Kybermittari - esittely

TRAFICOM
Liikenne- ja viestintävirasto

Esittelyn agenda

Kybermittarin esittelyn agenda

- Johdanto aiheeseen
- Kybermittarin arviointimalli
- Kybermittarin arviointiprosessi
- Kybermittari-työkalu

Johdanto aiheeseen

Kybermittarin tausta ja tarkoitus

Kybermittari lyhyesti

- Kybermittari auttaa
  - muodostamaan tilannekuvan kyberturvallisuuskyvykkyyksistä ja potentiaaliset kehityskohteet
  - mahdollistaa yritysten ja toimialojen vertailun ja parhaiden käytäntöjen jakamisen
  - tunnistamaan yrityksen ja yhteiskunnan kannalta kriittiset palvelut ja riskit

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen julkaisema kansallinen kyberturvallisuuden arviointimalli
  - Yhtenäinen lähestymistavan kyberturvallisuuden arviointiin ja kehittämiseen
  - Koottu kansallisista ja kansainvälisistä käytänteistä
  - Vapaasti saatavilla suomen, ruotsin ja englannin kielisenä

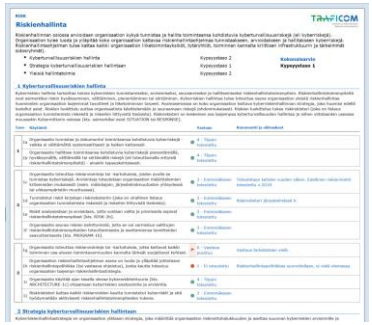
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

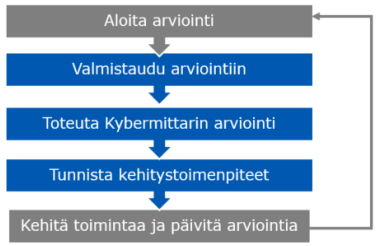
Kybermittarin kohdeyleisö

- Yksityiset ja julkiset organisaatiot
  - Voivat hyödyntää Kybermittaria vapaasti joko itse tai kaupallisen palveluntarjoajan tukemana
  - Halutessaan jakaa arviointituloksensa luottamuksellisesti Kyberturvallisuuskeskukselle ja hyötyä toimialansa anonyymin vertailutiedon rakentumisesta
- Kaupalliset palveluntarjoajat voivat käyttää, muokata ja levittää Kybermittaria vapaasti
- Kyberturvallisuuskeskus
  - Omistaa Kybermittarin tuotenimen ja vastaa Kybermittarin ylläpidosta ja jatkokehityksestä
  - Tarjoaa Kybermittarin yksityisten ja julkisten organisaatioiden, kaupallisten palveluntarjoajien ja viranomaisten vapaasti käytettäväksi, muokattavaksi ja levitettäväksi
  - Toimii kansallisena luottamuspisteenä anonyymin vertailutiedon keräämisessä, säilyttämisessä ja jakamisessa

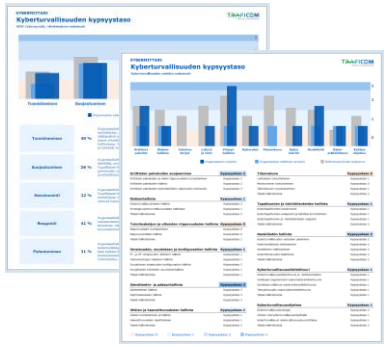
Kybermittarin materiaalit



- Arviointityökalu
  - Kohteena liiketoiminnalle ja yhteiskunnalle kriittiset toiminnot;
  - Kattaa yleisimmät kyberturvallisuuden riskienhallinnan osa-alueet;
  - Pohjana olemassa olevat NIST ja C2M2 -mallit ja parhaat käytännöt.



- Ohjeistus ja tuki arviointiprosessiin
  - Organisaation itse toteuttamana tai ulkoisen palveluntarjoajan tukemana.



- Automaattisesti tuotetut raportit
  - Tuloksena organisaation kyberturvallisuuden kypsyystaso eri näkökulmista.

Tietoa Kybermittarista

- Verkkosivusto https://www.kyberturvallisuuskeskus.fi/fi/kybermittari

Kybermittari

Kyberturvallisuuskeskuksen kehittämä Kybermittari auttaa yritysjohtoa ja organisaatioita saamaan kyberriskit kattavammin hallintaan ja turvaamaan toimintansa jatkuvuuden.

MATERIAALIT

Materiaali koostuu Kybermittarin arviointityökalusta ja käyttöohjeesta, joka tarjoaa ohjeita ja neuvoja mittarin käyttöön, arvioinnin toteuttamiseen ja tulosten hyödyntämiseen. Sivulle lisätään tulevaisuudessa myös muuta tukimateriaalia ja käyttöohjeen käännökset ruotsiksi ja englanniksi.

Tämän lisäksi marraskuusta alkaen järjestetään tilaisuuksia, joista tiedotetaan myös tällä sivulla.

- Kybermittarin käyttöohje (pdf, 1,48 Mt)
- Cybermätaren Bruksanvisning (pdf, 2,31 Mt)
- Arviointityökalu (suomi, ruotsi, englanti) (xlsx, 524,27 Kt)
- Käyttöehdot (pdf, 94,69 Kt)
- Tutustu myös: Kyberturvallisuus ja yrityksen hallituksen vastuu -opas
- Kyberturva-webinaari

Tapahtumakalenteri

Päivämäärä	Tapahtuma	
27.10.2020	Kybermittarin julkaisu	Kyberturva-webinaari
10.11.2020	Kybermittarin esittely ja Q&A	14.30 - 16 Esittelyn osu
11.11.2020	Kybermittarin esittely ja Q&A	14.00-15.30 Esittelyn c

Yhteystiedot ja turvallinen viestintä

- Kysymykset ja palaute: kybermittari@traficom.fi
  - Halutessasi voit lähettää palvelullamme salatun viestin osoitteeseen kybermittari@traficom.fi
  - https://www.traficom.fi/fi/traficom/yhteystiedot/salatun-viestin-lahettaminen-traficomiin

- Tulosten lähettäminen ja vertailutietojen vastaanottaminen
  1. Ilmoittaudu ja sovi tietojen vaihdosta Kyberturvallisuuskeskuksen kanssa, joko Kybermittarin osoitteen (kyberbittari@traficom.fi) tai yhteistyöverkostosi kautta
  2. Sovi Kyberturvallisuuskeskuksen kanssa tietojenvaihtokanavasta (esim. Traficom turvaposti tai muu vastaava suojattu palvelu)
  3. Kyberturvallisuuskeskus lähettää tarkemmat ohjeet tulosten ja vertailutietojen käsittelystä.

HUOM! Käytä aina salattua sähköpostia tulosten lähettämiseen Kyberturvallisuuskeskukselle!

Esimerkkejä julkaisuista, jotka sopivat tyypillisiin, tunnistettuihin kehityskohteisiin

Kybermittarin arviointimalli

Kybermittarin rakenne ja laskentamalli

Kybermittarin taustalla olevat viitekehykset

Kybermaturiteetin mittaminen

- Kybermittarin 10 osiota ja osioiden käytännöt perustuvat C2M2-malliin
- Lisäksi kehitetty kriittisten palveluiden suojaamisen osio
- Tulokset on ristiin kytketty soveltuvin osin NIST-malliin ja tulokset voidaan täten raportoida myös NIST CSF-mallin kyvykkyyksien näkökulmasta

Muut osa-alueet

- Investointi- ja kustannustietojen keräys siten että ne voidaan yhdistää muuhun dataan

NIST- ja C2M2-dimensiot

Tärkeimmät käsitteet

- **Kyvykkyys** tarkoittaa kykyä toimia tarkoituksenmukaisella tavalla tietyllä osa-alueella ja hyödyntää osaamistaan sekä resurssejaan, jotta tavoitteet saavutettaisiin.

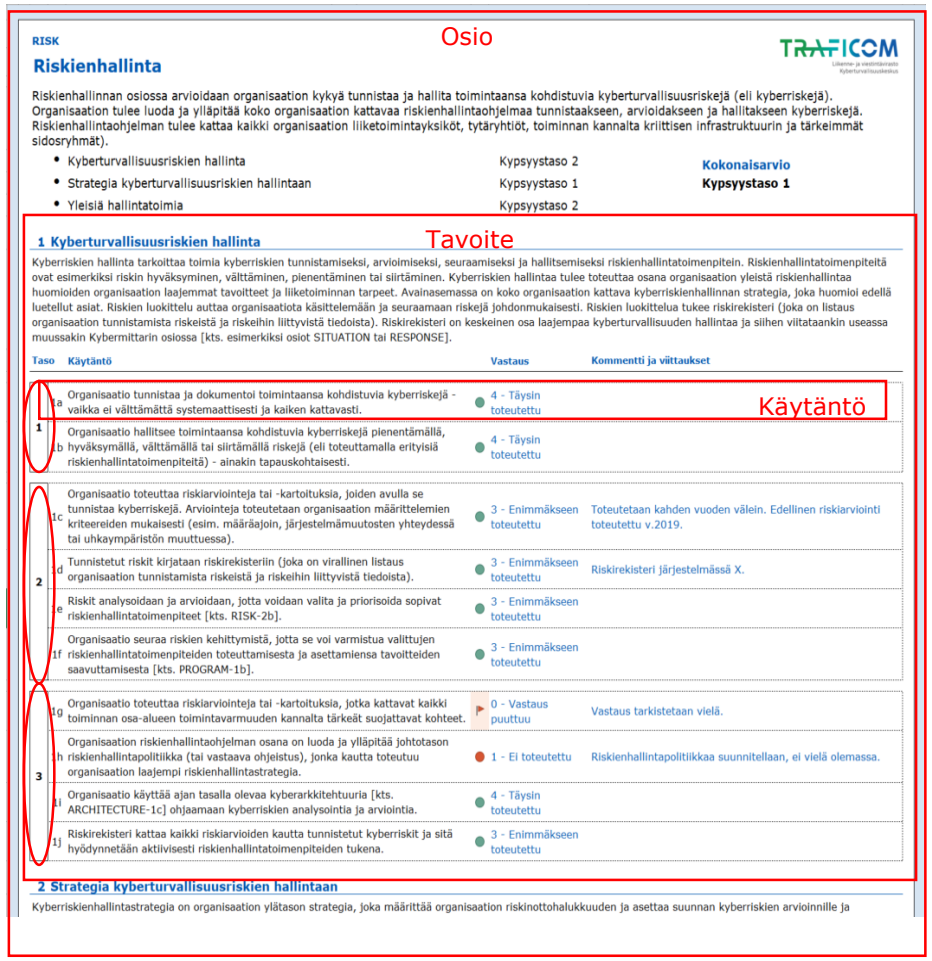
- **Kypsyysmalli** tarkoittaa mallia, jossa toimintaa tarkastellaan tasoina tai askelmina, joita kiivetään ylöspäin kohti järjestelmällisempää ja kehittyneempää toimintaa.

- **Toiminnan osa-alue** on Kybermittarin yhteydessä käytetty käsite, jolla tarkoitetaan niitä organisaation tai yhteiskunnan kannalta kriittisiä palveluita tai toimintoja, joiden kyberturvallisuutta arvioinnissa tarkastellaan.

Kybermittarin kypsyystasot

- **Taso 0** – Organisaatio ei toteuta kyberturvallisuuden hallintaan liittyviä käytäntöjä
- **Taso 1** – Organisaatio toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä
- **Taso 2** – Organisaatiolla dokumentoidut säännöllisesti toistettavat ja ylläpidettävät kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet kyberturvallisuuden toteuttamiseksi on määritetty.
- **Taso 3** – Organisaatio toteuttaa kyberturvallisuutta riskilähtöisesti, koko organisaation kattavia toimintamalleja ylläpidetään jatkuvasti ja kyberturvallisuudelle on määritetty tavoitteet, joita mitataan säännöllisesti.

Kybermittarin rakenne



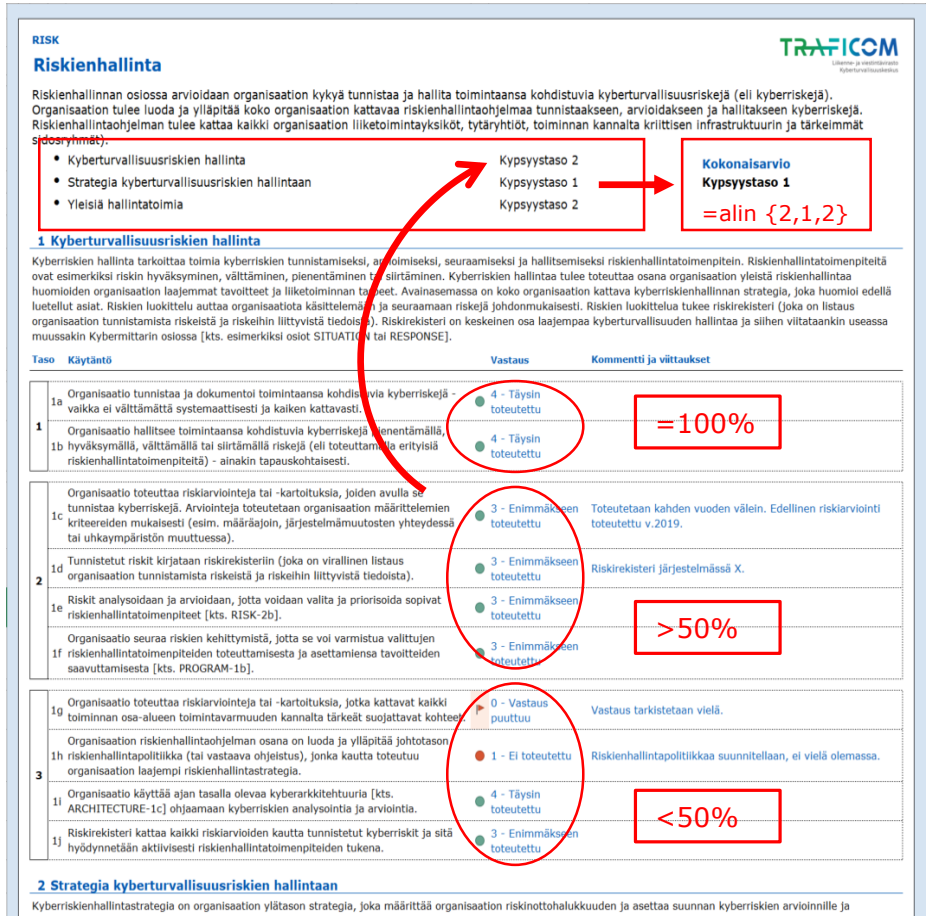
- Kybermittari koostuu
  - **Osioista** (yhteensä 11)
  - **Tavoitteista**, joita on asetettu jokaiselle osiolle (yhteensä 52)
  - **Käytännöistä**, joiden avulla mitataan tavoitteiden täyttymistä (yhteensä 325)
- Käytännöt edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuuden menettelytapoja
  - Käytännöt on järjestetty tavoitteiden mukaisesti – nousevaan kypsyysjärjestykseen

Käytännöt – arviointiasteikko

- Käytäntöjen toteutumisen arvioidaan seuraavasti:
  1. **Ei toteutettu** - organisaatio ei toteuta kuvattuja käytäntöjä
  2. **Osittain toteutettu** - organisaatio on vasta alussa kuvattujen käytäntöjen toteuttamisessa tai toiminta on käytännön osalta muuten puutteellista
  3. **Enimmäkseen toteutettu** - organisaatio toteuttaa kuvattuja käytäntöjä ainakin pääosin, vaikka kehitystyö saattaa olla vielä osittain kesken
  4. **Täysin toteutettu** - organisaatio toteuttaa kuvattuja käytäntöjä, eikä merkittäviä kehitystoimenpiteitä tarvita

- Kypsyystason laskentaa varten vaihtoehdot typistetään seuraavasti:
  - **Toteutettua** vastaavat 4) Täysin toteutetu ja 3) Enimmäkseen toteutettu
  - **Ei Toteutettua** vastaavat 2) Osittain toteuttetu ja 1) Ei toteutettu

Kybermittarin laskentamalli



- Kypsyystaso lasketaan kolmessa vaiheessa:
  1. **Käytännöt** arvioidaan joko Toteutuneeksi tai Ei toteutuneeksi:
  2. **Tavoitteen kypsyystaso** lasketaan toteutuneiden käytäntöjen (%) perusteella; ja
  3. **Osion kypsyystaso** määritetään osion heikoimman tavoitteen kypsyystason mukaisesti.

