Jatkuvuuden hallintajärjestelmän kehitys case-organisaatiolle

Jesse Rissanen

Opinnäytetyö, AMK
Marraskuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Rissanen, Jesse

Jatkuvuuden hallintajärjestelmän kehitys case-organisaatiolle

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2022, 98 sivua

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikka. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Liiketoiminnan jatkuvuuden hallintajärjestelmän avulla organisaatio pystyy tehokkaasti suunnittelemaan, harjoittelemaan sekä harjoittelemaan menettelyjä, joiden avulla organisaation toimintakyky varmistetaan kyvykkyyksillä palautua ja toipua erilaisista häiriötilanteista.

Opinnäytetyö toteutettiin yhteistyössä case-organisaation kanssa. Organisaatio halusi pysyä nimettömänä ja siksi organisaatiota ei esitellä tarkemmin, eikä myöskään kuvailla sen kokoa tarkemmin. Toimeksiantaja-organisaatio toimii tieto- ja viestintätekniikan alalla.

Opinnäytetyön tavoitteena oli kehittää jatkuvuuden hallintajärjestelmä toimeksiantajan liiketoiminnan tukemiseksi liiketoiminnan jatkuvuuden hallintajärjestelmälle vaatimuksia asettavan standardin ISO 22301:2019 mukaisesti ja pohjaksi opinnäytetyön ulkopuolella toteutettavan hallintajärjestelmän sertifioinnin mahdollistamiseksi.

ISO 22301-standardin mukaisella liiketoiminnan jatkuvuuden hallintajärjestelmällä varmistetaan häiriötilanteilta suojautuminen, häiriöiden esiintymisen todennäköisyyden pienentäminen, häiriöihin varautuminen ja reagoiminen sekä häiriöistä palautuminen. Standardin vaatimukset ovat yleisiä ja ne soveltuvat kaikille organisaatioille niiden koosta tai toimialueesta riippumatta.

Kehitystyö jaettiin kolmeen osaan: case-organisaation liiketoiminnan jatkuvuudenhallinnan tavoitetilan määrittely, jatkuvuuden hallinnan lähtötilanteen kartoitus ja puutteiden arviointi sekä liiketoiminnan jatkuvuuden hallintajärjestelmän rungon rakentaminen, joka toimii pohjana jatkokehitykselle.

Opinnäytetyö toteutettiin toiminnallisena opinnäytetyönä, joka perustuu työelämälähtöiseen toimeksiantoon. Opinnäytetyö tuotti tuloksia ja kehittämisehdotuksia toimeksiantajalle.

Opinnäytetyön lopputuloksena organisaatiolle saatiin hahmoteltua jatkuvuuden hallintajärjestelmän runko. Hallintajärjestelmälle asettuja vaatimuksia ja niiden toteutuksia arvioitiin ja kehitettiin. Hallintajärjestelmän lopullinen toteutus tapahtuu opinnäytetyön jälkeen.

Avainsanat (asiasanat)

Liiketoiminnan jatkuvuus, Jatkuvuudenhallinta, ISO 22301:2019, Liiketoiminnan jatkuvuuden hallintajärjestelmä.

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Rissanen, Jesse

Development of continuity management system for a case-company

Jyväskylä: JAMK University of Applied Sciences, November 2022, 98 pages.

Engineering and technology. Degree programme in Information and communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

A business continuity management system enables an organization to effectively plan, rehearse and practice procedures to ensure the organization's ability to recover and recover from various disruptive events.

The thesis was carried out in cooperation with a case organization. The organization wished to remain anonymous and therefore the organization will not be described in detail, nor will its size be described in more detail. The client organization is active in the ICT sector.

The aim of the thesis was to develop a business continuity management system to support the client's business in accordance with the ISO 22301:2019 standard, which sets requirements for a business continuity management system, and as a basis for the certification of the management system outside the thesis.

A business continuity management system in accordance with ISO 22301 ensures protection against disruptive events, reducing the likelihood of disruption, preparing for and responding to disruptions and recovering from disruptions. The requirements of the standard are general and apply to all organizations, regardless of their size or area of operation.

The development work was divided into three parts: defining the target state for business continuity management in the case organization, mapping the baseline situation and assessing the gaps, and building the framework for a business continuity management system to serve as a basis for further development.

The thesis was carried out as a functional thesis, based on a workplace-based assignment. The thesis produced results and development proposals for the client.

As a result of the thesis, a framework for a continuity management system was outlined for the organization. The requirements for the management system and their implementation were evaluated and developed. The final implementation of the management system will take place after the thesis.

Keywords/tags (subjects)

Business Continuity, Continuity management, ISO 22301:2019, Business Continuity Management System

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Taulukot

Lyhenteet

BCMS	Business Continuity Management System
BIA	Business Impact Analysis
ISMS	Information Security Management System
ISO	International Organization for Standardization
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
MTPD	Maximum Tolerable Period of Disruption
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFS	Suomen Standardisoimisliitto
SLA	Service Level Agreement

1 Johdanto

Nykyajan organisaatiot ja yritykset toimivat jatkuvasti ja nopeasti muuttuvissa toimintaympäristöissä. Erilaisten tilanteiden häiriöt, kuten kyberhyökkäykset, tuotteiden ja materiaalien saatavuusongelmat sekä avainhenkilöresurssin poistuminen, esimerkiksi pandemiatapaukset ja sairastumiset, voivat tapahtua nopeastikin ja aiheuttaa organisaatiolle erilaisia ongelmia. Teknologian ja sitä kautta kyberympäristön jatkuvat ja joskus nopeatkin muutokset aiheuttavat omat vaatimuksensa toimintaympäristölle. Myös asiakkaat, toimittajat ja muut sidosryhmät voivat lisätä muutoksia ja vaatimuksia toimintaympäristössä maailman ollessa yhä enemmän verkottuneempi ja kansainvälisempi.

Lisäksi esimerkiksi koronapandemia ja muut vastaavat pandemiat tai epidemiat voivat ja ovatkin jo vaikuttaneet yritysten ja organisaatioiden toimintaympäristöihin merkittävästi muun muassa etätyökäytänteiden ja niihin liittyvien teknologisten ratkaisujen osalta. Covid-19 lisäksi helmikuussa 2022 Venäjän aloittama hyökkäyssota Ukrainaan ja tästä johtuva fyysisen turvallisuusympäristön muuttumisen lisäksi muuttunut tietoverkkojen turvallisuusympäristö on oiva esimerkkitapaus siitä, miksi organisaatioiden tulisi toteuttaa jatkuvuudenhallintaa pelkästään jo kyber- ja tietoturvallisuuden näkökulmasta.

Opinnäytetyön aihe oli noussut esille case-organisaatiossa jo aiemmin ja Venäjän aloittama hyökkäyssota Ukrainaan teki aiheesta vieläkin ajankohtaisemman. Lisäksi opinnäytetyön kirjoitushetkellä Covid-19-pandemia ei ole edelleenkään ohi, vaikka toki liiketoiminnan näkökulmasta pandemiaan on jo melko hyvin sopeuduttukin. Venäjän hyökkäyssodan seurauksena on myös havahduttu enemmän mahdollisiin alihankkija- toimitusketjujen häiriöihin ja vuoden 2022 loppua kohti myös energian saatavuusongelmiin, johtuen muun muassa Venäjältä tuodun maakaasun tuonnin lakkaamisesta Eurooppaan.

Venäjän hyökkäyssota Ukrainaan on vuoden 2022 aikana enenevissä määrin vaikuttanut voimakkaasti sekä energia- että elintarvikemarkkinoihin. Sähkön saatavuuteen talvella liittyy epävarmuuksia muun muassa Suomen sähkönsiirron kantaverkon ylläpitäjän Fingrid Oyj:n (2022) mukaan ja mahdollisiin sähkönsaannin vaikeuksiin tulisikin varautua. Fingridin arvioiden mukaan sähkön säännöstelyn vuoksi toteutettavien sähkökatkojen pituus voisi olla noin kaksi tuntia (Helsingin Sanomat. 2022). Kiertävien sähkökatkojen tarkoituksena on välttää sähköjärjestelmän suurhäiriö,

jonka toteutumisella olisi vaikutuksia koko sähköjärjestelmän toimintakykyyn ja jonka palauttaminen voisi kestää useista tunneista useisiin vuorokausiin.

Jatkuvuudenhallinnan keinoin on mahdollista toimia ennakoivasti ja varautua sähkökatkoihin esimerkiksi määrittelemällä yrityskohtaiset vaatimukset ydintoiminnan jatkamiselle sähkökatkojen aikana. Kun vaatimukset on tunnistettu, voidaan niihin kohdistaa asianmukaisia toimenpiteitä, kuten hankkia yrityksen avaintoiminnoista vastaaville etätyöskentelyn varmistamiseksi varavirtalähteitä, tai toimitiloihin koko kiinteistölle varavirtaa tuottavia generaattoreita sähkökatkojen aikaisen toiminnan mahdollistamiseksi.

Varautumistoimissa tulisi huomioida myös mahdollisuus sille, etteivät sähkökatkot jäisi aina suunniteltujen noin kahden tunnin mittaisiksi tai että niitä tapahtuu suunniteltua frekvenssiä tiuhemmin. Lisäksi sähkökatkoja voi tapahtua muistakin syistä kuin kiertävien sähkökatkojen takia, joten katkot eivät välttämättä toteudu suunniteltuina ajankohtina. Yksi ratkaisu ei välttämättä ole aina riittävä ja siksi organisaatioiden tulisi ennakoimalla varautua myös siihen, että niillä on vaihtoehtoisia toimintamalleja ja ratkaisuja mahdollisiin eri skenaarioihin.

Euroopassa käytävän sodan ja siitä aiheutuvan energian saatavuusongelmien lisäksi myös kauempana on havaittavissa kuohuntaa. Kiinan ja Taiwanin suhteet ja mahdollinen sotilaallinen konflikti voivat vaikuttaa suuresti muun muassa toimitusketjuihin ja tuotteiden saatavuuteen. Myös tähän on mahdollista varautua ennakkoon liiketoiminnan jatkuvuuden keinoin, esimerkiksi käymällä toimitusketjuihin sekä alihankkijoihin liittyvät riskit läpi, tarkistamalla ja varmistamalla sopimukset ja niiden toteutuminen sekä tarvittaessa hankkimalla korvaavat palvelut vaihtoehtoisilta toimittajilta.

Taiwan on yksi maailman suurimmista puolijohdevalmistajista yli 50 % markkinaosuudellaan (Bhutada, G. 2021), joten mahdollisella sotilaallisella konfliktilla Kiinan ja Taiwanin välillä olisi todennäköisesti suuriakin vaikutuksia ICT-laitteiden, ja -tuotteiden saatavuuteen. ICT-laitteiden lisäksi puolijohteita käytetään lähes kaikessa elektroniikassa, joten pula puolijohteista vaikuttaa myös muun muassa ajoneuvojen tuotantoon ja huoltoon sekä lääketieteellisiin laitteisiin (Shiphub. N.d).

Sekä Shiphubin artikkelin, että Athanasian & Arcurin (2022) mukaan puolijohteissa käytettävää harvinaista jalokaasua, puolijohdetason neonia, tuotiin ennen Venäjän hyökkäystä Ukrainasta jopa

90 % markkinaosuudella ja jälkimmäinen mainitsee myös Kiinan yhtenä suurimmasta neljästä neonin tuottajamaasta. Euroopan tasolla tulisikin arvioida mahdollisuuksia kehittää omaa puolijohteiden valmistusta riippuvuuksien vähentämiseksi.

Lisäksi Kiinan ja Taiwanin välinen sota vaikuttaisi mitä todennäköisimmin meriteitse kulkeviin kauppareitteihin, joista yksi maailman vilkkaimmista on Malakansalmi (Wikipedia. 2022), joka yhdistää kolme Aasian suurinta taloutta, Kiina, Japani, Intia, toisiinsa sekä monia muita tärkeitä talouksia, kuten Malesian, Taiwanin sekä Etelä-Korean (Freightify. 2021), joten vaikutukset eivät rajoittuisi vain Kiinaan ja Taiwaniin ja niiden tuottamiin ICT-komponentteihin.

Kaikki nämä ovat vain jotain esimerkkejä, joihin organisaatioiden tulee varautua, ja kuvaavat hyvin asioiden keskinäisriippuvuuksia ja kuinka nykymaailma on verkottunut muun muassa toimitus- ja alihankintaketjujen osalta ja esimerkiksi kuinka helposti pelkästään energian saatavuus voi heikentyä. Aseellinen konflikti tai kaksi sopivissa sijainneissa voi pahimmillaan häiritä vakavastikin lähes koko maailmantaloutta.

Liiketoiminnan jatkuvuudenhallinnassa ennakointi on avain. Ennakoivalla toiminnalla pyritään varautumaan toimintaympäristön muutoksiin ja haasteisiin sekä luomaan edellytykset liiketoiminnan kehittymiselle ja kehittämiselle sekä sen jatkamiselle. Ennakoinnilla vähennetään häiriöiden mahdollisuutta, valmistaudutaan korjaamaan häiriöitä sekä palautumaan häiriöistä (Vahti 2/2016, 17).

Jatkuvuudenhallinnan keinoilla voidaan optimoida toimintojen jatkuvuutta sekä turvata organisaation suorituskykyä. Oikein tehty ja säännöllisesti päivittyvä jatkuvuudenhallinta mahdollistaa organisaatioille sen toiminnan jatkuvuuden normaaliolojen lisäksi myös haastavissa ja muuttuvissa olosuhteissa alati muuttuvassa toimintaympäristössä.

Jatkuvuudenhallinnaksi kutsutaan prosessia, jonka tarkoituksena on turvata liiketoiminnan ja sen keskeisten prosessien jatkuvuus keskeytystilanteissa (PwC Suomi. N.d). Jatkuvuudenhallintaan kuuluvat muun muassa liiketoiminnan uhkien, riskien, häiriötilanteiden sekä riippuvuuksien tunnistaminen, uhkien vaikutusten arviointi organisaatiossa sekä organisaation toimijaverkossa ja menettelytapojen organisointi ja toteutus häiriötilanteiden varalle.

Yleensä jatkuvuudenhallinta on omaehtoista toimintaa organisaatioille, mutta joillain aloilla laki voi velvoittaa organisaatioita varmistamaan toimintansa jatkuvuus eri olosuhteissa, kuten esimerkiksi poikkeusoloissa (Tietoa huoltovarmuudesta. N.d).

1.1 Tavoitteet

Opinnäytetyön ensisijaisena tavoitteena oli tehokkaan ja helposti hallittavan jatkuvuuden hallintajärjestelmän kehittäminen case-organisaatiolle, jonka lopullinen tavoite on jatkuvuuden hallintajärjestelmän ISO 22301-standardin mukainen sertifioituminen. Tavoitteena oli pyrkiä mahdollisimman valmiiseen hallintajärjestelmään, jota olisi mahdollista jatkokehittää myöhemmän sertifioinnin saavuttamiseksi. Toteutettava jatkuvuuden hallintajärjestelmä noudattelee pääpiirteittäin case-organisaation olemassa olevaa tietoturvan hallintajärjestelmää, ISMS-järjestelmää (Information Security Management System), joka on toteutettu ISO 27001-standardin vaatimusten mukaisesti.

Toteutettava jatkuvuuden hallintajärjestelmä noudattaa tietoturvan hallintajärjestelmän rakennetta yhdenmukaisuuden saavuttamiseksi hallintajärjestelmien välillä siltä osin kuin on soveltuvaa. Pääotsikkotasolla standardit ISO 22301 ja 27001 ovat identtisiä keskenään ja jotkin ISO 22301:n vaatimukset löytyvät vaatimuksina myös ISO 27001:ssä ja voivat näin ollen jo olla toteutettu aiemmin joko kokonaan tai lähes kokonaan standardin ISO 22301 vaatimusten mukaisesti.

Yksistään tieto- ja viestintätekniset- sekä tietoturvakontrollit eivät takaa laaja-alaista liiketoiminnan jatkuvuutta, sillä liiketoiminnan osia ovat myös muut organisaatiolle tärkeät toiminnot ja niiden mahdollistajat, kuten henkilöresurssit, hankinta ja talous. Jo toteutettu.

Koska hallintajärjestelmän tavoitteena on myöhemmin sertifioitua ISO 22301-standardia vasten, hallintajärjestelmää tuli kehittää ja arvioida jo sertifiointia ajatellen, jotta ensisijainen tavoite voidaan saavuttaa helpommin. Hallintajärjestelmän osien valmiutta ja kypsyyttä pyrittiin arvioimaan kolmiportaisella arviointiasteikolla, jaottelulla soveltuu – soveltuu osittain – ei sovellu. Käytetty arviointiasteikko noudattelee kuvion 1 mukaista Kuntaliiton ja Huoltovarmuuskeskuksen yhteistyönä toteuttaman Kuntien jatkuvuudenhallintahankkeen (KUJA. 2019) pikatestiä ja sen arviointiasteikkoa, jonka tarkoituksena on kartoittaa varautumisen ja jatkuvuudenhallinnan tasoa.

Kuvio 1. KUJA-pikatesti (KUJA. 2019).

Eri dokumenttien ja tallenteiden katselmoinnit olivat pääasiallinen keino jatkuvuuden hallintajärjestelmän opinnäytetyön aikaisessa kehitysvaiheessa. Jatkuvuuden hallintajärjestelmän eri vaatimuksia ja sitä, ovatko toteutuneet toimintamallit vaatimusten mukaisia (tavoite vs. toteutunut), arvioitiin heti jatkuvuuden hallintajärjestelmän kehittämisen alkuvaiheessa, tavoitetilan suuntaviivojen määrittelyn jälkeen. Mukana arviointien tulosten läpikäynneissä oli henkilöitä case-organisaatiosta, jolloin arvioinnit ovat luotettavampia ja niitä voitiin tarkentaa.

Eri politiikkojen, ohjeistusten, prosessien ja toimintaohjeiden kirjallisten dokumentoitujen tietojen katselmointi toimikin siis pääasiallisena lähteenä lähtötilanteen aikaisessa kartoituksessa, kehityskohteiden tunnistamisessa ja vaatimusten mukaisen hallintajärjestelmän kehittämisessä.

1.2 Vaatimukset ja rajaukset

Vaatimuksena oli case-organisaation kaikki liiketoiminta-alueet kattava liiketoiminnan jatkuvuuden hallintajärjestelmä. Hallintajärjestelmä toteutetaan case-organisaatiossa ja sen tuottamissa palveluissa sekä organisaation käyttämissä prosesseissa ja sisäisissä tukipalveluissa. Case-organisaation hallintajärjestelmän tarkoituksena on mahdollistaa organisaatiolle asetettujen tavoitteiden saavuttaminen sekä organisaation käsittelemien suojattavien kohteiden turvaaminen.

Opinnäytetyö keskittyy liiketoiminnan jatkuvuudenhallintaan ja sen osiin, kuten riskienhallintaan ja liiketoiminnan vaikutusanalyysiin, joita käydään opinnäytetyössä kattavasti läpi niiden oleellisuuden ja tärkeyden vuoksi. Myös muuta jatkuvuudenhallintaan liittyvää tietoperustaa käydään läpi lukijalle käsitteiden ja niiden merkitysten ja niiden välisten suhteiden havainnollistamiseksi.

Opinnäytetyössä esitellään myös kattavasti ISO 22301-standardi ja sen vaatimukset, sillä toteutettava liiketoiminnan jatkuvuuden hallintajärjestelmä toteutetaan ISO 22301-standardin vaatimusten mukaisesti. Case-organisaation saamia standardin mukaisesti toteutetun hallintajärjestelmän hyötyjä käsitellään muun muassa jatkuvuuden hallintajärjestelmän luvussa 3.3.

Opinnäytetyö käsittelee myös Kansallista auditointikriteeristöä (Katakri) jatkuvuudenhallinnan näkökulmasta, jonka lisäksi käydään myös läpi Vahti-ohjeita, jotka ovat ohjemuotoista materiaalia turvallisuuden kehittämiseksi organisaatioissa. Organisaatiot voivat hyödyntää eri Vahti-ohjeissa olevia parhaita käytäntöjä turvallisuuden eri osa-alueiden kehittämisessä.

Opinnäytetyössä käydään myös hieman läpi varautumista, valmiussuunnittelua sekä poikkeusoloja, mutta opinnäytetyö ei keskity näihin. Edellä mainittuja asioita käsitellään, jotta myös näiden käsitteiden merkitykset ja suhteet saadaan havainnollistettua lukijalle, sillä esimerkiksi jatkuvuudenhallinta ja varautuminen ovat käsitteinä lähes synonyymejä toisilleen.

Opinnäytetyö toteutetaan kehittämistyönä keskittyen case-organisaatiossa jo toteutettuihin jatkuvuudenhallinnan keinoihin, sekä jo olemassa olevien ja uusien jatkuvuudenhallinnan keinojen kehittämiseen ja käyttöönottoon ISO 22301-standardin vaatimusten mukaisesti.

2 Tutkimusideologia

Tutkimusideologiassa tuodaan esille opinnäytetyön tutkimuskysymykset sekä millä menetelmillä tutkimuskysymyksiin saadaan vastauksia. Tutkimusmenetelmissä tuodaan esille myös se, millä tutkimustavalla opinnäytetyö on toteutettu.

2.1 Tutkimuskysymys

Tutkimuskysymykset määrittävät sen, mitä tutkimuksella halutaan selvittää ja mihin opinnäytetyön tulisi vastata. Tutkimuskysymykset ohjaavat opinnäytetyön kirjoittajaa tutkimusmenetelmän ja opinnäytetyön toteuttamisessa (Tutkimusasetelma. N.d).

Tässä opinnäytetyössä tutkittava ilmiö on liiketoiminnan jatkuvuus toimeksiantajaorganisaatiossa. Liiketoiminnan jatkuvuudella tarkoitetaan toimintakyvyn ja jopa selviytymiskyvyn varmistamista organisaatiossa häiriön tai kriisin aikana. Kriisi voi johtua erilaisista häiriötilanteista.

Opinnäytetyön aihe ja tutkimuskysymykset, sekä käsitteiden määrittelyt luovat rajauksen opinnäytetyölle. Opinnäytetyössä nousi esiin kolme tutkimuskysymystä, jotka ovat seuraavat:

1. Kuinka liiketoiminnan jatkuvuudenhallintaa on toteutettu case-organisaatiossa ennen liiketoiminnan jatkuvuuden hallintajärjestelmän kehittämisen aloittamista?

2. Mitä kehitettäviä osa-alueita case-organisaatiossa on liiketoiminnan jatkuvuuden näkökulmasta?

3. Mitä hyötyjä case-organisaatio saa ISO 22301-standardin mukaisesti toteutetusta jatkuvuuden hallintajärjestelmästä?

2.2 Tutkimusmenetelmä

Opinnäytetyössä selvitetään tutkimuskysymyksien realiteetteja perehtymällä liiketoiminnan jatkuvuudenhallintaan liittyvään tietoperustaan, tutkimalla menneitä tapahtumia sekä nykytilannetta. Kaiken tämän tiedon pohjalta on mahdollista vastata esitettyihin tutkimuskysymyksiin ja kehittää niiden pohjalta ratkaisuja toimeksiantajana toimivan case-organisaation kysymyksiin.

Rakenteensa perusteella opinnäytetyö vastaa toiminnallista opinnäytetyötä, joka perustuu työelämälähtöiseen toimeksiantoon. Opinnäytetyö tuottaa tuloksia ja kehittämisehdotuksia toimeksiantajalle (Tutkimuksellinen kehittämishanke opinnäytetyönä vs projektityö. N.d). Tutkimusmenetelmän avulla saadaan käsitys toimeksiantajan liiketoiminnan jatkuvuudenhallinnan tavoitteista, lähtötilanteesta, kehitystyöstä sekä lopputuloksesta.

3 Keskeiset käsitteet

Luvun tarkoituksena on käydä läpi ja avata jatkuvuudenhallinnan kannalta keskeisimpiä ja oleellisimpia asioita ja käsitteitä, jotta lukija saa paremman käsityksen työstä. Lisäksi joitain käsitteitä on

hyvä käydä läpi, jotta tiettyjen käsitteiden suhtautuminen toisiinsa sekä niiden keskinäiset riippuvuussuhteet saadaan selkeämmiksi.

3.1 Jatkuvuussuunnittelu

Jatkuvuussuunnittelu koostuu niistä toimista, joiden avulla pyritään vähentämään toimintaa haittaavien tapahtumien vaikutusta ja kestoa. Jatkuvuussuunnittelu sisältää varajärjestelyitä sekä toimenpiteitä, joilla parannetaan toimintaa häiriötilanteissa ja toipumista ongelmista. Jatkuvuussuunnittelun konkreettinen tuotos on dokumentoitu jatkuvuussuunnitelma (Vahti 2/2016, 24).

Jatkuvuussuunnitelma ohjaa organisaatioita reagoimaan häiriöön, palautumaan niistä sekä jatkamaan tuotteiden ja palveluiden toimittamista liiketoiminnan jatkuvuutta koskevien tavoitteiden mukaisesti. Jatkuvuussuunnittelu sisältää myös suunnitelmat, jotka kuvaavat johtamisen, vastuut sekä toimenpiteet, joiden mukaan toimintoja voidaan jatkaa erilaisissa häiriötilanteissa ja niiden jälkeen (ISO 22301:2019, 9).

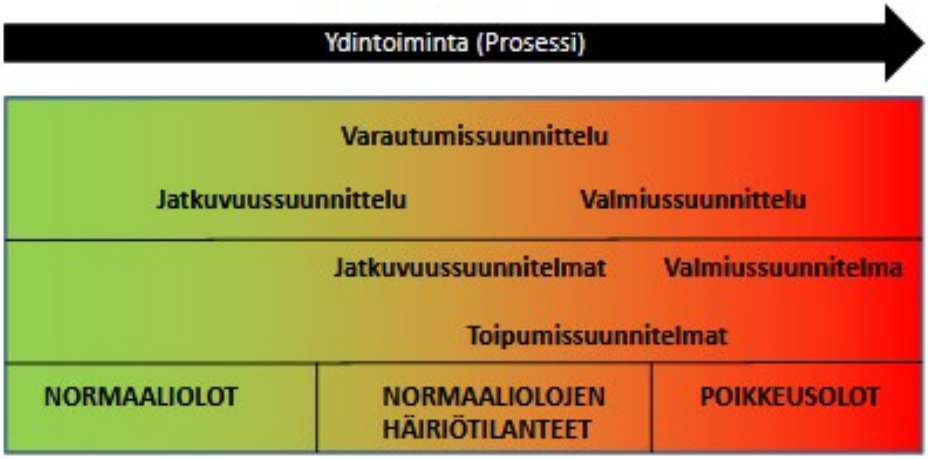
Olennainen osa jatkuvuussuunnittelua ovat liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt, joiden mukaisesti organisaatiota hallitaan, taikka palvelua, tuotetta, prosessia palautetaan, häiriön aikana. Näitä suunnitelmia ja menettelyjä on noudatettava, kun käynnistetään liiketoiminnan jatkuvuusratkaisuja (ISO 22301:2019, 22).

Jatkuvuussuunnitelmien on sisällytettävä erityyppisiä menettelyitä. Liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt tunnistetaan ja dokumentoidaan valittujen strategioiden ja ratkaisujen tuotosten perusteella. Valittujen menettelyjen on kuvattava yksityiskohtaisesti välittömät toimenpiteet, jotka suoritetaan häiriön aikana. Menettelyjen on silti oltava tarpeeksi joustavia, jotta menettelyillä voidaan vastata vaihtuviin sisäisiin ja ulkoisiin olosuhteisiin häiriön aikana (ISO 22301:2019, 22).

Menettelyjen on keskityttävä sellaisiin häiriötilanteisiin ja niiden vaikutuksiin, jotka voivat mahdollisesti ja realistisesti johtaa häiriöön (riskienhallinta ja liiketoiminnan vaikutusanalyysien tulokset) (ISO 22301:2019, 22). Jatkuvuusmenettelyjen on kuvattava, kuinka toimintaa haittaavien tapahtumien vaikutusta vähennetään tehokkaasti toteuttaen kirjattuja asianmukaisia ratkaisuja. Menettelyjen on sisällytettävä tehtävien roolit ja vastuut, niiden tulee olla jaettu ja osoitettu selkeästi.

Organisaation on myös määriteltävä valittavien liiketoiminnan jatkuvuusratkaisujen toteuttamiseen riittävät ja vaadittavat resurssit. Huomioitavia resurssityyppejä ovat muun muassa ihmiset, tieto ja data, fyysinen infrastruktuuri kuten työskentelypaikat ja toimitilat, varusteet ja tarvikkeet sekä tieto- ja viestintäteknologiajärjestelmät (ISO 22301:2019, 21–22).

Suunnitelmiin olisi hyvä myös sisällyttää suunnitelmien ylläpito ja viestintä, koulutus, harjoittelu ja testaus sekä suunnitelmien katselmointi ja raportointi johdolle (Vahti 2/2016, 69). Tämän opinnäytetyön luku 4 käsittelee suunnitelmien ylläpitämiseen liittyvää toimintamallia, vuosikelloa, tarkemmin Vahti-ohjeita käsittelevässä osiossa.



Kuvio 2. Jatkuvuussuunnittelun termien ja määritelmien suhde toisiinsa (Iivari & Laaksonen 2009).

Kuviossa 2 nähdään jatkuvuussuunnittelun termien ja määritelmien suhde toisiinsa. Jatkuvuussuunnittelu ja sen tuotokset keskittyvät normaaliolojen häiriötilanteisiin. Toipumissuunnitelmat ovat osa jatkuvuussuunnitelmia ja ne kattavat myös poikkeusolojen aikaista toimintaa. Poikkeusoloista ja valmiussuunnitelmista kerrotaan lisää luvussa 3.6 – Varautuminen.

Jatkuvuussuunnittelun yksi tärkeä osa on toipumissuunnittelu, joka liittyy yleensä tietojärjestelmiin ja niiden toipumiseen häiriötilanteissa (Vahti 2/2016, 24). Yksittäinen toipumissuunnitelma määrittelee sekä dokumentoi tietojärjestelmille käytännön toimenpiteet – jotka voivat olla kuvattu jopa komentorivitarkkuudella, eli mitä komentoja tulisi antaa toimintojen palauttamisen mahdollistamiseksi, esimerkiksi palvelinympäristöjä palauttaessa – sekä roolit ja vastuut normaalitilaan

palaamiseksi. Toipumissuunnitelmat ovat siis konkreettinen kuvaus operatiivisella tasolla järjestelmien palauttamisesta. Toipumissuunnitelmat sisältävät ohjeet häiriöstä toipumiseen, paluulle normaaliin toimintaan sekä toiminnan jatkamiselle. Jatkuvuussuunnitelmat ohjaavat toipumissuunnitelmia (Vahti 2/2016, 24).

