Prosessien riippuvuuskartan kehittäminen	Osaamisriskianalyysin toteuttaminen
	IT disaster recovery -suunnitelman (DRP) kehittäminen ja dokumentointi	Pilvipalveluntarjoajien tietoturva-auditoinnin toteuttaminen (SOC 2, ISO 27001 -sertifikaatti)	3-2-1-varmuuskopiointisääntöjen toteuttaminen (3 kopiota, 2 mediaa, 1 off-site)	Ulkoisten asiantuntijaverkoston ja konsulttisopimusten kehittäminen varakapasiteetiksi	Kriisijohtamisen kypsyysmallin kehittäminen ja säännöllinen arviointi	Prosessien yhtenäistämisen ja toimintaohjeiden kirjaaminen (vakioidut työskentelytavat)	Koulutuksen ja osaamisen kehittämisen vaikuttavuuden mittaaminen
	Kriittisten järjestelmien redundanssin (varajärjestelmien) toteuttaminen	Datan varmuuskopioinnin varmistaminen myös pilvipalveluntarjoajan ulkopuolelle	Datan palautustestauksen säännöllinen toteuttaminen ja RTO/RPO-tavoitteiden validointi	Asiantuntijaosaamisen riskien arviointi: mitkä osaamiset ovat kriittisiä, vaikeasti korvattavia tai harvinaisia markkinoilla	Häiriönsietokykykoulutuksen lisääminen osaksi johdon kehitysohjelmia	Prosessien haavoittuvuusanalyysin toteuttaminen	Osaamisen ennustemallin kehittäminen teknologiamurrosten ja markkinamuutosten varalle
	Kyberturvallisuuden riskiarvioinnin toteuttaminen säännöllisesti	Exit-suunnitelman kehittäminen pilvipalveluntarjoajan vaihtamista varten	Immutable backup -ratkaisun toteuttaminen ransomware-suojausvarmistamiseksi	Tekoäly- ja automaatio-ratkaisujen hyödyntäminen asiantuntija-tehtävien tukemiseksi ja riippuvuuden vähentämiseksi	Johdon harjoitusten järjestäminen päätöksenteon harjoittelemiseksi häiriötilanteissa	Tiedonhallintajärjestelmän käyttöönotto	Jatkuvaan oppimiseen perustuvan organisaatiomallin kehittäminen

Neljäs esimerkki koskee kuvitteellista metallin jalostuksen toimialan yritystä

Esimerkkiyritys 4: Metallin jalostus

- Kaivos- ja rikastustoimintaa harjoittava yritys, joka louhii ja jalostaa metallimalmia rikasteeksi
- Toiminta sisältää avolouhoksen ja maanalaisen kaivoksen sekä samalla alueella toimivan murskaamon ja rikastamon (vaahdotus- ja puristusprosessit). Sijaitsee Suomessa.
- Merkittävä osa tuotannosta menee vientiin. Rikaste kuljetetaan rautatie- ja maantielogistiikalla teollisuusasiakkaille ja satamiin jatkokäsittelyä varten.
- 430 työntekijää (kaivostoiminta, rikastuslaitos, kunnossapito, prosessioperaattorit, asiantuntijat ja johto)
- Liikevaihto 250 M€
- Toimintaan liittyy tiukat ympäristö-, turvallisuus- ja lupapalvelotteet

Esimerkkiyritys 4:n kriittisimmät toimintaedellytykset

- Omat tilat – Kaivosalue ja omat prosessitilat
- Tiloihin liittyvät peruspalvelut – Sähkö, lämpö, vesi
- Tuotantolaitteet - Louhintalaitteet, murskaimet, jauhatusmyllyt, rikastuslaitteet
- Asiantuntijat - Prosessisuunnittelijat, laadunvalvonta, tekniset johtajat
- Tuotantohenkilöstö – Kaivos- ja rikastamo-operaattorit
- Prosessit - Louhinta-, rikastus-, turvallisuus-, ympäristö- ja lupaprosessit
- Suorat hankinnat - Räjähdyksineet, kemikaalit, polttoaineet, varaosat, logistiikkapalvelut

Toimintasuunnitelma rakentuu näiden toimintaedellytysten ympärille!