- Lopputuloksena muodostuu jokaisen yhdentoista osion kypsyystaso asteikolla 0-3
  - Taso perustuu toteutettuihin käytäntöihin ja saavutettuihin tavoitteisiin
  - Jokaisen osion kypsyystaso on sama kuin heikoimman tavoitteen kypsyystaso

Tavoitteet ja osiot – kypsyystaso

- Osioiden ja tavoitteiden kypsyystason laskennassa käytetään seuraavia sääntöjä:
  - **Taso 0:** tason 1 käytännöt eivät toteudu kokonaan
  - **Taso 1:** tulee toteuttaa kaikki (100%) kyseisen tason käytännöistä
  - **Taso 2:** tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä ja kaikki (100%) tason 1 käytännöt
  - **Taso 3:** tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä ja kaikki (100%) tason 2 ja kaikki (100%) tason 1 käytännöt.

Jokaisen osion ja tavoitteen kypsyystaso on sama kuin
heikoimman tavoitteen kypsyystaso

- *Tämä poikkeaa C2M2-mallin käyttämästä laskentamallista, jossa tulee saavuttaa kaikki sekä kyseisen tason että kaikkien alempien tasojen käytänteistä

Kybermittarin arviointiprosessi

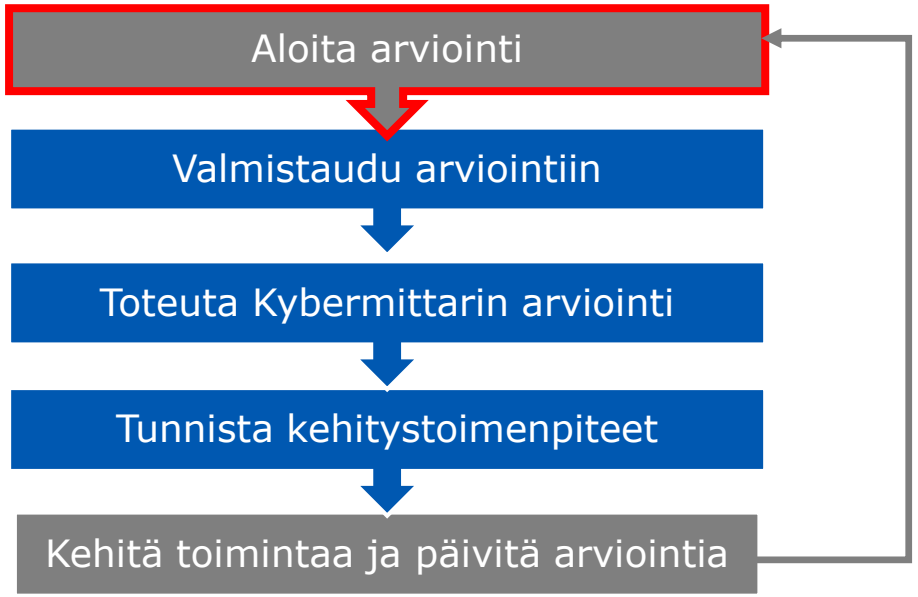
Kybermittarin hyödyntämiseen

Kybermittarin arviointiprosessi

- Kybermittaria suositellaan käytettäväksi osana viisivaiheista arviointiprosessia
- Prosessi on laadittu Kybermittarin pilottikartoituksista saatujen kokemusten perusteella
- Paras hyöty mittarista saadaan, kun se tuodaan osaksi toiminnan jatkuvaa kehittämistä

Aloita arviointi

Aloita arviointi



- **Osallistujat:**
  - Organisaation johtoryhmä tai muu päätöksentekoelin.
- **Tehtävä:**
  - Päättää arvioinnin toteuttamisesta ja arvioinnin kohteesta; ja
  - Nimittää arvioinnille sponsori ja vetäjä, jotka vastaavat jatkotoimenpiteistä.

Päätös arvioinnin toteuttamisesta ja kohteesta

- Tärkein päätös liittyy arvioitavan toiminnan osa-alueen valintaan
- Toiminnan osa-alueella tarkoitetaan niitä organisaation tai yhteiskunnan kannalta kriittisiä palveluita tai toimintoja, joiden kyberturvallisuutta arvioinnissa tarkastellaan.
- Mikäli halutaan arvioida useita erillisiä toiminnan osa-alueita, suositus on käynnistää jokaisesta oma arviointinsa

Sponsori ja vetäjä seuraavia vaiheita varten

- Arviointia varten tulee nimetä vähintään arvioinnin sponsori ja vetäjä

Arvioinnin sponsori

Johtoryhmän jäsen tai muu toimihenkilö, joka vastaa arvioinnin tuesta ja johdon sitouttamisesta kyberturvallisuuden arviointiin ja jatkuvaan kehittämiseen

Arvioinnin vetäjä

Organisaation oma tai ulkopuolisen palvelun-tarjoajan edustaja, joka vastaa arvioinnin käytännön toteutuksesta

Valmistaudu arviointiin

Valmistaudu arviointiin

- **Osallistujat:**
  - Arvioinnin sponsori ja vetäjä yhdessä.
- **Tehtävä:**
  - Rajata tarkemmin arvioitavana oleva toiminnan osa-alue ja tunnistaa osa-alueen kriittiset riippuvuudet;
  - Tunnistaa arviointiin tarvittavat asiantuntijat; ja
  - Sopia arviointitavasta ja arvioinnin aikataulusta.

Toiminnan osa-alueen rajaaminen

- Arviointia varten tulee tunnistaa ja rajat arvioitava toiminnan osa-alue
- Arviointi suositellaan kohdistamaan toimintoihin, joita organisaatio tarvitsee tuottaakseen joko
  - Yhteiskunnan kannalta kriittistä palvelua; tai
  - Organisaation oman liiketoiminnan kannalta kriittistä palvelua.
- Lisäksi rajaus voidaan toteuttaa esimerkiksi:
  - Kattamaan koko organisaatio, esim. pienissä ja keskisuurissa yrityksissä
  - Organisaatiorakenteen mukaisesti, esim. maa- tai liiketoimintayksikköön

Yhteiskunnan kannalta kriittiset palvelut

- Palvelu on yhteiskunnalle kriittinen, mikäli sen häiriö vaikuttaa merkittävään asiakasmäärään, laajaan maantieteelliseen alueeseen tai palvelun häiriöllä on vakavia seurannaisvaikutuksia.
- Organisaation yhteiskunnallista vaikutusta arvioitaessa Kybermittarin arviointityökalussa tarkastellaan seuraavia systeemisen vaikuttavuuden kriteereitä:

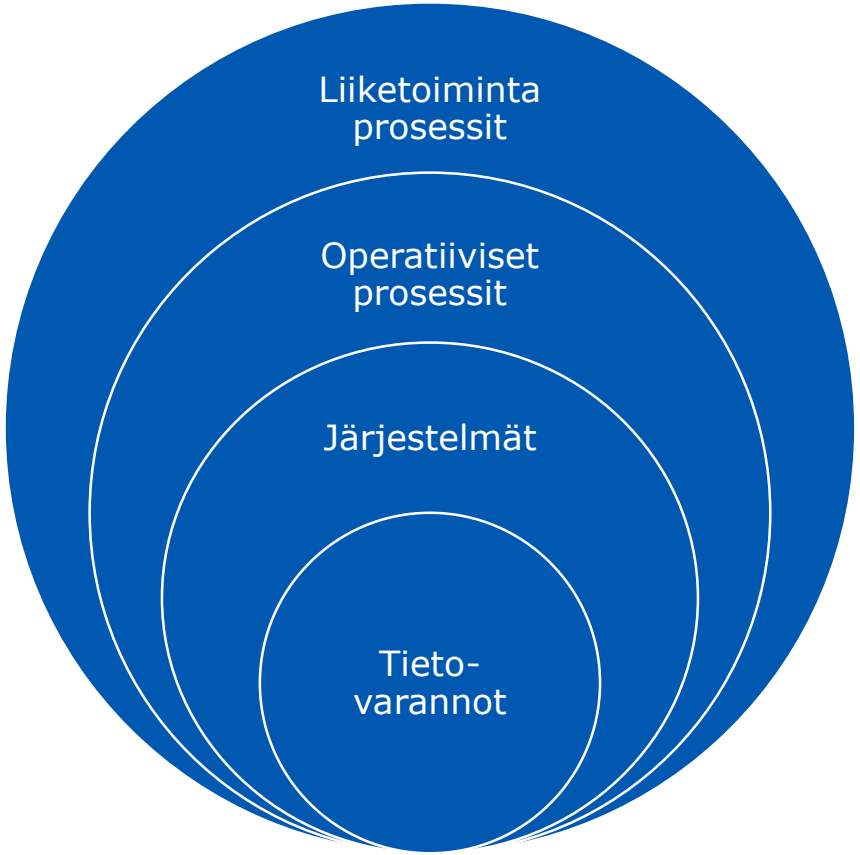
1. Vähäinen systeeminen vaikutus	2. Huomattava systeeminen vaikutus	3. Rampauttava systeeminen vaikutus
Vaikutus kohdistuu vain organisaatioon itseensä tai vain vähäiseen määrään partnereita ja/tai asiakasorganisaatioita, tai vaikutus rajautuu alle 50000 kansalaiseen.	Toiminta vaikeutuu huomattavalle määrälle partnereita ja/tai asiakasorganisaatioita tai yli 50000 kansalaisen elämä vaikeutuu tai he kärsivät vahinkoja.	Rampauttaa yhteiskunnan perustoimintoja tai aiheuttaa vahinkoa yli 100000 kansalaiselle.

Kriittisten riippuvuuksien tunnistaminen

- Kriittisten palveluiden lisäksi arvioinnin kohteen määrittämiseksi tulee tunnistaa näiden tärkeimmät riippuvuudet

- Kriittisiä riippuvuuksia ovat:
  - Liiketoimintaprosessit ja operatiiviset prosessit;
  - Järjestelmät ja osajärjestelmät; ja
  - Tietovarannot

Palvelun toimittaminen riippuu useista tekijöistä



- Arvoinnin piiriin kuuluvat ne prosessit, jotka tarvitaan palvelun tuotantoon
- Palvelun tuottamiseen liittyvä suojattava omaisuus koostuu etenkin järjestelmistä ja ohjelmistoista, voi kuitenkin kattaa myös fyysisiä kohteita
- Kriittinen tieto-omaisuus on kaikki ne järjestelmien perustiedot ja -arvot sekä liiketoimintakriittiset tiedot, jotka takavaat palvelun häiriöttömän toimittamisen loppuasiakkaalle

Kriittiset järjestelmät, osajärjestelmät, laitteet, ohjelmistot ja tieto-omaisuus

- Tunnista palvelun toimittamisen kannalta keskeinen suojattava omaisuus
  - Suojatta omaisuus voi olla tuotantolaite kuten lypsykone tai generaattori tai se voi olla fyysinen tila kuten tuotantolaitoksen valvomo tai kaupan alalla kassajärjestelmä
  - Suojattavaan omaisuuteen liittyy erilaista suojattavaa tietoa, jonka eheys, luottamuksellisuus ja saatavuus ovat edellytyksiä häiriöttömälle palvelun tuotannolle.

- Tunnista palvelun toimittamisen kannalta keskeinen suojattava tieto-omaisuus
  - Laitteiden ja prosessien toiminta perustuu määritettyihin asetuksiin ja arvoihin, nämä muodostavat osaltaan yhden suojattavan tieto-omaisuuden kokonaisuuden
  - Yrityksellä on näiden lisäksi tärkeitä tietovarantoja kuten tietokannat asiakkaista, toimittajista ja omasta henkilöstöstä

Lähestymistapoja kriittisyyden hahmottamiseen omassa toiminnassa

- Toimialakohtainen määrittely yhteiskunnallisesti kriittisestä palvelusta - Huoltovarmuuskeskuksen määritelmät eri toimialoille https://www.huoltovarmuuskeskus.fi/toimialat/
- Ei kriittisen toiminnan tunnistaminen ja pois sulkeminen – mistä palveluista tai prosesseista organisaatiosi voi luopua ja silti pystyy tuottamaan yhteiskunnalle kriittisen palvelun?
- Riippuvuuksien tunnistaminen toimitusketjussa – mikä on organisaatiosi rooli ja asema suhteessa toimittajiin? Millainen on toimitusketju organisaatiosta eteenpäin, oletko osa kriittisen toimijan toimitusketjua?
- Hankintasopimuksien vaatimukset organisaatiollesi – Voidaanko tätä kautta tunnistaa huoltovarmuuskriittiset kumppanit ja asiakkaat?

