Jatkuvuudenhallinta ja varautuminen

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

TURKU AMK

Euroopan unionin rahoittama

NextGenerationEU

Rahoittaja

Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Tavoitteet

Opintojakson suoritettuaan opiskelija

- Ymmärtää jatkuvuudenhallinnan merkityksen ja osaa tunnistaa sen roolin organisaation kokonaisvaltaisessa riskienhallinnassa ja liiketoiminnan varmistamisessa.
- Ymmärtää ISO 22301 –standardin keskeiset käsitteet liiketoiminnan jatkuvuuden hallintajärjestelmän suunnittelussa, toteutuksessa ja ylläpidossa.
- Tuntee ISO 31000 -standardin periaatteet ja ymmärtää riskienhallintaprosessit osana jatkuvuudenhallintaa.
- Osaa suunnitella ja toteuttaa ICT-järjestelmien jatkuvuudenhallintaa koskevia toimenpiteitä.
- Osaa kehittää ja dokumentoida jatkuvuussuunnitelmia
- Osaa laatia, toteuttaa ja testata jatkuvuussuunnitelmia varmistamaan organisaation toiminnan häiriöttömyyden ja palautumiskyvyn erilaisissa kriisitilanteissa.
- Tuntee parhaat käytännöt jatkuvuudenhallinnan koulutusten ja harjoitusten suunnittelussa ja toteutuksessa sekä osaa arvioida ja parantaa organisaation jatkuvuusvalmiuksia.

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Arviointi

- Palautetut tehtävät arvioidaan asteikolla 0-5
- Arvosana on tehtäväpalautusten keskiarvo
- Kaikki tehtävät palautetaan
- (Lähipäivien poissaolosta korvaava tehtävä)

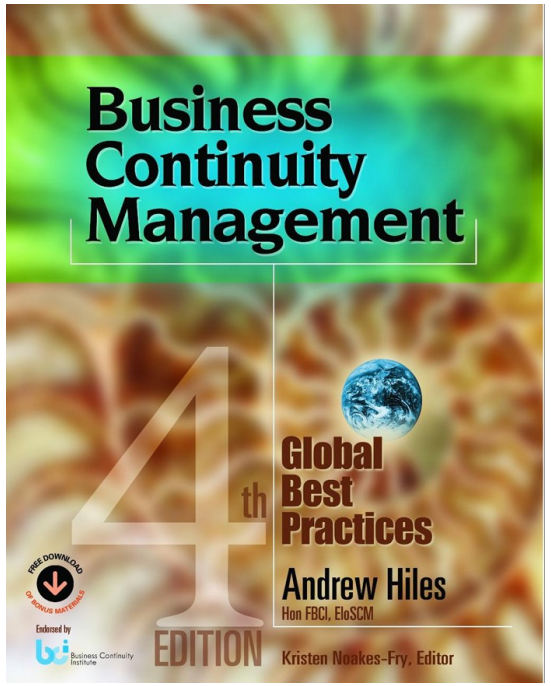
Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kuttuuriministeriö sekä työ- ja elinkeinoministeriö.

TURKU AMK

Kurssin materiaalit



Lähipäivä 1

- Jatkuvuudenhallinta ja varautuminen keskeiset perusteet, standardit ja viitekehykset

TURKU AMK

Kuukauden tunnuslukuja

CrowdStriken yksittäinen päivitys aiheutti merkittäviä käyttökatkoja ympäri maailmaa, mutta Suomessa kriittiset vaikutukset jäivät vähäisiksi.

JetBrains TeamCity -tuotteen haavoittuvuutta hyväksikäytettiin 22 minuuttia haavoittuvuuden hyväksikäyttömenetelmän julkaisun jälkeen. Tieto käy ilmi Cloudflaren tuottamasta raportista.[1]

Tietomurrosta aiheutuvat kustannukset ovat matalammat viranomaisten osallistuessa tietomurron selvittämiseen. Viranomaisten ollessa mukana tietomurron selvityksessä kustannus oli keskimäärin 4 miljoonaa euroa, kun ilman viranomaisten apua tietomurrosta kertyi yrityksille kustannuksia noin 5 miljoonaa euroa.[2]

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2.

Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.

3.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

Symbolit

Uusi

Päivitetty

4.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

5.

Tietoliikenneinfran suojaamisen tärkeys korostuu

Tietoliikenne- ja tietojärjestelmäinfran suojaaminen maailmalla ja kotimaassa on tärkeää, sekä siihen kohdistuvien vahinkojen ja luonnonilmiöiden että ulkopuolisten aiheuttamien tahallisten häiriöiden takia.

Varautuminen on strateginen päätös

KESKEINEN TERMISTÖ

1. BCP (Business Continuity Planning): prosessi, jossa organisaatio varmistaa, että sen liiketoiminta toiminta jatkuu häiriöttä erilaisissa häiriötilanteissa.
2. DRP (Disaster Recovery Planning): prosessi, joka keskittyy palauttamaan organisaation toiminnot mahdollisimman nopeasti normaaliksi, kun häiriö on jo tapahtunut.
3. RTO (Recovery Time Objective): aika, jonka organisaatio tarvitsee palauttaakseen toimintansa normaaliksi häiriön jälkeen.
4. RPO (Recovery Point Objective): aika, joka määrittää sen, kuinka kauan organisaation on siedettävä menetettyjä tietoja tai toimintaa, kunnes normaali toiminta voidaan palauttaa.
5. BCMS (Business Continuity Management System): jatkuvuussuunnittelun kokonaisvaltainen lähestymistapa, joka koostuu prosessista, menetelmistä ja työkaluista, joilla organisaatio varmistaa jatkuvuuden.
6. BIA (Business Impact Analysis): prosessi, joka tunnistaa ja arvioi organisaation toiminnan kannalta kriittiset prosessit ja resurssit.
7. HPR (High Priority Risks): riskejä, jotka ovat organisaation kannalta kaikkein merkittävimpiä ja joita varten on tärkeää kehittää kattavat jatkuvuussuunnitelmat.
8. BCMT (Business Continuity Management Team): organisaation sisäinen ryhmä, joka vastaa jatkuvuussuunnittelusta ja sen toteuttamisesta.
9. MTTR (Mean Time to Recovery): aikaa, jonka organisaatio tarvitsee keskimäärin toimintansa palauttamiseen häiriön jälkeen.
10. MTBF (Mean Time Between Failures): keskimääräinen häiriöiden välinen aika.

