DIGI- JA VÄESTÖTIETO-VIRASTO

Kustannus-vaikuttavuus -malli digitaalisen turvallisuuden riskien sekä riskienhallinnan analysointiin

VAHTI-hyvät käytännöt tukimateriaali

30.11.2023

Sisällysluettelo

1 Tiivistelmä ... 2
2 Johdanto ... 3
3 Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallin osat ... 5
3.1 Digiturvallisuus kattavan turvallisuuden ja riskienhallinnan mallina ... 7
4 Digitaalisen turvallisuuden riskien arvon laskeminen ... 8
4.1 Menetykset ennen ja jälkeen riskienhallintatoimenpiteiden ... 8
4.2 Riskienhallintatoimenpiteiden rahallinen vaikutus ... 10
5 Digitaalisen turvallisuuden kustannusten luokittelu ... 13
5.1 Mallit kulujen luokitteluun ... 14
5.1.1 Datalähtöinen tai toimintalähtöinen luokittelumalli ... 14
5.1.2 NIST CSF kustannusluokittelun perustana ... 16
5.1.3 ISO/IEC 27001 ja 27002 kustannusluokittelun perustana ... 17
5.2 NIST CSF- ja ISO- viitekehyksien hyödyntäminen kustannusten seurantaan ... 18
5.3 Kulujen kohdistamisen käytännön toteutuksesta ... 20
6 Digitaalisen turvallisuuden menetysten luokittelu ... 21
7 Digiturvallisuuden arvomalli – riskienhallintatoimenpiteiden vaikutus eri riskeihin ... 22
7.1 Arvomallin riskienhallintatoimenpiteiden käytännön esimerkkejä ... 23
7.2 Organisaation digitaalisen turvallisuuden maturiteetin vaikutus ... 25
7.2.1 Tietoturvainvestointien hyöty ja Gordon-Loeb -malli ... 26
7.2.2 Organisaation digiturvan maturiteetti arvomallissa - esimerkkejä ... 27
8 Kustannus-vaikuttavuus-malli ... 28
8.1 Digitaalinen turvallisuus koordinointitasolta strategiselle tasolle ... 28
8.2 Digitaalinen turvallisuus strategiselta tasolta koordinaatiotasolle ... 30
9 Digiturvallisuuden kustannus-vaikuttavuus-mallin merkitys ... 32
Termistöä
Liitteet

1 Tiivistelmä

Digitaaliseen turvallisuuteen kohdistuvat hallintatoimenpiteet pyrkivät lähtökohtaisesti vähentämään organisaatioon kohdistuvien uhkien vaikutuksia tai niiden todennäköisyyttä, ja täten ehkäistä menetyksiä, joita riskien toteutumisesta saattaisi seurata. Jotta uhkia ja niihin liittyviä riskejä ja menetyksiä voidaan hallita ja vähentää, tulee niiden ympärille luoda järjestelmällinen malli, joka mahdollistaa tämän. Osana tähän soveltuvia hallintamalleja ja johtamisen toimintatapoja kuuluu riskienhallinta, jonka prosesseissa tuotetaan tietoa päätöksenteon tueksi.

Digitaalisen turvallisuuden ylläpito ja parantaminen ei ole ilmaista, vaan vaatii toteutuakseen panostuksia ja kustannuksia, jotka on kohdistettava tehokkaasti ja perustellusti suojattaviin kohteisiin ja muihin arvokkaiksi koettuihin asioihin. Riskien ja niiden käsittelyn vaihtoehtojen analysoinnin ja arvioinnin eri vaiheissa riskejä tulee kyetä arvottamaan ja suhteuttamaan yhdenmukaisesti - niin digitaalisen turvallisuuden sisällä kuin muihin riskeihin nähden osana kokonaisriskienhallintaa. Tässä dokumentissa tähän liittyvän riskien arvottamisen eri vaiheita kolmella eri tasolla kokoavaa konseptirakennetta kutsutaan digitaalisen turvallisuuden kustannus-vaikuttavuus-malliksi.

Toiminnan käytännön tasolla digitaalisen turvallisuuden riskienhallintatoimille voidaan laskea rahallinen arvo tarkastelemalla arvioitua menetystä sekä huomioimalla jäännösriski. Tätä investointien kustannuksiin perustuvaa laskelmaa on kuitenkin rikastettava, mikäli pyritään tunnistamaan laajempia suojattavia arvoja[1] ja eri hallintatoimien merkitystä sekä kohdistamaan toimenpiteitä näihin oikeasuhtaisesti ja tehokkaasti. Tämä rikastaminen tapahtuu tarkasteltaessa organisaation hallinnon tasoa varten muodostettavalla arvomallilla, johon tuodaan toimintaan sekä tavoitteisiin sopivat luokittelutavat, jotka ovat yhteydessä digitaalisen turvallisuuden johtamiseen ja koordinaatioon. Tässä dokumentissa luotu esimerkki kustannusluokittelumallista hyödyntää laajasti käytössä olevia ISO 27000- ja NIST CSF-malleja.

Mallin kolmannella tasolla riskitietoa hyödynnetään vaikuttavuuden esiintuomiseksi, jotta arvotuksen merkityksiä voidaan tarkastella strategisessa kontekstissa tarvitulla tavalla. Digiturvallisuuden arvomallin riskit, menetykset ja kustannukset voidaan täten tuoda osaksi organisaation laajempaa riskienhallinnan kokonaisuutta, toiminnan ohjausta ja strategista johtamista. Ilman tätä vaihetta arvomallin hyödyntäminen toimintojen kehittämisessä ja riskien hallinnassa jää asiantuntijatasolle eikä integroitu organisaation johtamismalliin. Rahallisten kustannusten merkitys voi siis jäädä hämäräksi.

Digitaalisen turvallisuuden arvioinnin kannalta on oleellista, että turvallisuuteen liittyvät kustannukset voidaan tunnistaa ja luokitella oikein. Samalla tiedonkeräyksen toteutuksen pitää olla suhteessa asiantuntijoiden resursseihin, sillä automaatio ei vielä toistaiseksi kykene tuottamaan tarvittua tietoa oikealla tarkkuudella ja kontekstissa.

---

[1] Suojattavalla arvolla tarkoitetaan tässä dokumentissa sekä konkreettisia järjestelmiä, joilla nähdään rahallista arvoa, arvoa, joka sisältyy tietoon ja sen käyttöön, että laajempia yhteiskunnallisia tai perusarvoja. Nykyaikaisessa ja kompleksisessa maailmassa on huomioitava, että riskit voivat kohdistua useille eri tasoille. Tämä laajentaa niin sanotun suojattavan kohteen määritelmää, sillä esimerkiksi yksittäinen tietovarasto voi olla merkityksetön sen rinnalla, miten varmistetaan palvelukokonaisuuden jatkuvuus, tai miten se ja muut digitaalisen toimintaympäristön sosio-teknisen järjestelmän osaset vaikuttavat mm. luottamuksen muodostumiseen. Strategiset tavoitteet voidaan usein muotoilla laajemmiksi suojattaviksi arvoiksi. (kts. termiliite)

2 Johdanto

Digitaalisella turvallisuudella (lyhyemmin digiturvalla) pyritään organisaatioissa varmistamaan, että niiden digitaalinen toimintaympäristö on luotettava ja että toiminta siellä on turvallista ja hallittua normaalissa arjessa kaikille käyttäjille. Jotta tämä olisi toteutettavissa, tulee organisaatioiden pystyä tunnistamaan digitaaliseen toimintaympäristöön kohdistuvia uhkia ja varautumaan näistä muodostuviin riskeihin. Organisaatioiden tulisi myös ymmärtää digitaalisen turvallisuuden uhkiin liittyvät potentiaaliset menetykset ja systemaattisesti pyrkiä minimoimaan niitä.

Digiturvallisuuden arvo muodostuu uhkiin liittyvien menetysten arvon tunnistamisesta sekä riskienhallinnallisista toimenpiteistä, joilla menetyksiin pyritään vaikuttamaan. Yhtenä arvon yhteismitallistavana mittarina sovelletaan usein rahallista arvoa, mikäli sen katsotaan soveltuvan tarkastelun tarkoitukseen.

Keskeinen keino vaikuttaa organisaation digitaaliseen turvallisuuteen on investoida turvallisuuteen liittyviin menetelmiin, palveluihin ja järjestelmiin. Digitaaliseen turvallisuuteen kohdentuvat investoinnit pyrkivät lähtökohtaisesti vähentämään organisaatioihin kohdistuvia digitaalisia uhkia tai niiden todennäköisyyttä. Jotta investointien toimivuutta ja tehokkuutta voidaan seurata ja mitata tulee näihin liittyviä kuluja ja kustannuksia ymmärtää.

Tämän dokumentin tarkoituksena on määritellä kolmetasoinen lähestymistapa digitaalisen turvallisuuden kustannus-vaikuttavuuden tarkasteluun:

1. Ensimmäisellä tasolla määritellään yksittäisten riskien arvo ja miten niitä käsitellään (digiturvallisuuden riskien laskentamalli).
2. Toisella tasolla luokitellaan digitaalisen turvallisuuden kustannuksia sekä uhkakuvien myötä muodostuvia mahdollisia menetyksiä, joiden perusteella tuotetaan malli organisaatiokohtaiseen digitaalisen turvallisuuden riskienhallintaan organisaatiotasolla (digiturvallisuuden arvomalli).
3. Kolmannella tasolla kuvataan, miten malli liittyy osaksi organisaation kokonaisvaltaista riskienhallintaa, strategista johtamista ja hallinnollista vaikuttavuutta (digiturvallisuuden vaikuttavuusmalli).

Näiden kokonaisuutta kutsutaan digiturvallisuuden kustannus-vaikuttavuus-malliksi.

Digiturvallisuuden kustannus-vaikuttavuus-malli on konseptuaalinen malli sille, miten julkisissa organisaatioissa voidaan käsitellä digiturvan kustannuksia. Se on yhteensopiva ISO 31000-standardisarja[2] (ja siten mm. ISO 27000-sarjan) mukaisen riskienhallinnan kanssa analyysityökaluna eli riskien ja laajempien riskikokonaisuuksien (luokkien) tarkastelussa kvantitatiivisesti. Malli ei ota kantaa siihen, miten hallinta toteutetaan käytännön tasolla tai mitä hallintamallia digitaalisessa turvallisuudessa käytetään, vaikka on hyvin suositeltavaa, että käytetty luokittelu vastaa hallintarakennetta.

Mallin käytössä suositellaan vahvasti digitaalisia työkaluja ja automatisoituja järjestelmiä, jotka tukevat mallin mukaista tekemistä, tietojen tehokasta keräystä ja käsittelyä sekä mahdollistavat prosessin automaatioasteen nostamisen. Digiturvallisuuteen

[2] *Riskienhallintajärjestelmä ISO 31000* (https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-31000-riskienhallinta/)

liittyvän tiedonkeruun osalta voi olla tarpeen kehittää tähän liittyviä taloushallinnon järjestelmiä ja käytänteitä. Myös toimittajayhteistyön kautta voidaan sopia toimintamalleista, jotka edesauttavat kustannusluokittelua, erityisesti sen automatisoinnilla. Nämä on syytä huomioida, kun digiturvallisuuden kustannus-vaikuttavuus-mallin hyödyntämistä suunnitellaan. Mallin hyödyntäminen voi toimia osaltaan vahvistuksena perusteluille, miksi riskienhallintaa ja sitä tukevia hallinnon järjestelmiä tulisi kehittää.

Kustannusten ja arvon laskeminen osana riskienhallinnan analysointia ja arviointia edellyttää tiettyä maturiteettia organisaatiolta, sen turvallisuuden hallinnalta sekä riskienhallinnalta. Tämä on tunnistettu haaste useissa julkisen hallinnon organisaatioissa. Valtiontalouden tarkastusviraston vuonna 2017 tekemän selvityksen mukaan, julkisen hallinnon organisaatiot budjetoivat digitaaliseen turvallisuuteen käytettävät varat toimintamenomomentille erittelemättömänä osana organisaation toiminnasta aiheutuvia kustannuksia[3]. Haasteina ovat olleet sekä julkisen hallinnon toimintaan ja riskien logiikkaan liittyvät erityisyydet, että digitaalisen turvallisuuden alueella sovellettavissa olevan yhtenäisen mallin puuttuminen. Muun muassa näihin on pyritty vastaamaan osana Valtiovarainministeriön Haukka-hanketta[4], jota on toteutettu Digi- ja väestötietovirastossa JUDO-hankkeen[5] osana.

Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallin tarkoituksena on tarjota yhtenevästi sovellettava mekanismi, jolla tuotetun analyysin avulla organisaatiot voivat systemaattisesti arvioida riskejä sekä kvantifioida niihin liittyviä hallintatoimenpiteitä, erityisesti investointeja. Mallin tarkoituksena on myös integroida digiturvallisuuden riskienhallinta organisaation strategiseen päätöksentekoon sekä mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi saattaminen ja seuranta läpi koko organisaation. Kustannusten ja arvon kautta digitaalisen turvallisuuden riskit voidaan tuoda osaksi organisaation kokonaisriskienhallintaa.

Tämä asiakirja on tarkoitettu ensisijaisesti julkishallinnon eri organisaatioille, näissä toimiville riskienhallinnan ja digitaalisen turvallisuuden asiantuntijoille sekä näiden tehtävien parissa työskenteleville muille tahoille, kuten johdolle, hallinnon kehittäjille ja sisäiselle tarkastukselle. Malli on sovellettavissa myös esimerkiksi rakenteesta, jota voidaan soveltaa muihinkin riskiaihealueisiin digitaalisen toimintaympäristön lisäksi sekä myös julkishallinnon ulkopuolella keskeisiltä osin (huomioiden erot mm. lainsäädännöstä johtuvista luokitteluihin liittyvistä määräävistä reunaehdoista).

[3] *Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016.* (https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf)
[4] *Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka*) (https://vm.fi/hanke?tunnus=VM174:00/2020)
[5] *Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma* (https://julkaisut.valtioneuvosto.fi/handle/10024/161218)

3 Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallin osat

Digitaalisen turvallisuuden kustannus-vaikuttavuus-malli kokonaisuus pyrkii edesauttamaan ymmärrystä digitaaliseen turvallisuuteen tehtävistä panostuksista ja niiden tuottamista hyödyistä, eli niiden vaikutuksista digitaalisen turvallisuuden uhkien pienemiseen organisaatiossa. Malli kattaa taloudellisten riskien merkitysten analysoinnin ja arvioinnin eri tasoilla. Tähän sisältyy kolme tasoa, jotka ovat digiturvallisuuden riskien laskentamalli, arvomalli (joka sisältä kaksi luokittelua) sekä vaikuttavuusmalli. Kokonaisuuden tavoitteena on mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi tekeminen sekä riittävä yhdenmukaisuus kokonaisriskienarvioon sisällyttämiseksi.

Toiminnallisella tasolla, joka ymmärretään pääosin konkreettisena ja teknisenä, pyritään digitaaliseen turvallisuuteen kohdistuvilla investoinneilla lähtökohtaisesti vähentämään kohdistuvien riskien vaikutuksia tai niiden todennäköisyyttä suorasti tai välillisesti. Jotta riskien herättämien epävarmuuksien suojaksi tehtyjen investointien rahallisia arvoja sekä riskeihin liittyviä mahdollisia rahallisia menetyksiä voidaan kvantifioida ja seurata, tulee niiden ympärille luoda säännönmukainen laskutapa. Tätä mallia kutsutaan tässä dokumentissa **digiturvallisuuden riskien laskentamalliksi**. Siinä analysoidaan yksittäisten riskien osalta hallintakeinojen merkitystä riskien taloudelliseen vaikutukseen.