Arviointiin tarvittavat asiantuntijat

- Arviointia sponsorin ja vetäjän lisäksi tulee nimietä arviointiin osallistuvat asiantuntijat ja tulevien kehityssuunnitelmien omistajat

Arvioinnin sponsori

Johtoryhmän jäsen tai muu toimihenkilö, joka vastaa arvioinnin tuesta ja johdon sitouttamisesta kyberturvallisuuden arviointiin ja jatkuvaan kehittämiseen

Arvioinnin vetäjä

Organisaation oma tai ulkopuolisen palvelun-tarjoajan edustaja, joka vastaa arvioinnin käytännön toteutuksesta

Arvioinnin asiantuntijat

Asiantuntijat, jotka tuovat osaamista organisaation eri osa-alueilta mm. liiketoiminnan, kyberturvallisuuden tai riskien- ja henkilöstönhallinnon aloilta

Kehityssuunnitelman omistajat

Arvioinnin jälkeisen kyberturvallisuuden kehittämisen mahdollistaja ja koordinaattori

Kybermittarin aihealueiden keskeiset roolit

Kybermittarin osio	Keskeiset roolit
CRITICAL Kriittisten palveluiden suojaaminen	Riskienhallintapäällikkö, tietoturvajohtaja ja -päällikkö, sekä liiketoiminnan edustajat yhdessä
RISK Riskienhallinta	Riskienhallintapäällikkö, tietoturvajohtaja ja -päällikkö
ASSET Suojattavien kohteiden, muutosten ja konfiguraatioiden hallinta	Tietoturva- ja tietohallintojohtaja yhdessä (*OT omaisuus: lisäksi asiasta vastaavat liiketoiminnan edustajat)
PROGRAM Kyberturvallisuuden kehitysohjelman hallinta	Tietoturvajohtaja/päällikkö tai muu kyberturvallisuudesta organisaatiossa vastaava henkilö
DEPENDENCIES Toimitusketjun ja ulkoisten riippuvuuksien hallinta	Hankintapäällikkö, riskienhallintapäällikkö, Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä

Kybermittarin osio	Keskeiset roolit
ACCESS Käyttövaltuuksien ja pääsynhallinta	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
RESPONSE Tapahtumien ja poikkeamien hallinta	Tietoturvajohtaja/päällikkö, tietohallintojohtaja ja riskienhallintapäällikkö yhteisesti sekä asiaa hoitavat liiketoiminnan edustajat
ARCHITECTURE Kyberturvallisuus-arkkitehtuuri	Tietoturvajohtaja/päällikkö yhdessä relevanttien arkkitehtien kanssa
SITUATION Tilannekuva	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
THREAT Uhkien ja haavoittuvuuksien hallinta	Tietoturvajohtaja ja -päällikkö yhteisesti, sekä asiaa hoitavat liiketoiminnan edustajat
WORKFORCE Henkilöstöhallinta	Tietoturvajohtaja yhteistyössä henkilöstöjohtajan kanssa

Arvioinnin toteutustapa

- Arvioinnin vetäjä auttaa organisaatiota valitsemaan sopivimman toteutustavan
- Suositeltuja toteutustapoja ovat joko
  - Ohjattu työpajamuotoinen toimintamalli; tai
  - Henkilövetoinen arviointi
- Toteutustavasta riippuen vetäjä huolehtii joko työpajan käytännön järjestelyistä tai koordinoi muutoin arvioinnin toteuttamisen asiantuntijoiden kanssa

Ohjattu työpajamuotoinen toimintamalli

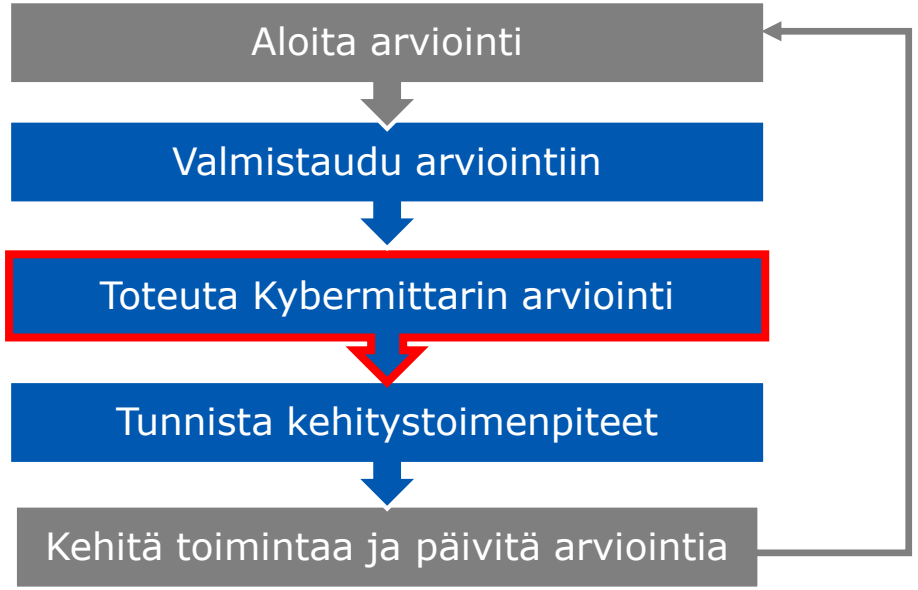
- Vaiheet, joiden koordinoinnista arvioinnin vetäjä vastaa (mahdollisesti yhdessä arvioinnin sponsorin ja organisaation asiantuntijoiden kanssa), ovat:
  1. Asiantuntijoiden nimeäminen ja sitouttaminen työpajaan;
  2. Aloituskokous (1 h) tai -viesti arviointiin osallistuville henkilöille;
  3. Yksi tai useampi työpaja (voidaan toteuttaa myös sarjana työpajoja pienryhmissä, esim. 2-3 h/työpaja)
  4. Tulosten kerääminen yhteen ja analysointi viimeistä työpajaa varten;
  5. Tulosten läpikäynti, kehityskohteiden tunnistaminen sekä kehitystoimista vastaavien henkilöiden nimeäminen lopputyöpajassa (2 h)

Henkilövetoinen arviointi

- Vaiheet, joiden koordinoinnista arvioinnin vetäjä vastaa, ovat:
  1. Asiantuntijoiden nimeäminen ja sitouttaminen työpajaan;
  2. Aloituskokous (1-2 h) arviointiin osallistuville henkilöille
  3. Nimetyt asiantuntijat täyttävät itsenäisesti Kybermittarin heille osoitetut aihealueet sovitun aikataulun mukaisesti
  4. Tulosten kerääminen yhteen ja analysointi työpajaa varten
  5. Tulosten läpikäynti lopputyöpajassa (2-4 h), johon osallistuvat kaikki arvioinnin täyttämiseen osallistuneet henkilöt

Toteuta arviointi

Toteuta Kybermittarin arviointi

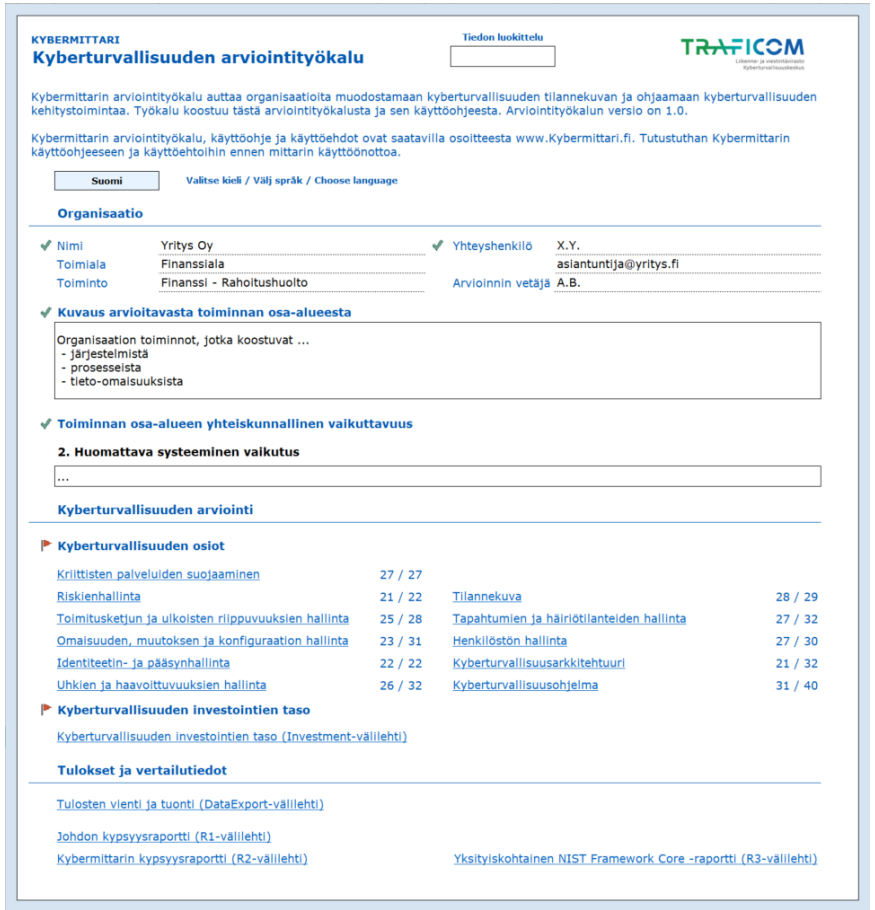


- **Osallistujat:**
  - Arvioinnin vetäjä, arvioinnin sponsori ja organisaation asiantuntijat.
- **Tehtävä:**
  - Toteuttaa arviointi valitulla arviointitavalla Kybermittari-työkalun avulla.

Kybermittarin osiot

CRITICAL – Kriittisten palveluiden suojaaminen
RISK - Riskienhallinta
DEPENDENCIES– Toimitusketjun ja ulkoisten riippuvuuksien hallinta
ASSET – Omaisuuden, muutoksen ja konfiguraation hallinta
ACCESS – Identiteetin- ja pääsynhallinta
THREAT – Uhkien ja haavoittuvuuksien hallinta
SITUATION - Tilannekuva
RESPONSE – Tapahtumien ja häiriötilanteiden hallinta
WORKFORCE – Henkilöstön hallinta
ARCHITECTURE - Kyberturvallisuusarkkitehtuuri
PROGRAM - Kyberturvallisuusohjelma

Yhteenveto – Kybermittari-välilehti



KYBERMITTARI
Kyberturvallisuuden arviointityökalu

Tiedon luokittelu

Kybermittarin arviointityökalu auttaa organisaatioita muodostamaan kyberturvallisuuden tilannekuvan ja ohjaamaan kyberturvallisuuden kehitystoimintaa. Työkalu koostuu tästä arviointityökalusta ja sen käyttöohjeesta. Arviointityökalun versio on 1.0.

Kybermittarin arviointityökalu, käyttöohje ja käyttöehdot ovat saatavilla osoitteesta www.Kybermittari.fi. Tutustuthan Kybermittarin käyttöohjeeseen ja käyttöehtoihin ennen mittarin käyttöönottoa.

Suomi — Valitse kieli / Välj språk / Choose language

Organisaatio

Nimi: Yritys Oy
Toimiala: Finanssiala
Toiminto: Finanssi - Rahoitushuolto
Yhteyshenkilö: X.Y.
asiantuntija@yritys.fi
Arvioinnin vetäjä: A.B.

Kuvaus arvioitavasta toiminnan osa-alueesta

Organisaation toiminnot, jotka koostuvat ...
- järjestelmistä
- prosesseista
- tieto-omaisuuksista

Toiminnan osa-alueen yhteiskunnallinen vaikuttavuus

2. Huomattava systeeminen vaikutus

...

Kyberturvallisuuden arviointi

Kyberturvallisuuden osiot

Kriittisten palveluiden suojaaminen	27 / 27		
Riskienhallinta	21 / 22	Tilannekuva	28 / 29
Toimitusketjun ja ulkoisten riippuvuuksien hallinta	25 / 28	Tapahtumien ja häiriötilanteiden hallinta	27 / 32
Omaisuuden, muutoksen ja konfiguraation hallinta	23 / 31	Henkilöstön hallinta	27 / 30
Identiteetin- ja pääsynhallinta	22 / 22	Kyberturvallisuusarkkitehtuuri	21 / 32
Uhkien ja haavoittuvuuksien hallinta	26 / 32	Kyberturvallisuusohjelma	31 / 40

Kyberturvallisuuden investointien taso

Kyberturvallisuuden investointien taso (Investment-välilehti)

Tulokset ja vertailutiedot

Tulosten vienti ja tuonti (DataExport-välilehti)

Johdon kypsyysraportti (R1-välilehti)
Kybermittarin kypsyysraportti (R2-välilehti)
Yksityiskohtainen NIST Framework Core -raportti (R3-välilehti)

- Työkalun kielivalinta (suomi, ruotsi tai englanti);
- Tiedon luokittelu organisaation määrittelemänä;
- Organisaatio ja toiminnan osa-alue; ja
- Kyberturvallisuuden arviointi, tulokset ja vertailutiedot.

Osiokohtaiset välilehdet

RISK

Riskienhallinta

TRAFICOM

Riskienhallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimintaansa kohdistuvia kyberturvallisuusriskejä (eli kyberriskejä). Organisaation tulee luoda ja ylläpitää koko organisaation kattavaa riskienhallintaohjelmaa tunnistaakseen, arvioidakseen ja hallitakseen kyberriskejä. Riskienhallintaohjelman tulee kattaa kaikki organisaation liiketoimintayksiköt, tytäryhtiöt, toiminnan kannalta kriittisen infrastruktuurin ja tärkeimmät sidosryhmät).

- Kyberturvallisuusriskien hallinta — Kypsyystaso 2
- Strategia kyberturvallisuusriskien hallintaan — Kypsyystaso 1
- Yleisiä hallintatoimia — Kypsyystaso 2

Kokonaisarvio
Kypsyystaso 1

1 Kyberturvallisuusriskien hallinta

Kyberriskien hallinta tarkoittaa toimia kyberriskien tunnistamiseksi, arvioimiseksi, seuraamiseksi ja hallitsemiseksi riskienhallintatoimenpitein. Riskienhallintatoimenpiteitä ovat esimerkiksi riskin hyväksyminen, välttäminen, pienentäminen tai siirtäminen. Kyberriskien hallintaa tulee toteuttaa osana organisaation yleistä riskienhallintaa huomioiden organisaation laajemmat tavoitteet ja liiketoiminnan tarpeet. Avainasemassa on koko organisaation kattava kyberriskienhallinnan strategia, joka huomioi edellä luetellut asiat. Riskien luokittelu auttaa organisaatiota käsittelemään ja seuraamaan riskejä johdonmukaisesti. Riskien luokittelua tukee riskirekisteri (joka on listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista). Riskirekisteri on keskeinen osa laajempaa kyberturvallisuuden hallintaa ja siihen viitataankin useassa muussakin Kybermittarin osiossa [kts. esimerkiksi osiot SITUATION tai RESPONSE].

