TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari

Perusperiaatteet
13.06.2023

Sisältö ja tavoite

- Kybermittari 2023-
- Johdanto aiheeseen
- Kybermittarin arviointimalli
- Kybermittarin arviointiprosessi
- Kybermittari-työkalu

TRAFICOM

Kyberturvallisuus on...

- **tavoitetila**, jossa **kybertoimintaympäristöön** eli koko nykyiseen verkottuneeseen digitaaliseen yhteiskuntaamme **voidaan luottaa** ja jossa sen **toiminta turvataan.**

Lähde: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Kyberturvallisuuskeskus –tammikuun kybersää

”Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista”.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Tärkein tietoturvateko on tiedostaa, mikä on organisaation nykyinen tietoturvallisuuden taso. Mitä tulisi kehittää? Tämän jälkeen pitäisi myös viedä läpi tarvittavat kehitystoimet.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2023-

Kybermittari 2023->
Pääteemat

- Tietoisuus Kybermittarista
- Kybermittarin käyttöönoton edistäminen
- Vertailutieto ja verkostot
- Kehitys ja tuki

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Johdanto aiheeseen

Kybermittarin tausta ja tarkoitus

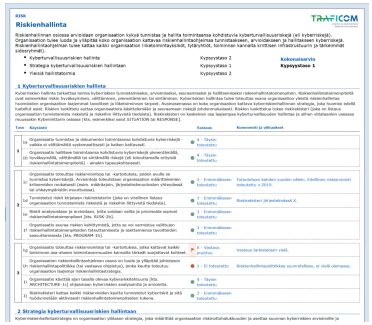
Kybermittari-palvelun tarkoitus

- Onko organisaatiollanne ymmärrys, **millainen kyberkyvykkyys teillä on suojautua kyberuhilta** ja varmistaa liiketoimintanne **jatkuvuus** häiriötilanteissa?
  - Kybermittari auttaa
    - **johtamaan** kyberturvallisuuden sekä henkilöstöä **ymmärtämään ja kehittämään** toiminnan kyberturvallisuutta myös **suomen ja ruotsin** kielellä.
    - Arvioimaan **säännöllisesti** ja systemaattisesti kyberkyvykkyyttänne eri osa-alueilla
    - ***tunnistamalla kehityskohteita****, asettamaan* ***tavoitetason*** *ja* ***investoimaan*** *oikeisiin asioihin.*
- Kybermittari antaa myös **vertailutietoa ja helpottaa yhteistyötä sekä tiedonjakoa** verkostoissa ja sidosryhmien kanssa.
  - Kerätty vertailutieto auttaa myös **kansallisen tilannekuvan muodostamisessa** ja investointien kohdentamisessa.

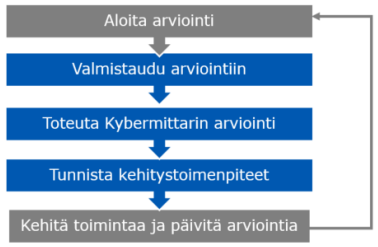
Kenelle Kybermittari on tarkoitettu?

- Kybermittari on tarkoitettu kaikille organisaatioille, jotka tarvitsevat **toimintansa kehittämisen ja päätöksenteon tueksi mitattua tietoa** organisaation kyvystä vastata ja ehkäistä kyberhäiriöitä.
- Organisaatioille, jotka haluavat toimialan vertailutietoa ja osallistua **kansallisen tilannekuvan muodostamiseen**
- Organisaatioille jotka haluavat työkalun, joka **helpottaa yhteistyötä sekä vuorovaikutusta** verkostoissa, sidosryhmien tai palveluntarjoajien kanssa.
- Kybermittaria voi **muokata** omiin tarpeisiin ja käyttää vaikka osittain.
- Työkalun **kieltä voi vaihtaa** lennosta suomen-, ruotsin- ja englanninkieliseksi.

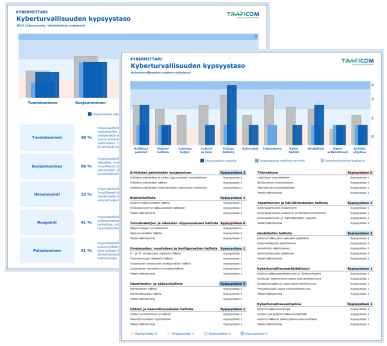
Kybermittarin materiaalit



- 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.

Kybermittarin käytön ehdot, tarkemmin

- Cybersecurity Capability Maturity Model (C2M2) ehdot:

© 2022 Carnegie Mellon University. This version of C2M2 is being released and maintained by the U.S. Department of Energy (DOE). ***The U.S. Government has, at minimum, unlimited rights to use, modify, reproduce, release, perform, display, or disclose this version the C2M2 or corresponding tools provided by DOE, as well as the right to authorize others, and hereby authorizes others, to do the same****.*

During the creation of the original C2M2, Capability Maturity Model® and CMM® were registered trademarks of Carnegie Mellon University. Information Systems Audit and Control Association, Inc. (ISACA) is the current owner of these marks but did not participate in the creation of C2M2.

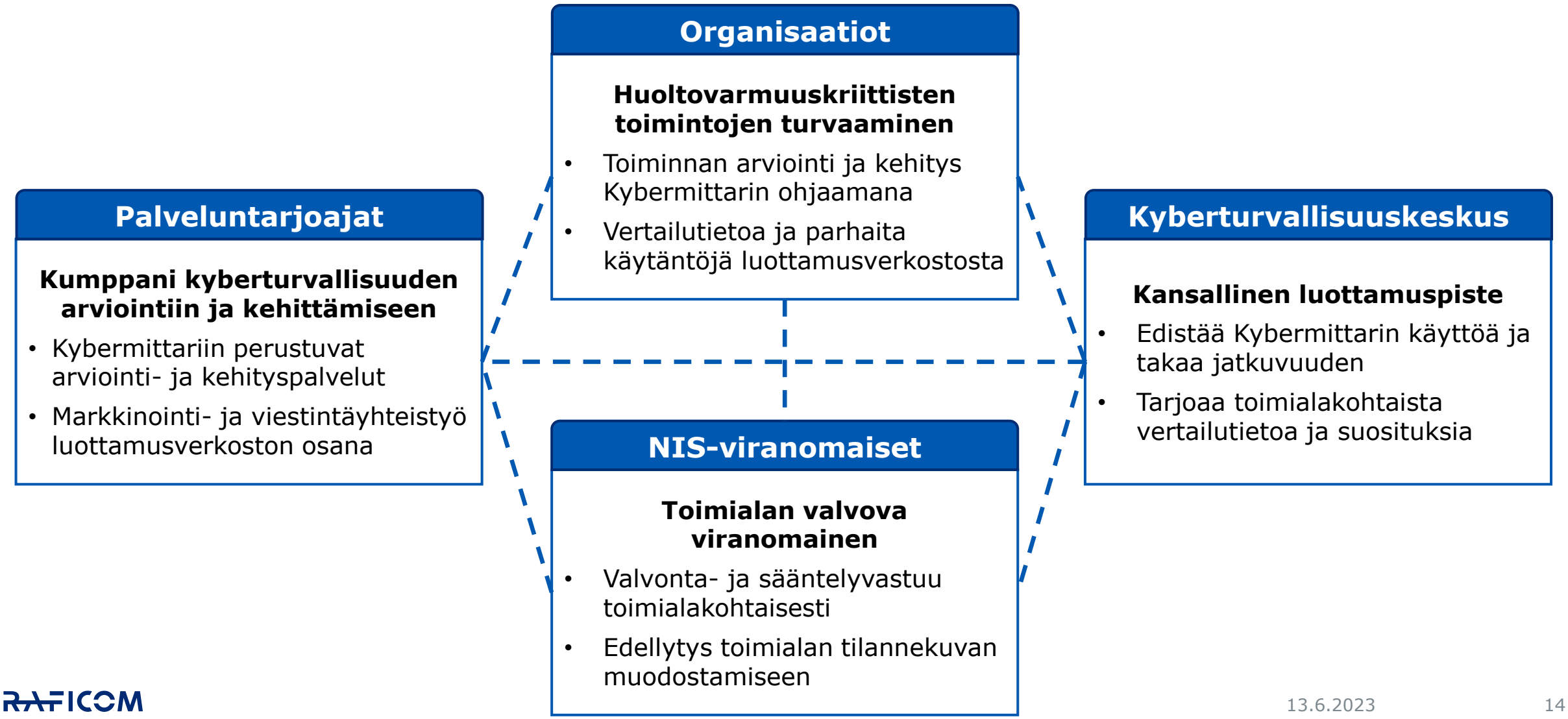
- Kybermittarin ehdot:

1. *”Kybermittari” on Kyberturvallisuuskeskuksen omistama tavaramerkki (sanamerkki) (PRH, Rno: 279095)*

2. *Kybermittariin liittyvä materiaali on julkaistu* ***Creative Commons Nimeä 4.0 -lisenssillä (CC BY 4.0).*** *Se tarkoittaa, että saat käyttää listaa mihin tarkoitukseen haluat, muokata sitä niin kuin haluat ja jakaa sitä eteenpäin niin kuin haluat, seuraavilla ehdoilla:*

- *Nimeä - Sinun on mainittava lähde asianmukaisesti, tarjottava linkki lisenssiin sekä merkittävä, mikäli olet tehnyt muutoksia. Voit tehdä yllä olevan millä tahansa kohtuullisella tavalla, mutta et siten, että annat ymmärtää lisenssinantajan suosittelevan sinua tai teoksen käyttöäsi.*
- *Ei muita rajoituksia - Et voi asettaa sellaisia oikeudellisia ehtoja tai teknisiä estoja, jotka estävät oikeudellisesti muita tekemästä mitään sellaista, minkä lisenssi sallii*

Kybermittarin luottamusverkosto



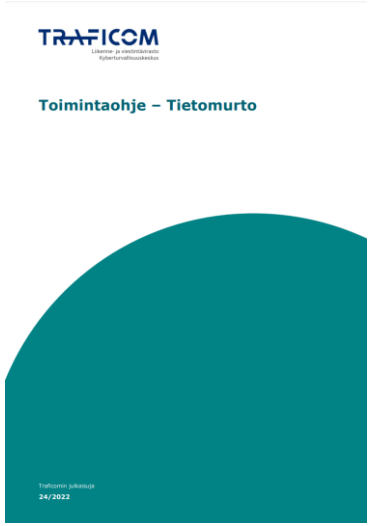
Lisätietoa

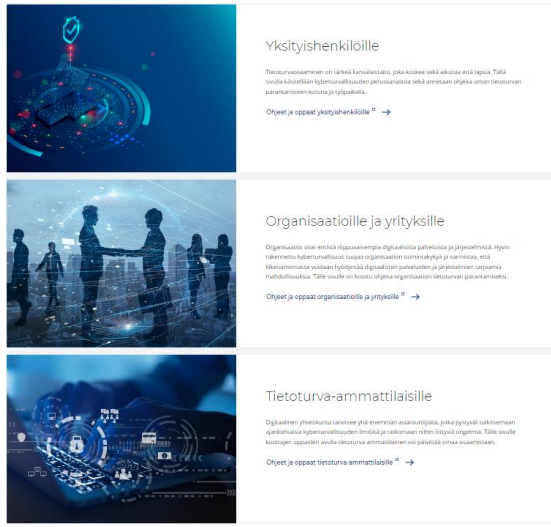
Kybermittari.fi –sivusto

- **Kybermittarin työkalut ja tuki**
- **Tapahtumat**
- **Ohjeet vertailutiedon jakamiseen.**
- **Mahdollisuudet osallistua kehitykseen**
- **Palveluntarjoajat**, jotka ovat ilmoittaneet tarjoavansa tukipalveluita Kybermittarin käyttöön
- **Yhteystiedot ja palautekanavat**

