Kyber-mittari

Kansallinen kyberuhkilta suojaavien kyvykkyyksien kypsyystason arviointi- ja kehittämismalli

kybermittari.fi
kybermittari@traficom.fi

PALVELUT ORGANISAATIOILLE

Kybermittari

kybermittari.fi, kybermittari@traficom.fi

Miten suojaudutte kyberuhilta ja varmistatte liiketoiminnan jatkuvuuden häiriötilanteissa?

Ilmainen työkalu

kyberkyvykkyyksien selvittämiseen ja hallintaan

Johdolle ja tietoturva-ammattilaisille

yrityksissä ja organisaatioissa

Tiedolla johtamiseen

- tilannekuva omasta tietoturvasta
- kyberkyvykkyyksien arviointi ja vuotuinen seuraaminen
- kehityskohteiden tunnistaminen
- tavoitteiden asettaminen
- resurssien kohdentaminen
- oman tilanteen vertaaminen alan yleiseen tasoon

Kyberturvallisuus on...

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

Miksi turvallisuutta pitäisi arvioida?

- Millainen turvallisuustaso on ?
- Onko tulos parempi kuin edellisellä kerralla?
- Onko turvallisuusresursointi sopivalla tasolla?
- Kuinka hyvällä tasolla turvallisuus on verrattuna muihin?
- Mitä riskinsiirtovaihtoehtoja on?

- Vaatimustenmukaisuus (E-ITS, GDPR, NIS2, välttämättömät palvelut jne.)
- Edistys
- Haavoittuvuuksien tuntemus ja riskien hallinta
- Epävarmuuksien vähentäminen
- Kumppaneihin luottaminen
- Suunnittelun tukitoimet (kansallisella tasolla)
- Budjetointi

Hubbard, D.W., Seiersen, R., How to measure anything in cybersecurity risk, (2014)

Tärkein tietoturvateko on tiedostaa, mitkä ovat yrityksen tuotannolliset 'kruununjalokivet', mikä on niiden nykyinen tietoturvallisuuden taso ja mitä tulisi kehittää?

Tämän jälkeen pitäisi myös viedä läpi tarvittavat kehitystoimet,

ja pystyä osoittamaan, että yritys on tehnyt riittävät riskiperustaiset toimenpiteet.

”Puutteet perustason käytännöissä aiheuttavat edelleen valtaosan poikkeamista, jotka liittyvät tietoturvaan”.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Yleistä kypsyysmalleista

Tärkeimmät käsitteet

- **Kypsyysmalli** tarkoittaa mallia, jossa toimintaa tarkastellaan tasoina tai askelmina, joita kiivetään ylöspäin kohti järjestelmällisempää ja kehittyneempää toimintaa.
- **Kypsyystasot** on määritelty tavoittein tai vaatimuksin, jotka arvioinnin kohteena olevan toiminnan tulisi kyseisellä kypsyystasolla täyttää.
- **Kyvykkyys** tarkoittaa kykyä toimia tarkoituksenmukaisella tavalla tietyllä osa-alueella ja hyödyntää osaamistaan sekä resurssejaan, jotta tavoitteet saavutettaisiin.
- **Käytännöt** edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuuden menettelytapoja jotka voivat perustua esim. standardeihin tai lakiin
- **Arvioitavat toiminnot** on Kybermittarin yhteydessä käytetty käsite, jolla tarkoitetaan niitä organisaation tai yhteiskunnan kannalta tärkeitä/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.
- **Jokainen yksittäinen käytäntö on liitetty jollekin kypsyystasoista 1, 2 tai 3.**

Kypsyysarvioinnin suuntaukset

- Miksi – avaintekijät
  - Vaatimuksenmukaisuus
  - Kyberturvallisuusuhkien sietokyky
  - Tietosuoja
  - Riskien hallinta ja vähentäminen
  - Poikkeamanhallintavalmius
  - Investoinnit kyberturvallisuuteen
  - Turvallisuuskulttuurin vahvistaminen
  - Liiketoiminnan jatkuvuuden varmistaminen
  - Kustannustehokkaat tietoturvaratkaisut
- Päähaasteet
  - Resurssikapeikot (suunniteltu suuremmille organisaatioille)
  - Mallien monimutkaisuus
  - Räätälöinti tietyille aloille
  - Käytännön opastuksen puute
  - Kulttuurilliset ja inhimilliset tekijät (tietoisuus, muutosvastarinta)
  - Yhdenmukaistaminen liiketoiminnan tavoitteiden kanssa
  - Automaation ja työkalujen tuen puute
  - Epäjohdonmukainen metriikka ja arviointi (standardisointi vertailuarvojen tarjoamiseksi, vertailukelpoisuus)
  - Integrointi olemassa oleviin järjestelmiin
  - Taloudelliset esteet
  - Rajoitettu tuki/soveltuvuus uusille teknologioille
  - Aikaa vievä arviointi

Kybermittari kypsyysarvioinnin välineenä

Edut

- Perusta systemaattiselle mittaamiselle ja seurannalle
- Raportointi päätöksenteon tueksi, tukee kehitysohjelman toteutusta ja seurantaa
- Vuorovaikutus, yhteinen kieli
- Toistettavissa oleva
- Toimittajariippumaton
- Vertailutietoa

Pohdittavaa

- Toimiala- ja yrityskohtainen tulkinta
- Itsearvioinnin objektiivisuus ja vertailtavuus. Miten välttää kognitiiviset vinoumat arvionnissa
- Korrelaatio vai syy–vaikutussuhde
- Miten hyödyntää tietoa tehokkaasti hyödyntäminen päätöksenteossa?
- Mikä on tavoiteltava kypsyystaso? Riskiperustaisuus vs kypsyystaso

Pari toimintaohjeita kognitiivisten vinoumien välttämiseksi

Arviointien onnistumiseen vaikuttaa useita tekijöitä. Yksi huomioitava tekijä on erilaiset vinoumat, jotka vaikuttavat arvioinnin luotettavuuteen.

- **Käytä tiimiä**: Varmista, että kysymyksiin vastaa ryhmä ihmisiä, joilla on erilaisia näkemyksiä organisaation kyberturvallisuudesta.
- **Arvioi objektiivisesti**: Pohdi jokaista vastausta faktojen, ei tunteiden tai aiempien uskomusten pohjalta.
- **Tarkista priorisointi**: Suuntaa resurssit sinne, missä on eniten riskejä tai kehittämistarpeita, ei sinne, missä asiat ovat jo hyvällä mallilla.
- **Päivitä säännöllisesti**: Toista Kybermittarin käyttö esimerkiksi kerran vuodessa ja hyödynnä aiempien arvioiden kehitystä peilinä nykyhetkelle.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Johdanto aiheeseen

Kybermittarin tausta ja tarkoitus

PALVELUT ORGANISAATIOILLE

Kybermittari

kybermittari.fi, kybermittari@traficom.fi

Miten suojaudutte kyberuhilta ja varmistatte liiketoiminnan jatkuvuuden häiriötilanteissa?

Ilmainen työkalu

kyberkyvykkyyksien selvittämiseen ja hallintaan

Johdolle ja tietoturva-ammattilaisille

yrityksissä ja organisaatioissa

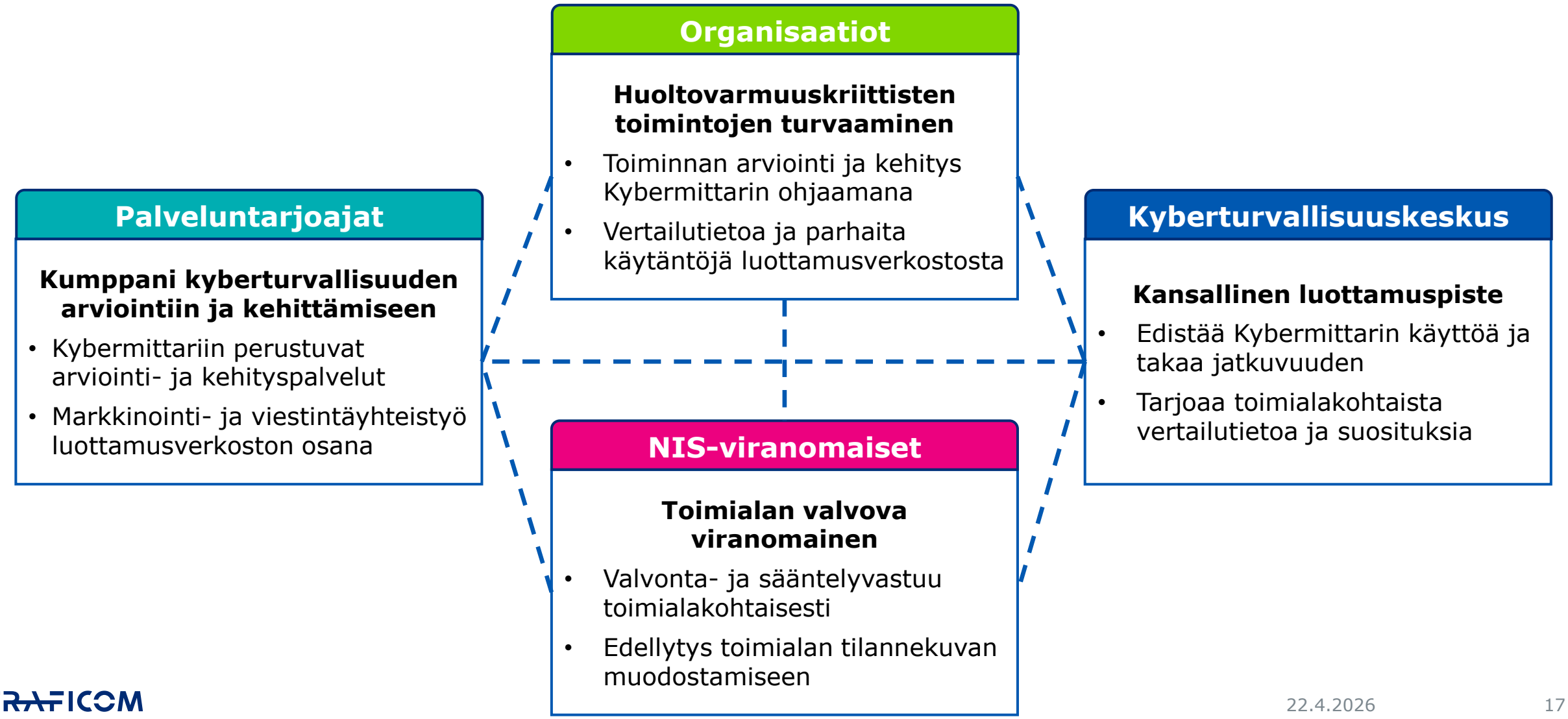
Tiedolla johtamiseen

- tilannekuva omasta tietoturvasta
- kyberkyvykkyyksien arviointi ja vuotuinen seuraaminen
- kehityskohteiden tunnistaminen
- tavoitteiden asettaminen
- resurssien kohdentaminen
- oman tilanteen vertaaminen alan yleiseen tasoon

Sisäänrakennettu turvallisuus – Kybermittari auttaa

- Turvallisuuden tulisi olla sisäänrakennettua ja osa organisaation prosesseja (Secure by Design)
- Organisaatiossa tulisi hyödyntää erilaisia kyberturvallisuuden viitekehyksiä
  - Riskienhallinta
  - Tietoturvallisuuden hallinta
  - Tietoturvakontrollit
  - Liiketoiminta-arkkitehtuuri
- Kypsyysmalli auttaa seuraamaan ja todentamaan organisaation tietoturvatavoitteiden toteutumista

Kybermittarin luottamusverkosto



Kybermittari

- Kansallinen kyberkyvykkyyksien **kypsyystason arviointi- ja kehittämismalli**
- Kybermittari **auttaa organisaatioita arvioimaan ja kehittämään kyvykkyyttään** suojautua kyberuhilta ja parantaa toimintansa kyberturvallisuutta.
- Kybermittari antaa **vertailutietoa ja helpottaa yhteistyötä sekä tiedonjakoa** verkostoissa.
- Tietoturvastandardit edellyttävät että tietoturvan kehittymistä **mitataan**. Kybermittari hoitaa tämä osan riippumatta käytössä olevasta viitekehyksestä.
- Kerätty vertailutieto auttaa **kansallisen tilannekuvan muodostamisessa** ja investointien kohdentamisessa

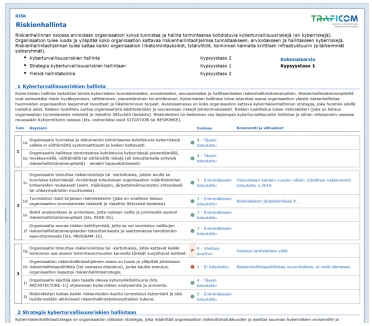
Kenelle Kybermittari on tarkoitettu?