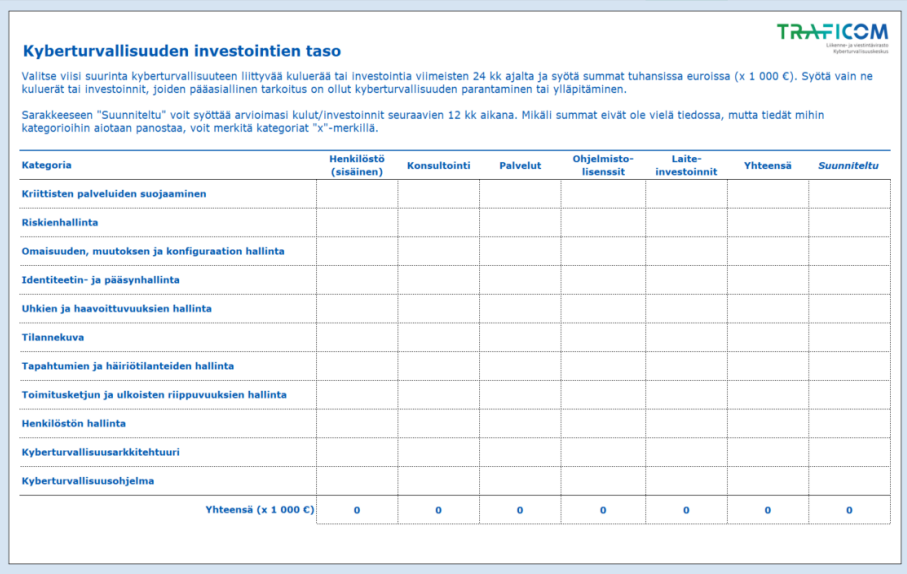
Taso		Käytäntö	Vastaus	Kommentti ja viittaukset
1	1a	Organisaatio tunnistaa ja dokumentoi toimintaansa kohdistuvia kyberriskejä - vaikka ei välttämättä systemaattisesti ja kaiken kattavasti.	4 - Täysin toteutettu	
	1b	Organisaatio hallitsee toimintaansa kohdistuvia kyberriskejä pienentämällä, hyväksymällä, välttämällä tai siirtämällä riskejä (eli toteuttamalla erityisiä riskienhallintatoimenpiteitä) - ainakin tapauskohtaisesti.	4 - Täysin toteutettu	
2	1c	Organisaatio toteuttaa riskiarviointeja tai -kartoituksia, joiden avulla se tunnistaa kyberriskejä. Arviointeja toteutetaan organisaation määrittelemien kriteereiden mukaisesti (esim. määräajoin, järjestelmämuutosten yhteydessä tai uhkaympäristön muuttuessa).	3 - Enimmäkseen toteutettu	Toteutetaan kahden vuoden välein. Edellinen riskiarviointi toteutettu v.2019.
	1d	Tunnistetut riskit kirjataan riskirekisteriin (joka on virallinen listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista).	3 - Enimmäkseen toteutettu	Riskirekisteri järjestelmässä X.
	1e	Riskit analysoidaan ja arvioidaan, jotta voidaan valita ja priorisoida sopivat riskienhallintatoimenpiteet [kts. RISK-2b].	3 - Enimmäkseen toteutettu	
	1f	Organisaatio seuraa riskien kehittymistä, jotta se voi varmistua valittujen riskienhallintatoimenpiteiden toteuttamisesta ja asettamiensa tavoitteiden saavuttamisesta [kts. PROGRAM-1b].	3 - Enimmäkseen toteutettu	
3	1g	Organisaatio toteuttaa riskiarviointeja tai -kartoituksia, jotka kattavat kaikki toiminnan osa-alueen toimintavarmuuden kannalta tärkeät suojattavat kohteet.	0 - Vastaus puuttuu	Vastaus tarkistetaan vielä.
	1h	Organisaation riskienhallintaohjelman osana on luoda ja ylläpitää johtotason riskienhallintapolitiikka (tai vastaava ohjeistus), jonka kautta toteutuu organisaation laajempi riskienhallintastrategia.	1 - Ei toteutettu	Riskienhallintapolitiikkaa suunnitellaan, ei vielä olemassa.
	1i	Organisaatio käyttää ajan tasalla olevaa kyberarkkitehtuuria [kts. ARCHITECTURE-1c] ohjaamaan kyberriskien analysointia ja arviointia.	4 - Täysin toteutettu	
	1j	Riskirekisteri kattaa kaikki riskiarvioiden kautta tunnistetut kyberriskit ja sitä hyödynnetään aktiivisesti riskienhallintatoimenpiteiden tukena.	3 - Enimmäkseen toteutettu	

2 Strategia kyberturvallisuusriskien hallintaan

Kyberriskienhallintastrategia on organisaation ylätason strategia, joka määrittää organisaation riskinottohalukkuuden ja asettaa suunnan kyberriskien arvioinnille ja

- Osion nimen, esittelyn ja yhteenvedon osiolle asetetuista tavoitteista;
- Jokaista tavoitetta kohden nimi, esittely sekä asetetut käytännöt; ja
- Jokaista käytäntöä kohden (vasemmalta oikealle):
  - Kypsyystaso, käytännön tunniste ja kuvaus;
  - Vastausvaihtoehto 1-4 (monivalinta); ja
  - Tilaa kommenteille ja viittauksille (vapaa tekstikenttä).

Kyberturvallisuuden investoinnit -välilehdet



Kyberturvallisuuden investointien taso

Valitse viisi suurinta kyberturvallisuuteen liittyvää kuluerää tai investointia viimeisten 24 kk ajalta ja syötä summat tuhansissa euroissa (x 1 000 €). Syötä vain ne kuluerät tai investoinnit, joiden pääasiallinen tarkoitus on ollut kyberturvallisuuden parantaminen tai ylläpitäminen.

Sarakkeeseen "Suunniteltu" voit syöttää arvioimasi kulut/investoinnit seuraavien 12 kk aikana. Mikäli summat eivät ole vielä tiedossa, mutta tiedät mihin kategorioihin aiotaan panostaa, voit merkitä kategoriat "x"-merkillä.

Kategoria	Henkilöstö (sisäinen)	Konsultointi	Palvelut	Ohjelmisto-lisenssit	Laite-investoinnit	Yhteensä	*Suunniteltu*
Kriittisten palveluiden suojaaminen							
Riskienhallinta							
Omaisuuden, muutoksen ja konfiguraation hallinta							
Identiteetin- ja pääsynhallinta							
Uhkien ja haavoittuvuuksien hallinta							
Tilannekuva							
Tapahtumien ja häiriötilanteiden hallinta							
Toimitusketjun ja ulkoisten riippuvuuksien hallinta							
Henkilöstön hallinta							
Kyberturvallisuusarkkitehtuuri							
Kyberturvallisuusohjelma							
Yhteensä (x 1 000 €)	0	0	0	0	0	0	0

- Tarkoituksena arvioida ja kategorisoida kyberturvallisuuteen käytettävien investointien ja kustannusten suuruutta
- Investointien tarkastelujakso on viimeiset 24 kk
- Tarkastelu suositellaan rajaamaan esimerkiksi 5-10 suurimpaan kuluerään
- Suunnitelluista menoista kirjataan tulevien 12 kk aikana odotetut investoinnit ja kulut

CRITICAL Kriittisten palveluiden suojaaminen

Organisaation tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja hallita riskejä sen mukaisesti.

Tavoitteet:

- Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
- Kriittisten palveluiden hallinta
- Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

Huom. tähän osioon ei kuulu Yleisiä hallintatoimia, eikä osio perustu C2M2-malliin.

RISK Riskienhallinta

Riskienhallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimintaansa kohdistuvia kyberturvallisuusriskejä (eli kyberriskejä). Organisaation tulee luoda ja ylläpitää koko organisaation kattavaa riskienhallintaohjelmaa tunnistaakseen, arvioidakseen ja hallitakseen kyberriskejä.

Riskienhallintaohjelman tulee kattaa kaikki organisaation liiketoimintayksiköt, tytäryhtiöt, toiminnan kannalta kriittisen infrastruktuurin ja tärkeimmät sidosryhmät).

Tavoitteet:

- Kyberturvallisuusriskien hallinta
- Strategia kyberturvallisuusriskien hallintaan
- Yleisiä hallintatoimia

DEPENDENCIES
Toimitusketjun ja ulkoisten riippuvuuksien hallinta

Toimitusketjun ja ulkoisten riippuvuuksien hallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä.

Organisaation tulee määritellä ja ylläpitää kontrolleja, joiden avulla se hallitsee organisaation ulkopuolisista toimijoista riippuvaisten yhteiskunnalle kriittisten palveluiden kyberriskejä.

Tavoitteet

- Riippuvuuksien tunnistaminen
- Riippuvuusriskien hallinta
- Yleisiä hallintatoimia

ASSET
Omaisuuden, muutoksen ja konfiguraation hallinta

Omaisuuden, muutoksen ja konfiguraation hallinnan osiossa arvioidaan organisaation kykyä hallita toiminnan osa-alueen toimintavarmuuden kannalta tärkeää omaisuutta ja tähän omaisuuteen liittyviä muutoksia ja konfiguraatioita.

Omaisuudella tarkoitetaan organisaation IT- ja OT-omaisuutta (mkl. laitteet ja ohjelmistot) sekä tietovarantoja. Organisaation tulee hallinnoida tätä omaisuutta suhteessa sekä omaisuuteen kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- IT- ja OT-omaisuuden rekisterin hallinta
- Tietovarantojen rekisterin hallinta
- Suojattavan omaisuuden konfiguraation hallinta
- Suojattavien kohteiden muutoksenhallinta
- Yleisiä hallintatoimia

ACCESS Identiteetin- ja pääsynhallinta

Identiteetin ja pääsynhallinnan osiossa arvioidaan organisaation kykyä hallita ja rajoittaa pääsyä suojattaviin kohteisiin. Organisaation tulee luoda ja ylläpitää identiteettejä toimijoille, joille halutaan myöntää pääsy fyysisesti tai verkon yli organisaation suojattaviin kohteisiin.

Organisaation tulee hallita käyttöoikeuksia suojattaviin kohteisiin suhteessa sekä niihin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- Identiteettien hallinta
- Käyttöoikeuksien hallinta
- Yleisiä hallintatoimia

THREAT Uhkien ja haavoittuvuuksien hallinta

Uhkien ja haavoittuvuuksien hallinnan osiossa arvioidaan organisaation kykyä havaita ja hallita mahdollisia kyberuhkia ja haavoittuvuuksia.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa, joiden avulla havaita, tunnistaa, analysoida, hallita ja vastata kyberuhkiin ja haavoittuvuuksiin. Toimien tulee olla suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- Uhkien tunnistaminen ja hallinta
- Haavoittuvuuksien rajoittaminen
- Yleisiä hallintatoimia

SITUATION Tilannekuva

Tilannekuvan osiossa arvioidaan organisaation kykyä määritellä ja ylläpitää organisaation kyberturvallisuuden tilannekuvaa. Organisaation tulee määritellä ja ylläpitää prosesseja ja teknisiä ratkaisuja operatiivisen ja kyberturvallisuustiedon keräämiseen, analysointiin, hälytysten nostamiseen, esittämiseen ja käyttämiseen, hyödyntäen muissa Kybermittarin osioissa mainittua informaatiota.

Tilannekuva muodostetaan sekä organisaation toiminnan, että kyberturvallisuuden tasosta.

Tavoitteet

- Lokituksen toteuttaminen
- Monitoroinnin toteuttaminen
- Tilannekuvan muodostaminen
- Yleisiä hallintatoimia

RESPONSE Tapahtumien ja häiriötilanteiden hallinta

Tapahtumien ja häiriötilanteiden hallinnan osiossa arvioidaan organisaation kykyä hallita, reagoida ja palautua kybertapahtumista ja -häiriöistä.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa kyberturvallisuuteen liittyvien tapahtumien ja häiriöiden havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- Kybertapahtumien havainnointi
- Kybertapahtumien analysointi ja häiriöksi korottaminen
- Kybertapahtumiin ja -häiriötilanteisiin reagointi
- Yleisiä hallintatoimia

WORKFORCE Henkilöstön hallinta

Henkilöstön hallinnan osiossa arvioidaan organisaation kykyä kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista ja -valmiutta.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja, teknologiaa ja kontrolleja organisaation kyberturvallisuuskulttuurin luomiseksi ja sopivan ja osaavan henkilöstön takaamiseksi, suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- Kyberturvallisuuden vastuiden jakaminen
- Kyberhenkilöstön kehittäminen
- Henkilöstön hallintatoimet
- Kybertietoisuuden lisääminen
- Yleisiä hallintatoimia

ARCHITECTURE Kyberturvallisuusarkkitehtuuri

Kyberturvallisuusarkkitehtuurin osiossa arvioidaan organisaation kykyä hallita ja ylläpitää kyberturvallisuustoimintaansa.

Organisaation tulee luoda ja ylläpitää rakenteita, joilla se hallinnoi ja ohjaa organisaation kyberturvallisuuskontrolleja, -prosesseja ja muiden kyberturvallisuuden osa-alueiden toimintaa suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

- Kyberturvallisuusarkkitehtuuris ja -kehitysohjelma
- Verkkojen segmentointi osana kyberarkkitehtuuria
- Sovellusturvallisuus osana kyberarkkitehtuuria
- Tietojensuojelu osana kyberarkkitehtuuria
- Yleisiä hallintatoimia

PROGRAM Kyberturvallisuusohjelma

Kyberturvallisuusohjelman osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuista kyberturvallisuusohjelmaa.

Kyberturvallisuusohjelman tarkoitus on määritellä kyberturvallisuuden hallintamalli ("governance"), kyberturvallisuuden strateginen kehittäminen ja liiketoimintajohdon tuki kyberturvallisuudelle tavalla, joka on suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin nähden.