TRAFICOM

Kyberturvallisuuskeskuksen ilmaiset ohjeet ja oppaat



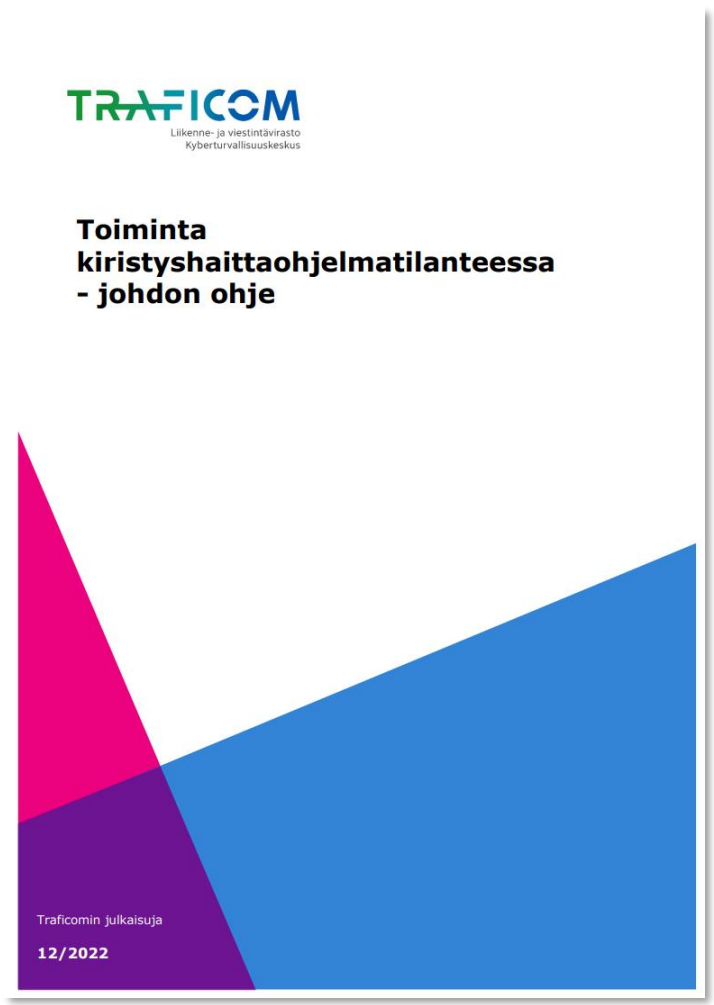


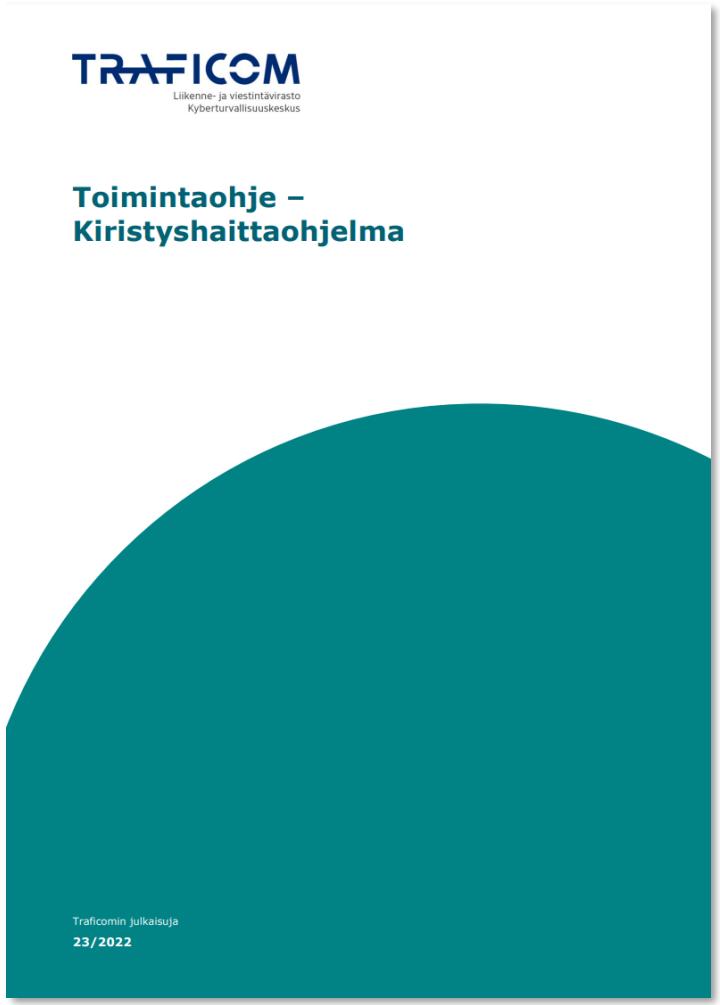
https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

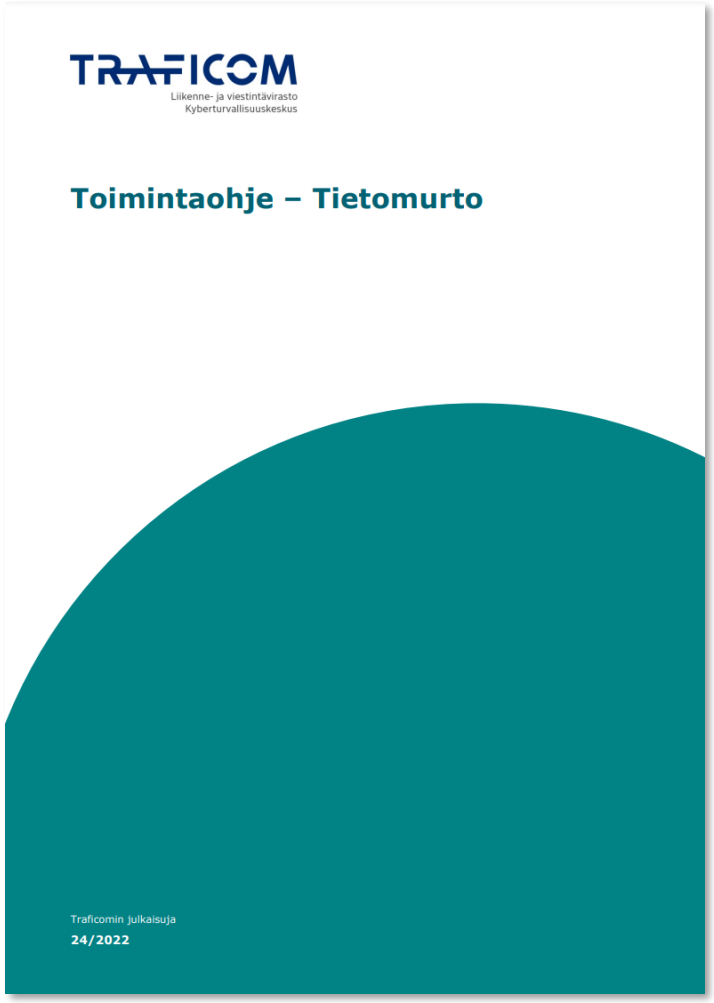
TRAFICOM

TLP:CLEAR

Lukusuositus ... ENNEN tietomurtoa!







https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointimalli

Kybermittarin rakenne ja laskentamalli

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 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

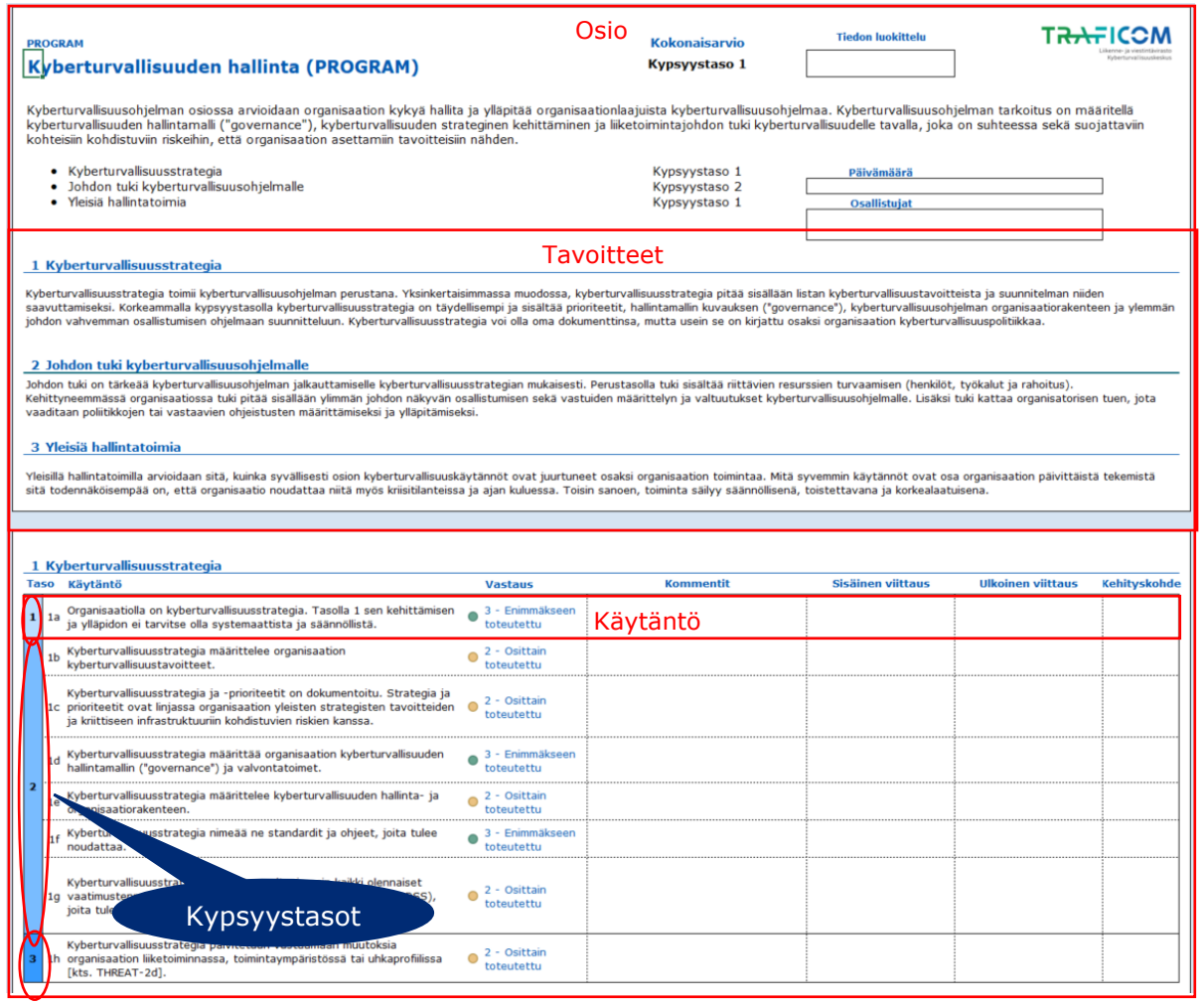
- Arvioinnin kohteen määrittely ohjeet (Summary–välilehti)
- Investointi- ja kustannustietojen välilehti (ei vaikuta kypsyystason laskentaan)

NIST CSF- ja C2M2-dimensiot

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.
- **Jokainen yksittäinen käytäntö on liitetty jollekin kypsyystasoista 1, 2 tai 3.**