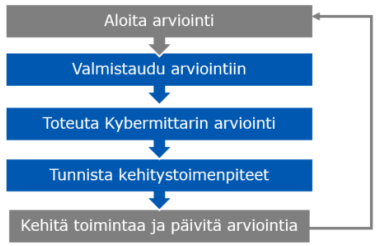
- Kybermittari on tarkoitettu kaikille organisaatioille, jotka tarvitsevat **toimintansa kehittämisen ja päätöksenteon tueksi mitattua tietoa** organisaation kyvystä ehkäistä, havaita, reagoida ja palautua kyberturvallisuuspoikkeamista.
- Organisaatioille, jotka haluavat toimialan vertailutietoa ja osallistua **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.

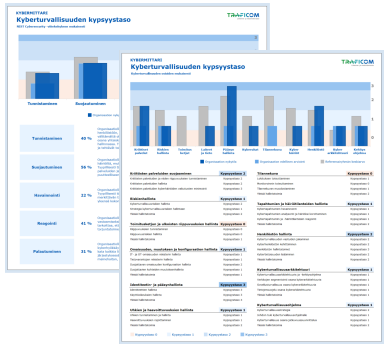
Kybermittari-palvelun tarkoitus

- 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.

Kybermittarin materiaalit







- Arviointityökalu
  - Kohteena esimerkiksi organsaation koko toiminta tai ydinliiketoiminnalle ja/tai yhteiskunnalle kriittiset toiminnot;
  - Käytännöt kattavat yleisimmät kyberturvallisuuden riskienhallinnan osa-alueet;
  - Tuottaa automaattisesti raportteja kypsyystasosta ja kehityskohteista
- Ohjeistus ja tuki arviointiprosessiin
  - Organisaation itse toteuttamana tai ulkoisen palveluntarjoajan tukemana.
- Muuta tukimateriaali
  - Erilaisia tuki ja tiedon rikastus materiaaleja eri käyttötapauksiin
  - Myös taustalla olevien viitekehysten (C2M2 ja NIST CSF) materiaalit soveltuvat

Kybermittarin 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 ehdot, tarkemmin

Kybermittarin käyttöehdot, palvelunkuvaus ja markkinointiehdot

Kybermittarin käyttöehdot, palvelunkuvaus ja markkinointiehdot

- Kybermittari - käyttöehdot (pdf, 113,49 Kt)
- Kybermittari - palvelukuvaus (pdf, 231,11 Kt)
- Kybermittari - markkinointiehdot (palveluntarjoajille) (pdf, 143,51 Kt)

Lisätietoa

Kybermittari.fi –sivusto

- **Kybermittarin työkalut ja tuki**
- **Palveluntarjoajat**, jotka ovat ilmoittaneet tarjoavansa tukipalveluita Kybermittarin käyttöön
- **Yhteystiedot ja palautekanavat**

TRAFICOM

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ristiinviittaus, vertailutieto ja import-ominaisuudet

Tuontiominaisuudet

- Kybermittarissa on toteutettu Import ja Infoimport välilehtien kautta ominaisuuksia, joilla voi tuoda välilehdille tietoa helpottamaan arviointia, ohjeita, vertailutietoa
  - Ristiinviittaukset voivat olla joko käytäntökohtaisia tai tavoitekohtaisia
  - Import-työkalussa on valmiita pohjia hyödynnettäväksi.
  - Import ominaisuudella voi tuoda myös vanhat arviointitulokset uuden arvioinnin viereen tai vastausten pohjaksi.

		ISO/IEC27001:2023	ISO/IEC27002:2022
ACCESS-1a	Työntekijöille ja muille entiteeteille (kuten prosesseille tai laitteille, jotka tarvitsevat pääsyn toimintoon kuuluviin laitteisiin, ohjelmistoihin tai tietovarantoihin) osoitetaan erilliset identiteetit. (Huom. tällä vaatimuksella ei kuitenkaan rajoiteta jaettujen identiteettien käyttöä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	A5.16 A5.18	5.16 5.18
ACCESS-1b	Työntekijöille ja muille entiteeteille jaetaan pääsyvaltuustiedot (kuten salasanat, älykortit tai avaimet). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	A5.16	5.16

Ristiinviittausesimerkkejä

- Kybermittari vs
  - Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä
    - Tavoitetasolle koko suositus
    - Perustason käytännöt viitattu Kybermittarin käytäntöjen tasolle (oma välilehti)
  - Implementing Guidance On Commission Implementing Regulation (EU) 2024/2690
  - ISO/IEC 27001:2022 (https://www.iso.org/standard/27001)
  - ISO/IEC 27002:2022 (https://www.iso.org/standard/75652.html
  - IEC 62443-2-1:2024 (https://webstore.iec.ch/en/publication/62883) (luonnos)
  - Raideliikenteen suositus

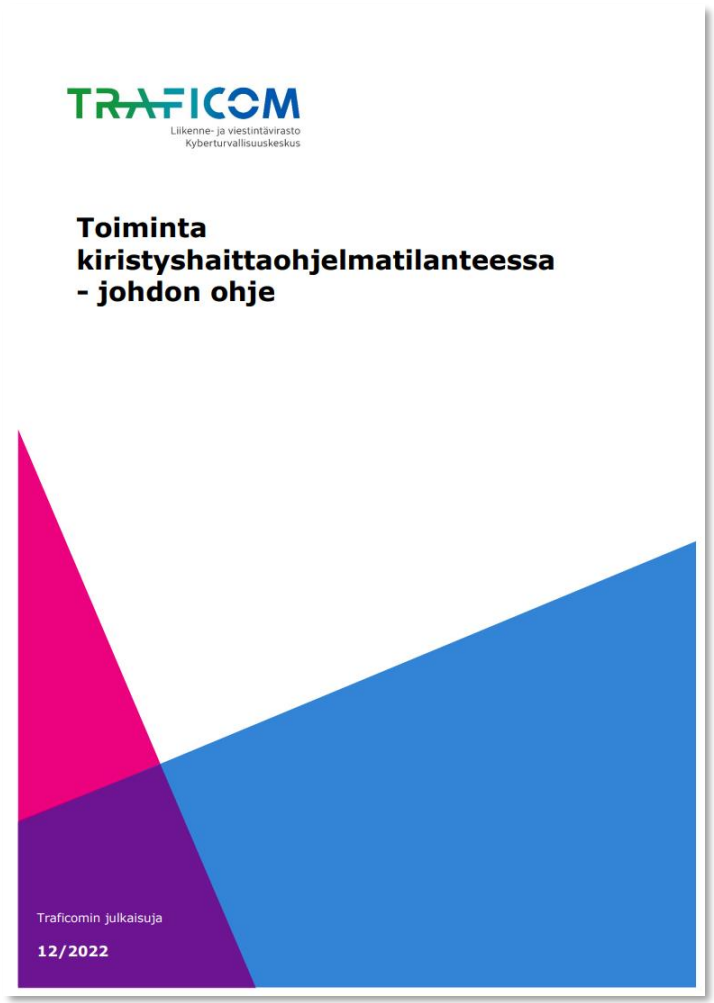
NIS2 – suositus – Kybermittari, ristiinviittaus – vastuuvapauslauseke

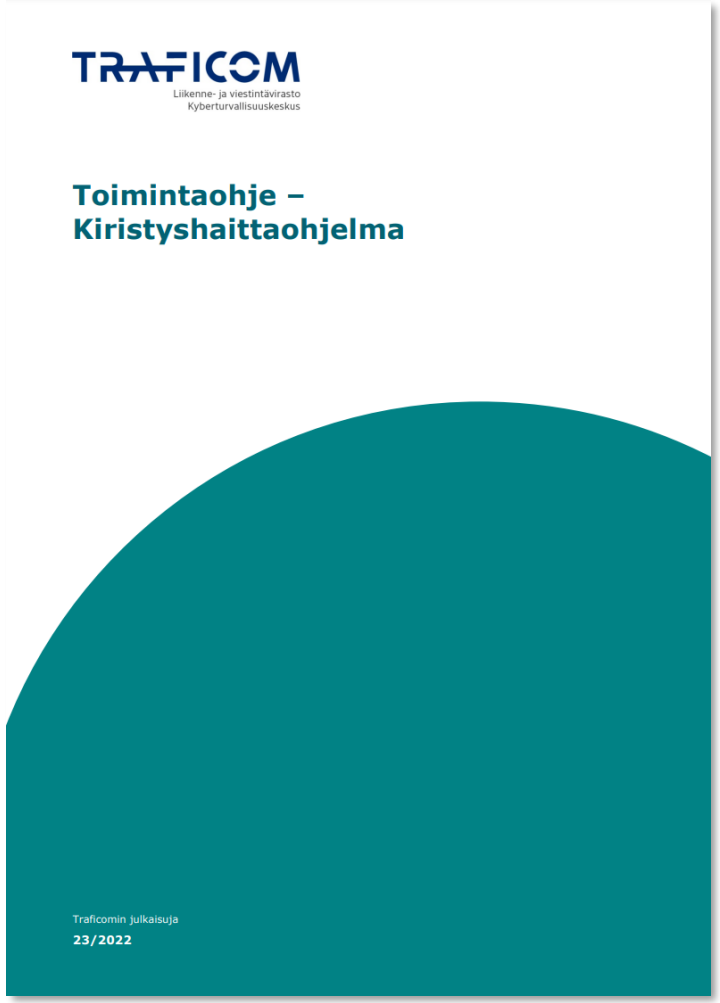
- Kybermittari-työkalussa, dokumentaatiossa ja tietojen tuontiin luodussa Import-työkalussa **tarjottavat ristiinviittaukset suositukseen, standardeihin ja kriteeristöihin ovat ohjeellisia. Keskenään ristiinviitatut kohdat voivat erota esimerkiksi laajuudeltaan, joten ne eivät välttämättä ole keskenään samansisältöisiä.**
- Kybermittari-palvelu tarjoaa työkalut ja dokumentaation sellaisena, kuin se tällä sivustolla on tarjolla. Kybermittarin käyttäjä vastaa ristiinviittausten pohjalta tekemistään toimenpiteistä, mukaan lukien palvelut, joita se tarjoaa kolmannelle osapuolelle. Kyberturvallisuuskeskus jatkaa Kybermittari-palvelun kehitystä ja palvelun sisältöä, kuten ristiinviittauksia, tullaan muokkaamaan tulevaisuudessa. Muutoksista ilmoitetaan ja ne päivitetään verkkosivuillemme.