Mikäli jokin palvelu on tuotettu alihankkijan tai muun toimittajan toimesta, tulisi toipumissuunnitelmat vaatia näiltä sekä sopia suunnitelmien säännöllisestä ylläpidosta, niiden katselmoinneista sekä mahdollisesti tarvittavista harjoitteluista (Vahti 2/2016, 24). Toipumissuunnitelmia tulisi noudattaa palautumistoimenpiteitä suoritettaessa, harjoittelun ja testaamisen avulla varmistetaan, että toipumissuunnitelmat toimivat oikein, jolloin varmistetaan nopea ja luotettava palautuminen.

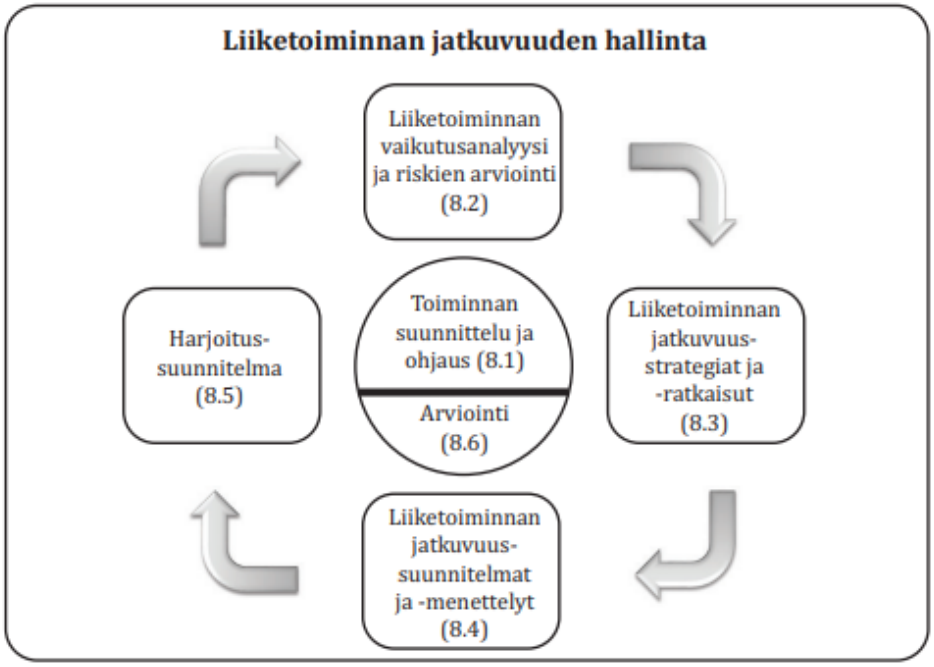
3.2 Jatkuvuudenhallinta

Jatkuvuudenhallinnan tarkoituksena on toteutuneiden riskien vaikutusten vähentäminen sekä joskus jopa riskien poistaminen kokonaan. Jatkuvuudenhallinta on prosessi, jonka avulla voidaan tunnistaa uhkat, riskit, häiriötilanteet sekä erilaiset riippuvuudet, olivat ne sitten sisäisiä, esimerkiksi organisaation tietojärjestelmien keskinäiset riippuvuudet, tai ulkoisia riippuvuuksia, kuten erilaiset toimitusketjuriippuvuudet (Huoltovarmuuskeskus. 2020).

Jatkuvuudenhallinnan keinoin voidaan arvioida uhkien vaikutuksia organisaatiossa ja toimijaverkostossa esimerkiksi liiketoiminnan vaikutusanalyysien avulla. Jatkuvuudenhallinnassa organisoidaan ja toteutetaan toimintamallit ja menettelytavat häiriötilanteiden varalle. Jatkuvuudenhallinnan keinoja voidaan käyttää varmistamaan kriittisten kumppaneiden, esimerkiksi alihankkijoiden tai jopa alihankkijoiden käyttämien alihankkijoiden kyky toimia häiriötilanteissa (Huoltovarmuuskeskus. 2020).

Jatkuvuudenhallinta on yleensä vapaaehtoista toimintaa, mutta joitakin toimijoita ja joillakin aloilla laki voi velvoittaa organisaatioita varmistamaan toimintansa jatkuvuuden eri olosuhteissa. Valmiuslain 3 luvussa (Valmiuslaki 1552/2011) säädetään varautumisesta poikkeusoloihin. Varautumisvelvollisuus velvoittaa valmiuslaissa mainittuja viranomaisia sekä muita tahoja jo normaalioloissa (HE 63/2022 vp. 2022). Varautumisesta tarkemmin luvussa 3.6. Varautuminen.

Kansainvälisen standardisoimisjärjestön (ISO, International Organization for Standardization) mukaan jatkuvuudenhallinta kohdistuu liiketoimintaan. Kuviossa 3 esitellään jatkuvuudenhallinnan eri osat, joille ISO 22301-standardi asettaa vaatimuksia. Vaatimukset esitellään tarkemmin ISO 22301-standardia käsittelevässä luvussa 4.1.



Kuvio 3. Liiketoiminnan jatkuvuuden hallinnan osat (ISO 22313:2020, 31).

Jatkuvuudenhallinta ja sen kehittäminen on jatkuvaa ja säännöllistä toimintaa. Nykyajan jatkuvuuden suunnittelussa tulee huomioida omien toimintojensa lisäksi myös yhteistyö- ja alihankintaverkostot ja niiden kyky toimia häiriötilanteissa. Yllättäviin häiriötilanteisiin varaudutaan ennalta ja organisaatio todennäköisemmin selviää häiriötilanteista pienemmillä kustannuksilla, mainehaitoilla sekä vaurioilla (Huoltovarmuuskeskus. 2020).

Alihankkijalta voidaan muun muassa pyytää selvitys siitä, kuinka he varmistavat sen, ettei heiltä hankittavat tuotteet, esimerkiksi tietoliikennekaapelit, tuhoudu esimerkiksi alihankkijan käyttämän varaston tulipalossa. Alihankkijan tulee pystyä näyttämään toteen, että he ovat varautuneet tällaisiin tilanteisiin esimerkiksi sammutusjärjestelmin tai muilla korvaavilla toimenpiteillä.

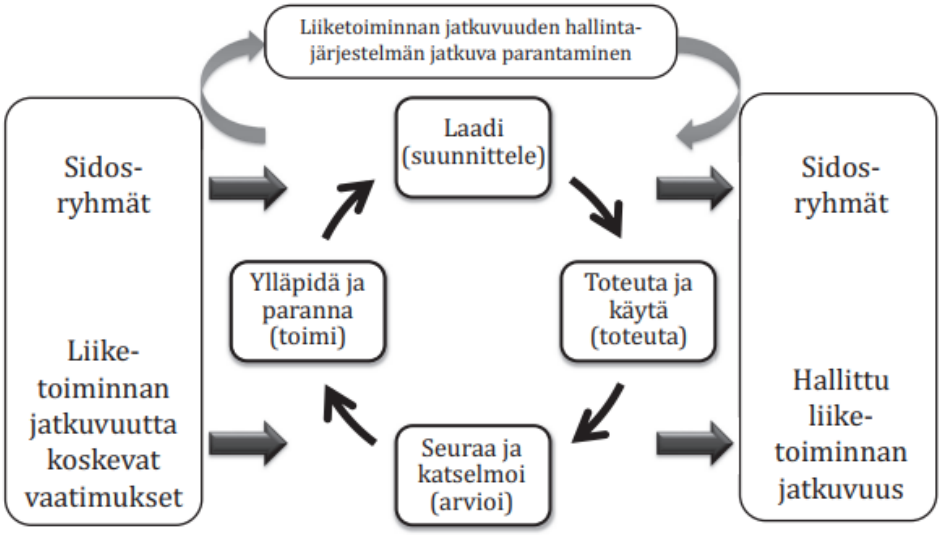
Liiketoiminnan jatkuvuudenhallinnan kuvion 3 mukaisista osista tämä opinnäytetyö käsittelee tarkemmin liiketoiminnan vaikutusanalyysin sekä riskienhallinnan ja sen osia, kuten riskien arvioinnin.

3.3 Jatkuvuuden hallintajärjestelmä

Tässä alaluvussa kuvataan jatkuvuuden hallintajärjestelmän perusperiaatteita sekä avataan hallintajärjestelmän tarkoitusta ja hyötyjä. Koska opinnäytetyön toimeksianto toteutetaan ISO 22301:2019-standardin mukaisesti, keskittyy tämä luku kyseisen standardin mukaisen hallintajärjestelmän kuvaamiseen, mutta esittelee myös ISO 22301-standardin toteutusta ohjaavan standardin, ISO 22313:2020, sekä toisen liiketoiminnan jatkuvuudenhallinnan standardin, BSI 100-4 (Bundesamt fur Sicherheit in der Informationstechnik), jonka on tuottanut Saksan liittovaltion tietoturvavirasto vuonna 2009.

Organisaation jatkuvuudenhallintaan liittyvät prosessit voidaan kuvata hallintajärjestelmän avulla. Jatkuvuuden hallintajärjestelmän muodostavat kaikki prosessit, työkalut, toimenpiteet, suunnitelmat ja tavoitteet, joiden tarkoitus on varmistaa organisaation toiminnan jatkuvuus (Vahti 2/2016, 29).

ISO 22301-standardin mukainen hallintajärjestelmä perustuu PDCA-mallin mukaiseen jatkuvaan parantamiseen, jolla varmistetaan hallintajärjestelmän jatkuva kehittäminen, vaatimusten seuraaminen ja päivittäminen (ISO 22313:2020, 66). PDCA-malli on kuvattu tarkemmin ISO 22301-standardia laajemmin käsittelevässä luvussa 4.1.



Kuvio 4. PDCA-malli ja sen käyttö liiketoiminnan jatkuvuuden hallintajärjestelmissä (ISO 22313:2020, 8).

Kuviossa 4 esitetään, kuinka liiketoiminnan jatkuvuuden hallintajärjestelmän syötteitä ovat sidosryhmien vaatimukset, ja kuinka toimenpiteiden ja prosessien tuloksena saadaan tuloksia, jotka täyttävät vaatimukset ja edistävät siten liiketoiminnan jatkuvuutta.

Liiketoiminnan jatkuvuuden hallintajärjestelmän tarkoitus on valmistella organisaatio häiriön aikaiseen toimintaan, tuottaa tähän vaadittavat hallintakeinot ja kyvykkyydet, mahdollistettava niiden käyttö sekä ylläpidettävä niitä (ISO 22301:2019, 5). Organisaation tulisi määritellä ja tunnistaa kriittiset toimintonsa jatkuvuuden hallinnan onnistumiseksi. Kun kriittiset toiminnot on tunnistettu, voidaan niihin kohdistaa toimenpiteitä, kuten riskienhallinta ja toiminnan vaikutusanalyysi (Vahti 2/2016, 29).

ISO 22301-standardin mukaisen liiketoiminnan jatkuvuuden hallintajärjestelmän hyötyjä ovat muun muassa liiketoiminnan näkökulmasta maineen ja uskottavuuden suojaaminen ja parantaminen sekä organisaation kriisinkestävyyden vahvistaminen. Taloudellisesta näkökulmasta hyötyjä ovat taloudellisien riskien pienentäminen sekä häiriöiden aiheuttamien kustannuksien pienentäminen, sidosryhmien näkökulmasta hyötyjä ovat omaisuuden suojelu ja sisäisten prosessien näkökulmasta organisaation parempaa kykyä toimia vaikuttavasti häiriöiden aikana (ISO 22301:2019, 5–6).

Muita ISO 22301-standardin mukaisesti toteutetun liiketoiminnan jatkuvuuden hallintajärjestelmän etuja ja hyötyjä ovat myös paremmat tiedot mahdollisen häiriön todellisista vaikutuksista (riskienhallinnan ja liiketoiminnan vaikutusanalyysin tulosten kautta), minkä ansiosta organisaatio voi muun muassa arvioida paremmin tarvitsemansa vakuutusturvan tyypin ja arvon.

Lisäksi koska ISO 22301 -sertifiointi antaa maailmanlaajuisesti hyväksytyn osoituksen liiketoiminnan jatkuvuuden tehokkuudesta, se tekee tarpeettomaksi toistuvat asiakastarkastukset ja vähentää ulkoisten asiakastarkastusten määrää. Asiakkaat näkevät sen, että sertifioituneet toimittajat tai yhteistyökumppanit ovat nähneet vaivaa varmistaakseen, että ne voivat jatkaa liiketoimintaa vaikeissa olosuhteissa (Benefits of Business Continuity Management. N.d).

Lisäksi ohjaava standardi ISO 22313:2020 mainitsee liiketoiminnan jatkuvuuden hallintajärjestelmän hyötyinä paremman ymmärryksen organisaation sisäisistä ja ulkoisista suhteista, parantuneen viestinnän sidosryhmien kanssa sekä jatkuvaan parantamiseen perustuvan ympäristön luomisen (ISO 22313:2020, 6). Liiketoiminnan jatkuvuuden hallintajärjestelmän standardien mukaisella toteutuksella on siis mahdollista saavuttaa hyötyjä todella kokonaisvaltaisesti organisaatiossa ja yritys- ja liiketoiminnassa.

Jatkuvuussuunnittelun ympärille rakentuvia standardeja ISO 22301 (2019) lisäksi ovat ISO 22313 (2020), sekä BSI 100-4 (2009). ISO 22313 antaa ISO 22301-standardissa esitettyjä vaatimuksia koskevaa tarpeellista ohjeistusta käytännön soveltamiseen. Standardi ISO 22301 ei kerro toteutustapoja, vaan esittää pelkät vaatimukset. ISO 22313 sisältää samat otsikot kuin ISO 223013-standardi, mutta se ei toista vaatimuksia eikä liittyviä termejä ja määritelmiä. Näistä kolmesta standardista laajin on BSI 100-4, joka antaa jatkuvuussuunnittelun vaatimusten lisäksi ohjeistuksen vaatimusten täyttämiseksi.

Tässä opinnäytetyössä keskitytään liiketoiminnan jatkuvuudenhallintastandardiin ISO 22301 BSI 100-4:n sijaan muun muassa siksi, että ISO 22301 on standardina uudempi ja myös jo kerran julkaisuvuotensa 2012 jälkeen päivitetty. ISO 22301:n mukaisesti on myös mahdollista sertifioitua, jolloin voidaan osoittaa organisaation toteuttavan liiketoiminnan jatkuvuudenhallintaa standardin vaatimusten mukaisesti. Myös tämä ohjaa hyvinkin vahvasti standardivalintaa, sillä case-organisaation tavoite on sertifioitua ISO 22301-standardin mukaisesti.

Lisäksi case-organisaatiolla on jo olemassa ISO-standardin mukainen hallintajärjestelmä (tietoturvallisuus), joten toisenkin hallintajärjestelmän toteutus ISO 22301-standardin mukaisesti säästää aikaa ja resursseja, sillä hallintajärjestelmien vaatimukset ovat osittain samat. Eri ISO-hallintajärjestelmien toteutuksia voidaan käyttää vähintäänkin soveltuvana pohjana toisen hallintajärjestelmän toteutuksessa, ellei jopa käyttää aiemmin toteutettua vaatimukset täyttävää toteutusta myös kokonaan toisen hallintajärjestelmän vaatimuksen toteuttamiseksi.

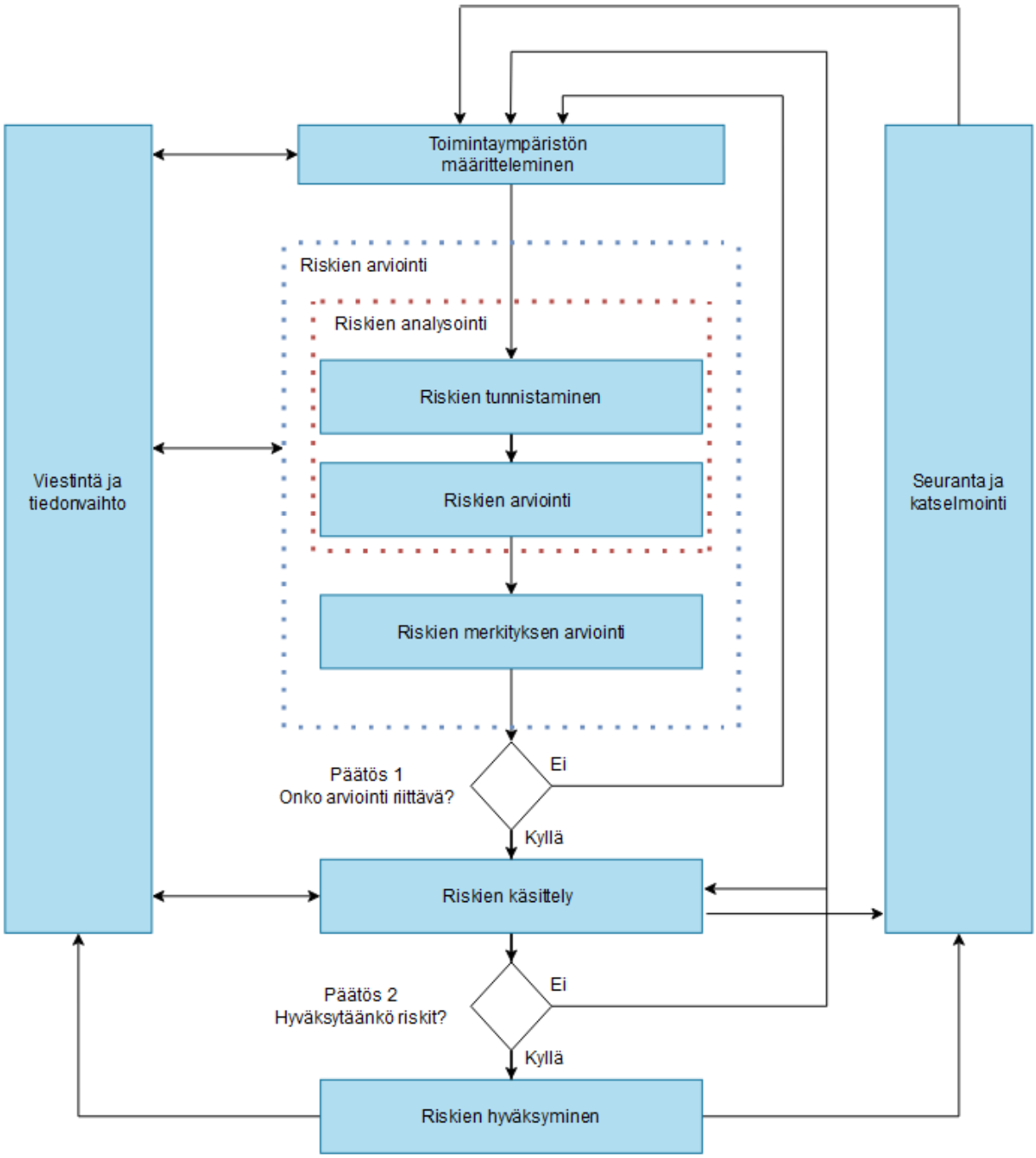
ISO 22301 tai BSI 100-4 -standardin mukainen hallintajärjestelmä toimii runkona tai viitekehyksenä liiketoiminnan jatkuvuudelle. Hallintajärjestelmää voisi kuvailla myös liimana, joka liittää liiketoiminnan jatkuvuuden eri osat yhteen. Liiketoiminnan jatkuvuuden hallintajärjestelmän tarkoitus on ylläpitää liiketoiminnan prosesseja ja varmistaa liiketoiminnan jatkuvuus.

Hallintajärjestelmän avulla voidaan varmistaa liiketoiminnan kyky jatkaa toimintaa erilaisissa häiriötilanteissa sekä palautua häiriötilanteista etukäteen valmistelemalla organisaatio häiriön aikaiseen toimintaan (ISO 22301:2019, 5). Liiketoiminnan jatkuvuuden hallintajärjestelmä on isolta osalta ennakointia, ja häiriötilanteisiin varaudutaan ennakolta valmistelemalla, tuottamalla sekä ylläpitämällä valmiuksia ja suorituskykyä toiminnan jatkuvuudelle, joilla saavutetaan häiriön aikaiseen toimintaan vaadittavat hallintakeinot ja kyvykkyydet.

3.4 Riskienhallinta

Riskienhallinta on prosessi, jossa tunnistetaan ja arvioidaan riskejä, vähennetään riskejä hyväksyttävälle tasolle ja varmistetaan, että riski säilyy hyväksytyllä tasolla. Riskienhallinnan tarkoituksena ei ole poistaa kaikkia mahdollisia riskejä (Maymí & Harris 2022, 53). Riskienhallinnan tarkoitus on organisaation menestymisen mahdollistaminen, toiminnan jatkuvuuden takaaminen sekä asetettujen tavoitteiden saavuttaminen. Riskienhallinta tukee organisaation johtamista ja kehittymistä ja riski voi olla myös positiivinen asia, jolloin riskillä on mahdollisuus saada esimerkiksi liiketaloudellista hyötyä (Vahti 22/2017, 11).

Kuvio 5 esittää riskienhallintaan kuuluvat prosessit. Tämä luku avaa tarkemmin riskienhallintaa muun muassa esittelemällä kvalitatiivisen sekä kvantitatiivisen riskien arvioinnin keinoja, riskien käsittelykeinoja sekä kuinka riskienhallinta toteutuu jatkuvuussuunnittelussa.



Kuvio 5. ISO 27005 mukainen riskienhallinnan prosessi (Maymí & Harris 2022, 177).

Kuten liiketoiminnan jatkuvuudenhallinnalle, myös riskienhallintaan on olemassa valmiina eräänlaisia runkoja, viitekehyksiä, jolloin organisaatioiden ei tarvitse kehittää prosessejaan täysin alusta asti itse. Eri viitekehyksien tarkoituksena on tuottaa rakenne, jonka perusteella voidaan lähteä muodostamaan riskienhallintaa (Maymí & Harris 2022, 171) ja näin ollen mahdollistaa muun muassa riskien tunnistaminen ja arviointi sekä hallintatoimenpiteet.

Riskienhallintaan soveltuvia viitekehyksiä ovat Maymín ja Harriksen (2022, 172–179) mukaan muun muassa:

- National Institute of Standards and Technologyn, Risk Management Framework (NIST RMF)
- ISO 27005
- Enisan the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®)
- FAIR-instituutin Factor Analysis of Information Risk (FAIR)

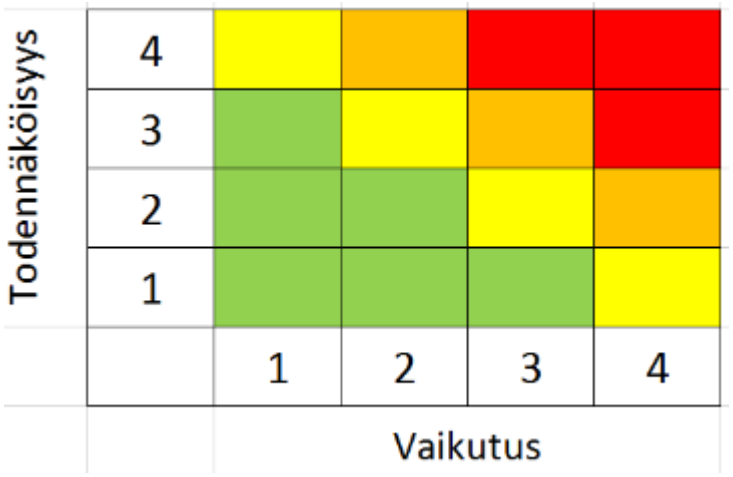
Riskienhallinnan osa on riskien arviointi, joka on järjestelmällinen prosessi riskien analysointiin seurausten ja todennäköisyyden perusteella. Riskien arviointi vastaa muun muassa seuraaviin kysymyksiin (ISO 22313:2020, s. 36):

- Mitä voi tapahtua?
- Mikä on tapahtuman todennäköisyys?
- Mitä seurauksia tapahtumalla voi olla?
- Voidaanko tapahtuman seurauksia pienentää tai voidaanko tapahtuman todennäköisyyttä alentaa?

Organisaation on valittava tarkoituksenmukainen menetelmä sellaisten riskien tunnistamiseen, analysointiin sekä arviointiin, jotka voisivat johtaa häiriöihin. ISO-standardeista riskienhallinnan periaatteita kuvaa standardi ISO 31000, joka antaa myös riskienhallinnan opastusta. Myös standardit ISO 27001 ja ISO 27005 käsittelevät riskien arviointia. Jatkuvuudenhallinnan toteutusta ohjaava standardi ISO 22313:2020 viittaa ISO 31000-standardiin käsitellessään riskien arviointia.

Riskienhallintaan ja riskien käsittelyyn on sekä kvalitatiivisia että kvantitatiivisia viitekehyksiä. Kvalitatiivisessa lähestymistavassa eri komponenteille ja tappioille ei aseteta numeraalista arvoa, vaan riskejä arvioidaan todennäköisyyden ja vakavuuden perusteella.

Kvalitatiivisessa riskien analysoinnissa käytettäviä tekniikoita ovat yleensä käsitykset asioista, parhaat käytännöt, intuitio sekä kokemus (Maymí & Harris 2022, 76). Tietoa kerätään ja tekniikoita voidaan käyttää muun muassa kyselymuodossa, haastatteluissa tai ryhmäarvioinneissa. Kvalitatiivisen riskien arvioinnin tuloksena on useimmiten riskimatriisi, johon on merkitty kuvion 6 esimerkissä y-akselille tapahtuman todennäköisyys, ja x-akselille tapahtuman seurauksien vakavuus tai vaikutus.



Kuvio 6. Kvalitatiivinen riskimatriisi (Vahti 22/2017, 16).

Eri riskit sijoittuvat kuvion 6 matriisissa eri vaiheille. Organisaation tulee päättää, mitkä riskit se hyväksyy ja mihin sen tulee kohdistaa toimia. Esimerkiksi todennäköisyys kertaa vakavuus -vaikutuksiltaan korkeat riskit (oranssi) ja sitä vakavammat tulisi käsitellä ja pyrkiä pienentämään niiden kokonaisvaikutusta hyväksyttävälle tasolle, joka voi olla organisaation riskinottohalusta ja -kyvystä riippuen esimerkiksi kuvion 6 keltaisella tai vihreällä alueella.

Kvantitatiivisessa lähestymistavassa riskejä taas arvioidaan matemaattisen lähestymistavan kautta muun muassa käyttämällä eri laskentakaavoja sekä määrittelemällä numeraalisia tuloksia, jotka voivat kertoa todennäköisyyden sekä vaikutukset rahallisesti laskettuna.

Yleisimpiä käytettyjä kaavoja ovat yksittäisen tappion odotusarvo, (SLE, single loss expectancy) sekä vuotuinen tappio-odotus, (ALE, annualized loss expectancy) (Maymí & Harris 2022, 73). Maymí & Harris (2022, 179) mainitsevat kvantitatiivisista riskienhallintametodeista viitekehyksen Factor Analysis of Information Risk (FAIR), joka on heidän mukaansa ainoa kansainvälinen kvantitatiivisen riskienhallinnan viitekehys.

SLE-arvo laskee rahallisen arvon yksittäiselle tapahtumalle, joka edustaa organisaation potentiaalista yksittäistä rahallista menetystä, mikäli jokin tietty riski realisoituisi. SLE:n kaava on:

Omaisuuden arvo * altistumiskerroin = SLE

Altistumiskerroin voi tarkoittaa esimerkiksi konesalin tapauksessa sitä, että 25 % konesalista tuhoutuisi tulipalon sattuessa. Mikäli konesalin kokonaisarvo olisi 200 000 euroa, laskettaisiin yhden toteutuneen riskin, esimerkiksi tulipalon, vaikutukseksi, eli SLE-arvoksi:

Omaisuuden arvo (200 000 €) * altistumiskerroin (25 %) = 50 000 €

Organisaatio voisi siis menettää 50 000 euroa mahdollisessa tulipalossa.

Koska organisaatiot toimivat vuosibudjeteilla, tulee myös pystyä laskemaan vuosittaiset potentiaaliset tappiot (tappio-odotus). ALE-arvo laskee vuosittaiset mahdolliset tappiot kaavalla:

SLE * vuotuinen esiintymisaste = ALE

Vuotuinen esiintymisaste kuvaa, kuinka usein per vuosi jokin tapahtuma voi tapahtua. Arvo voi olla väliltä 0,0 (ei koskaan) ja 1,0 (kerran vuodessa) sekä myös suurempi kuin 1 (useita kertoja vuodessa) (Maymí & Harris 2022, 74). Esimerkiksi jos tulipalon todennäköisyys konesalissa vuoden aikana on kerran kymmenessä vuodessa, olisi vuotuisen esiintymisasteen arvo 0,1.

50 000 euron yksittäinen tapahtuma joka 10. vuosi olisi siis vuosittaiselta arvoltaan:

50 000 € x 0,1 = 5000 €

Vuosittaisen tappion suuruudeksi tulisi siis tällä laskentatavalla 5000 euroa. Näin mahdolliset vastatoimenpiteet, kuten sammutusjärjestelmien hankinta, voidaan perustella matemaattisesti eikä intuitiolla, kuten kvalitatiivisessa riskienhallinnassa. Esimerkinmukaisessa konesalissa on siis perusteltua käyttää 5000 euroa tai alle per vuosi konesalin suojaamiseen tulipaloilta.

Kvantitatiivisen riskienhallinnan tuloksia ovat kvalitatiiviseen verrattuna muun muassa rahalliset arvot omaisuudelle (assets) sekä numeraalinen arvo todennäköisyyksille.

Kvantitatiivinen ja kvalitatiivinen riskien arviointi koostettuna (Maymí & Harris 2022, 116–117):

- Kvantitatiivinen riskien arviointi pyrkii asettamaan rahalliset arvot eri komponenteille
- Täysin kvantitatiivinen riskien arviointi ei ole mahdollinen, koska kvalitatiivisia ominaisuuksia ei voida kvantifioida tarkasti ja luotettavasti
- Kvalitatiivinen riskien arviointi luottaa numeroiden sijaan intuitioon ja käsitykseen asioista
- Kvalitatiivinen riskien arviointi vaatii siihen osallistuvilta kokemusta ja osaamista, jotta arviointien teko olisi mahdollista ja tuloksiltaan totuuden mukaisia
- Riippumatta valitusta riskien arvioinnin metodista, on tavoitteena tunnistaa riskit sekä arvioida niiden vaikutuksia, tunnistaa haavoittuvuuksia ja uhkia, arvioida potentiaalisia vaikutuksia sekä löytämään tasapaino riskien toteutumisien aiheuttamien kustannusten ja riskien hallintaan käytettävien kustannusten välillä

Riippumatta käytetyistä riskienhallinnan metodeista, tulee riskit käsitellä. Riskien arvioinnin tarkoituksena on siis antaa organisaatioille mahdollisuuksia arvioida häiriöriskejä, jotta organisaatio voi toteuttaa riskien käsittelyyn tarvittavat toimenpiteet (ISO 22313:2020, 36). Toimenpiteitä voidaan nimittää myös vastatoimenpiteiksi (riskejä vastaan) tai kontrolleiksi, joilla riskien todennäköisyyttä ja/tai vakavuutta pyritään pienentämään kustannustehokkaasti siten, etteivät toimenpiteet riskien pienentämiseksi tai poistamiseksi ylitä toteutuvan riskin kustannuksia (Maymí & Harris 2022, 82).