Kybermittarin rakenne



- Kybermittari koostuu
  - **Osioista** (yhteensä 11)
  - **Tavoitteista**, joita on osioilla yhteensä (46, hallintatoimia näistä 10)
  - **Käytännöistä**, joiden avulla mitataan tavoitteiden täyttymistä (yhteensä 383)
- 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 toteutettu ja 3) Enimmäkseen toteutettu
  - **Ei Toteutettua** vastaavat 2) Osittain toteuttetu ja 1) Ei toteutettu

Esimerkki kuvaavasta tekstistä (ASSET-2g)

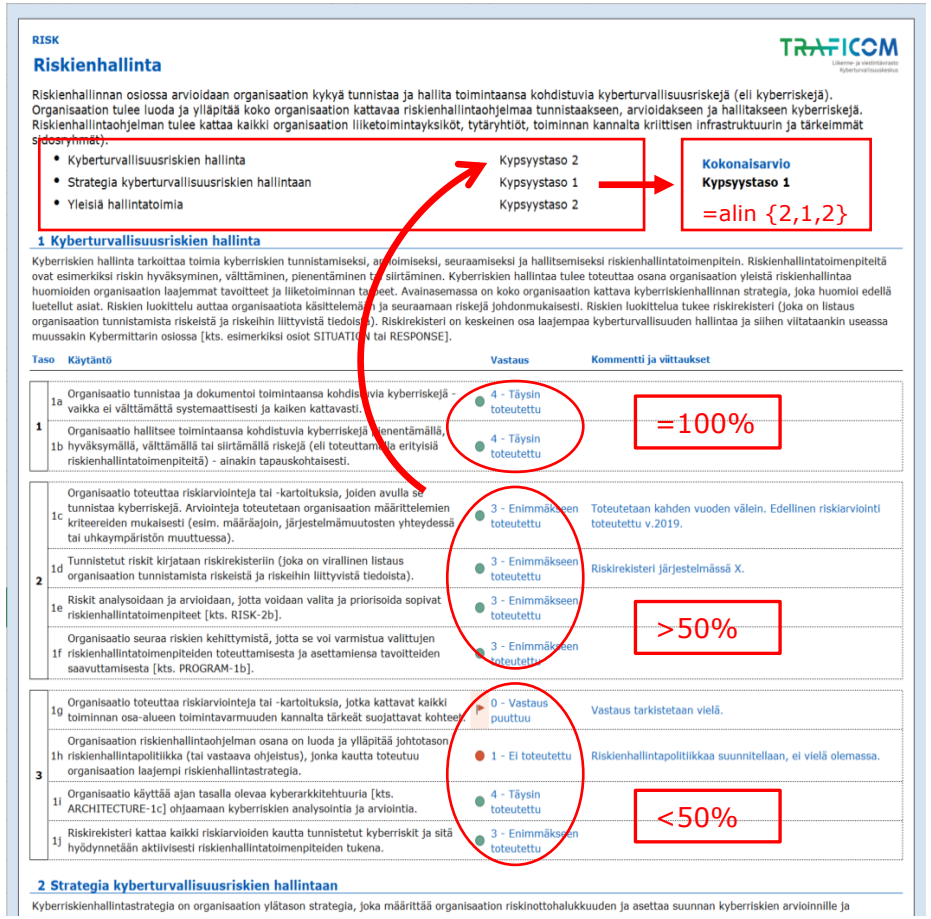
ASSET-2g (MIL 3) The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes

The inventory of information assets should be updated and maintained as assets change throughout their lifecycle to ensure the inventory is complete and accurate. Ensuring that the information asset inventory is current might involve change management procedures that require inventory updates any time assets are significantly altered. The organization might also conduct inventory reviews, both periodically (such as quarterly or yearly) and based on events (such as changes in organizational structure, major changes in critical systems, and the acquisition and consolidation of another business).

Related Practices

· *Progression*: This practice is part of a practice progression. Practice progressions are groups of related practices that represent increasingly complete or more advanced implementations of an activity. The practices in this progression include: ASSET-2a, ASSET-2b, ASSET-2f, ASSET-2g.

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

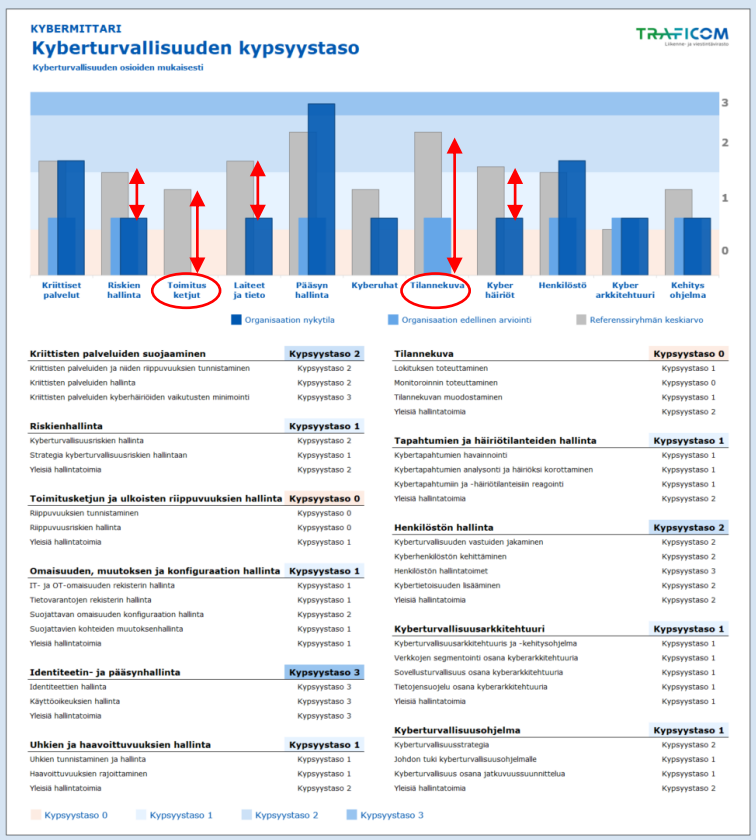
Tavoitteet ja osiot – kypsyystaso

- Osioiden ja tavoitteiden kypsyystason laskennassa käytetään seuraavia sääntöjä:
  - **Taso 0:** kaikki tason 1 käytännöt eivät toteudu kokonaan (*4) Täysin tai 3) Enimmäkseen toteutettu*)
  - **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

Kehitysalueiden tunnistaminen - esimerkiksi näin



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

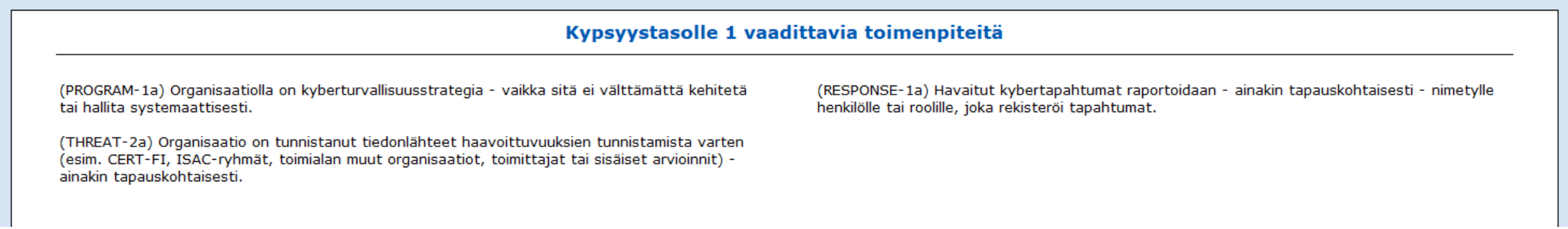
Kyberturvallisuusarkkitehtuuri	Kypsyystaso 1
Kyberturvallisuusarkkitehtuuris ja -kehitysohjelma	Kypsyystaso 1
Verkkojen segmentointi osana kyberarkkitehtuuria	Kypsyystaso 1
Sovellusturvallisuus osana kyberarkkitehtuuria	Kypsyystaso 1
Tietojensuojelu osana kyberarkkitehtuuria	Kypsyystaso 1
Yleisiä hallintatoimia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

- Kybermittarin kypsyysraportista (R2), 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

Kehitysalueiden tunnistaminen - esimerkiksi näin



Kypsyystasolle 1 vaadittavia toimenpiteitä

(PROGRAM-1a) Organisaatiolla on kyberturvallisuusstrategia - vaikka sitä ei välttämättä kehitetä tai hallita systemaattisesti.

(THREAT-2a) Organisaatio on tunnistanut tiedonlähteet haavoittuvuuksien tunnistamista varten (esim. CERT-FI, ISAC-ryhmät, toimialan muut organisaatiot, toimittajat tai sisäiset arvioinnit) - ainakin tapauskohtaisesti.

(RESPONSE-1a) Havaitut kybertapahtumat raportoidaan - ainakin tapauskohtaisesti - nimetylle henkilölle tai roolille, joka rekisteröi tapahtumat.

- Kybermittarin kypsyysraportista (R4):
  - Raportoin alaosasta löytyy osio, jossa on listattu kypsyystasolle 1 vaadittavat käytännöt.
  - Yksittäisen käytännön puuttuminen voi pudottaa koko osion tasolle 0, joten tässä listattujen käytäntöjen toteuttaminen voi nostaa kypsyystasoa merkittävästi.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointiprosessi

Kybermittarin hyödyntämiseen

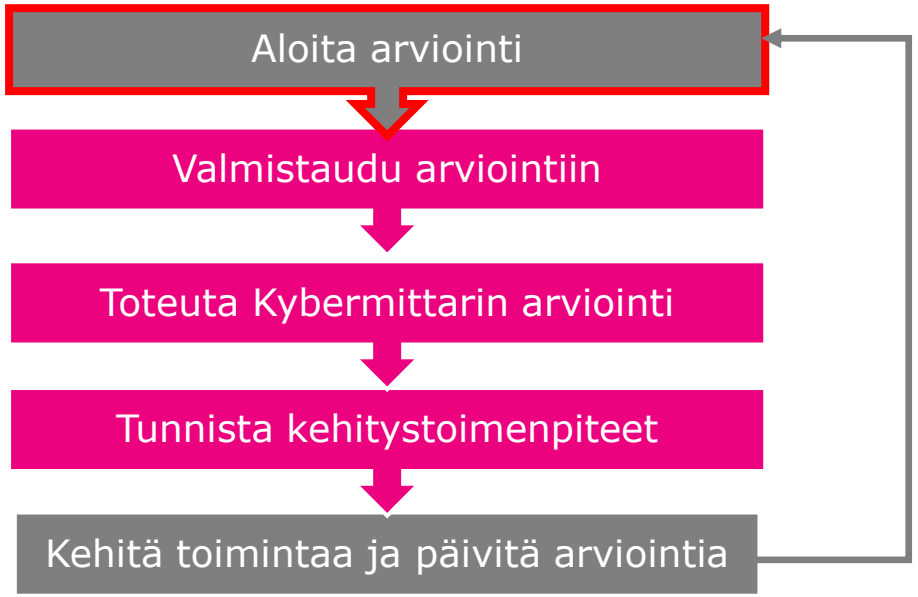
Kybermittarin arviointiprosessi

- 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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Aloita arviointi

Aloita arviointi



- **Osallistujat:**
  - Organisaation johtoryhmä tai muu päätöksentekoelin.
- **Tehtävä:**
  - Tunnistaa tarpeen arvioinnin toteuttamiselle
  - 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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

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 Omaisuuden, muutosten ja konfiguraatioiden hallinta	Tietoturva- ja tietohallintojohtaja yhdessä (*OT omaisuus: lisäksi asiasta vastaavat liiketoiminnan edustajat)
PROGRAM Kyberturvallisuuden hallinta	Tietoturvajohtaja/päällikkö tai muu kyberturvallisuudesta organisaatiossa vastaava henkilö
THIRDPARTY Kumppaniverkoston riskien hallinta	Hankintapäällikkö, riskienhallintapäällikkö, Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä

Kybermittarin osio	Keskeiset roolit
ACCESS Identiteetin ja pääsynhallinta	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
RESPONSE Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus	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 Henkilöstön johtaminen ja kehittäminen	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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toteuta arviointi

Toteuta Kybermittarin arviointi

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

Kybermittarin osiot

ASSET – Omaisuuden, muutoksen ja konfiguraation hallinta

THREAT – Uhkien ja haavoittuvuuksien hallinta

RISK - Riskienhallinta

ACCESS – Identiteetin- ja pääsynhallinta

SITUATION - Tilannekuva

RESPONSE – Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus

THIRD-PARTIES – Kumppaniverkoston riskien hallinta

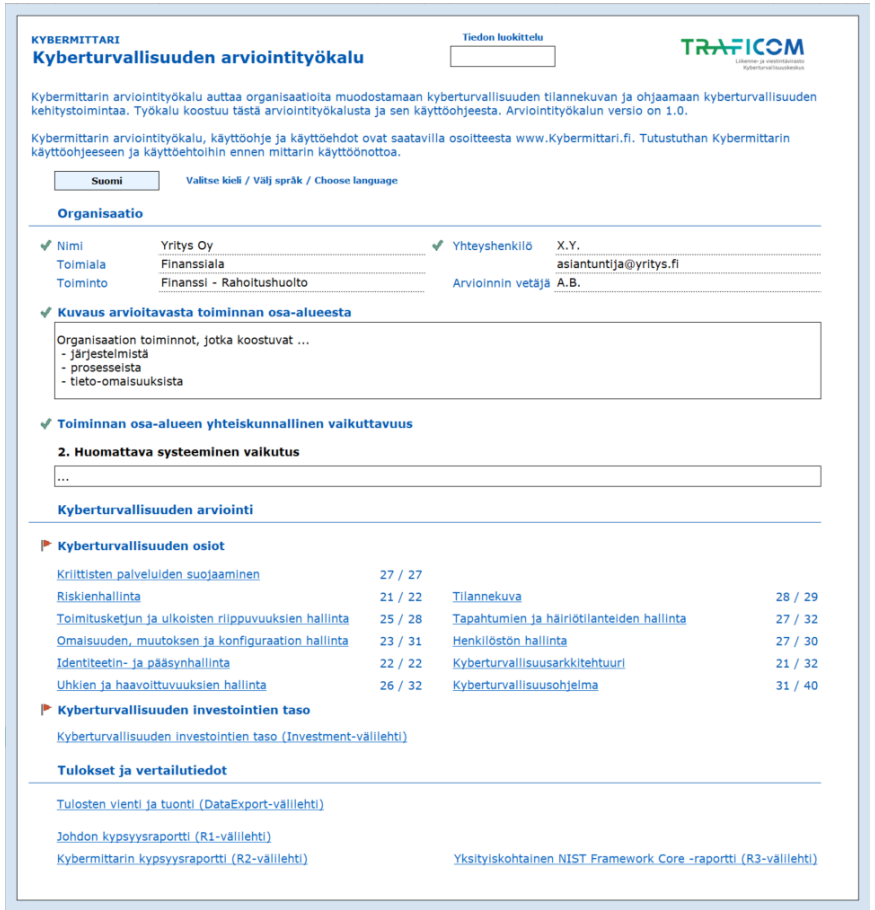
WORKFORCE – Henkilöstön johtaminen ja kehittäminen

ARCHITECTURE - Kyberturvallisuusarkkitehtuuri

PROGRAM – Kyberturvallisuuden hallinta

CRITICAL – Kriittisten palveluiden suojaaminen

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	**Kokonaisarvio**
• Strategia kyberturvallisuusriskien hallintaan	Kypsyystaso 1	**Kypsyystaso 1**
• Yleisiä hallintatoimia	Kypsyystaso 2	

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].

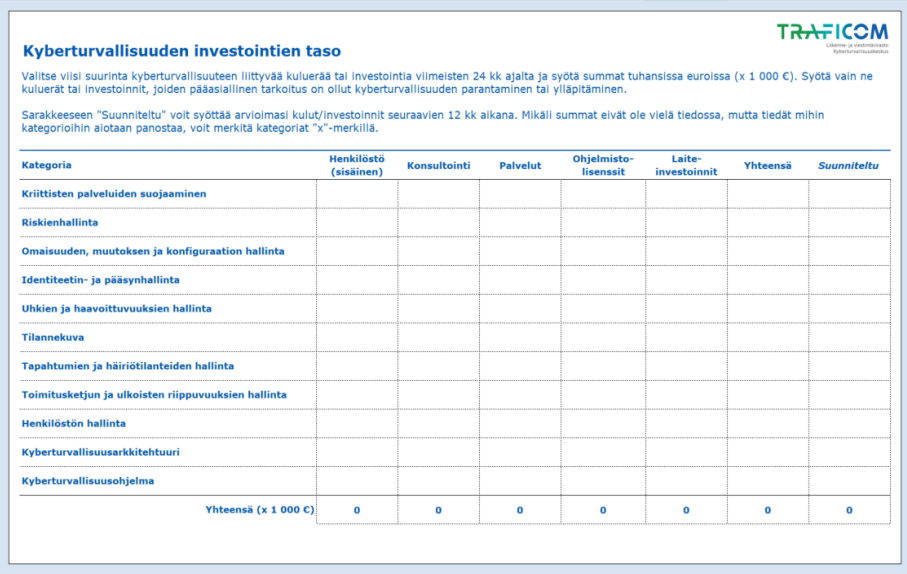
Taso	Käytäntö		Vastaus	Kommentti ja viittaukset
1	1a	Organisaatio tunnistaa ja dokumentoi toimintaansa kohdistuvia kyberriskejä - vaikka ei välttämättä systemaattisesti ja kaiken kattavasti.	4 - Täysin toteutettu	
	1b	Organisaatio hallitsee toimintaansa kohdistuvia kyberriskejä pienentämällä, hyväksymällä, 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
- Välilehden sisältö ei vaikuta raportteihin R1-R7 eikä kerätä vertailutiedoksi

YLEISIÄ HALLINTATOIMIA
Yhteinen tavoite kaikkien osioiden arvioinnissa

- Seuraavat käytännöt arvioidaan erikseen jokaisen osion yhteydessä *(pl. osio CRITICAL)*:
  - a) osioon liittyen on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.
  - B) osion toimintaan on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).
  - c) osion toimintaa ohjataan vaatimuksilla, jotka on asetettu organisaation johtotason politiikassa (tai vastaavassa ohjeistuksessa).
  - d) Osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.
  - e) osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.
  - f) osion toiminnan vaikuttavuutta arvioidaan ja seurataan.
- Mikäli organisaatio noudattaa samoja käytäntöjä läpi koko organisaation tai useammalla kuin yhdellä osa-alueella, voi samoja vastauksia hyödyntää noissa osioissa

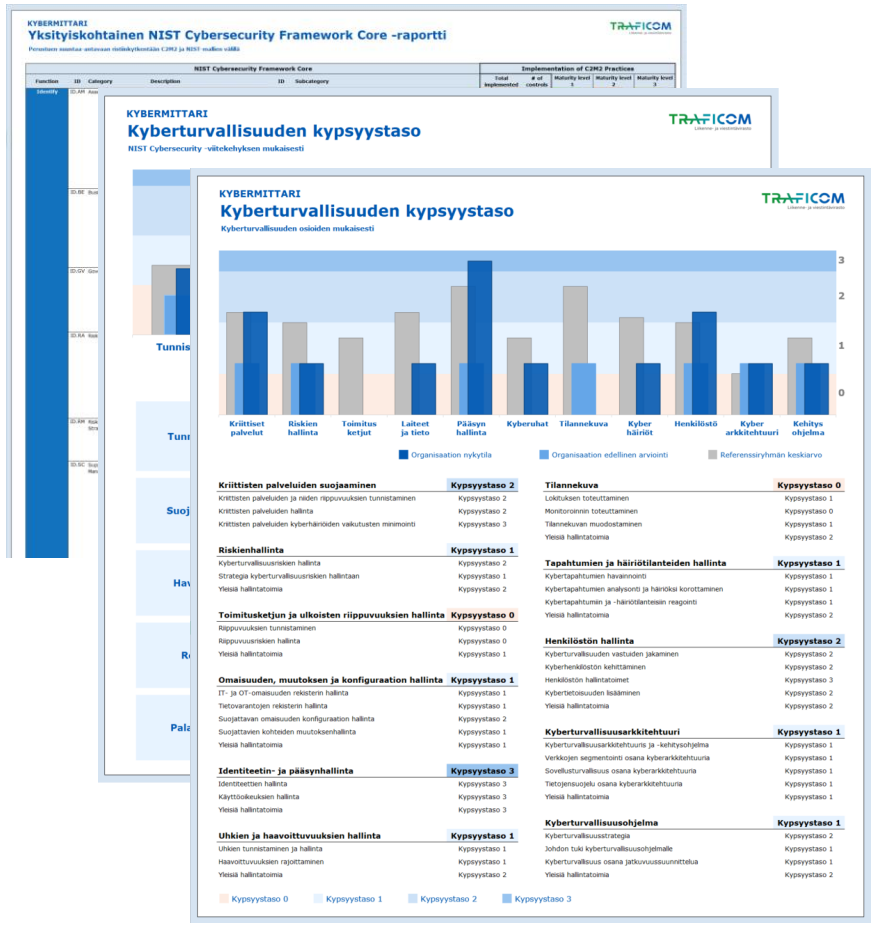
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tunnista kehitystoimen-piteet

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 seitsemän erilaista raporttia kyberturvallisuuden kypsyystasosta
- Raportteja on mahdollista rikastaa vertailutiedolla organisaation aiemmasta arvioinnista tai esimerkiksi viiteryhmän keskiarvotuloksilla

Johdolle suunnattu kypsyysraportti (R1)

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.