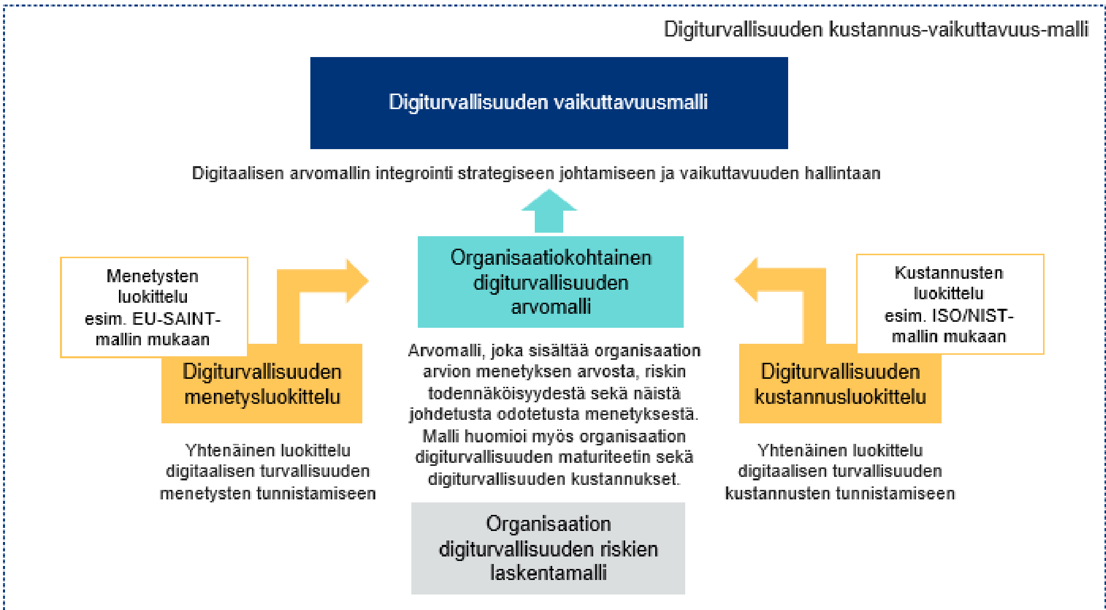
Yksittäisiä riskejä laajemman hallittavuuden ja toiminnan koordinoinnin vuoksi organisaation tulee käyttää yhtenäistä mallia niihin liittyvien investointien kustannusten seuraamiseen, sen osalta, miten riskien käsittelytoimet kohdistuvat eri osa-alueille, kokonaisuuksina. Tätä mallia kutsutaan tässä dokumentissa **digiturvallisuuden kustannusluokitteluksi**. Riskejä käsitellään tiettyjen vakiintuneiden hallintakeinoluokkien ja -kokonaisuuksien kautta, mutta ne eivät välttämättä kata kaikkia riskin osatekijöitä tai kohtaa uhkia symmetrisesti. Tarkastelemalla, minne kustannukset kerääntyvät, voidaan arvioida riskien hallintatoimien kohdentamista.

Laskenta- ja kustannusmallien tarkoituksena on tarjota mallit, joiden avulla organisaatiot voivat systemaattisesti arvioida digiturvaan tehtäviä investointeja. **Digiturvallisuuden menetysluokittelu** tarjoaa mallin tarkastella yksittäisiä riskejä niitä laajempien, organisaatiolle merkittävien, suojattavien arvojen kannalta. Näiden suojaamista voidaan myös pitää tavoitteina, joihin digiturvalla ja sen ohjauksessa käytettävien hallintamallien toimilla pyritään. Potentiaalisten menetysten tarkastelu auttaa priorisoimaan toimenpiteitä sekä suhteuttamaan erilaisia hallintatoimien vaihtoehtoja. Menetysten laskennallinen arviointi on pääosin lähinnä suuntaa antavaa, joidenkin luokkien ollessa abstraktimpia samalla kun toisiin voidaan soveltaa tilastodataa.

Molemmille luokittelumalleille on tässä dokumentissa esimerkinomaiset perustellut luokittelukokonaisuudet, jotka mahdollistavat yhdenmukaisen seurannan ja vertailtavuuden organisaatioiden sisällä sekä poikkihallinnollisesti niiden välillä.

Kun kustannusluokittelu ja menetysluokittelu yhdistetään, organisaatio voi arvioida digitaalisen turvallisuuden kustannuksia ja menetysten arvoja osana riskienhallinnan arviointeja. Tätä kokonaisuutta on avattu tässä dokumentissa organisaatiokohtaisena **digiturvallisuuden arvomallina**. Koska digitaaliseen turvallisuuteen kohdistuvien investointien vaikutus ja hyötysuhde riskeihin on ainakin osin riippuvainen organisaation nykytilasta, voidaan digitaalisen turvallisuuden maturiteetti huomioida osana näitä analyysejä ja arviointeja arvomallin sisällä.

Kun arvomallia tarkastellaan suhteessa organisaation strategisiin tavoitteisiin, voidaan tietoa hyödyntää tavalla, joka luo **digiturvallisuuden vaikuttavuusmallin**. Tällä mallilla organisaation tunteva voi tulkita arvomalliin sisältyvien kustannusten ja luokitteluiden merkitystä organisaation toiminnalle ja strategialle (digitaalisen toimintaympäristön poikkileikatessa nykyisin kaikki toiminnot) sekä digitaalisen turvallisuuden kontekstissa muodostuville strategisille riskeille. Alla olevassa kuvassa 1 on esitetty digiturvallisuuden kustannus-vaikuttavuus-malli kokonaisuudessaan, sisällyttäen sen eri osien muodostamat tarkastelutasot.



Kuva 1: Digiturvallisuuden kustannus-vaikuttavuus-malli ja sen eri osat.

Kuvassa keltaiset laatikot kuvaavat digiturvallisuuden menetysten luokittelumallia (”menetysluokittelu”) ja kustannusten seuranta- ja luokittelumallia (”kustannusmalli”), joissa suositellaan käytettäväksi organisaation omaan hallintajärjestelmään sekä kansainvälisiin standardeihin pohjautuvia rakenteita. Riskeihin liittyviin kustannuksiin ja menetyksiin kohdistettavat arviot ja laskenta ovat sinänsä yksinkertaisia ja esitetyn kokonaismallin keskeinen merkitys on kuvata arvonmuodostumisen ketju läpi eri tarkastelun tasojen. Prosessina malli tukee eri toimijoiden ja toiminnan tasojen välisten merkitysten erojen viestintää. Sen avulla tuotettu data, analyysit ja näiden visualisoinnit tukevat riskitietoista johtamista. Kustannus-vaikuttavuus-malli tulisikin integroida osaksi organisaation johtamisen tukena käytettävää tietoa ja luoda sen avulla mitattavaa tavoitteellista toimintaa. Sitä voidaan hyödyntää alhaalta ylöspäin sekä ylhäältä alaspäin, riippuen mallin käyttötarkoituksesta. Mallia voidaan käyttää esimerkiksi reaalitilanteen kuvaamiseen, suunnitteluun, mutta myös esimerkiksi ennakoivan skenaarion luomiseen tai näiden vertailuun.

3.1 Digiturvallisuus kattavan turvallisuuden ja riskienhallinnan mallina

Digiturvallisuudella pyritään varmistamaan muun muassa, että organisaatioiden digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla oleva. Jotta tämä olisi toteutettavissa organisaatioiden eri toimijoiden tulisi olla riittävän varautuneita digitaaliseen toimintaympäristöön kohdistuviin epävarmuuksiin. Organisaatioiden tulisi pystyä kestämään erilaiset häiriötilanteet sekä palautumaan niistä mahdollisimman tehokkaasti. Digiturvallisuuteen luetaan ainakin viisi toteutusaluetta (kuva 2)

Kuva 2: Digitaalisen turvallisuuden hallintamallin pääluokat.

Digitaalisen turvallisuuden hallintamalli perustuu valtioneuvoston periaatepäätökseen (dnro VN/1465/2020)[6] ja se ilmentää ns. monen turvallisuuden mallia; minimiä kattavalle turvallisuudelle digitaalisessa toimintaympäristössä toimimiseen. Sen täydennykseksi voidaan organisaation toimintaan liittyen huomioida tarve nostaa tarkasteluun myös muita turvallisuuden toteutusalueita. Keskeiset viisi periaatepäätöksessä nimettyä toteutusaluetta kattavan digiturvallisuuden toteuttamiselle[7]:

- Hallinnollisesta näkökulmasta digiturvallisuuden johtaminen ja riskienhallinta tulisi olla luonnollinen osa koko organisaation johtamista, hallintoa ja kokonaisturvallisuutta.
- Jatkuvuudenhallinnalla tarkoitetaan toimenpiteitä, jotka liittyvät erilaisten häiriötilanteiden ennaltaehkäisemiseen. Häiriötilanteisiin tulisi kyetä varautumaan, hallitsemaan niiden aiheuttamia vaikutuksia, oppimaan häiriötilanteista palautua niistä sekä varmistaa organisaation toiminnan jatkuvuus.
- Kyberturvallisuus pyritään varmistamaan sähköisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta. Toiminnon tarkoituksena on pyrkiä turvaamaan yhteiskunnan tai organisaation elintärkeät ja kriittiset toiminnot.
- Tietosuojan tarkoituksena on suojata yksilöiden yksityisyys ja siihen liittyvät tiedot kaikissa tilanteissa.
- Tietoturva takaa organisaatioiden tietojen luottamuksellisuuden, eheyden ja saatavuuden. Tämän avulla pyritään siihen, että vain oikeutetut tahot pääsevän käsiksi tarvittaviin tietoihin.

Digitaalista turvallisuutta ohjaavana mallina tämä luokittelu on tarpeellinen laajassa kuvassa, mutta luokittelujärjestelmänä tai taloudellisena ohjaajana organisaatiotasolla haasteellinen. Mallissa käytetyt luokat eivät määritelmällisesti ole saman tasoisia ja näillä on useita päällekkäisyyksiä. Vaikka juuri päällekkäisyyksiä voidaan pitää riskienhallinnallisena syvyytenä puolustuksessa uhkia vastaan, ne eivät sovellu toisensa poissulkevaan rakenteeseen, jonka tulisi olla käytettävyydeltään kevyt ja helposti ymmärrettävissä. Siksi tätä mallia tulee soveltaa laajemmassa tai strategisessa tarkastelussa soveltaen, vaikuttavuusmallin tasolla.

---

[6] *Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta, VM/2020/47* (https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f806928f5)
[7] *Digi- ja väestötietovirasto: Mitä on digiturva?* (https://dvv.fi/mita-on-digiturva)

4 Digitaalisen turvallisuuden riskien arvon laskeminen

Digitaalisen turvallisuuden tärkeä osa on oikein toteutettu ja toimiva riskien arviointi.[8]

Riskienhallinnan perustoimenpiteitä on tarkastella todennäköisyyden ja vaikutuksen dimensioiden (sekä niiden tulon muodostaman riskin suuruuden, riskiluvun) kautta mahdollisia seurauksia riskien toteutuessa. Näihin dimensioihin voidaan pyrkiä vaikuttamaan eri tavoin. Kuitenkin vain riskien luonteen tarkempi analysointi ja ominaisuuksien tuntemus kertoo, miten riski toimii ja vaikuttaa. Näiden erilaisten analyysien kautta organisaation tietoisuus kasvaa, ja kehittyy luomaan monipuolisesti hallintatoimenpiteitä, joihin sisältyy kustannuksia, merkityksiä ja vaikuttavuutta.

Aidossa riskienhallinnan prosessissa käsittely tulee aloittaa toimintaympäristön kuvauksesta, muutosten ennakoinnista sekä omien suojattavien kohteiden, hyödykkeiden, voimavarojen, tavoitteiden jne. arvojen tunnistamisesta – eli mihin riskeihin sisältyvä epävarmuus kohdistuu.

4.1 Menetykset ennen ja jälkeen riskienhallintatoimenpiteiden

Riskienhallinnan perustyökalu on arvioida riskeille sopiva mittaria käyttäen sitä kuvaava todennäköisyys ja vaikutus. Näiden avulla voidaan arvioida riskin mahdollisesta toteutumisesta aiheutuvan arvonmenetyksen suuruusluokkaa. Niiden kautta hahmotetaan myös hallintatoimien aiheuttamat muutokset riskiin. Käytettäessä rahallisia arvioita riskien arvioinnissa, niiden suuruus on parhaimmillaan käypä arvio mahdollisesta menetyksestä (kyseisen tarkastelujakson aikavälille). Tämänkaltaisella itsearvioinnilla pohjalta jokaisessa organisaatiossa on mahdollista analysoida riskien ja hallintatoimenpiteiden taloudellisia vaikutuksia.

Hallintatoimenpiteet aiheuttavat useimmiten kustannuksia (lähinnä ajan, rahan ja resurssien käyttö). Riskien hallintatoimenpiteitä ovat riskin torjuminen (toiminnasta pidättäytyminen), lähteen poistaminen, todennäköisyyden muuttaminen, seurausten muuttaminen, jakaminen (siirtäminen) sekä riskin pitäminen (ottaminen ja mahdollinen lisääminen, mikäli siinä nähdään riittäviä hyötyjä). Lisäksi riskin toteutumiseen tai sen hallintatoimiin voi sisältyä mahdollisuuksia, jotka vaikuttavat kokonaisarvioon.

Kustannuksilla on parhaassa tapauksessa hyvinkin suora syy-yhteys suojattaviin kohteisiin ja nämä voidaan arvioida jollain karkeustasolla. Syy-seuraus-yhteys kustannusten ja menetysten välillä (siltä osin kuin sitä on) ei välttämättä kuitenkaan ole lineaarinen, joten toimenpiteitä on mietittävä tilanteen mukaan. Syy-seuraus saattaa olla epälineaarinen, painotettu, binäärinen tai jokin muu tuntematon yhteys. Kustannuksia aiheuttavilla investoinneilla saatavat vaikutukset voivat kohdistua eri tavoin useisiin eri riskeihin. Toisaalta saatetaan tarvita investointeja useaan eri toimenpiteeseen, jotta saadaan yksi riski kontrolloitua halutulle tai vaaditulle tasolle (riittävän matala jäännösriski).

Parhaan näkemyksen riskien käyttäytymisestä tuovat arviointiin useimmiten organisaation omat asiantuntijat. Organisaatio itse osaa parhaiten tehdä arvioinnin omasta riskiprofiilistaan ennen ja jälkeen riskienhallinnallisten toimenpiteiden.

[8] *Riskienhallinnan käsikirja valtionhallinnon toimijoille 2023* (http://urn.fi/URN:ISBN:978-952-367-633-6)

Alla olevassa esimerkissä 1 on hahmotettu riskienhallinnan perustyökaluilla riskien arvioiminen ennen ja jälkeen kustannusten käytön. Siinä on käytetty yksinkertaista kokonaislukuarviota, mutta suuruusarvioiden ja euromäärien kohdalla voitaisiin myös soveltaa esimerkiksi vaihteluväliä ja keskihajontaa.

Esimerkki 1: Riskien arviointi ennen ja jälkeen riskienhallinnan toimenpiteiden

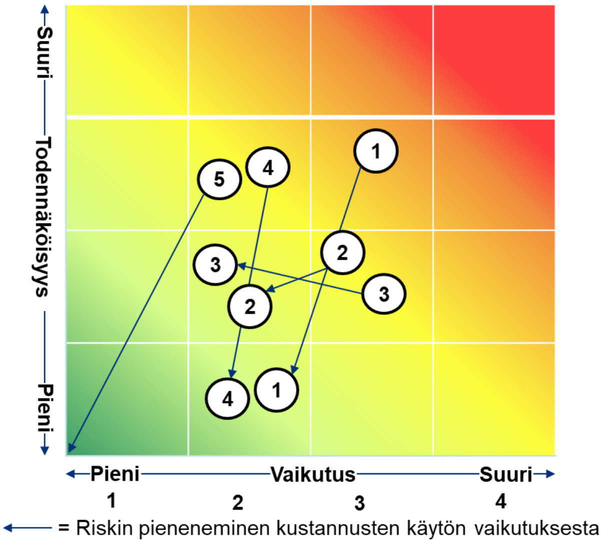
Alla olevassa kuvassa 4 on esimerkki, jossa esimerkkiorganisaatio *Roskienhallintavirasto* on tehnyt riskianalyysin viidestä keskeisimmästä digiturvallisuusriskistään. *Roskienhallintavirasto* on arvioinut riskin toteutumisen todennäköisyyttä asteikolla 1-4 (epätodennäköinen, mahdollinen, todennäköinen, lähes varma). Riskin vaikutus sen toteutuessa on myös arvioitu asteikolla 1-4, johon on sisältynyt euromääräinen kokoluokka osana asteikon kuvausta (1 pienin ja 4 suurin).

Keskeisimmät 10 digiturvallisuusriskiä		Todennäköisyys ennen toimenpiteitä	Vaikutus ennen toimenpiteitä	Todennäköisyys toimenpiteiden jälkeen	Vaikutus toimenpiteiden jälkeen
Riski-nro	**Nimike**				
1	Riski sille, että…	3	3	1	2
2	Riski sille, että…	2	3	2	2
3	Riski sille, että…	2	3	2	2
4	Riski sille, että…	3	2	1	2
5	Riski sille, että…	3	2	Ei ole	Ei ole

Kuva 4: Roskienhallintaviraston riskiarviointi ennen ja jälkeen riskienhallinnallisten toimenpiteiden.

Taulukon kahdessa ensimmäisessä sarakkeessa on riskin numero ja kuvaus. Kahdessa keskimmäisessä sarakkeessa on arvioitu riskin todennäköisyys ja vaikutus ennen riskienhallinnan toimenpiteitä (eli nykytila). Kaksi viimeistä saraketta taulukossa kuvaavat arviota jäännösriskiksi, mikäli tehtäisiin tiettyjä riskienhallinnallisia toimenpiteitä.