Riskeihin vastaamiseen on neljä peruskeinoa tai strategiaa: riskin siirtäminen, riskin välttäminen, riskin pienentäminen tai riskin hyväksyminen (Wojno, 2022). Riski voidaan siirtää esimerkiksi vakuutuksen kautta vakuutusyhtiölle. Riskin välttäminen tarkoittaa riskin aiheuttavan aktiviteetin tai toiminnon lopettamista kokonaan, jolloin riski ei voi realisoitua.

Riskien pienentäminen sisältää vastatoimenpiteitä ja kontrolleja, joiden tarkoituksena on pienentää riski hyväksyttävälle tasolle. Riskin hyväksyminen on riskien vastaamisen neljäs ja viimeinen keino. Hyväksymisellä tarkoitetaan sitä, että organisaatio ymmärtää riskin tapahtumisen todennäköisyyden sekä mahdolliset vaikutukset kustannuksineen, mutta päättää silti ”elää” riskin kanssa ja olla kohdistamatta siihen vastatoimenpiteitä. Riskin hyväksyminen perusteena voi olla se, että riskin pienentämisen tai poistamisen kustannukset ovat riskin toteutumisen kustannuksia suuremmat (Maymí & Harris 2022, 79).

Riskeihin vastaamisen kontrollityypit ovat jaoteltu kolmeen kategoriaan, hallinnolliset, tekniset ja fyysiset kontrollit. Näistä tyypeistä voidaan vielä johtaa erikseen kuusi eri tyypin turvallisuuskontrollia, jotka ovat (Maymí & Harris 2022, 85):

- Estävät – Estetään tapahtuma (insidentti)
- Havaitsevat – Havaitaan ja tunnistetaan tapahtuma

- Korjaavat – Tapahtuman korjaavat toimenpiteet
- Pidättelevät tai pelotevaikutukset – Lannistetaan potentiaalinen hyökkääjä ja taivutellaan luopumaan hyökkääjä tavoitteestaan
- Palauttavat – Ympäristön täydellinen palauttaminen normaalitoimintoihin
- Korvaavat – Voi olla myös vaihtoehtoinen kontrolli. Tarjotaan vaihtoehtoinen kontrollikeino.

Standardi ISO 22301 (2019, 16–17) asettaa vaatimuksia riskienhallintaprosessille jatkuvuussuunnittelussa. Organisaation on käsiteltävä riskit ja mahdollisuudet, jotta voidaan taata liiketoiminnan jatkuvuuden hallintajärjestelmän asetettujen tulosten saavuttaminen, jotta voidaan estää tai pienentää ei-toivottuja vaikutuksia sekä mahdollistaa jatkuvan parantamisen aikaan saaminen.

Organisaation on myös suunniteltava riskeihin ja mahdollisuuksiin kohdistuvat toimenpiteet sekä yhdistettävä kyseiset toimenpiteet organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän prosesseihin ja toteutettava kyseiset toimenpiteet. Toimenpiteiden vaikuttavuus on arvioitava klausuulinumeron 9.1 (Seuranta, mittaus, analysointi ja arviointi) mukaisesti. Riskienhallinnan vaatimus voidaan toteuttaa esimerkiksi käyttämällä riskienhallintastandardia ISO 31000, sillä ISO 22301 ei sisällä ohjeistusta riskienhallinnalle.

3.5 Liiketoiminnan vaikutusanalyysi

Esimerkiksi BSI 100-4 standardi määrittelee liiketoiminnan jatkuvuusanalyysin (BIA, Business Impact Analysis) analyysina, jonka tarkoituksena on määrittää mahdolliset suorat ja epäsuorat vahingot organisaatiolle, mikäli jokin haitallinen tapahtuma yhdessä tai useammassa organisaation liiketoiminnan prosessissa toteutuisi (BSI-Standard 100–4, 103). BIA-analyysin avulla tunnistetaan kriittiset liiketoiminnan prosessit sekä määritellään näiden prosessien saatavuusvaatimukset ja resurssit, joita ne vaativat toimiakseen (BSI-Standard 100–4, 10).

Myös ISO 22301:n toteuttamista ohjaava standardi, ISO 22313:2020, kuvailee BIA-prosessia samoin, lisäten vielä priorisoinnin näkökulmaa prosesseissa. BIA-analyysi mahdollistaa häiriölle altistuneiden toimintojen jatkamisen. BIA-analyysin tarkoituksena on mahdollistaa organisaation kyky tunnistaa ja luokitella toimintonsa. Priorisoinnin tarkoituksena on luokitella toiminnot siten, että ensisijaisiksi luokitellut toiminnot tunnistetaan, ja niiden häiriytyessä niihin voidaan kohdistaa nopeita toimenpiteitä häiriön vaikutusten pienentämiseksi tai poistamiseksi ja häiriöiden vaikutusten alaisten toimintojen nopeaan uudelleen käyttöönottoon (ISO 22313:2020, 32).

Myös muita kuin ensisijaisia toimintoa on mahdollista priorisoida (ISO 22313:2020, 32), ja lopputuloksena voisi olla esimerkiksi kuvion 7 mukainen kolmiportainen luokittelu, jossa niin sanotun ykköprioriteetin toimintoja ovat organisaation toiminnan kannalta välttämättömät tuotteet, palvelut ja tehtävät sekä niitä tukevat toiminnot ja resurssit, joiden toiminnan jatkuvuuden varmistaminen on etusijalla. Tätä seuraisivat toiminnot, joiden toiminnan jatkuvuus varmistetaan, kun prioriteetin 1 toiminnoista on ensin huolehdittu. Kolmantena olisivat toiminnot, joiden toiminnan jatkuvuus varmistetaan, kun prioriteetin 2 toiminnoista on ensin huolehdittu (Digi- ja väestötietovirasto. 2022).

A1. Tuotosten priorisointi varautumisen ja toiminnan jatkuvuuden näkökulmasta (arvot säädettäviä)		
Kriittisyysluokka (1,2,3)	**Kuvaus**	**Kriittisyysluokkien rajat (yläraja 4)**
1	Tuotteet, palvelut ja tehtävät sekä niitä tukevat toiminnot ja resurssit, joiden toiminnan jatkuvuuden varmistaminen on etusijalla.	3,3
2	Tuotteet, palvelut ja tehtävät sekä niitä tukevat toiminnot ja resurssit, joiden toiminnan jatkuvuus varmistetaan, kun prioriteetin 1 toiminnoista on ensin huolehdittu.	2
3	Tuotteet, palvelut ja tehtävät sekä niitä tukevat toiminnot ja resurssit, joiden toiminnan jatkuvuus varmistetaan, kun prioriteetin 2 toiminnoista on ensin huolehdittu.	0

Kuvio 7. Digi- ja väestötietoviraston ”Kriittisten kohteiden luokittelu” -työkalun luokitteluasteikko tuotosten priorisointiin (Digi- ja väestötietovirasto. 2022).

ISO 22313:n mukaan organisaatiot voivat käyttää omia termistöjään ja priorisointijärjestyksiään, ja prioriteettien määrittelyn voisi tehdä myös käyttäen termejä kuten kriittinen, välttämätön, elintärkeä ja keskeinen (ISO 22313:2020, 32). Prioriteettilistaus tai kriittisyysluokkien määritelmä voi olla myös kolmiportaisen sijaan esimerkiksi neli- tai viisiportainen ja käytettyjä kriittisyysluokkien rajoja voidaan määritellä eri tavoin. Jokainen organisaatio kuvaa toimintansa omalla tavallaan.

BIA-analyysin olisi katettava kaikki liiketoiminnan hallintajärjestelmän soveltamisalaan kuuluvat toiminnot. Maymí & Harris (2022, 109) kuvaavat BIA-analyysiä toiminnallisena analyysinä, jossa liiketoiminnan vaikutusanalyysiä suorittava ryhmä kerää tietoa arvioitavasta kohteesta haastatteluiden ja dokumentaatioiden kautta, dokumentoi liiketoiminnot ja -aktiviteetit, muodostaa liiketoimintojen välisen hierarkian ja viimeisenä muodostaa ja toteuttaa luokittelujärjestelmän, jonka avulla muodostetaan kriittisyysluokittelu toimintojen välille.

BIA-analyysit olisi hyvä toteuttaa yhteistyössä analyysin kohteena olevan palvelun tai toiminnon asiantuntijoiden kanssa, sillä heillä on analyysin kohteesta todennäköisesti parhain tietämys, eikä BIA-analyysi ole pelkän arvioijan, esimerkiksi konsultin, varassa. Näin voidaan luotettavimmin määrittää analyysin kohteeseen mahdollisesti kohdistuvat vaikutustyypit (Maymí & Harris. 2022, 109). ISO 22313-standardin (2020, 36) mukaan BIA-analyysin tieto voi olla peräisin haastatteluista, kyselyistä, työpajoista tai muista sisäisistä ja ulkoisista lähteistä.

Vaikutustyyppejä, joita voidaan kutsua myös vaikutusluokiksi, voivat olla molempien Maymín & Harriksen (2022, 109) sekä ohjaavan standardin ISO 22313 (2020, 34) mukaan seuraavat:

- Taloudellinen – Rahalliset tappiot voivat syntyä sakoista, menetetyistä voitoista tai pienentyneestä markkinaosuudesta
- Mainehaitta – Yrityksen tai organisaation maine tai brändi vahingoittuu
- Toiminnallinen – Liiketoimintoihin ja/tai sen osiin kohdistuva häiriön laajuus ja häiriön kesto
- Lakeihin tai viranomaisvaatimuksiin liittyvä – Riski joutua oikeuteen ja jopa menettää liiketoimintalupa
- Sopimuksellinen – Organisaatioiden välisen velvoitteen täyttämättä jättäminen tai sopimusrikko.
- Liiketoimintatavoitteet – Tavoitteiden täyttämisen tai mahdollisuuksien hyödyntämisen epäonnistuminen.

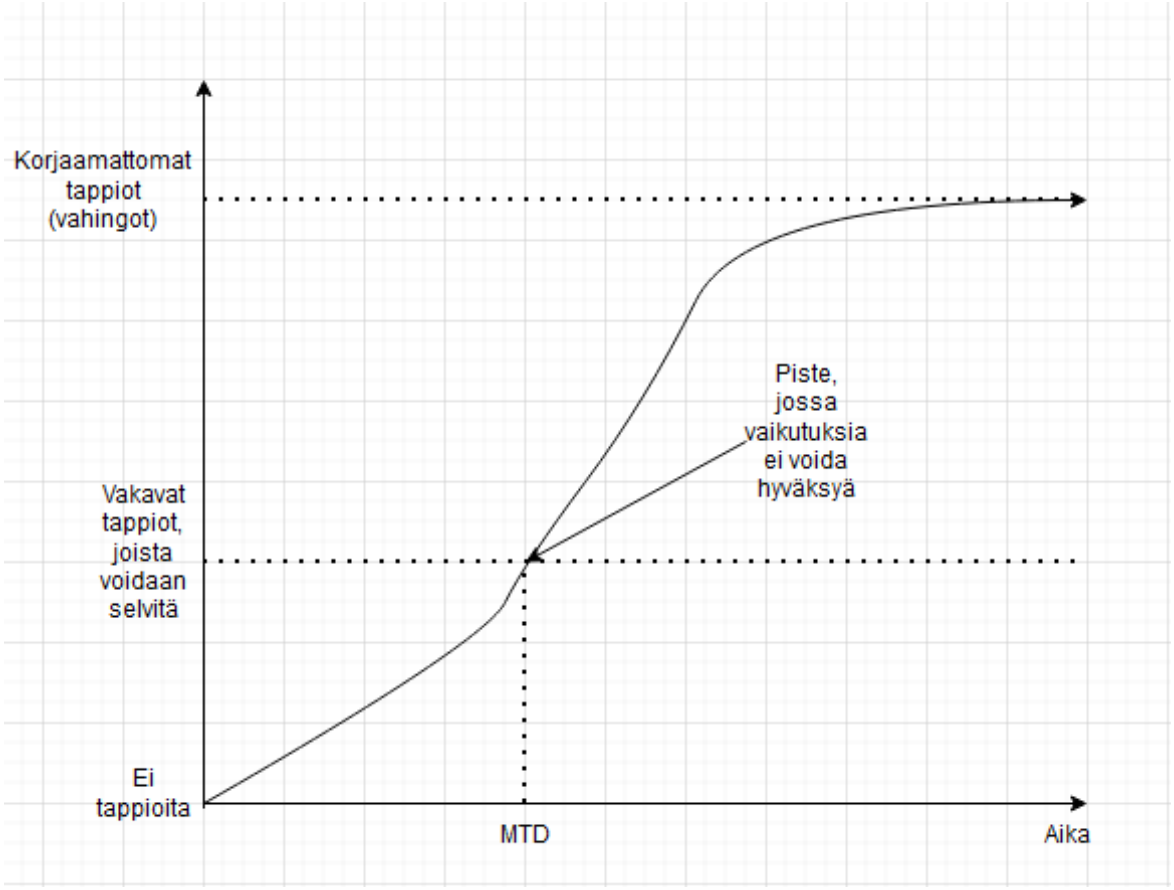
ISO 22301 asettaa liiketoiminnan vaikutusanalyysille 8 vaatimusta ja standardin mukaiset vaatimukset ovat (ISO 22301:2019, 20):

1. Liiketoiminnan vaikutusanalyysiprosessissa on määriteltävä olennaisimmat vaikutustyypit ja kriteerit organisaation toimintaympäristön kannalta.
2. Tunnistettava tukevat toiminnot tuotteiden ja palveluiden toimittamiseen.
3. Käytettävä määriteltyjä vaikutustyyppejä ja kriteerejä (kohdan 2) toimintojen häiriöistä syntyvien vaikutusten arviointiin ajan kuluessa (1pv, 2pv, 7pv, 14pv jne.).
4. Tunnistettava aikaväli, jonka kuluessa toimintojen pysähtymisestä johtuvat vaikutukset muuttuvat organisaatioille kestämättömiksi – Tästä aikavälistä voidaan käyttää myös termiä ”pisin siedettävä häiriön kesto” (MTPD tai MTD).

5. On asetettava kohdassa 4 tunnistetun aikavälin sisälle sellaiset aikataulut, joiden mukaisesti toiminnot voidaan priorisoidusti saada jälleen käynnistettyä määritellyllä hyväksyttävissä olevalla tasolla – Tästä aikavälistä voidaan käyttää myös termiä ”palautumisaikatavoite” (RTO).
6. On tunnistettava ensisijaiset toiminnot BIA-analyysin avulla.
7. Määritettävä tarvittavat resurssit ensisijaisten toimintojen tueksi – Esimerkiksi ihmiset, tieto (data), rakennukset, välineistöt, ICT-järjestelmät, logistiikka.
8. On määritettävä riippuvuussuhteet: Yhteistyökumppanit, toimittajat ja kohdassa 6 tunnistettujen ensisijaisten toimintojen keskinäiset riippuvuussuhteet – Esimerkiksi hankinta on riippuvainen rahoituksesta.

Standardin asettamia vaatimuksia ei ole pakko toteuttaa, ellei tavoitteena ole ISO 22301-standardin mukainen sertifiointi. Organisaatiot voivat soveltaa ohjeistuksia ja vaatimuksia itselleen soveltuvin tavoin.

Kuvio 8 kuvaa BIA-analyysin 4. vaatimusta, pisintä siedettävää käyttökatkoa, josta voidaan käyttää lyhenteitä MTPD (maximum tolerable period of disruption) sekä myös MTD (maximum tolerable downtime), jotka molemmat kuvaavat pisintä siedettävää liiketoimintaprosessien käyttökatkoa tai toiminta-aikakatkoa.

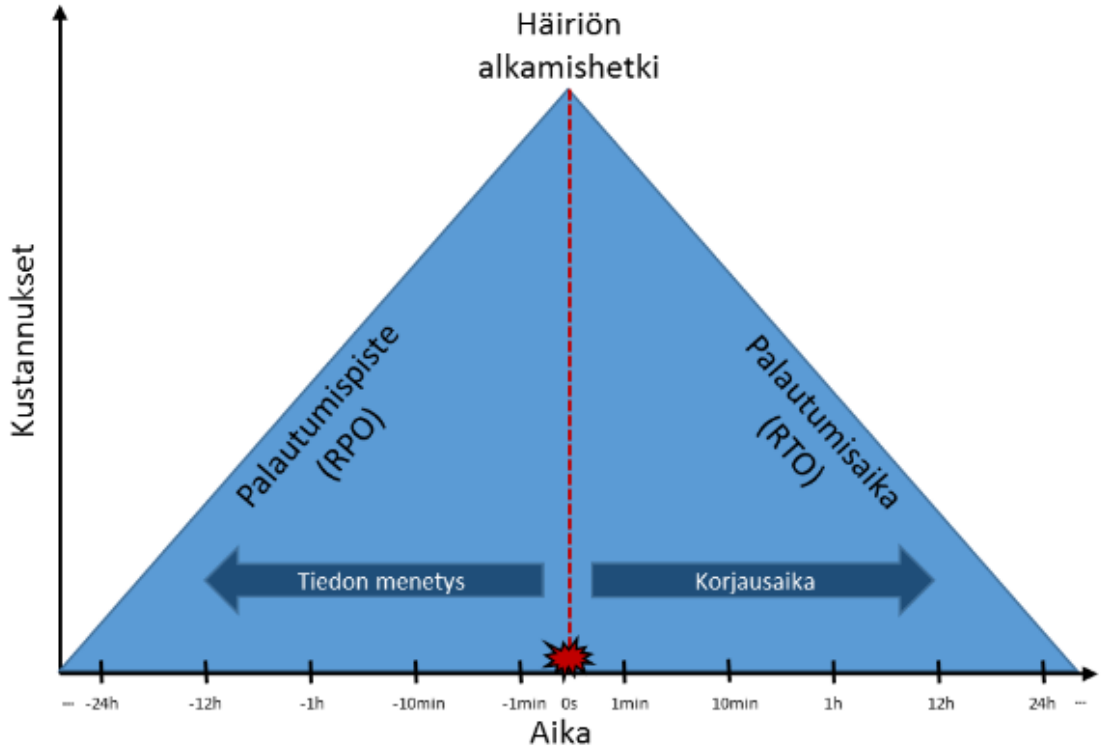


Kuvio 8. Suurin sallittu käyttökatko. Maximum Tolerable Downtime, MTD (Maymí & Harris. 2022, 114).

Kuviosta 8 nähdään tappioiden kasvu ajan kuluessa. BIA-analyysissä tulisi määrittää piste, jonka jälkeisiä vaikutuksia ei enää voida hyväksyä ja palautumistoimien tulisin olla määritetty siten, että palautuminen toteutetaan ennen MTPD- tai MTD-pistettä. Määritetyn pisteen jälkeen tappiot voivat kasvaa niin nopeasti niin suuriksi, ettei yritys tai organisaatio voi enää toipua niistä. Vaikutukset voivat olla mitä tahansa aiemmin esitetyistä vaikutustyypeistä. Mitä lyhyempi tai pienempi MTD-arvo on, sitä korkeampi palautusprioriteetti kyseisellä toiminnolla on (Maymí & Harris. 2022, 114). MTD-arvo voidaan ilmaista esimerkiksi minuuteissa, tunneissa, päivissä tai viikoissa.

Palautumisaikatavoite (RTO, recovery time objective), määrittää ajan, jossa palautumistoimet tulisi suorittaa. Kuvio 9 havainnollistaa kustannusten nousun suhteessa palautumisaika- ja palautumispistetavoitteisiin (RPO, recovery point objective). Mitä nopeammin pyritään palautumaan ja mitä lyhyemmältä ajalta tietoa halutaan menettää, sitä suuremmaksi taloudelliset kustannukset nousevat.

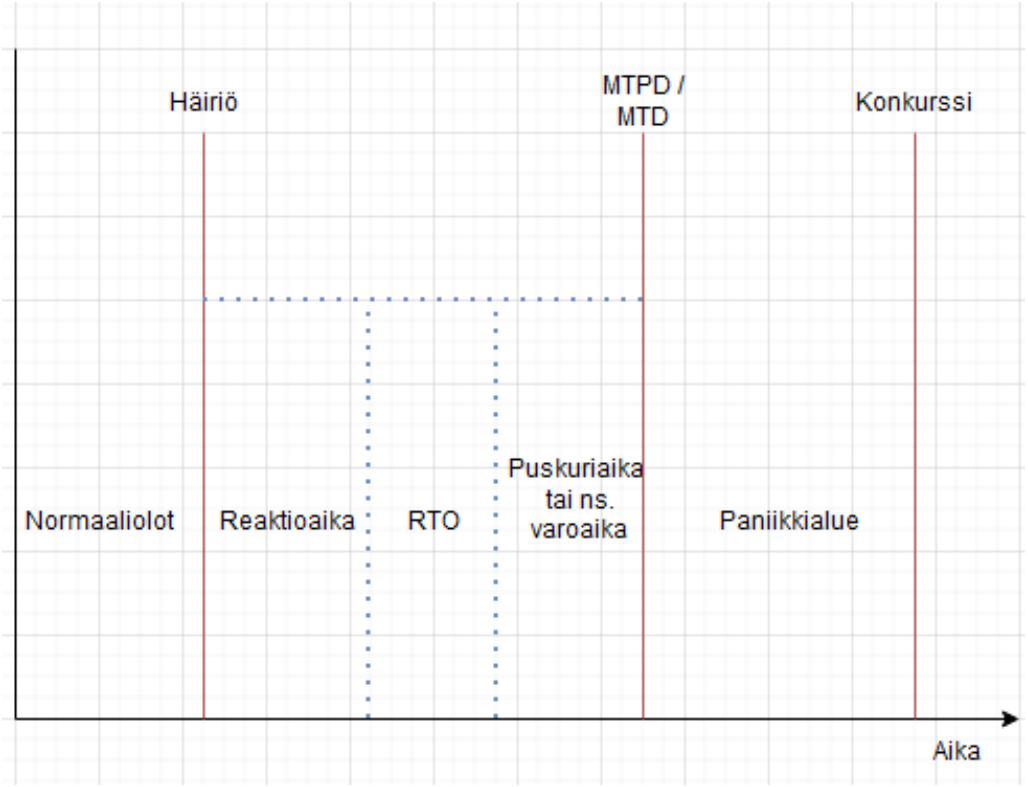
Esimerkiksi korkean käytettävyyden ratkaisut, jotka voivat olla kahdennettuja ympäristöjä tai maantieteellisesti hajautettuja ratkaisuja, nostavat kustannuksia ja takaavat nopeamman palautumisen (Vahti 2/2016, 48). Palautumispisteeksi (RPO) voidaan olla määritelty esimerkiksi kaksi minuuttia, jolloin tietoa ei tulisi menettää yli kahden minuutin ajalta.



Kuvio 9. Palautumispiste (RPO) ja palautumisaika (RTO). Kustannusten ja ajansuhde määriteltäessä palautumistavoitteita (Vahti 2/2016, 48).

Palautumispisteen määrittely ei ole aina tarpeellinen. Esimerkiksi jos palautettava järjestelmä ei sisällä itsessään dataa, jolloin ei menetetä tietoakaan. Kaikkia arvoja määritellessä tulee huomioida palvelutasosopimukset ja mahdolliset vasteaika- ja ratkaisuaikavaateet (Vahti 2/2016, 49).

Kuvio 10 havainnollistaa termien RTO ja MTPD / MTD erot ja sen, miksi niitä ei määritellä samaksi, vaikka niiden voisi kuvitella voivan merkitsevän samaa asiaa.



Kuvio 10. Häiriön aikajana, palautumisaikatavoitteen RTO ja pisimmän siedettävän käyttökatkon MTPD suhde toisiinsa (Hübert, R. 2011).

Kun häiriö tapahtuu, kestää siihen reagoinnissa aina jokin määrä aikaa, ennen kuin palautumistoimenpiteet alkavat. Tätä kuvataan kuviossa 10 reaktioaikana. RTO-arvo tulisi määritellä MTPD-arvoa pienemmäksi, jotta palautumisaikatavoitteen ja pisimmän siedettävän käyttökatkon välille jäisi vielä aikaa, mikäli palautumistoimenpiteiden tavoitteita ei saavuteta oletetussa tai tavoitellussa ajassa. Näin voidaan parhaiten varmistaa se, että palautumistavoitteet saavutetaan ennen kuin tappioiden suuruus saavuttaa pisteen (MTPD), jota ei voida hyväksyä.

Paniikkialueeksi nimetty ajanjakso häiriön aikajanalla kuvaa määritellyn pisimmän siedettävän käyttökatkon jälkeistä aikaa, jonka aikana tappiot voivat kasvaa niin nopeasti niin suuriksi, että organisaation toiminta voi jopa lakata kokonaan (konkurssi). Tällöin tappiot ovat nousseet niin suuriksi, että saavutetaan kuvan 8 mukainen korjaamattomien tappioiden tai vahinkojen piste.

Esimerkiksi käyttäen apuna Digi- ja väestötietoviraston, DVV:n, kriittisten kohteiden luokittelun työkalua (Digi- ja väestötietovirasto. 2022) sekä standardin ISO 22301:2019 asettamia vaatimuksia liiketoiminnan vaikutusanalyysille, voidaan BIA-analyysin tiedonkeruun aiheille johtaa esimerkkikysymyksiä taulukon 1 mukaisesti:

Taulukko 1. Esimerkkikysymyksiä ja -aiheita liiketoiminnan vaikutusanalyysin kyselyssä.

Aihe:	**Esimerkkikysymyksiä:**
Resurssit (tuotannontekijät)	Mitä resursseja (prosessi, tietojärjestelmä, toiminto, muu) toiminnan palauttaminen vaatii? Mitä muut toiminnot vaativat jatkaakseen? Mitkä palautumisen resurssit tulevat organisaation ulkopuolelta?
Sidosryhmät	Mitkä sidosryhmät ovat riippuvaisia toiminnosta? Mistä sidosryhmistä toiminto on riippuvainen? Millaisia palvelutasosopimuksia (SLA) on olemassa?
Palautustiedostot (RPO)	Kuinka usein palautuspisteitä luodaan? Kuinka varmuuskopiot palautetaan?
Riippuvuudet	Mistä toiminnoista tämä toiminto on riippuvainen? Mitkä toiminnot ovat riippuvaisia tästä toiminnosta?
Toiminnon palauttaminen	Mitä toimenpiteitä palauttaminen vaatii? Mitä resursseja palauttaminen vaatii? Vaatiiko toimintojen palauttamisen testaaminen testiympäristön? Vaatiiko toimintojen palauttaminen varotoimenpiteitä? Missä ajassa toiminto tulisi palauttaa?

Vasemmassa sarakkeessa ovat kyselyn, haastattelun tai työpajan aiheet tai teemat. Oikeassa sarakkeessa on esimerkkikysymyksiä. Tiedonkeruun aiheet vaihtelevat prosessien ja toimintojen mukaisesti, joten liiketoiminnan vaikutusanalyysissä voidaan esimerkiksi jättää käsittelemättä palvelutasosopimukset, mikäli toimintoon tai sen palauttamiseen ei liity ulkoisia toimijoita.

Betan, H. (2010) mukaan liiketoiminnan vaikutusanalyysissä tehtävän kyselyn kysymyksien tulisi olla hieman epämääräisiä, jolloin kysely sopii tarvittaessa useampaan eri palvelun tai toiminnon arviointiin. Epämääräiset kysymykset myös pakottavat vastaajan vastaamaan kysymyksiin paremmalla tarkkuudella ja kattavammin lyhyiden vastausten sijaan.

Liiketoiminnan vaikutusanalyysin vaiheet, vielä summattuna, ovat Maymín & Harriksen (2022, 114) mukaan seuraavat:

1. Valitse osallistujat tiedonkeruun vaiheeseen.
2. Luo tiedonkeruun tekniikat, joita voivat olla esimerkiksi kyselyt, kyselylomakkeet sekä kvalitatiiviset ja kvantitatiiviset lähestymistavat.
3. Tunnista organisaation kriittiset toiminnot.
4. Tunnista resurssit, joista kriittiset toiminnot ovat riippuvaisia.
5. Laske, kuinka kauan kriittiset toiminnot voivat selviytyä ilman tunnistettuja resursseja.
6. Tunnista toimintoihin kohdistuvat uhkat ja haavoittuvuudet.
7. Laske jokaisen eri liiketoimintoihin kohdistuvat riskit.
8. Dokumentoi löydökset ja raportoi niistä johdolle.

Teknisessä spesifikaatiossa ISO/TS 22317 on liiketoiminnan vaikutusanalyysin suorittamista koskevaa lisäohjeistusta. Kyseisessä spesifikaatiossa esitetään vaiheittainen toimintamalli standardissa ISO 22301 esitettyjen vaatimusten täyttämiseen (ISO 22313, 33).

Tässä vaiheessa on vielä hyvä kerrata riskien arvioinnin ja liiketoiminnan vaikutusanalyysin ero lyhyesti. Riskien arvioinnissa analysoidaan potentiaalisia uhkia ja niiden todennäköisyyksiä. BIA-analyysi mittaa ja arvioi uhkien toteutumisien vakavuutta sekä kuinka ne voisivat vaikuttaa liiketoimintoihin ja muun muassa talouteen (vaikutustyypit). BIA-analyysi onkin siis tavallaan jatke riskien arvioinnille. BIA-analyysissä tunnistetaan potentiaaliset riskit, jonka lisäksi mitataan niiden vaikutuksia (MacNeil, C. 2022).