https://www.itgovernance.co.uk/files/BCIGlossary.pdf → 29 sivua termistöä

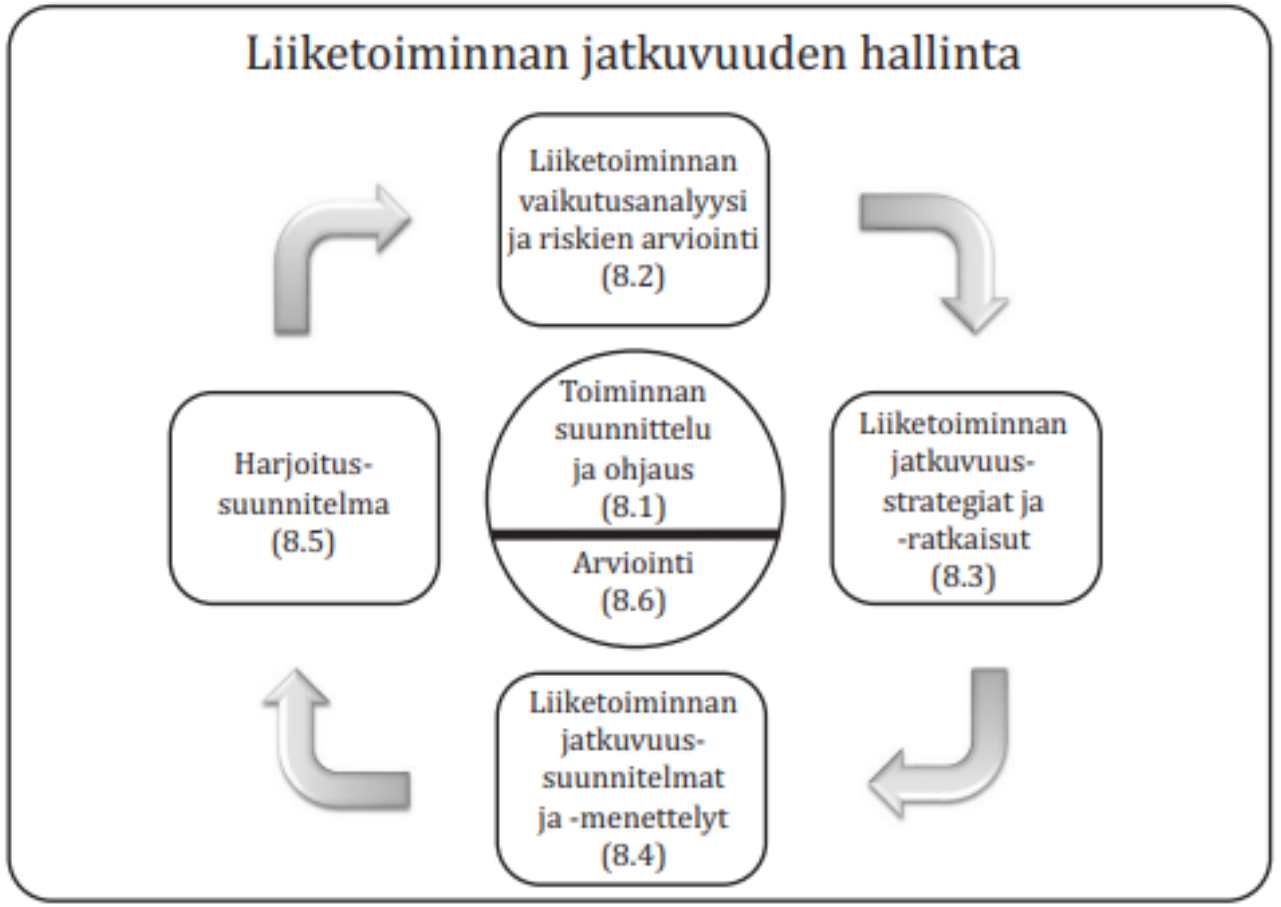
TURKU AMK

Tunnetuimmat standardit

1. **ISO 22301:2019** Kansainvälinen standardi, joka sisältää suositukset liittyen jatkuvuuden hallintaan. Standardi kattaa kaikenlaiset organisaatiot, mukaan lukien julkinen sektori, yksityinen sektori ja voittoa tavoittelemattomat organisaatiot.
2. **SFS-EN ISO 22313:2020** Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. **Ohjeistusta standardin ISO 22301 käyttöön**
3. **ISO/TS 22317:2021** Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Ohjeita liiketoiminnan vaikutusanalyysiin
4. **NIST SP 800-34**: Yhdysvaltalainen standardi, joka antaa ohjeita tietotekniikan jatkuvuussuunnittelusta. Standardi tarjoaa yksityiskohtaiset ohjeet jatkuvuussuunnittelun prosessista ja sen toteuttamisesta.

Liiketoiminnan jatkuvuus

- Yrityksen toiminnan turvaaminen
- Ennakoivat toimenpiteet (varautuminen)
  - Toimintavaikutusarviot
  - Harjoittelu
- Toiminnan palauttaminen hyväksytylle tasolle
- LL



Lähde: ISO 22313:2020, kuva 5.

Kuva 1 Liiketoiminnan jatkuvuuden hallinnan osat

ISO 22301

https://advisera.com/27001academy/knowledgebase/business-continuity-plan-how-to-structure-it-according-to-iso-22301/

Miksi jatkuvuussuunnittelua tehdään?

