



DIGI- JA
VÄESTÖTIETO-
VIRASTO

Kustannus-vaikuttavuus -malli digitaalisen turval- lisuuden riskien sekä riskienhallinnan analy- sointiin - lyhennelmä

VAHTI-hyvät käytännöt tukimate-
riaali

1.12.2023

1.12.2023

Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallilla ote riskeistä ja riskienhallinnasta kaikilla organisaation tasoilla

Digitaalisen turvallisuuden parantaminen vaatii toimenpiteitä, joista syntyy kustannuksia, jotka on kohdistettava tehokkaasti ja perustellusti. Kustannus-vaikuttavuus-malli tarjoaa rakenteen, jonka avulla organisaatiot voivat systemaattisesti arvioida suojattavia kohteita, niihin liittyviä riskejä sekä kvantifioida toimenpiteitä, joilla riskejä pyritään hallitsemaan ja pienentämään. Täten saadaan näkyväksi digitaalisen turvallisuuden vaikuttavuus ja kustannukset, jolloin voidaan varmentaa, että digiturvaan liittyvät toimenpiteet kohdistetaan oikein ja toteutetaan oikean suuruisella resursoinnilla.

Kustannus-vaikuttavuus-malli pyrkii edesauttamaan johdon, digiturvan asiantuntijoiden sekä riskin omistajien (substanssiasiantutijat, projektipäälliköt yms.) ymmärrystä digitaalisesta turvallisuudesta ja sillä tuottavasta hyödystä. Malli huomioi riskien ja niiden merkityksen muutokset eri tasoilla eri käyttötarkoituksiin, kooten tätä arvoketjua yhteen:

1. **Riskien laskentamalli:** Riskien analysointi ja tarvittavien hallintatoimien rahallisen arvon laskeminen yksittäisille riskeille käytännötasolla
2. **Arvomalli:** Arvon määrittäminen ryhmiteltyihin riskeihin liittyville mahdollisille menetyksille sekä niiden hallintatoimille menetys- ja kustannusluokittelun kautta:
 - digitaalisen turvallisuuden uhkien vaikutuksiin yhdistettävien menetysten tunnistaminen rakenteellisesti ("menetysluokittelu")
 - digitaalisen turvallisuuden toteuttamiseen liittyvien kulujen ja kustannusten tunnistaminen ja seuranta rakenteellisesti ("kustannusluokittelu")
3. **Vaikuttavuusmalli:** arvojen merkityksen linkittyminen osaksi organisaation kokonaisriskienhallintaa, strategista johtamista ja hallinnollista vaikuttavuutta.



Kuva 1: Digitaalisen turvallisuuden kustannus-vaikuttavuus-mallin yleisrakenne ja sen eri tasot.

Mukautusvaihtoehtoja, yksityiskohtia ja taustaa mallista avataan tämän tiivistelmän lähteenä olevassa Digi- ja väestötietoviraston (DVV) julkaisemassa laajemmassa dokumentissa¹. Malli on tarkoitettu ensisijaisesti julkishallinnon eri organisaatioille, mutta se on sovellettavissa myös näiden ulkopuolella.

¹ Kustannus-vaikuttavuus-malli digitaalisen turvallisuuden riskien sekä riskienhallinnan analysointiin (<https://dvv.fi/digiturvajulkaisut>)

1.12.2023

Digiturvallisuuden kustannus-vaikuttavuus-mallin integroimisella strategiseen johtamiseen merkittäviä hyötyjä

Riittävällä tasolla oleva digiturvallisuus tukee omalta osaltaan organisaation strategisia tavoitteita. Myös johdon vastuut ja rooli digitaalisen turvallisuuden varmistamisessa tulevat kasvamaan (mm. EU:n NIS2-sääntely). Näihin kustannus-vaikuttavuus-mallin soveltaminen antaa työkaluja. Kustannus-vaikuttavuus-mallin tuella hyvän riskienhallinnan hyötyjen muodostumista voidaan optimoida strategisen vaikuttavuuden suhteen. Kokonaisuuteen sisältyvässä arvomallissa kerättyä ja arvoitettua riskitietoa jatkokäsitellään, jotta riskien arvoitusten merkityksiä voidaan tarkastella tarvittavalla tasolla ja hyödynnettävissä olevina kokonaisuuksina. Laadukas tieto mahdollistaa riskitietoisesta ja tietoon perustuvan johtamisen niin kyberturvallisuuteen, tietoturvaan, tietosuojaan kuin jatkuvuudenhallintaan.