3.6 Varautuminen

Valmiuslain (1552/2011, 12 §) mukaan muun muassa valtion hallintoviranomaisilla, Valtioneuvostolla, hyvinvointialueilla (1.1.2023 alkaen) sekä muilla valtion viranomaisilla on valmiuslain perusteella velvollisuus varautua hoitamaan tehtävänsä myös poikkeusoloissa. Velvollisuus voi koskea myös julkishallintoon palvelusopimussuhteessa olevia yrityksiä niiden tuottaman palvelun osalta (Vahti 2/2012). Poikkeusolojen suhde normaalioloihin ja normaaliolojen häiriötilanteisiin voitiin nähdä kuviossa 2. Poikkeusoloilla tarkoitetaan valmiuslain 3 § mukaan:

1. *Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila.*
2. *Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii tämän lain mukaisten toimivaltuuksien välitöntä käyttöön ottamista*
3. *Väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat*
4. *Erityisen vakava suuronnettomuus ja sen välitön jälkitila*
5. *Vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti sekä*
6. *Sellainen*

   a) julkisen vallan päätöksentekokykyyn

   b) rajaturvallisuuden tai yleisen järjestyksen ja turvallisuuden ylläpitämiseen

   c) välttämättömien sosiaali- ja terveydenhuollon tai pelastustoimen palvelujen saatavuuteen

   d) energian, veden, elintarvikkeiden, lääkkeiden tai muiden välttämättömien hyödykkeiden saatavuuteen

   e) välttämättömien maksu- ja arvopaperipalvelujen saatavuuteen

   f) yhteiskunnallisesti kriittisten liikennejärjestelmien toimivuuteen tai

   g) edellä a–f alakohdassa lueteltuja toimintoja ylläpitävien tieto- ja viestintäteknisten palvelujen tai tietojärjestelmien toimivuuteen

   kohdistuva uhka, toiminta, tapahtuma tai näiden yhteisvaikutus, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti ja laajamittaisesti estyvät tai lamaantuvat tai joka muulla näihin vakavuudeltaan rinnastuvalla tavalla erityisen vakavasti ja olennaisesti vaarantaa yhteiskunnan toimintakykyä tai väestön elinmahdollisuuksia.

Poikkeusolot astuvat voimaan, kun Tasavallan presidentti yhdessä Valtioneuvoston kanssa toteaa maassa vallitsevan poikkeusolot (Valmiuslaki 1552/2011, 6 §).

Varautumista voidaankin kuvailla toimintana, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen sekä mahdolliset tarvittavat, tavanomaisesta poikkeavat toimenpiteet normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumistoimenpiteitä ovat esimerkiksi valmiussuunnittelu, jatkuvuudenhallinta, erilaiset etukäteisvalmistelut, koulutukset sekä valmiusharjoitukset. Valmiuslain (1552/2011) lisäksi varautuminen perustuu pelastuslakiin (379/2011) ja muun erityislainsäädännön varautumisvelvollisuuteen (Yhteiskunnan turvallisuusstrategia. 2017, 9).

Varautumistoimenpiteissä on listattuna jatkuvuudenhallinta. Termit varautuminen ja jatkuvuudenhallinta ovatkin melkein synonyymejä toisilleen eikä niitä erotella sen tarkemmin. Liiketoiminnan jatkuvuudenhallinnan standardi ISO 22301:2019 käyttää termiä varautuminen kaksi kertaa. Ensimmäisen kerran standardi mainitsee varautumisen ensimmäisessä luvussa, jossa termillä viitataan häiriöihin varautumiseen. Toisen kerran standardi mainitsee varautumisen luvun 3.6 alahuomautuksessa 1, jossa standardin mukaan myös yrityksiltä voidaan edellyttää varautumista poikkeusoloihin, joko jatkuvuussuunnitelmien osana tai erillisellä valmiussuunnitelmalla. Varautumisen ja jatkuvuudenhallinnan termit ovat erilaisia, mutta ne ovat olemukseltaan samankaltaisia.

Varautumisen päämäärät ovat osittain samat kuin jatkuvuudenhallinnassa, mutta ne voidaan silti eritellä toisistaan esimerkiksi mainitulla valmiussuunnitelmalla, jota voidaan pitää varautumisen tuotoksena aivan kuten jatkuvuussuunnitelmia voidaan pitää jatkuvuudenhallinnan tuotoksina. Varautumisen päämääriä ovat huolehtia onnettomuuksien sekä häiriötilanteiden ehkäisystä, valmistautumisesta toimintaan onnettomuuksien tai häiriötilanteiden uhatessa tai sattuessa sekä myös toipumisen suunnittelu (Yhteiskunnan turvallisuusstrategia. 2017, 9). Toimintaa pyritään jatkamaan mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa valmiussuunnitelmin, etukäteisvalmisteluin ja muilla tarvittavilla toimenpiteillä.

Yksi esimerkki muista tarvittavista toimenpiteistä toimijalle taikka organisaatioille poikkeusolojen varautumiseen voisivat olla sen henkilöstön jäsenien varaaminen töihin myös poikkeusoloissa. Toimenpidettä, jolla tämä toteutetaan, kutsutaan henkilövaraamiseksi (Puolustusvoimat. N.d), joka tunnetaan myös lyhenteellä VAP, eli vapautettu aseellisesta palveluksesta sodan aikana (VAHTI 2/2016, 25). Yhteiskunnan häiriöttömän toiminnan kannalta kriittiset organisaatiot, sekä niille

kriittisiä palveluita toimittavat tahot, voivat esittää varattavaksi henkilöstöään jatkuvuuden varmistamiseksi poikkeusoloissa (VAHTI 2/2016, 25). Puolustusvoimien aluetoimistot ratkaisevat asevelvollisia koskevat varaushakemukset (Puolustusvoimat. N.d).

Varautumisen prosessissa kuviossa 11 voidaan havaita hyvinkin paljon yhteistä liiketoiminnan jatkuvuudenhallinnan kanssa:

Kuvio 11. Varautumisen yleinen prosessi (Yhteiskunnan turvallisuusstrategia. 2017, 9).

Myös yhteiskunnan turvallisuusstrategiassa kuvattu prosessimalli perustuu jatkuvaan kehittämiseen (palaute), ja kuvasta voidaan myös huomata PDCA-mallista tuttuja termejä, kuten suunnittelu (plan) ja toiminta (do). Myös varautumisessa otetaan huomioon elintärkeitä toimintoja, tehdään riski- ja resurssiarviota sekä harjoitellaan, koulutetaan sekä testataan. Yhteiskunnan turvallisuusstrategian (2017, 10) mukaan myös varautumisessa, kuten jatkuvuudenhallinnassa, pyritään reagoinnin sijaan ennakointiin.

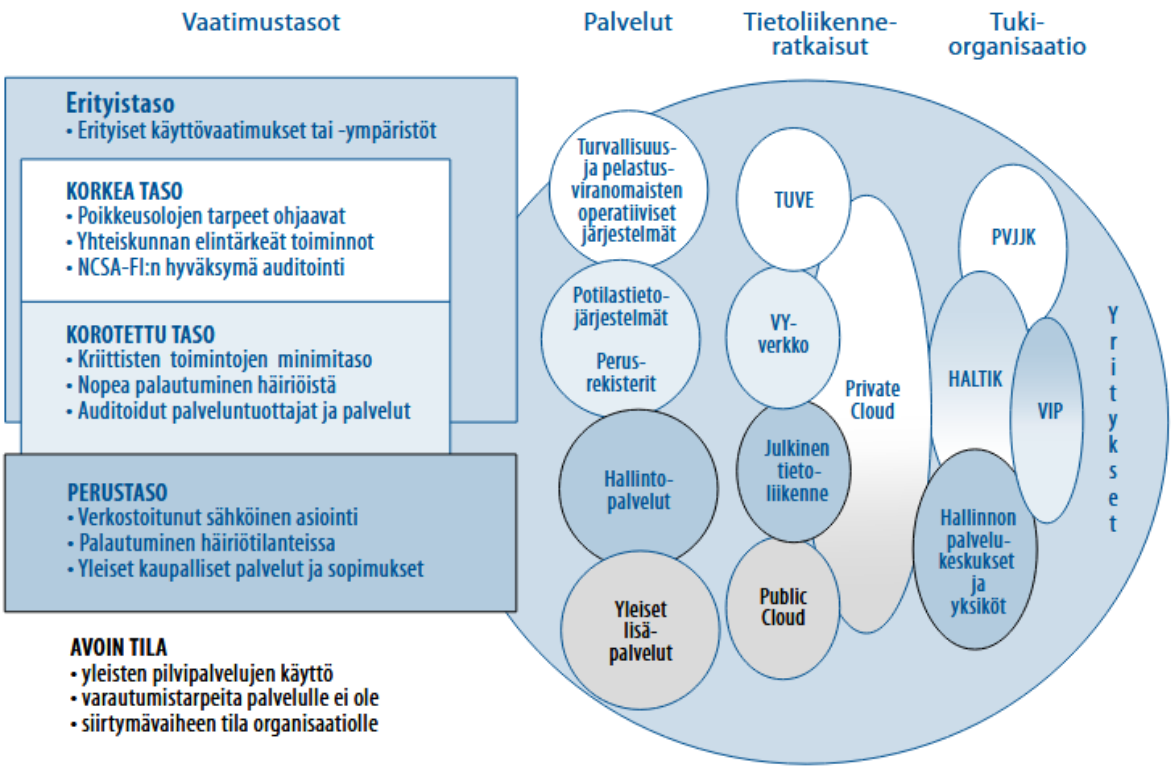
Mikäli toimijalla tai organisaatiolla on varautumislain mukainen varautumisvelvollisuus, tai toimija tai organisaatio muuten haluaa varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin, voivat ne saada apua riskienhallintaansa, uhkamalleihin ja mahdollisiin häiriötilanteisiin Yhteiskunnan turvallisuusstrategian (2017) lisäksi muun muassa julkaisuista ”Kansallinen riskiarvio 2018” (2018) sekä ”Viranomaisten toimivaltuudet häiriötilanteissa” (2019).

Esimerkiksi kansallisen riskiarvion laadinnassa on hyödynnetty paljon jo tehtyjä eri toimijoiden tekemiä riskiarvioita tai vastaavia prosesseja. Kansallinen riskiarvio on käytännössä yhteen sovitettu kooste eri toimijoiden omista riskiarvioista. Eri hallinnonalat ovat valinneet vaikuttavia uhkamalleja sekä häiriötilanteita, jotka voivat kohdistua yhteiskunnan elintärkeisiin toimintoihin kansallisella tasolla (Sisäministeriö. 2019).

Kansallinen riskiarvio (2018) listaa yhtenä yhteiskunnan turvallisuuteen liittyvänä uhkamallina ja häiriötilanteena tietoliikenteen ja tietojärjestelmien häiriöt, mukaan lukien kyberuhkat (Sisäministeriö. 2019, 48). Kansallisessa riskiarviossa (2018, 48) tietoliikenteeseen ja tietojärjestelmiin kohdistuvien häiriöiden arvioidaan voivan vaikuttaa hyvinkin vakavasti lähes kaikkiin yhteiskunnan elintärkeisiin toimintoihin, kuten johtaminen ja sisäinen turvallisuus. Tietoliikennehäiriöitä vakavampana uhkana pidetään Oikeusministeriön julkaiseman Viranomaisten toimivaltuudet häiriötilanteissa (2019, 28) mukaan vain Suomeen kohdistuvaa sotilaallisen voiman uhkaa.

Viranomaisten toimivaltuudet häiriötilanteissa (2018) tulkitseekin viranomaisten häiriönhallinnan näkökulmasta sekä Kansallisen riskiarvion sekä Yhteiskunnan turvallisuusstrategia -julkaisuja ja voi auttaa julkaisujen ymmärtämisessä, esimerkiksi eri uhkien, uhkien kohteiden, ja uhkien toteutumistapojen tulkinnassa.

Varautumista voidaan tehdä eri tasoilla, ja Valtiovarainministeriön julkaisu Vahti 2/2012 antaakin ohjausta ICT-palveluiden varautumiseen ja sen tasoihin julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille, liittyen yritysten tuottamiin palveluihin. Kuvio 12 kuvaa ICT-varautumisen tasoja.



Kuvio 12. ICT-varautumisen vaatimustasot. Vahti 2/2012, 21.

Tasoja ei avata tässä opinnäytetyössä tarkemmin. Vaatimustasojen esittelyn tarkoituksena on tuoda esille varautumisen tasojen ja siihen ohjeistavan julkaisun olemassaolo. Vahti 2/2012-ohjeen mukaan (2012, 19) vaatimusten muodostamisen viitekehyksenä on hyödynnetty yleisesti käytettyjä EFQM (European Foundation for Quality Management) ja CAF (Common Assessment Framework) laadunarviointimalleja, sekä vaatimuksissa ISO 27001 ja 22301-standardeja, joten Vahti-ohjeen käyttö tarvittaessa on tässäkin mielessä perustelua, sekä mahdollisimman yhteensopivaa liiketoiminnan jatkuvuuden hallintajärjestelmän standardin, ISO 22301, kanssa.

Vaatimustasojen tarkoituksena on ohjata organisaatioita kehittämään toimintaansa, sen tuottamia palveluja sekä omistamiaan järjestelmiä, ja varautumaan erilaisiin uhkatilanteisiin ja ennalta ehkäisemään häiriöiden syntymistä eri tasoilla. ICT-varautumisen tasojen avulla myös yhtenäistetään varautumistoimenpiteitä, jotta verkostoituneessa toiminnassa tunnettaisiin eri osien edellytykset kestää häiriötilanteita (Vahti 2/2012, 19–20).

4 ISO 22301:2019, Vahti-ohjeet & KATAKRI 2020

Tässä luvussa käydään läpi opinnäytetyön olennaisinta tietoperustaa, standardia ISO 22301:2019. Case-organisaation liiketoiminnan jatkuvuuden hallintajärjestelmä toteutetaan kyseisen standardin vaatimusten mukaisesti sertifioinnin mahdollistamiseksi tulevaisuudessa ja siksi standardin rakennetta ja periaatetta on syytä avata. Luvussa käydään läpi myös standardin asettamat vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmälle, sekä niin sanotut voidaan-vaatia-tiedot, joita voidaan tarvittaessa vaatia dokumentoituna tietona, jotta voidaan varmistua liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuudesta. Lopuksi käsitellään lyhyesti ISO-standardien soveltamaa PDCA-mallia ja kuinka liiketoiminnan jatkuvuuden hallintajärjestelmän rakenne suhteutuu PDCA-malliin.

Luvussa käydään myös läpi kansallista auditointikriteeristöä Katakria keskittyen sen turvallisuusjohtamisen osioon, jossa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen. Luvussa esitellään myös lyhyesti Vahti-ohjeistuksia ja niiden tuottamisesta vastaavaa tahoa.

4.1 ISO 22301:2019-standardi

ISO 22301-standardi on yleispätevä lähestymistapa organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän toteutukseen ja käyttöönottoon. Standardissa määritellään jatkuvuuden hallintajärjestelmän rakenne sekä vaatimukset hallintajärjestelmän toteuttamiselle ja ylläpidolle (ISO 22301:2019, 5). Koska ISO 22301-standardi ohjaa tässä opinnäytetyössä liiketoiminnan jatkuvuuden hallintajärjestelmän kehitystä, tutustutaan standardiin hieman tarkemmin. Opinnäytetyössä käydään läpi kyseisen standardin yleisperiaatetta, rakennetta, painotuksia, vaatimuksia sekä esitellään lopuksi ISO-standardien käyttämää PDCA-mallia.

ISO 22301-standardi määrittelee liiketoiminnan jatkuvuuden hallintajärjestelmän rakenteen, sekä hallintajärjestelmän toteuttamista ja ylläpitämistä koskevat vaatimukset. Standardi ei anna varsinaisia konkreettisia toteutusohjeita, vaan kuvaa vaatimukset yleisellä tasolla. ISO 22301-standardi noudattaa ISO:n hallintajärjestelmiä koskevia vaatimuksia. Vaatimuksiin sisältyvät hallintajärjestelmästandardien yleisrakenne ja vakiotekstit, yhteiset termit sekä keskeiset määritelmät. ISO 22301-

standardin osia voidaan yhdistää ja yhdenmukaistaa myös muihin hallintajärjestelmiin, kuten ISO 27001:en (ISO 22301:2019, 7).

ISO 22301-standardin mukaiseen liiketoiminnan jatkuvuuden hallintajärjestelmään sisältyvät seuraavat tekijät (ISO 22301:2019, 5):

- Toimintaperiaatteet
- Pätevät henkilöt, joille on määritelty vastuita
- Hallintaprosessit, jotka liittyvät
    - toimintaperiaatteisiin
    - suunnitteluun
    - toteutukseen ja käyttöön
    - suorituskyvyn arviointiin
    - johdon katselmukseen
    - jatkuvaan parantamiseen
- Dokumentoitu tieto, joka tukee toiminnan ohjausta ja mahdollistaa suorituskyvyn arvioinnin

ISO 22301:2019-standardi koostuu 10 luvusta, joista kolme ensimmäistä lukua kuuluvat johdantoon ja loput luvut (4–10) ovat liiketoiminnan jatkuvuuden hallintajärjestelmän ymmärtämisen ja toteuttamisen lukuja. Standardin luvut ovat:

1. Soveltamisala
2. Velvoittavat viittaukset
3. Termit ja määritelmät
4. Organisaation toimintaympäristö
5. Johtajuus
6. Suunnittelu
7. Tukitoiminnot
8. Toiminta
9. Suorituskyvyn arviointi
10. Parantaminen

ISO 22301-standardin jatkuvuuden hallintajärjestelmälle vaatimuksia asettavat luvut 4–10 ja niiden sisältö on tiivistetysti taulukossa 2.

Taulukko 2. ISO 22301:2019-standardin vaatimuksia liiketoiminnan jatkuvuuden hallintajärjestelmälle asettavat luvut ja niiden sisältö tiivistetysti.

Luku	**Sisältö**
Luku 4 – Organisaation toimintaympäristö	Luvussa esitetään vaatimukset jatkuvuudenhallintajärjestelmän toimintaympäristön määrittämiseksi. Toimintaympäristö voi olla ulkoinen tai sisäinen. Sidosryhmien tarpeet tulee tunnistaa. Lakien ja viranomaisten vaatimuksille ja niiden seurannalle tulee olla menettelytavat. Lisäksi luvussa 4 esitetään vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalalle (ISO 22301:2019, 14–15).
Luku 5 - Johtajuus	Luvussa esitetään ylimpään johtoon kohdistuvat vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmän suhteen sekä tavat, joilla johdon tulee ilmaista odotuksensa organisaation toiminnalle (ISO 22301:2019, 15–16).
Luku 6 - Suunnittelu	Luvussa esitetään liiketoiminnan jatkuvuuden hallintajärjestelmän strategisten tavoitteiden laatimista koskevat vaatimukset. Asetettujen tavoitteiden saavuttamiseksi organisaation on määritettävä riskit ja mahdollisuudet aiemmin tunnistetuissa ulkoisissa ja sisäisissä toimintaympäristöissä (ISO 22301:2019, 16–18).
Luku 7 - Tukitoiminnot	Luvussa esitetään vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmän tukitoiminnoille, jotka ovat - Resurssivaatimukset - Pätevyysvaatimukset - Tietoisuusvaatimukset - Viestintävaatimukset - Viestintävaatimukset - Dokumentoidun tiedon vaatimukset (ISO 22301:2019, 18–19)

Luku 8 - Toiminta	Luvussa esitetään vaatimukset toiminnan suunnittelulle, toteutukselle ja ohjaukselle. Jatkuvuudenhallinta vaatii toimia, joita ovat luvun 8 mukaisesti toiminnan suunnittelu ja ohjaus, liiketoiminnan vaikutusanalyysit ja riskien arviointi, liiketoiminnan jatkuvuusstrategiat ja -ratkaisut, liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt, harjoitussuunnitelmat sekä liiketoiminnan jatkuvuuden dokumentaation ja kyvykkyyksien arvioinnin (ISO 22301:2019, 20–25).
Luku 9 – Suorituskyvyn arviointi	Luvussa esitetään vaatimukset liiketoiminnan jatkuvuuden hallintajärjestelmän tason ja vaikuttavuuden arvioinnille. Organisaation on määriteltävä hallintajärjestelmän arvioimiseksi toimenpiteet, joista selviää mitä seurataan ja mitataan, millä menetelmillä varmistetaan vaatimustenmukaiset tulokset, milloin seurantaa ja mittausta toteutetaan ja kenen toimesta, sekä milloin mittausten tuloksia analysoidaan ja arvioidaan (ISO 22301:2019, 25–27).
Luku 10 – Parantaminen	Luvussa esitetään vaatimukset poikkeamien hallintaan ja korjaaville toimenpiteille, jotta liiketoiminnan jatkuvuuden hallintajärjestelmän halutut tulokset saavutetaan, sekä hallintajärjestelmän jatkuvalle soveltuvuuden parantamiselle (ISO 22301:2019, 27–28).

ISO 22301-standardin tarkoituksena on tarjota rakenne ja vaatimukset, joiden avulla voidaan toteuttaa ja ylläpitää liiketoiminnan jatkuvuuden hallintajärjestelmää. Standardissa määritellyt vaatimukset ja ohjeet ovat yleisiä ja ne ovat määritelty soveltuviksi kaikenlaisiin organisaatioihin riippumatta organisaation koosta, tyypistä tai luonteesta. Vaatimusten käyttölaajuus riippuu organisaation toimintaympäristöstä, organisaation monimutkaisuudesta, tarpeista ja olosuhteista (ISO 22301:2019, 8).

ISO 22301:n esitelty korkean tason rakenne, joka on yhteinen muiden ISO-johtamisjärjestelmästandardien, kuten ISO 27001 ja ISO 9001 (standardi organisaation laadunhallintajärjestelmän rakentamiseen ja kehittämiseen) kanssa, auttaa organisaatioita integroimaan useita johtamisjärjestelmiä. Tämä voi auttaa organisaatioita parantamaan tehokkuutta, poistamaan päällekkäisyyksiä ja saavuttamaan kustannussäästöjä.

Esimerkiksi ISO 22301:n vaatimukset ”1” ja ”2” voivat jo löytyä organisaation toteuttamasta ISO 27001:n mukaisesta tietoturvallisuuden hallintajärjestelmästä, jolloin useamman hallintajärjestelmän implementointi on nopeampaa ja kustannustehokkaampaa. Esimerkiksi toteuttamalla ja sertifioitumalla standardien ISO 9001, ISO 27001 ja ISO 22301 mukaisesti, organisaatio osoittaa sillä olevan kykyjä laadukkaaseen, turvalliseen ja jatkuvaan toimintaan.

ISO 22301-standardin mukaisessa jatkuvuuden hallintajärjestelmässä painotetaan seuraavia asioita ja niiden tärkeyttä (ISO 22301:2019, 5):

1. Organisaation tarpeiden ymmärtäminen. Liiketoiminnan jatkuvuutta koskevien toimintaperiaatteiden ja tavoitteiden laatiminen.
2. Varmistetaan organisaation selviäminen häiriöistä käyttämällä ja ylläpitämällä selviytymisen mahdollistavia prosesseja, kyvykkyyksiä ja reagointimalleja.
3. Seuranta ja katselmointi. Liiketoiminnan jatkuvuuden hallintajärjestelmän suorituskyvyn arviointi.
4. Jatkuva parantaminen käyttäen laadullisia ja määrällisiä mittareita.

ISO 22301-standardissa edellytetty dokumentoitu tieto tarjoaa näyttöä vaatimustenmukaisuudesta ja jatkuvuuden hallintajärjestelmän vaikuttavasta toiminnasta (ISO 22313:2020, 27). Edellytystä tiedosta voidaan myös käyttää termiä vaatimus, sillä ISO 22301-standardin mukaisen sertifioinnin saamiseksi organisaation on toteutettava liiketoiminnan jatkuvuuden hallintajärjestelmä sisällyttämällä edellytetty dokumentoitu tieto organisaation jatkuvuuden hallintajärjestelmään.

Liiketoiminnan jatkuvuuden hallintajärjestelmän dokumentoidun tiedon laajuus voi vaihdella riippuen organisaatiosta, sillä siihen vaikuttavat muun muassa organisaation koko ja prosessien monimutkaisuus (ISO 22301:2019, 19). Lisäksi yksittäinen asiakirja voi kattaa yhden tai useamman dokumentoidun tiedon vaatimuksen, eikä esimerkiksi liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalan määrittely vaadi välttämättä omaa erillistä dokumentaatiotaan. Dokumentoitua menettelyä koskeva vaatimus voidaankin siis kattaa yhdellä tai useammalla

asiakirjalla. Termi menettely tarkoittaa tiettyä tapaa suorittaa jokin toiminto tai prosessi (ISO 22313:2020, 27).

Standardin ISO 22301 käyttöä ohjaava standardi ISO 22313 (2020, 27–28) listaa seuraavat dokumentoidut tiedot ISO 22301-standardin edellytyksinä:

- *Organisaation ja sen toimintaympäristön ymmärtämisen (ks. 4.1)*
- *Lakien ja viranomaisten vaatimukset (ks. 4.2.2)*
- *Liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalan ja rajaukset (ks. 4.3)*
- *Toimintaperiaatteet (ks. 5.2)*
- *Liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelun (ks. 6.2)*
- *Pätevyyden (ks. 7.2)*
- *Liiketoiminnan vaikutusanalyysin ja riskien arvioinnin (ks. 8.2)*
- *Liiketoiminnan jatkuvuusstrategiat ja -ratkaisut (ks. 8.3)*
- *Liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt (ks. 8.4)*
- *Harjoitussuunnitelman (ks. 8.5)*
- *Seurannan, mittauksen, analysoinnin ja arvioinnin (ks. 9.1)*
- *Sisäisen auditoinnin (ks. 9.2)*
- *Johdon katselmuksen (ks. 9.3)*
- *Poikkeamat ja korjaavat toimenpiteet (ks. 10.1).*

Dokumentoidun tiedon perässä on mainittu tietoon liittyvä ISO 22301-standardin klausuulinumero. ISO-standardi 22313:2020 antaa klausuulinumerot vain vaatimuksille, ei seuraavana listatuille tarvittaessa vaadittaville tiedoille.

ISO 22301-standardi ei tee koontia vaatimuksista, ja siksi kaikkien vaatimuksien listaamiseksi on hyvä käyttää joko ulkoisia kolmansien osapuolien tekemiä vaatimuslistauksia, jotka eivät toisaalta välttämättä pidä täysin paikkaansa (esimerkiksi vanhentunut tieto), jolloin on suositeltavaa myös tulkita itse standardin vaatimuksia, tai kuten tässä opinnäytetyössä, käyttää ohjaavaa standardia ISO 22313:2020.

Standardin ISO 22301 vaatimukset ja suositukset on etsittävä erikseen standardista ja standardia tulkittava oikein, jottei vaatimuksia jäisi huomaamatta. ISO 22031-standardin (2019, 7) mukaan asiakirjassa käytettävät verbirakenteet määrittävät sen, mikä on vaatimus ja mikä suositus.

1) *Rakenne ”on tehtävä” merkitsee vaatimusta*
2) *Rakenne ”olisi tehtävä” merkitsee suositusta*
3) *Modaaliverbi ”voida” ja siihen liittyvä infinitiivi merkitsee lupaa*
4) *Rakenne ”voi tehdä” voi tarkoittaa myös jonkin mahdollisuutta ja toimintakykyä*

Organisaatioiden ei ole pakko toteuttaa jokaista edellytettyä vaatimusta, mikäli organisaation ei ole tarkoitus sertifioitua ISO 22301 mukaisesti. Tällaisissa tapauksissa toteutettava liiketoiminnan jatkuvuuden hallintajärjestelmä on vapaamuotoisempi ja ISO 22301-standardin vaatimuksista voidaan esimerkiksi toteuttaa vain osa. Organisaatioiden tulee itse arvioida tarpeensa.

Edellytetyn tiedon lisäksi voidaan vaatia, että dokumentoitu tieto kattaa seuraavat asiat (ISO 22313:2020, 27–28):

- *Asiakassopimukset ja palvelutasot*
- *Liiketoiminnan vaikutusanalyysien tulokset*
- *Riskien arviointien tulokset*
- *Liiketoiminnan jatkuvuuden ratkaisujen määrittäminen ja valinta*
- *Häiriötilanteisiin reagoimisen yleiskatsaus*
- *Tietoisuussuunnitelma*
- *Liiketoiminnan jatkuvuuden hallintajärjestelmästä ja häiriötilanteista viestiminen henkilöstölle ja sidosryhmille, esim. Uutiskirjeillä, kokouspöytäkirjoilla ja varoituksilla*
- *Koulutusohjelmat koko organisaatiolle ja yksittäisille henkilöille*
- *Harjoitusaikataulu*
- *Toimittajien kanssa solmitut sopimukset ja palvelutasosopimukset*
- *Alihankkijoiden ja toimittajien liiketoiminnan jatkuvuuden toimintaperiaatteet ja suunnitelmat, mukaan lukien näyttö niiden itsensä käyttämien toimittajien riskien seurannasta ja siitä, että niiden itsensä käyttämien toimittajien jatkuvuussuunnitelmat on toteutettu ja niitä noudatetaan*
- *Tiedotus- ja vastemenettelyt alihankkijoille ja toimittajille*
- *Näyttöä tarkastuksista, ylläpidosta ja kalibroinneista*
- *Häiriötilanteiden ja läheltä piti -tilanteiden jälkiraportit*
- *Liiketoiminnan jatkuvuuden hallintajärjestelmän katselmointikokousten pöytäkirjat.*

Jälkimmäisenä listatuilla asioilla voidaan varmistaa liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuus (ISO 22313:2020, 27). Ohjaavan standardin ISO 22313:2020 käyttämä sanavalinta ”lisäksi voidaan vaatia” viittaa jälkimmäisenä listattujen tietojen vapaaehtoisuuteen eikä suoranaiseen vaatimukseen ISO 22301-standardin mukaisen liiketoiminnan jatkuvuuden hallintajärjestelmän toteuttamiseksi. Tässä opinnäytetyössä listatuista tarvittaessa vaadittavista tiedoista käytetään joskus myös termiä voidaan-vaatia-tieto.

ISO 22301-standardi soveltaa PDCA-mallia organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän toteuttamiseen ja ylläpitoon sekä sen vaikuttavuuden jatkuvaan parantamiseen. Myös muut ISO-standardit, kuten ISO 9001 ja ISO 27001 soveltavat PDCA-mallia. Standardien yhtenäi-

sellä PDCA-mallin soveltamisella tuetaan standardien yhdenmukaista toteuttamista ja käyttöä yhdessä muiden organisaation mahdollisesti käyttämien hallintajärjestelmien kanssa (ISO 22301:2019, 6).