Case-esimerkit toimialoittain

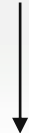
Toimenpidesuunnitelmassa korostetaan teollisen tuotannon fyysisten edellytysten, laitteiden ja kriittisen henkilöstön suojaamista

Yritys yhdistää perus- ja keskitason toimenpiteitä, ja lisää toimintoihin myös edistyksellisiä toimenpiteitä, sillä yrityksellä on paljon resursseja ja toimialan riskitaso on suhteellisen korkea

Metallin jalostuksen toimialan esimerkkiyrityksen toimintaedellytykset ja niitä suojelevat toimenpiteet (ESIMERKKI)

Omat tilat	Tiloihin liittyvät peruspalvelut	Tuotantolaitteet	Asiantuntijat	Tuotantohenkilöstö	Prosessit	Suorat hankinnat
Toimitilojen rekisterin ylläpito	Kriittisten peruspalvelujen (esim. sähkö) riippuvuuksien tunnistaminen ja dokumentointi	Kaikkien tuotantolaitteiden rekisterin ylläpito	Kriittisten asiantuntijaroolien tunnistaminen ja dokumentointi	Kriittisten tuotantoroolien ja avainhenkilöiden tunnistaminen	Kriittisten liiketoimintaprosessien tunnistaminen ja dokumentointi	Ajantasaisen listan ylläpito kaikista suorista toimittajista ja hankintasopimuksista
Kriittisten toimitilojen tunnistaminen ja BIA:n toteuttaminen	Peruspalvelujen toimittajien ja sopimusten dokumentointi	Kriittisten laitteiden tunnistaminen ja niiden palautumisajan ja maksimikeskeytysajan arviointi	Varahenkilöjärjestelmän toteuttaminen avainasiantuntijoille	Varahenkilöjärjestelmän toteuttaminen kriittisiin tuotantotehtäviin	Prosessien omistajuuden ja vastuiden selkeä määrittely	Kriittisimpien raaka-aineiden ja niiden korvaavuuksien tunnistaminen
Toimitilojen fyysisen turvallisuuden varmistaminen	Varavoimaratkaisujen perustason varmistaminen	Huolto- ja kunnossapito-ohjelman ylläpito kriittisille laitteille	Asiantuntijoiden hiljaisen tiedon tallentamisen perusprosessin luominen	Työterveys- ja turvallisuusohjelman ylläpito	Kriittisten prosessien vara toimintatapojen kirjaaminen häiriötilanteiden varalle	Force majeure -ehtojen ja toimitushäiriölausekkeiden varmistaminen hankintasopimuksissa
Toimitilojen pelastussuunnitelman laatiminen ja ylläpito	BIA:n (toiminnan keskeytymisen vaikutusten arviointi) toteuttaminen peruspalvelujen katkon vaikutusten arvioimiseksi	Varaosien saatavuuden varmistaminen kriittisille laitteille	Asiantuntijoiden osaamiskartoitus ja osaamisen hajauttamisen toteuttaminen	Moniosaajuusohjelman (cross-training) kehittäminen tuotantohenkilöstölle	Hiljaisen tiedon tallentamisprosessin luominen avainprosesseille	Lakisääteisten ja sääntelyvaatimusten tunnistaminen ja dokumentointi hankintaketjulle
Toimitilojen riskiarvioinnin toteuttaminen	Varmistetaan kriittisiin tiloihin varayhteydet ja varasyöttö (esim. kahdennettu sähkönsyöttö)	Varalaitteiston ja varakapasiteetin kartoittaminen (oma, vuokra, kolmas osapuoli)	Asiantuntijoiden pysyvyyteen vaikuttavien tekijöiden analysointi ja retention-ohjelman kehittäminen	Työvoiman saatavuusriskianalyysin toteuttaminen	Prosessien riippuvuuskartan kehittäminen	Liiketoiminnan vaikutusanalyysin (BIA) toteuttaminen suorien hankintojen osalta
Toimitilojen vakuutusturvan riittävyys arviointi ja päivittäminen	Varavoimakapasiteetin riittävyys arviointi suhteessa kriittisten toimintojen tarpeeseen	Laittekohtaisen riskiarvioinnin toteuttaminen	Ulkoisten asiantuntijaverkoston ja konsulttisopimusten kehittäminen varakapasiteetiksi	Henkilöstön kouluttaminen häiriötilanteiden varalle ja harjoitusten järjestäminen	Prosessien yhtenäistämisen ja toimintaohjeiden kirjaaminen (vakioidut työskentelytavat)	Vaihtoehtoisten toimittajien rekisterin kehittäminen
Kriittisten tilojen teknisten järjestelmien (HVAC, sprinklerit, generaattorit) kunnossapito-ohjelman ylläpito	Peruspalveluhäiriöiden varasuunnitelmien kehittäminen	Ennakoivan kunnossapito-ohjelman kehittäminen (predictive maintenance)	Asiantuntijaosaamisen riskien arviointi: mitkä osaamiset ovat kriittisiä, vaikeasti korvattavia tai harvinaisia markkinoilla	Henkilöstön selviytymiskyvyn arviointi erilaisissa häiriötilanteissa	Tiedonhallintajärjestelmän käyttöönotto	Säännöllisen toimittajariskianalyysin toteuttaminen
Toimitilojen ilmastoriskien (tulvat, helleaallot, myrskyt) pitkän aikavälin arviointi ja sopeutumissuunnitelma	Peruspalveluntarjoajien jatkuvuusvalmiuden arviointi	Laitteiden vakuutusturvan riittävyys arviointi ja päivittäminen	Tekoäly- ja automaatio-ohjelmien hyödyntäminen asiantuntijatehtävien tukemiseksi ja riippuvuuden vähentämiseksi	Automaatio- ja robotisaatioinvestointien arviointi kriittisten tehtävien henkilöriippuvuuden	Prosessien haavoittuvuusanalyysin toteuttaminen	Varastointitasoista ja puskurivarastojen ylläpidosta sopiminen ennakkoon