Tavoitteet

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Kyberturvallisuus osana jatkuvuussuunnittelua
- Yleisiä hallintatoimia

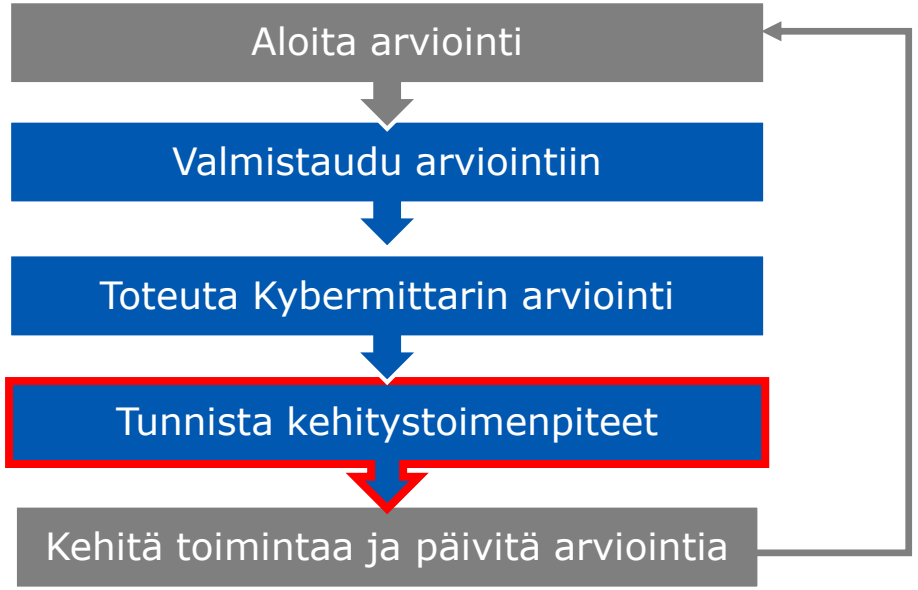
YLEISIÄ HALLINTATOIMIA
Yhteinen tavoite kaikkien osioiden arvioinnissa

- Seuraavat käytännöt arvioidaan erikseen jokaisen osion yhteydessä *(pl. osio CRITICAL)*:
  - a) osioon liittyen on määritetty dokumentoidut käytännöt, joita noudatetaan ja pidetään yllä.
  - B) osion toimintaan on saatavilla riittävät resurssit (henkilöstö, rahoitus ja työkalut).
  - c) osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.
  - d) osion toiminnan suorittamiseen liittyvät vastuut ja valtuudet on osoitettu nimetyille työntekijöille.
  - e) osion toiminta perustuu organisaation määrittämään ja ylläpitämään johtotason politiikkaan (tai vastaavaan ohjeistukseen), jossa asetetaan nimenomaisia vaatimuksia tämän osion toiminnalle.
  - f) osion toiminnalle on määritetty suoriutumistavoitteet, joiden toteutumista seurataan [kts. PROGRAM-1b].
  - g) osioon liittyvät käytännöt on standardoitu läpi koko organisaation ja niitä kehitetään aktiivisesti.

- Mikäli organisaatio noudattaa samoja käytäntöjä läpi koko organisaation tai useammalla kuin yhdellä osa-alueella, voi samoja vastauksia hyödyntää noissa osioissa

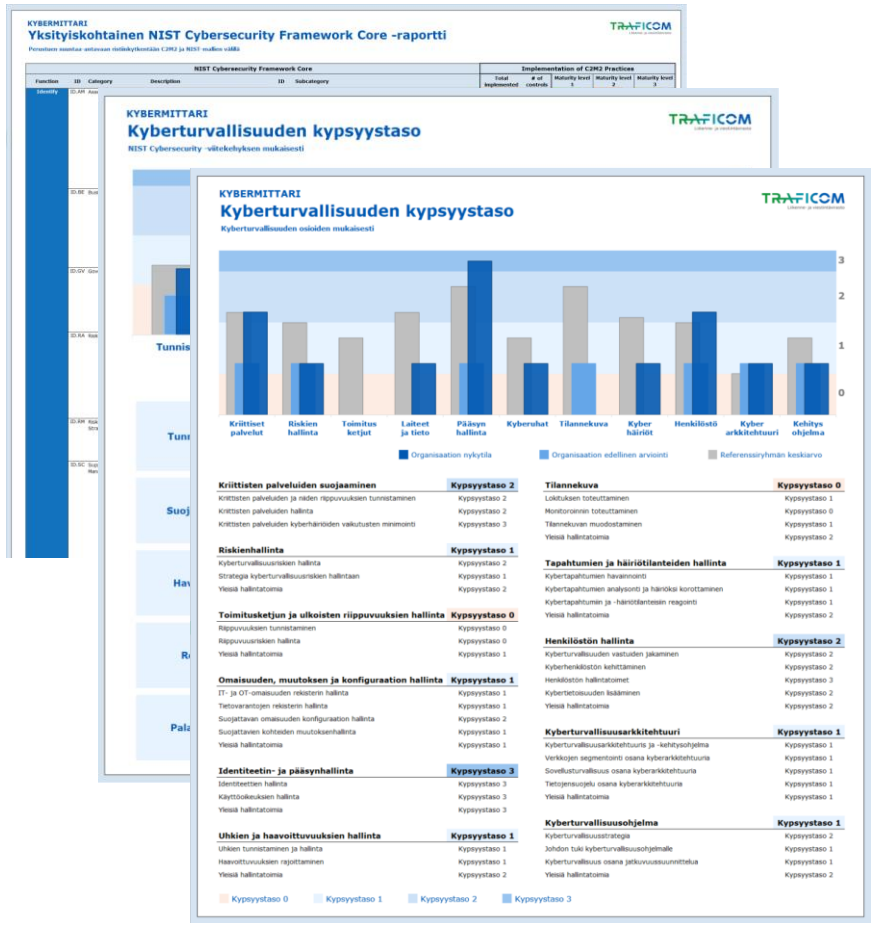
Tunnista kehitystoimenpiteet

Tunnista kehitystoimenpiteet



- **Osallistujat:**
  - Arvioinnin vetäjä, arvioinnin sponsori, organisaation asiantuntijat ja kehityssuunnitelmien omistajat.
- **Tehtävä:**
  - Analysoida arvioinnin tulokset;
  - Määrittää mahdollinen toiminnan tavoitetaso; sekä
  - Tunnistaa ja priorisoida tärkeimmät kehitystoimenpiteet.

Arviointityökalun raportit tulosten analysoinnin ja tavoitetason asettamisen tukena



- Työkalu tuottaa automaattisesti kolme erilaista raporttia kyberturvallisuuden kypsyystasosta
- Raportit ovat
  - Johdolle suunnattu kypsyysraportti
  - Kybermittarin kypsyysraportti
  - Yksityiskohtainen NIST CSF -raportti
- Raportteja on mahdollista rikastaa vertailutiedolla organisaation aiemmasta arvioinnista tai esimerkiksi viiteryhmän keskiarvotuloksilla

Johdolle suunnattu kypsyysraportti

Sisältö	Ylätason yhteenveto Kybermittarin tuloksista. Raportti luo kuvan organisaation kyberturvallisuuden tasosta viiden kyvykkyyden näkökulmasta; kyky tunnistaa, suojautua, havainnoida, reagoida ja palautua kyberuhista.
Kohdeyleisö	Organisaation ylin johto, liiketoimintajohto, riskienhallinnan ja jatkuvuuden hallinnan vastuuhenkilöt
Hyödyntäminen	Kyberturvallisuuden tilan raportointi ylimmälle johdolle. Kyberturvallisuus-strategian arviointi ja tavoitteiden asettaminen. Raportti mahdollistaa organisaation vertaamisen referenssi- tai suositustasoihin.

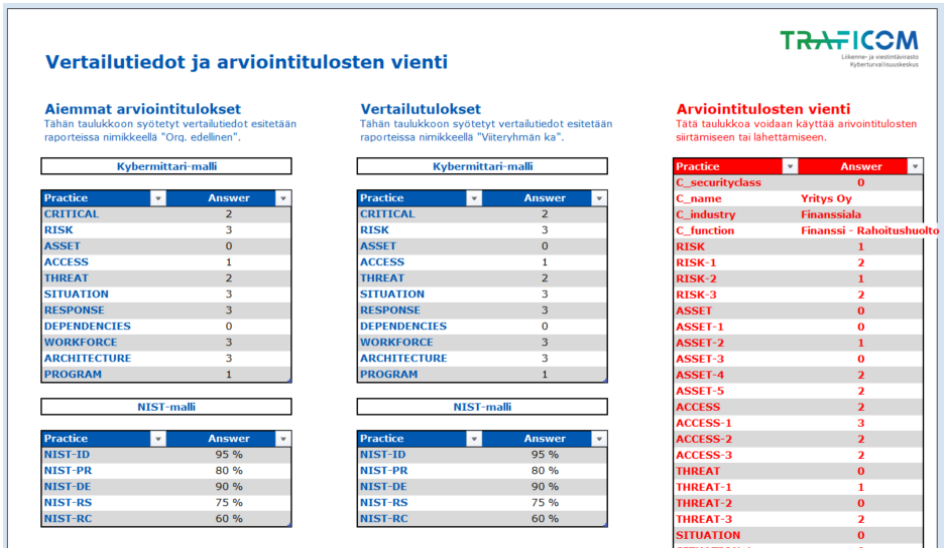
Kybermittarin kypsyysraportti

Sisältö	Raportti luo kattavan näkymän Kybermittarin tuloksiin yhdentoista arvioitavan osion sekä niihin liittyvien tavoitteiden kypsyystasojen suhteen.
Kohdeyleisö	Kyberturvallisuuden johto- ja kehitystehtävissä toimivat, liiketoiminnan kyberturvallisuuden vastuuhenkilöt ja aihealueisiin liittyvien prosessien omistajat
Hyödyntäminen	Kehitystä vaativien aihealueiden ja tavoitteiden tunnistaminen sekä kehitystoimenpiteiden priorisoiminen heikoimpiin alueisiin. Kyberturvallisuuden johtamisen tueksi ja uudelleen arvioinnin yhteydessä osoittamaan tavoitekohtaista kehitystä yhdistettynä kerättyyn tietoon kyberturvallisuuden investoinneista voidaan arvioida niiden vaikuttavuutta.

Yksityiskohtainen NIST CSF -raportti

Sisältö	Esittää Kybermittarin tulokset NIST-mallin vaatimusten kautta. Perustuu suuntaa-antavaan ristiin kytkentään C2M2 ja NIST -mallien kysymysten välillä.
Kohdeyleisö	Tietoturvallisuusden johto- ja kehitystehtävissä toimivat, liiketoiminnan kyberturvallisuuden vastuuhenkilöt, aihealueisiin liittyvien prosessien omistajat
Hyödyntäminen	Yksityiskohtaisen toimenpidesuunnitelman laatimisen tueksi, auttaa tulkitsemaan Kybermittarin osoittamia kehityskohteita eri näkökulmasta ristiin kytkennän avulla. Käsiteltäväksi kyberturvallisuuden ydinryhmän kesken ja mahdollisten nopeiden ja kevyiden kehitystoimenpiteiden tunnistamiseen.

Vertailutiedot ja tulosten vienti



Vertailutiedot ja arviointitulosten vienti

TRAFICOM

Aiemmat arviointitulokset

Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa nimikkeellä "Org. edellinen".

Kybermittari-malli

Practice	Answer
CRITICAL	2
RISK	3
ASSET	0
ACCESS	1
THREAT	2
SITUATION	3
RESPONSE	3
DEPENDENCIES	0
WORKFORCE	3
ARCHITECTURE	3
PROGRAM	1

NIST-malli

Practice	Answer
NIST-ID	95 %
NIST-PR	80 %
NIST-DE	90 %
NIST-RS	75 %
NIST-RC	60 %

Vertailutulokset

Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa nimikkeellä "Viiteryhmän ka".

Kybermittari-malli

Practice	Answer
CRITICAL	2
RISK	3
ASSET	0
ACCESS	1
THREAT	2
SITUATION	3
RESPONSE	3
DEPENDENCIES	0
WORKFORCE	3
ARCHITECTURE	3
PROGRAM	1

NIST-malli

Practice	Answer
NIST-ID	95 %
NIST-PR	80 %
NIST-DE	90 %
NIST-RS	75 %
NIST-RC	60 %

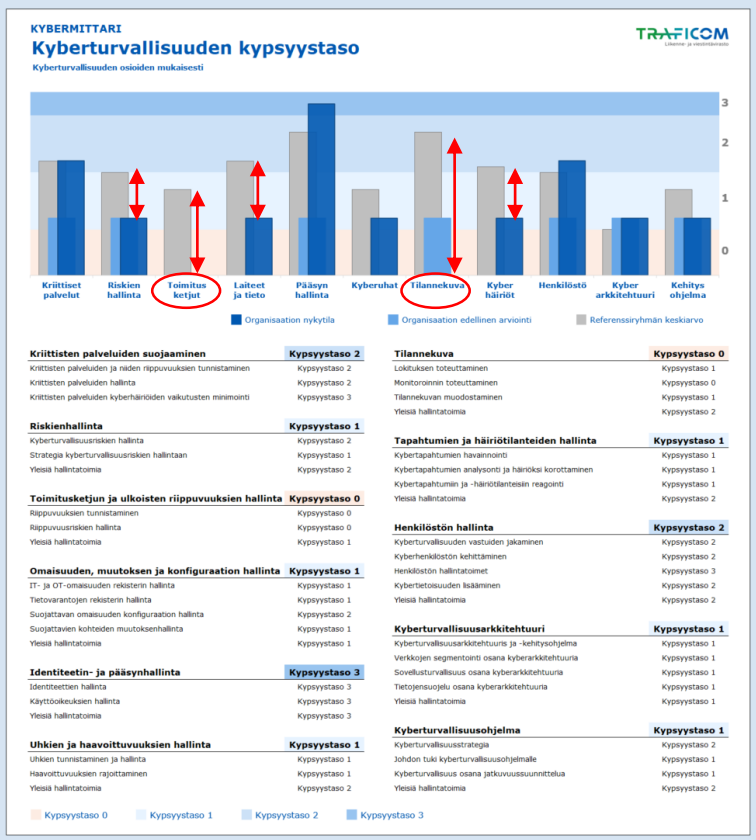
Arviointitulosten vienti

Tätä taulukkoa voidaan käyttää arviointitulosten siirtämiseen tai lähettämiseen.