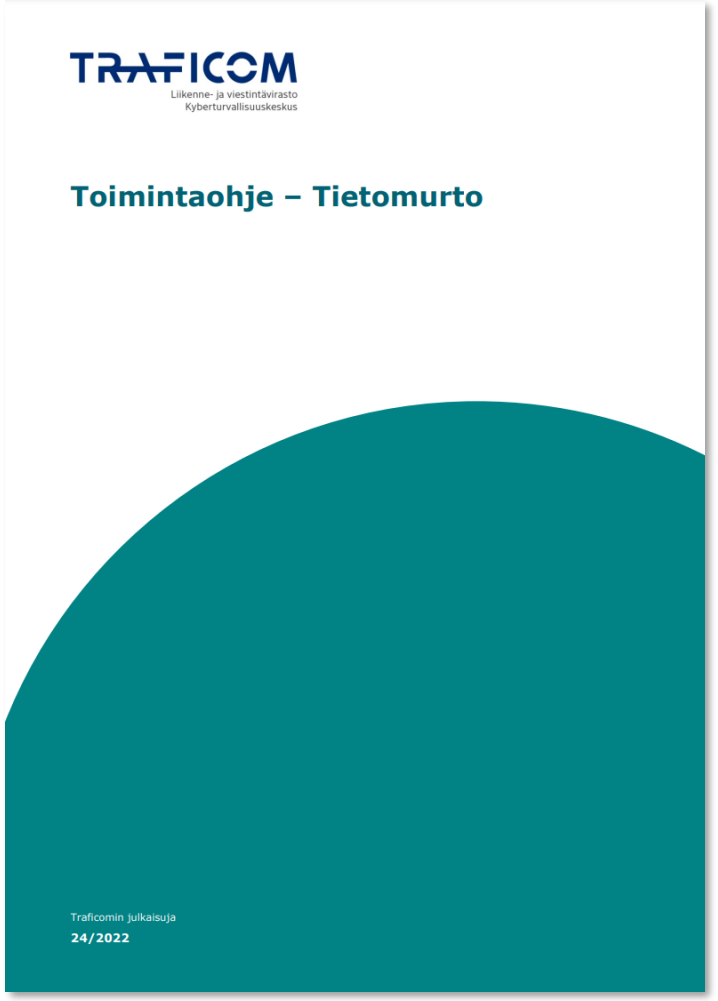
Hyöky - haavoittuvuusskannaus

Taso	Avain	Käytäntö	Lisätieto	Vastaus	Kommentit
1	THREAT-1b	Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.		0	Hyöky
1	THREAT-1c	Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.		0	Hyöky
2	THREAT-1f	Haavoittuvuusarviointeja suoritetaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.		0	Hyöky
3	THREAT-1k	Haavoittuvuusarvioinnit suorittaa toiminnon operatiivisesta toiminnasta irrallaan oleva riippumaton taho.		0	Hyöky
3	THREAT-1l	Haavoittuvuuksien seurantaan kuuluu myös toimenpiteiden katselmus, jolla varmistetaan, että haavoittuvuuksia rajaavat tai korjaavat toimenpiteet ovat olleet tehokkaita.		0	H

Response-3: Tapahtumiin ja häiriöihin reagoiminen







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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Sääntelystä ja suosituksista

Kyberturvallisuusstrategian toimeenpanosuunnitelma 3.12.2024 – VN/36693/2023

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”					
Nro	**Toimenpide**	**Tavoitteet**	**Aikataulu ja rahoitus**	**Vaikutusarvio ja vaikuttavuusanalyysi**	**Vastaa** / toimijat
2.5.	**Varmistetaan yhdenmukainen kyberturvallisuuslain toimeenpano** **Kori 1**	• Vahvistetaan NIS2-valvovien viranomaisten sekä tietosuojavaltuutetun yhteistyötä ja yhteistoimintaa. • Parannetaan toimialoille suunnattua neuvontaa ja ohjeistusta kyberturvallisuuslain ja lain julkisen hallinnon tiedonhallinnasta toimeenpanoon. • Laaditaan kansallinen laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma. • Parannetaan tietosuojavaltuutetun toimintaedellytyksiä.	2025-2029 Toiminta-menot, osin lisä-resurssit	NIS2 -direktiivi on keskeinen kyberturvallisuuden säädös, joka yhtenäistää kriittisten toimialojen kyberturvallisuusvaatimuksia ja kasvattaa kansallista resilienssiä. Valvovien viranomaisten yhteistyöllä voidaan yhdenmukaistaa menettelyjä sekä tehostaa resurssien käyttöä. Yhteisillä ohjeistuksilla voidaan parantaa ja tehostaa lain toimeenpanoa organisaatioissa. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, OM** VM, Traficom, TSV, NIS2 valvovat viran-omaiset

Kyberturvallisuusstrategian toimeenpanosuunnitelma 3.12.2024 – VN/36693/2023

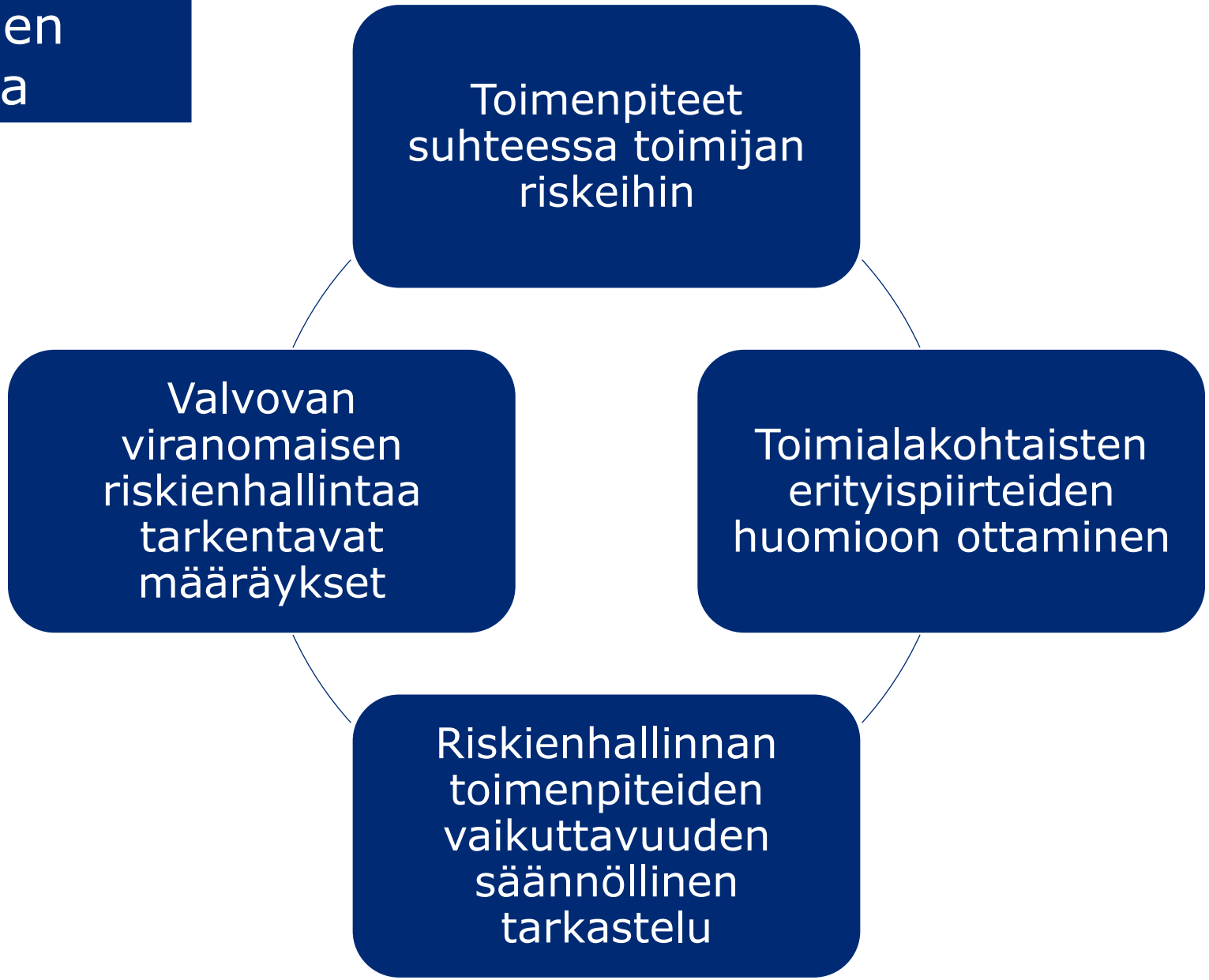
Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”					
Nro	**Toimenpide**	**Tavoitteet**	**Aikataulu ja rahoitus**	**Vaikutusarvio ja vaikuttavuusanalyysi**	**Vastaa** / toimijat
3.7.	**Julkinen sektori yhdessä yksityisen sektorin kanssa kehittää ja tarjoaa keskitettyjä kyberturvallisuus-palveluja** **Kori 1**	• Varmistetaan Traficomin Kyberturvallisuuskeskuksen tuottamien palveluiden jatkuvuus ja laajennetaan palveluiden, kuten Kybermittarin ja Hyökyn käyttöä laajemmille kohderyhmille. • Vahvistetaan DVV:n Vahti-verkoston, Taisto-harjoitusten ja Julkri-työkalun vaikuttavuutta. • Kasvatetaan DVV:n hallinnollisen digiturvan kokonaiskuvapalvelun käyttöastetta, vaikuttavuutta ja hyödyntämistä julkisessa hallinnossa. • Tuotetaan mallipohjia, neuvotellaan keskitetysti sopimuksia. • Tunnistetaan ja kehitetään tarvittavia uusia palveluita.	2024-2030 Toiminta-menot, osin lisäresurssit	Yhteiset keskitetyt kyberturvallisuuspalvelut tehostavat resurssien käyttöä. Niiden laaja käyttö on edellytys merkittävälle julkisten palveluiden turvallisuuden ja toimintavarmuuden parantamiselle. Palveluiden jatkuvuuden turvaaminen, uudet palvelut ja palveluiden laajennukset edellyttävät lisäresursseja. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM**, **VM,** HVK, Traficom, DVV, julkisen hallinnon ICT-yhtiöt, yksityinen sektori, muu julkinen hallinto

Suosituksen soveltamisesta

Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä tai Kybermittari

- Eivät sido viranomaisia eikä toimijoita. Sitovat velvoitteet säädetään:
  - **Laeissa**,
  - Euroopan komission antamassa **tarkentavassa sääntelyssä** ja
  - toimialakohtaisen viranomaisen **määräyksissä**.
- Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää suosituksesta poikkeavia, tiukempia vaatimuksia.
  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.
  - Toimijan on toteutettava toimenpiteitä riskiperustaisesti. Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

Riskiperustainen lähestymistapa



Kybermittari myös valvonnan apuna? – tekninen apuväline parempaan vuorovaikutukseen?