Kustannus-vaikuttavuus-malli tulee integroida osaksi johtamista ja riskienhallintaa, jotta organisaatio voi saada strategisia hyötyjä digiturvallisuuden toteuttamisesta. Näin digiturvallisuudesta tulee kiinteämpi osa organisaation riskienhallintaa selkeyttämällä kokonaiskuvaa digiturvasta. Lisäksi mallin käyttöönoton myötä digiturvaan liittyviä kustannuksia on helpompi hahmottaa, jolloin voidaan tehdä parempia tietoisia päätöksiä ja resurssien kohdentamista, jotta organisaatiota, sen sidosryhmiä sekä omaisuutta voidaan suojata tehokkaammin. Johtotasolla käsitellyllä digitaalisella turvallisuudella on vahva merkitys sidosryhmäviestinnässä, maineen ja luotettavuuden rakentajana, mikä puolestaan heijastuu asiakasrajapinnassa palveluiden käyttöön.



Kuva 2: Digitaalinen turvallisuus mahdollistaa strategisia hyötyjä. Vaikuttavuusmallilla pyritään avaamaan tätä sekä linkittämään strateginen tarkastelu organisaation hallintaan ja koordinaatioon.

Kustannus-vaikuttavuus-mallin hyödyntäminen on linjassa valtionhallinnon riskikäsi-kirjassa esitetyn kanssa². Mallissa esitetty tarkastelu on yksi tarkastelumalli digitaaliselle turvallisuudelle, mutta johdon tulisi tämän lisäksi olla tietoinen muistakin tämän aihealueen toiminnoista ja haasteista³.

² Valtiovarainministeriön julkaisu 2023:54: *Riskienhallinnan käsikirja valtionhallinnon toimijoille* (<http://urn.fi/URN:ISBN:978-952-367-633-6>)

³ Lisää vinkkejä organisaation johdon näkökulmasta tehtävään digitaalisen turvallisuuden toteutuksen varmistamiseen 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)

1.12.2023

Digiturvallisuuden painotusten kohdistamisen avuksi hallintaa tukeva menetysten ja kustannusten luokittelu

Uhkien toteutumisesta aiheutuvien seurausten ymmärtämiseksi on tärkeää, että digiturvallisuuden kustannukset ja mahdolliset menetykset arvioidaan. Kustannus-vaikutavuus-mallissa arvomalli yhdistää menetys- ja kustannusluokittelun. Digiturvallisuuden kustannukset tulisi kyetä erottaa organisaation muista kustannuksista, jotta digiturvan kustannuksia voidaan seurata, mitata ja hyödyntää. Tämä edellyttää kulujen ja kustannusten tunnistamista sekä niiden luokittelua. Yhtenevä luokittelutapa edesauttaa kehittämään yhtenäistä ymmärrystä kustannusten sisällöstä ja rakenteesta, ja tukee kustannusten seurantaa sekä resurssien käytön optimointia.

Oleellista on, että kustannusluokat ovat yhdistettävissä digitaalisen turvallisuuden johtamisessa ja riskien arvioinneissa käytettäviin luokitteluihin, jotta mahdollistetaan digitaalisen turvallisuuden kustannuksiin liittyvien hyötyjen mittaaminen todellisuutta parhaiten vastaavalla tavalla. Kustannus-vaikutavuus-mallissa luokittelu voidaan toteuttaa datalähtöisesti tai toimintalähtöisesti. Digitaaliset työkalut mahdollistavat useiden luokittelutapojen rinnakkaisen käytön – usealta kantilta tarkastelu parantaa kokonaiskäsitystä. Mallia varten on lähdedokumentissa esitetty esimerkki käytettävyyden kannalta tasapainotetusta kustannusten luokittelumatriisista, joka perustuu yleisiin tietoturvallisuuden viitekehyksiin ja niiden rakenteisiin; NIST CSF pääluokkiin sekä ISO 27002 standardin pääkohtiin.