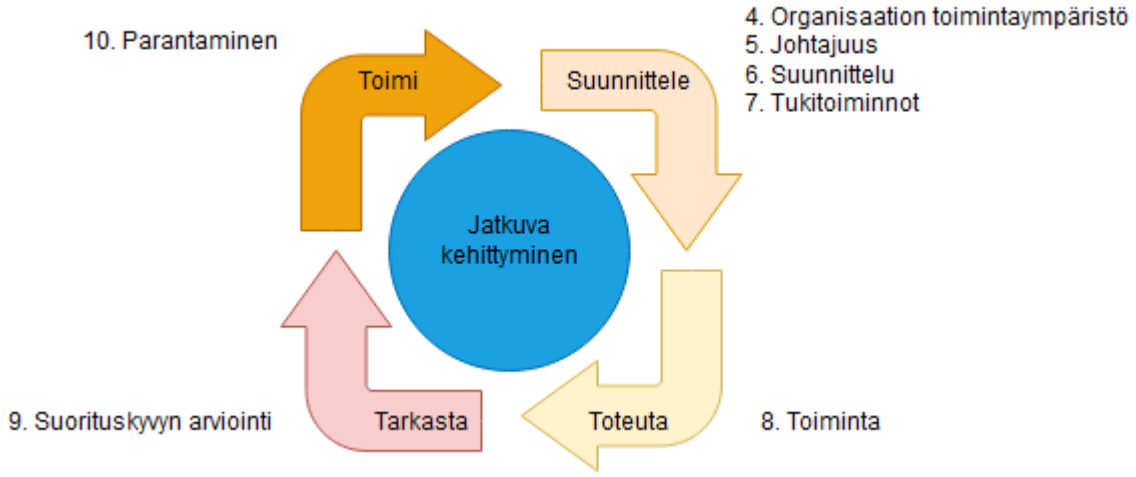
PDCA-mallissa prosessi ensin suunnitellaan, toteutetaan, tarkistetaan (arvioidaan), sekä ylläpidetään ja parannetaan. PDCA-malli ei ole ISO-standardeille uniikki malli, ja PDCA-mallia voidaan käyttää jatkuvan parantamisen lisäksi myös monissa muissa tarkoituksissa, kuten datan keräykseen ja datan analysointiin sekä minkä tahansa muutoksen toteuttamiseen (American Society for Quality. N.d)

PDCA-malli tunnetaan myös nimillä Shewhartin kehä, Demingin ympyrä tai Demingin kehä, sekä PDSA-malli, joka on lyhenne sanoista Plan-Do-Study-Act, suomeksi Suunnittele-Toteuta-Opiskele-Toimi (Lean Enterprise Institute. N.d). Mallin alkuperäinen luoja Walter A. Shewhart kehitti kolmitasoisen mallin 1920-luvulla, jota W. Edwards Deming jatkokehitti nelitasoiseksi 2. maailmansodan aikaan tehostamaan Yhdysvaltojen tuotantoprosesseja (Hargrave. 2021, Henshall, A. 2020).

PDCA-mallin käyttö auttaa ratkaisemaan ongelmia paljon tehokkaammin. Hyötyjä ovat muun muassa iteroivan työskentelytavan mahdollistama kohteena olevan tuotoksen jatkuva kehittäminen sekä työprosessien toistuvien virheiden estäminen (Kanbanize. N.d).

PDCA-mallia voidaan soveltaa jokaiseen liiketoiminnan jatkuvuuden hallintajärjestelmän osa-alueeseen ja jatkuvuudenhallinnan eri toimenpiteet, mukaan lukien itsensä jatkuvuuden hallintajärjestelmän, olisivatkin suositeltavaa kirjata jatkuvuudenhallinnan vuosikelloon, jolloin ne tulisivat määrävälein tarkistettua (Vahti 2/2016, 65–66). Vuosikelloa esitellään luvussa 4.2 Vahti-ohjeiden ohella.

Kuvio 13 avaa ISO 22301-standardin rakenteen suhdetta PDCA-mallin mukaiseen jatkuvaan kehittämiseen, kuvaten vaatimuksia asettavien lukujen ajoittumista kehitystyön eri vaiheissa.



Kuvio 13. ISO 22301-standardin rakenne suhteessa PDCA-malliin (Mukaillen: Roskoski, M. 2020).

Luvut 4-10 asettavat vaatimuksia liiketoiminnan jatkuvuuden hallintajärjestelmälle. Luvut 1-3 kuuluvat ISO 22301-standardin johdantoon ja eivät siksi ole osana PDCA-mallin mukaista toteutusta ja jatkuvaa kehittämistä.

Suunnittele-vaiheessa laaditaan jatkuvuudenhallinnan olennaisimmat tavoitteet, strategiat, menettelytavat, toimintaperiaatteet ja prosessit. Toteuta-vaiheessa toteutetaan ja käytetään valittuja hallintakeinoja, menettelyjä, toimintaperiaatteita sekä prosesseja. Tarkasta-vaiheessa liiketoiminnan jatkuvuuden hallintajärjestelmän suorituskykyä arvioidaan ja katselmoidaan suhteessa asetettuihin tavoitteisiin ja toimintaperiaatteisiin. Arviointitulokset raportoidaan johdolle (johdon katselmus). Toimi-vaiheessa liiketoiminnan jatkuvuuden hallintajärjestelmää ylläpidetään ja parannetaan. Parannuksista käytetään myös termiä korjaavat toimenpiteet. Toimi-vaiheen toimenpiteet määräytyvät johdon katselmuksen tulosten perusteella sekä hallintajärjestelmän soveltamisalan, jatkuvuuden toimintaperiaatteiden sekä tavoitteiden uudelleen arvioinnilla.

4.2 Vahti-ohjeet

Vahti-ohjeita on käytetty tässä opinnäytetyössä usein lähteenä ja tästä syystä Vahti-ohjeistuksien tarkoitusta sekä ohjeista vastaavaa toimijaa avataan tässä luvussa hieman yleisellä tasolla. Lisäksi esitellään myös Vahti 2/2016 toiminnan jatkuvuuden hallinnalle -ohjeen mukainen jatkuvuuden hallinnan vuosikello, joka on osa jatkuvaa kehittämistä, ylläpitämistä ja päivittämistä.

Vahti-termi tulee Valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmästä, lyhyesti VAHTI, joka toimi ensimmäisenä johtoryhmänä vuosina 1992–2013 (Suomidigi. N.d) julkisen hallinnon tietoturvallisuuden sekä tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- sekä koordinaatioelimenä (Valtiovarainministeriö. N.d). Nykyisin johtoryhmä tunnetaan nimellä Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmänä.

Vahti-ryhmän tavoitteena on valtionhallinnon toimintojen luotettavuuden parantaminen, kehittää jatkuvuutta, laatua, riskienhallintaa ja varautumista tieto- ja kyberturvallisuuden kautta sekä niitä kehittämällä. Tavoitteena on edellä mainittujen lisäksi myös tieto- ja kyberturvallisuuden sekä ICT-varautumisen edistäminen ja saattaminen kiinteäksi osaksi hallinnon toimintaa, edistää hallinnon johtamista ja tulosohjausta sekä tietojärjestelmien ja -verkkojen sekä ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä (Valtiovarainministeriö. N.d).

Vahtin yhteistoiminta hallinnossa sekä sen ulkopuolella on laajaa. Vahtin hankkeisiin kootaan kohteeseen parhaiten soveltuva asiantuntemus eri hallinnonaloilta. Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset (Valtiovarainministeriö. N.d).

Vahti-tietoturvaohjeisto on Valtiovarainministeriön ohjausta käsittelevän sivuston mukaan yksi maailman kattavimmista yleisistä tietoturvallisuusohjeistoista (Valtiovarainministeriö. N.d). Hallinnon lisäksi Vahti-ohjeita käytetään laajasti hyväksi kansainvälisessä tietoturvatyössä, elinkeinoelämässä, yrityksissä, organisaatioissa, kunnissa sekä opetus- ja kansalaistoiminnassa (Valtiovarainministeriö. N.d).

Vahti-ohjeet voidaan ryhmitellä kuta kuinkin seuraavalla jaottelulla:

- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Ohjelmistoturvallisuus
- Laitteistoturvallisuus
- Tietoaineistoturvallisuus

Kaikki Vahti-ohjeet ovat saatavilla Suomidigin verkkosivuilta osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet (Suomidigi. N.d). Vuoden 2009 jälkeen ohjeita on julkaistu 21 kappaletta. Ohjeita on alun perin vuodelta 2001 alkaen, mutta Suomidigin Vahti-ohjeet -sivusto listaa vuoden 2001–2008 ohjeet otsikon ”Vanhemmat VAHTI-ohjeet” alle. Vanhentuneita suosituksia voidaan kuitenkin hyödyntää soveltaen, kun otetaan huomioon muuttunut lainsäädäntö (Suomidigi. N.d).

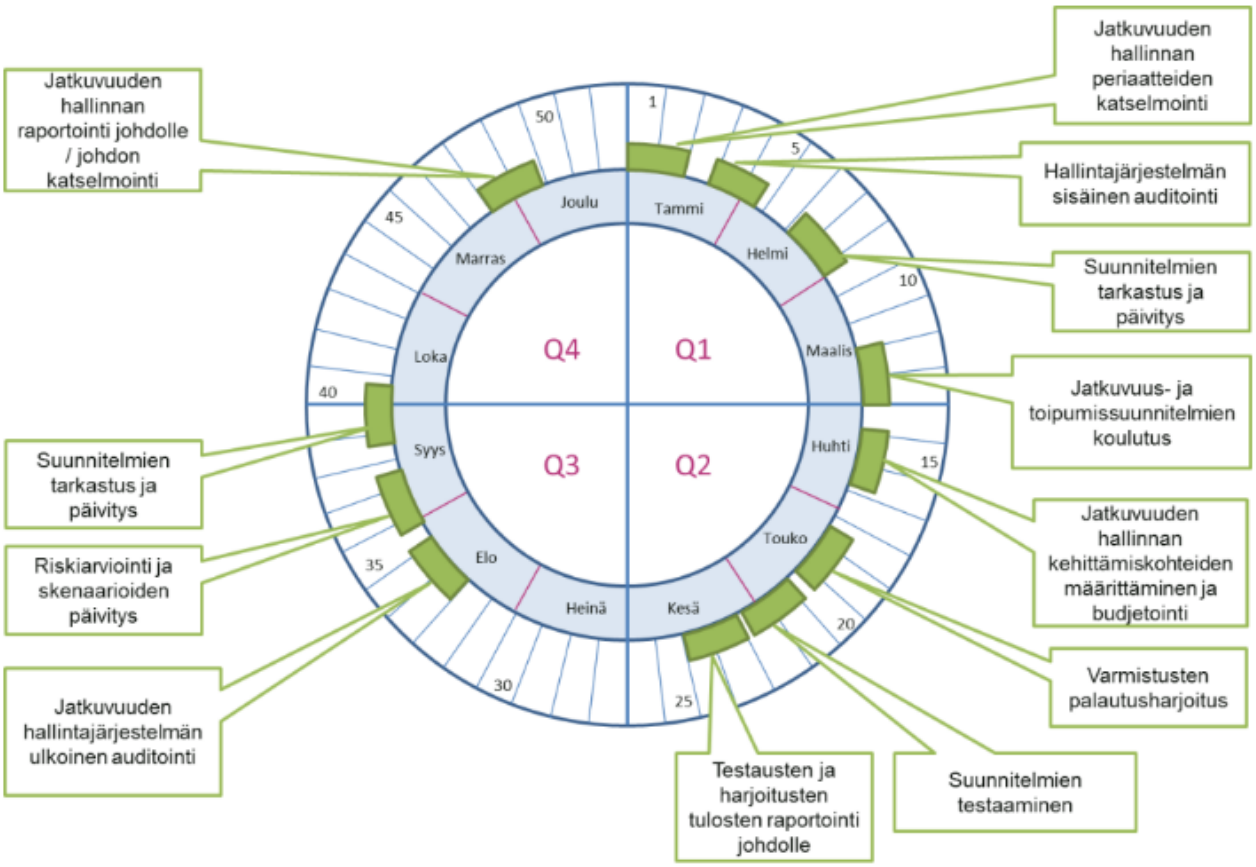
Uusimmasta vanhimpaan järjestyksessä listatut 10 esimerkki-Vahti-ohjetta käsittelevät muun muassa seuraavia asioita (Suomidigi. N.d):

- Sähköisen asioinnin tietoturvaohje (2017)
- Ohje riskienhallintaan
- Tietoturvapoikkeamatilanteidenhallinta
- Toiminnan jatkuvuuden hallinta
- Ohje salauskäytännöistä
- Tietoturvallisuuden arviointiohje
- Henkilöstön tietoturvaohje
- Toimitilojen tietoturvaohje
- Sovelluskehityksen tietoturvaohje
- ICT-varautumisen vaatimukset (2012)

Opinnäytetyössä vaikuttaa eniten usein lähteenäkin käytetty Vahti 2/2016-ohje, joka on toiminnan jatkuvuuden hallinnan ohje ja jonka tarkoituksena on jatkuvuuden hallinnan tehostaminen ja yhdenmukaistaminen valtioneuvostossa, hallinnonalojen organisaatioissa sekä julkisessa hallinnossa (Vahti 2/2016, johdanto). Ohjeistusta voivat seurata myös muut organisaatiot kehittääkseen liiketoimintansa jatkuvuutta.

Tässä luvussa avataan myös jatkuvuudenhallinnan yksi olennainen aiemmin käsittelemätön osa, vuosikello, joka esitellään Vahti 2/2016-ohjeessa. ISO-standardien keskeinen osa on järjestelmien arviointi ja jatkuva kehitys. ISO-standardien osuuksien lisäksi myös Katakri-osiossa luvussa 4.3 käsitellään säännöllisen arvioinnin osuus tietoturvassa, esimerkiksi turvallisuustyön resurssien säännöllisen arvioinnin osalta.

Vuosikello on osa kehittämistä, ylläpitoa ja päivittämistä ja sen avulla voidaan aikatauluttaa jatkuvuuden hallinnan toimenpiteitä vuoden ajalle ja se voidaan esittää joko kuvana, kuten kuviossa 14, tai kirjallisesti (Vahti 2/2016, 26).



Kuvio 14. Jatkuvuuden hallinnan vuosikelloesimerkki (Vahti 2/2016, 67).

Vuosikellon käyttötarkoitus on pidemmän aikajakson tapahtumien hahmottaminen kokonaisuutena. Vahti 2/2016 (2016, 26) suosittelee vuosikellon käyttöä myös esimerkiksi riskienhallinnassa sekä tieto- ja kyberturvallisuuden hallinnassa. Digi- ja väestötietoviraston digiturvallisuuden hallinnan tukimateriaali digiturvan kehittäjille (Digi- ja väestötietovirasto. 2021) esittelee myös tietosuojan vuosikellon, jota kuvataan samankaltaisesti kuin Vahti 2/2016-ohjeessa (2016, 26), eli suunnitelmallisuuden ja toteutumisen seurannan työkaluna sekä eräänlaisena muistilistana.

Vuosikelloon kuvataan eri kuukausille erilaiset esimerkiksi jatkuvuuden hallintaan liittyvät tehtävät. Tehtävien aikataulutuksen lisäksi tehtävien vastuut tulisivat olla jaettu, eli kuka tehtävän toteuttaa. Esimerkiksi jatkuvuuden hallinnasta sen vuosikelloon tulisi kirjata asioita kuten jatkuvuussuunnitelmien ylläpito ja päivitys, suunnitelmien koulutus sekä suunnitelmien testaus ja testausten tai harjoitusten tulosten raportointi johdolle. Kuviossa 14 nähdään esimerkki jatkuvuuden hallintajärjestelmän ulkoisesta auditoinnista elokuun kohdalla, joten aikataulutus voi olla tehty myös vuosineljännestä tarkemmin.

Luvussa 4.3 käsiteltävä kansallinen auditointikriteeristö, Katakri, käyttää toteutusesimerkeissään lähteinä muun muassa Vahti-ohjeita. Esimerkiksi turvallisuusjohtamisen osion 3. vaatimus T-03 – Tietoturvallisuusriskien hallinta viittaa lisätietoja-kohdassa ISO-standardien lisäksi Vahti 22/2017-ohjeeseen riskienhallinnasta ja saman osion vaatimus toimintahäiriöistä ja poikkeustilanteista (T-06) viittaa Vahti-ohjeisiin 2/2009 - ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin ja 2/2016 - Toiminnan jatkuvuuden hallinta.

Molemmista, eri Vahti-ohjeista sekä Katakrista, on hyötyä jatkuvuuden hallinnan toteuttamisessa ja niiden välillä onkin eräänlainen suhde toisiinsa, jolloin esimerkiksi tietoturvallisuuden hallintajärjestelmän ja osittaisten yhteisten vaatimusten myötä myös liiketoiminnan jatkuvuuden hallintajärjestelmän toteutus helpottuu.

4.3 Katakri 2020

Tässä luvussa esitellään kansallista auditointikriteeristö Katakria, kuvataan kuinka Katakri 2020:n turvallisuusjohtamisen T-osiota voidaan hyödyntää hallintajärjestelmien toteutuksien osien arvioinneissa, toteutuksissa ja hallinnoimisessa tietoturvajohtamisen osalta. Luvussa annetaan yksi käytännön esimerkki Katakrin turvallisuusjohtamisen vaatimusten mukaisuuden arvioinnista.

Katakri 2020 on Kansallisen turvallisuusviranomaisen NSA:n (National Security Authority) vuonna 2020 julkaisema viranomaisten tietoturvallisuuden auditointityökalu (Valtioneuvosto. 2020). Katakria voidaan käyttää auditointityökaluna arvioitaessa yritysten turvallisuusjärjestelyjä yritysturvallisuusselvityksissä sekä viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Katakria voidaan edellä mainittujen lisäksi käyttää apuna myös yritysten, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja turvallisuustyön kehittämisessä (Ulkoministeriö. N.d).

Katakrin avulla pyritään varmistumaan siitä, että kohdeorganisaation turvallisuusjärjestelyt viranomaisten salassa pidettävien tietojen paljastumisen ehkäisemiseksi ovat riittävät kaikissa ympäristöissä, joissa näitä tietoja käsitellään. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset (Ulkoministeriö. N.d). Katakrin vaatimukset eivät ole tietoturvallisuuden ehdottomia vaatimuksia. Katakriin kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja kansainvälisiin Suomea sitoviin tietoturvallisuusvelvoitteisiin. Katakri sisältää vaatimusten lisäksi hyödyllistä lisätietoa vaatimusten toteuttamiseen, kuten käytännön

toteutusesimerkkejä vaatimusten täyttämiseksi ja muuta lisätietoa, kuten viitteitä ISO-standardeihin.

Katakri on osoittautunut toimivaksi työkaluksi ja sillä on todettu olevan merkittävää arvoa myös Suomen maineelle niin tietoturvallisuuteen liittyvissä kysymyksissä kuin suomalaiselle yritysmaailmalle laajemminkin (Valtioneuvosto. 2020). Katakri 2020 on Katakrin neljäs versio. Katakrin ensimmäinen versio julkaistiin vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa, 2. versio vuonna 2011 Sisäministeriön koordinoimana ja 3. versio vuonna 2015, jonka ylläpito- ja hallinnointivastuu siirtyi Kansalliselle turvallisuusviranomaiselle tammikuussa 2014 (Katakri 2020, esipuhe).

Katakri 2020 sisältää kolme eri osa-aluetta, jotka muodostavat Katakrin rakenteen. Osa-alueet ovat (Katakri 2020, 5):

Turvallisuusjohtaminen (T) – Turvallisuusjohtamisen osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt suojatakseen turvallisuusluokiteltua tietoa.

Fyysinen turvallisuus (F) – Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan turvallisuusluokiteltujen (TL) tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.

Tekninen tietoturvallisuus (I) – Teknisen tietoturvallisuuden osa-alueessa kuvataan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.

Tässä opinnäytetyössä keskitytään Katakrin ensimmäiseen osa-alueeseen, tietoturvajohtamiseen, eli Katakrin T-osioon. Kuten aiemmin on todettu, on case-organisaatiolla jo olemassa ISO 27001-standardin mukainen tietoturvallisuuden hallintajärjestelmä, ja että hallintajärjestelmien vaatimukset ovat osittain samat. Katakrin T-osion vaatimuksia voidaan siis käyttää arvioimaan osia jatkuvuuden hallintajärjestelmän toteutuksesta.

Turvallisuusjohtamisen T-osio sisältää hallinnollisen tietoturvallisuuden sekä henkilöstöturvallisuuden (Katakri 2020, 8). Tämä opinnäytetyö antaa myös esimerkin Katakrin T-osion käyttämisestä

liiketoiminnan jatkuvuuden hallintajärjestelmän osien arviointeihin. Katakrin vaatimusten toteuttaminen ei välttämättä takaa ISO 22301-standardin vaatimusten täyttymistä, mutta voi auttaa niiden täyttämisessä. Katakrin turvallisuusjohtamisen osiosta vaatimukset T-01–08 käsittelevät hallinnollista tietoturvaa ja vaatimukset T-09-13 henkilöstöturvallisuutta.

Liikenne- ja viestintäministeriön alainen kyberturvallisuuskeskuksen kuvaus (Liikenne- ja viestintäministeriö. 2020) tietoturvasta kertoo tietoturvan tarkoittavan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus. Nämä kolme tunnetaan myös termillä CIA-malli, joka muodostuu englanninkielisistä sanoista confidentiality, integrity, availability (Fortinet. N.d).

Luottamuksellisuus tarkoittaa, että tiedot ovat saatavilla vain tietoon oikeutetuilla. Eheys tarkoittaa, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut ja että tietoon voidaan luottaa. Saatavuus (joskus myös käytettävyys) on sitä, että tiedot ja tietojärjestelmät ovat käytettävissä ja hyödynnettävissä oikeutetuille henkilöille (Fortinet. N.d).

4.3.1 Hallinnollinen tietoturva

Suomalainen hallinnollisenkin tietoturvan palveluita tarjoava tietoturvayritys Second Nature Security Oy, eli 2NS, kuvailee turvallisuusjohtamisen toista osa-aluetta, hallinnollista tietoturvallisuutta, keinona hallita ja ohjata teknisiä kontrolleja ja niiden määriä ja ominaisuuksia. Erilaisia kontrolleja voidaan luoda 2NS:n mukaan miltei loputon määrä, mutta kontrollien tarpeellisuutta ja kustannuksia tulisi arvioida ja hallita. Näin voidaan varmistaa, etteivät kontrollit vie resursseja muualta ja että kontrollit vastaavat oikeaa tarvetta (Second Nature Security. N.d).

Hallinnollisen tietoturvan tehtävänä on tasapainottaa kustannustehokkaan tietoturvan toteuttamista. Tästä syystä hallinnollinen tietoturva linkittyy vahvasti liiketoimintaan ja johtoon. Kaikessa tässä kokonaisuudessa onnistumisen edellyttämiseksi tulisi tietoturvaa lähestyä riskipohjaisesti, aivan kuten muitakin liiketoiminnan osa-alueita (Second Nature Security. N.d).

Esimerkiksi Katakri 2020:n T-osion vaatimus T-03 – Tietoturvallisuusriskien hallinta asettaa vaatimuksia riskipohjaiselle tietoturvallisuusriskien hallinnalle, joka tarkoittaa järjestelmällistä ja koordinoitua sekä jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään

ja seurataan tietoturvallisuusriskejä. Organisaation on arvioitava olennaiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti (Katakri 2020, 11).

Seclionin ”Mitä on hallinnollinen tietoturvallisuus?” -artikkelin (Seclion. 2020) yksinkertaistama kuvaus hallinnollisesta tietoturvallisuudesta kuvaa hallinnollista tietoturvallisuutta tietoturvallisuuden johtamisena. Tietoturvallisuutta tulee johtaa ja eri suojaustavat suunnitellaan nykytilanteen kartoituksen ja riskinarvioinnin mukaan.

Riskienhallinnan kautta tunnistetaan liiketoimintaan vaikuttavia epävarmuuksia. Hallinnollisen tietoturvan tuottamat kontrollit ovat vähemmän teknisiä ja keskittyvätkin enemmän muun muassa ihmisten toiminnan ohjaamiseen (Second Nature Security. N.d). Hallinnollinen tietoturva ottaa kantaa siihen, mitä tietoa on suojattava, miten ja kuinka vahvasti, sekä kenellä on pääsy kyseiseen tietoon ja miten tietoa voidaan käyttää.

Esimerkkejä yleisesti käytetyistä hallinnollisen tietoturvallisuuden viitekehyksistä ovat tietoturvallisuuden auditointityökalu viranomaisille eli Katakri 2020, valtionhallinnon toimitilojen tietoturvaohje Vahti 2/2013 sekä ISO 27001, joka käsittelee tietoturvallisuuden hallintajärjestelmän vaatimukset (Seclion. 2020).

4.3.2 Henkilöstöturvallisuus

Vahti-ohjeen 2/2008 mukaan toisella turvallisuusjohtamisen osa-alueella, henkilöstöturvallisuudella, tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa (Vahti 2/2008, 11–12). Tietoturvallisuuden alaterminä henkilöstöturvallisuus tarkoittaa henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa, kun käytetään tietoja tai tietojärjestelmiä. Henkilöstöturvallisuustoiminnassa haasteena on ihminen. Henkilöstö käsittelee tietoa eri tavoin, kuten vastaanottamalla tietoa, muokkaamalla, tallentamalla, välittämällä sekä tuhoamalla tietoa tiedon käsittelyn päätyttyä. Lisäksi henkilöstö ylläpitää tietovarastoja ja tietojärjestelmiä (Vahti 2/2008, 11–12).

Henkilöstöturvallisuutta tulee toteuttaa organisaation henkilöstöprosessin kaikissa vaiheissa, eli työsuhteen alussa, työsuhteen aikana sekä työsuhteen päättyessä. Työsuhteen alun henkilöstöturvallisuuden toimenpiteitä ovat muun muassa turvallisuusselvitykset, salassapitosopimukset sekä

työntekijöiden perehdyttäminen. Työsuhteen aikaisia toimenpiteitä voivat olla esimerkiksi kehityskeskustelut ja osaamisen kehittäminen. Työsuhteen päättyessä korostuvat avainten, aineistojen, materiaalien ja tunnusten luovutukset (Vahti 2/2008, 12).

Henkilöstöturvallisuuden yleisperiaatteita ovat:

- Monitasoisten turvajärjestelyjen käyttö
- Tietojen saaminen vain työtehtävään, sen suorittamiseen ja vähimmäistarpeeseen
- Tietojen lokerointi henkilöryhmittäin ja luokittain (esimerkiksi julkinen tieto, luottamuksellinen tieto, salassa pidettävä tieto)
- Vaarallisten työyhdistelmien välttäminen
- Kriittisissä toiminnoissa usean henkilön yhtäaikainen läsnäolo
- Pääsy-, valtuus- ja hallintatietojen salaisuuksien jakaminen
- Henkilöstön tekemien toimenpiteiden valvonta (ristiin- ja kaksoistarkastuksin)

Henkilöstöturvallisuustyö on luonteeltaan ennaltaehkäisevää ja se koskettaa kaikkia työntekijöitä. Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa, ja henkilöstöturvallisuuden osa-alueen arvioitavia kohteita ovat muun muassa henkilöstön soveltuvuus, toimenkuvat tai työnkuvat, sijaisjärjestelyt, tiedonsaantioikeudet, käyttöoikeudet, turvallisuuskoulutus ja valvonta (Vahti 2/2008, 19). Katakri 2020:n turvallisuusjohtamisen T-osion avulla voidaan arvioida turvallisuusjohtamisen molemmat osa-alueet.

4.3.3 Turvallisuusjohtaminen

Turvallisuusjohtaminen on siis kokonaisvaltaista toimintaa, jolla hallitaan organisaation turvallisuutta. Turvallisuusjohtaminen koostuu yritys- ja työnjohdon toimenpiteistä, joilla pyritään kehittämään organisaation turvallisuustasoa. Jatkuvuudenhallinnan onnistumisessa organisaation johdolla on merkittävä rooli. Johdon tulee osoittaa sitoutumista ja johtajuutta jatkuvuudenhallinnan suhteen muun muassa varmistamalla jatkuvuudenhallinnalle asetettujen tavoitteiden olevan yhdenmukaisia organisaation strategioiden ja tavoitteiden kanssa. Johdon tulee myös varmistaa liiketoiminnan jatkuvuuden hallintajärjestelmän vaatimuksien yhdistämisestä organisaation liiketoimintaprosesseihin (ISO 22301:2019, 15).

Turvallisuusjohtamisessa yhdistyvät menetelmien, toimintatapojen sekä ihmisten johtaminen. Katakrin turvallisuusjohtamisen osa-alue kattaa läpikäydyt hallinnollisen tietoturvallisuuden sekä

henkilöstöturvallisuuden. Opinnäytetyö antaa seuraavaksi arviointi- ja toteutusesimerkin yhdestä Katakri 2020 T-osion vaatimuksen arvioinnista, vaatimuksesta T-05 – Turvallisuustyön resurssit.

ISO 22301-standardi asettaa ohjaavan standardin ISO 22313 (2020, 23–24) mukaan pätevyysvaatimuksia organisaation palveluksessa työskenteleville henkilöille, jotka suorittavat liiketoiminnan jatkuvuuden hallintajärjestelmään liittyviä tehtäviä, joten Katakrin vaatimus T-05 soveltuu hyvin kyseisen vaatimuksen arviointiin. Organisaatiot voivat määritellä hallintajärjestelmiensä parissa työskentelevien henkilöiden pätevyys-, koulutus-, kokemus- ja osaamisvaatimukset itse (ISO 22301:2019, 18).

Vaatimus T-05 turvallisuustyön resursseista on seuraava (Katakri 2020, 13):

Organisaatiolla on käytössään riittävä asiantuntemus turvallisuusperiaatteiden varmistamiseksi.

Vaatimuksen toteuttamisen ja arvioimisen helpottamiseksi Katakri kertoo vaatimuksen lisäksi myös lisätietoja vaatimuksesta. Lisätieto sisältää laajempaa kuvausta vaatimuksesta, toteutusesimerkin sekä muita lisätietoja, jotka viittaavat muihin lähteisiin, kuten vaatimuksen T-05 tapauksessa standardiin ISO 27001:2017 ja sen lukuihin 5.1 (johtajuus ja sitoutuminen), 7.1 (resurssit) ja 7.2 (pätevyys) (ISO 27001:2017, 7 & 10).