- Viranomaisten sekä viranomaisten ja asiakkaiden välinen tiedonvaihto ja yhteinen kieli
  - Yhtenäisempi tilannekuva ja ymmärrys toimialojen välisistä riippuvuuksista
  - Vertailutieto ja toimialojen hyvien käytäntöjen siirto toisille toimialoille
  - Valmiit viittaukset mm. suositukseen
  - Yhtenevä viesti asiakkaille esimerkiksi monialayritysten tapauksessa
- Sisältää välineitä arvioida aiemmin mainittujen aiheiden kypsyystason arviointiin.
  - Käytäntöjä voi soveltaa valvontaan valikoiden ja riskiperustaisesti
  - Sisältyvät kehityspolut auttavat tavoiteltavan kypsyystason riskiperusteissa valinnassa
- Yhteinen tukimateriaali, koulutus ja ylläpito
  - Vapaus tehdä omat valinnat, muokkaukset, suositukset ja linkitykset toimialakohtaisesti
  - Raportit muokattavissa myös valvonnan tarpeisiin

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointimalli

Kybermittarin rakenne ja laskentamalli

Tärkeimmät käsitteet

- **Kypsyysmalli** tarkoittaa mallia, jossa toimintaa tarkastellaan tasoina tai askelmina, joita kiivetään ylöspäin kohti järjestelmällisempää ja kehittyneempää toimintaa.
- **Kypsyystasot** on määritelty tavoittein tai vaatimuksin, jotka arvioinnin kohteena olevan toiminnan tulisi kyseisellä kypsyystasolla täyttää.
- **Kyvykkyys** tarkoittaa kykyä toimia tarkoituksenmukaisella tavalla tietyllä osa-alueella ja hyödyntää osaamistaan sekä resurssejaan, jotta tavoitteet saavutettaisiin.
- **Käytännöt** edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuuden menettelytapoja jotka voivat perustua esim. standardeihin tai lakiin
- **Arvioitavat toiminnot** on Kybermittarin yhteydessä käytetty käsite, jolla tarkoitetaan niitä organisaation tai yhteiskunnan kannalta tärkeitä/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 CSF-malliin ja tuloksia voidaan myös peilata NIST CSF-mallin kanssa (Raportti R1)

Muut osa-alueet

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

Kyberturvallisuuden kokonaiskuva - kypsyystaso C2M2 v2.1 ja NIST CSF v2

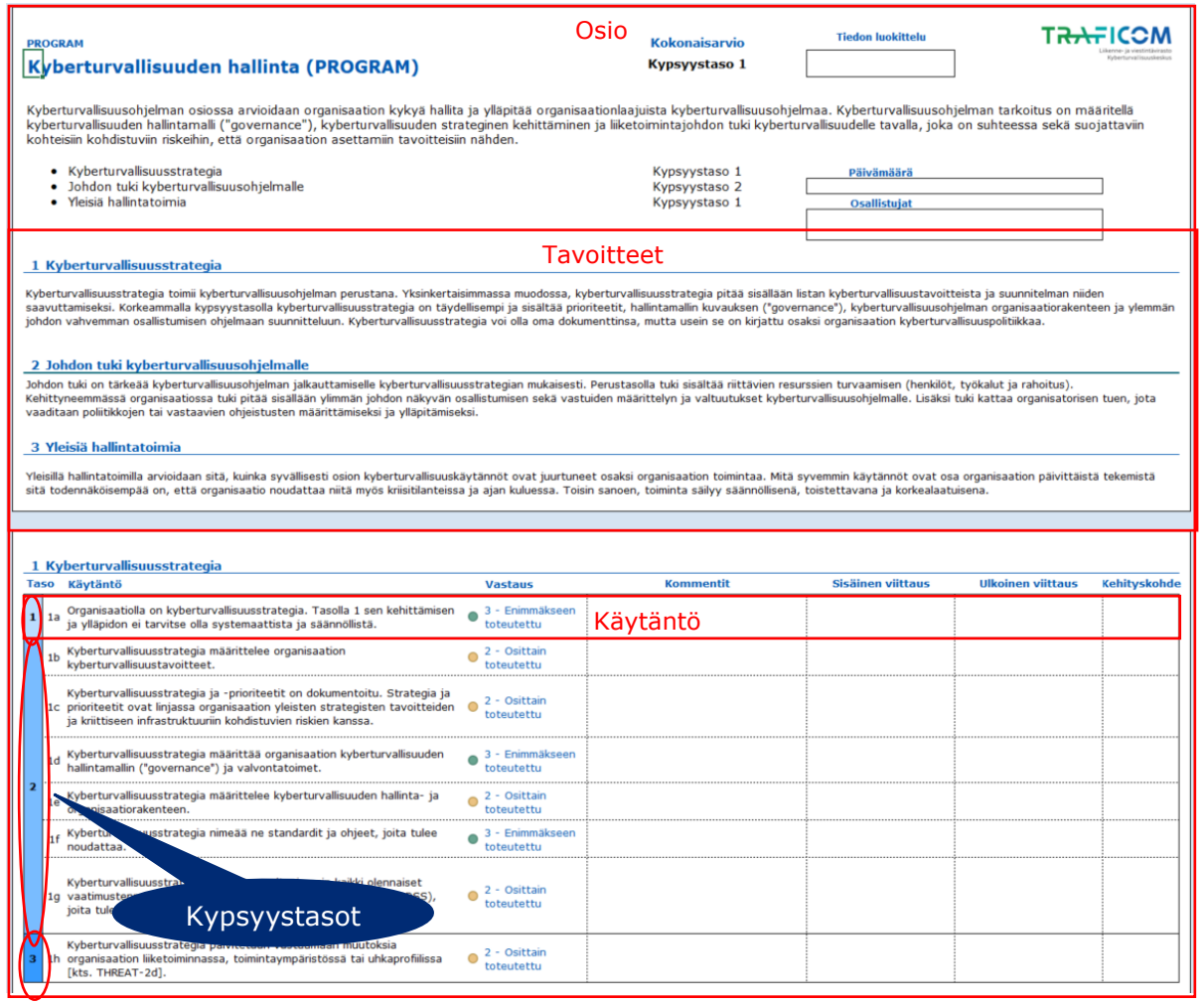
Hallinta Riskienhallinta strategia, toimintatavat ja seuranta	**Tunnistaminen** Uhkien, haavoittuvuuksien ja riskien tunnistaminen	**Suojautuminen** Suojautuminen	**Havainnointi** Poikkeamien havainnointi	**Reagointi Vaste** Poikkeamiin reagointi	**Palautuminen** Palauttavat toimenpiteet
ASSET – Omaisuuden, 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

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

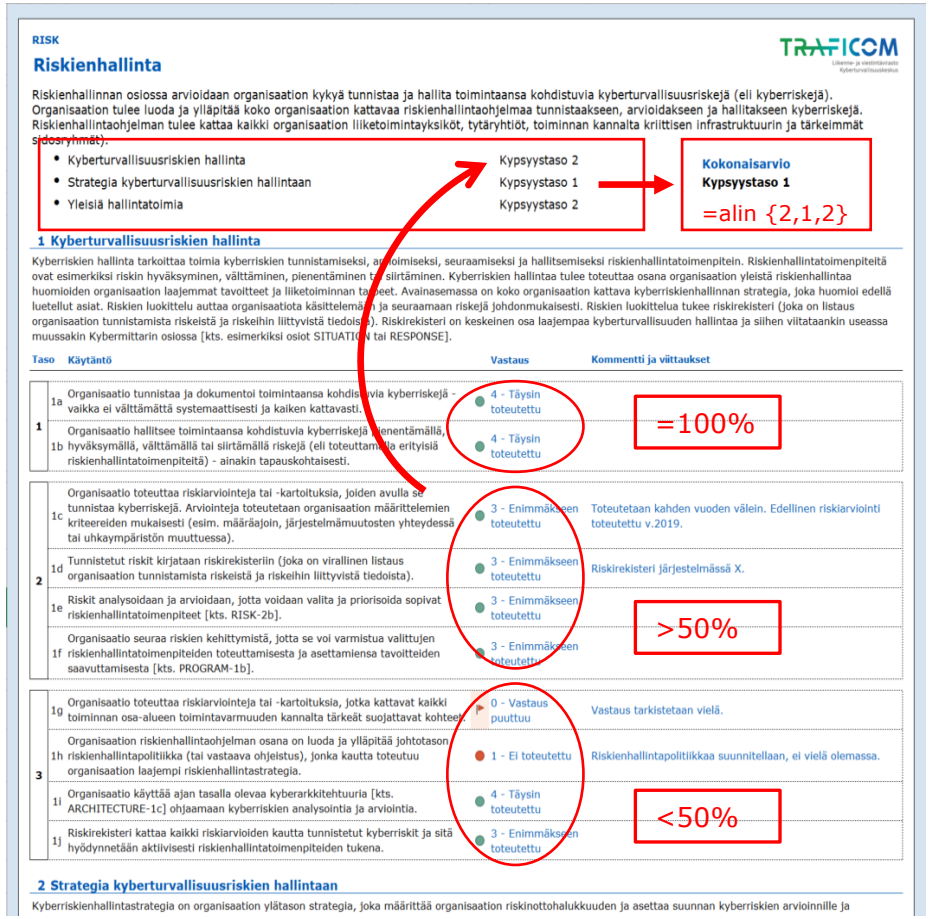
Tavoitteet ja osiot – kypsyystaso

- 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

Kybermittarin laskentamalli


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
=alin {2,1,2}

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		=100%
	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.	>50%
	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.	<50%
	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

- 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 <u>heikoimman tavoitteen kypsyystaso</u>

Esimerkki kuvaavasta tekstistä (ASSET-2g)

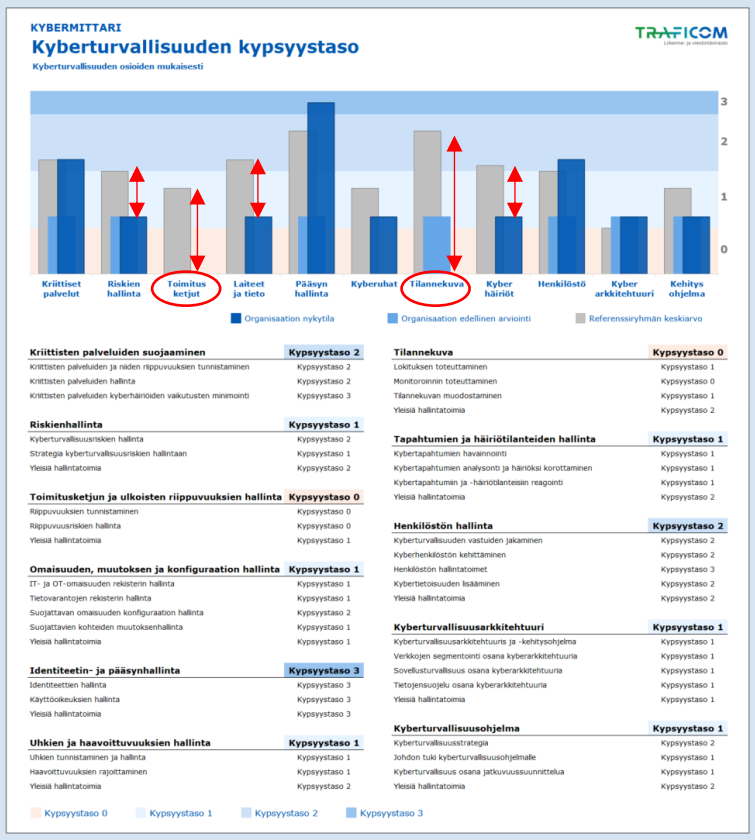
ASSET-2g (MIL 3) The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes

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.