Sama asia on kuvattu visuaalisemmin kuvassa 5, jossa pallojen sijainnit kuvaavat riskejä ennen ja jälkeen riskienhallintatoimenpiteiden, ja nuolet kuvaavat kuinka paljon riskienhallinnan toimenpiteillä arvioidaan voitavan pienentää riskiä (joko todennäköisyyden, vaikutusten tai molempien kautta).



Kuva 5: Roskienhallintaviraston graafinen riskikuvaus taulukossa esitetyn arvion pohjalta. Yksinkertaistetussa esimerkkigraafissa jokainen ruutu on kokonaisluku (riskiluku).

4.2 Riskienhallintatoimenpiteiden rahallinen vaikutus

Riskejä tulisi ensisijaisesti arvioida tarvittavien toimenpiteiden toteuttamiseksi, mutta samalla tulisi huomioida ja tuottaa myös rahallinen analyysi ja arviointi. Se voi täydentää riskin merkityksen ymmärtämistä, mutta ennen kaikkea se tukee pidemmän aikavälin ja kokonaisriskienhallinnan arviointitarpeiden kautta talouden suunnittelua. Euromääräisyys riskin merkityksestä on yhteismitallinen esittämistapa, joka edistää riskienhallinnan toimenpiteiden liittyvän vaikuttavuuden todentamista.

Mikäli riskianalyysissä käytetään euromääräisiä arvioita vaikutukselle ja prosentuaalisia arvioita vuosittaiselle todennäköisyydelle, toimija pystyy karkealla tasolla laskemaan euromääräisen odotusarvon riskitoteutumalle vuositasolla kulloisellekin riskille sekä kaikkien digitaalisen turvallisuuden riskien kokonaisvaikutukselle. Tällä tavalla saadaan laskettua odotettu digitaalisen turvallisuuden menetysriski mukaan tietylle ajanjaksolle. Erityisesti julkisessa hallinnossa on tosin huomioitava, että menetyksiä on arvioitava myös rahallisia menetyksiä laajemmin, mitä avataan enemmän sekä arvomallin että vaikuttavuuden osioissa tässä asiakirjassa. Menetysten realistisen arvioinnin tulisi toimia motivaattorina ja perusteluna hallintatoimille organisaatiossa.

Tämän jatkeena toimija voi arvioida riskejä euromääräisesti riskienhallinnan toimenpiteiden jälkeen. Nämä usein vaativat toimenpiteitä, joilla on euromääräisiä kustannuksia ja ne sisältyvät joko aiemmin arvioituun normaalin toiminnan menokehykseen tai niitä varten on tehtävä muita toimia (esimerkiksi erilliset hankkeet ja projektit, mahdollisesti osana jatkuvuudenhallinnan varautumista) ja siten varmistettava erillinen rahoitus. Käyttäen odotusarvoa riskien toteutumisen arvolle ennen ja jälkeen (ns. jäännösriski) hallintatoimien kustannuksia, saadaan näiden erotuksena laskettua hallintatoimien vaikutus. Tämä laskennallinen arvioiden erotus antaa suuntaa antavasti turvallisuuteen vaikuttavien toimien euromääräisen arvon.

Digiturvallisuuden taloudellisen hyödyn laskemiseen voidaan käyttää suoraviivaista laskentakaavaa:

$$T = Z - (I + J)$$

jossa digitaalisen turvallisuuden investointien taloudellinen hyöty (T) saadaan vähentämällä odotetuista menetyksistä (Z), eli riskien euromääräisestä arvosta, digitaalisen turvallisuuden kustannukset (I) sekä jäännösriski (J).

Mikäli tarpeen, kaavassa voidaan huomioida myös esimerkiksi arvon diskonttaus (D), eli nykyarvon laskeminen, jotta rahamäärät ovat vertailukelpoisia keskenään. Diskonttaus tulee toteuttaa vain kerran, valitulle aikavälille. Tällöin kaavasta tulee:

$$T = (Z - (I + J))/D$$

Investoinnin vaikutuksen suuruus suhteessa riskin pienentämiseen ei tule huomioiduksi tässä laskentakaavassa. Asiaa käsitellään laajemmin maturiteetin yhteydessä.

Esimerkki 2: Riskien toteutuman odotusarvon pienentäminen kohdistamalla kustannuksia riskiä pienentäviin toimenpiteisiin

Roskienhallintavirasto arvioi edellisen esimerkin kuvassa 4 digitaalisen turvallisuuden riskinsä ennen ja jälkeen riskienhallintatoimenpiteiden. Virasto on tunnistanut riskienhallintatoimenpiteiden kokonaiskustannukseksi 1,2 MEUR, ja tämä investointi kohdistetaan eri toimenpiteisiin. Kuvassa 6 on eritelty tarkemmin kustannusten kohdistaminen ja miten ne vaikuttavat eri riskeihin.

Roskienhallintavirasto on antanut prosentuaalisia arvoja todennäköisyyden asteikolle 1-4 seuraavasti: 1 = 25%, 2 = 50%, 3 = 75% ja 4 = 100%.

Roskienhallintavirasto on antanut euromääräisiä arvoja vaikutuksen asteikolle 1-4 seuraavasti: 1 = 1 MEUR, 2 = 5 MEUR, 3 = 10 MEUR ja 4 = 15 MEUR.

Yllä olevien asteikkojen avulla virasto pystyy laskemaan riskiarvioihin perustuvan riskien teoreettisen toteutuman odotusarvon kertomalla todennäköisyysluvun vaikutusluvulla (odotettu menetys = todennäköisyys * vaikutus). Nämä laskelmat näkyvät kuvassa 6 odotettuina menetyksinä ennen ja jälkeen riskienhallintatoimenpiteiden.

Keskeisimmät 10 digiturvallisuusriskiä		Todennäköisyys ennen toimenpiteitä	Vaikutus ennen toimenpiteitä	Odotetun menetyksen laskelma	Odotettu menetys ennen	Riskienhallinnan kustannukset	Todennäköisyys kustannusten käytön jälkeen	Vaikutus kustannusten käytön jälkeen	Odotetun menetyksen laskelma	Odotettu menetys jälkeen	Odotettu riskienhallinnan säästö
Riski-nro	**Nimike**										
1	Riski sille, että…	3	3	75%*10 MEUR	7,5 MEUR	0,2 MEUR	1	2	25%*5 MEUR	1,25 MEUR	6,05 MEUR
2	Riski sille, että…	2	3	50%*10 MEUR	5 MEUR	0,4 MEUR	2	2	50%*5 MEUR	2,5 MEUR	2,1 MEUR
3	Riski sille, että…	2	3	50%*10 MEUR	5 MEUR	0,1 MEUR	2	2	50%*5 MEUR	2,5 MEUR	2,4 MEUR
4	Riski sille, että…	3	2	50%*5 MEUR	2,5 MEUR	0,5 MEUR	1	1	25%*1 MEUR	0,25 MEUR	1,75 MEUR
	Odotettu kokonais-menetys				**20 MEUR**					**6,5 MEUR**	
	Kokonais-kustannus					**1,2 MEUR**					

Menetysten laskeminen Mallin B mukaan:
- Odotettu tappio (Expected loss) = todnäk*vaikutus

Kuva 6: Odotetut menetykset ennen ja jälkeen riskienhallintatoimenpiteiden.

Roskienhallintaviraston odotettu kokonaismenetys ja investointien kokonaiskustannus ovat laskettavissa yhteen kaikkien digitaalisen turvallisuuden riskien osalta. Viimeisessä sarakkeessa on laskettu odotettu riskienhallinnan säästö (=odotettu menetys ennen – (riskienhallinnan kustannukset + odotettu menetys jälkeen)).

- *Roskienhallintavirasto* pystyy arvionsa mukaan pienentämään riskin numero 1 odotettua menetystä 7,5 MEUR:sta 1,25 MEUR:iin panostamalla 0,2 MEUR digitaalista turvallisuutta edistäviin toimenpiteisiin. Riskin numero 2 odotettua menetystä pystytään pienentämään 5 MEUR:sta 2,5 MEUR:iin panostamalla 0,4 MEUR:in edestä riskiä pienentäviin toimenpiteisiin jne.
- *Roskienhallintavirasto* arvioi pienentävänsä odotettua menetystä neljästä suurimmasta digiriskistä 20 MEUR:sta 6,5 MEUR:iin panostamalla 1,2 MEUR riskienhallinnan toimenpiteisiin. Kokonaisuutena *Roskienhallintavirasto* arvioi myös, että sijoittamalla tämän 1,2 MEUR vaikutus muihin kuin suurimpaan neljään riskiin on vielä merkittävämpi. Eli sijoitukset näihin riskeihin pienentävät samalla myös monia muita pienempiä riskejä, jolloin hyöty on vielä suurempi kuin taulukossa huomioidut neljän suurimman riskien vaikutus.

Esimerkissä 2 huomioitavia asioita:

- Riskien vaikutuksia voidaan myös havainnollistaa laadullisilla mittareilla kvantitatiivisen mittareiden (euron) sijaan, jolloin kustannusten määrän vertailu saatuun lopputulemaan on kvalitatiivinen. Yllä olevan esimerkin voisi myös tehdä täysin kvalitatiivisilla oletuksilla, mutta tällöin suora vertailtavuus riskien (laadullinen mittaus) ja kustannusten (EUR) välillä hämärtyy. Kvalitatiivisten seurausten ymmärtäminen saattaa kuitenkin olla tärkeämpää kuin kvantitatiivisten seurausten ymmärtäminen. Tätä näkökulmaa ei saa unohtaa menetyksien merkitystä arvioitaessa. Euromääräinen mitattavuus ei siten ole riskien arvioinnin ainoa tavoite, vaan se helpottaa asian seurantaa, arviointia, yhteismitallisuutta ja kommunikointia.

- Jäännösriskejä hallitaan osana organisaation normaalia riskienhallinnan prosessia ja niiden koko ohjaa tyypillisesti sitä, millä organisaation tasolla niistä päätetään ja missä niistä otetaan vastuu. Jäännösriski saattaa olla luonteeltaan erilainen kuin alkuperäinen riski. On mahdollista, että riskin omistajuus saattaa siirtyä organisaatiossa alkuperäiseltä riskin omistajalta toiselle. Sekä omistajuus että jäännösriskien hyväksyminen tulee tehdä dokumentoidusti.
- Kustannuksia aiheuttavat investoinnit saattavat vaikuttaa riskin toteutumisen todennäköisyyteen, vaikutukseen tai molempiin. Yksittäinen toimenpide tai hankinta saattaa vaikuttaa moneen riskiin, ja toisaalta vain useiden eri toimenpiteiden kautta saatetaan saada aikaan riittävä kontrolli tietyn riskin kohdalla. Kattavan ja varmemman hallintatoimien kokonaisuuden tulisi sisältää päällekkäisyyttä, joka voi muodostua myös eri tasoilla (esimerkiksi järjestelmäkohtaisen teknisen toiminnallisen kontrollin lisäksi myös organisaation laajuisesti hallinnollisella tasolla annetaan koulutusta ja johtotasolta viestitään uusista toimintaohjeista – näistä jälkimmäisten kustannuksia ja vaikutuksia voi kuitenkin olla haastavampi osoittaa).

5 Digitaalisen turvallisuuden kustannusten luokittelu

Digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin kannalta on oleellista, että turvallisuuteen liittyvät kustannukset voidaan tunnistaa ja luokitella julkishallinnon organisaatioissa yhteneväisellä tavalla. Valtiontalouden tarkastusviraston vuonna 2017 tekemän selvityksen mukaan, julkisen hallinnon organisaatiot budjetoivat digitaaliseen turvallisuuteen käytettävät varat toimintamenomomentille erittelemättömänä osana organisaation toiminnasta aiheutuvia kustannuksia.[9]

Jotta digiturvallisuuteen liittyviä kustannuksia voidaan seurata, mitata ja hyödyntää osana digitaalisen turvallisuuden kustannus-vaikuttavuusanalyysiä on välttämätöntä pyrkiä erottamaan digitaaliseen turvallisuuteen liittyvät kustannukset muista tietohallinnon, palveluhankintojen sekä organisatorisista kustannuksista. Tämä edellyttää kustannusten tunnistamista ja siitä seuraavaa kustannusten luokittelua.[10]

Yksi tapa luokitella riskejä on jakaa ne neljään perinteisesti käytettyyn pääluokkaan (strategiset riskit, operatiiviset riskit, taloudelliset riskit ja vahinkoriskit), mutta nämä soveltuvat kuitenkin vain lähinnä ylätason kokonaisriskienhallintaan, eivätkä välttämättä kata julkishallinnon organisaation tarpeita merkityksellisten riskikokonaisuuksien ja -luokkien seurannan osalta. Riskien luokitteluun ei ole yhtä kaikille sopivaa mallia tai tapaa, vaan organisaation riskien luokittelu tulee suunnitella ja toteuttaa organisaation toiminnan erityispiirteet huomioon ottaen. Useiden luokittelu- ja analyysitapojen käyttäminen on suositeltavaa kattavan riskiymmärryksen saamiseksi.

Kustannusten tunnistaminen ja luokittelu ovat toisistaan riippuvaisia. Kustannusten tunnistaminen edellyttää, että organisaatioilla on yhtenäinen käsitys siitä, mitä digitaalisen turvallisuuden kustannuksiin sisältyy. Yhtenäinen tapa luokitella kustannuksia edesauttaa kehittämään yhtenäistä ymmärrystä kustannusten sisällöstä ja rakenteesta ja auttaa täten myös kustannusten seurannassa sekä optimoimaan paremmin resurssien käyttöä.

Kustannuksia voidaan luokitella monin eri tavoin. Ohjaavana tekijänä tulee pitää, että kustannukset luokitellaan tavalla, joka on:

- Ymmärrettävä eli merkitykset ja tarkkuudet ovat sopivia
- Toteutettavissa oleva (tehokkaasti) eli hyöty suhteessa vaivaan on sopiva
- Hallintomallia eli toimintaa kuvaava sekä koordinaatiota ja kehittämistä tukeva
- Linkitettävissä (potentiaalisiin) menetyksiin eli riskiperusteista

---

[9] *Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016*. (https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf)

[10] *Digitaalisen turvallisuuden kustannus- vaikuttavuusarviointi julkishallinnossa – selvitystyöraportti 2020, Valtiovarainministeriö*. (https://vm.fi/documents/10623/306832/Digitaalisen+turvallisuuden+kustannus-vaikuttavuusarviointi+julkisessa+hallinnossa+%28selvitysty%C3%B6n+raportti+1.6.2020%29/c79cab0d-ba57-1d20-1e17-772cd24a9d62/Digitaalisen+turvallisuuden+kustannus-vaikuttavuusarviointi+julkisessa+hallinnossa+%28selvitysty%C3%B6n+raportti+1.6.2020%29.pdf)

Ymmärrettävällä luokittelulla tarkoitetaan sitä, että luokkien määrittely on niin selkeää, että kustannuksia käsittelevät henkilöt pystyvät yhtenäisellä tavalla luokittelemaan kulut oikeisiin kustannusluokkiin ja hahmottamaan niiden merkityksen. Toteutettavissa olevalla luokittelulla tarkoitetaan sitä, että luokiteltavassa aineistossa (esimerkiksi laskut) tulee olla (tai siihen voidaan liittää) riittävästi tietoa, jotta kulu osataan ohjata oikeaan luokkaan. Myös tämän tiedon kerääminen tulee tapahtua käytännössä toteutettavissa olevalla tavalla, minkä haasteellisuuteen vaikuttaa kulujen käsittelyprosessi ja järjestelmien integraatio. Asia on merkittävä, sillä hienojakoisemman tiedon tarve, automatisointi sekä reaaliaikaisuus tulevat korostumaan tulevaisuudessa.

Hallintomallia tukevalla luokittelulla tarkoitetaan sitä, että luokittelumalli on julkishallinnon organisaation käyttämään toimintaa ohjaavaan hallintomalliin soveltuvaksi todettu, siten, että luokittelu kuvaa sen osa-alueita riittävän uskottavasti (parhaimmillaan todennettavasti) muodostettaessa tilannekuvia, raportteja ja muuta päätöksenteon tukea.

5.1 Mallit kulujen luokitteluun

Kulujen luokitteluun on kaksi lähtökohtaista mallia: datalähtöinen malli ja toimintalähtöinen malli. Mallit yhdistämällä voidaan pyrkiä hyödyntämään molempien parhaat puolet sekä tuottamaan tehokas toteutus. Molemmat mallit edellyttävät julkishallinnon organisaatioilta käytännön toimenpiteitä kulujen käsittelyssä ja merkitsemissä. Tarkoituksena on erottaa ”IT-kuluista” turvallisuuteen keskeisesti liittyvät menot riittävällä tarkkuudella ja systemaattisuudella, jotta kustannusten kohdistuksen merkitystä voidaan arvioida ja siten ohjata.