Varmistetaan liiketoiminnan jatkuvuus:

Toiminta voi keskeytyä omaan tai yhteistyökumppanin toimintaan, tietojärjestelmiin, omaisuuteen tai henkilöstöön kohdistuvien vahinkojen ja häiriötilanteiden vuoksi.

Varaudutaan:

- Odottamattomiin ja suunnittelemattomiin (tietojärjestelmien) häiriöihin
- Tietoturvaloukkauksiin (tietovuoto, tietovarkaus)
- Verkkohyökkäyksiin (haittaohjelmat, palvelunestohyökkäykset)
- Äkillisiin resurssiongelmiin
- Toiminnan jatkamiseen tiedon ja/tai tietojärjestelmän menetyksen jälkeen

Dilbert

Euroopan unionin rahoittama NextGenerationEU
Rahoittaja Jatkuvan oppimisen ja työllisyyden palvelukeskus
TURKU AMK
Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopeasti toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Yleistä jatkuvuussuunnittelusta

- Jatkuvuussuunnittelu on varautumisen prosessi (ICT-varautuminen), joka sisältää:
    - Johdon määrittämät tavoitteet ja vastuut
    - Priorisoinnin
    - Resursoinnin
    - Toimintavaikutusarvioinnin; toimintaympäristön kuvaus (tekninen ja toiminnallinen) ja riski- ja uhka-analyysi
    - Toipumissuunnitelmat
    - Palautussuunnitelmat
    - Sopimukset (SLA:t)
    - Dokumentoinnin
    - Testaamisen ja harjoittelun
    - Yhteistyöfoorumit

Jatkuvuussuunnitelma on häiriötilanteiden johtamisen ja riskienhallinnan työkalu

Teknisiä ratkaisuja tärkeämpää ovat ihmiset ja johtaminen – tekniikkaa on helpompi rakentaa kun ihmiset ovat mukana

Tavoite

- Rakentaa organisaatioon toiminnan jatkuvuutta tukeva **kulttuuri ja yhteistoimintamallit**
- Tunnistaa organisaation toimintaa uhkaavat tekijät ja niiden **seuraukset**
- Tunnistaa ja kirjata toimet, jotka pienentävät toimintaa haittaavien tapahtumien **vaikutusta ja kestoa**
- Luoda perusta toipumiskyvylle ja tehokkaille vastatoimenpiteille **toimintojen turvaamiseksi**
- Varautua ennalta toimintaa uhkaaviin häiriöihin ja **harjoitella** niiden varalta → lyhentävät häiriöiden kestoa ja minimoivat menetetyn tiedon määrää.
- Tuottaa kyky **jatkaa toimintaa** häiriöstä huolimatta mahdollisin pienin menetyksin
- Antaa käsitys toipumis- ja palautumistilanteessa tarvittavista **resursseista**
- Tavoitteena, että It-palvelut toimivat ja ovat sitä, mitä liiketoiminta odottaa ja mitä on sovittu