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
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

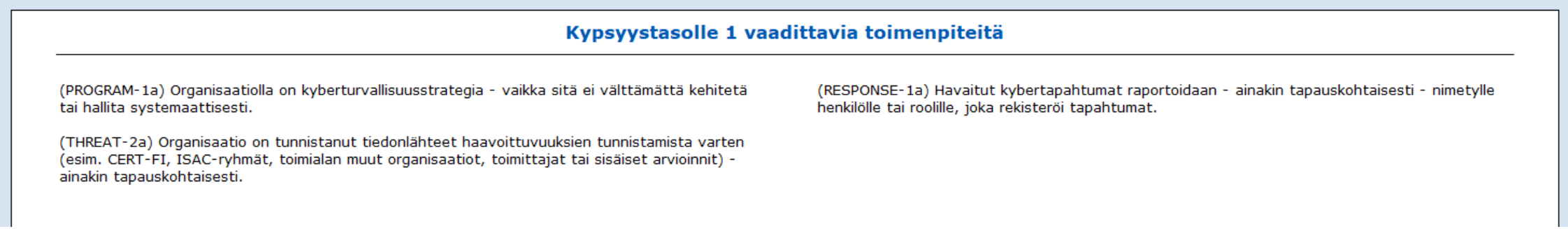
Kyberturvallisuusarkkitehtuuri	Kypsyystaso 1
Kyberturvallisuusarkkitehtuuris ja -kehitysohjelma	Kypsyystaso 1
Verkkojen segmentointi osana kyberarkkitehtuuria	Kypsyystaso 1
Sovellusturvallisuus osana kyberarkkitehtuuria	Kypsyystaso 1
Tietojensuojelu osana kyberarkkitehtuuria	Kypsyystaso 1
Yleisiä hallintatoimia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

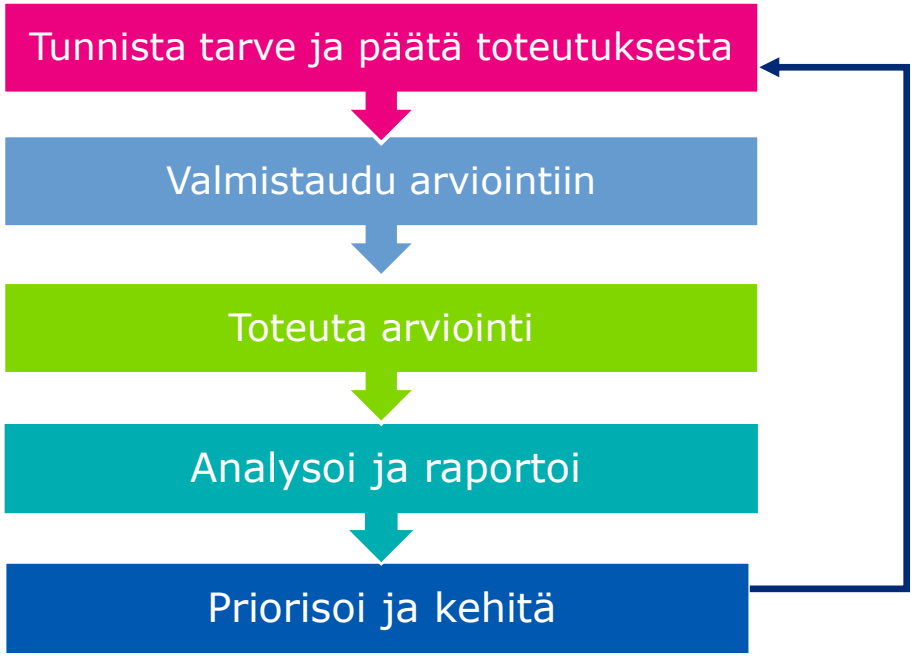
- Kybermittarin kypsyysraportista (R4):
  - Raportissa on listattu kypsyystasolle 1 vaadittavat käytännöt.
  - Yksittäisen käytännön puuttuminen pudottaa koko osion tasolle 0, joten tässä listattujen käytäntöjen toteuttaminen voi nostaa kypsyystasoa merkittävästi.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointiprosessi

Kybermittarin hyödyntämiseen

Kybermittari – itsearviointiprosessi
Kybermittarin ohjeistusta parannetaan tukemaan arvioinnin eri vaiheita



- Paras hyöty mittarista saadaan, kun se tuodaan osaksi toiminnan jatkuvaa kehittämistä
- Kybermittaria suositellaan käytettäväksi osana viisivaiheista arviointiprosessia
- Prosessi on laadittu Kybermittarin pilottikartoituksista saatujen kokemusten perusteella
- Toteutukseen tarvittava aika vaihtelee paljon riippuen mm. arviointitavasta, organisaation kypsyystasosta ja arvioinnin laajuudesta

Esimerkki Kybermittarin arviointiprosessista

Perustuen Kyberturvallisuuskeskuksen 2020-22 toteuttamiin pilottiarvointeihin

ITSEARVIOINTI	HAASTATTELU	TULOSTEN RAPORTOINTI

Organisaatio

Vastuuhenkilöiden nimeäminen	Vastausten täydentäminen	½ päivän työpaja	Raportointi johdolle

Arvioinnin fasilitoija

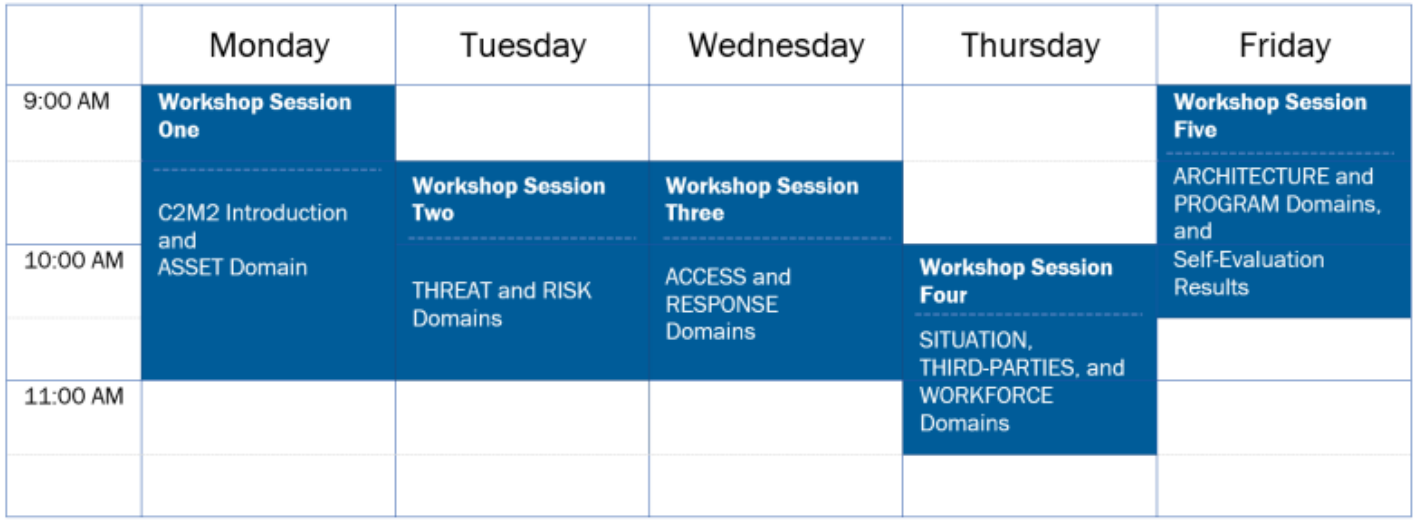
Valmistelu	Tuki, tarvittaessa	½ päivän työpaja	Loppuraportti

Esimerkki rooleista ja vastuista

Organisaatio nimeää vastuualueiden edustajat vastaamaan mittarin arviointikysymyksiin. Fasilitoija valmistelee ja aikatauluttaa arvioinnin ja tukee tarvittaessa vastausten tulkinnassa.	Yhteistyöpaja, jossa käydään läpi ja täydennetään organisaation täyttämät vastaukset. Tässä vaiheessa voidaan jo käydä läpi tärkeimpiä kehitysalueita.	Fasilitoija analysoi tulokset ja valmistelee loppuraportin, jota organisaatio voi käyttää raportointiin ja kehitystoiminnan ohjaamiseen.

C2M2 mallin ehdottama aikataulutus

- Järjestäjän tulee varata työpajalle vähintään kahdeksan tuntia. Työpaja voidaan tehdä yhdessä päivässä tai jakaa kahteen neljän tai viiden tunnin istuntoon kahtena peräkkäisenä päivänä.
- Jos työpajaa johdetaan virtuaalisesti, se tulisi koostua 60-90 minuutin työpajoista useiden päivien aikana. Suositeltavaa tehdä kaikki työpajat kahden viikon kuluessa.
- **Todennäköisesti liian tiukka aikataulu, jos havainnot kirjataan huolellisesti**



	Monday	Tuesday	Wednesday	Thursday	Friday
9:00 AM	**Workshop Session One**				**Workshop Session Five**
	C2M2 Introduction and ASSET Domain	**Workshop Session Two**	**Workshop Session Three**		ARCHITECTURE and PROGRAM Domains, and Self-Evaluation Results
10:00 AM		THREAT and RISK Domains	ACCESS and RESPONSE Domains	**Workshop Session Four**	
				SITUATION, THIRD-PARTIES, and WORKFORCE Domains	
11:00 AM					

Figure 1: Example of a C2M2 Self-Evaluation Virtual Workshop Schedule

Itsearvioinnin tarkistuslista

- Itsearvioinnin tarkistuslistan tarkoituksena on auttaa organisaatiota itsearvioinnin läpiviennissä ja tulosten raportoinnissa päätöksenteon tueksi

- Muuta uudistuvaa materiaalia
  - Materiaali- ja linkkilista
  - Kybermittarin lyhyt esittelymateriaali
  - Koulutusmateriaali
  - Koulutusvideot (tulossa)

LIITE A: ITSEARVIOINTITARKISTUSLISTA

Tavoite: helpottaa itsearvionnin suorittamista.
Osa tarkistuslistan tehtävistä koskee vain lähi-itsearviointityöpajoja ja osa vain virtuaalityöpajoja. Tehtävien aikajaksot, rooli ym. on sisällytetty suosituksina, ja niitä kannattaa muokata oman tarpeen mukaan.
Päivitys 24.11.2024
Piiloitettuna löytyy tehtäviä englanninkielellä.

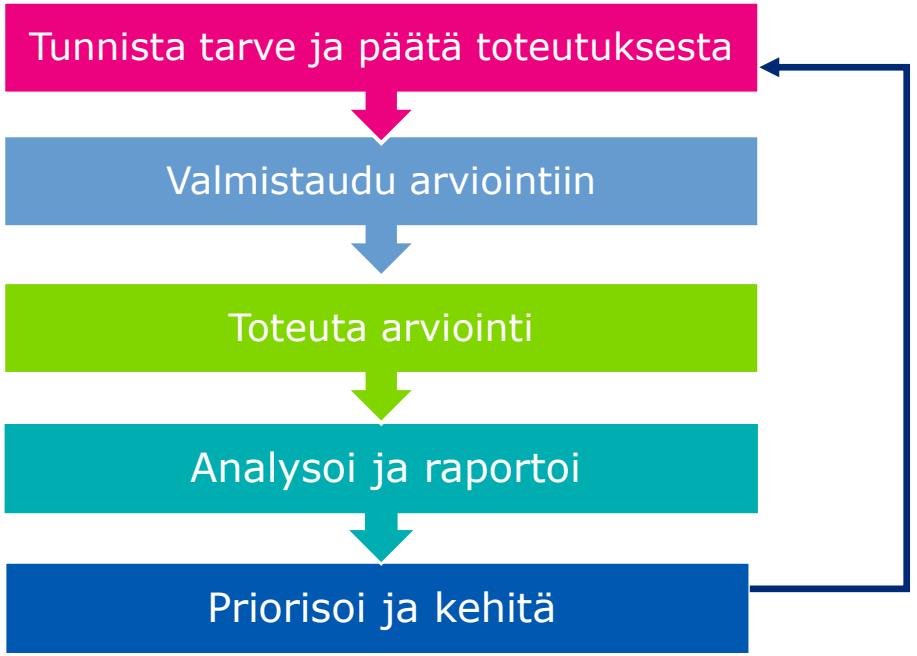
Lähde, soveltaen: https://c2m2.doe.gov/resources