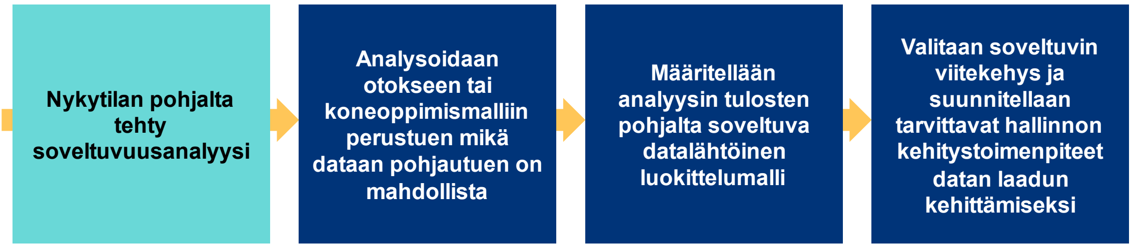
Mallien tukena on syytä käyttää sellaisia rakenteita, jotka mahdollisuuksien mukaan ovat jo organisaatioissa eri tavoin käytössä, todettu käyttöön toimiviksi digitaalisen turvallisuuden hallinnassa sekä ovat sovellettavissa yhteiseen yhdenmukaiseen käyttöön. Näiden viitekehysten rakennetta (niiden osa-alueiden määrittelyä ja niissä käytettyjä otsikointeja, jotka kuvaavat alaosioita eri tarkkuuksilla) voidaan soveltaa käytettäväksi luokitteluina. Näillä ei ole tarkoitus korvata olemassa olevia prosesseja vaan organisaatio voi käyttää niitä myös turvallisuusprosessien lisäksi tai rinnakkaisena prosesseina, vaihtoehtoisena mallina/luokitteluna hallintatoimissa tai näiden analysoinnissa. Erityisesti digitaalisten ja automatisoitujen hallinta-, toiminnanohjaus- ja raportointijärjestelmien (mm. koontinäkymät ja mittaristot) kehittyessä on mahdollista hyödyntää useita tapoja käsitellä ja tarkastella myös digiturvallisuuden ja riskienhallinnan tietoja. Systemaattisen tarkastelun myötä voidaan määritellä mittareita ja raja-arvoja, joilla tuetaan priorisointia, erityiseen tarkasteluun nostamista ja strategisia valintoja, ohjaamista ja päätöksiä.

5.1.1 Datalähtöinen tai toimintalähtöinen luokittelumalli

Datalähtöisellä mallin kehittämisellä tarkoitetaan lähestymistapaa, jossa kustannusluokkien muodostaminen on datalähtöistä, eli luokkien muodostumista ohjaavat esimerkiksi ne tiedot, joita voidaan tunnistaa laskuista ja muista kustannusasiakirjoista. Datalähtöinen luokittelumalli on esitetty kuvassa 7.

Mallin hyviin puoliin kuuluu, että luokittelusta tulee käytännönläheinen. Parhaimmillaan data saadaan jo olemassa olevien prosessien sivutuotteena, mutta tavallista on, että niitä pitää täydentää. Hankintojen kohdalla voidaan jo esimerkiksi tehdä suuntaa antavia päätelmiä siitä, mistä hankinta on tehty, ketkä sitä ovat käsitelleet ja mitä avainsanoja siinä on tunnistettavissa. Mikäli luokittelu halutaan kytkeä johonkin viitekehykseen “data kertoo” mihin se parhaiten sopii.

Mallin heikkoudet liittyvät data-aineiston (esimerkiksi laskujen) laadulliseen selkeyteen. Mikäli laskut eivät ole riittävän selkeitä ja yksilöityjä luokittelusta voi tulla hyvin geneerinen, jolloin esimerkiksi luokittelun kytkentä toimenpiteisiin sekä niiden menetyksiin ja hyötyihin voi vaikeutua. Liian yksinkertainen luokittelu ei palvele kustannusvaikuttavuuden arvioinnin käyttötarkoitusta, eikä siten tuota riittävästi lisäarvoa riskienhallinnan analyysien tueksi suhteessa vaivaan ja kustannuksiin, vaikka joillekin organisaatioille jo turvallisuuteen pääosiltaankin liittyvien kustannusten tunnistaminen on askel eteenpäin.

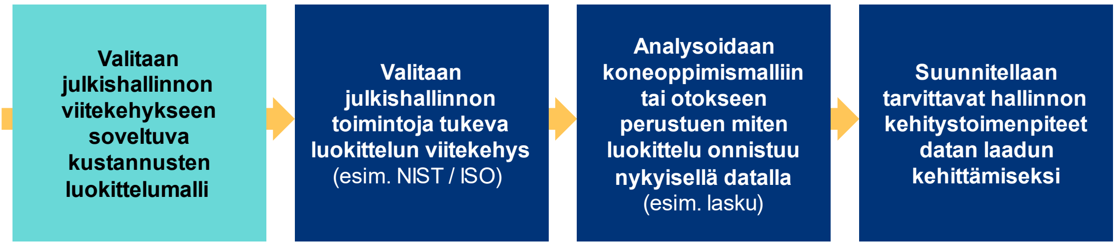


Kuva 7: Datalähtöinen luokittelumalli: Luokittelumallissa huomioidaan mitä “data mahdollistaa” ja kehitystoimenpiteet keskittyvät matalalla roikkuviin hedelmiin.

Toimintalähtöisen luokittelumallin lähtökohtana toimivat valmiit viitekehykset, kuten ISO 27000-sarjan tai NIST Cybersecurity Framework (NIST CSF), joita hyödynnetään organisaatioissa digitaalisen turvallisuuden hallinnan tukena.[11] Toimintalähtöinen luokittelumalli on esitetty kuvassa 8. Valmiin viitekehyksen hyödyntäminen palvelee julkishallinnon hallintoperiaatteita. Ne ovat jatkuvan kehityksen ansiosta pääsääntöisesti selkeitä ja ymmärrettäviä sekä yleisesti tunnettuja ja hyväksyttyjä. On myös oletettavaa, että yleisesti käytössä olevaan rakenteeseen perustuva luokittelumalli on selkeämmin kytkettävissä riskien ja menetysten hallinnassa käytettävään malliin.

Toimintoperusteisen mallin heikkoutena on sen käytännön toteutus, eli esimerkiksi laskuissa tunnistettavan datan käyttö sellaisenaan, ei useinkaan ole suoraviivaista. Laskuissa olevan datan ymmärtämiseen saatetaan esimerkiksi tarvita lisätietoa, jossa voi olla mukanaan aikasidonnaisuutta. Kustannusten luokittelun käytännön haasteet voivat vääristää mallin vertailukelpoisuutta. Esimerkiksi tulkintaerot luokittelussa voivat merkittävästi vinouttaa tuloksia. Lisäksi mallien mahdollistaman yksityiskohtaisuuden tason suhteen on löydettävä tasapaino riittävän tiedon tarkkuuden ja käytännön toteutettavuuden välillä. Tämä ongelma tosi muuttuu merkityksettömäksi, mikäli toiminnanohjaus- tai maksujärjestelmät kykenevät automatisoidusti oikean kontekstin tunnistamiseen.

[11] *Standardit toimivat esimerkkeinä ja suuntaviivoina monille digitaalisen turvallisuuden organisoitumisen ja hallinnan rakenteille, mutta usein kyseessä on niiden soveltava käyttö.*



Kuva 8: Toimintalähtöinen luokittelumalli: Luokittelumallissa huomioidaan julkishallinnon kontekstin hallintomallin tarpeet.

5.1.2 NIST CSF kustannusluokittelun perustana

NIST Cybersecurity Framework -viitekehys[12] (NIST CSF) toimii työkaluna, jolla organisaatiot voivat järjestää sekä parantaa omaa digiturvallisuuden hallintaansa erityisesti käytännön tasolla. Se ohjaa organisaatioita rakentamaan tehokkaampaa ja organisoidumpaa digiturvallisuutta perustuen häiriöiden ilmenemiseen ja tämän ennakointia tukevaan prosessirakenteeseen (ns. alhaalta-ylös tai toimintalähtöinen rakenne). Malli on sovellettavissa myös turvallisuusarkkitehtuuriin[13].

Viitekehys antaa erilaisia suosituksia ja selkeitä ohjeita siitä, kuinka kyberhäiriöitä tulisi ennaltaehkäistä, miten niihin tulisi reagoida häiriön toteutuessa ja kuinka niistä voidaan palautua. Toimintojen avulla suojataan mm. organisaation data, ohjelmat, infrastruktuuri ja työntekijät. Viitekehystä hyödyntämällä kaiken kokoiset organisaatiot pystyvät paremmin ymmärtämään, hallitsemaan ja vähentämään heihin kohdistuvaa kyberturvallisuuden riskiä. Viitekehyksen hyödyntäminen vaatii sen käyttäjiltä osaamista ja kokemusta digitaalisesta turvallisuudesta laajasti, vaikka sen taksonomia erityisesti ohjaa käyttämään riskejä kontrolloivia yleisesti tunnettuja tietoturvallisuuden hallintakeinoja.

NIST CSF 1.1 sisältää 5 avaintoimintoa, joilla on 23 kategoriaa ja 108 alakategoriaa:
- Tunnistaminen
- Suojautuminen
- Havainnointi
- Reagoiminen
- Palautuminen

NIST CSF 2.0 kehitteillä olevassa versiossa on otettu huomioon edellä mainittujen viiden avaintoiminnon lisäksi myös hallinnolliset avaintoiminnot. Hallinnollisten avaintoimintojen tarkoitus on perustaa ja seurata organisaation kyberturvallisuusriskien hallintastrategiaa, odotuksia ja politiikkaa. Tulossa oleva NIST CSF 2.0 versio tulee siten huomioimaan entistä laajemmin hallinnollisten toimintojen näkyvyyden osana viitekehystä. Uusien versioiden omaksuminen ja käyttöönotto on organisaatiokohtaista. [14]

[12] *Tässä viitataan CSF versioon 1.1 (2023):* (https://www.nist.gov/cyberframework)
[13] *DVV:* (https://wiki.dvv.fi/display/DTARK)
[14] NIST CSF 2.0 luonnos: (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf)

5.1.3 ISO/IEC 27001 ja 27002 kustannusluokittelun perustana

ISO/IEC 27000 -sarja on joukko kansainvälinen standardointijärjestön International Standardisation Organisation (ISO) luomia tietoturvastandardeja, jotka liittyvät informaatioteknologiaan. Se tarjoaa parhaat käytännöt tietoturvariskien hallintaan ISMS:n (Information Security Management System) avulla. Näihin liittyvät myös muut hallintajärjestelmät, kuten laadunhallinta ja ympäristönsuojelu. Tietoturvallisuuden hallintajärjestelmä tukee organisaatioita rakentamaan tehokkaampaa ja organisoidumpaa digiturvallisuutta hallinta- ja koordinointitoimenpiteitä järjestelmällisesti ohjaavalla hallintarakenteen kehittyvällä prosessilla (ns. ylhäältä-alas rakenne). ISO 27000-sarjasta voidaan hyödyntää muun muassa ISO 27005 standardia sekä noudattaa ISO 31000-sarjassa kuvattua standardoitua yleistä riskienhallinnan prosessia. ISO 27000 ja ISO 31000-sarjat ovat yhteensopiva erilaisten muiden johtamisen, turvallisuuden, laadun kehittämisen ja hallinnoinnin standardien kanssa. Näitä voidaan käyttää suoraviivaisesti ja todennetusti (erityisesti vaatimuksenmukaisuuden toteuttamiseksi), mutta myös esimerkinomaisina suuntaviivoina.

ISO 27000-sarja kattaa useita kokonaisuuksia. Siinä ISO 27002 standardi on tarkoitettu organisaatioiden käyttöön standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa tai ohjeistukseksi organisaatioille, jotka toteuttavat yleisesti hyväksyttyjä tietoturvallisuuden hallintakeinoja. Standardi ISO 27002 on suunniteltu organisaatioille, jotka aikovat valita hallintakeinoja standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessin puitteissa, huomioiden, että jokaisen organisaation on itse määriteltävä oma toimintaympäristönsä, tarpeensa ja riskinsä.

Laajasti käytössä oleva ISO 27002:2017 sisältää 14 pääkohtaa, joiden alla on 35 pääturvallisuusluokkaa ja 114 hallintakeinoa:

1. Tietoturvapolitiikat
2. Tietoturvallisuuden organisointi
3. Henkilöstöturvallisuus
4. Suojattavan omaisuuden hallinta
5. Pääsynhallinta
6. Salaus
7. Fyysinen turvallisuus ja ympäristön turvallisuus
8. Käyttöturvallisuus
9. Viestintäturvallisuus
10. Järjestelmien hankkiminen, kehittäminen ja ylläpito
11. Suhteet toimittajiin
12. Tietoturvahäiriöiden hallinta
13. Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
14. Vaatimustenmukaisuus

Uudistetun ISO 27002:2022 rakenne sisältää neljä hallintakeinojen pääluokkaa, jotka ovat; organisaatio, henkilöstö, fyysiset ja teknologiset hallintakeinot. ISO 27002:2022 versio on toteutettu erilaiseen rakenteeseen kuin ISO 27002:2017, mutta hallintakeinojen osalta ISO 27002:2022 sisältää näiden vastaavuustaulukon ISO 27002:2017 suhteen. Uutta versiota ei ole vielä omaksuttu laajasti käyttöön. Siirtyminen tapahtuu tarpeen mukaan organisaatiokohtaisesti. [15]

Tämän dokumentin liitetaulukoilla voi tarkastella luokitteluversioiden vastaavuuksia.

[15] *ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.*

1.1 NIST CSF- ja ISO- viitekehyksien hyödyntäminen kustannusten seurantaan

NIST CSF -mallin häiriöprosessin suunnasta rakentuva käsittelytapa, yhdistettynä ISO 27002:n mallin yleisesti käytetystä johtamisrakenteesta, luovat yhdessä kattavan tavan luokitella digitaalisen turvallisuuden ja siihen liittyvien riskien kustannuksia. Tässä esiteltävässä digiturvallisuuden kustannusten luokittelumallissa kustannukset luokitellaan lisäksi organisaatiolliselle tasolle ja toiminnalliselle tasolle. Organisaatiollinen taso koostuu digiturvallisuuden hallinnointiin liittyvistä kuluista kuten palkat, tietoisuuden kasvattaminen, koulutukset ja vastaavat yleisluontoiset menot, jotka rakentavat pohjaa tai mahdollistavat toiminnan, kun taas toiminnalliset kulut liittyvät suorempiin ja digiturvallisuuden kohdistettavampiin kuluihin käytännön tasolla.

Sekä organisaatiollisten että toiminnallisten kustannusten seurantaan ja luokitteluun käytetään NIST CSF:n pääluokkia (5 luokkaa) sekä pääluokkien alle soveltuvia ISO 27002 hallintastandardin pääkohtia (14 kohtaa), jotka on esitetty kuvassa 9. Uudempia versioita ISO 27000 -sarjasta ja NIST CSF:stä käyttävät voivat soveltaa aikaisempia versioita käyttäen versioiden välisiä kääntötaulukoita (liitteet).

Koska osa digiturvallisuuteen liittyvistä yleisemmistä kustannuksista, kuten henkilökulut, on vaikea kohdistaa NIST CSF:n pääluokkien alle, on kustannusten luokittelua jatkettu lisäämällä kaksi kustannusluokkaa: Henkilökulut sekä Muut kulut. Henkilökuluiksi voidaan luokitella sekä organisaation omia henkilökuluja että ulkopuolisia digiturvallisuuteen liittyviä henkilökuluja, mikäli nämä eivät suorasti liity esimerkiksi tiettyyn toimenpiteeseen. Henkilökulujen erittelyä puoltaa myös helposti järjestelmistä saatavilla oleva nimenomainen data. Muihin digiturvallisuuskuluihin voidaan luokitella yleisiä hallinnollisia menoja (koulutus, tiedottaminen, verkostotoiminta, seminaarikulut jne.) jotka eivät ole suoraan osoitettavissa ISO 27002 tai NIST CSF luokkiin.

Kustannusten luokittelumallista tulee näin matriisi, jossa olisi teoreettisesti 98 kustannusluokkaa. Käytännössä kustannusluokkia on kuitenkin vähemmän, sillä ISO 27002 ja NIST CSF luokat ovat osin sisäkkäisiä: esimerkiksi ISO 27002 Jatkuvuuden hallintaan liittyvät kulut ja NIST CSF Palautuminen -pääluokka ovat pääosin yhtenevät.

Luokittelu on myös luonteeltaan suuntaa antava ja kuvastaa enemmän kustannusten seurannan tavoitetilaa. On oletettavaa, että kustannusten seurannan luokittelun käytännön pilotit ja testit vaikuttavat luokittelun käytännön granularisuuteen. Tällä tarkoitetaan, että käytäntö ja tietotarpeet (jotka ovat kehittyneet hienovaraisemman tiedon suuntaan) osoittavat minkälainen tasapaino on löydettävä tiedon tarkkuuden ja toteuttamisen vaivan välillä, huomioiden myös tieto tuottavien järjestelmien kehityksen tätä tukemaan. Luokittelu itsessään siis vain indikoi sen muodostamaa lisätyötä, sillä järjestelmien ja prosessien toiminnan muotoilulla on merkittävä vaikutus lopputulokseen. Keskeinen tekijä luokittelun liittyen on tunnistaa kustannukseen liittyvä konteksti.