Turvallisuustyön resurssien osalta toteutusesimerkki sisältää neljä kohtaa:

1. *Turvallisuustehtäviä hoitavilla on riittävä asiantuntemus sekä näistä on näyttöjä.*
2. *Turvallisuustyön resurssit, tehtävät, vastuut ja valtuudet on määritelty organisaation toimintaan, kokoon ja riskeihin nähden riittävän kattavasti.*
3. *Resurssit riittävät tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen.*
4. *Resurssien riittävyyttä arvioidaan säännöllisesti.*

Toteutusesimerkin 3. kohta mainitsee tietoturvallisuuden hallintajärjestelmän. Kuten todettu, eri hallintajärjestelmiä voidaan integroida, ja hallintajärjestelmien vaatimuksissa on päällekkäisyyksiä, jolloin aiemmin toteutetun hallintajärjestelmän osatoteutus voi myös soveltua myöhemmin toteutettavan hallintajärjestelmän osatoteutukseksi (esimerkiksi koulutus). Siispä ISO 22301-standardin vaatimus pätevyydelle voitaisiin toteuttaa käyttämällä jopa täysin tai suurimmilta osin standardin ISO 27001:2017 mukaista toteutusta pätevyyden määrittelyllä ja osaamisen varmistamiselle.

Vaatimuksen täyttäminen vaatimusesimerkin tapauksessa voidaan osoittaa esimerkiksi dokumentoidulla tiedolla vastuullisesta yksiköstä, ryhmästä tai rooleista, joiden tehtävänä on hoitaa turvallisuustehtäviä, kuten eri hallintajärjestelmiä ja niihin kuuluvia toteutuksia, kuten esimerkiksi liiketoiminnan vaikutusanalyysiprosessi. Mikäli turvallisuustehtäviä on enemmänkin, esimerkiksi suuremmassa organisaatiossa, tulee työnjaon ja vastuiden olla jaettu, dokumentoitu ja kaikkien osallisten tiedossa.

Turvallisuustehtäviä hoitavien tulee kouluttautua organisaation ohjeiden mukaisesti esimerkiksi vuosittain. Koulutuksissa voidaan esimerkiksi suosia sertifikaattien suorittamista, jolloin organisaatiolla voi paremmin osoittaa vastuuhenkilöstönsä osaamisen sidosryhmilleen. Organisaation itse määrittämää riittävää koulutusta voivat olla myös organisaation sisäiset koulutukset tai vaikkapa henkilöstön suorittamat erilaiset tutkinnot.

ISO 22301-standardin toteutusta ohjaava standardi ISO 22313 (2020, 24) listaa erityyppisiä mahdollisia koulutuksia ja pätevyyksiä, joita ovat muun muassa liiketoiminnan vaikutusanalyysin suorittaminen, viestintätaidot tai harjoitussuunnitelman toteuttaminen. Nämä kaikki ovat myös ISO 22301-standardin vaadittua dokumentoitua tietoa, jotka ovat listattu luvussa 4.1 ISO 22301:2019-standardi.

Turvallisuustyön resurssien riittävyyttä voidaan arvioida esimerkiksi vuosittain. Resurssien arviointi voidaan tehdä päällikkötasolla esimiestyöskentelynä ja tarvittaessa käsitellä johdon kanssa. Yksi osa resurssien varmistamisessa on myös henkilöiden rekrytointi. Henkilön eli resurssin rekrytoimiselle tulisi olla määritelty esimerkiksi osaamisvaatimukset, kuten rekrytoitavaan tehtävänkuvaan sopivat osaamiset.

Katakri 2020:n turvallisuusjohtamisen osion vaatimus T-05 – Turvallisuustyön resurssit tarkoittaakin tiivistettynä sitä, että organisaatiolla on riittävästi henkilöitä, henkilöillä on riittävästi osaamista turvallisuudesta, ajantasaiset ohjeet, koulutusta, asianmukaiset työvälineet ja että kaikkia turvallisuustyön resursseja ja niiden riittävyyttä arvioidaan säännöllisesti.

Katakri-arviointien lopputuloksena syntyy raportti, josta nähdään arviointien tulokset. Katakri 2020-arviointien Excel-työkalun voi ladata vapaasti Kyberturvallisuuskeskuksen kotisivuilta (Kyberturvallisuuskeskus. 2021).

Katakri 2020:n havaintoluokittelu on kuvion 15 mukainen.

Havaintoluokka	Kuvaus
Vakava poikkeama	Mahdollistaa ulkopuoliselle pääsyn salassa pidettävään tietoon. Tyypillisesti puute salassa pidettävän tiedon suojaamisen ulkorajapinnassa (esimerkiksi rajapinta Internetin kanssa). Myös merkittävät puutteet prosesseissa (esimerkiksi henkilöstön koulutusprosessin puuttuminen), johtaen ennen pitkää ulkopuolisen pääsyyn salassa pidettävään tietoon.
Keskitason poikkeama	Voi mahdollistaa ulkopuolisille pääsyn salassa pidettävään tietoon, tai/ja mahdollistaa sisäpuolisille pääsyn heille kuulumattomaan tietoon (tiedonsaantitarpeen ylittyminen). Tyypillisesti vähäiset puutteet tiedon suojaamisen ulkorajapinnassa tai/ja merkittävät puutteet sisäpuolen rajapinnoissa. Myös keskitason puutteet prosesseissa, mikä voi johtaa ulkopuolisen pääsyyn salassa pidettävään tietoon.
Lievä poikkeama	Voi mahdollistaa sisäpuolisille pääsyn heille kuulumattomaan tietoon. Tyypillisesti vähäiset puutteet tiedon suojaamisen sisäpuolen rajapinnoissa. Myös vähäiset puutteet prosesseissa, mikä voi johtaa sisäpuolisille pääsyn heille kuulumattomaan tietoon.
OK	Vaatimus täyttyy sellaisenaan, tai vastaavan tasoisen suojauksen tarjoavilla korvaavilla suojauksilla.

Kuvio 15. Katakri 2020 havaintoluokat (Kyberturvallisuuskeskus. 2021).

Lisäksi voidaan käyttää tarpeen mukaan kuviossa 16 esitettyjä merkintöjä.

Havaintoluokka	Kuvaus
Ei sovellu	Vaatimus ei sovellu ko. arviointikohteeseen. Esimerkiksi I-05 (Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langaton tiedonsiirto) kohteessa, jossa ei käytössä langattomaan viestintään kykeneviä fyysisiä laitteita/liityntöjä.
Ei arvioitu	Ko. vaatimuskohdan arviointia ei toteutettu.
Arviointi kesken	Ko. vaatimuskohdan arviointi kesken.

Kuvio 16. Katakri 2020 lisämerkinnät (Kyberturvallisuuskeskus. 2021).

Käytettäessä Kyberturvallisuuskeskuksen Katakri 2020 arviointityökalua (Excel), kirjataan kuvaus vaatimusten toteutustavasta kuten arvioinnissa käytetyt aineistot, arviointitulos sekä muut oleelliset arviointiin liittyvät kommentit. Näin arvioinnin tulos voidaan tarvittaessa toistaa ja todentaa.

5 Liiketoiminnan jatkuvuuden hallintajärjestelmän kehittäminen

Tässä luvussa käydään läpi liiketoiminnan jatkuvuuden hallintajärjestelmän kehitystyötä. Kehitystyö on osa case-organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän kehittämisen kokonaisuutta. Kehitystyö jatkuu myös opinnäytetyön kirjoittamisen jälkeen, arviolta seuraavan vuoden ajan johtuen muun muassa case-organisaation toimintojen kompleksisuudesta ja organisaation koosta johtuen, jolloin kokonaan sertifioinnin vaatimusten mukainen liiketoiminnan jatkuvuuden hallintajärjestelmän toteuttaminen ei ollut realistinen tavoite opinnäytetyöprojektin keston aikana. Hallintajärjestelmän itsenä lisäksi kaikki ISO 22301-standardissa asetetut hallintajärjestelmään kuuluvat prosessit tulee toteuttaa vaatimusten mukaisiksi.

Case-organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän kehittäminen saatiin liikkeelle ja se muodostaa vaadittavan pohjatyön jatkuvuuden hallintajärjestelmän kehittämiselle jatkossa. Opinnäytetyön ulkopuolelle jää täysin valmiin hallintajärjestelmän toteutus ja jalkauttaminen case-organisaatiossa. Toteuttamisesta on kuitenkin sovittu case-organisaation kanssa ja opinnäytetyöprojektin liiketoiminnan jatkuvuuden hallintajärjestelmä toteutetaan jatkoprojektina opinnäytetyössä kuvatun kehitystyön jälkeen.

Luvuissa 5.1–5.3 käsitellään tarkemmin kehitystyön kokonaisuuden muodostavat vaiheet, jotka olivat toteutettavan hallintajärjestelmän tavoitetilan määrittely, kehitystyön alkuun saamiseksi riittävän tietoperustan kehittäminen ja viitekehyksen rakentaminen sekä case-organisaation jatkuvuudenhallinnan lähtötilanteen arviointi ja puutteiden tunnistaminen.

5.1 Tavoitetilan määrittely

Case-organisaation jatkuvuudenhallinnan tavoitteeksi määriteltiin ISO 22301-standardin mukainen liiketoiminnan jatkuvuuden hallintajärjestelmä. Koska case-organisaatiolla oli jo olemassa ISO 27001-standardin mukainen tietoturvallisuuden hallintajärjestelmä, tulisi toteutettava jatkuvuu-

den hallintajärjestelmä noudattelemaan rakenteeltaan ja toteutukseltaan olemassa olevaa hallintajärjestelmää. Molempien standardien rakenteet ovat samat, joten tietoturvallisuuden hallintajärjestelmän ollessa jo käytössä, on saman rakenteisen hallintajärjestelmän käyttöönotto ja kehittäminen sujuvampaa.

Toteutettavan jatkuvuuden hallintajärjestelmän tulisi täyttää lopulta kaikki ISO 22301-standardin mukaiset vaatimukset hallintajärjestelmälle sertifioitumisen mahdollistamiseksi ja tämä tavoite pidettiin koko kehitysprojektin aikana tähtäimessä. Näin toimimalla jatkuvuuden hallintajärjestelmän kehittäminen on loogista, järkevää ja tavoitteen mukaista.

Opinnäytetyön toteutusajan puitteissa toteutettavan hallintajärjestelmän valmiusasteen tavoitteeksi ei määritelty sertifioinnin mahdollistamaa valmista hallintajärjestelmää, vaan niin sanottu jatkokehityksen mahdollistava runko jatkuvuudenhallinnan kehittämiseen case-organisaatiossa.

5.2 Tietoperustan ja viitekehyksen rakentaminen

Kehitystyön toteuttamisen mahdollistamiseksi tuli ensin muodostaa riittävä tietoperusta aihealueesta sekä rakentaa viitekehys. Kehitystyön alkuvaiheessa käytettiin standardien lisäksi myös jatkuvuudenhallintaan liittyviä julkaisuja ja erilaisia oppaita, jotta aiheen viitekehys hahmottuisi paremmin ja olisi selvää, mitä tullaan tutkimaan ja tuottamaan.

Tietoperustaa rakentaessa ja standardin ISO 22301 vaatimuksia tulkitessa havaittiin eroavaisuuksia eri lähteiden tulkinnoissa muun muassa vaatimusten osalta. ISO 22301 asettaa dokumentoidulle tiedolle vaatimuksia sekä määrittelee myös tiedon, jota voidaan vaatia tarvittaessa, jotta liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuudesta voidaan varmistua. Koska hallintajärjestelmän lopullisena tavoitteena on sertifioitua sille vaatimuksia asettavaa standardia vasten, ei vaatimusten tulkinnassa ja toteutuksessa voi olla varaa tulkinnanvaraisuudelle.

Opinnäytetyöprojektin pääasiallisena tietoperustana toimivat lopulta standardit ISO 22301:2019 - Liiketoiminnan jatkuvuudenhallintajärjestelmät (vaatimukset), ISO 22313:2020 – Ohjeistusta standardin ISO 22301 käyttöön sekä Vahti 2/2016 - Toiminnan jatkuvuuden hallinta -ohje. Valitut eni-

ten käytetyt lähteet ovat myös kolmansien osapuolien, esimerkiksi tietoturvatalojen tai -konsulttien julkaisemia lähteitä kuten oppaita huomattavasti luotettavampia niiden ollessa standardeja ja valtionhallinnon ohjeita kolmansien osapuolien lähteiden tekemien standarditulkintojen sijaan.

Osa jatkuvuuden hallintajärjestelmän kehittämisen alkukartoitusta oli case-organisaation sisäisiin toimintoihin perehtyminen ja niiden tutkiminen pääosin dokumentaatioita läpi käymällä. Case-organisaation sisäisiin ohjeisiin, prosesseihin ja menetelmiin perehdyttiin, kun viitekehys alkoi hahmottumaan ja tavoitteet jatkuvuuden hallintajärjestelmälle olivat määritelty.

Tutustumalla ensin tarvittavaan tietoperustaan ja rakentamalla viitekehys, oli helpompaa tulkita, mikä on hyödyllistä ja opinnäytetyöprojektin kannalta oleellista tietoa. Case-organisaation ohjeisiin ynnä muihin dokumentaatioihin kuului organisaation koko henkilöstölle osoitettuja julkaisuja, kuten koulutuksia ja ohjeita sekä vain tietyille käyttäjäryhmille tarkoitettuja dokumentteja, kuten jatkuvuus- ja toipumissuunnitelmapohjat.

Case-organisaatiossa oli aiemmin luotu tietoturvallisuuden hallintajärjestelmä. Osa tietoperustan ja viitekehyksen rakentamista oli tutusta dokumenttien lisäksi myös kyseiseen hallintajärjestelmään. Eri hallintajärjestelmiä voidaan integroida, mikä tarkoittaa sitä, että jotkin vaatimukset ja niiden toteutukset soveltuvat yhdestä hallintajärjestelmä toiseen. Jo olemassa olevaa hallintajärjestelmää katselmoimalla saatiin vastauksia joihinkin jatkuvuuden hallintajärjestelmän standardin asettamiin vaatimuksiin. Hallintajärjestelmän katselmoinnin kautta saatiin selville esimerkiksi riskienhallinnan toimintamalleja sekä kuinka case-organisaatiossa seurataan ja mittaroidaan työntekijöiden koulutusta ja osaamista.

Kirjallisuuteen ja organisaation toimintoihin tutustumalla myös työpajat tukivat tietoperustan tulkinnassa ja dokumenttianalyyseissä esiin tulleita asioita ja toimivat myös tarkentavana tekijänä dokumenttien katselmoinneissa ja niiden tuloksissa. Työpajat olivat pienen porukan, yleensä kolmen henkilön, tilaisuuksia, missä käytiin läpi tehtyä soveltuvuusarviointia ja kartoitettiin sekä arvioitiin ISO 22301-standardin asettamien vaatimusten toteutumista. Näissä tilaisuuksissa pääaiheina olivat soveltuvuusarviointi sekä se, kuinka standardin asettamiin vaatimuksiin voidaan vastata, esimerkiksi mitä tulisi kehittää ja päivittää seuraavaksi sekä kuinka kehitystyössä edetään.

5.3 Jatkuvuudenhallinnan lähtötilanteen arviointi ja puutteiden tunnistaminen

Case-organisaatiossa oli aiemmin luotu ISO 27001-standardin mukainen tietoturvallisuuden hallintajärjestelmä. Tästä toteutuksesta vastannut ja jatkuvuuden hallintajärjestelmän kehitystyössä mukana ollut henkilö pystyi tämän aiemman kokemuksen perusteella ohjaamaan myös jatkuvuuden hallintajärjestelmän toteutuksessa ja perehdyttämään kirjoittajaa tarkemmin tietoturvallisuuden hallintajärjestelmään, jotta jo toteutettua voitaisiin hyödyntää hallintajärjestelmien toteutusten välillä soveltuvilta osin kehitystyön tehostamiseksi.

Opinnäytetyöprojektin alkukartoitusvaiheen aikana pystyikin jo toteamaan, että case-organisaatiosta löytyy jo paljon jatkuvuuden hallintajärjestelmässä hyödynnettävää tai ISO 22301-standardin vaatimaa dokumentoitua tietoa. Iso osa olemassa olevasta tiedosta kuitenkin vaati joitain tarkennuksia liiketoiminnan jatkuvuuteen liittyen. Katselmoitu tieto ei yleensä ottanut mitään kantaa organisaatiotasoiseen jatkuvuuteen, vaan oli tietoturvan hallintajärjestelmälle ominaisesti keskittynyt tieto- ja viestintäteknisiin aiheisiin, mutta myös turvallisuusjohtamiseen sekä koulutuksiin.

Case-organisaation turvallisuuskulttuurin vaikutti olevan keskimääräistä korkeatasoisempaa, mikä näkyi muun muassa tietoturvallisuuden hallintajärjestelmään tutustumisen myötä, muun muassa sen toteutuksen kattavuudessa. Tietoturvallisuuden hallintajärjestelmä keskittyy nimensä mukaisesti tietoturvallisuuteen ja siksi siinä ei kuulukaan löytyä esimerkiksi kaikkea jatkuvuuden hallintajärjestelmän vaatimuksia. Mitään liiketoiminnan jatkuvuuden hallintajärjestelmän vaatimuksiin tai voidaan-vaatia-dokumentoitavaksi-tietoon kuuluvaa hallintajärjestelmän osaa ei tarvinnut aloittaa toteuttamaan täysin alusta alkaen.

Kokonaisuudessaan lähtötilanteen arvioinnin jälkeen lähtötaso oli vakuuttava ja muodosti tukevan pohjan liiketoiminnan jatkuvuuden kehittämiselle. Puutteiden arviointia tehtiin kehitystyön jokaisessa vaiheessa. Liitteissä 1 ja 2 nähtävät arvioinnit ovat tuloksia neljännestä iteraatioista.

ISO 22301-standardin vaatimusten kartoittamisessa ja puutteiden tunnistamisessa käytettiin kyseisen standardin lisäksi ohjaavaa standardia ISO 22313. Näistä kootut vaatimukset kerättiin liitteiden 1 ja 2 mukaisiin vaatimustaulukoihin. Taulukon jaottelu on kaksiosainen, standardissa ISO 22301 edellytetty dokumentoitu tieto (niin sanotut pakolliset vaatimukset, liite 1) ja dokumentoitu tieto,

joita voidaan vaatia hallintajärjestelmän vaikuttavuuden arvioinnissa (liite 2). Jaottelu esiteltiin myös ISO 22301-standardia käsittelevässä luvussa 4.1.

Soveltuvuusarviointitaulukon jaottelu ei mene suoraan kuten tämän työn luvussa 4.1 esitetty muun muassa siksi, että tarvittaessa vaadittavalle dokumentoidulle tiedolle ei ole numerointia ISO 22313:ssa, jolloin oikein kohdistaminen arviointitaulukkoon klausuulinumeroittain on hankalaa joidenkin tietojen osalta. Lisäksi osa tarvittaessa vaadittavasta tiedosta sisällytetään pakollisten dokumenttien osuuksiin – näin voidaan tehdä esimerkiksi liiketoiminnan vaikutusanalyysin prosessin kuvaamisessa (klausuulinumero 8.2), johon yhdistettäisiin analyysien tulokset (klausuulinumero 8.2.2) - tai lopullinen toteutus on nimeltään poikkeava standardin vaatimukseen verrattuna. Lopullinen hallintajärjestelmän toteutus voi myös sisältää useamman vaatimuksen yhden toteutuksen alla.

Puutteiden tunnistamisessa käytetty soveltuvuusarviointitaulukko (liite 1 ja 2) on jaoteltu klausuulinumeroittain, eikä se tee niin sanottuja alakoonteja vaatimuksista. Esimerkkinä liiketoiminnan vaikutusanalyysiprosessi, BIA, ja sen vaatimukset, jossa ISO 22301-standardi (2019, 20) asettaa BIA-prosessille 8 eri vaatimusta (a-h), jolloin vaatimukset voitaisiin kuvata soveltuvuusarvioinneissa myös yhden esitetyn vaatimuksen sijaan kahdeksana vaatimuksena. Tarkemmat vaatimukset huomioidaan kunkin liiketoiminnan jatkuvuuden prosessin omissa kehityspoluissa.

Soveltuvuusarviointien tulokset (liitteet 1 ja 2) ovat yhdistetty hallintajärjestelmän hahmotelmaversioon liitteessä 3.

6 Tulokset

Jatkuvuuden hallintajärjestelmän kehitystyön myötä sen tuloksia ovat liitteiden 1 ja 2 mukaiset soveltuvuusarvioinnit case-organisaation toiminnoista suhteessa ISO 22301-standardin vaatimuksiin dokumentoidulle tiedolle, sekä liitteen 3 mukainen hallintajärjestelmän runko.

Tietoperustan ja viitekehyksen rakentamisen, toimintamalleihin tutustumisen ja soveltuvuusarviointien tuloksena pystyttiin muodostamaan ISO 22301 standardin mukainen hallintajärjestelmärunko. Pääpaino jatkuvuuden hallintajärjestelmän kehitystyössä oli kartoittaa olemassa olevat

toimintamallit, arvioida niiden soveltuvuutta jatkuvuuden hallintajärjestelmän vaatimuksia vasten koko kehitysprojektin aikana, kehittää ja päivittää toimintamalleja soveltuvimmiksi jatkuvuuden hallintaan sekä rakentaa liiketoiminnan jatkuvuuden hallintajärjestelmän runko, joka toimii perustana lopulliselle sertifioinnin mahdollistamalle hallintajärjestelmän toteutukselle.

Vaaditut toimintamallien toteutukset ja niiden soveltuvuusarvioinnit ovat yhdistetty hallintajärjestelmän dokumentissa, liitteessä 3, joka muodostaa dokumentaatiokokonaisuuden sisältäen myös soveltuvuusarviointien tulokset (liitteet 1 ja 2) suppeammin esitettynä.

Liitteestä 1 ”Soveltuvuusarviointi – BCMS:ssä edellytetty dokumentoitu tieto” ja liitteestä 2, ”Soveltuvuusarviointi - Voidaan vaatia dokumentoituna tietona BCMS:n vaikuttavuuden arvioinnissa” nähdään hallintajärjestelmän asettamien vaatimusten toteutuminen case-organisaatiossa.

Soveltuvuusarviointi on jaettu kahteen osaan, jossa ensimmäisenä liitteessä 1 listataan ISO 22301-standardin vaatimukset, ja toisena liitteessä 2 tarvittaessa vaadittava tieto. Case-organisaation jatkuvuudenhallinnan tilaa on arvoitu asteikolla, soveltuu (vihreä väri) – soveltuu osittain (keltainen) – ei sovellu (punainen), joka näkyy arviointitaulukon vasemmassa laidassa sarakkeessa ”Tila”

Soveltuvuusarvioinnissa on soveltuvuuden lisäksi taulukoitu sarakkeeseen ”Lauseke nro.” vaatimuksen klausuulinumero, jonka avulla vaatimus voidaan tarkastaa standardeista ISO 22301 ja 22313 ketterästi. Taulukossa on myös kuvattu asetettu vaatimus sanallisesti sarakkeessa ”Lauseke”. Taulukon sarake ”Toteutustapa” kuvaa, kuinka vaatimus on toteutettu ja ohjaa mahdollisuuksien mukaan löytyvään tietoon. Liitteissä 1 ja 2 tämä on osoitettu esimerkkiteksteillä, kuten vaatimuksen 4.1 kohdalla tekstillä ”Toimintaympäristön kuvauksen linkki”.

Case-organisaatiolle tehtävässä lopullisessa toteutuksessa linkit vievät asianmukaisiin tietosijainteihin. Toteutustavassa on voitu myös tiedon linkityksen lisäksi kuvailla toteutusta kirjallisesti, jolloin arviointitaulukosta tulee ymmärrettävämpi. Joskus toteutustavan sarakkeeseen voi tulla useita linkkejä, mikäli jollekin toteutukselle, kuten viestinnälle, on olemassa ajantasaista tietoa useista eri lähteistä. Liitteinä olevat versiot taulukoista ovat tietojen osalta karsittuja case-organisaation tietojen suojaamisen vuoksi.

Arviointitaulukon sarake ”Kuvaus lausekkeesta” antaa lyhyen kuvauksen vaatimuksesta. ”Lisätietoa / huomioitavaa” sarake ohjaa tapauksesta riippuen hyödylliseen lisätietoon, kuten esimerkiksi ohjaavan standardin ISO 22313 vaatimusta käsittelevään lukuun. Saraketta voidaan myös käyttää lisätietokenttänä, mikäli jokin hallintajärjestelmän vaatimus on toteutukseltaan epäselvä tai vaatii muita tarkennuksia. Kenttään voidaan myös kirjata tulevat toimenpiteet muun muassa jatkokehityksen osalta.

Arviointitaulukon lisätyn informatiivisuuden tarkoituksena on edistää laadukasta dokumentaatiota, jotta muutkin kuin kehitystyön päävastuulliset voivat tarvittaessa osallistua kehitystyöhön mahdollisimman matalalla kynnyksellä. Hyvä dokumentaatio on itsessään myös jatkuvuudenhallintaa. Jos hallintajärjestelmän kehitystyön kannalta kriittinen henkilöresurssi poistuu äkillisesti, saadaan tilalle korvaava osaava resurssi nopeammin, koska aiheeseen on helpompaa perehtyä.

Soveltuvuusarviointitaulukon viimeinen sarake, ”Myös ISO 27001:n vaatimus?” kertoo sen, onko ISO 22301:n vaatimus myös vaatimus case-organisaation toteuttamassa ISO 27001 mukaisessa tietoturvallisuuden hallintajärjestelmässä. Mikäli vastaus tässä sarakkeessa on jonkin vaatimuksen kohdalla kyllä, soveltuu vaatimus mitä todennäköisimmin joko suoraan tai pienin tarkennuksin liiketoiminnan jatkuvuuden hallintajärjestelmään, jolloin ISO-standardeille ominainen hallintajärjestelmien välinen integrointi toteutuu.

”Soveltuvuusarviointi – BCMS:ssä edellytetty dokumentoitu tieto” (liite 1) sisältää suoraan ohjaavan standardin ISO 22313 (2020, 27) mukaiset vaatimukset. Kyseisen standardin listaama tarvittaessa vaadittava tieto (2020 27–28) on listattu liitteeseen 2, ”Soveltuvuusarviointi - Voidaan vaatia dokumentoituna tietona”, BCMS:n vaikuttavuuden arvioinnissa soveltuvin osin. Osa näistä tiedoista sisällytetään muihin vaatimuksiin ja niiden toteutuksiin, kuten esimerkiksi useat eri vaatimukset koulutukselle ja pätevyydelle tai tietoisuudelle organisaation jatkuvuuden hallinnasta. Yhdistämisellä muun muassa selkeytetään soveltuvuusarviointitaulukkoa, jossa eri klausuulien yhdistämistä koordinoidaan.

Soveltuvuusarviointien tuloksia liitteistä tarkastelemalla voidaan todeta, että case-organisaatiossa liiketoiminnan jatkuvuudelle vaatimuksia asettavan standardin ISO 22301 mukaisia vaatimuksia alkaa olla kehitystyön tässä vaiheessa hyvin kartoitettu sekä toteutettu. Opinnäytetyössä näkyvät

tulokset ovat arviointien tulos neljännen iteraation jälkeen, ja arviot ovatkin tarkentuneet ja toteutuksissa on tapahtunut kehitystä työn aikana. Kehitettäviä osa-alueita case-organisaatiossa ovat liiketoiminnan jatkuvuuden näkökulmasta arviointien perusteella vielä eri politiikkojen, strategioiden ja joidenkin käytännön toimenpiteiden tarkentaminen, kuten liiketoiminnan vaikutusanalyysit ja organisaatiotason jatkuvuussuunnitelmat ja -menettelyt.

Liiketoiminnan jatkuvuuden hallintajärjestelmän hahmotelmaversion (liite 3) rakenne noudattelee ISO 22301-standardin rakennetta. Liitteestä 3 on poistettu case-organisaation tietoja, joten kyseessä on vain runko hallintajärjestelmän todellisesta versiosta, joka on todelliselta laajuudeltaan suurempi. Liitteen 3 mukainen versio hallintajärjestelmästä kuvaa toteutusta yleistasolla muun muassa kuvaamalla vastuita, mittareita ja politiikkoja vain osittaisilla tiedoilla tai esittämällä toteutuksen niin sanotuilla placeholder-tiedoilla, kuten ”toimintamalli 1, 2 ja 3”. Case-organisaation anonymiteetin varmistamiseksi ja tietojen suojaamiseksi esitellään vain hallintajärjestelmän rakenne osittaisilla ja esimerkkitiedoilla.

Hallintajärjestelmän runko sisältää esimerkinomaisesti alleviivattuja kohtia, jotka demonstroivat lopullisen toteutuksen mukaisia hyperlinkkejä (case-organisaation sisäverkossa), jotka osoittavat ja viittaavat organisaatiosta löytyvään tietoon, jonka sijainti on jossain muualla, kuin suoraan itse hallintajärjestelmässä. Viitattu tieto voi löytyä esimerkiksi osana jo olemassa olevan tietoturvallisuuden hallintajärjestelmän toteutusta, tai viitata perehdytysmateriaaleihin muissa sijainneissa.

Näin toimimalla dokumentoidun tiedon versionhallinta helpottuu, jolloin tieto ei ole tallennettu useampaan paikkaan, mikä mahdollistaisi useampien versioiden yhtäaikaisen olemassaolon ja tätä kautta mahdollisen ristiriidan tiedoissa. Lopullinen hallintajärjestelmän toteutus ei tule olemaan Word-dokumentin muodossa. Liitteen 3 mukaisen hallintajärjestelmän on tarkoitus kuvata kehitystyön aikaansaannoksia yleistasolla. Lopullinen hallintajärjestelmä toteutetaan case-organisaation sisäverkkoon.

Hallintajärjestelmän runko sisältää kehitystyön tässä vaiheessa myös vaaditut dokumentoidut tiedot sekä tarvittaessa vaadittavat tiedot kunkin luvun lopussa, jotta soveltuvuusarviointien (liitteet 1 ja 2) tulokset ovat nähtävissä hallintajärjestelmässä kuvatun toteutustavan yhteydessä, jolloin

voidaan nähdä toteutustapa ja sen soveltuvuus hallintajärjestelmään yhdestä paikasta. Kehitystyön edetessä lukujen lopusta löytyvät soveltuvuusarvioinnit siirrettäneen kokonaisuudessaan lopullisen hallintajärjestelmän suorituskyvyn arvioinnin lukuun, jossa suorituskykyä ja mittarointia toteutetaan ja hallintajärjestelmää arvioidaan jatkuvasti. Tällöin opinnäytetyön aikaisessa kehitysvaiheessa käytetty soveltuvuusarviointi-Excel poistuu käytöstä ja siirtyy myös organisaation sisäverkkoon.