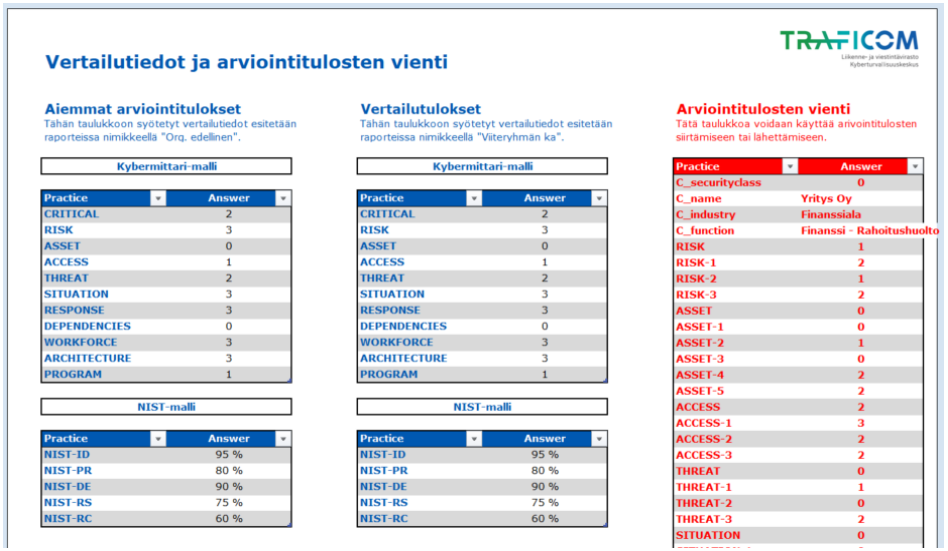
Kybermittarin kypsyysraportti (R2)

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 (R3)

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

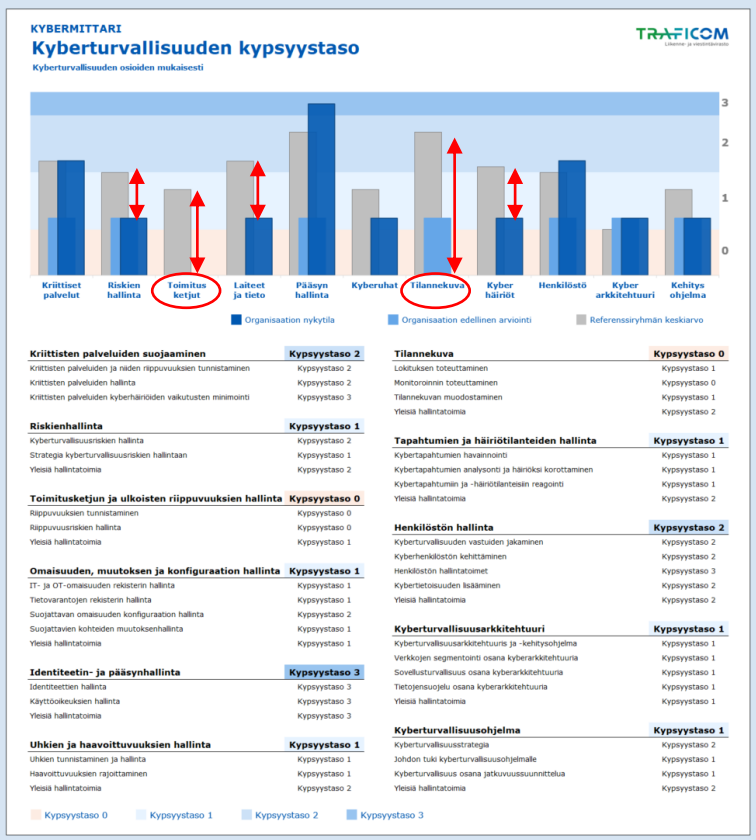
Practice	Answer
NIST-ID	95 %
NIST-PR	80 %
NIST-DE	90 %
NIST-RS	75 %
NIST-RC	60 %

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 (R1 ja R2)
  - Taulukoita on import-välilehdellä kaksi kahta eri käyttötarkoitusta varten
- Arviointitulosten vienti
  - Tulokset on mahdollista viedä työkalusta toiseen kopioimalla vastaukset export-välilehdeltä

Esimerkkejä kehitystoimenpiteiden tunnistamiseen


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
Kybertapahtumin 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

- 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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

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

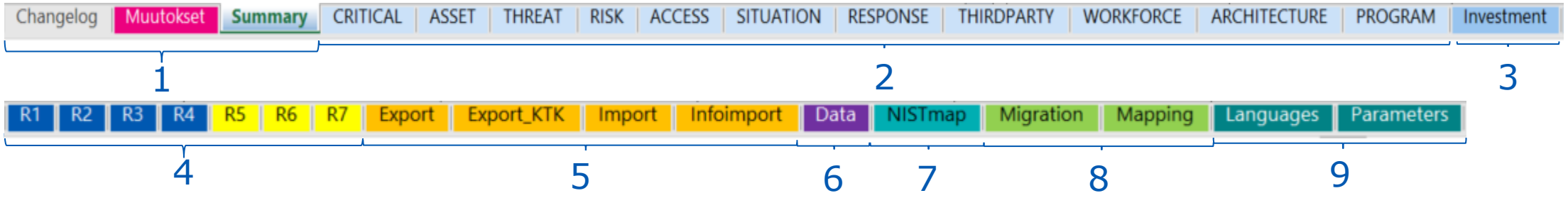
- Arvioinnin päivitys tai uudelleenarviointi tulee ajankohtaiseksi esimerkiksi, kun
  - kehityssuunnitelmat etenevät tai
  - organisaation toimintaympäristö muuttuu
- Kybermittari-työkalu mahdollistaa aikaisempien arviointien vertailun, mikä helpottaa kehitystoimenpiteiden vaikutusten seurantaa ja raportointia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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointityökalu

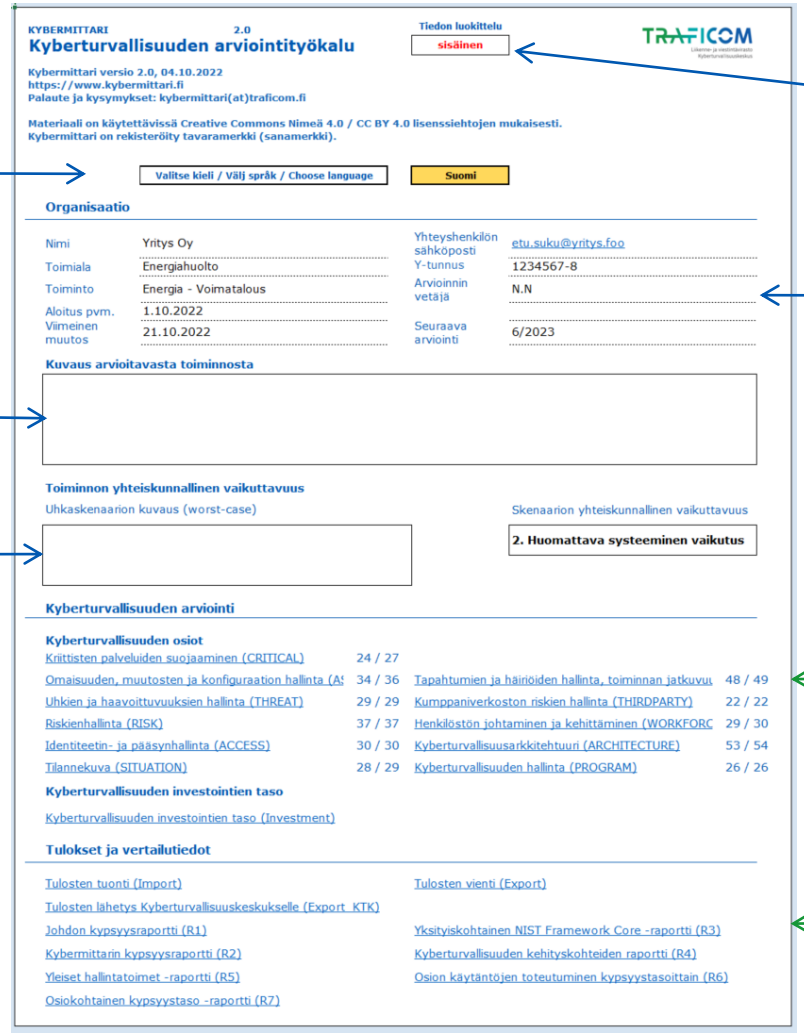
Ohjeita teknisen työkalun hyödyntämiseen

Kybermittarin arviointityökalun rakenne



1. **Taustatiedot sekä muutoshistoria**
2. **Osiokohtaiset välilehdet (11kpl)**
3. **Investoinnit-välilehti**
4. **Raportit**
5. **Tiedon tuonti ja vienti**
6. **Laskentavälilehti**
7. **C2M2 – NIST CSF ristiin viittaus**
8. **V1 – V2 migraatiotyökalu**
9. **Kieliversiot ja muuttujia**

1. Kybermittari-välilehti – yhteenveto


KYBERMITTARI 2.0
Kyberturvallisuuden arviointityökalu
Tiedon luokittelu
sisäinen
TRAFICOM
Kybermittari versio 2.0, 04.10.2022
https://www.kybermittari.fi
Palaute ja kysymykset: kybermittari(at)traficom.fi
Materiaali on käytettävissä Creative Commons Nimeä 4.0 / CC BY 4.0 lisenssiehtojen mukaisesti.
Kybermittari on rekisteröity tavaramerkki (sanamerkki).
Valitse kieli / Välj språk / Choose language
Suomi
Organisaatio
Nimi Yritys Oy
Toimiala Energiahuolto
Toiminto Energia - Voimatalous
Aloitus pvm. 1.10.2022
Viimeinen muutos 21.10.2022
Yhteyshenkilön sähköposti etu.suku@yritys.foo
Y-tunnus 1234567-8
Arvioinnin vetäjä N.N
Seuraava arviointi 6/2023
Kuvaus arvioitavasta toiminnosta
Toiminnon yhteiskunnallinen vaikuttavuus
Uhkaskenaarion kuvaus (worst-case)
Skenaarion yhteiskunnallinen vaikuttavuus
2. Huomattava systeeminen vaikutus
Kyberturvallisuuden arviointi
Kyberturvallisuuden osiot
Kriittisten palveluiden suojaaminen (CRITICAL) 24 / 27
Omaisuuden, muutosten ja konfiguraation hallinta (A 34 / 36
Uhkien ja haavoittuvuuksien hallinta (THREAT) 29 / 29
Riskienhallinta (RISK) 37 / 37
Identiteetin- ja pääsynhallinta (ACCESS) 30 / 30
Tilannekuva (SITUATION) 28 / 29
Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvu 48 / 49
Kumppaniverkoston riskien hallinta (THIRDPARTY) 22 / 22
Henkilöstön johtaminen ja kehittäminen (WORKFORC 29 / 30
Kyberturvallisuusarkkitehtuuri (ARCHITECTURE) 53 / 54
Kyberturvallisuuden hallinta (PROGRAM) 26 / 26
Kyberturvallisuuden investointien taso
Kyberturvallisuuden investointien taso (Investment)
Tulokset ja vertailutiedot
Tulosten tuonti (Import)
Tulosten lähetys Kyberturvallisuuskeskukselle (Export_KTK)
Johdon kypsyysraportti (R1)
Kybermittarin kypsyysraportti (R2)
Yleiset hallintatoimet -raportti (R5)
Osiokohtainen kypsyystaso -raportti (R7)
Tulosten vienti (Export)
Yksityiskohtainen NIST Framework Core -raportti (R3)
Kyberturvallisuuden kehityskohteiden raportti (R4)
Osion käytäntöjen toteuturninen kypsyystasoittain (R6)

Kielivalinta

Toiminnan osa-alue

Yhteiskunnallinen vaikuttavuus

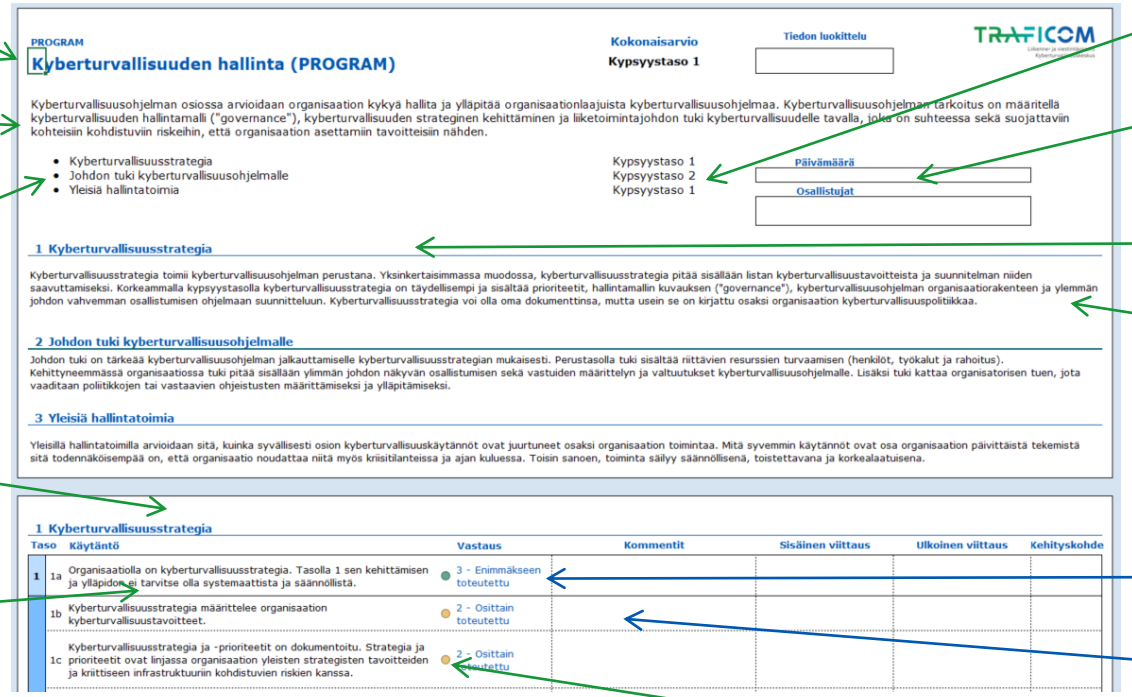
Tiedon luokittelu

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

Tavoitteiden kypsyystasot

Osion kypsyystaso

Tavoitteen nimi

Tavoitteen kuvaus

Vastaus (1-4 tai 0)