Practice	Answer
C_securityclass	0
C_name	Yritys Oy
C_industry	Finanssiala
C_function	Finanssi - Rahoitushuolto
RISK	1
RISK-1	2
RISK-2	1
RISK-3	2
ASSET	0
ASSET-1	0
ASSET-2	1
ASSET-3	0
ASSET-4	2
ASSET-5	2
ACCESS	2
ACCESS-1	3
ACCESS-2	2
ACCESS-3	2
THREAT	0
THREAT-1	1
THREAT-2	0
THREAT-3	2
SITUATION	0

- Vertailutiedot
  - Työkalun raportteja voi rikastaa lisäämällä vertailutietoa DataExport-välilehden kautta
  - Tiedot luetaan automaattisesti työkalun tuottamiin raportteihin
  - Taulukoita on kaksi kahta eri käyttötarkoitusta varten
- Arviointitulosten vienti
  - Tulokset on mahdollista viedä työkalusta toiseen muotoon joko kopioimalla tai .xml-tiedostona
  - Vienti siirtää organisaation perustiedot, numeeriset arviointitulokset ja arvot investointien tasosta

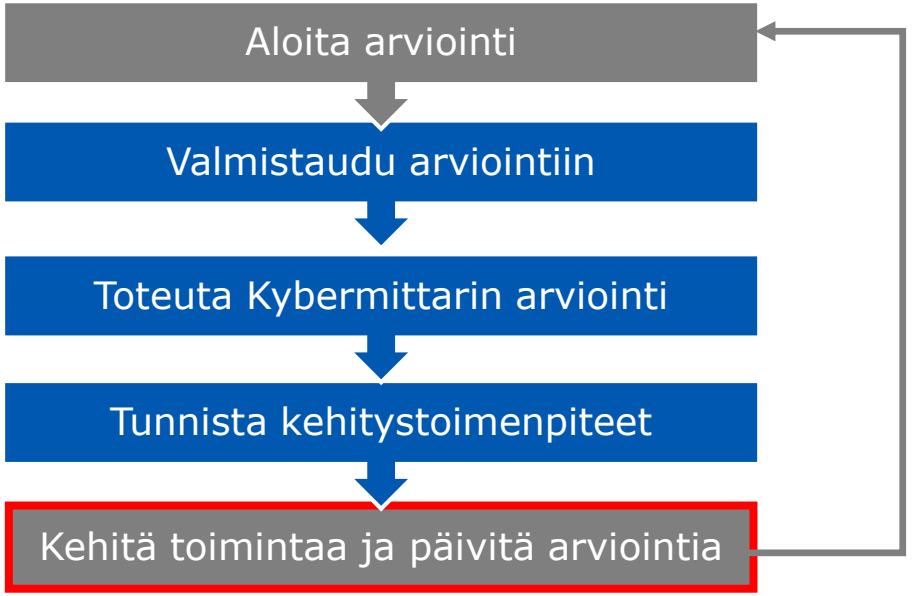
Esimerkkejä kehitystoimenpiteiden tunnistamiseen



- Kybermittarin kypsyysraportista, esimerkiksi:
  - Osiot ja tavoitteet, joiden kypsyystaso 0
  - Osiot, joiden kypsyystaso on merkittävästi toimialan referenssi- tai suositustasoja matalampi
  - Alhaisimmin suoriutuneet osiot
  - Alhaisimmin suoriutuneet osiot suhteessa aihealueen muihin tavoitteisiin

Kehitä toimintaa ja päivitä arviointia

Kehitä toimintaa ja päivitä arviointia



- **Osallistujat:**
  - Kehityssuunnitelmien omistajat, organisaation asiantuntijat sekä organisaation johtoryhmä tai muu päätöksentekoelin.
- **Tehtävä:**
  - Toteuttaa suunniteltuja kehitystoimenpiteitä, päivittä arviointia ja käynnistää tarvittaessa uusi arviointiprosessi.

Kehityssuunnitelman toteuttaminen

- Kehityssuunnitelmien omistajat koordinoivat suunnitelmien toteutusta ja ylläpitävät kokonaiskuvaa toimenpiteiden etenemisestä.

- Tavoitteena on varmistaa päätettyjen toimenpiteiden toteutuminen ja tunnistaa oikea aika arvioinnin päivittämiselle.

- Kybermittarin käyttäminen tulee nähdä prosessina, jossa arviointi ja kehitystoimenpiteiden toteuttaminen vuorottelevat säännöllisesti

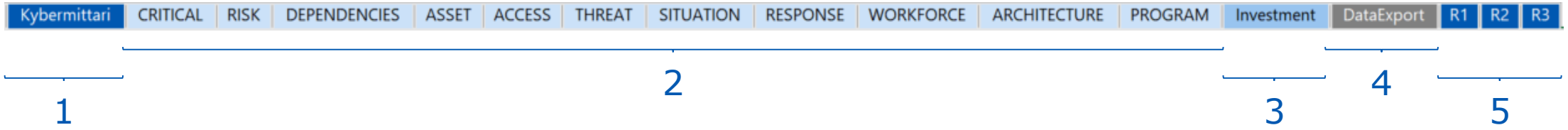
Arvioinnin päivittäminen ja uusi arviointi

- Arvioinnin päivitys tai uudelleenarviointi tulee ajankohtaiseksi esimerkiksi, kun
  - kehityssuunnitelmat etenevät tai
  - organisaation toimintaympäristö muuttuu
- Kybermittari-työkalu mahdollistaa aikaisempien arviointien vertailun, mikä helpottaa kehitystoimenpiteiden vaikutusten seurantaa ja raportointia
- Kybermittarin hyödyt tulevat parhaiten käyttöön, kun toimintaa arvioidaan säännöllisesti uudelleen ja kehitystoimenpiteiden vaikutukset nähdään myös raporteissa
- Sopiva aikaväli uudelleenarvioinnille voi olla esimerkiksi 1-2 vuotta edellisestä arviosta

Kybermittarin arviointityökalu

Ohjeita teknisen työkalun hyödyntämiseen

Kybermittarin arviointityökalun rakenne



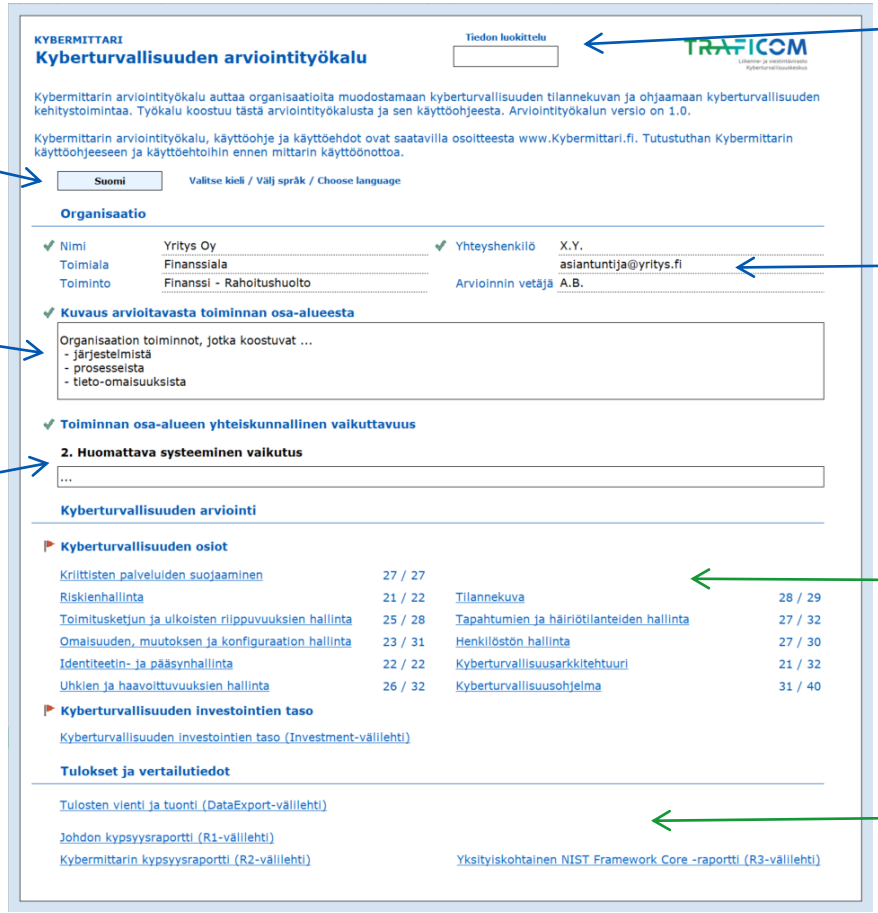
1. **Kybermittari-välilehti**
2. **Osiokohtaiset välilehdet (11kpl)**
3. **Investoinnit-välilehti**
4. **DataExport**
5. **Raportit (3kpl)**

1. Kybermittari-välilehti – yhteenveto

Kielivalinta

Toiminnan osa-alue

Yhteiskunnallinen vaikuttavuus



Tiedon luokittelu

Organisaation tiedot

Linkit arvioitaviin osioihin

Linkit raportteihin ja vertailutietoihin

2. Osiokohtaiset välilehdet (11 kpl)

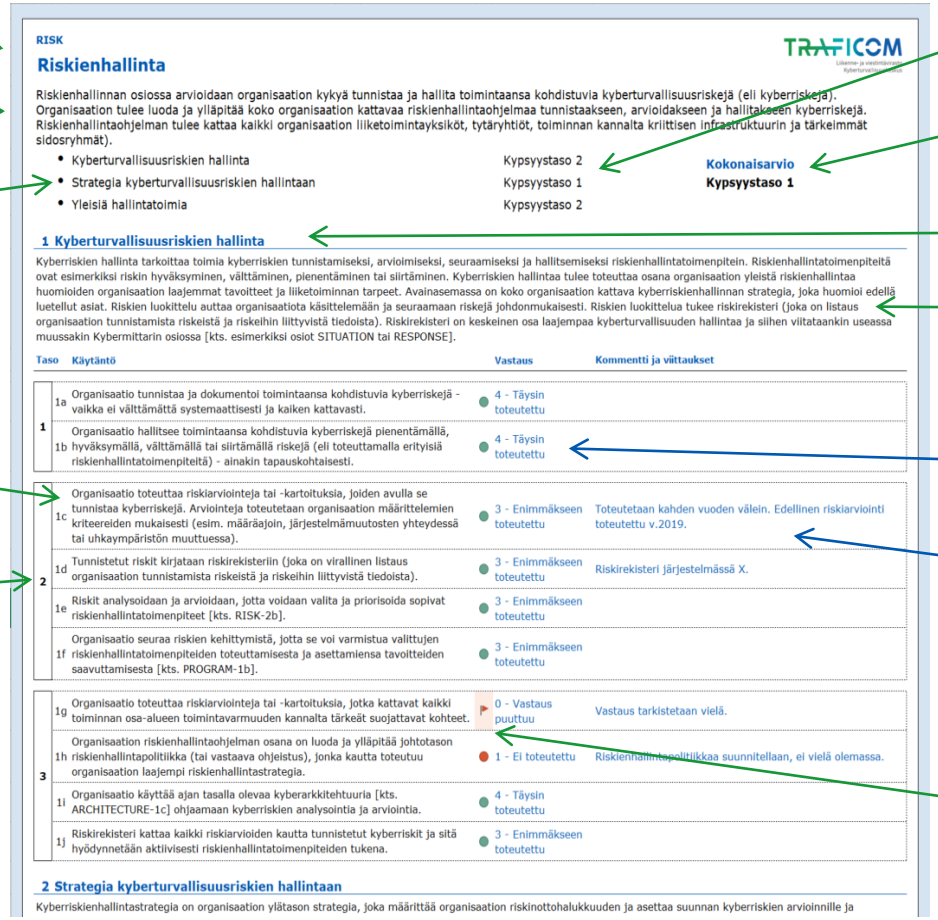
Osion tunniste ja nimi

Osion kuvaus

Osion tavoitteet

Käytäntö (tunniste ja kuvaus)

Käytännön kypsyystaso


RISK

TRAFICOM

Riskienhallinta

Riskienhallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimintaansa kohdistuvia kyberturvallisuusriskejä (eli kyberriskejä). Organisaation tulee luoda ja ylläpitää koko organisaation kattavaa riskienhallintaohjelmaa tunnistaakseen, arvioidakseen ja hallitakseen kyberriskejä. Riskienhallintaohjelman tulee kattaa kaikki organisaation liiketoimintayksiköt, tytäryhtiöt, toiminnan kannalta kriittisen infrastruktuurin ja tärkeimmät sidosryhmät).

- Kyberturvallisuusriskien hallinta — Kypsyystaso 2
- Strategia kyberturvallisuusriskien hallintaan — Kypsyystaso 1
- Yleisiä hallintatoimia — Kypsyystaso 2

Kokonaisarvio
Kypsyystaso 1

1 Kyberturvallisuusriskien hallinta

Kyberriskien hallinta tarkoittaa toimia kyberriskien tunnistamiseksi, arvioimiseksi, seuraamiseksi ja hallitsemiseksi riskienhallintatoimenpitein. Riskienhallintatoimenpiteitä ovat esimerkiksi riskin hyväksyminen, välttäminen, pienentäminen tai siirtäminen. Kyberriskien hallintaa tulee toteuttaa osana organisaation yleistä riskienhallintaa huomioiden organisaation laajemmat tavoitteet ja liiketoiminnan tarpeet. Avainasemassa on koko organisaation kattava kyberriskienhallinnan strategia, joka huomioi edellä luetellut asiat. Riskien luokittelu auttaa organisaatiota käsittelemään ja seuraamaan riskejä johdonmukaisesti. Riskien luokittelua tukee riskirekisteri (joka on listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista). Riskirekisteri on keskeinen osa laajempaa kyberturvallisuuden hallintaa ja siihen viitataankin useassa muussakin Kybermittarin osiossa [kts. esimerkiksi osiot SITUATION tai RESPONSE].