NR	Tehtävä	Teht	Vaihe	Vaihe	Järjestäjä Organizer	Facilitator	Tukija, Sponsor	Muut Osanottajat, Other	Tuki Support Staff
1	Hanki viimeisimmät versiot Kybermittarin tai C2M2-dokumentaatiosta ja fasilitointimateriaaleista		Aloita arviointi	Neljä viikko					
2	Perehdy tarvitsemiisi itsearviointimateriaaleihin		Aloita arviointi	Neljä viikko		x			
3	Perehdy keskeisiin rooleihin C2M2:n itsearviointiprosessissa		Aloita arviointi	Neljä viikko		x			
4	Pidä valmistelukokous, jossa arvioidaan tarve kypsyysarvioinnille ja niiden tarjoama itsearviointiarviointi ja siitä saatavat tulokset tukevat organisaation toimintaa ja päätöksentekoa		Aloita arviointi	Neljä viikko	x	x	x	x	
5	Määritä itsearvioinnin laajuus: organisaation, tarkasteltavien käytäntöjen ja toimintojen osalta		Aloita arviointi	Neljä viikko	x	x	x	x	
6	Tunnista keskeiset sidosryhmät, roolit ja tukihenkilöstö		Aloita arviointi	Neljä viikko	x	x	x		
7	Hankitaanko ulkopuolinen taho tukemaan itsearvionnissa (hankinta?)		Aloita arviointi	Neljä viikko	x	x	x		
8	Esittele suunnitelma ja varmista tuki arvionnin toteuttamiselle (johdon / liiketoiminnasta vastuullisen antama tuki)		Aloita arviointi	Neljä viikkoa enn		x			
9	Tunnista henkilöt/osallistujat, jotka tarvitaan arvionnin toteuttamiseen		Valmistaudu arviontiin	Neljä viikkoa enn		x			
10	Kommunikoi osallistujille itsearvioinnin merkityksestä ja aktiivisesta osallistumisesta		Valmistaudu arviontiin	Neljä viikko			x		
11	Tunnista ja varaa sopiva kokoustila työpajalle		Valmistaudu arviontiin	Neljä viikko	x				
12	Valitse työskentely ja työpajapäivät fasilitaattorin, sponsorin, osallistujien ja kokoustilan saatavuuden perusteella (tarvittaessa)		Valmistaudu arviontiin	Neljä viikko	x	x	x		
13	Lähetä kutsuja ja esityslista osallistujille ja pyydä vahvistusta		Valmistaudu arviontiin	Neljä viikko	x				
14	Lähetä valmistelevaa luettavaa osallistujille		Valmistaudu arviontiin	Neljä viikko	x				
15	Tarkenna tarvittaessa itsearvioinnin laajuutta organisaation, tarkasteltavien käytäntöjen ja toimintojen osalta. Käytä tarvittaessa Import-pohjille luotuja mäppäyksiä apuna.		Valmistaudu arviontiin			x	x		
16	Tee tarvittaessa matkajärjestelyjä		Valmistaudu arviontiin	Neljä viikko		x			x
17	Järjestä tarvittaessa tarjoilut		Valmistaudu arviontiin	Kaksi viikk					x
18	Järjestä tarvittaessa pääsy kohteisiin (vierailijat ym)		Valmistaudu arviontiin	Kaksi viikk	x				
19	Tee tarvittaessa salassapitosopimukset (erityisesti ulkopuoliset)		Valmistaudu arviontiin	Neljä viikko	x				x

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tunnista tarve ja päätä toteutuksesta

Tunnista tarve ja päätä toteutuksesta



- **Osallistujat:**
  - Organisaation johtoryhmä tai muu päätöksentekoelin sekä tarvittavat asiantuntijat.
- **Tehtävä:**
  - Tunnistetaan arvioinnilla tavoiteltavat hyödyt ja tuloksia mahdollisesti hyödyntävät prosessit.
  - Päätetään arvioinnin resursoinnista, kohteesta, laajuudesta, toteuttamistavasta ja ajankohdasta; ja
  - Nimitetään 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

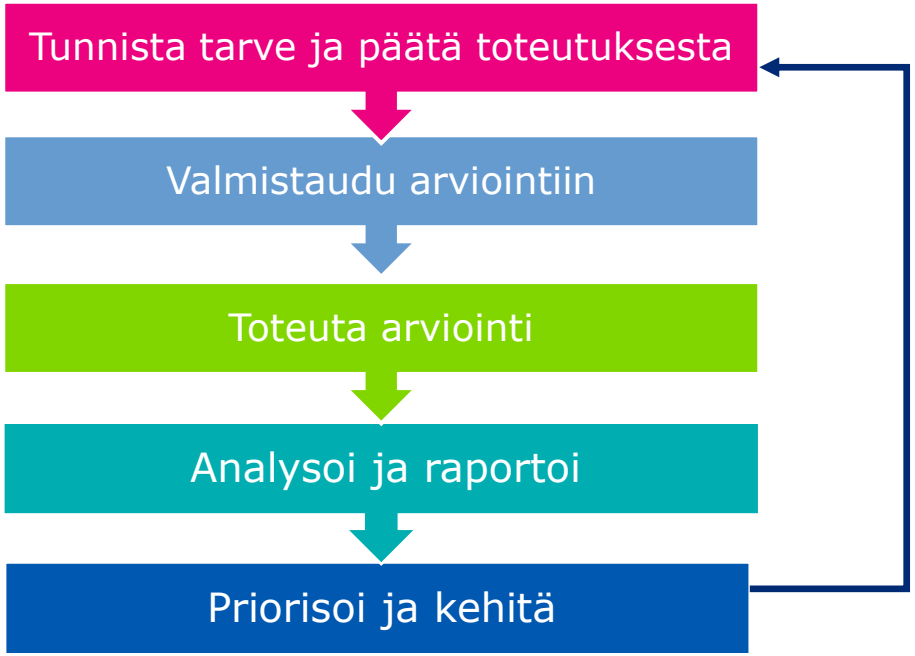
Arvioinnin vetäjä

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:**
  - Rajataan tarkemmin arvioitavana oleva toiminnan osa-alueet ja tunnistetaan osa-alueiden kriittiset riippuvuudet
  - Tunnistetaan arviointiin tarvittavat asiantuntijat ja viestitään heille arvioinnista
  - Sovitaan arvioinnin toteutustavasta ja arvioinnin tarkemmasta aikataulusta

Toiminnan osa-alueen rajaaminen

- Arviointia varten tulee tunnistaa ja rajat arvioitava toiminnan osa-alue
- Arviointi suositellaan kohdistamaan vähintään 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
  - Rajaus voidaan tehdä myös esimerkiksi tiettyihin Kybermittarin osioihin, kuten riskienhallintaan (huom. osa raporteista ei käyttökelpoisia)

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:

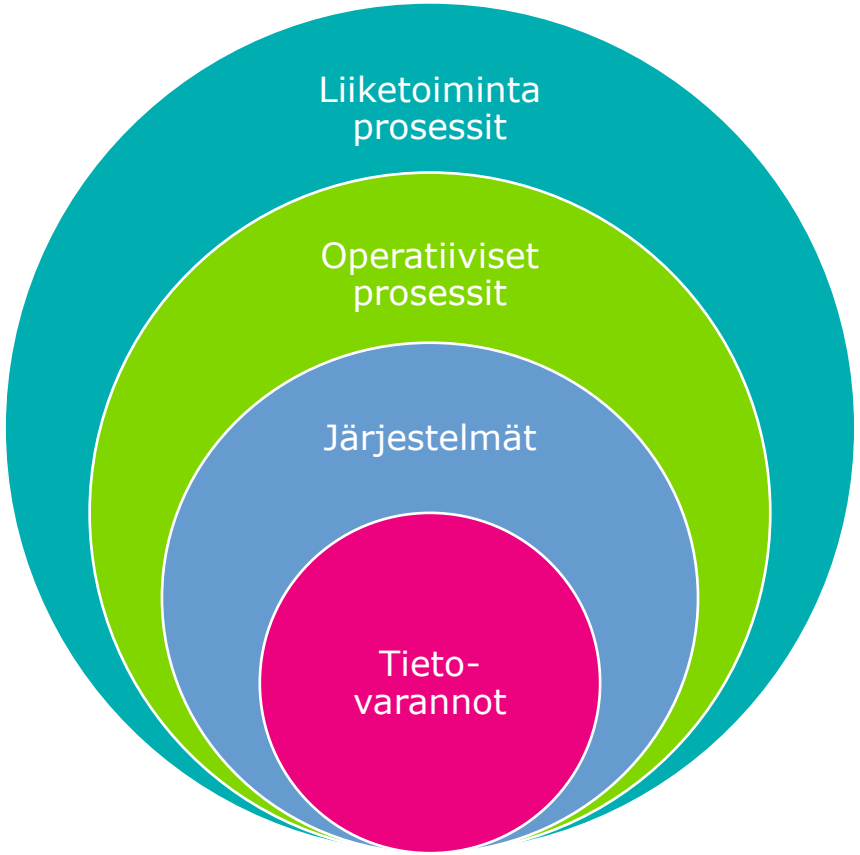
1. Vähäinen systeeminen vaikutus	2. Huomattava systeeminen vaikutus	3. Rampauttava systeeminen vaikutus
Vaikutus kohdistuu vain organisaatioon itseensä tai vain vähäiseen määrään partnereita ja/tai asiakasorganisaatioita, tai vaikutus rajautuu alle 50000 kansalaiseen.	Toiminta vaikeutuu huomattavalle 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 takaavat palvelun häiriöttömän toimittamisen loppuasiakkaalle

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

- Tunnista palvelun toimittamisen kannalta keskeinen suojattava omaisuus
  - Suojattava 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
  A. Ohjattu työpajamuotoinen toimintamalli; tai
  B. Henkilövetoinen arviointi

- Toteutustavasta riippuen vetäjä huolehtii joko työpajan käytännön järjestelyistä tai koordinoi muutoin arvioinnin toteuttamisen asiantuntijoiden kanssa

A. 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)
- Hyvät puolet: Edistää vuorovaikutusta ja yhteistä ymmärrystä
- Huonot puolet: Vie enemmän resursseja.