TURKU AMK

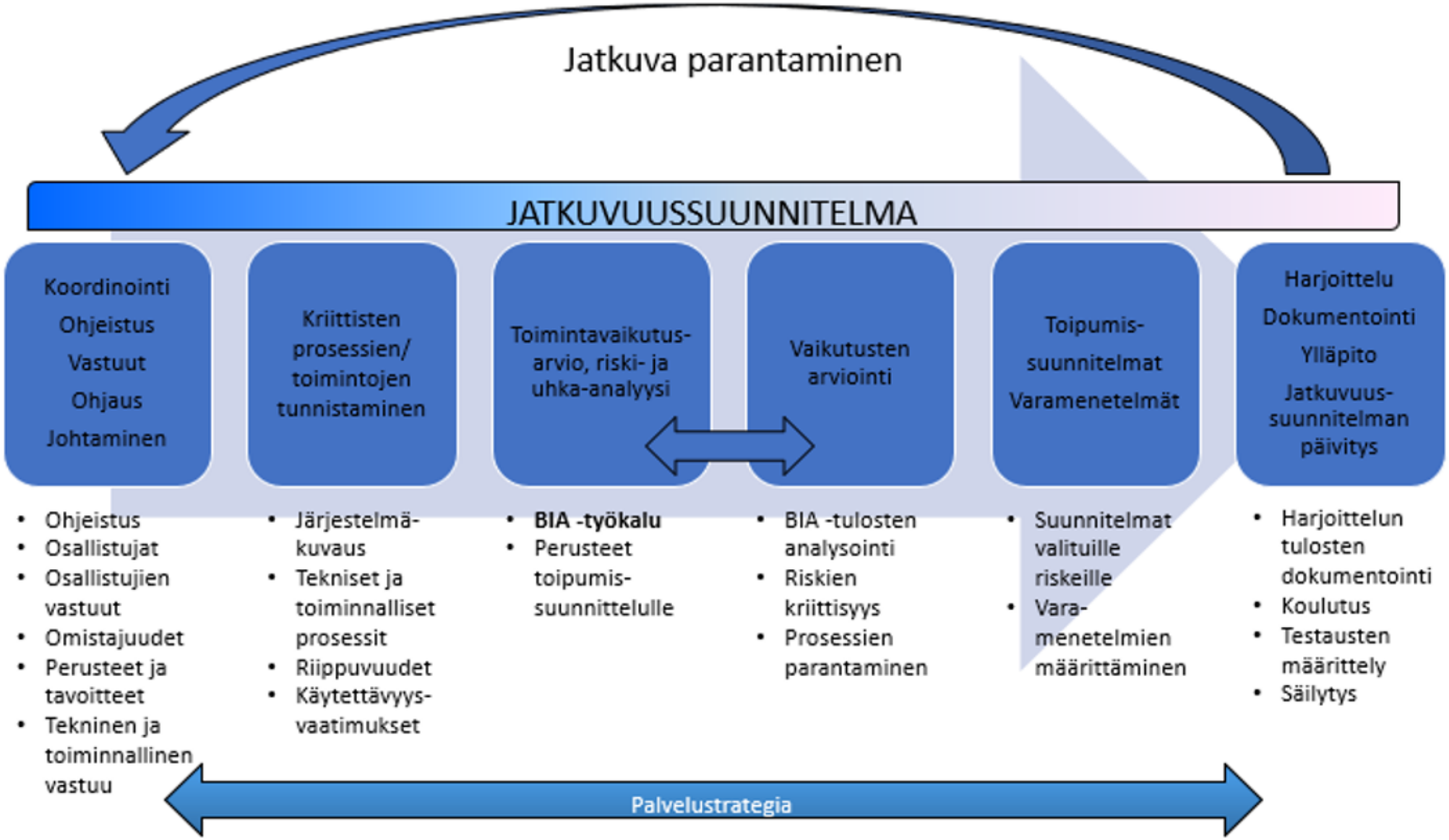
Hyödyt

- Kattava käsitys järjestelmän/toiminnan/palvelun/prosessin **tärkeydestä ja ydintehtävistä → priorisointi ja kriittisyys**
- Tunnistetaan **omistajuudet** sekä tekninen ja toiminnallinen vastuu
- Tunnistetaan kriittiset prosessit ja niiden **riippuvuudet (myös ulkoiset)**
- Tunnistetaan järjestelmään/toimintaan/palveluun/prosessiin kohdistuvat **käytettävyysvaatimukset yhteistyössä liiketoiminnan ja IT:n kanssa**
- Määritellään häiriötilanteen aikainen **viestintä**
- Määritellään **toipumisvaatimukset ja varamenettelyt**
- Määritellään **palautumismekanismit**
- **Kriisitilanteen johtamisen mahdollistaminen**