Kommentti ja viittaus

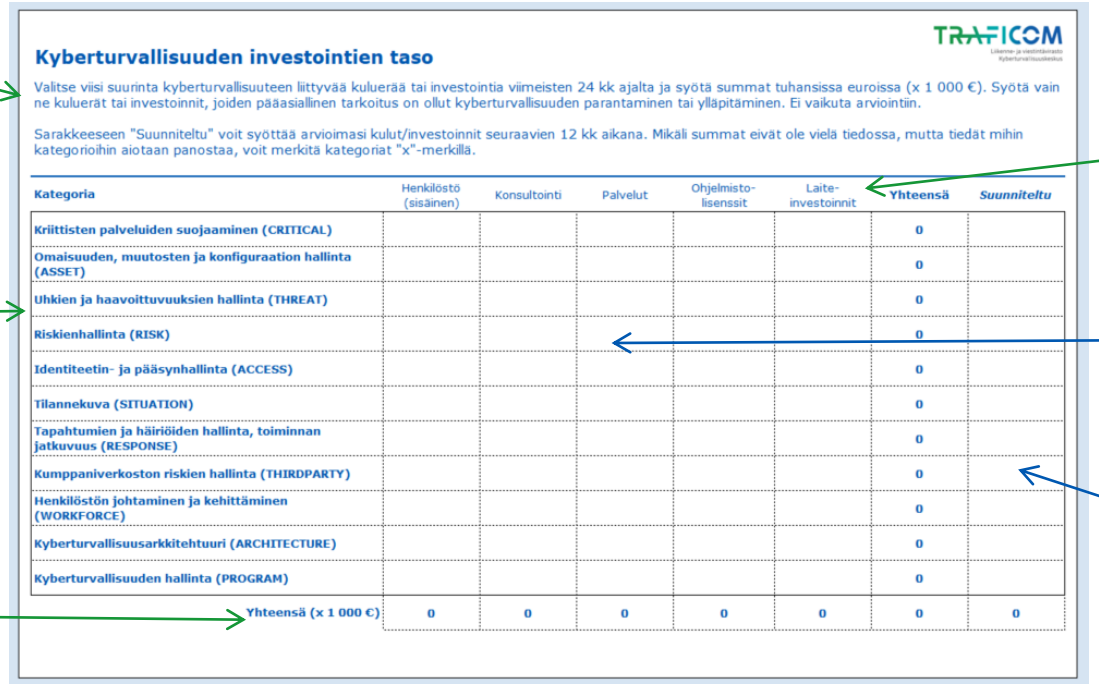
Vastauksen indikaattori

3. Kyberturvallisuuden investoinnit -välilehdet

Lyhyt ohjeistus

Kybermittarin osiot

Summat



Kyberturvallisuuden investointien taso

TRAFICOM

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. Ei vaikuta arviointiin.

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 (CRITICAL)						0	
Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)						0	
Uhkien ja haavoittuvuuksien hallinta (THREAT)						0	
Riskienhallinta (RISK)						0	
Identiteetin- ja pääsynhallinta (ACCESS)						0	
Tilannekuva (SITUATION)						0	
Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus (RESPONSE)						0	
Kumppaniverkoston riskien hallinta (THIRDPARTY)						0	
Henkilöstön johtaminen ja kehittäminen (WORKFORCE)						0	
Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)						0	
Kyberturvallisuuden hallinta (PROGRAM)						0	
Yhteensä (x 1 000 €)	0	0	0	0	0	0	0

Investointilajit

Tehdyt investoinnit (24 kk)

Tulevat investoinnit (12 kk)

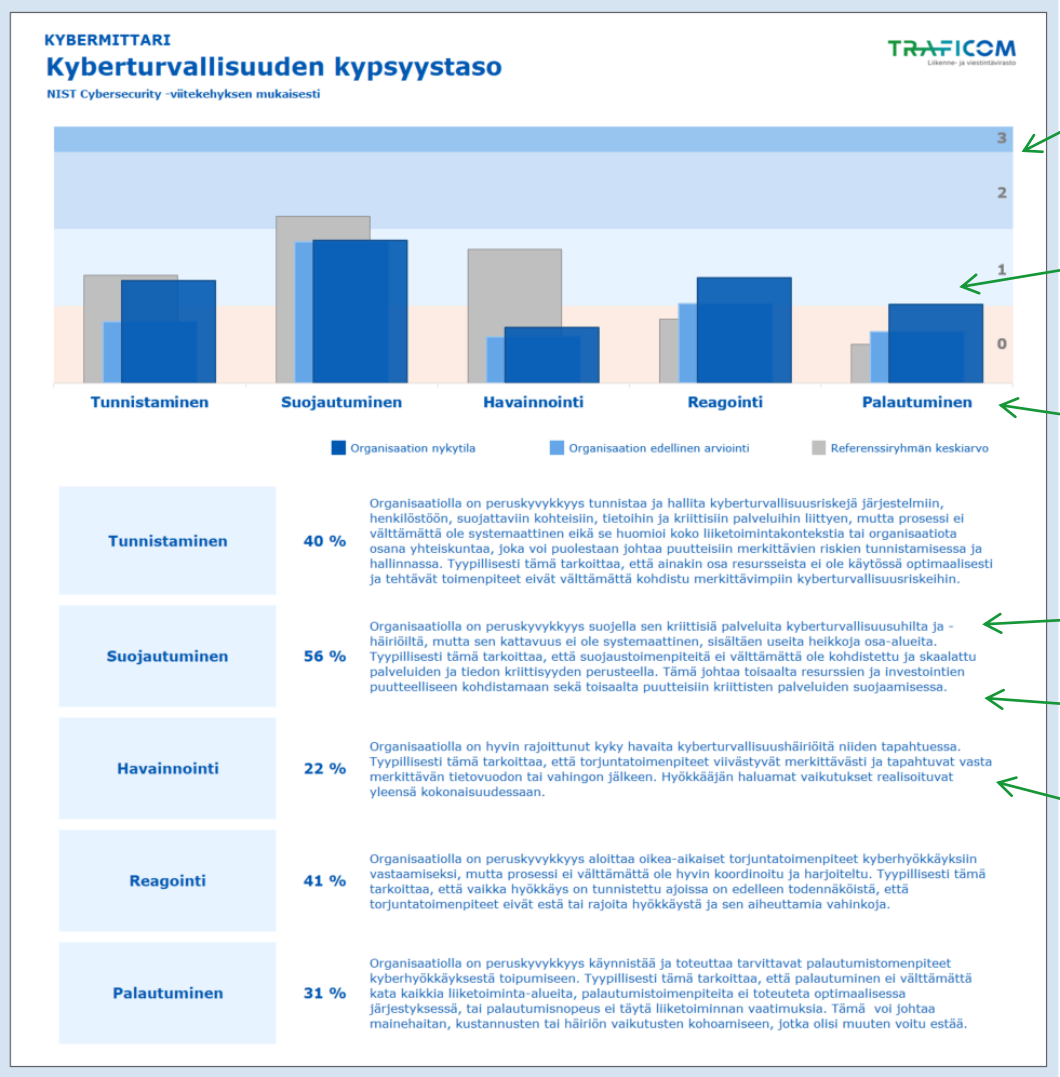
4. Raportoinnin sisältö ja merkittävät muutokset

- R1: taustalla oleva NIST CSF – Kybermittari ristiin viittaus päivitetty
- R2: päivitetty
- R3: taustalla oleva NIST CSF – Kybermittari ristiin viittaus päivitetty
- R4: Toteutumattomat tason yksi käytännöt on erotettu omaksi raportikseen. Oli ennen R2:n lopussa.

4. Raportointi, uudet

- R5: Kaavio esittää koosteen kymmenen osion lopussa arvioiduista hallintatoimista.
- R6: Kaaviot esittävät prosentuaalisen yhteenvedon käytäntöjen toteutumisesta osioittain sekä sen mukaan, mille kypsyystasolle käytäntö on sijoitettu.
- R7: Kaaviot esittävät yhteenvedon käytäntöjen arvionnista niinkuin ne on arvioitu neliportaisella asteikolla sekä osioittain että sen mukaan, mille kypsyystasolle käytäntö on sijoitettu.
- Jokaiseen raporttiin on lisätty ohjeita oikeaan yläkulmaan

4. R1 NIST CSF ristiinviittaus



Kypsyysasteikko 0-3

Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

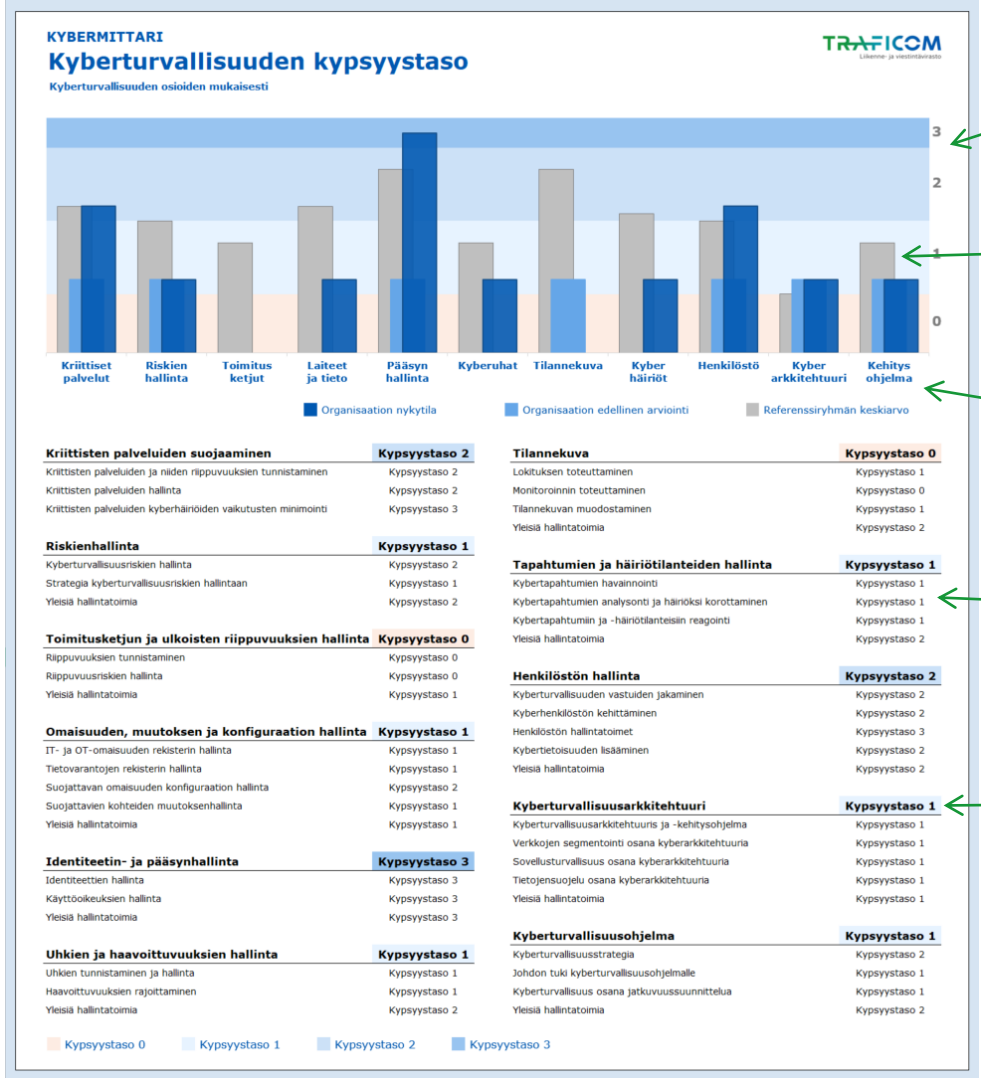
NIST CSF 5 osa-aluetta

Osa-alue

Toteutuneiden käytäntöjen osuus (%)