Liiketoiminnan jatkuvuuden hallintajärjestelmän standardin ISO 22301 mukaisella toteutuksella on mahdollista saavuttaa hyötyjä todella kokonaisvaltaisesti yritys- ja liiketoiminnassa, kuten jatkuvuuden hallintajärjestelmää käsittelevässä luvussa 3.3 todettiin peilaten kyseiseen standardiin.

Hyötyjä ovat muun muassa organisaation kriisinkestävyyden vahvistaminen ja organisaation parempi kykyä toimia vaikuttavasti häiriöiden aikana. Hallintajärjestelmän vaatimukset toteuttavat ratkaisut mahdollistavat paremmat tiedot mahdollisen häiriön todellisista vaikutuksista riskienhallinnan ja liiketoiminnan vaikutusanalyysin tulosten kautta. ISO-hallintajärjestelmien mukaiset toteutukset edistävät jatkuvaan parantamiseen perustuvan ympäristön luomista.

Asetetut tavoitteet saavutettiin pääosin, eli jatkuvuuden hallintajärjestelmän ensimmäinen versio tai runko, josta jatkuvuudenhallintaa lähdetään kehittämään hallintajärjestelmän sertifikaattia kohti. Olennaisin osa hallintajärjestelmän kehittämistyötä oli kartoittaa ISO 22301-standardin asettamat vaatimukset, selvittää niiden toteutuminen case-organisaatiossa ja arvioida toteutusten soveltuvuus standardin asettamia vaatimuksia vasten, jonka jälkeen kaikki tämä pyrittiin koostamaan yhdeksi kokonaisuudeksi eli jatkuvuuden hallintajärjestelmän rungoksi.

Kehitystyön ja hallintajärjestelmän ensimmäisen version toteuttamisen myötä saatiin vastauksia aiemmin esitettyihin tutkimuskysymyksiin, jotka olivat:

1. Kuinka liiketoiminnan jatkuvuudenhallintaa on toteutettu case-organisaatiossa ennen liiketoiminnan jatkuvuuden hallintajärjestelmän kehittämisen aloittamista?

2. Mitä kehitettäviä osa-alueita case-organisaatiossa on liiketoiminnan jatkuvuuden näkökulmasta?

3. Mitä hyötyjä case-organisaatio saa ISO 22301-standardin mukaisesti toteutetusta jatkuvuuden hallintajärjestelmästä?

6.1 Jatkokehitys

Case-organisaatiolle toteutettava liiketoiminnan jatkuvuuden hallintajärjestelmää on pyritty kehittään hallintajärjestelmän sertifioinnin mahdollistamiseksi tulevaisuudessa. Tämä tarkoittaa kaikkien ISO 22301-standardin asettamien vaatimusten toteuttamista. Myös opinnäytetyön luvussa 4.1 listatut voidaan-vaatia-tiedot ja niiden dokumentit on pyritty huomioimaan heti hallintajärjestelmän toteutuksen elinkaaren alkuvaiheista asti, jolloin voidaan varmistaa hallintajärjestelmän ja sen osien kattavuus. Kehitystyössä oli tarkoitus huomioida eri osa-alueet heti projektin aloittamisesta asti, ettei jossain kehitystyön vaiheessa huomata jonkin osa-alueen tai toteutuksen osan-puuttuvan kokonaan.

Liiketoiminnan jatkuvuuden hallintajärjestelmää ei saatu täysin valmiiksi tämän opinnäytetyön puitteissa, mutta sen kehitystyötä jatketaan case-organisaatiossa samoin toimintaperiaattein kuin tähänkin mennessä. Tulevia jatkokehitystoimenpiteitä ovat soveltuvuusarviointien edelleen iterointi ja havaittujen kehitystarpeiden edistäminen. Arviointeja on tehty kehitystyön eri vaiheissa ja vaatimuksia on saatu toteutettua ja näin tapahtunee jatkossakin.

Liitteiden 1 ja 2 käyttämä arviointiasteikko on muuttunut värimaailmaltaan kehitystyön ajanjaksolla keltaisesta tai punaisesta väristä vihreämmäksi, kuvaten vaatimusten soveltuvuusarvioinnin parantunutta tilaa vaatimustenmukaisemmiksi. Joidenkin vaatimusten, esimerkiksi case-organisaatioin politiikkojen ja strategioiden osalta, on vielä päivitettävää ja myös joitain käytännön toimenpiteitä on vielä toteutettava ja kuvattava.

Kun soveltuvuusarviointien perusteella tehdyt muutokset ovat valmiita, voidaan ne tuoda osaksi hallintajärjestelmää. Lopullinen hallintajärjestelmä perustunee pääosin liitteen 3 mukaiseen liiketoiminnan jatkuvuuden hallintajärjestelmän hahmotelmarunkoon. Liite on Word-tiedoston muodossa, lopullinen hallintajärjestelmä ei tule olemaan Word-dokumentti ja siksi hallintajärjestelmän

rakennetta kuvaava liite ei anna todellista kuvaa lopullisesta toteutuksesta, mutta se kuvaa sen perusperiaatteen. Lopullisen hallintajärjestelmän toteutus on case-organisaation sisäverkkoon tehtävä toteutus.

Lopullinen hallintajärjestelmä perustunee liitteistä 1–3 muodostettavaan kokonaisuuteen, jossa on hallintajärjestelmän toteutusten sanallisia kuvauksia sekä linkkejä eri tieto- ja toteutussijainteihin. Näin toimimalla tarvittavat tiedot löytyvät yhdestä paikasta mikä helpottaa muun muassa dokumentoinnin versionhallintaa. Lisäksi näen, että hallintajärjestelmän kehityksessä voitaneen hyödyntää case-organisaatiossa toteutettavaa jatkuvuudenhallinnan prosessikuvausta ja siitä saatuja oppeja myös jatkuvuuden hallintajärjestelmässä ja sen vaatimuksissa.

Jatkuvuuden hallintajärjestelmän kehitystyön aikana tein myös havaintoja, ettei case-organisaatiossa ollut joiltain osin tietoutta olemassa olevasta tietoturvallisuuden hallintajärjestelmästä. Joissain tapauksissa tietoisuus hallintajärjestelmästä ja myös pääsy sen sisältämään tietoon olisi voinut edistää joitain työtehtäviä. Yksi jatkokehitysidea molempien hallintajärjestelmien osalta voisi olla paremman tietoisuuden edistäminen hallintajärjestelmistä ja niiden toteutuksista, toki työtehtävään, käyttö- ja tiedontarpeeseen sekä tiedonluokitteluun perustuen.

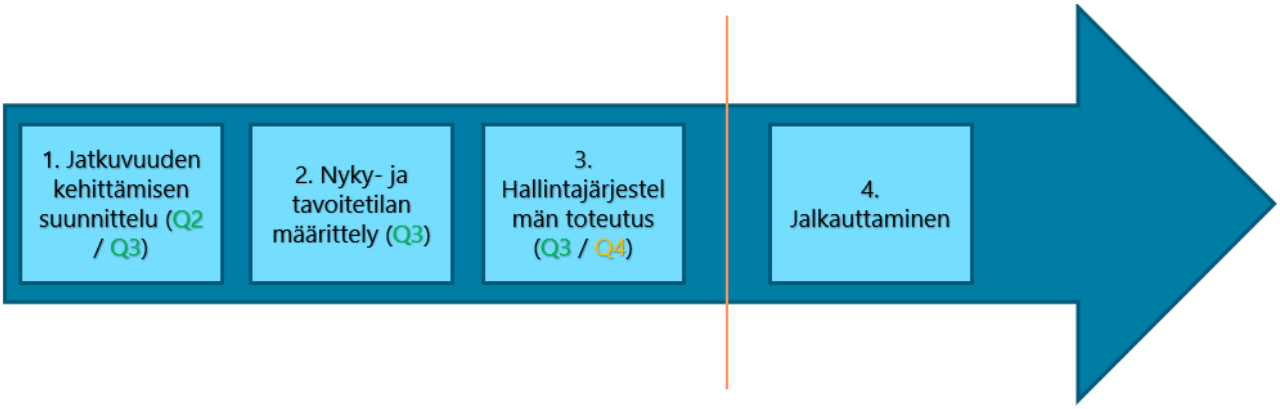
7 Pohdinta

Opinnäytetyön tavoite oli kehittää case-organisaation liiketoiminnan jatkuvuuden hallintajärjestelmää. Kehitystyö jaettiin kolmeen osaan, jotka olivat case-organisaation liiketoiminnan jatkuvuuden hallintajärjestelmän tavoitetilan määrittely (käsitelty luvussa 5.1), tietoperustan ja viitekehyksen rakentaminen (luku 5.2) sekä jatkuvuudenhallinnan alkukartoitus ja puutteiden arviointi (luku 5.3).

Jatkuvuuden hallintajärjestelmän lopulliseksi – opinnäytetyön ulkopuoliseksi – tavoitteeksi asetettu standardin ISO 22301 mukainen sertifioituminen määritteli myös kehitystyötä, sillä kehitystyö on tällöin tehtävä standardin vaatimusten mukaisesti. Standardin valinnassa ei siis ollut valinnan varaa, mutta kyseisen standardin mukainen toteutus on parhaiten integroitavissa muiden ISO-hallintajärjestelmien kanssa.

Koko hallintajärjestelmän toteuttaminen opinnäytetyön teon aikataulun puitteissa ei ollut lopulta realistinen tavoite johtuen muun muassa case-organisaation toimintojen laajuudesta ja kompleksisuudesta. Täysin valmiin hallintajärjestelmän toteutus ja kuvaaminen opinnäytetyössä olisi vaatinut opinnäytetyön venyttämistä yli tutkinnon valmistumisen tavoiteaikataulun.

Kuviossa 17 näkyy kehitystyön alussa toisella vuosineljänneksellä esitetty aikataulutus opinnäytetyön sisältämille kehitystyön vaiheille 1–3. Jatkuvuuden hallintajärjestelmän ensimmäisen version tavoitteena oli valmistua viimeisen vuosineljänneksen aikana.



Kuvio 17. Alustava aikataulusuunnitelma.

Kehitystyö eteni kuitenkin koko ajan ja hallintajärjestelmän kehittäminen jatkuu case-organisaatiossa opinnäytetyön aikaisen kehitystyön pohjalta myös opinnäytetyön jälkeen.

Pääpaino hallintajärjestelmän kehitystyökokonaisuuden osalta oli kartoittaa kaikki olemassa olevat toimintamallit ja prosessit ja arvioida niiden soveltuvuutta (useita iteraatioita kehitysprojektin aikana) jatkuvuuden hallintajärjestelmän vaatimuksia vasten, kehittää ja päivittää toimintamalleja soveltuvimmiksi jatkuvuuden hallintaan sekä rakentaa liiketoiminnan jatkuvuuden hallintajärjestelmän runko, joka toimii perustana lopulliselle hallintajärjestelmän toteutukselle opinnäytetyön jälkeen.

Case-organisaation ohjaamana kehitettiin myös hallintajärjestelmän lisäksi hallintajärjestelmän muodostavia osakokonaisuuksia, joista osaa myös ISO 22301-standardissa vaaditaan toteutetta-

viksi, kuten BIA-prosessia, BIA-analyysien perusteella tehtävää riippuvuuskartoitusta sekä jatkuvuudenhallinnan prosessikuvausta, jossa prosessikuvauksen lisäksi luodaan kokonaiskuvaa muun muassa rooleista ja vastuista sekä syntyvästä dokumentoidusta tiedosta.

Haasteena opinnäytetyössä oli standardin tulkitsemisen vaatimusten osalta ja vaatimusten ”kääntämisen” teoriasta käytäntöön, eli kuinka standardin asettama vaatimus tulisi toteuttaa. Opinnäytetyön kirjoittamisen ja hallintajärjestelmän kehittämisen edetessä ja aihetta käsittelevään teoriaan enemmän tutustuessa alettiin paremmin hahmottamaan kuinka rajata työtä sekä teoreettista aineistoa tarkemmin, ja mitä standardinmukaisuus vaatimuksissa tarkoittaa. Isoin yllätys kehitystyössä oli työn määrä. Hallintajärjestelmän asettamien vaatimusten kartoitus ja toteutusten arviointi työllistivät huomattavan paljon enemmän, kuin oltiin alun perin ajateltu.

Opinnäytetyön ja jatkuvuuden hallintajärjestelmän kehittäminen koettiin kokonaisuudessaan pääosin onnistuneeksi, vaikka tavoitteena oli toteuttaa hallintajärjestelmän niin sanottu 1. vedos valmiimmaksi opinnäytetyön toteutuksen aikana, eli kuvion 17 mukaisen aikataulusuunnitelman mukaisesti. Kehitystyötä aloittaessa, yhdessä toimeksiantajan kanssa määriteltynä, tavoitteena oli saada hallintajärjestelmän runko pääosin valmiiksi, mutta työn edetessä realiteetit, kuten työajan jakautuminen, kävivät selviksi ja että kehitystyö vaatisi lisäaikaa opinnäytetyön toteutuksen jälkeenkin.

Toimeksiantajaorganisaation kanssa alkuperäisiä tavoitteita määritellessä keskustelimme hallintajärjestelmän kehitystyön jatkamisesta myös opinnäytetyön jälkeen. Kuvion 17 esittämän alkuperäisen aikataulun mukaisena tavoitteena oli saada ensimmäinen versio hallintajärjestelmästä valmiiksi viimeisen vuosineljänneksen aikana, mutta valmistuminen siirtynee seuraavan vuoden ensimmäiselle vuosineljännekselle.

Jos aloittaisin jatkuvuuden hallintajärjestelmän kehitystyön alusta, uskoisin pystyväni tekemään sen paremmin ja varsinkin vähemmällä vaivalla. Esimerkiksi tarkempi suunnittelu ja aikataulutus olisivat voineet auttaa, vaikka toisaalta aikataulujen toteutumiseen ei aina voi itse vaikuttaa. Myös tarkemmin tutustuminen hallintajärjestelmiin ennen toteutuksen aloittamista olisi voinut helpottaa kehitystyötä, nyt aihepiiriin tutustuminen oli käynnissä osittain yhtä aikaa toteutuksen kanssa,

mikä näkyi muun muassa siinä, että jatkuvuuden hallintajärjestelmän vaatimusjaottelu (soveltuvuusarviointitaulukko) meni kertaalleen osittain uusiksi uuden tiedon myötä ja tästä syntyi lisätyötä. Lisäksi koen, että karttuneen osaamisen lisäksi tiedon haku sekä tulkinta kehitystyön aihepiirin osalta ovat kehittyneet ja näitä oppeja voin hyödyntää jatkossakin.

Opinnäytetyö käsittelee kattavasti jatkuvuudenhallinnan eri osa-alueita sekä avaa perusteellisesti ISO 22301-standardia, sen toimintaperiaatetta, sen asettamia vaatimuksia jatkuvuuden hallintajärjestelmän kehittämiselle sekä tuottaa tuloksia liitteiden 1–3 mukaisilla toteutuksilla. Täten opinnäytetyötä voidaan soveltaa käsikirjan omaisesti jatkuvuuden hallintajärjestelmän kehittämisessä.

Jatkuvuuden hallintajärjestelmän kehittämisen toimeksiannolla saavutettiin hyötyjä toimeksiantajalle. Jatkuvuudenhallinnan kehittämisen prosessi on käynnistetty, vaatimuksia ja niiden toteutuksia sekä puutteita on arvioitu, ja kehitystyö niin itse hallintajärjestelmän lopullisen toteutuksen osalta kuin myös jatkuvuuden hallintajärjestelmän vaatimusten osalta on edennyt ja etenee myös opinnäytetyön jälkeen.

Hallintajärjestelmän toteutuessa ISO 22301-standardin mukaisesti, saavuttaa case-organisaatio myös standardin mukaiset hyödyt, joita on kuvattu muun muassa jatkuvuuden hallintajärjestelmää käsittelevässä luvussa 3.3 ja tulokset-luvussa.

Lähteet

American Society for Quality. N.d. What is the Plan-Do-Check-Act (PDCA) Cycle?. Viitattu 30.8.2022. https://asq.org/quality-resources/pdca-cycle.

Athanasia, G. & Arcuri, G. 2022. Russia's Invasion of Ukraine Impacts Gas Markets Critical to Chip Production. Viitattu 16.10.2022. https://www.csis.org/blogs/perspectives-innovation/russias-invasion-ukraine-impacts-gas-markets-critical-chip-production.

Benefits of Business Continuity Management. N.d. Benefits of ISO 22301. Viitattu 30.8.2022. https://www.itgovernance.asia/iso22301-business-continuity-standard/benefits-of-iso-22301.

Betan, H. 2010. What is a business impact analysis questionnaire and what types of questions should be included? Viitattu 29.10.2022. https://www.techtarget.com/searchdisasterrecovery/answer/What-is-a-business-impact-analysis-questionnaire-and-what-types-of-questions-should-be-included.

Bhutada, G. 2021. The Top 10 Semiconductor Companies by Market Share. Viitattu 16.10.2022. https://www.visualcapitalist.com/top-10-semiconductor-companies-by-market-share/.

BSI-Standard 100–4. 2009. Business Continuity Standard. Viitattu 24.10.2022. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1.

Digi- ja väestötietovirasto. 2021. Digiturvallisuuden hallinta – tukimateriaali digiturvan kehittäjille. Viitattu 15.11.2022. https://dvv.fi/documents/16079645/0/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf/.

Digi- ja väestötietovirasto. 2022. Työkalut ja mallipohjat, Kriittisten kohteiden luokittelu (xlsx, 3/2022). Viitattu 29.10.2022. https://dvv.fi/digiturvajulkaisut.

Fingrid. 2022. Arvio sähkön riittävyydestä. Viitattu 16.10.2022 https://www.fingrid.fi/ajankohtaista/tiedotteet/2022/fingrid-paivitti-arvion-sahkon-riittavyydesta-tulevana-talvena-sahkon-kaytto-vahentynyt--saastotoimenpiteita-jatkettava/.

Fortinet. N.d. What is the Information Security Triad? Viitattu 5.11.2022.https://www.fortinet.com/resources/cyberglossary/cia-triad.

Freightify. 2021. Top 5 Busiest Global Major Shipping Routes 2022. Viitattu 1.10.2022. https://www.freightify.com/blog/busiest-global-trade-shipping-routes-2021.

Hargrave, M. 2021. PDCA Cycle. Viitattu 30.8.2022. https://www.investopedia.com/terms/p/pdca-cycle.asp.

HE 63/2022 vp. 2022. Hallituksen esitys eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta. Viitattu 16.10.2022. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_63+2022.aspx.

Helsingin Sanomat. 2022. Sähköpulassa on nyt tosi kyseessä: Talvella edessä ehkä kahden tunnin sähkökatkot. Viitattu 16.10.2022. https://www.hs.fi/kotimaa/art-2000009106010.html.

Henshall, A. 2020. How to Use The Deming Cycle for Continuous Quality Improvement. Viitattu 30.8.2022. https://www.process.st/deming-cycle/.

Huoltovarmuuskeskus. 2020. Jatkuvuudenhallinta. Viitattu 12.8.2022. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta.

Hübert, R. 2011. RTO, MTPD and putting the cart before the horse. Viitattu 25.10.2022. https://www.continuitycentral.com/feature0934.html.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tietosanoma.

Kanbanize. N.d. What is Plan-Do-Check-Act (PDCA) Cycle?. Viitattu 30.8.2022. https://kanbanize.com/lean-management/improvement/what-is-pdca-cycle.

Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 5.11.2022. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.

KUJA-pikatesti. 2019. KUJA-hanke ja varautumisen työkalut. Viitattu 24.9.2022. https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen.

Kyberturvallisuuskeskus. 2021. Katakri 2020 -arviointityökalu. Viitattu 10.11.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Katakri-2020-arviointityokalu.xlsx.

Lean Enterprise Institute. N.d. Plan, Do, Check, Act (PDCA). Viitattu 30.8.2022. https://www.lean.org/lexicon-terms/pdca/.

Liikenne- ja viestintäministeriö. 2020. Tietoturva. Viitattu 5.11.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

MacNeil, C. 2022. What is a business impact analysis (BIA)? 4 steps to prepare for anything. Viitattu 30.10.2022. https://asana.com/resources/business-impact-analysis.

Maymí, F. & Harris, S. 2022. CISSP All-in-One Exam Guide, Ninth Edition. McGraw Hill.

Oikeusministeriö. 2019. Viranomaisten toimivaltuudet häiriötilanteissa. Viitattu 30.10.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161604/OM_2019_18_Viranomaisten_toimivaltuudet_hairiotilanteissa.pdf.

Puolustusvoimat. N.d. Henkilövaraukset. Viitattu 30.10.2022. https://puolustusvoimat.fi/asiointi/henkilovaraukset.

PwC Suomi. N.d. Liiketoiminnan jatkuvuudenhallinta. Viitattu 24.9.2022. https://www.pwc.fi/fi/palvelut/riskienhallinta/liiketoiminnan-jatkuvuudenhallinta.html.

Roskoski, M. 2020. Understanding the updated ISO 22301 business continuity management systems standard. Viitattu 25.10.2022. https://www.fmlink.com/articles/understanding-updated-iso-22301-business-continuity-management-systems-standard/.

Seclion. 2020. Mitä on hallinnollinen tietoturvallisuus? Viitattu 5.11.2022. https://blog.seclion.fi/turvallisuus/hallinnollinen-tietoturvallisuus.

Second Nature Security. N.d. Hallinnollinen tietoturva – Mitä se on? Viitattu 5.11.2022. https://www.2ns.fi/hallinnollinen-tietoturva-mita-se-on/.

SFS-ISO 22301:2019. Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallinta järjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto.

SFS-ISO 22313:2020. Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuudenhallintajärjestelmät. Ohjeistusta standardin ISO 22301 käyttöön. Helsinki: Suomen Standardoimisliitto. Viitattu 8.8.2022. https://janet.finna.fi/, SFS Online.

Shiphub. N.d. World's top semiconductor producers. Viitattu 16.10.2022. https://www.shiphub.co/worlds-top-semiconductors-producers/.

Sisäministeriö. 2019. Kansallinen riskiarvio 2018. Viitattu 30.10.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf?sequence=4&isAllowed=y.

Suomidigi. N.d. VAHTI-ohjeet. Viitattu 14.11.2022. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet.

Tietoa huoltovarmuudesta. N.d. Huoltovarmuuskeskuksen kuvaus jatkuvuudenhallinnasta. Viitattu 24.9.2022. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta.

Tutkimuksellinen kehittämishanke opinnäytetyönä vs projektityö. N.d. Viitattu 1.11.2022. https://oppimateriaalit.jamk.fi/yamk-kasikirja/tyoelaman-tutkiva-kehittamistoiminta/projektityo-vs-ns-toiminnallinen-tutkimuksellinen-kehittamishanke-opinnaytetyo/.

Tutkimusasetelma. N.d. Jyväskylän ammattikorkeakoulun ohjeet opinnäytetyön tutkimusasetelmasta. Viitattu 1.11.2022. https://oppimateriaalit.jamk.fi/raportointiohje/4-opinnaytetyon-rakenne/4-2-opinnaytetyon-runko-osa/4-2-4-tutkimusasetelma/.

Ulkoministeriö. N.d. Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 4.11.2022. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille.

Vahti 2/2012. 2012. ICT-varautumisen vaatimukset. Viitattu 30.10.2022. https://www.suomidigi.fi/sites/default/files/2020-07/2012_VAHTI_ohje_ICT_varautuminen_vaatimukset.pdf.

Valmiuslaki 1552/2011. Laki viranomaisten toimivaltuuksista poikkeusoloissa. Annettu 29.12.2011. Viimeisin muutos 1.8.2022. Viitattu 16.10.2022. https://www.finlex.fi/fi/laki/ajantasa/2011/20111552#O1L3P12.

Valtioneuvosto. 2020. Kansallinen turvallisuusauditointikriteeristö Katakri 2020. Viitattu 4.11.2022. https://valtioneuvosto.fi/-/kansallinen-turvallisuusauditointikriteeristo-katakri-2020-julkaistu.

Valtionvarainministeriö. 2016. Toiminnan jatkuvuuden hallinta. Vahti 2/2016. Viitattu 8.8.2022. https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf.

Valtionvarainministeriö. 2017. Ohje riskienhallintaan. Vahti 22/2017. Viitattu 16.10.2022. https://www.suomidigi.fi/sites/default/files/2020-06/VM_22_2017_1.pdf.

Valtiovarainministeriö. 2008. Vahti 2/2008, Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Viitattu 511.2022. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2008.pdf.

Valtiovarainministeriö. N.d. Ohjaus. Viitattu 14.11.2022. https://vm.fi/ohjaus.

Wikipedia. 2022. Malakansalmi. Viitattu 1.10.2022. https://fi.wikipedia.org/wiki/Malakansalmi.

Wojno, R. 2022. 4 Practical risk mitigation strategies for your business. Viitattu 22.10.2022. https://monday.com/blog/project-management/risk-mitigation/.

Yhteiskunnan turvallisuusstrategia. 2017. Valtioneuvoston periaatepäätös / 2.11.2017. Viitattu 30.10.2022. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf.

Liitteet

Liite 1. Soveltuvuusarviointi – BCMS:ssä edellytetty dokumentoitu tieto

Arviointiasteikko:
Soveltuu
Soveltuu osittain
Ei sovellu
Arviointi kesken

Ohjaavan standardin ISO 22313 mukaan jatkuvuuden hallintajärjestelmän dokumentoidun tiedon tulee sisältää:

Tila	Lausekenro	Lauseke	Toteutustapa	Kuvaus lausekkeesta	Lisätietoa / huomioitavaa	Myös ISO 27001:n
	4.1	Organisaation ja sen toimintaympäristön ymmärtäminen	Toimintaympäristö kuvauksen linkki	Organisaation on määritettävä ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta ja jotka vaikuttavat sen kykyyn saavuttaa liiketoiminnan jatkuvuuden hallintajärjestelmältä halutut tulokset.		
	4.2.2	Lakien ja viranomaisten vaatimukset		Vaatimukset oltava dokumentoituna sekä pidettävä ajantasalla. Organisaatio on tietoinen sovellettavista lakien ja viranomaisten vaatimuksista.		Kyllä
	4.3	Liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalan ja rajaukset		Varmistetaan kaikkien merkityksellisten tuotteiden, palveluiden, toimintojen, toimipaikkojen, resurssien, toimittajien ja muiden riippuvuussuhteiden sisältyminen hallintajärjestelmään.		
	5.2	Liiketoiminnan jatkuvuuden toimintaperiaatteet (politiikka)		Organisaation tavoitteiden ja velvollisuuksien mukaiset liiketoiminnan jatkuvuuden periaatteet.		
	6.2	Liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu		Ylimmän johdon dokumentti siitä, mitä hallintajärjestelmällä halutaan saavuttaa ja millä keinoilla (ylätason kuvaus)		
	7.2	Työntekijöiden pätevyys/osaaminen		BCMS:n parissa tai siihen liittyvien henkilöiden osaamisen määrittäminen, hankkiminen ja varmistaminen (mittaaminen tms.)	Organisaatio itse määrittää mm. mikä on riittävä pätevyys. Henkilöt, joiden työ vaikuttaa ISMS/BCMS tai niiden osiin. Osaaminen muodostuu kokemuksesta, harjoittelusta, koulutuksista. *Organisaation olisi laadittava tarkoituksenmukainen ja vaikuttava järjestelmä pätevyyden hallintaan palveluksessaan työskenteleville henkilöille, jotka suorittavat liiketoiminnan jatkuvuuden hallintajärjestelmään*	Kyllä
	8.2	Liiketoiminnan vaikutusanalyysi ja riskien arviointi		Toteutettava järjestelmällinen prosessi häiriön aiheuttamien liiketoiminnallisten vaikutusten analysointia ja sen aiheuttamien riskien arviointia varten sekä ylläpidettävä kyseistä prosessia. Katselmoitava ja arvioitava kyseisiä prosesseja.		
	8.3	Liiketoiminnan jatkuvuusstrategiat ja -ratkaisut	Eri politiikat	BIA:n ja riskien arvioinnin tuotosten perusteella organisaation on tunnistettava ja valittava liiketoiminnan jatkuvuusstrategiat (Ks. ISO22313, 8.3), joissa otetaan huomioon eri vaihtoehtoja häiriötä edeltävälle ajalle, häiriön tapahtuma-ajalle ja sen jälkeiselle ajalle. Liiketoiminnan jatkuvuusratkaisut koskevat priorisoidun toiminnon vakauttamista, jatkamista tai palauttamista (ISO 22313:2020).	Tarkemmat kuvaukset strategioiden ja ratkaisujen valinnoista ISO 22313:n luvussa 8.3.3.	