Toiminnallinen ja organisaatiollinen taso

DIGITURVALLISUUDEN KUSTANNUKSET

ISO27002 / NIST CSF	Tunnistaminen	Suojautuminen	Havainnointi	Reagointi	Palautuminen	Henkilökulut	Muu
Tietoturvapolitiikat							
Suojattavan omaisuuden hallinta							
Vaatimustenmukaisuus							
Tietoturvallisuuden organisointi							
Henkilöstöturvallisuus							
Pääsynhallinta							
Salaus							
Fyysinen turvallisuus ja ympäristön turvallisuus							
Käyttöturvallisuus							
Viestintäturvallisuus							
Järjestelmien hankkiminen, kehittäminen ja ylläpito							
Suhteet toimittajiin							
Tietoturvahäiriöiden hallinta							
Jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia							

Kuva 9: Digiturvallisuuden kustannusten luokittelu esitettynä matriisina. Sen toteuttaminen käyttöliittymässä edellyttäisi esimerkiksi vain kahta alasvetovalikkoa.

NIST CSF luokat (vaaka-akseli) sekä ISO 27002 (pystyakseli) muodostavat mallin kustannusluokittelumatriisista. Jokaisen kustannuksen osalta määritetään siis kaksi muuttujaa. Koska kaikki NIST CSF / ISO 27002 yhdistelmät eivät ole loogisia, esim. tietoturvapolitiikat liittyvät tyypillisesti tietoturvauhkien tunnistamiseen, suojautumiseen ja havainnointiin, mutta ei reagointiin tai palautumiseen, ei matriisiin kaikkiin soluihin kirjaudu kustannuksia.

Kuva 9 havainnollistaa esimerkkiorganisaation erilaisia kustannusluokkia, jaettuna vaakatasolla NIST CSF luokkiin (sekä henkilö-/hallinnointi ja muihin kuluihin) sekä pystytasolla ISO 27002 mukaiseen 14 pääkohtaan. Koska kaikki ISO luokat eivät kohdistu kaikille NIST CSF toiminnoille on kuvassa esimerkinomaisesti muutettu harmaaksi sellaisia yhdistelmiä, jotka eivät ole todennäköisiä.

Luokittelu on käytettyjen mallien johdosta yleiseen käyttöön soveltuva, mutta sikäli suuntaa antava, että siihen voi kohdistua poikkeuksia. Muiden, esimerkiksi hallinnollisten kustannusten, luokittelun osalta organisaatio voi lisätä tarvittaessa malliin uusia kategorioita, kuten esimerkiksi NIST CSF 2.0 versio huomioi hallinnon osana luokittelua. Lisäksi on mahdollista, että joillain organisaatioilla on poikkeavia järjestelyitä, jolloin jokin yksittäinen ruutu jää merkityksettömäksi.

Mallissa esimerkkiorganisaatio kohdistaa itse digiturvallisuuteen liittyviä kustannuksia ja kuluja valmiiksi määritellyn matriisin mukaisesti sen mukaan mihin luokkaan kulu arvioidaan kuuluvan. Lopputuloksena on kustannusrakenne yrityksen digiturvallisuuteen rahallisista panostuksista. Malli auttaa organisaatioita sekä seuraamaan digitaaliseen turvallisuuteen liittyviä kustannuksia yhdenmukaisesti että yhdistämään ne riskien- ja taloushallinnan prosesseihin, nähden niiden vaikutukset.

1.2 Kulujen kohdistamisen käytännön toteutuksesta

Digitaaliseen turvallisuuteen liittyviä kustannusten luokittelua, eli yksittäisten kuluerien kohdistamista eri kustannusluokkiin, voidaan tehdä eri tavoin. Kulujen luokitteluun voidaan hyödyntää esimerkiksi laskussa tai hankintapäätöksessä olevia tietoja kuten toimittajatietoja, viitetietoja, hyväksyjätietoa ja muuta informaatioita.

Organisaatiossa yksittäisen kulun luokittelua voidaan tehdä:

- Osana laskujen tarkastus ja hyväksyntäprosessia, jolloin laskun tarkastanut / hyväksynyt henkilö subjektiivisen näkemyksen mukaan luokittelee kulun oikeaan luokkaan.
- Kulujen luokitteluun voidaan myös hyödyntää tekoälyyn pohjautuvia oppivia järjestelmiä, jotka mahdollistavat kulujen automaattisen tunnistamiseen ja luokitteluun.

Takautuvasti tehtävä kulujen luokittelu voi olla työläs tehtävä, mikäli kuluja tulee luokitella usean vuoden ajalta. Massaluokittelua voidaan helpottaa joko otokseen perustuvalla luokittelulla tai hyödyntäen oppivia järjestelmiä:

- Massaluokittelua, eli takautuvasti laskettavaa kulujen arviointia voidaan tehdä otokseen perustuvalla selvitystyöllä, jolloin esimerkiksi ICT-kuluista otokseen pohjautuvasti arvioidaan kulujen jakautuminen eri luokkiin. Otokseen perustuvassa luokittelussa on omat ongelmansa. Jos otos tehdään organisaatiokohtaisesti mutta rajataan ajallisesti (esimerkiksi tutkitaan 6kk:n kulut) on mahdollista, että harvemmin toteutuvat kuluerät vääristyvät. Jos taas otos rajataan organisaatio näkökulmasta (tarkastellaan muutamaa organisaatioita ja oletetaan että näiden kulujakauma on samanlainen, kun muilla) voivat organisaatiokohtaiset erovaisuudet jäädä piiloon.
- Vaihtoehtoisesti myös takautuvasti tapahtuvaan kulujen luokitteluun voidaan hyödyntää tekoälyä ja oppivia järjestelmiä, jolloin voidaan tarkastella ja luokitella isompia tapahtumamääriä. Vaikka tämänkaltainen lähestymistapa mahdollista kaikkien kulujen tarkastelun isona massana voi lähestymistapa kuitenkin edellyttää mittavaa järjestelmän opettamistyötä.

Luokiteltuja kuluja voidaan kirjata seurannan alkuvaiheessa esimerkiksi taulukkolaskennalla, mutta pidemmällä aikavälillä voi seuranta vaatia tilikarttamuutoksen, jonka avulla digiturvallisuuden kustannukset voidaan luokitella suoraan organisaatioiden talousjärjestelmiin. Molemmissa tapauksissa hyvä tietorakenne ja laadukas data ovat ehtoina tarkoituksenmukaisen analyysin tuottamiselle.

6 Digitaalisen turvallisuuden menetysten luokittelu

On tärkeää, että digitaalisen turvallisuuden mahdolliset menetykset arvioidaan jollain tavalla organisaatioissa, jotta uhkien toteutumisesta aiheutuvia seurauksia osattaisiin ennakoida paremmin. Menetykset voivat olla esimerkiksi kustannuksia, jotka muodostuvat aiempaan tilanteeseen palautumisesta, menetyksiä tulevaisuuden ennakoiduista tuloista, maksettavista ulkoisista korvauksista tai kadotetusta varallisuudesta. Menetykset voivat olla tilapäisiä tai pidempiaikaisia. Menetykset riippuvat paljolti tapahtumatyypistä, kontekstista sekä organisaation tilanteesta.

Koska mahdolliset toteutuvat menetykset voivat olla hyvinkin erilaisia sisällöltään, niitä on luontevaa luokitella tarkemmalle tasolle. Tällaiseen luokitteluun voidaan käyttää esimerkiksi EU:n SAINT-hankkeessa käytettyä luokittelua (kuva 3)[16]. SAINT (Systemic Analyzer In Network Threats) oli EU:n rahoittama hanke, jossa tarkasteltiin tietoturvallisuuden kustannuksia. Erilaisia variaatioita mitata menetyksiä löytyy paljon, mutta tärkeintä organisaatiolle on valita sellainen malli, joka parhaiten sopii juuri sille (ja tarvittaessa muokattuna). SAINT-hankkeessa käytetty luokittelu on tähän tarkoitukseen hyvä lähtökohta, sillä siinä huomioidaan erityyppisiä menetyksiä laajalti digiturvan kontekstiin kohdistetusti, vaikkei sitä ole erityisesti sovitettu suomalaiseen julkishallintoon.

Menetykset yhteensä									
Strategisen tason menetykset									
Organisatorisen tason menetykset									
Toiminnallisen tason menetykset									
Immateriaali-oikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristys-tapauksista ja petoksista aiheutuneet menetykset	Luottamuk-sellisen tiedon vuotamisesta aiheutuvat seuraukset	Korvaus-velvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset

Kuva 3: Menetyksiä, joita digiturvalla pyritään ehkäisemään voidaan tarkastella eri tasojen osalta.

Tämän esimerkkimallin kustannuksia kokoavat menetysten luokat ovat:
- Immateriaalioikeudelliset menetykset
- Toiminnan keskeytykset
- Datan ja ohjelmistojen menetykset
- Kiristystapauksista ja petoksista aiheutuneet menetykset
- Luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset
- Korvausvelvollisuudet kolmansille osapuolille
- Vaikutukset maineeseen
- Fyysiseen omaisuuteen kohdistuvat menetykset
- Henkeen ja terveyteen kohdistuvat menetykset
- Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset

Luokkia voidaan tarkastella organisaation hallinnan eri tasoilla, kuten kuvassa on esitetty. Suojattavia asioita (arvoja, kohteita ja muita menetysluokkien kokonaisuuksia) kuvaavan mallin kautta voidaan pohtia menetysten laadullista ulottuvuutta strategisella, organisatorisella ja toiminnallisella tasolla. Alimmalla tasolla menetykset konkretisoituvat helpommin mitattaviin kokonaisuuksiin, jotka saattavat toteutua yksin tai yhdessä muiden menetysten kanssa. Esimerkiksi korvauksia voidaan laskea oikeuden päätösten tilastoja hyödyntämällä, mitä tulee muun muassa tietosuojarikkeisiin.

[16] *EU SAINT: D4.4 Report on Cost-Benefit Analysis of Cyber-security Solutions, Products and Models, sivu 48* (https://project-saint.eu/sites/default/files/d4.4.pdf), perustuen Marsh, 2014.

7 Digiturvallisuuden arvomalli – riskienhallintatoimenpiteiden vaikutus eri riskeihin

Digitaalisen turvallisuuden kustannusmallissa on useita erilaisia luokitteluista syntyviä kustannuseriä, jotka vaikuttavat eri tavalla digitaalisen turvallisuuden menetyksiin ja riskeihin. Näiden yhteys on tärkeä hahmottaa, jotta kustannukset saadaan kohdistettua optimaalisesti. Kustannusten käyttö vaikuttaa usein useampaan riskiin. Mallia, joka sisältää organisaation arvion menetyksen arvosta, riskin todennäköisyydestä sekä näistä johdetusta odotetusta menetyksestä nimitetään digiturvallisuuden arvomalliksi.

Mikäli kustannukset kohdistuvat esimerkiksi tietoturvahenkilöstön palkkaukseen, se useimmiten vaikuttaa useisiin riskeihin. Toisaalta tietyt kustannuserät vaikuttavat selkeästi enemmän tiettyihin menetyksiin, esimerkiksi salaukseen investoiminen vaikuttaa mm. luottamuksellisen tiedon vuotamisesta aiheutuviin seurauksiin, mutta ei välttämättä ollenkaan esimerkiksi ihmisten henkeen ja terveyteen kohdistuviin menetyksiin. Oheiseen kuvaan 10 on hahmoteltu tätä syy-yhteyttä. Kustannukset on digitaalisen turvallisuuden kustannusmallin mukaisesti hahmoteltu pystysuoraan sarakkeeseen, kun taas menetykset digitaalisen turvallisuuden arvomallin mukaisesti on hahmotettu vaakasuoralle riville.

On hyvä huomioida, että mallin on tarkoitus toimia taustalla automaattisesti (tietojärjestelmä, taulukkolaskenta tai muu työkalu) - **tarkoitus ei siis ole, että taulukkoa ja sen sarakkeisiin liittyviä laskutehtäviä työstettäisiin manuaalisesti**, ellei kyse ole kertaluonteisesta rajatusta tarkastelusta. Tällöinkin se tulisi olla vähintäänkin avusteista. Luokittelut sekä kulujen ja kustannusten tunnistaminen tulisi olla mahdollista riittävällä tarkkuudella perustuen luokittelumalliin sekä esimerkiksi hyväksyjän tai laskuntarkastajan tietoon ja mahdolliseen toimittajalta vaadittuun viitetietoon. Viitetietojen yhdenmukaisuus voidaan varmistaa esimerkiksi tarkentamalla tässä esitettyjä luokitteluita toteutuksessa tai kokeilussa saatavan kokemuksen kautta.

Menetykset / Toimenpiteet	Immateriaali-oikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristys-tapauksista ja petoksista aiheutuneet menetykset	Luottamuk-sellisen tiedon vuotamisesta aiheutuvat seuraukset	Korvaus-velvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset
Tietoturvapolitiikat	●	●	●	●	●	●	●	●	●
Suojattavan omaisuuden hallinta	●	●	●	●	●	●	●	●	●
Vaatimustenmukaisuus	●	●	●	●	●	●	●	●	●
Tietoturvallisuuden organisointi	●	●	●	●	●	●	●	●	●
Henkilöstöturvallisuus	●	●	●	●	●	●	●	●	●
Pääsynhallinta	●	●	●	●	●	●	●	●	●
Salaus	●	●	●	●	●	●	●	●	●
Fyysinen turvallisuus ja ympäristön turvallisuus	●	●	●	●	●	●	●	●	●
Käyttöturvallisuus	●	●	●	●	●	●	●	●	●
Jne…									

Kustannuserän vaikutus mahdolliseen menetykseen käyttäen 5-tason luokitusta — Suuri ● ◕ ◑ ◔ ○ Ei vaikuta

Kuva 10: Toimenpiteiden ja niihin liittyvien kustannusten taulukointi riskeihin ja niihin liittyviin menetyksiin nähden, kuvaten tyhjän esimerkkitaulukon muodostamaa rakennetta. Kukin taulukon solu vastaa kustannuserää (yhteenlaskettuja kustannuksia), jotka kohdistuvat siihen. Kussakin solussa voidaan esittää lukuarvoja, niitä voidaan nyt visualisoida halutulla tavalla (7.1) tai toteuttaa niihin muita analyysejä.

Ensimmäinen sarake ”Toimenpiteet” kuvaa organisaation investointeja erilaisiin mahdollisiin toimenpiteiseen, jotka on kuvattu digitaalisen turvallisuuden kustannusmallin luokitteluiden mukaisesti. Ne koostuvat erilaisia kustannuseristä, joihin organisaatiot voivat investoida saavuttaakseen mahdollisia menetyksien vähennyksiä, joita kuvataan ensimmäisellä ”Menetykset” rivillä. Nämä koostuvat mahdollisista menetyksistä, joita organisaatio voi kokea. Kuvassa siis esitetään palloilla investointien vaikutuksia mahdollisiin menetyksiin kategorioittain.

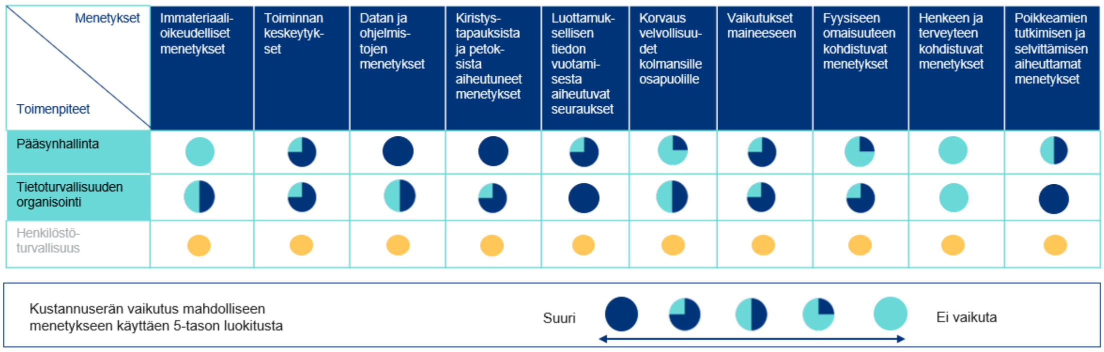
Mallissa olevat toimenpiteet ja menetykset eivät osu symmetrisesti yhteen ja organisaatioiden tilanteet vaikuttavat toimintakykyyn ja sen hetkisiin arvotuksiin. Tulosten todenmukaisuutta on kuitenkin mahdollista tarkentaa mallissa käytetyillä suhdeluvuilla. Arvomallin taulukolla voidaan hahmottaa miten erilaiset toimenpiteet vaikuttavat organisaatioon kohdistuviin mahdollisiin menetyksiin, esimerkiksi kuvan alalaidassa kuvatuilla piirakkakaavioiden palloilla. Siinä pallot on jaettu esimerkin omaisesti karkeasti (25% välein) viiteen suuruusluokkaan pienimmästä (”ei vaikuta”) suurimpaan (”suuri”), ja ne määrittelevät millainen vaikutus toimenpiteellä on kuhunkin menetysluokkaan. Jo tämä tarkkuus antaa suuntaa antavaa tietoa. On huomioitavaa, että vaikutukset vaihtelevat organisaation mukaan monista eri muuttujista johtuen. Kuvassa 10 asiaa on havainnollistettu yleisellä tasolla, mutta jokaisen organisaation on itse pohdittava miten kustannukset vaikuttavat mihinkin riskiin ja kuinka paljon sekä vietävä tämä osaksi taulukon tuloksia (esimerkiksi kuten kuvassa 11).