1. SUUNNITTELU JA VARAUTUMINEN



Viides esimerkki koskee kuvitteellista suunnittelu- ja konsultointialan yritystä

Esimerkkiyritys 5: Konsultointi

- Monialainen suunnittelu- ja asiantuntijayritys
- 85 työntekijää, joista valtaosa asiantuntijoita (insinöörit, arkkitehdit, projektipäälliköt)
- Palvelut: prosessi- ja tehdassuunnittelu, projektijohtaminen, investointiselvitykset, ympäristökonsultointi
- Liikevaihto 12 M€, tasainen kasvu viime vuosina
- Toimipiste Helsingissä, projektit ympäri Suomea
- Toimintamalli projektivetoista; samanaikaisesti 20–30 käynnissä olevaa projektia
- Korkea riippuvuus asiantuntijoiden osaamisesta ja projektien sujuvasta läpiviennistä
- Runsas määrä projektikohtaista dataa ja dokumentaatiota eri asiakasjärjestelmissä

Esimerkkiyritys 5:n kriittisimmät toimintaedellytykset

- Oma IT-infrastrukturi – projektityökalut, palvelimet
- Ulkoinen IT-infrastrukturi – pilvipalvelut, dokumenttialustat
- Data – projektidata: suunnitelmat, dokumentaatio, laskelmat, asiakastiedot
- Asiantuntijat – suunnittelijat, projektipäälliköt
- Tukitoiminnot – laadunhallinta, tietohallinto jne.
- Prosessit – hiljainen ja tallennettu tieto, projektien prosessit
- Osaaminen – toimialakohtainen ja tekninen erityisosaaminen

Toimintasuunnitelma rakentuu näiden toimintaedellytysten ympärille!

Case-esimerkit toimialoittain

Toimenpidesuunnitelmassa korostetaan IT-ympäristön sekä projektitiedon ja asiantuntijoiden turvaamista

Yritys haluaa kohdentaa resurssejaan aluksi strategisesti. Näin ollen yhdistetään perus- ja keskitason toimenpiteitä, ja kaikista kriittisimpiin toimintoihin suunnitellaan myös vaativampia toimenpiteitä.

Suunnittelu- ja konsultointialan esimerkkiyrityksen toimintaedellytykset ja niitä suojelevat toimenpiteet (ESIMERKKI)