Taso	Käytäntö	Vastaus	Kommentti ja viittaukset
1	1a Organisaatio tunnistaa ja dokumentoi toimintaansa kohdistuvia kyberriskejä - vaikka ei välttämättä systemaattisesti ja kaiken kattavasti.	4 - Täysin toteutettu	
	1b Organisaatio hallitsee toimintaansa kohdistuvia kyberriskejä pienentämällä, hyväksymällä, välttämällä tai siirtämällä riskejä (eli toteuttamalla erityisiä riskienhallintatoimenpiteitä) - ainakin tapauskohtaisesti.	4 - Täysin toteutettu	
2	1c Organisaatio toteuttaa riskiarviointeja tai -kartoituksia, joiden avulla se tunnistaa kyberriskejä. Arviointeja toteutetaan organisaation määrittelemien kriteereiden mukaisesti (esim. määräajoin, järjestelmämuutosten yhteydessä tai uhkaympäristön muuttuessa).	3 - Enimmäkseen toteutettu	Toteutetaan kahden vuoden välein. Edellinen riskiarviointi toteutettu v.2019.
	1d Tunnistetut riskit kirjataan riskirekisteriin (joka on virallinen listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista).	3 - Enimmäkseen toteutettu	Riskirekisteri järjestelmässä X.
	1e Riskit analysoidaan ja arvioidaan, jotta voidaan valita ja priorisoida sopivat riskienhallintatoimenpiteet [kts. RISK-2b].	3 - Enimmäkseen toteutettu	
	1f Organisaatio seuraa riskien kehittymistä, jotta se voi varmistua valittujen riskienhallintatoimenpiteiden toteuttamisesta ja asettamiensa tavoitteiden saavuttamisesta [kts. PROGRAM-1b].	3 - Enimmäkseen toteutettu	
3	1g Organisaatio toteuttaa riskiarviointeja tai -kartoituksia, jotka kattavat kaikki toiminnan osa-alueen toimintavarmuuden kannalta tärkeät suojattavat kohteet.	0 - Vastaus puuttuu	Vastaus tarkistetaan vielä.
	1h Organisaation riskienhallintaohjelman osana on luoda ja ylläpitää johtotason riskienhallintapolitiikka (tai vastaava ohjeistus), jonka kautta toteutuu organisaation laajempi riskienhallintastrategia.	1 - Ei toteutettu	Riskienhallintapolitiikkaa suunnitellaan, ei vielä olemassa.
	1i Organisaatio käyttää ajan tasalla olevaa kyberarkkitehtuuria [kts. ARCHITECTURE-1c] ohjaamaan kyberriskien analysointia ja arviointia.	4 - Täysin toteutettu	
	1j Riskirekisteri kattaa kaikki riskiarvioiden kautta tunnistetut kyberriskit ja sitä hyödynnetään aktiivisesti riskienhallintatoimenpiteiden tukena.	3 - Enimmäkseen toteutettu	

2 Strategia kyberturvallisuusriskien hallintaan

Kyberriskienhallintastrategia on organisaation ylätason strategia, joka määrittää organisaation riskinottohalukkuuden ja asettaa suunnan kyberriskien arvioinnille ja

Tavoitteiden kypsyystasot

Osion kypsyystaso

Tavoitteen nimi

Tavoitteen kuvaus

Vastaus (1-4 tai 0)

Kommentti ja viittaus

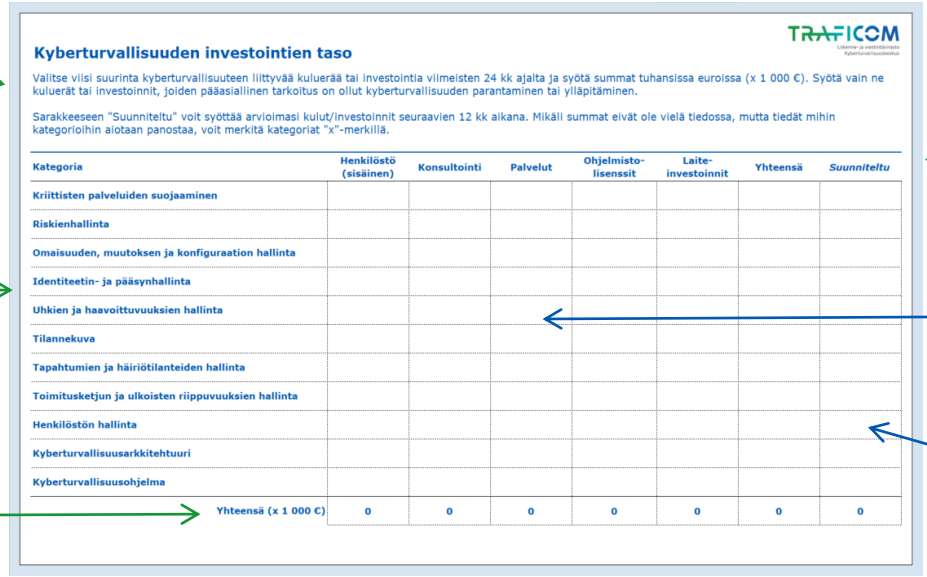
Vastauksen indikaattori

3. Kyberturvallisuuden investoinnit -välilehdet

Lyhyt ohjeistus

Kybermittarin osiot

Summat



Kyberturvallisuuden investointien taso

Valitse viisi suurinta kyberturvallisuuteen liittyvää kuluerää tai investointia viimeisten 24 kk ajalta ja syötä summat tuhansissa euroissa (x 1 000 €). Syötä vain ne kuluerät tai investoinnit, joiden pääasiallinen tarkoitus on ollut kyberturvallisuuden parantaminen tai ylläpitäminen.

Sarakkeeseen "Suunniteltu" voit syöttää arvioimasi kulut/investoinnit seuraavien 12 kk aikana. Mikäli summat eivät ole vielä tiedossa, mutta tiedät mihin kategorioihin aiotaan panostaa, voit merkitä kategoriat "x"-merkillä.

Kategoria	Henkilöstö (sisäinen)	Konsultointi	Palvelut	Ohjelmisto-lisenssit	Laite-investoinnit	Yhteensä	*Suunniteltu*
Kriittisten palveluiden suojaaminen							
Riskienhallinta							
Omaisuuden, muutoksen ja konfiguraation hallinta							
Identiteetin- ja pääsynhallinta							
Uhkien ja haavoittuvuuksien hallinta							
Tilannekuva							
Tapahtumien ja häiriötilanteiden hallinta							
Toimitusketjun ja ulkoisten riippuvuuksien hallinta							
Henkilöstön hallinta							
Kyberturvallisuusarkkitehtuuri							
Kyberturvallisuusohjelma							
Yhteensä (x 1 000 €)	0	0	0	0	0	0	0

Investointilajit

Tehdyt investoinnit (24 kk)

Tulevat investoinnit (12 kk)

4. DataExport-välilehti

Vertailutulokset – esim. aiempi arviointi

Vertailutulokset – esim. viiteryhmän ka

Kybermittarin osio

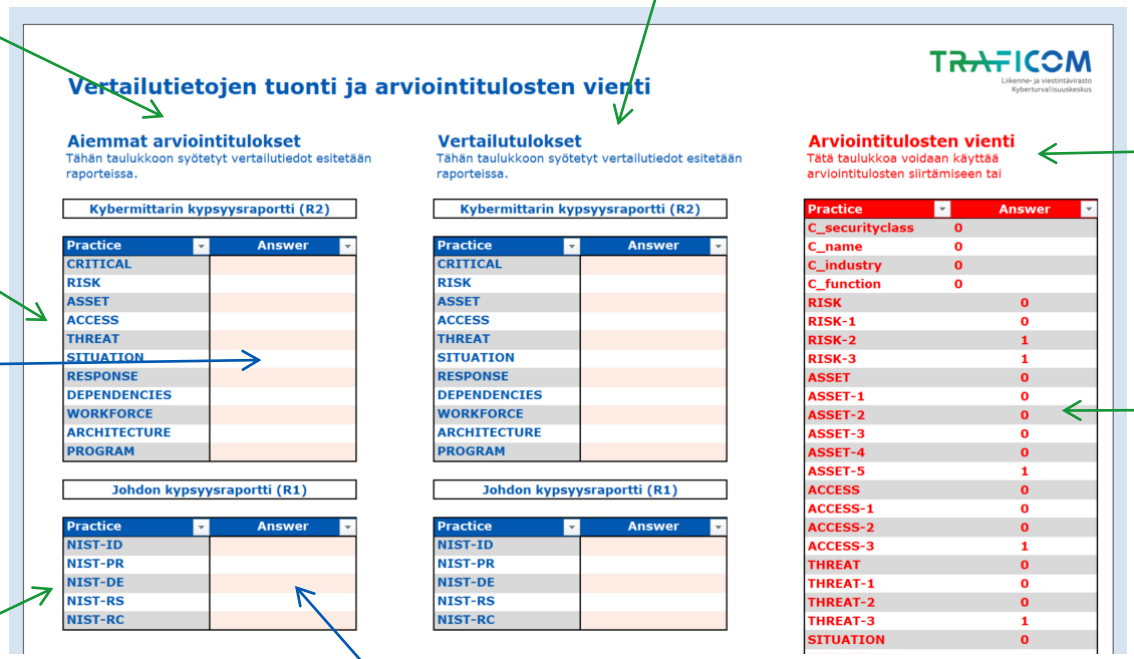
Vertailutulokset (Kokonais-/desimaalilukuina)

NIST CSF -osio

Vertailutulokset (Prosenttilukuina)

Tulosten vienti

Taulukko tulosten kopiointiin tai vientiin .xml-muodossa



TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Vertailutietojen tuonti ja arviointitulosten vienti

Aiemmat arviointitulokset
Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa.

Kybermittarin kypsyysraportti (R2)

Practice	Answer
CRITICAL	
RISK	
ASSET	
ACCESS	
THREAT	
SITUATION	
RESPONSE	
DEPENDENCIES	
WORKFORCE	
ARCHITECTURE	
PROGRAM	

Johdon kypsyysraportti (R1)

Practice	Answer
NIST-ID	
NIST-PR	
NIST-DE	
NIST-RS	
NIST-RC	

Vertailutulokset
Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa.

Kybermittarin kypsyysraportti (R2)

Practice	Answer
CRITICAL	
RISK	
ASSET	
ACCESS	
THREAT	
SITUATION	
RESPONSE	
DEPENDENCIES	
WORKFORCE	
ARCHITECTURE	
PROGRAM	

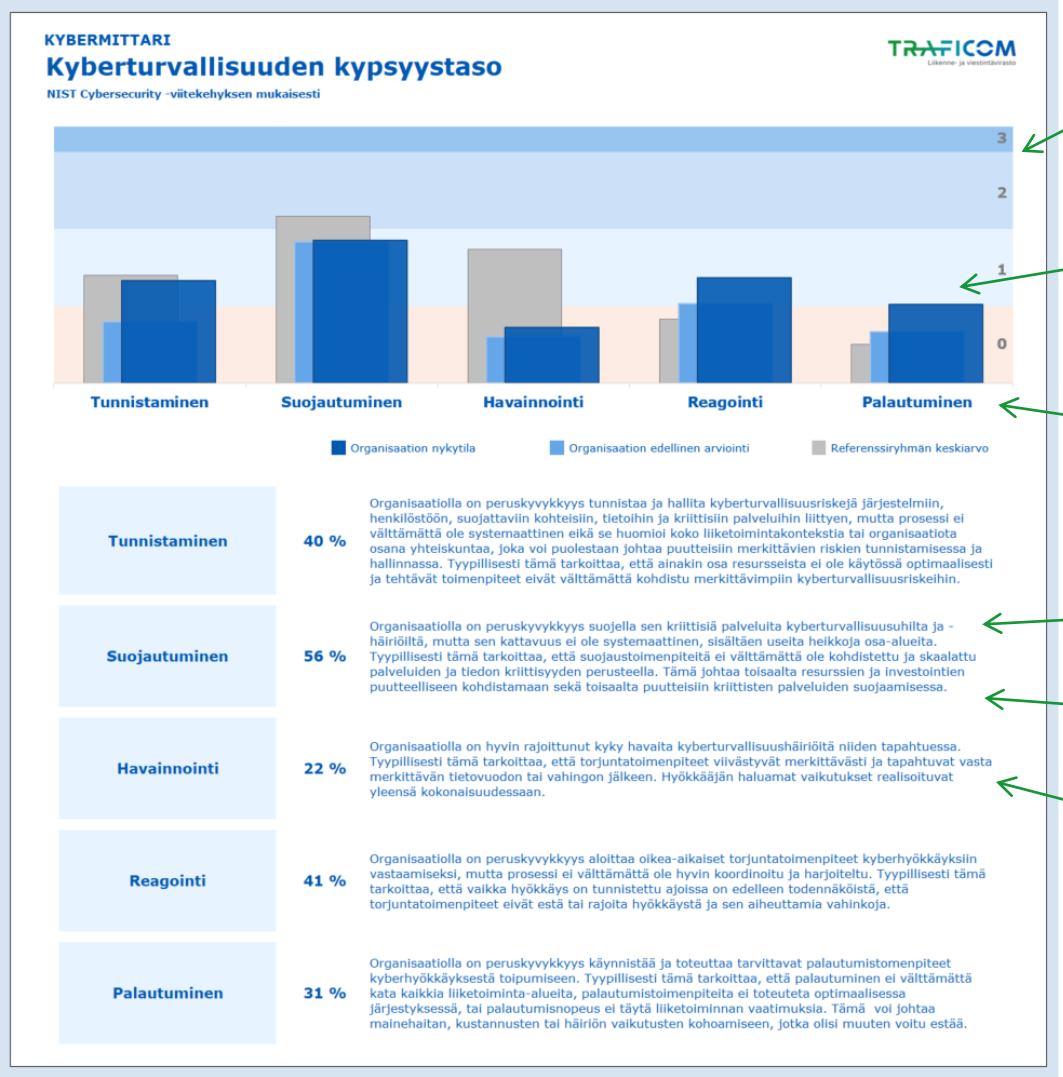
Johdon kypsyysraportti (R1)

Practice	Answer
NIST-ID	
NIST-PR	
NIST-DE	
NIST-RS	
NIST-RC	

Arviointitulosten vienti
Tätä taulukkoa voidaan käyttää arviointitulosten siirtämiseen tai

Practice	Answer
C_securityclass	0
C_name	0
C_industry	0
C_function	0
RISK	0
RISK-1	0
RISK-2	1
RISK-3	1
ASSET	0
ASSET-1	0
ASSET-2	0
ASSET-3	0
ASSET-4	0
ASSET-5	1
ACCESS	0
ACCESS-1	0
ACCESS-2	0
ACCESS-3	1
THREAT	0
THREAT-1	0
THREAT-2	0
THREAT-3	1
SITUATION	0

5. Raportit (1/3)



KYBERMITTARI

Kyberturvallisuuden kypsyystaso

NIST Cybersecurity -viitekehyksen mukaisesti

TRAFICOM

Liikenne- ja viestintävirasto

Tunnistaminen	**40 %**	Organisaatiolla on peruskyvykkyys tunnistaa ja hallita kyberturvallisuusriskejä järjestelmiin, henkilöstöön, suojattaviin kohteisiin, tietoihin ja kriittisiin palveluihin liittyen, mutta prosessi ei välttämättä ole systemaattinen eikä se huomioi koko liiketoimintakontekstia tai organisaatiota osana yhteiskuntaa, joka voi puolestaan johtaa puutteisiin merkittävien riskien tunnistamisessa ja hallinnassa. Tyypillisesti tämä tarkoittaa, että ainakin osa resursseista ei ole käytössä optimaalisesti ja tehtävät toimenpiteet eivät välttämättä kohdistu merkittävimpiin kyberturvallisuusriskeihin.
Suojautuminen	**56 %**	Organisaatiolla on peruskyvykkyys suojella sen kriittisiä palveluita kyberturvallisuusuhilta ja -häiriöiltä, mutta sen kattavuus ei ole systemaattinen, sisältäen useita heikkoja osa-alueita. Tyypillisesti tämä tarkoittaa, että suojaustoimenpiteitä ei välttämättä ole kohdistettu ja skaalattu palveluiden ja tiedon kriittisyyden perusteella. Tämä johtaa toisaalta resurssien ja investointien puutteelliseen kohdistamaan sekä toisaalta puutteisiin kriittisten palveluiden suojaamisessa.
Havainnointi	**22 %**	Organisaatiolla on hyvin rajoittunut kyky havaita kyberturvallisuushäiriöitä niiden tapahtuessa. Tyypillisesti tämä tarkoittaa, että torjuntatoimenpiteet viivästyvät merkittävästi ja tapahtuvat vasta merkittävän tietovuodon tai vahingon jälkeen. Hyökkääjän haluamat vaikutukset realisoituvat yleensä kokonaisuudessaan.
Reagointi	**41 %**	Organisaatiolla on peruskyvykkyys aloittaa oikea-aikaiset torjuntatoimenpiteet kyberhyökkäyksiin vastaamiseksi, mutta prosessi ei välttämättä ole hyvin koordinoitu ja harjoiteltu. Tyypillisesti tämä tarkoittaa, että vaikka hyökkäys on tunnistettu ajoissa on edelleen todennäköistä, että torjuntatoimenpiteet eivät estä tai rajoita hyökkäystä ja sen aiheuttamia vahinkoja.
Palautuminen	**31 %**	Organisaatiolla on peruskyvykkyys käynnistää ja toteuttaa tarvittavat palautumistomenpiteet kyberhyökkäyksestä toipumiseen. Tyypillisesti tämä tarkoittaa, että palautuminen ei välttämättä kata kaikkia liiketoiminta-alueita, palautumistoimenpiteita ei toteuteta optimaalisessa järjestyksessä, tai palautumisnopeus ei täytä liiketoiminnan vaatimuksia. Tämä voi johtaa mainehaitan, kustannusten tai häiriön vaikutusten kohoamiseen, jotka olisi muuten voitu estää.