7.1 Arvomallin riskienhallintatoimenpiteiden käytännön esimerkkejä

Alla on kuvattu joitakin esimerkkejä siitä, miten digitaalisen turvallisuuden arvomallia voi hyödyntää käytännössä.

Esimerkki 3 investointien kohdistuminen eri osa-alueille:

Roskienhallintavirasto on todennut tarpeen investoida kyberturvallisuuteen liittyviin toimenpiteisiin, jotta se pystyy pienentämään mahdollisia menetyksiä mahdollisen riskin toteutuessa. Tässä esimerkissä (kuva 11) virasto investoi pääsynhallintaan sekä tietoturvallisuuden organisointiin, jotta se saisi riittäviä vaikutuksia mahdollisiin menetyksiin kustannus-vaikuttavuus-mallin mukaisesti. Esimerkissä kuvattu voisi olla etukäteisesti tehty vaikuttavuusanalyysi hankintaesityksen tueksi tai jälkikäteinen toteutuksen arviointi tehtyjen toimien osalta (jotka voidaan laskea yhteen jo olemassa olevien turvallisuustoimien, -järjestelmien ja -järjestelyiden kanssa.



Kuva 11: Roskienhallintaviraston arvio toimenpiteiden ja investointien vaikutuksista menetyksiin.

Kuvan 11 mukaisesti, *Roskienhallintaviraston* investoiminen toimenpiteisiin *”Pääsynhallinta*” -osa-alueella nähdään vaikuttavan eniten datan ja ohjelmistojen menetyksiin sekä kiristystapauksista ja petoksista aiheutuneet menetyksiin. Vaikutukset ovat kohtuullisen suuret myös toiminnan keskeytyksestä aiheutuviin menetyksiin, luottamuksellisen tiedon vuotamisesta aiheutuviin menetyksiin, vaikutukseen organisaation maineeseen sekä poikkeamien tutkimisesta ja selvittämisestä aiheutuviin menetyksiin. Esimerkissä investoinneilla nähdään olevan pienempi vaikutus fyysiseen omaisuuteen kohdistuviin menetyksiin sekä mahdollisiin korvausvelvollisuuksiin kolmansille osapuolille. Investoinnilla ei nähdä olevan vaikutusta lainkaan immateriaalioikeudelliset menetyksiin eikä henkeen ja terveyteen kohdistuvissa menetyksissä.

Investointi toimenpiteeseen *”Tietoturvallisuuden organisointi”* vaikuttaa eniten luottamuksellisen tiedon vuotamisesta aiheutuviin menetyksiin sekä poikkeamien tutkimisesta ja selvittämisestä aiheutuviin menetyksiin. Vaikutusten nähdään olevan kohtuullisen suuret myös toiminnan keskeytyksestä aiheutuviin menetyksiin, fyysiseen omaisuuteen kohdistuviin menetyksiin, organisaation maineeseen sekä kiristyksistä ja petoksista aiheutuviin menetyksiin. Investoinnilla nähdään olevan keskinkertainen vaikutus datan ja ohjelmiston menetyksistä kohdistuviin menetyksiin sekä mahdollisiin korvausvelvollisuuksiin kolmansille osapuolille ja immateriaalioikeudellisiin menetyksiin. Investoinnilla ei nähdä olevan vaikutusta lainkaan henkeen ja terveyteen kohdistuviin menetyksiin.

Investoinnit eri toimenpiteisiin voidaan tehdä riskiperusteisesti kohdentaen, eli digitaalisen turvallisuuden suurimpia riskejä tulisi jollain tavalla vähentää. Samalla on kuitenkin hyvä pohtia mihin kaikkiin riskeihin yksi investointi itse asiassa vaikuttaa, sillä usein investointi yhteen alueeseen vaikuttaa moneen eri riskiin, myös vähemmän tärkeisiin. Tällä tasolla voidaankin siis tarkan priorisoinnin sijaan puhua painotuksista, joiden ohessa toteutetaan riskienhallintaa myös muilta osin.

Esimerkki 4: Investointi ja sen vaikutus useampaan riskiin

Edellisen esimerkin 3 mukaisesti pääsynhallintaan tehty investointi vaikuttaa *Roskienhallintavirastossa* eniten Datan ja ohjelmistojen menetyksiin, Kiristystapauksista aiheutuneisiin menetyksiin, mutta myös moniin muihin riskeihin.

Roskienhallintavirasto on päättänyt riskiperusteisesti investoida niihin digiturvallisuuden asioihin, joissa riskit ovat olennaisimmat. Riski datan ja ohjelmistojen menetyksiin heikon pääsynhallinnan takia on koettu isona riskinä, joten virasto on päättänyt investoida pääsynhallinnan kehittämiseen 0,5 MEUR (kuva 12). Tällä investoinnilla virasto uskoo pystyvänsä pienentämään teoreettista odotettua toteuman arvoa Datan ja ohjelmistojen menetysten osalta 2,5 MEUR:sta 0,5 MEUR:iin.

Menetykset / Toimenpiteet	Immateriaali-oikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristys-tapauksista ja petoksista aiheutuneet menetykset	Luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset	Korvaus velvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Ei tehdä mitään			2,5 MEUR							
Versus			Riskin toteutuman odotusarvon pienennys							
Pääsynhallinta-investointi 0,5 MEUR			0,5 MEUR							

Kuva 12: Datan ja ohjelmistojen menetysten riski ennen ja jälkeen pääsynhallintaan tehdyn investoinnin.

Samalla *Roskienhallintavirasto* laskee, että tällä yhdellä investoinnilla pystytään pienentämään odotettua riskitoteutumaa muidenkin riskien osalta. Virasto arvioi, että muut riskit pienenevät kuvan 13 mukaisesti pääsynhallintainvestoinnin kautta.

Menetykset / Toimenpiteet	Immateriaalioikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristystapauksista ja petoksista aiheutuneet menetykset	Luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset	Korvausvelvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Ei tehdä mitään		0,5 MEUR	2,5 MEUR	0,5 MEUR	1,0 MEUR		1,0 MEUR			
Versus		↓	↓	↓	↓		↓			
Pääsynhallinta-investointi 0,5 MEUR		0,3 MEUR	0,5 MEUR	0,2 MEUR	0,2 MEUR		0,3 MEUR			

Kuva 13: Kaikki merkittävimmät digiriskiluokat ennen ja jälkeen pääsynhallintaan tehdyn investoinnin.

Investoinnin pääsynhallintaan (0,5 MEUR) uskotaan kokonaisuutena pienentävän useiden riskien jäännösarvoa. Osoittautuu, että 0,5 MEUR investointi pääsynhallintaan pienentää esimerkissä useiden riskien kokonaisodotusarvon summaa arvioidusta 5,5 MEUR tasosta (kuvan 13 ylemmän rivin summa) arvioidulle 1,5 MEUR (tasolle kuvan 13 alemman rivin summa). Tätä yksinkertaista esimerkkiä monipuolisemmin tarkasteltuna, investoinnista syntynee myös jatkuvia käyttö- ja ylläpitomenoja tuleville vuosille, joiden kulut olisi eri vaihtoehtojen vertailuja varten ositettava kertaluontoisuuden sijaan pidemmälle aikavälille, jotta vältetään ”piilokustannuksia”.

Esimerkin mukaisesti tehtävissä euromääräisissä arvioinneissa voidaan käyttää sopivaksi katsottua (mutta läpinäkyvää ja selitettävää) tarkkuutta ja ne voidaan tuottaa myös hyödyntäen esimerkiksi todennäköisyysjakaumia laskennassa tai perustaen olemassa olevaan tietoon. On suotavaa sisällyttää tietoa arvioiden varmuudesta, rajoista sekä rahallisen arvion ulkopuolelle jäävistä arvoista.

7.2 Organisaation digitaalisen turvallisuuden maturiteetin vaikutus

Digitaalisen turvallisuuden riskienhallinnan arvomalli on rakenteeltaan lähtökohtaisesti samankaltainen eri organisaatioille. Organisaation maturiteetti voi kuitenkin vaihdella ja se olisi hyvä tiedostaa investointeja tehtäessä.

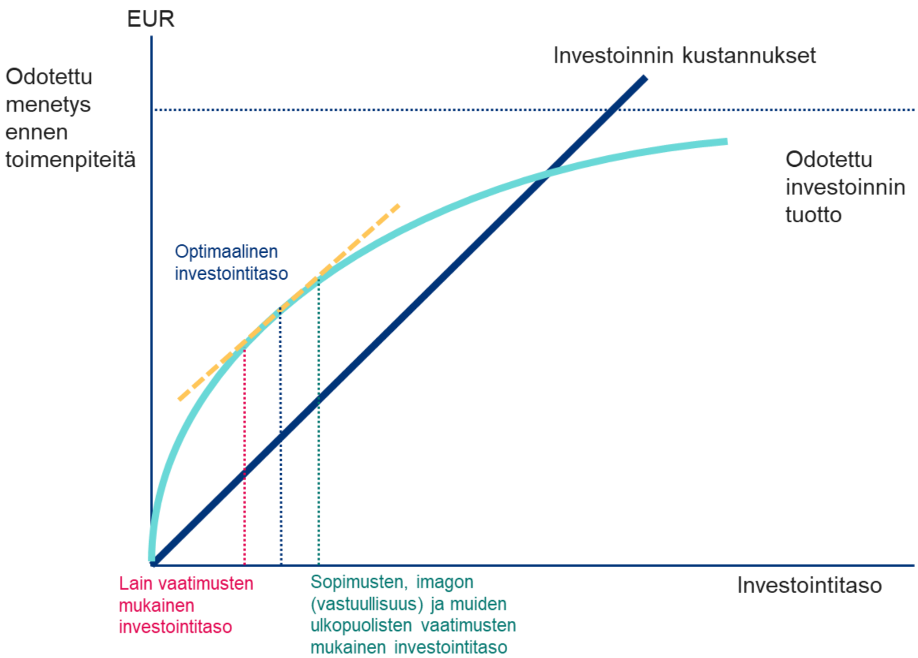
Organisaatio, joka on hyvin kypsällä maturiteettitasolla digitaalisessa turvallisuudessa, ei luultavasti saa suhteellisesti yhtä paljon hyötyä lisäinvestoinneista kuin organisaatio, joka on alkeellisemmalla tasolla, mikäli aiempaa kehitystä ei voida hyödyntää. Esimerkiksi organisaatiossa, jonka pääsyn hallinnan ratkaisut ovat selvästi vanhentuneet, saa uuteen kokonaisratkaisuun vaihtamisen investoinneilla merkittäviä hyötyjä. Verrokki organisaatiossa, jossa jo aiemmin investoitu pääsynhallintaan, ei samalle uudelle tasolle pääsemiseen vaaditusta uudesta investoinnista saada yhtä suurta suhteellista hyötyä. Silti, molempien organisaatioiden voi olla tarpeen saavuttaa tämä uusi taso ja jo pelkkä paikallaan pysyminen voi vaatia panostuksia.

Hyödyn (investointi suhteessa turvallisuuden paranemiseen) on myös tunnistettu vähenevän lisäpanostuksilla, kun pyritään täydelliseen vaikutukseen. Lisäksi suhteellisen hyödyn tarkastelu voi olla tarpeen organisaation riskienhallintatoimien priorisoinnissa – halutaanko tukea heikoimman maturiteetin osa-aluetta tasaisemman kokonaisuuden saamiseksi vai panostetaanko jollekin osa-alueelle huipputason saavuttamiseksi.

7.2.1 Tietoturvainvestointien hyöty ja Gordon-Loeb -malli

Kuten edellä todettiin, organisaation maturiteetti kokonaisuudessaan riskienhallinnassa sekä digiturvan eri osa-alueilla vaikuttaa siihen, mitä toimia kyetään tekemään ja kuinka paljon hyötyä eri investoinneilla saadaan aikaiseksi. Optimaalisten panostusten ongelmaa digitaalisessa turvallisuudessa on tutkittu rajallisesti. Tunnetuin on pari vuosikymmentä vanha malli, joka lisäksi perustuu hieman toisenlaiseen kontekstiin ja ympäristöön, mutta joka tarjoaa edelleen ajatusmallin.

Gordon-Loeb -mallissa[17] investoinnin tuotto, vaikutus, on kuvattu epälineaarisena funktiona, jossa marginaalinen lisähyöty investoinneista jossain vaiheessa rupeaa pienenemään. Kun optimaalinen kohta investoinneille löytyy (kuva 14: keltaisen katkoviivan risteämä, tangentti), lisäinvestoinnit tuovat vähemmän ja vähemmän marginaalihyötyä organisaatiolle. Täydellisen turvallisuuden saavuttaminen on pääsääntöisesti sekä taloudellinen että teknologinen mahdottomuus – etenkin teknologian kehittyessä jatkuvasti – ja siksi myös digitaalinen turvallisuus tulee rakentaa siten, että eri osa-alueet täydentävät toisiaan.



Kuva 14: Gordon-Loeb -malli: Digitaalisen turvallisuuden investoinnin hyötyfunktio. Muiden vaatimusten ohjaamat optimaaliset investointitasot voivat olla myös toisessa järjestyksessä, kuin tässä on esitetty.

Kuten kuvassa 14 on esitetty, investointien kasvaessa niistä saatava rajahyöty pienenee, jolloin voidaan tunnistaa laskennallisesti optimaalisin investointitaso. Investointien kohdistamiseen kohdistuu usein muita vaatimuksia, esimerkiksi lainsäädännöstä tai sopimuksista johtuen, jotka ohjaavat poikkeamaan laskennallisesta euromääräisestä optimista. Alkuperäisen mallin mukaan tietoturvaan ei kannattaisi investoida enempää kuin karkeasti 1/3 odotetun tappion arvosta. Tämä rahallinen arvio ei

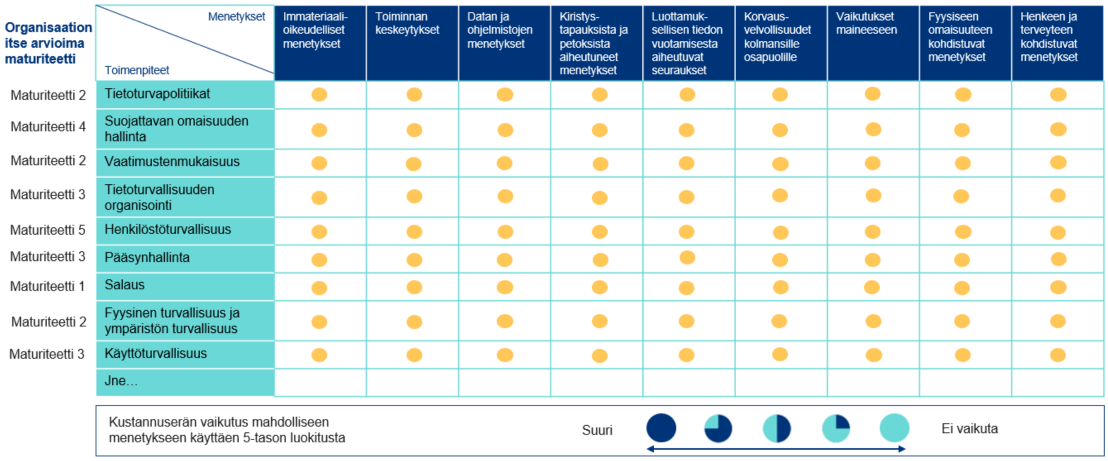
[17] *The economics of information security investment* (https://doi.org/10.1145/581271.581274) ja *Investing in Cybersecurity: Insights from the Gordon-Loeb Model* (https://www.scirp.org/journal/paperinformation.aspx?paperid=64892)

kuitenkaan välttämättä ole optimaalinen muiden arvojen ja vaatimusten suhteen tai mitä edellytetään julkishallinnolta tiettyjen arvojen suojaamiseksi.