Sanallinen kuvaus kypsyystasosta

4. R2 Kyberturvallisuuden kypsyystaso



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

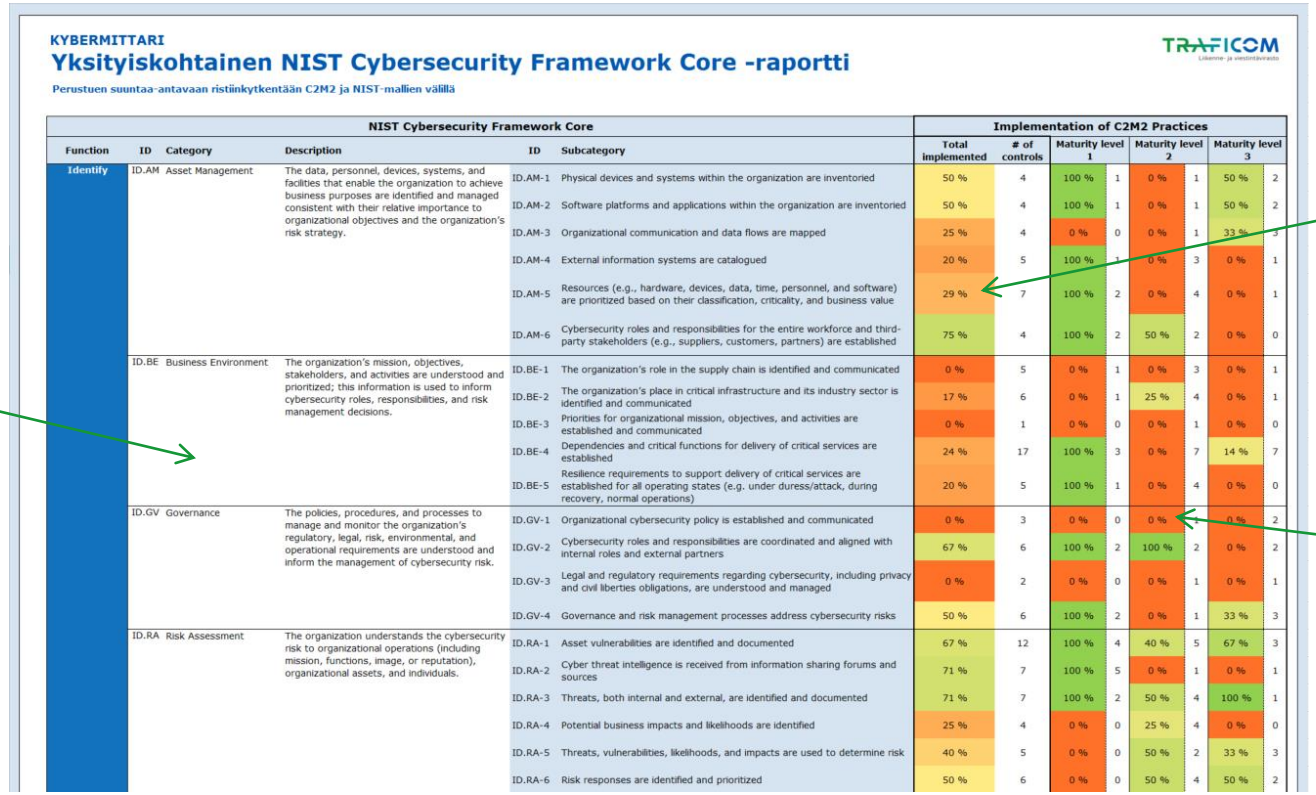
Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

Kybermittarin 11 osa-aluetta

Yksityiskohtaisemmin
- Osiot
- Tavoitteet

Osion tai tavoitteen kypsyystaso

4. R3 Yksityiskohtainen NIST Cybersecurity Framework Core -raportti



KYBERMITTARI

Yksityiskohtainen NIST Cybersecurity Framework Core -raportti

TRAFICOM

Perustuen suuntaa-antavaan ristiinkytkentään C2M2 ja NIST-mallien välillä

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 %	2	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

NIST CSF Osa-alueet ja tavoitteet

Käytäntöjen määrä ja toteutumisprosentti

(kokonaisuudessaan)

Käytäntöjen määrä ja toteutumisprosentti

(jaettuna kypsyystasojen mukaisesti)

4. R5 Yleiset hallintatoimet, yhteenveto

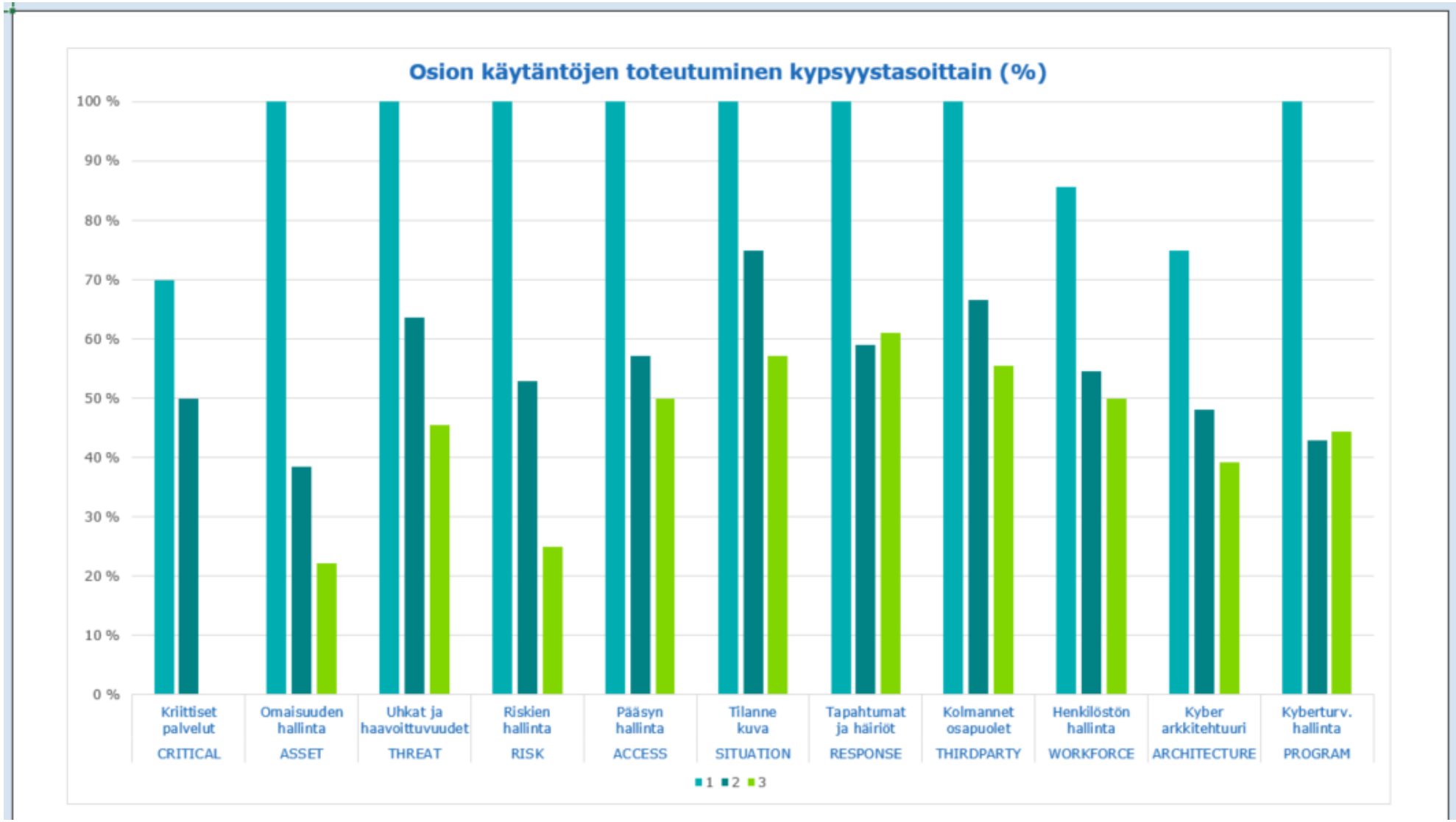
KYBERMITTARI

Yleiset hallintatoimet

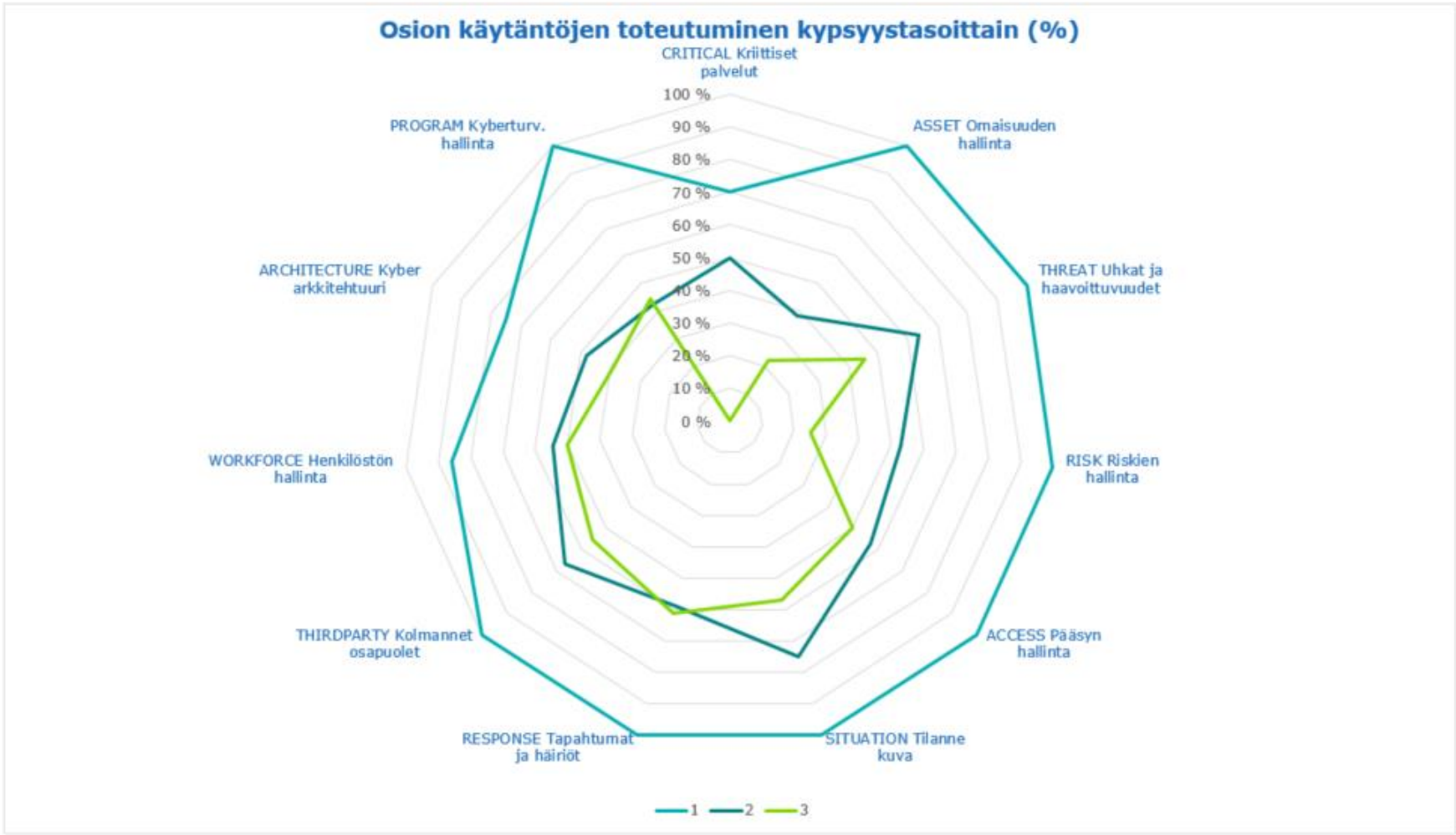
Selite:	0 - Vastaus	1 - Ei toteutettu	2 - Osittain toteutettu	3 - Enimmäkse	4 - Täysin toteutettu