Kypsyysasteikko 0-3

Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

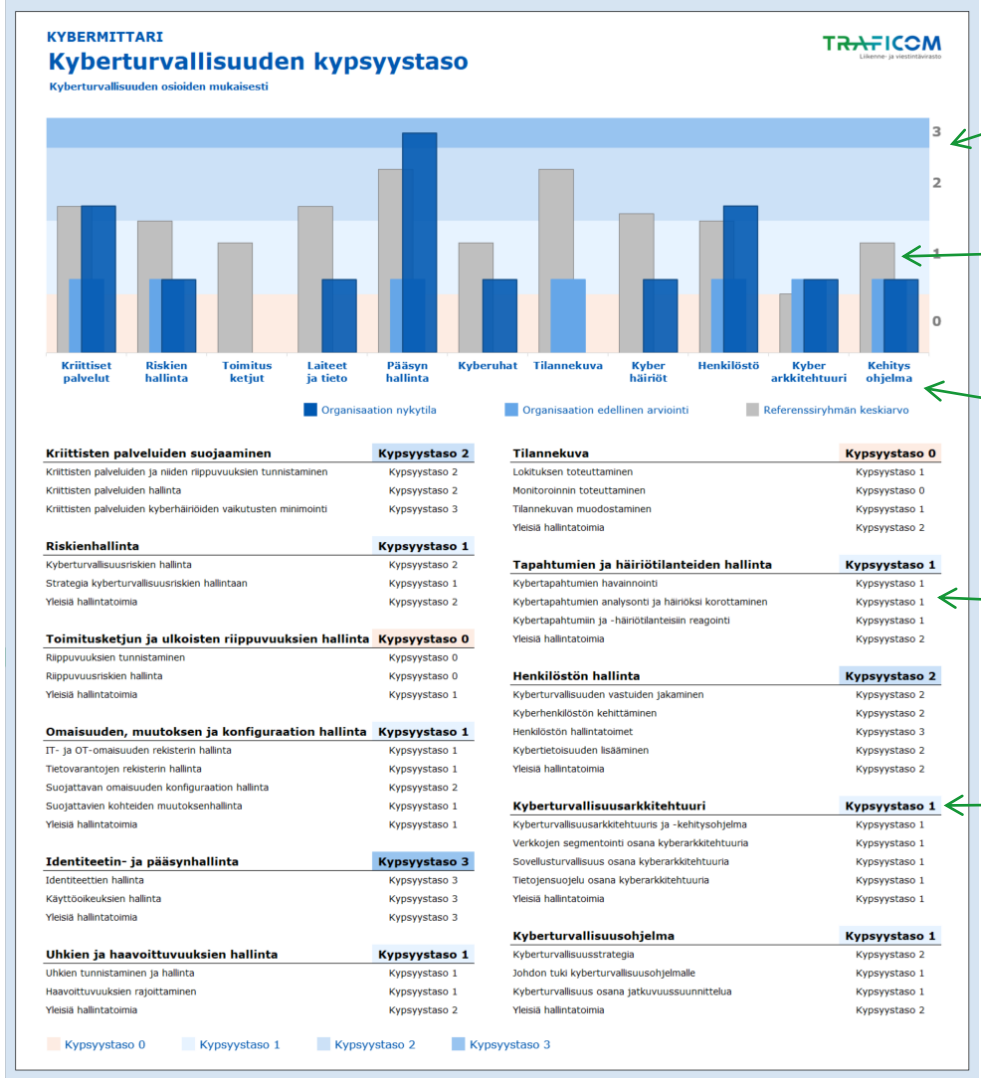
NIST CSF 5 osa-aluetta

Osa-alue

Toteutuneiden käytäntöjen osuus (%)

Sanallinen kuvaus kypsyystasosta

5. Raportit (2/3)



KYBERMITTARI

Kyberturvallisuuden kypsyystaso

Kyberturvallisuuden osioiden mukaisesti

TRAFICOM

Kriittisten palveluiden suojaaminen	Kypsyystaso 2
Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen	Kypsyystaso 2
Kriittisten palveluiden hallinta	Kypsyystaso 2
Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi	Kypsyystaso 3

Riskienhallinta	Kypsyystaso 1
Kyberturvallisuusriskien hallinta	Kypsyystaso 2
Strategia kyberturvallisuusriskien hallintaan	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 2

Toimitusketjun ja ulkoisten riippuvuuksien hallinta	Kypsyystaso 0
Riippuvuuksien tunnistaminen	Kypsyystaso 0
Riippuvuusriskien hallinta	Kypsyystaso 0
Yleisiä hallintatoimia	Kypsyystaso 1

Omaisuuden, muutoksen ja konfiguraation hallinta	Kypsyystaso 1
IT- ja OT-omaisuuden rekisterin hallinta	Kypsyystaso 1
Tietovarantojen rekisterin hallinta	Kypsyystaso 1
Suojattavan omaisuuden konfiguraation hallinta	Kypsyystaso 2
Suojattavien kohteiden muutoksenhallinta	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 1

Identiteetin- ja pääsynhallinta	Kypsyystaso 3
Identiteettien hallinta	Kypsyystaso 3
Käyttöoikeuksien hallinta	Kypsyystaso 3
Yleisiä hallintatoimia	Kypsyystaso 3

Uhkien ja haavoittuvuuksien hallinta	Kypsyystaso 1
Uhkien tunnistaminen ja hallinta	Kypsyystaso 1
Haavoittuvuuksien rajoittaminen	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 2

Tilannekuva	Kypsyystaso 0
Lokituksen toteuttaminen	Kypsyystaso 1
Monitoroinnin toteuttaminen	Kypsyystaso 0
Tilannekuvan muodostaminen	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 2

Tapahtumien ja häiriötilanteiden hallinta	Kypsyystaso 1
Kybertapahtumien havainnointi	Kypsyystaso 1
Kybertapahtumien analysointi ja häiriöksi korottaminen	Kypsyystaso 1
Kybertapahtumiin ja -häiriötilanteisiin reagointi	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 2

Henkilöstön hallinta	Kypsyystaso 2
Kyberturvallisuuden vastuiden jakaminen	Kypsyystaso 2
Kyberhenkilöstön kehittäminen	Kypsyystaso 2
Henkilöstön hallintatoimet	Kypsyystaso 3
Kybertietoisuuden lisääminen	Kypsyystaso 2
Yleisiä hallintatoimia	Kypsyystaso 2

Kyberturvallisuusarkkitehtuuri	Kypsyystaso 1
Kyberturvallisuusarkkitehtuuris ja -kehitysohjelma	Kypsyystaso 1
Verkkojen segmentointi osana kyberarkkitehtuuria	Kypsyystaso 1
Sovellusturvallisuus osana kyberarkkitehtuuria	Kypsyystaso 1
Tietojensuojelu osana kyberarkkitehtuuria	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 1

Kyberturvallisuusohjelma	Kypsyystaso 1
Kyberturvallisuusstrategia	Kypsyystaso 2
Johdon tuki kyberturvallisuusohjelmalle	Kypsyystaso 1
Kyberturvallisuus osana jatkuvuussuunnittelua	Kypsyystaso 1
Yleisiä hallintatoimia	Kypsyystaso 2

Kypsyystaso 0 Kypsyystaso 1 Kypsyystaso 2 Kypsyystaso 3

Kypsyysasteikko 0-3

Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

Kybermittarin 11 osa-aluetta

Yksityiskohtaisemmin
- Osiot
- Tavoitteet

Osion tai tavoitteen kypsyystaso

5. Raportit (3/3)

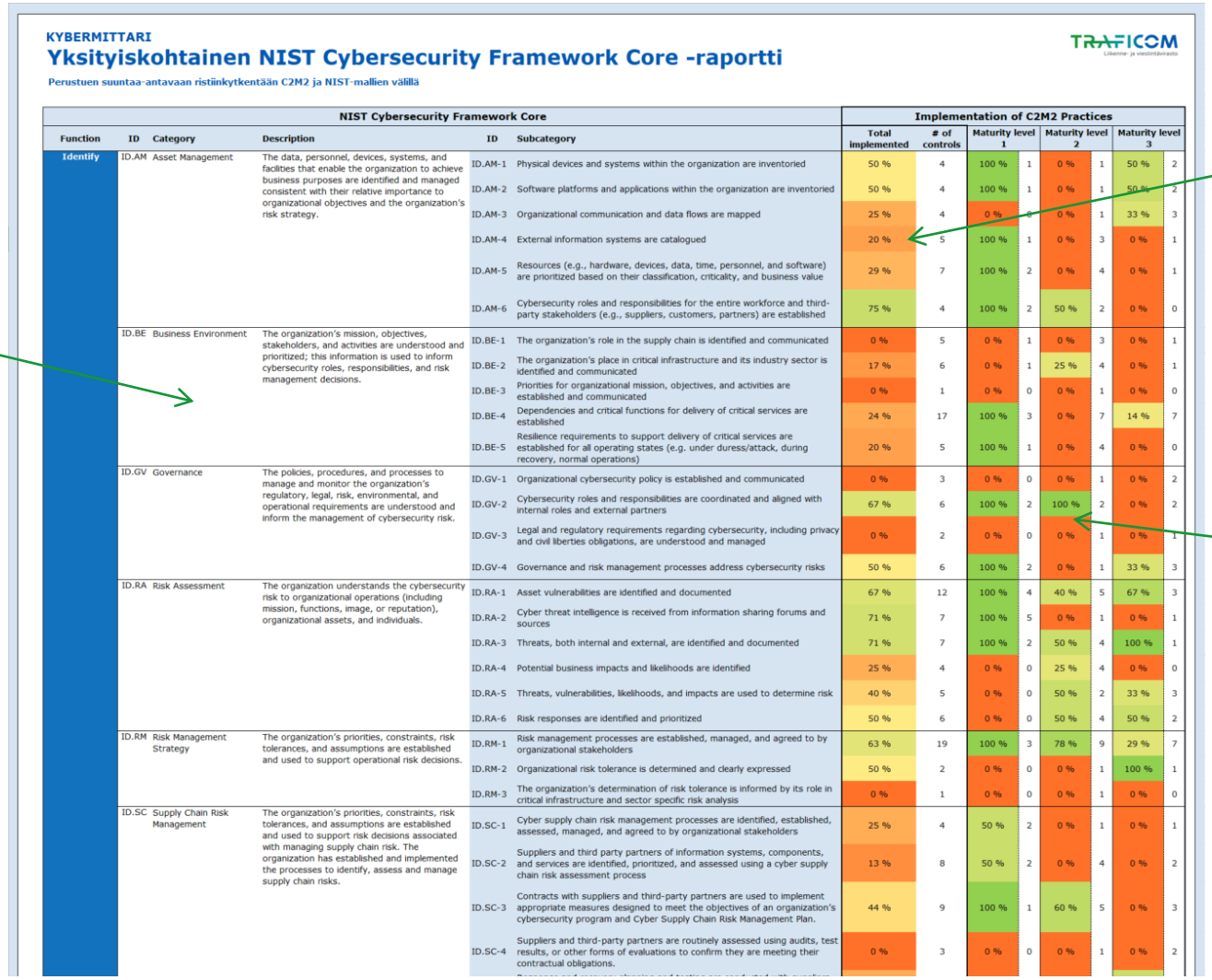
NIST CSF Osa-alueet ja tavoitteet

Käytäntöjen määrä ja toteutumisprosentti

(kokonaisuudessaan)

Käytäntöjen määrä ja toteutumisprosentti

(jaettuna kypsyystasojen mukaisesti)



KYBERMITTARI

Yksityiskohtainen NIST Cybersecurity Framework Core -raportti

Perustuen suuntaa-antavaan ristiinkytkentään C2M2 ja NIST-mallien välillä

TRAFICOM Liikenne- ja viestintävirasto

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-3	Organizational communication and data flows are mapped	25 %	4	0 %	0	0 %	1	33 %	3
				ID.AM-4	External information systems are catalogued	20 %	5	100 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	29 %	7	100 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	17 %	6	0 %	1	25 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	24 %	17	100 %	3	0 %	7	14 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	100 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	1	0 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	67 %	6	100 %	2	100 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	50 %	6	100 %	2	0 %	1	33 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	67 %	12	100 %	4	40 %	5	67 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	71 %	7	100 %	5	0 %	1	0 %	1
				ID.RA-3	Threats, both internal and external, are identified and documented	71 %	7	100 %	2	50 %	4	100 %	1
				ID.RA-4	Potential business impacts and likelihoods are identified	25 %	4	0 %	0	25 %	4	0 %	0
				ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	40 %	5	0 %	0	50 %	2	33 %	3
				ID.RA-6	Risk responses are identified and prioritized	50 %	6	0 %	0	50 %	4	50 %	2
	ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	63 %	19	100 %	3	78 %	9	29 %	7
				ID.RM-2	Organizational risk tolerance is determined and clearly expressed	50 %	2	0 %	0	0 %	1	100 %	1
				ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	0 %	1	0 %	0	0 %	1	0 %	0
	ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	25 %	4	50 %	2	0 %	1	0 %	1
				ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	13 %	8	50 %	2	0 %	4	0 %	2
				ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	44 %	9	100 %	1	60 %	5	0 %	3
				ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	0 %	3	0 %	0	0 %	1	0 %	2

Kybermittarin toiminnallisuuksiin liittyvät välilehdet

Piilotetut välilehdet

- Languages
  - Selitetekstien kieliversiot (FI, SE, EN)
- Parameters
  - Työkalun käyttämät vaihtoehdot ja säätöparametrit
- Data
  - Kypsyystasojen koonti- ja laskentasivu
- NISTMap
  - Kybermittarin / C2M2 –mallien ja NIST CSF –mallien välinen ristiin kytkentä