7.2.2 Organisaation digiturvan maturiteetti arvomallissa - esimerkkejä

Digitaaliseen turvallisuuteen voi panostaa useilla eri tavoilla. Riskienhallinnan toteutuksessa kannattaa pohtia oman organisaation maturiteettia ja maturiteettiin sopivia hallintakeinoja, joiden kautta saadaan eniten hyötyjä. Seuraavassa esimerkissä 5 on kuvattu kahden eri organisaation investointeja ja niiden riskiä pienentäviä vaikutuksia.

Organisaatio voisi itsearvioinnilla luokitella kustannusmallin mukaisesti digiturvan osa-alueensa eri maturiteettitasoille (kuvassa 15 esimerkkinä vasemmalla oleva numerointi asteikolla 0-5, jossa 1=alkutaso ja 5=optimoitu) [18,19]. Mitä kehittyneempi organisaatio jo on jollakin osa-alueella, sen vähemmän rajahyötyä lisäinvestointi tuo riskin määrässä (todennäköisyyden ja/tai vaikutuksen kautta). Maturiteettitasoa voidaan käyttää kertoimena, osana taulukon soluissa tehtävää laskentaa.



Kuva 15: Itsearvioinnin kautta voidaan saada tuntumaa investointien vaikuttavuudesta.

Esimerkki 5: Tietoturvainvestointien tuoma rajahyöty

Roskienhallintavirasto ja *Riskienhallintavirasto* panostavat kukin 0,3 MEUR viestintäturvallisuuden kehittämiseen. Organisaatiot ovat muuten hyvin samankaltaiset, mutta *Riskienhallintavirastossa* on jo vuosia panostettu viestintäturvallisuuteen, kun taas *Roskienhallintavirastossa* ollaan aika lailla lähtökuopissa. Sama tilanne voi päteä samaan organisaatioon eri ajankohtina eri tavoin. Täten investoinnin tuoma rajahyöty on pienempi *Riskienhallintavirastossa* kuin *Roskienhallintavirastossa*. Samalla 0,3 MEUR:in investoinnilla *Roskienhallintavirasto* saattaa pienentää riskiään noin 50%, kun taas *Riskienhallintavirastossa* sama riski pienenisi vain esimerkiksi 10% (fiktiivinen esimerkki Gordon-Loeb -mallia mukaillen).

[18] CMMI-maturiteettitasot (https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi)

[19] Itsearvioinnin apuna voi hyödyntää myös esimerkiksi kybermittaria (https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari)

8 Kustannus-vaikuttavuus-malli

Arvomallia voidaan käyttää digitaalisen turvallisuuden johtamiseen eli painotusten koordinaatioon ja eri osa-alueiden haasteiden tarkasteluun. Jotta organisaatio kykenisi turvaamaan arvoa laajemmin, strategisella tasolla, arvomalli tulee liittää strategiseen johtamiseen oikealla tavalla. Muuten riskinä on, että digiturvan ymmärrys jää asiantuntijatasolle ja arvomallin hyödyntäminen toimintojen kehittämisessä sekä riskien hallinnassa jää rajalliseksi, integroitumatta organisaation johtamismalliin. Kun digitaaliseen turvallisuuteen määritellään sen toimintaa ohjaavat ja kuvaavat rakenteet riittävällä tarkkuudella, näistä tulee eri tasojen toimijoiden (mukaan lukien asiantuntijoiden ja johdon) välistä yhteistä kieltä, jolla eri arvojen merkitykset välittyvät tehokkaasti.

Osana tätä on huomioitava, että informaatio on sovitettava kulloiseenkin johtamis- ja riskienhallintatarpeeseen soveltuvaksi. Analyysiä ja arviointia on kehitettävä strategiseen näkökulmaan (johtamisen ja päätöksenteon näkökulmaan ja työtapaan) soveltuvaksi ja siinä tehokkaasti hyödynnettäväksi. Tietosisältöjen viestiminen tehokkaasti edellyttää myös visuaaliseen ulkoasuun ja ymmärrettävyyteen panostamista. Kun tieto ja sen pohjalta tehdyt selvitykset ovat helposti ymmärrettäviä ja selkeästi johdettavissa toimenpiteiksi, kasvaa todennäköisyys, että näin tapahtuu.

8.1 Digitaalinen turvallisuus koordinointitasolta strategiselle tasolle

ISO 31000-standardissa korostetaan ylimmän johdon roolia ja riskienhallinnan sisällyttämistä organisaation johtamisjärjestelmään. Riskienhallinta on osa hallintotapaa ja johtajuutta. Se on keskeinen tekijä siinä, kuinka organisaatiota johdetaan kaikilla tasoilla. Riskienhallinta edesauttaa johtamisjärjestelmän kehittämistä. Keskeinen osa ISO 31000-standardia on organisaation arvon luominen ja säilyttäminen sisällyttämällä riskienhallinta organisaation johtamisjärjestelmään. Tämä tavoite on sovellettavissa myös julkisen hallinnon organisaatioihin, kun arvoa ajatellaan rahaa laajemmin.

Kustannus-vaikuttavuus-mallin merkitys johtamiselle ja organisaation digiturvallisuuden kustannusten optimoinnille ei tapahdu ilman siihen tarkoitettua prosessia ja metodiikkaa. Vaikuttavuuden arvioinnin kannalta on ratkaisevaa, että prosessit ja tulokset yhdistellään eikä tarkastella vaan jompaakumpaa[20]. Mikäli arvomallia ei hyödynnetä strategisen johtamisen taustalla, kustannusten kohdentaminen ja niistä saatava hyöty riskien käsittelyssä eivät toteudu optimaalisella tavalla. Vaarana on, että kohdennetaan resursseja ja varoja asioihin, jotka eivät ole strategisesta näkökulmasta keskeisimpiä ja merkittävimpiä. Lisäksi panostusten tulee olla oikeassa suhteessa niistä saatavaan hyötyyn.

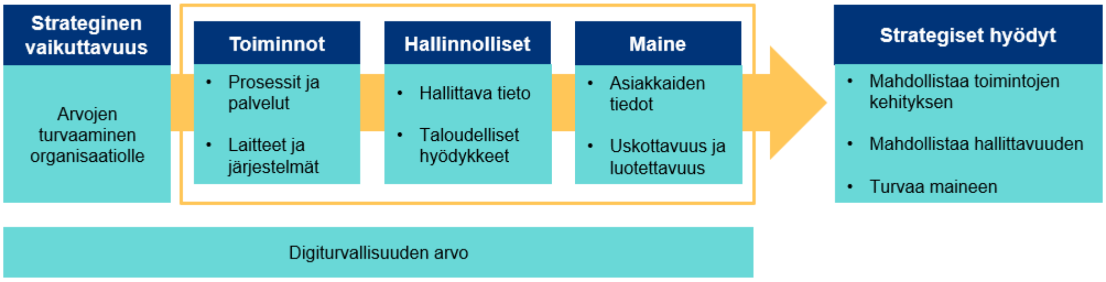
Julkisella sektorilla on huomioitava, että optimointi ja oikeasuhtaisuus rakentuvat osin toisella tavalla kuin yksityisellä sektorilla, johtuen ensin mainitun erilaisesta olemassaolon tarkoituksesta ja sitä määrittävästä lainsäädännöstä. Toisin kuin yksityisellä sektorilla, julkisella sektorilla ei voida hyväksyä tiettyjen riskien toteutumista (kuten

[20] *Peter Dahler-Larsen: Vaikuttavuuden arviointi, Hyvät käytännöt-käsikirja, Stakes 2005* (https://www.julkari.fi/handle/10024/77071)

turvaluokitellun tiedon paljastuminen) ja niiden käsittelyn on tapahduttava lainsäädännön asettamissa reunaehdoissa (vaikuttaa esim. riskin siirtoon muualle yhteiskunnassa).

Digiturvallisuuden vaikuttavuus on sitä, että organisaation digitaalisen toimintaympäristön muodostavat, siellä olevat ja siellä toimivat arvot (muun muassa prosessit, palvelut, laitteet, järjestelmät, hallittava tieto, taloudelliset hyödykkeet – kuten esimerkissä kuvassa 16), joiden varaan organisaatio rakentuu, ovat turvattuja. Näiden kautta myös esimerkiksi organisaation maine, luotettavuus ja lainsäädännöllisten tehtävien toteuttaminen on varmistettu. Siten digitaalisen turvallisuuden vaikuttavuus mahdollistaa toimintojen kehityksen, tiedon ja taloudellisten hyödykkeiden hallittavuuden sekä maineen turvaamisen.

Arvomallista päästään vaikuttavuustasolle varmistamalla, että arvomalliin sisältyvä analyysi otetaan osaksi organisaation strategisen tason suunnittelua ja johtamista. Tämä tapahtuu käytännössä huomioimalla johtamisen tiedon tarpeet paremmin käsittelytason vaihtuessa raportoitaessa. Tarkempi näkemys tässä analyysissä ja arvioinnissa on mahdollista vain tuntemalla kohdeorganisaatio ja sen toiminta riittävän laajasti arvojen merkityksen tulkitsemiseksi.



Kuva 16: Digiturvallisuuden strateginen vaikuttavuus tapahtuu arvojen turvaamisella, mikä mahdollistaa strategiset hyödyt.

Kuvassa 16 on yleisellä tasolla esitetty organisaation strategisella tasolla merkittäviä johtamisen alueita, joita digitaalinen turvallisuus kannattelee. Kuvassa toiminnot, hallinnolliset ja maine -kohdat ovat esimerkkejä keskeisistä suojattavista ja tuettavista osa-alueista ja niihin sisältyvistä asioista, joilla kuvassa päästään vasemmasta reunasta oikeaan reunaan, vaikuttavuudesta hyötyihin. Kun toimintojen, hallinnolliset ja maine -kysymykset ovat riittävällä tavalla turvattu, digiturvallisuus omalta osaltaan tukee strategisten hyötyjen muodostumista. Tätä hyötyjen muodostumista pyritään osaltaan optimoimaan hyvällä riskienhallinnalla ja sen sisällä käytettävällä vaikuttavuusmallilla.

Kuvassa alimmaisena oleva digiturvallisuuden arvo kuvaa strategisen vaikuttavuuden laskettavissa olevaa osuutta, joka kannattelee sen yllä olevia abstraktimpia strategisia tarpeita ja hyötyjä. Digiturvallisuuden arvo siis mahdollistaa kustannus-vaikuttavuus-mallista saatavat strategiset hyödyt ja on osa strategisten tavoitteiden saavuttamiseen tarvittavia kustannuksia.

8.2 Digitaalinen turvallisuus strategiselta tasolta koordinaatiotasolle

Mallien on tarkoitus parantaa johdon käsitystä ja kontrollia digitaalisesta turvallisuudesta. Tätä varten kustannus-vaikuttavuus-mallia voidaan tarkastella myös ylhäältä alaspäin, johdon suunnasta. Tällöin tunnistetaan (ja sanoitetaan) strateginen tavoite sekä sitä tukevat, mahdollistavat ja suojaavat hyödyt, joihin digitaalinen turvallisuus liittyy. Näiden perusteella rajautuu se osa – mahdollisesti hyvin monipuolinenkin kokonaisuus – digitaalista turvallisuutta, jota halutaan tarkastella. Tämän tyyppinen tarkastelu voi olla tarpeen esimerkiksi, kun muodostetaan uusi strateginen tavoite, jonka onnistuminen halutaan varmistaa, tai halutaan tietää, ovatko toimintaympäristön ennakoidut muutokset luomassa tarpeita uusille panostuksille, jotta haluttu taso voidaan säilyttää valittujen hyötyjen osalta. [21]

Pitkäjänteisessä ja pysyväisluonteisessa tarkoituksessa, kuten toimintaa ohjaavissa prosesseissa tulee olla etukäteen määritettynä tavoitteita ja digitaalisessa turvallisuudessa näitä ovat suojattavien arvojen määrittäminen johdon toimesta. Ne voivat sisältää priorisointia sekä mittareita (esimerkiksi määriä). Näiden pohjalta voidaan muodostaa osin tai kokonaan menetysluokittelu. Tämä on johdon työkalu tarkastella organisaation onnistumista välttämään toimintaa haittaavia menetyksiä.

Arvomallin ja hallintarakennetta mukailevan kustannusluokittelumallin avulla johto voi tarkastella rahallisten panostusten kautta tapahtuvaa ohjausta riskienhallinnallisesta näkökulmasta digitaalisen turvallisuuden osalta. Sen tulisi kertoa miten digitaalinen turvallisuus on muodostettu, miten sen kehitystä on ohjattu panostusten painotuksilla ja miten sen toteuttajille on ohjattu investointien kautta mahdollisuuksia toimia. Nämä itsessään antavat kuvaa siitä, onko johto riittävässä määrin huomioinut digitaaliseen turvallisuuteen liittyvät tarpeet, mutta syvempiä analyysejä saadaan vertaamalla näitä aiemmin mainittuun johdon määrittelemään menetysluokitteluun ja niihin liittyviin tavoitteisiin, organisaation toimintaan tai kykyyn vastata muutoksiin (resilienssi).

Digitaaliset riskit tulisi käsitellä osana organisaation muita riskejä (organisaation kokonaisriskienhallinta), jolloin niitä voidaan muotoilla osaksi muun muassa palveluiden tai prosessien riskejä, kyse on monimutkaisesta kokonaisuudesta, joka ylittää digitaalisen toimintaympäristön. Tällöin haasteeksi voi tulla oikea luokittelu, mutta hyvässä riskienhallinnassa hyödynnetään kattavan näkemyksen saamiseksi useita, joiden käyttö onnistuu moderneilla digitaalisilla työkaluilla. Ylätasolla näkökulma riskeihin on usein julkishallinnonkin johdolla COSO-ERM[22]-tyyppiseen jaotteluun perustuva (strategiset, operatiiviset, taloudelliset ja vahinkoriskit – tai tämän variaatio).

Digitaalisen turvallisuuden merkityksen voidaan nähdä kasvaneen digitaalisen toimintaympäristön ja digitaalisen toiminnan kasvaessa. Tämän tulisi näkyä myös talousraportoinnissa, absoluuttisina ja suhteellisina osina organisaation kokonaismenoista ja tulevien tilikausien ennustetuista budjeteista, mutta tarkemmalla tasolla myös eri

---

[21] Lisää organisaation johdon muista tehtävistä esimerkiksi: *Traficom: Kyberturvallisuus ja yrityksen hallituksen vastuu* (https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf) ja *NCSC: Questions for the board to ask about cyber security* (https://www.ncsc.gov.uk/files/NCSC_Board-Toolkit-Questions-for-Boards.pdf)

[22] *COSO-ERM* (https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf)

toimialueiden, prosessien, palveluiden tarkasteluissa. Kunkin kohdalla tulisi pystyä hahmottamaan suuntaa antavalla tarkkuudella johtamisen mahdollistamiseksi mikä on sopivaa ja oikeasuhtaista. Rahallinen arvio täydentää riskin merkityksen ymmärtämistä ja tukee talouden suunnittelua tuomalla konkretiaa. Organisaatio itse on vastuussa määrittelemään merkitykselliset seurattavat tarkastelut ja niiden frekvenssin – milloin on kyse pidemmän aikavälin tarkasteluista tai halutaanko joiltain osin tietoja päivittäisjohtamisen tueksi.