Menetysten ja kustannusten arviointi auttaa tiedostamaan digiturvan merkityksen paremmin, tunnistamaan kriittiset digiturvaan liittyvät ongelmat, priorisoimaan toimenpiteitä sekä suunnittelemaan digiturvaan liittyviä investointeja. Arviointi tukee organisaation budjetin suunnittelua, perusteltuja hankintoja sekä oikeaa suhteutusta muihin priorisoitaviin hankkeisiin.

Digiturvallisuuden kustannus-vaikutavuus-malli työkaluna yksittäisten digitaalisten riskien hallinnassa ja priorisoinnissa

Riskien mahdollisesta toteutumisesta aiheutuu menetyksiä ja riskien hallintatoimenpiteet aiheuttavat kustannuksia. Riskien analysointi – rahallista arvoa syvemmin – on edellytys menetysten ja kustannusten luokittelulle sekä koko kustannus-vaikutavuus-mallin käytölle. Riskien arviointi ja luokittelu antavat organisaatiolle systemaattisen lähestymistavan uhkien tunnistamiseen ja riskiprofiilin muodostamiseen. Digitaaliset riskit tulee pyrkiä sisällyttämään mukaan organisaation kokonaisriskienhallintaan.

Riskejä tulee ensisijaisesti arvioida niiden merkityksen ja hallinnan kannalta, mutta riskeistä tulisi myös tuottaa rahallinen arvio. Rahallinen arvio täydentää riskin merkityksen ymmärtämistä ja tukee talouden suunnittelua tuomalla konkretiaa. Tämä antaa pohjan menetysten ja kustannusten luokittelulle sekä digiturvaan liittyvien toimenpiteiden, resurssien ja investointien kohdentamiselle.

Mallin käyttöönotto osana riskienhallintaa auttaa hahmottamaan mistä suurimmat menetykset ja kustannukset aiheutuvat, ja sitä kautta ohjaa digiturvaan liittyviä riskienhallintatoimia ja päätöksiä. Lähdedokumentissa olevalla digiturvallisuuden taloudellisen hyötyarvioinnin laskentakaavalla voidaan laskea digiturvallisuuden investointien taloudellinen hyöty. Euromääräisillä luvuilla organisaation asiantuntijat pystyvät perustelemaan digiturvaan liittyviä tarpeita, hankintoja ja prioriteetteja. Tämä kokonaisuudessaan kehittää johdon suuntaan tehtävää raportointia, niin nyky- kuin tulevista tavoitetilasta ja mahdollistaa siten johdon päätöksenteon tukemisen ja toimenpiteiden käynnistämisen organisaatioiden toimintaympäristössä.



Valikoidut keskeiset käsitteet tiivistetysti

Arvo: Arvo on tässä kontekstissa omaisuuden, tavaran tai palvelun rahallinen, aineellinen tai arvioitu arvo (kts. myös suojattava arvo).

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

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

Kulu: Osuus menosta, joka jaksotetaan tietylle tilikaudelle ja kirjataan tuloslaskelmaan.

Kustannus: Resurssin käytöstä aiheutuva taloudellinen uhraus.

Kustannusluokittelu: Kustannusluokittelumallin tarkoitus on tunnistaa ja seurata digitaaliseen turvallisuuteen liittyviä kuluja ja kustannuksia.

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 (kts yllä) 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.

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.

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

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.

Uhka: Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku.

Termit laajemmin taustadokumentissa. Lähteinä mm. [VAHTI-riskienhallintasanasto](#), Suomi.fi [Yhteentoimivuusalustan sanastot](#) sekä [TEPA-termipankki](#).