B. Henkilövetoinen arviointi

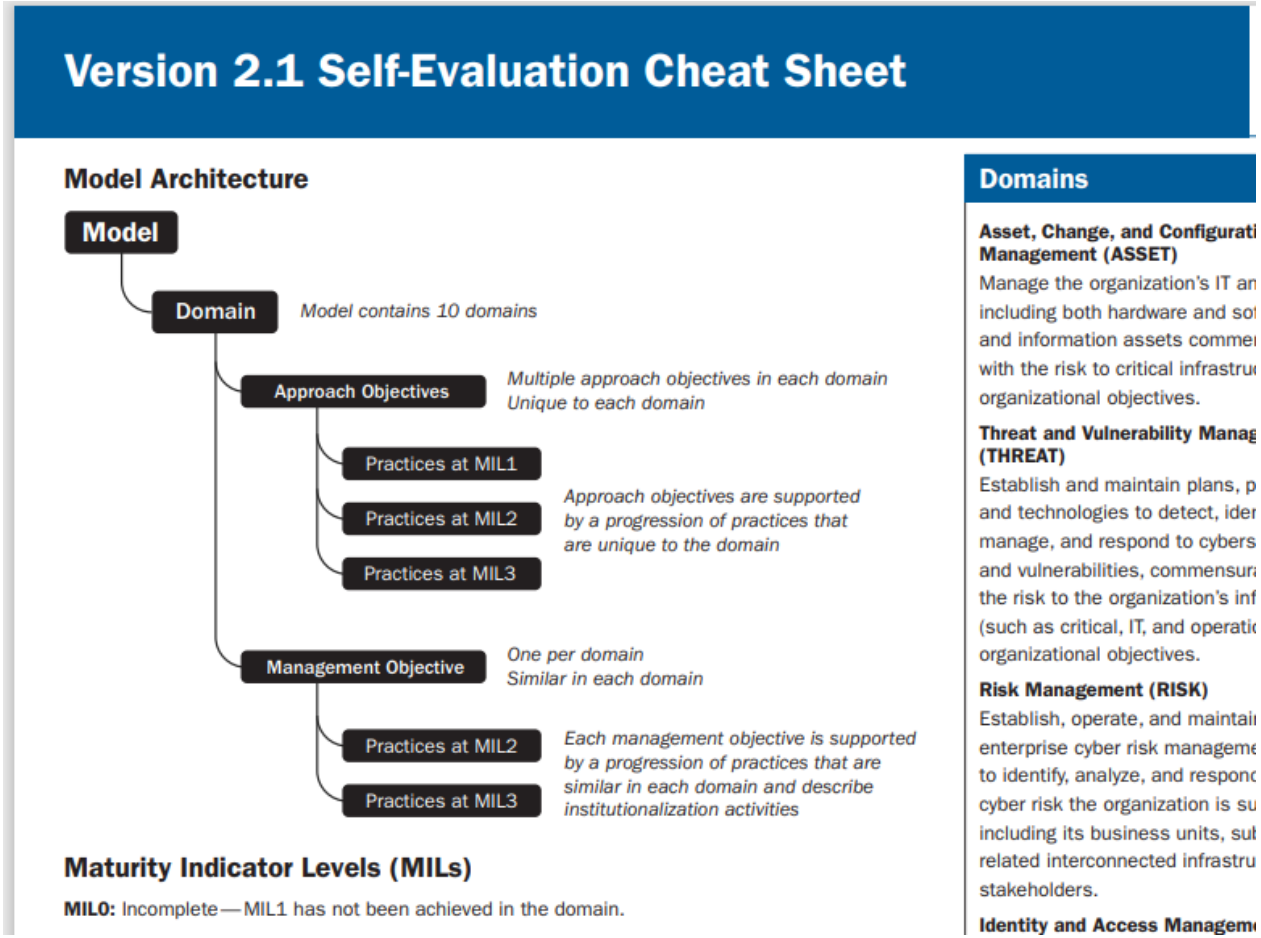
- Vaiheet, joiden koordinoinnista arvioinnin vetäjä vastaa, ovat:
  1. Asiantuntijoiden nimeäminen ja sitouttaminen työpajaan;
  2. Aloituskokous (1-2 h) arviointiin osallistuville henkilöille
  3. Nimetyt asiantuntijat täyttävät itsenäisesti Kybermittarin heille osoitetut aihealueet sovitun aikataulun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

Toimintaohjeita kognitiivisten vinoumien välttämiseksi

- Käytä tiimiä: Varmista, että kysymyksiin vastaa ryhmä ihmisiä, joilla on erilaisia näkemyksiä organisaation kyberturvallisuudesta.
- Arvioi objektiivisesti: Pohdi jokaista vastausta faktojen, ei tunteiden tai aiempien uskomusten pohjalta.
- Tarkista priorisointi: Suuntaa resurssit sinne, missä on eniten riskejä tai kehittämistarpeita, ei sinne, missä asiat ovat jo hyvällä mallilla.
- Päivitä säännöllisesti: Toista Kybermittarin käyttö esimerkiksi kerran vuodessa ja hyödynnä aiempien arvioiden kehitystä peilinä nykyhetkelle.

Itsearvioinnin lunttauslista (cheat sheet)

- Itsearvioinnin lunttauslista ei ole vielä käännetty suomeksi. Alkuperäinen löytyy C2M2:n sivuilta
  - C2M2 V2.1 Cheat Sheet.pdf



Version 2.1 Self-Evaluation Cheat Sheet

Model Architecture

Model

Domain — *Model contains 10 domains*

Approach Objectives — *Multiple approach objectives in each domain*
Unique to each domain

Practices at MIL1
Practices at MIL2
Practices at MIL3

Approach objectives are supported by a progression of practices that are unique to the domain

Management Objective — *One per domain*
Similar in each domain

Practices at MIL2
Practices at MIL3

Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

Maturity Indicator Levels (MILs)

MIL0: Incomplete—MIL1 has not been achieved in the domain.

Domains

Asset, Change, and Configurati Management (ASSET)
Manage the organization's IT an including both hardware and sot and information assets commer with the risk to critical infrastruc organizational objectives.

Threat and Vulnerability Manag (THREAT)
Establish and maintain plans, p and technologies to detect, ider manage, and respond to cybers and vulnerabilities, commensura the risk to the organization's inf (such as critical, IT, and operatic organizational objectives.

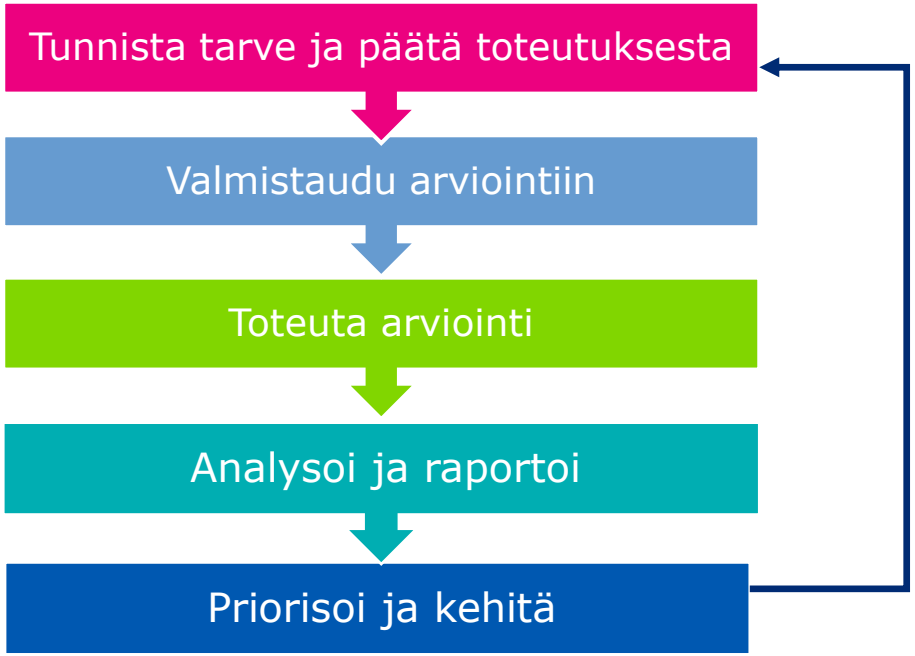
Risk Management (RISK)
Establish, operate, and maintai enterprise cyber risk manageme to identify, analyze, and respond cyber risk the organization is su including its business units, sul related interconnected infrastru stakeholders.

Identity and Access Managem

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toteuta arviointi

Toteuta arviointi



- **Osallistujat:**
  - Arvioinnin vetäjä, arvioinnin sponsori ja organisaation asiantuntijat. (tarvittaessa ulkoinen fasilitoija sekä esimerkiksi kriittisen palveluntarjoajan asiantuntijoita)
- **Tehtävä:**
  - Toteuttaa arviointi valitulla arviointitavalla Kybermittarin 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 poikkeamanhallinta, toiminnan jatkuvuus

THIRD-PARTIES – Kumppaniverkoston riskien hallinta

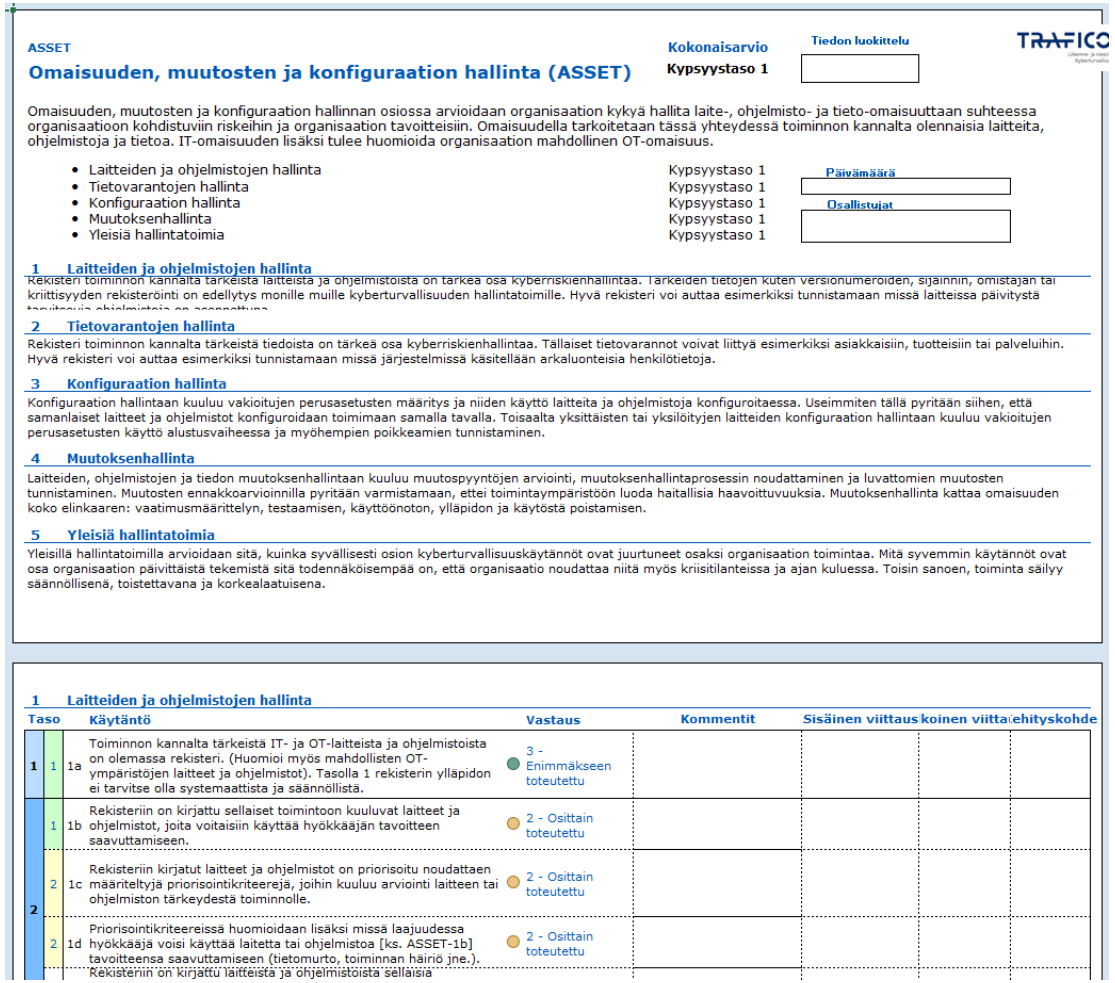
WORKFORCE – Henkilöstön johtaminen ja kehittäminen

ARCHITECTURE - Kyberturvallisuusarkkitehtuuri

PROGRAM – Kyberturvallisuuden hallinta

CRITICAL – Kriittisten palveluiden suojaaminen

Osiokohtaiset välilehdet



ASSET

Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Kokonaisarvio
Kypsyystaso 1

Tiedon luokittelu

TRAFICOM

Omaisuuden, muutosten ja konfiguraation hallinnan osiossa arvioidaan organisaation kykyä hallita laite-, ohjelmisto- ja tieto-omaisuuttaan suhteessa organisaatioon kohdistuviin riskeihin ja organisaation tavoitteisiin. Omaisuudella tarkoitetaan tässä yhteydessä toiminnon kannalta olennaisia laitteita, ohjelmistoja ja tietoa. IT-omaisuuden lisäksi tulee huomioida organisaation mahdollinen OT-omaisuus.