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Jatkuvuussuunnittelun prosessi



kuva Pia Satopää mukaillen Iivari Laaksonen: Jatkuvuussuunnittelujja ICT -varautuminen

TURKU AMK

Toimintavaikutusarvio ja toipumissuunnittelu

Toimintavaikutusarvio
(BIA = Business Impact Analysis)

- Kansainvälisesti tunnettu prosessi liiketoiminnan (prosessien/toiminnallisuuksien) häiriötilanteiden tunnistamiseen, priorisointiin ja vaikutusten arviointiin
- Toimintavaikutusarvion (BIA) on tarkoitus tuottaa **perusteet toipumissuunnittelulle**
- Toimintavaikutusarvio antaa järjestelmän, prosessin, suorituskyvyn **käytettävyysvaatimukset** ylläpidolle
- Toimintavaikutusarvion tulos kertoo **riskitason** ilman suojaamistoimenpiteitä
- Lopputuotteena **riskiarvio**, **toipumissuunnitelma** ja **varamenetelmän kuvaus**

Toimintavaikutusarvion (BIA) tarkoitus

ON ANTAA KÄSITYS:

- Järjestelmän merkityksestä ja vaikutuksesta
- Järjestelmän rakenteesta ja vastuista
- Järjestelmän riippuvuuksista
- Minkälaisia riskejä järjestelmään kohdistuu ja mikä niiden vaikutus toteutuessaan on
- Minkälaisia käytettävyysvaatimuksia järjestelmään kohdistuu

TEHDÄÄN VUOSITTAIN

PERUSTEET TOIPUMISSUUNNITELMILLE

TURKU AMK

Elements of business impact analysis

	Fire in data center	Loss of specialized staff	Vehicle crash in front entrance of office building	Vandalism to primary product assembly line	Loss of staff due to COVID-19 illness
BUSINESS ACTIVITY AFFECTED	All activities in data center	Activities that require specialized staff	All activities at that location unless an alternate access option is available	Loss of primary production line	Loss of possibly key employees needed to run the business
POTENTIAL OPERATIONAL LOSS	Inability to function normally	Reduced ability to function normally	Nominal disruption based on how quickly the vehicle can be removed and the front entrance reopened	Inability to produce the company's primary product	May be nominal to significant depending on who is affected
POTENTIAL FINANCIAL LOSS	$3,000 to $4,000 revenue loss per hour	None, assuming backup staff is available	None, assuming alternate entrance is available and access to building facilities is available	$25,000 to $40,000 per hour in lost revenue	Could be minimal assuming employees can work remotely
MINIMUM TIME NEEDED TO RECOVER OPERATIONS	Three to four hours	One to two hours	Depending on the damage from the crash, up to one day	Days if a work-around can be built; weeks if an alternate production facility must be found and launched	24-48 hours depending on health status and if employees can work remotely
					

SOURCE: PAUL KIRVAN; ICONS: JUSTINROQUE, ANTTOHOHO, APPLEUZR/GETTY IMAGES

TURKU AMK

BIA

(Business Impact Analyse)

HUOMIOI

- Myös liitännäiset palvelut/palveluntuottajat otetaan huomioon
- Palveluverkoston riskiarviointi
- Toimittajaverkoston auditoinnit/haastattelut

Toipumissuunnitelma

- On usein jatkuvuussuunnitelman liite

  → yhdellä järjestelmällä voi olla monta toipumissuunnitelmaa

- Konkreettinen ja yksityiskohtainen kirjallinen ohje niistä toimenpiteistä, joilla ongelma- ja epäkäytettävyystilanteista siirrytään joko varamenetelmään tai takaisin normaaliin toimintaan
- Perustuu uhka- ja riskianalyysiin (BIA)
- Sisältää kattavan yhteystietoluettelon ja tiedot, kenen vastuulla toipumisen käynnistäminen kunkin kohdeympäristön/prosessin/toiminnallisuuden osalta on
- Sisältää kuvauksen viestinnästä toipumisen aikana
- **Sisältää järjestelmän teknisen kuvauksen sillä tarkkuudella, että kohdejärjestelmä/toiminnallisuus/prosessi voidaan rakentaa uudelleen.**