Osio	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRDPARTY	WORKFORCE	ARCHITECTURE	PROGRAM
Yleisiä hallintatoimia -osan järjestysnumero	5	3	5	4	4	5	3	5	6	3
a Osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.	2	2	3	3	2	3	3	3	2	2
b Osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).	3	2	3	2	3	2	3	0	2	2
c Osion toimintaa ohjataan vaatimuksilla, jotka on asetettu organisaation johtotason politiikassa (tai vastaavassa ohjeistuksessa).	3	2	3	3	3	3	3	1	2	3
d Osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.	2	3	2	2	2	4	1	3	3	2
e Osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.	2	3	3	3	3	2	3	3	2	3
f Osion toiminnan vaikuttavuutta arvioidaan ja seurataan.	3	3	2	1	3	3	2	2	2	2

R6


Osion käytäntöjen toteutuminen kypsyystasoittain (%)
100 %
90 %
80 %
70 %
60 %
50 %
40 %
30 %
20 %
10 %
0 %
Kriittiset palvelut
CRITICAL
Omaisuuden hallinta
ASSET
Uhkat ja haavoittuvuudet
THREAT
Riskien hallinta
RISK
Pääsyn hallinta
ACCESS
Tilanne kuva
SITUATION
Tapahtumat ja häiriöt
RESPONSE
Kolmannet osapuolet
THIRDPARTY
Henkilöstön hallinta
WORKFORCE
Kyber arkkitehtuuri
ARCHITECTURE
Kyberturv. hallinta
PROGRAM
1 2 3

R6

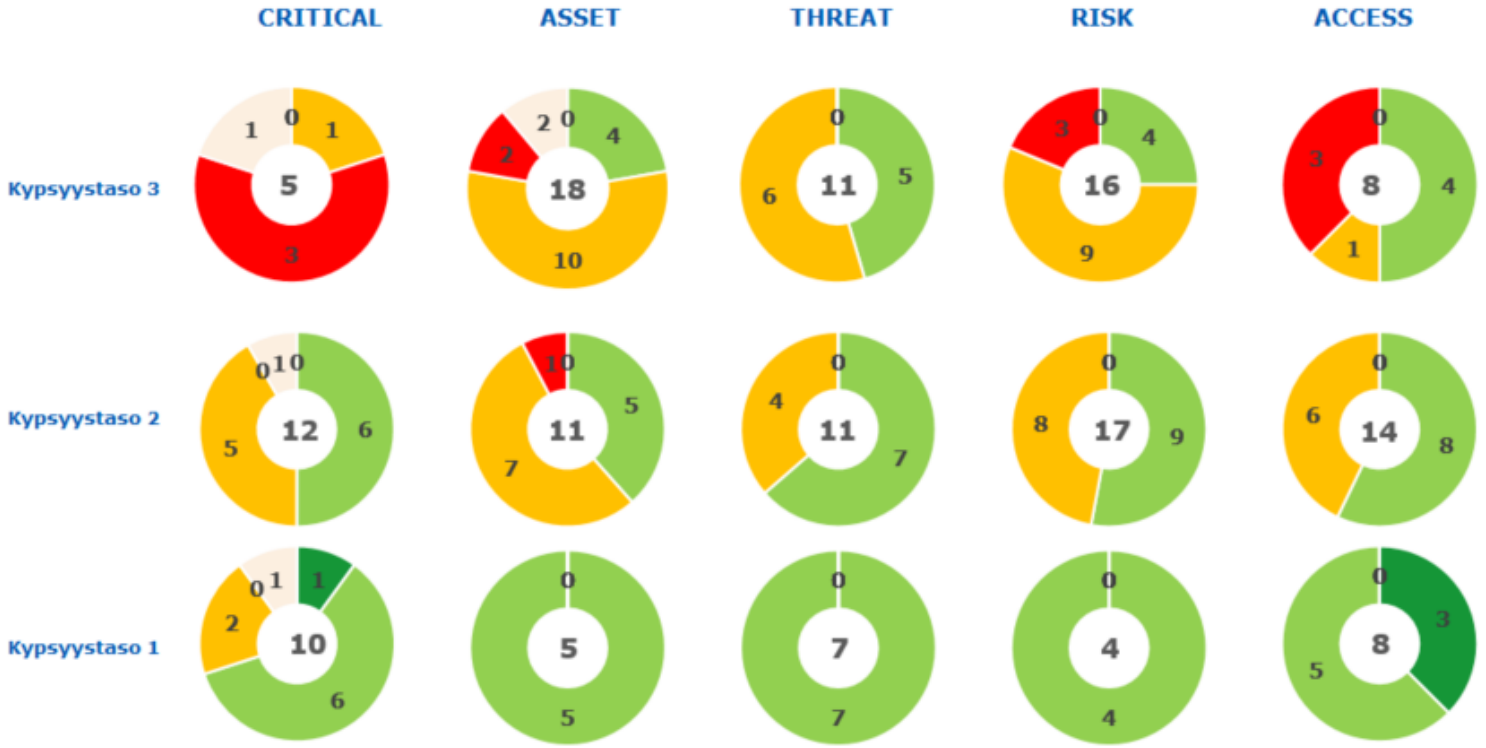

Osion käytäntöjen toteutuminen kypsyystasoittain (%)
CRITICAL Kriittiset palvelut
ASSET Omaisuuden hallinta
THREAT Uhkat ja haavoittuvuudet
RISK Riskien hallinta
ACCESS Pääsyn hallinta
SITUATION Tilanne kuva
RESPONSE Tapahtumat ja häiriöt
THIRDPARTY Kolmannet osapuolet
WORKFORCE Henkilöstön hallinta
ARCHITECTURE Kyber arkkitehtuuri
PROGRAM Kyberturv. hallinta
100 %
90 %
80 %
70 %
60 %
50 %
40 %
30 %
20 %
10 %
0 %
1
2
3

R7

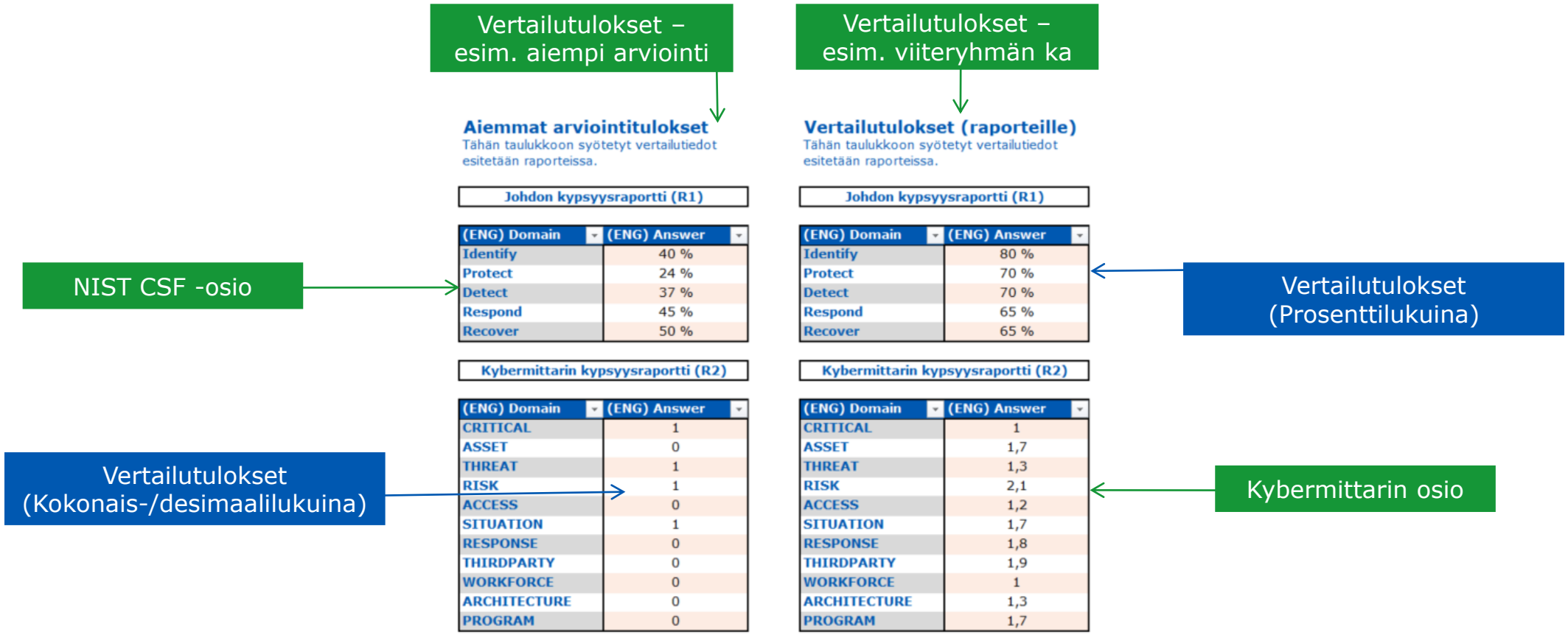
KYBERMITTARI

Osiokohtainen kypsyystasoraportti

Selite:	0 - Vastaus puuttuu	1 - Ei toteutettu tai ei tietoa	2 - Osittain toteutettu	3 - Enimmäkseen toteutettu	4 - Täysin toteutettu



5. Import-välilehti



Muut Kybermittarin toiminnallisuuksiin liittyvät välilehdet

- Data
  - Kypsyystasojen koonti- ja laskentasivu
- NISTMap
  - Kybermittarin / C2M2 –mallien ja NIST CSF –mallien välinen ristiin kytkentä
- Migration ja Mapping
  - V1 -> V2 siirto
- Languages
  - Selitetekstien kieliversiot (FI, SE, EN)
- Parameters
  - Työkalun käyttämät vaihtoehdot ja säätöparametrit