	8.4	Liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt	Jatkuvuus- ja toipumissuunnitelmien tallennuspaikat	Organisaation on toteutettava reagointimallit, jotka mahdollistavat varhaisen hälytyksen ja viestinnän olennaisille sidosryhmille. Siinä on oltava suunnitelmia ja menettelyitä, joiden mukaisesti organisaatiota hallitaan häiriön aikana. Suunnitelmia ja menettelyjä on noudatettava, kun liiketoiminnan jatkuvuusratkaisuja on käynnistettävä (ISO 22301:2019). HUOM. Liiketoiminnan jatkuvuussuunnitelmiin sisältyy erityyppisiä menettelyitä Ks. esim. I-sarakkeen dokumentti sekä ISO 22313:2020, luku 8.4.2.2.		Kyllä
	8.5	Harjoitussuunnitelmat		Organisaation on toteutettava harjoitus- ja testaussuunnitelma, jolla todennetaan sen liiketoiminnan jatkuvuusstrategioiden ja -ratkaisujen vaikuttavuus ajan mittaan. Sen on myös ylläpidettävä tätä suunnitelmaa.		
	9.1	Suorituskyvyn arviointi - Seuranta, mittaus, analysointi ja arviointi		Organisaation on arvioitava liiketoiminnan jatkuvuuden hallintajärjestelmän tasoa ja liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuutta		Kyllä
	9.2	Sisäinen auditointi		Organisaation on tehtävä suunniteltuin aikavälein sisäisiä auditointeja varmistaakseen hallintajärjestelmän vaatimuksenmukaisuus ja vaikuttavuus. Dokumentoitava sisäisen auditoinnin menettelytavat		Kyllä
	9.2	Sisäisen auditoinnin tulokset		Dokumentoitu tieto hallintajärjestelmän sisäisten auditointien tuloksista		Kyllä
	9.3	Johdon katselmus ja sen tulokset		Tieto johdon tekemistä päätöksistä ja mahdollisista muutoksista		Kyllä
	10.1	Poikkeamat ja korjaavat toimenpiteet		Usually, this is covered through the procedure of corrective actions - **if you already have ISO 27001**, then you can use the existing procedure for this purpose. *Organisaation olisi määritettävä liiketoiminnan jatkuvuuden hallintajärjestelmän parantamismahdollisuudet ja toteutettava haluttujen tulosten saavuttamiseen tarvittavat toimenpiteet, jotta liiketoiminnan jatkuvuuden hallintajärjestelmän haluut tulokset saavutetaan.* (ISO		Kyllä
	10.1	Poikkeamien toimenpiteiden tulokset		Organisaation on säilytettävä dokumentoitua tietoa näyttönä tehtyjen jatkuvuudenhallintaan tehtyjen korjaavien toimenpiteiden tuloksista.		Kyllä

Liite 2. Soveltuvuusarviointi - Voidaan vaatia dokumentoituna tietona BCMS:n vaikuttavuuden arvioinnissa

Lisäksi voidaan vaatia, että dokumentoitu tieto kattaa seuraavat asiat, jotta voidaan varmistaa liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuus (ISO 22313:2020, luvun 7.5 mukaisesti):

Tila	Lauseke nro.	Dokumentit ja tallenteet (ei lausekkeen nimi)	Miten toteutettu / Linkki / Viittaus	Kuvaus lausekkeesta (mitä tarkoitus saavuttaa)	Lisätietoa tai huomioitavaa	Myös ISO 27001:n vaatimus?
	7.2 *	Koulutus- ja tietoisuussuunnitelma		Hallintajärjestelmän tai sen osien parissa työskentelevien, **organisaation itsensä määrittelemä**, asianmukainen ja tehokas koulutus- ja osaamissuunnitelma. Koulutus voi liittyä esim. BIAan tai riskienarviointiin	Henkilöt, joiden työ vaikuttaa ISMS/BCMS tai niiden osiin. Esim. vuosittainen koulutus. "Koulutusrekisteri". Näin voidaan todeta, että koulutuksia on järjestetty asianmukaisesti.	Kyllä
	7.3	Tietoisuus	Tukitoiminnot - Tietoisuus ja viestintä		Osaltaan samaa kuin 7.2. Tietoisuus esimerkiksi politiikoista ja ohjeista sekä työntekijöiden omista rooleista liittyen ISMS/BCMS.	
	7.5	Menettelytapa dokumentoidun tiedon hallinnalle		Standardissa ISO 22301 edellytetty dokumentoitu tieto tarjoaa näyttöä vaatimustenmukaisuudesta ja hallintajärjestelmän vaikuttavasta toiminnasta. **Dokumentoitua tietoa ovat ISO 22313:n mukaan kaikki ISO 22301:n pakolliset ja suosittelemat dokumentit, jotka ovat tähänkin Exceliin listattu.**	If you already implemented some other standard like ISO 9001, ISO 14001, ISO 22301, or similar, you can use the same procedure for all these management systems. ISO 22313:2020, luku 7.5.1, sivu 27 listaa kaikki ISO 22301-standardissa edellytetyn dokumentoidun tiedon - pakolliset ja ei-pakolliset dokumentit, joita tähänkin Excel-tiedostoon on kerätty. ISO 22313 ei listaa tätä pakollisena eikä suositeltuna. 22313 listaa tässä luvussa dokumentoidun tiedon vaatimukset ja suositukset, joihin tämänkin dokumentin jaottelu perustuu	
	8.1	Sopimukset ja SLA:t - Toimittajat (esim. laitetoimittajat), alihankkijat yms.	Sopimushallinta	Varmistetaan toimittajien, alihankkijoiden yms. Reagoivan sovituin keinoin häiriötilanteisiin.		
	8.2.2	Liiketoiminnan vaikutusanalyysin (BIA) tulokset		Ohjaava standardi 22313 listaa BIA-tulokset ei-pakollisina		
	8.2.3	Riskinarvioinnin tulokset		Toteutettava riskien arviointiprosessi ja ylläpidettävä sitä. Riskienarvioinnin tulokset dokumentoitava. Ohjaava standardi 22313 listaa BIA- ja riskien arviointien tulokset ei-pakollisina.	Riskien arviointia käsitellään standardeissa ISO 27001, ISO 27005, ISO 31000. ISO 22301 ei aseta vaatimuksia itse prosessille.	Kyllä
	8.4.3.1	Dokumentoitu tieto viestinnästä sisäisten ja ulkoisten olennaisten sidosryhmien kanssa		Dokumentoitava ja ylläpidettävä menettelyjä ja toimintatapoja, joilla varmistetaan häiriön aikainen **sisäinen ja ulkoinen** viestintä olennaisille sidosryhmille ja osapuolille (ISO 22301:2019). Ks. ISO 22313:2020 s. 49 tarkennukset		
	8.4.3.1	Tallennetaan häiriötä, suoritettuja toimintoja ja tehtyjä päätöksiä koskeva tieto.		Tärkeän häiriötilannetta, suoritettuja toimintoja ja tehtyjä päätöksiä koskevan tiedon tallentaminen.		
	8.5	Insidenttiskenaariot (Harjoitusten tapahtumaskenaariot)		Riskien arviointiin perustuvia harjoitusskenaarioita ja niiden kuvauksia suurimpien kokonaisvaikutusten riskeistä ja kuinka ne voisivat toteutua yrityksessä + niiden vaikutukset yritykselle		

	8.5	Harjoitus- ja testaussuunnitelmat		Organisaation on toteutettava harjoitus- ja testaussuunnitelma, jolla todennetaan sen liiketoiminnan jatkuvuusstrategioiden ja -ratkaisujen vaikuttavuus ajan mittaan. Sen on myös ylläpidettävä tätä suunnitelmaa	Jokaisen suunnitelman tulisi määritellä harjoituksen tavoitteet sekä harjoitusskenaariot	
	8.5	Harjoitusraportit ja tulokset		Harjoittelun jälkeinen dokumentointi, josta käy ilmi mm. saavutettiinko harjoituksen tavoitteet		
	8.6	Liiketoiminnan jatkuvuuden dokumentaatioiden ja kyvykkyyksien arviointi		Nämä arvioinnit on suoritettava suunnitelluin aikavälein, häiriötilanteen tai käynnistämisen jälkeen sekä jos tapahtuu merkittäviä muutoksia. *Organisaation olisi arvioitava liiketoiminnan vaikutusanalyysiään, riskien arviointiaan, strategioitaan ja ratkaisujaan, liiketoiminnan jatkuvuussuunnitelmiaan ja -menettelyitään, jotta se kykenee varmistamaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia (ISO 22313:2020)* .	Arvioinnit voidaan suorittaa sisäisinä tai ulkoisina auditointeina tai itsearviointeina. ISO 22313:2020 listaa, mitä arvioinneilla olisi varmennettava.	
	9.1 *	Suorituskyvyn arvioinnin menettelytavat - Seuranta, mittaus, analysointi ja arviointi		Organisaation on arvioitava liiketoiminnan jatkuvuuden hallintajärjestelmän tasoa ja liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuutta.	Organisaation tulee määritellä mm. mitä ja miten mitataan/monitoroidaan. Lisätietoa ISO 22313:2020.	

Liite 3. Liiketoiminnan jatkuvuuden hallintajärjestelmän hahmotelmaversio

Sisällys

Versio: x.x

Asiakirjasta vastaa:

Versionhallinta:

Versio	Päivitetty	Muutokset	Tekijä

Johdanto

Tässä asiakirjassa määritetään sisäiset ja ulkoiset asiat, jotka ovat merkityksellisiä organisaation jatkuvuuden hallinnan kannalta, ja jotka vaikuttavat organisaation kyvykkyyteen saavuttaa sille asetetut tavoitteet.

Tämän asiakirjan tarkoituksena on määritellä, mitä liiketoimintakriittisiä toimintoja organisaatio suojaa liiketoiminnan jatkuvuuden hallintajärjestelmällään eli BCMS-järjestelmällään (Business Continuity Management System). Asiakirjassa kuvataan myös itse BCMS-järjestelmä ja se, mitä hallintajärjestelmään kuuluu, jotta sille asetetut vaatimukset toteutuvat.

BCMS-järjestelmään on sovellettu ISO 22301:2019-standardin rakennetta, joka on myös yhtenevä organisaatiossa jo käytössä olevan standardiin ISO 27001 perustuvan tietoturvallisuuden hallinta-järjestelmän kanssa.

BCMS on osa yleistä johtamisjärjestelmää, joka luo, toteuttaa ja käyttää, seuraa, tarkistaa, ylläpitää ja parantaa liiketoiminnan jatkuvuutta.

Liiketoiminnan jatkuvuuden hallinnan standardissa määritellään vaatimukset, jotka koskevat dokumentoidun hallintajärjestelmän suunnittelua, perustamista, toteuttamista, käyttöä, seurantaa, tarkistamista, ylläpitoa ja jatkuvaa parantamista, jotta voidaan suojautua häiriötilanteilta, vähentää niiden esiintymistodennäköisyyttä, varautua niihin, reagoida niihin ja toipua niistä.

Tämä asiakirja sisältää kuvaustavat vaatimusten toteuttamiselle, sekä soveltuvuusarvioinnin vaaditulle dokumentoidulle tiedolle sekä tarvittaessa käytettävälle tiedolle, jota voidaan vaatia hallinta-järjestelmän vaikuttavuuden arviointiin. Soveltuvuusarviointi käyttää asteikkoa soveltuu – sovel-tuu osittain – ei sovellu. Tulokset löytyvät hallintajärjestelmän lukujen lopusta

klausuulinumeroineen. Arviointi- ja toteutus-Excel löytyy erikseen työtilasta X ja sen ylläpidosta vastaa henkilö Y.

ISO 22301:2019-standardin mukaisen liiketoiminnan jatkuvuuden hallintajärjestelmän vaatimukset dokumentoidulle tiedolle:

7.5.1 Yleistä (EN)

Standardissa ISO 22301 edellytetty dokumentoitu tieto tarjoaa näyttöä vaatimustenmukaisuudesta ja hallintajärjestelmän vaikuttavasta toiminnasta.

Termi *menettely* tarkoittaa tiettyä tapaa suorittaa toiminto tai prosessi. *Dokumentoitu menettely* tarkoittaa, että menettelyn olisi oltava määritelty ja sitä olisi ylläpidettävä soveltuvassa muodossa.

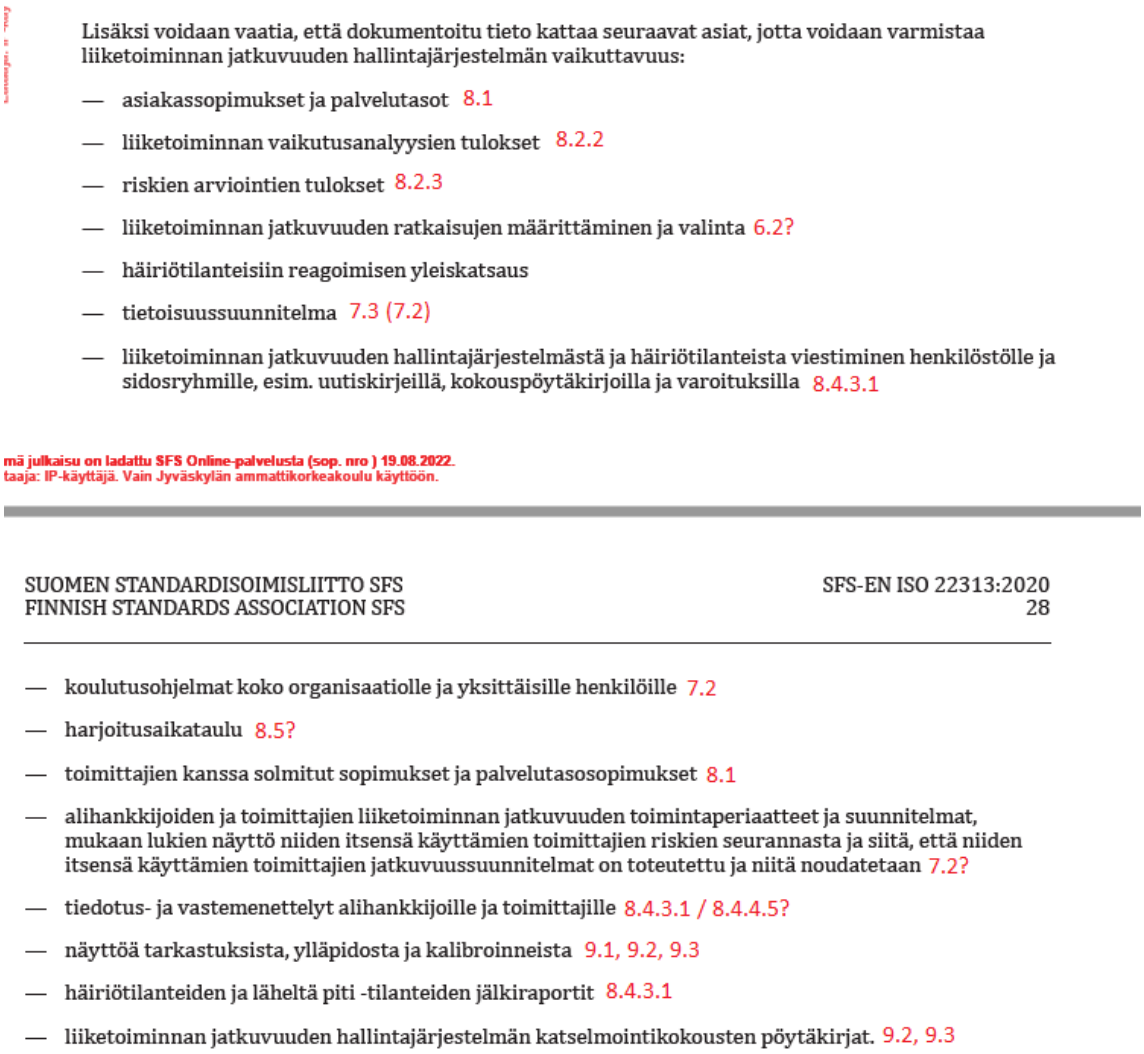
Yksittäinen asiakirja voi kattaa yhden tai useamman dokumentoidun menettelyn vaatimukset, ja dokumentoitua menettelyä koskeva vaatimus voidaan kattaa yhdellä tai useammalla asiakirjalla.

Dokumentoitu tieto sisältää

- organisaation ja sen toimintaympäristön ymmärtämisen (ks. 4.1)
- lakien ja viranomaisten vaatimukset (ks. 4.2.2)
- liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalan ja rajaukset (ks. 4.3)
- toimintaperiaatteet (ks. 5.2)
- liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelun (ks. 6.2)
- pätevyyden (ks. 7.2)
- liiketoiminnan vaikutusanalyysin ja riskien arvioinnin (ks. 8.2)
- liiketoiminnan jatkuvuusstrategiat ja -ratkaisut (ks. 8.3)
- liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt (ks. 8.4)
- harjoitussuunnitelman (ks. 8.5)
- seurannan, mittauksen, analysoinnin ja arvioinnin (ks. 9.1)
- sisäisen auditoinnin (ks. 9.2)
- johdon katselmuksen (ks. 9.3)
- poikkeamat ja korjaavat toimenpiteet (ks. 10.1).

Kuva 1. ISO 22313:2020 ohjeistus vaatimuksista ISO 22301-standardissa.

Ns. ei-pakolliset, mutta usein käytetyt dokumentit jatkuvuuden hallintajärjestelmissä.



Lisäksi voidaan vaatia, että dokumentoitu tieto kattaa seuraavat asiat, jotta voidaan varmistaa liiketoiminnan jatkuvuuden hallintajärjestelmän vaikuttavuus:

— asiakassopimukset ja palvelutasot 8.1
— liiketoiminnan vaikutusanalyysien tulokset 8.2.2
— riskien arviointien tulokset 8.2.3
— liiketoiminnan jatkuvuuden ratkaisujen määrittäminen ja valinta 6.2?
— häiriötilanteisiin reagoimisen yleiskatsaus
— tietoisuussuunnitelma 7.3 (7.2)
— liiketoiminnan jatkuvuuden hallintajärjestelmästä ja häiriötilanteista viestiminen henkilöstölle ja sidosryhmille, esim. uutiskirjeillä, kokouspöytäkirjoilla ja varoituksilla 8.4.3.1

— koulutusohjelmat koko organisaatiolle ja yksittäisille henkilöille 7.2
— harjoitusaikataulu 8.5?
— toimittajien kanssa solmitut sopimukset ja palvelutasosopimukset 8.1
— alihankkijoiden ja toimittajien liiketoiminnan jatkuvuuden toimintaperiaatteet ja suunnitelmat, mukaan lukien näyttö niiden itsensä käyttämien toimittajien riskien seurannasta ja siitä, että niiden itsensä käyttämien toimittajien jatkuvuussuunnitelmat on toteutettu ja niitä noudatetaan 7.2?
— tiedotus- ja vastemenettelyt alihankkijoille ja toimittajille 8.4.3.1 / 8.4.4.5?
— näyttöä tarkastuksista, ylläpidosta ja kalibroinneista 9.1, 9.2, 9.3
— häiriötilanteiden ja läheltä piti -tilanteiden jälkiraportit 8.4.3.1
— liiketoiminnan jatkuvuuden hallintajärjestelmän katselmointikokousten pöytäkirjat. 9.2, 9.3

Kuva 2. ISO 22313:n ohjeistus.

Ohjaava standardi ISO 22313 ei anna klausuulinumeroita näille dokumenteille. Punaiset tekstit ovat aputekstejä, joista selviää parhaiten soveltuva ISO 22301-standardin klausuulinumero, jotta vaatimuksia voidaan tarkastella helpommin.

Tämän asiakirjan luvut 4–10 ovat ISO 27001 & 22301 rakenteiden mukaisia ”hahmotelmia” hallintajärjestelmän sisällöstä. Lukujaottelu alkaa luvusta 4 kuvaten mainittujen standardien vaatimuksia asettavia lukuja, jolloin tämän hallintajärjestelmän dokumentin luvut sopivat yhteen standardien lukujen kanssa. Esimerkiksi tämän dokumentin luku 4 Organisaation toimintaympäristö on myös ISO 22301:ssa luku 4 Organisaation toimintaympäristö.

Luvuista löytyvät alleviivatut alaluvut ovat hallintajärjestelmästä löytyviä / siihen kuuluvia hyperlinkkejä, jotka osoittavat kyseisen toteutuksen sijainnin. Näin toimimalla voidaan viitata jo ISO 27001 mukaisesti toteutetun hallintajärjestelmän toteutuksen myötä syntyneeseen tietoon, joka soveltuu myös liiketoiminnan jatkuvuuden hallintajärjestelmän toteutukseen.

4. Organisaation toimintaympäristö

Hallintajärjestelmään vaikuttava toimintaympäristö

Hallintajärjestelmään vaikuttavia toimintaympäristöjä ovat ulkoiset ja sisäiset asiat.

Ulkoinen toimintaympäristö tarkoittaa ympäristöä, jossa organisaatio pyrkii saavuttamaan tavoitteensa.

Sisäinen toimintaympäristö tarkoittaa ympäristöä, jonka avulla organisaatio pyrkii saavuttamaan tavoitteensa.

Hallintajärjestelmän kattavuus

Hallintajärjestelmää toteutetaan organisaatiossa ja sen tuottamissa palveluissa sekä käyttämissä prosesseissa ja sisäisissä tukipalveluissa.

ISO 22301 -standardin vaatimat pakolliset dokumentit:

4.2.2 Listaus lakien, säännösten ja viranomaisten vaatimuksista. Soveltuu.

4.2.2 Menettelytavat vaadittavien lakien ja säännösten vaatimusten tunnistamiseen. Soveltuu.

4.3 Liiketoiminnan jatkuvuuden hallintajärjestelmän soveltamisalan (scope) määrittäminen, sekä perustelut rajauksille, jos niitä on. Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

-

5. Johtajuus

Ylimmän johdon on osoitettava johtajuutta ja sitoutumista liiketoiminnan jatkuvuuden hallintajärjestelmän suhteen mm. seuraavin keinoin: - liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet laaditaan ja liiketoiminnan jatkuvuuden tavoitteet asetetaan ja että ne ovat yhdenmukaisia organisaation strategian kanssa - viestimällä siitä, miten tärkeää on, että liiketoiminnan jatkuvuuden hallinta on vaikuttavaa ja että liiketoiminnan jatkuvuuden hallintajärjestelmää koskevia vaatimuksia noudatetaan

Politiikat ohjaavat liiketoiminnan jatkuvuuden toimintaperiaatteita.

- Politiikka 1
- Tietoturva- ja tietosuojapolitiikka
- Politiikka 3
- Politiikka 4

Organisaation jatkuvuuden hallintajärjestelmä on laadittu yhdessä johdon kanssa.

Johtajuutta osoitetaan keinoilla X, Y, Z.

Johtamisen tarkoituksena on…

ISO 22301 -standardin vaatimat pakolliset dokumentit:

5.2 Liiketoiminnan jatkuvuuden toimintaperiaatteet (politiikat). Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

-

6. Suunnittelu

1. Riskienhallinta

2. Tavoitteet ja niiden suunnitelmat

3. Jatkuvuuden tavoitteet – Vastuuhenkilöittäin

ISO 22301 -standardin vaatimat pakolliset dokumentit:

6.2 Liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu. Soveltuu osittain (vaatii tarkennusta).

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

-

7. Tukitoiminnot

1. Resurssit ja pätevyys

Organisaation on määriteltävä, hankittava sekä varmistettava liiketoiminnan jatkuvuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit.

Hallintajärjestelmän ylläpidosta vastaa X yhdessä Y sekä Z kanssa. Hallintajärjestelmää kehitetään johdolta saatujen tulostavoitteiden mukaisesti.

Hallintajärjestelmän ylläpito vaatii…

Hallintajärjestelmää ylläpitävän tahon tulee saada riittävä perehdytys hallintajärjestelmän ylläpitämiseen.

Hallintajärjestelmän sisäiset auditoinnit edellyttävät auditoijalta jääviyttä hallintajärjestelmän ylläpitoa kohtaan sekä dokumentointikykyä.

Ulkoisten sertifiointiarviointien osalta arvioijan tulee olla vaatimusten mukaisesti akkreditoitu sertifiointiarvioinnin suorittamiseksi.

Hallintajärjestelmän tai sen osien parissa työskentelevien, organisaation itsensä määrittelemä, asianmukainen ja tehokas koulutus- ja osaamissuunnitelma.

2. Tietoisuus ja viestintä

Turvallisuutta koskevaa viestintää toteutetaan usealla eri saralla.

- 1
- 2
- 3

Sisäistä viestintää toteutetaan seuraavissa tapauksissa ja seuraavilla menetelmillä:

- Tapaus 1
- Tapaus 2
- Tapaus 3

Häiriötilanteissa viestintää toteutetaan häiriötilanteiden hallintaprosessin mukaisesti.

3. Dokumentoitu tieto

Hallintajärjestelmää koskevat määräykset, politiikat ja raportit luodaan ohjeistuksen mukaisesti.

Tärkeimpiä dokumentteja ovat:

- Politiikka 1
- Politiikka 2

- Politiikka 3

ISO 22301 -standardin vaatimat pakolliset dokumentit:

7.2 Työntekijöiden pätevyys/osaaminen. Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

7.3 Tietoisuussuunnitelma. Soveltuu.

8. Toiminta

Organisaation olisi määritettävä, suunniteltava ja toteutettava prosessit, joita tarvitaan vaatimukset täyttävän liiketoiminnan jatkuvuuden hallinnan toteuttamiseen ja ylläpitämiseen (ks. organisaation toimintaympäristö / ISO 22301, kohta 4), sekä ohjattava niitä, ja toteutettava kohdassa Suunnittelu - Riskien ja mahdollisuuksien käsittely (ISO 22301 kohta 6.1), määritetyt toimenpiteet (ISO 22313, 8.1.1).

Nämä prosessit olisi yhdistettävä organisaation liiketoimintaprosesseihin, jotta voidaan varmistaa, että niitä hallitaan asianmukaisesti ja että niiden vaikuttavuutta ylläpidetään (ISO 22313, 8.1.1).

Organisaation olisi arvioitava liiketoiminnan vaikutusanalyysiään, riskien arviointiaan, strategioitaan ja ratkaisujaan, liiketoiminnan jatkuvuussuunnitelmiaan ja -menettelyitään, jotta se kykenee varmistamaan, että ne ovat edelleen soveltuvia, asianmukaisia ja vaikuttavia.

Arvioinneissa olisi käsiteltävä tarvetta muokata toimintaperiaatteita, tavoitteita ja muita liiketoiminnan jatkuvuuden hallintajärjestelmän osia esim. harjoitusten tulosten, häiriötilanteita koskevien katselmusten ja organisaation muuttuvien olosuhteiden perusteella.

Arvioinnit voidaan suorittaa sisäisinä tai ulkoisina auditointeina tai itsearviointeina. Katselmointien suoritusväli ja ajoitus voi riippua laeista ja viranomaisvaatimuksista sekä organisaation koosta, luonteesta ja oikeudellisesta asemasta. Myös sidosryhmien vaatimukset voivat vaikuttaa niihin

ISO 22301 -standardin vaatimat pakolliset dokumentit:

8.2.1 Prosessi liiketoiminnan vaikutusanalyysille ja riskien arvioinnille. Soveltuu osittain.

8.3.3 Strategiat ja ratkaisut liiketoiminnan jatkuvuudelle. Soveltuu osittain.

8.4 Liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt. Soveltuu osittain.

8.5 Harjoitus- ja testaussuunnitelmat. Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

8.1 Sopimukset ja SLA:t. Soveltuu.

8.2.2 Liiketoiminnan vaikutusanalyysin tulokset. Soveltuu.

8.2.3 Riskinarvioinnin tulokset. Soveltuu.

8.4.3.1 Dokumentoitu tieto viestinnästä sisäisten ja ulkoisten olennaisten sidosryhmien kanssa. Soveltuu.

8.4.3.1 Tallennetaan häiriötä, suoritettuja toimintoja ja tehtyjä päätöksiä koskeva tieto. Soveltuu.

8.5 Insidenttiskenaariot (Harjoitusten tapahtumaskenaariot). Soveltuu.

8.5 Harjoitusraportit ja -tulokset. Soveltuu.

8.6 Liiketoiminnan jatkuvuuden dokumentaatioiden ja kyvykkyyksien arviointi. Soveltuu.

9. Suorituskyvyn arviointi

1. Seuranta, mittaus, analysointi ja arviointi

2. Sisäinen auditointi

3. Johdon katselmus

Liiketoiminnan jatkuvuuden hallintajärjestelmän suorituskyvyn ja vaikuttavuuden seurannan, mittaamisen, analysoinnin ja arvioinnin menettelyjen olisi sisällettävä

a) seuranta-, mittaus-, analysointi- ja arviointimenetelmien määrittäminen, johon kuuluu esimerkiksi

1) sen määrittely, mitä täytyy seurata ja mitata

2) sen tunnistaminen, milloin ja kenen toimesta seuranta ja mittaus olisi toteutettava

3) organisaation tarpeisiin sopivien ja validit tulokset varmistavien suorituskykymittarien asettaminen, mukaan lukien määrälliset ja laadulliset mittarit

4) aineiston ja tulosten tallentaminen korjaavien toimenpiteiden analyysien helpottamiseksi

b) historiallisen tiedon tutkiminen

c) organisaation liiketoiminnan jatkuvuuden toimintaperiaatteiden ja tavoitteiden toteutumislaajuuden seuranta

d) liiketoiminnan jatkuvuuden hallintajärjestelmän vaatimustenmukaisuuden mittaaminen sovellettavien lakien ja viranomaisten vaatimusten suhteen

e) liiketoiminnan jatkuvuuden hallintajärjestelmän suorituskyvyn puutteita koskevien poikkeamien ja muun näytön seuranta.

Arvioitavat toiminnot:

- Liiketoiminnan vaikutusanalyysi
- Riskien arviointi
- Liiketoiminnan jatkuvuusstrategiat ja -ratkaisut
- Liiketoiminnan jatkuvuussuunnitelmat ja -menettelyt
- Toiminto X
- Toiminto Y
- Toiminto Z

Käytettäviä mittareita ovat muun muassa:

- BIA-analyysien kattavuus (montako prosenttia toiminnoista arvioitu)
- Riskien arviointien suorittaminen
- Jatkuvuus- ja toipumissuunnitelmien ajantasaisuus
- Toteutuneet testaukset ja harjoitukset
- Suoritetut kurssit ja koulutukset
- Vakavat poikkeamat

Mittareille on asetettu tavoitearvot, arvioitu mittaustulos -> verrataan tavoitetta ja toteutumaa. Mittareille on määritetty voimassaoloajat ja vastuutahot.

ISO 22301 -standardin vaatimat pakolliset dokumentit:

9.1 Suorituskyvyn arviointi - Seuranta, mittaus, analysointi ja arviointi. Soveltuu.

9.2 Sisäisen auditoinnin menettelytavat. Soveltuu.

9.2 Sisäisen auditoinnin tulokset. Soveltuu.

9.3 Johdon katselmus ja sen tulokset. Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

9.3 Liiketoiminnan jatkuvuuden hallintajärjestelmän katselmointikokousten pöytäkirjat. Soveltuu.

10. Parantaminen

Organisaation on määritettävä parantamismahdollisuudet ja toteutettava tarvittavat toimenpiteet, jotta liiketoiminnan jatkuvuuden hallintajärjestelmän halutut tulokset saavutetaan.

Organisaation on parannettava jatkuvasti liiketoiminnan jatkuvuuden hallintajärjestelmän soveltuvuutta, tarkoituksenmukaisuutta ja vaikuttavuutta laadullisten ja määrällisten mittarien perusteella.

Hallintajärjestelmän vaikuttavuutta parannetaan korjaavilla ja ehkäisevillä toimenpiteillä. Tätä toteutetaan käyttämällä hyväksi:

- auditointien tuloksia
- johdon katselmointeja
- riskiarviointeja
- käyttäjien havaintoja
- keino 5
- keino 6
- keino 7

ISO 22301-standardin vaatimukset poikkeamille ja korjaaville toimenpiteille sekä jatkuvalle parantamiselle ovat samat, kuin ISO 27001-standardissa.

ISO 22301 -standardin vaatimat pakolliset dokumentit:

10.1 Poikkeamat ja tehdyt toimenpiteet. Soveltuu.

10.1 Poikkeamien toimenpiteiden tulokset. Soveltuu.

ISO 22301 -standardin suosittelemat (ei-pakolliset) dokumentit:

10.1 Menettelytavat korjaaville toimenpiteille (poikkeamat). Soveltuu.