Palautumissuunnitelma

Määritellään:

- Missä järjestyksessä toiminnallisuudet palautetaan
- Miten (ja kuka) häiriötilanteen aikana kertyneet tiedot palautetaan järjestelmään
- Miten palautumisesta viestitään toiminnallisuuksien välillä

Euroopan unionin rahoittama NextGenerationEU
Rahoittaja Jatkuvan oppimisen ja työllisyyden palvelukeskus

Harjoittelu

- 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

Kokemukset 1/2

- Sisältää paljon kartoitus- ja selvitystyötä ennen kuin pääsee varsinaiseen jatkuvuussuunnitteluun
    - Tietoa paljon hajallaan eri tahoilla (arkkitehtuuri, tekninen alusta, tietokannat)
    - Monta toimijaa ja riippuvuutta (sisäiset, ulkoiset)
    - Työkalujen opettelua
- Vaatii tiukkaa priorisointia
    - Jokaisen toiminnallisuuden omistaja pitää omaansa tärkeimpänä
- Vaatimusten/käytettävyysvaatimusten saaminen ja yhdistäminen hankalaa → monta toimijaa → liiketoiminnan käytettävyysvaatimukset eivät aina ole realistisia
- Kun aloitat, kokoa vastuuhenkilöt yhden pöydän ääreen:
    - järjestelmän tekniset ja toiminnalliset omistajat
    - sovellusvastaavat
    - prosessivastaavat
    - järjestelmävastaavat…

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Kokemukset 2/2

- Prosessi antaa hyvän kokonaiskuvan toiminnallisuudesta ja sen osista (järjestelmästä)
- Prosessi toimii ja vaikutuksia on hyvä arvioida vuosittain tai aina kun "jotain sattuu"
- → ymmärretään vaikutukset ja se, ettei kaikkeen voi varautua → “Nothing works” –skenaarion pohdinta
- → menetyksiä voi minimoida ennalta sovituilla ja harjoitelluilla menettelyillä
- Sopimukset
- → sopimukset päivitetään vastaamaan käytettävyysvaatimuksia /realistista toipumiskykyä
- Varmistuksia otetaan useammin tietomenetysten minimoimiseksi
- → Huomioi varmistusten säilytys ja käytettävyys

Materiaalia

- https://dynamics.folio3.com/blog/business-continuity/
- https://www.techtarget.com/searchstorage/definition/business-impact-analysis
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
- https://jyx.jyu.fi/bitstream/handle/123456789/69909/URN%3aNBN%3afi%3ajyu-202006124154.pdf?sequence=1&isAllowed=y
- https://vm.fi/documents/10623/307669/ICT-varautumisen+vaatimukset/9fa21bee-efcc-485a-8677-4eb4e0a2fa1f/ICT-varautumisen+vaatimukset.pdf
- FINNA E-kirja: **A Risk Management Approach to Business Continuity : Aligning Business Continuity and Corporate Governance**: Julia Graham and David Kaye
- FINNA E-kirja: **Business Continuity Management : Global Best Practices**; Andrew Hiles and Kristen Noakes-Fry
- FINNA E-kirja: **Validating Your Business Continuity Plan : Ensuring Your BCP Actually Works**, Robert Clark
- **Introduction to Business Continuity Planning:** https://www.sans.org/white-papers/559/
- https://teknologiateollisuus.fi/sites/default/files/inline-files/T-Varautuminen-ja-liiketoiminnan-jatkuvuus_0.pdf
- https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta
- FINNA: SFS-EN ISO 22313:2020 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät.
- https://dvv.fi/documents/16079645/110183105/Kriittisten+kohteiden+luokittelu.pdf/4a8e7aae-40d1-2d1a-52eb-bb41a546cea0/Kriittisten+kohteiden+luokittelu.pdf?t=1647262290920