	Oma IT-infrastruktuuri	Ulkoinen IT-infrastruktuuri	Data	Asiantuntijat	Tukitoiminnot	Prosessit	Osaaminen
1. SUUNNITTELU JA VARAUTUMINEN ↓	IT-omaisuusrekisterin (CMDB) ylläpito kaikista laitteista, ohjelmistoista ja lisenssistä	Kaikkien pilvipalveluiden ja ulkoisten IT-palveluntarjoajien dokumentointi	Kriittisten datatyyppejen ja -varantojen tunnistaminen ja luokittelu	Kriittisten asiantuntijaroolien tunnistaminen ja dokumentointi	Tukitoimintojen (HR, talous, viestintä, lakiasiat) kriittisyyden arviointi	Kriittisten liiketoimintaprosessien tunnistaminen ja dokumentointi	Kriittisten osaamisten tunnistaminen ja osaamiskartan laatiminen
	Kriittisten IT-järjestelmien tunnistaminen ja BIA:n toteuttaminen	Pilvipalveluiden kriittisyyden arviointi ja riippuvuusanalyysin toteuttaminen	Datan varmuuskopiointipolitiikan ja -menettelyiden dokumentointi	Varahenkilöjärjestelmän toteuttaminen avainasiantuntijoille	Varahenkilöjärjestelmän toteuttaminen kriittisiin tukitoimintorooleihin	Prosessien omistajuuden ja vastuuden selkeä määrittely	Osaamisvajeiden tunnistaminen suhteessa jatkuvuustarpeisiin
	Säännöllisen varmuuskopioinnin varmistaminen ja palautustestauksen suorittaminen	Palvelutasosopimusten (SLA) saatavuusehtojen ja tietoturvavastuuden varmistaminen	Tietosuoja-lainsäädännön (GDPR) vaatimusten huomioiminen datan hallinnassa	Asiantuntijoiden hiljaisen tiedon tallentamisen perusprosessin luominen	Tukitoimintojen jatkuvuussuunnitelmien kehittäminen	Kriittisten prosessien vara-toimintatapojen kirjaaminen häiriötilanteiden varalle	Koulutussuunnitelman kehittäminen kriittisten osaamisten varmistamiseksi
	Tietoturvan perushallinnan toteuttaminen (palomuurit, virusohjelmistot, päivitykset)	Datan sijainnin, omistajuuden ja siirrettävyyden selvittäminen ja dokumentointi	Datan saatavuuden, eheyden ja luottamuksellisuuden perusvaatimusten määrittely	Asiantuntijoiden osaamiskartoitus ja osaamisen hajauttamisen toteuttaminen	Tukitoimintojen etätöyvalmiuden varmistaminen	Hiljaisen tiedon tallentamisprosessin luominen avainprosesseille	Osaamisen haja utuksen varmistaminen
	IT-tilojen fyysisen turvallisuuden varmistaminen (kulunvalvonta, paloturvallisuus, jäähdytys)	Multi-cloud- tai hybrid-strategian kehittäminen toimittajalukon välttämiseksi	Datan hallintamallin (data governance) kehittäminen: omistajuus, vastuut, elinkaari	Asiantuntijoiden pysyvyyteen vaikuttavien tekijöiden analysointi ja retention-ohjelman kehittäminen	Tukitoimintojen keskinäisten riippuvuuksien kartoittaminen	Prosessien riippuvuuskartan kehittäminen (prosessien väliset syötöt ja tuotokset)	Osaamisriskianalyysin toteuttaminen
	IT disaster recovery -suunnitelman (DRP) kehittäminen ja dokumentointi	Pilvipalveluntarjoajien tietoturva-auditoinnin toteuttaminen (SOC 2, ISO 27001 -sertifikaatti)	3-2-1-varmuuskopiointisäännön toteuttaminen (3 kopiota, 2 mediaa, 1 off-site)	Ulkoinen asiantuntija verkostojen ja konsulttisopimusten kehittäminen varakapasiteetiksi	Tukitoimintojen palveluiden ulkoistamisvaihtoehtojen kartoittaminen varakapasiteetiksi	Prosessien yhtenäistämisen ja toimintaohjeiden kirjaaminen (vakioidut työskentelytavat)	Koulutuksen ja osaamisen kehittämisen vaikuttavuuden mittaaminen
	Kriittisten järjestelmien redundanssin (varajärjestelmien) toteuttaminen	Exit-suunnitelman kehittäminen pilvipalveluntarjoajan vaihtamista varten	Datan palautustestauksen säännöllinen toteuttaminen ja RTO/RPO-tavoitteiden validointi	Asiantuntijaosaamisen riskien arviointi: mitkä osaamiset ovat kriittisiä, vaikeasti korvattavia tai harvinaisia markkinoilla		Prosessien haavoittuvuusanalyysin toteuttaminen	Jatkuvaan oppimiseen perustuvan organisaatiomallin kehittäminen
	Kyberturvallisuuden riskiarvioinnin toteuttaminen säännöllisesti	Kyberturvallisuuden riskiarvioinnin toteuttaminen säännöllisesti	Tietojen salauksen käyttöön otto levossa ja siirrossa olevalle datalle	Tekoäly- ja automaatio ratkaisujen hyödyntäminen asiantuntija-tehtävien tukemiseksi ja riippuvuuden vähentämiseksi		Tiedonhallintajärjestelmän käyttöönotto	Osaamisen ennustemallin kehittäminen teknologiamurrosten ja markkinamuutosten varalle

Transforming
society
together