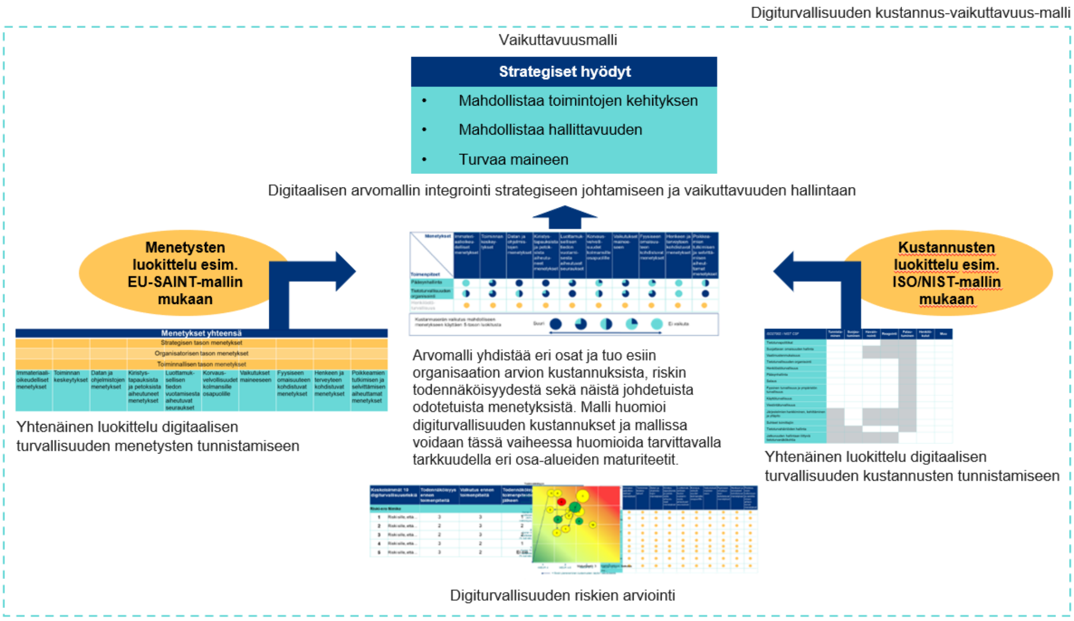
On hyvä huomioida, että digitaalinen turvallisuus ja siihen liittyvä riskienhallinta voi toimia myös joidenkin strategisten valintojen mahdollistajana. Ilman hyvää digitaalista turvallisuutta muu kehittäminen voi vaarantua. Tietyt organisaation kehityshankkeet tai suunnanvalinnat, esimerkiksi digitaalisen kehityksen saralla, vaativat että digitaalisen turvallisuuden valmiudet ovat tarpeeksi hyvällä tasolla. Esimerkiksi automaatio, datan hallinta, ulkoistukset, pilvipalvelut yms. vaativat asianmukaista digitaalisen turvallisuuden riskien käsittelyä. Tulevien tarpeiden riskien tarkastelu on usein yhteydessä tulevaisuuden ennakointityöhön ja organisaation strategityöhön.

9 Digiturvallisuuden kustannus-vaikuttavuus-mallin merkitys

Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallin tavoitteena on mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi tekeminen sekä varmentaa, että toimenpiteet kohdistetaan oikeisiin kohteisiin ja toteutetaan oikean suuruisilla panostuksilla. Mallissa tarjotaan toimintatavat, joiden avulla organisaatiot voivat systemaattisesti hallita arvojen suojaamista, analysoida järjestelmällisellä tavalla panostuksia ja vaikutusketjuja digiturvassa sekä kvantifioida yhdenmukaisella tavalla euromääräisesti toimenpiteitä (investointeja), joilla riskejä pyritään hallinnoimaan ja pienentämään. Yleisesti, digitaalisen turvallisuuden taloudellisia merkityksiä on voitava analysoida organisaatioissa sekä laajemmin julkisessa hallinnossa jo hyvän hallintotavan varmistamiseksi.

Yhteenvetona voidaan todeta, että digitaalisen turvallisuuden kustannus-vaikuttavuus-malli ja sen mahdollistamat hyödyt perustuvat kokonaisuuteen, jossa organisaatio osaa yksittäisen riskin hallintatoimien kustannusten laskennan lisäksi:

- tunnistaa digitaalisen turvallisuuden uhat ja näihin yhdistettävät menetykset (”Menetysluokittelu”)
- tunnistaa ja seurata digitaaliseen turvallisuuteen liittyviä kuluja ja kustannuksia (”Kustannusluokittelu”)
- määritellä arvon uhkaan liittyvälle menetykselle sekä riskin uhan toteutumisesta (”Arvomalli”)
- integroida edellä mainitut mallit osaksi organisaation strategista johtamista ja hallintomallia ja täten mahdollistaa digiturvallisuuden strateginen vaikuttavuus (”Vaikuttavuusmalli”)



Kuva 17: Digitaalisen turvallisuuden kustannus-vaikuttavuus-malli ja sen osaset yhteen koottuna.

Kustannus-vaikuttavuus-mallissa esitetty arvoketjun kokonaisrakenteen voidaan olettaa olevan pysyvämpi rakenne, kun taas erilaisten luokitteluiden tulee voida sekä organisaatiokohtaisten erityisyyksien ja tarpeiden, että digitaalisen toimintaympäristön kehityksen vuoksi, joustaa ja muuttua. Rakenne kuitenkin auttaa välttämään pistemäisiä ja kertaluonteisia tapoja tehdä näitä tarkasteluita.

Tämän mallin toteuttamisessa tulisi tavoitella sen sisällyttämistä osaksi automatisoitua taloushallintoa. Tulevaisuudessa on tietotarpeiden täyttämiseksi tärkeää pyrkiä automatisoimaan riskienhallintatiedon keruuta, luokittelua ja analyysiä, jotta näiden toteuttaminen ei tarpeettomasti kuormita organisaatioita ja niiden asiantuntijoita. Ennen kuin tähän kuitenkaan päästään, mallia voidaan soveltaa myös otosmaisiin analyyseihin, joissa voitaisiin hyödyntää myös tekoälypohjaisia sovelluksia.

Käytettyjen käsitteiden tukisanasto

Alla on selvennettynä tässä dokumentissa käytetyt keskeiset termit, perustuen eri lähteisiin. Digitaalisen turvallisuuden riskienhallinnan käsitteiden ylläpidetty sanasto on VAHTI-riskienhallintasanasto osoitteesta: http://uri.suomi.fi/terminology/digiriski/

Arvo: Arvo on tässä kontekstissa omaisuuden (aineellinen tai aineeton), tavaran tai palvelun rahallinen, aineellinen tai arvioitu arvo (kts. myös suojattava arvo). Arvo voi olla suoraa tai välillistä, jolloin arvoa voidaan nähdä myös esimerkiksi tavassa toimia, organisaatioiden ja muiden verkostojen rakenteessa sekä yksilöä suojaavien perusarvojen toteuttamisessa. Yhtenä arvon yhteismitallisena mittarina sovelletaan usein rahallista arvoa, mikäli se soveltuu tarkastelutapaan.

Arvomalli: Määrittelee arvon uhkaan liittyvälle menetykselle sekä riskin uhan toteutumisesta. Arvomalli yhdistää kustannus- ja menetysluokittelun.

Digitaalisen toiminnan riski: Digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski.

Digitaalinen turvallisuus: Tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa ja toiminta sekä siellä että siihen liittyen on turvallista ja hallittua, myös häiriötilanteissa.

Diskonttaus: Diskonttaus on tulevaisuudessa suoritettavan hinnan tai maksun nykyarvon laskemista eli koron osuuden poistamista tulevaisuudessa tapahtuvasta maksusuorituksesta.

Hallintakeino: Termiä hallintakeino käytetään joskus kontrollin synonyyminä, mutta usein hallintakeino viittaa kokonaisratkaisuun (esimerkiksi tunnistautuminen tai hyvä hallintotapa), joka voi sisältää useita konkreettisia kontrolleja. Kontrolleja voidaan tarkastella tyypeittäin tai suojeltavan kohteen mukaan, esimerkiksi valvontatoimenpiteet eli valvontakontrollit omana ryhmänään tai tiedon saatavuutta suojaavat kontrollit erillisenä kokonaisuutena.

Investointi: Investoinneilla tarkoitetaan organisaation toimintaan tarvittavien tuotantohyödykkeiden hankkimista tulevien tuottojen [tai muiden hyötyjen] saamiseksi. Voivat sisältää hankinta- ja käyttökustannuksia niiden vaikutukset voivat jakautua usealle vuodelle.

Jäännösriski: Riskin käsittelyn jälkeen jäljellä oleva riski.

Koordinointitaso: Organisaation päätöksenteon taso, jolla strategisen tason päätökset huomioiden tehdään yksittäisten liiketoiminta-alueiden ja yksiköiden toiminnan järjestämistä koskevat päätökset.

Kulu: Kululla tarkoitetaan vastaanotetun tuotannontekijän hankintamenon osaa, joka jaksotetaan tietylle tilikaudelle ja joka kirjataan tuloslaskelmaan. Kulu on tässä dokumentissa spesifi digiturvallisuuden kustannuksien osa, kuten ICT-kulu, salaukseen liittyvä kulu tai henkilöstökulu.

Kustannus: Kustannuksella tarkoitetaan suoritteiden aikaansaamiseksi tehtyä taloudellista uhrausta, joka aiheutuu tuotannontekijöiden käytöstä tai kulutuksesta. Kustannuksella viitataan tässä dokumentissa pääosin digiturvaan liittyvänä kokonaiskustannuksena, jonka sisällä kustannukset voidaan jaotella yksittäisiksi ja spesifimmiksi kuluiksi.

Kustannusluokittelu: Kustannusluokittelumallin tarkoitus on tunnistaa ja seurata digitaaliseen turvallisuuteen liittyviä kuluja ja kustannuksia valitun luokittelutavan mukaisesti. Sen ymmärtämistä helpottaa, mikäli se vastaa käytettyä hallinnan rakennetta eli turvallisuuden johdettujen osa-alueiden muodostamaa jakoa.

Kustannus-vaikuttavuus-malli: Kustannus-vaikuttavuus-malliksi kutsutaan kokonaisuutta, joka muodostuu riskien analysoinnista, menetysten luokittelusta, kustannusten luokittelusta ja arvomallista sekä näiden integroimisesta osaksi organisaation strategista johtamista ja hallintomallia.

Laskentamalli: Laskentamallilla viitataan tässä dokumentissa riskien laskentamalliin, jossa määritellään yksittäisten riskien arvo ja miten niitä käsitellään.

Menetys: Menetys on tässä kontekstissa arvon menetys.

Menetysluokittelu: Menetysluokittelun tarkoitus on tunnistaa digitaalisen turvallisuuden uhat ja näihin yhdistettävät menetykset.

Riski: Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Riskien arviointi: Riskien toteutumisen todennäköisyyden ja niiden mahdollisten vaikutusten selvittäminen.

Riskienhallinta: Riskienhallinnalla tarkoitetaan koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Se on systemaattista ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan riskejä.

Riskienhallintapolitiikka: Organisaatiokohtainen kuvaus riskienhallintaperiaatteista ja keskeisinä pidetyistä riskienhallinnan puitteista.

Riskienhallintaprosessi: Menettely riskien arviointiin (tunnistamiseen, analysointiin, merkityksen arviointiin), käsittelyyn, seurantaan ja viestintään.

Riskienhallinnan läpinäkyvyys: Riskienhallinnan arvioinnin mahdollistaminen sidosryhmille ja sisäisille toimijoille siten, että siihen liittyvät tiedot välitetään niiltä osin, kuin tietojen välittäminen ei itsessään tuota merkittäviä riskejä.

Riskien luokittelu: Riskien tehokasta arviointia ja käsittelyä varten tehtävät ryhmittelyt, joiden ansiosta samankaltaisia tai samaan vastuualueeseen kuuluvia riskejä tai niiden osia voidaan tarkastella yhtenä kokonaisuutena.

Strateginen taso: Organisaation päätöksenteon taso, jolla tehdään toimintaympäristöön ja toiminnan rahoittamiseen liittyvät, koko organisaation toimintaa ja kehittämistä koskevat päätökset.

Suojattava arvo: Suojattavalla arvolla tarkoitetaan tässä dokumentissa sekä konkreettisia järjestelmiä, joilla nähdään rahallista arvoa, arvoa, joka sisältyy tietoon ja sen käyttöön, että laajempia yhteiskunnallisia tai perusarvoja. Nykyaikaisessa ja kompleksisessa maailmassa on huomioitava, että riskit voivat kohdistua useille eri tasoille. Tämä laajentaa niin sanotun suojattavan kohteen määritelmää, sillä esimerkiksi yksittäinen tietovarasto voi olla merkityksetön sen rinnalla, miten varmistetaan palvelukokonaisuuden jatkuvuus, tai miten se ja muut digitaalisen toimintaympäristön sosioteknisen järjestelmän osaset vaikuttavat mm. ”luottamuksen” muodostumiseen. Strategiset tavoitteet voidaan usein muotoilla laajemmiksi suojattaviksi arvoiksi.

Toiminnallinen taso: Organisaation päätöksenteon taso, jolla strategisen tason ja koordinointitason päätökset huomioiden tehdään toteutusta ja toimeenpanoa koskevat päätökset.

Toteutumattoman vaikutuksen arvo: Vältetyn riskin vaikutuksen käänteinen arvo, jonka avulla voidaan kuvata riskienhallinnan vaikuttavuutta

Uhka: Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku.

Liite 1. Viitekehysten kääntötaulukko ISO 27002:2017 ja 2022 sekä NIST CSF 2.0 luonnos

ISO 27002:2017 ja 2022 rakenteen kääntötaulukko – ISO 27002 – NIST CSF 2.0.

ISO 27002:2017 PÄÄTURVALLISUUSLUOKAT / ISO 27002:2022 HALLINTAKEINOT / NIST CFS 1.1/(2.0)	KYBERTURVALLISUUSKÄSITTEET					HALLINTA						
	TUNNISTUS	SUOJAUS	HAVAINTO	VASTE	PALAUTUS	Hallintotapa	Hallintotapa ja ekosysteemi	Omaisuudenhallinta	Identiteetti ja käyttövaltuushallinta	Toimittajasuhteiden hallinta	Uhkien ja haavoittuvuuksien hallinta	Tietoturvatapahtumien hallinta
5 TIETOTURVAPOLITIIKAT	2					2	2					
6 TIETOTURVALLISUUDEN ORGANISOINTI	4	6	1	3	2	5	3	2	1		1	
7 HENKILÖSTÖTURVALLISUUS	1	5		1		1	6	1				
8 SUOJATTAVAN OMAISUUDEN HALLITA	3	7					4	8				
9 PÄÄSYNHALLINTA		14							13			
10 SALAUS		2										
11 FYYSINEN TURVALLISUUS JA YMPÄRISTÖJEN TURVALLISUUS		16	2					7	2			
12 KÄYTTÖTURVALLISUUS	2	14	8	1	2		4	1	1		2	6
13 VIESTINTÄTURVALLISUUS		8	1				1	3		1		
14 JÄRJESTELMIEN HANKKIMINEN, KEHITTÄMINEN JA YLLÄPITO	3	11	1			2				1		
15 SUHTEET TOIMITTAJIIN	5	1					6			6		
16 TIETOTURVAHÄIRIÖIDEN HALLINTA	1	1	3	3	2							7
17 LIIKETOIMINNAN JATKUVUUDEN HALLINTAAN LIITTYVIÄ TIETOTURVANÄKÖKOHTIA		3		4				1				
18 VAATIMUKSENMUKAISUUS	8	5					6	1				
Kontrolleja yhteensä	*29*	*93*	*16*	*12*	*6*	*10*	*32*	*24*	*17*	*8*	*3*	*13*

Kääntötaulukkoa voidaan hyödyntää esimerkiksi, kun vertaillaan ISO 27002: 2017, ISO 27002:2022 ja NIST CSF 2.0 (luonnos) keskeisiä hallintakeinoja ja niiden sijoittumista ISO 27002:2017 tietoturvallisuuden hallintakeinojen pääluokkiin. NIST CSF 2.0 hallinnolliset osuudet jakautuvat mahdollisesti organisatorisiin ja henkilöstö-hallintakeinoihin. NIST CSF 2.0 on tämän dokumentin julkaisuhetkellä luonnosvaiheessa.

Liite 2. Vaihtoehtoinen kustannusluokitteluesimerkki soveltaen ISO27002:2022

ISO27002:2022 perustuva vaihtoehtoinen esimerkki kustannusluokittelulle. Taulukon rakenne perustuu standardin liitteen A taulukossa käytettyyn hallintakeinojen luokitteluun ”Toiminnalliset kyvykkyydet”. Toiminnalliset kyvykkyydet on attribuutti, jolla hallintakeinoja voidaan tarkastella toteuttajan tietoturvakyvykkyyksiä koskevasta näkymästä. Taulukossa ne yhdistyvät toisena akselina käytetyn standardin rakenteen hallintakeinojen jaottelun kanssa. Kontrollitoimenpiteet asettuvat valkoisille alueille, harmaat eivät sisällä hallintakeinoja.

Toiminnalliset kyvykkyydet / Hallintakeinoalueet	Organisaatio	Henkilöstö	Fyysiset	Teknologiset
Hallintotapa				
Omaisuudenhallinta				
Tietojen suojaaminen				
Henkilöstönturvallisuus				
Fyysinen turvallisuus				
Järjestelmän ja verkon turvallisuus				
Sovelluksen turvallisuus				
Turvallinen konfigurointi				
Identiteetti - ja käyttövaltuushallinta				
Uhkien ja haavoittuvuuksien hallinta				
Toimittajasuhteiden hallinta				
Lait ja vaatimustenmukaisuus				
Tietoturvatapahtumien hallinta				
Tietoturvallisuuden varmentaminen				
Jatkuvuus				

Standardi ISO 27002:2022 liite A sisältää useita attribuutteja, jotka sisältävät eri tapoja ryhmitellä hallintakeinoja. Organisaatiot voivat hyödyntää näitä tietoturvallisuuden hallinnassa ja luokitteluiden rakentamisessa. Kattavan digitaalisen turvallisuuden näkymän saavuttamiseksi tulee huomioida, että näitä voidaan joutua täydentämään.