- Laitteiden ja ohjelmistojen hallinta — Kypsyystaso 1
- Tietovarantojen hallinta — Kypsyystaso 1
- Konfiguraation hallinta — Kypsyystaso 1
- Muutoksenhallinta — Kypsyystaso 1
- Yleisiä hallintatoimia — Kypsyystaso 1

Päivämäärä

Osallistujat

1 Laitteiden ja ohjelmistojen hallinta

Rekisteri toiminnon kannalta tärkeistä laitteista ja ohjelmistoista on tärkeä osa kyberriskienhallintaa. Tärkeiden tietojen kuten versionumeroiden, sijainnin, omistajan tai kriittisyyden rekisteröinti on edellytys monille muille kyberturvallisuuden hallintatoimille. Hyvä rekisteri voi auttaa esimerkiksi tunnistamaan missä laitteissa päivitystä tarvitsevia ohjelmistoja on asennettuna.

2 Tietovarantojen hallinta

Rekisteri toiminnon kannalta tärkeistä tiedoista on tärkeä osa kyberriskienhallintaa. Tällaiset tietovarannot voivat liittyä esimerkiksi asiakkaisiin, tuotteisiin tai palveluihin. Hyvä rekisteri voi auttaa esimerkiksi tunnistamaan missä järjestelmissä käsitellään arkaluonteisia henkilötietoja.

3 Konfiguraation hallinta

Konfiguraation hallintaan kuuluu vakioitujen perusasetusten määritys ja niiden käyttö laitteita ja ohjelmistoja konfiguroitaessa. Useimmiten tällä pyritään siihen, että samanlaiset laitteet ja ohjelmistot konfiguroidaan toimimaan samalla tavalla. Toisaalta yksittäisten tai yksilöityjen laitteiden konfiguraation hallintaan kuuluu vakioitujen perusasetusten käyttö alustusvaiheessa ja myöhempien poikkeamien tunnistaminen.

4 Muutoksenhallinta

Laitteiden, ohjelmistojen ja tiedon muutoksenhallintaan kuuluu muutospyyntöjen arviointi, muutoksenhallintaprosessin noudattaminen ja luvattomien muutosten tunnistaminen. Muutosten ennakkoarvioinnilla pyritään varmistamaan, ettei toimintaympäristöön luoda haitallisia haavoittuvuuksia. Muutoksenhallinta kattaa omaisuuden koko elinkaaren: vaatimusmäärittelyn, testaamisen, käyttöönoton, ylläpidon ja käytöstä poistamisen.

5 Yleisiä hallintatoimia

Yleisillä hallintatoimilla arvioidaan sitä, kuinka syvällisesti osion kyberturvallisuuskäytännöt ovat juurtuneet osaksi organisaation toimintaa. Mitä syvemmin käytännöt ovat osa organisaation päivittäistä tekemistä sitä todennäköisempää on, että organisaatio noudattaa niitä myös kriisitilanteissa ja ajan kuluessa. Toisin sanoen, toiminta säilyy säännöllisenä, toistettavana ja korkealaatuisena.

1 Laitteiden ja ohjelmistojen hallinta

Taso			Käytäntö	Vastaus	Kommentit	Sisäinen viittaus	oinen viitta	ehityskohde
1	1	1a	Toiminnon kannalta tärkeistä IT- ja OT-laitteista ja ohjelmistoista on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen laitteet ja ohjelmistot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu				
2	1	1b	Rekisteriin on kirjattu sellaiset toimintoon kuuluvat laitteet ja ohjelmistot, joita voitaisiin käyttää hyökkääjän tavoitteen saavuttamiseen.	2 - Osittain toteutettu				
	2	1c	Rekisteriin kirjatut laitteet ja ohjelmistot on priorisoitu noudattaen määriteltyjä priorisointikriteerejä, joihin kuuluu arviointi laitteen tai ohjelmiston tärkeydestä toiminnolle.	2 - Osittain toteutettu				
	2	1d	Priorisointikriteereissä huomioidaan lisäksi missä laajuudessa hyökkääjä voisi käyttää laitetta tai ohjelmistoa [ks. ASSET-1b] tavoitteensa saavuttamiseen (tietomurto, toiminnan häiriö jne.).	2 - Osittain toteutettu				
			Rekisteriin on kirjattu laitteista ja ohjelmistoista sellaisia					

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

Esimerkki kuvaavasta tekstistä (ASSET-2g) Auttaa käytäntöjen tulkinnassa (saatavilla myös erillisenä taulukkona: suomi ja englanti)

ASSET-2g (MIL 3) Tietovarantorekisteri on ajan tasalla (eli rekisteriä päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä).

Tietovarantorekisteriä / -luetteloa olisi päivitettävä ja ylläpidettävä sitä mukaa kuin tietovarannot muuttuvat niiden elinkaaren aikana, jotta voidaan varmistaa, että rekisteri / luettelo on riittävän täydellinen ja tarkka. Omaisuuseräluettelon ajantasaisuuden varmistaminen saattaa edellyttää muutoksenhallinnan menettelyjä, jotka edellyttävät luettelon päivittämistä aina, kun omaisuuseriä muutetaan merkittävästi. Organisaatio saattaa myös tehdä rekisterin / luettelon tarkistuksia sekä säännöllisesti (esimerkiksi neljännesvuosittain tai vuosittain) että tiettyjen tapahtumien seurauksena (esimerkiksi organisaatiorakenteen muutokset, kriittisten järjestelmien merkittävät muutokset ja toisen yrityksen hankinta ja yhdistäminen).

Aiheeseen liittyvät käytännöt:
Eteneminen: Tämä käytäntö on osa kehityspolkua. Samaan toimintaan liittyvät käytännöt muodostavat kehityspolun, johon kuuluu käytäntöjä alkaen perustasolta kohti täydellisempiä tai kehittyneempiä toteutuksia. Tämän kehityspolun käytäntöjä ovat: ASSET-2a, ASSET-2b, ASSET-2f, ASSET-2g.

Kehityspolut 1/2

- Kehityspolut auttavat löytämään toisiinsa liittyvät, eri kypsyystason käytännöt ja suunnittelemaan tavoitetason riskiperustaisesti ja valitsemaan kehitystoimenpiteitä
- Helpottavat ja nopeuttavat arviointia, koska voi käydä kehityspolun kerrallaan
- Kehityspolut on numeroitu käytäntöriville kypsyystason viereen
  - Lista kehityspoluista ja taulukointi löytyvät Kybermittarin ”Ohje Kehitys” ja ”Kehitys”-välilehdiltä

1		Haavoittuvuuksien vähentäminen	
Taso		Käyt	Vastaus
1	9	1a tie… …ttu soveltuvia …emaattista ja sään…	1 - Ei toteutettu tai ei tietoa
	10	1b Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	1 - Ei toteutettu tai ei tietoa
	11	1c Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
	12	1d Toiminnon kannalta olennaisiin haavoittuvuuksiin puututaan (esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
2	9	1e Haavoittuvuustiedon lähteet kattavat korkean prioriteetin laitteet ja ohjelmistot ja näitä tietolähteitä seurataan säännöllisesti.	3 - Enimmäkseen toteutettu
	11	1f Haavoittuvuusarviointeja suoritetaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.	3 - Enimmäkseen toteutettu
	12	1g Tunnistetut haavoittuvuudet analysoidaan, priorisoidaan ja niihin puututaan tilanteen edellyttämin keinoin.	3 - Enimmäkseen toteutettu
		1h Ohjelmistokorjausten vaikutus toiminnon operatiiviseen toimintaan arvioidaan ennen korjausten asentamista tai rajoitustoimia (mitigation).	3 - Enimmäkseen toteutettu
	10	1i Tietoa löydetyistä kyberturvallisuushaavoittuvuuksista jaetaan organisaation määrittelemille sidosryhmille.	3 - Enimmäkseen toteutettu
3	9	1j Kaikkille toimintoon kuuluvien IT- ja OT-omaisuuserille (laitteet, ohjelmistot ja tietovarannot) on tunnistettu haavoittuvuustietolähteet, joita myös seurataan.	2 - Osittain toteutettu
	11	1k Haav… …iivisesta to…	2 - Osittain toteutettu
	12	1l Haavoittuvuu… …toimenpiteiden katselmus, jolla varmistetaan, että haavoittuvuuksia rajaavat tai korjaavat toimenpiteet ovat olleet tehokkaita.	2 - Osittain toteutettu
	10	1m Organisaatiolla on prosessit vastaanottaa ja käsitellä ulkoisien sidosryhmien lähettämiä raportteja mahdollisista haavoittuvuuksista (esim Bug Bounty), jotka koskevat organisaation IT- tai OT-laitteita.	3 - Enimmäkseen toteutettu

Kehityspolut 2/2

- Kybermittarin käytännöistä noin 280kpl voidaan ryhmitellä kehityspoluille (73kpl)

Kypsyysmalli sisältää kehityspolkuja, joiden numero on merkitty jokaisen käytännön kohdalle osiovälilehtien D-sarakkeeseen. (muut paitsi CRITICAL)

Kehitys-välilehdellä voit suodatustoiminnolla myös tutkia eri polkuja ja vastauksia yksittäisiin käytäntöihin.
Kuvaus kehityspoluista:
https://c2m2.doe.gov/C2M2%20Self-Evaluation%20Guide.pdf Appendix C:Related practices, Table 7: Practice progression

Tavoitteena jatkossa sisällyttää tiedot myös koulutusmateriaaleihin. (31.10.2024)

nro	Välilehti	Kehityspolut	Subject of Progression
1	ASSET	IT- ja OT-omaisuuden rekisteri	IT and OT asset inventory
2	ASSET	Omaisuuserien priorisointi	Prioritization of inventoried assets
3	ASSET	Tietovarantojen hallinta	Information asset inventory
4	ASSET	Luetteloidun omaisuuden luokittelu	Categorization of inventoried assets
5	ASSET	Vakioitujen perusasetusten määritys ja ylläpito	Creating and maintaining configuration baselines
6	ASSET	Vakioitujen perusasetusten käyttö	Using configuration baselines
7	ASSET	Muutosten ja päivitysten tekeminen turvallisesti	Making changes to assets in a secure manner
8	ASSET	Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtyjen muutosten dokumentointi	Documentation of changes to assets

Tiedonvaihdon oleellisimmat käytännöt (10 kpl)

- Oman raportin sovellus, johon on valittu olennaisimmat tiedonvaihtoon liittyvät käytännöt
  - Listaus arvioiduista käytännöistä, jotka liittyvät tiedonvaihtoon. Tulokset haetaan automaattisesti välilehdiltä.
  - Esimerkki: Organisaatio saa arvioinnissa kerralla yleiskuvan vastauksistaan tiedonvaihdon käytäntöihin
  - Kybermittarissa välilehdellä ”Tiedonvaihto”

Taso	Avain	Käytäntö	Lisätieto	Vastaus
2	RESPONSE-2g	Sisäiset ja ulkoiset sidosryhmät (esimerkiksi johtajat, lakimiehet, viranomaiset, kumppanit, palveluntoimittajat, toimialan muut organisaatiot, ISAC-ryhmät tai organisaation muut sisäiset ja ulkoiset sidosryhmät) on tunnistettu ja näitä informoidaan kyberturvallisuustapahtumista ja -poikkeamista tilannekuva-osiossa määritettyjen raportointivaatimusten mukaisesti [kts. SITUATION-3d].		3
1	RESPONSE-3c	Kyberpoikkeamista tuotetaan raportointia (esimerkiksi sisäisesti, CERT-FI tai soveltuville ISAC-ryhmille). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.		3
2	RESPONSE-3f	Kyberpoikkeamien hallintasuunnitelma sisältää viestintäsuunnitelman, joka kattaa sekä sisäiset että ulkoiset sidosryhmät		2
2	RISK-1d	Kyberriskienhallinnan toimenpiteistä jaetaan tietoa soveltuville sidosryhmille.		3
2	SITUATION-3a	Toiminnon kyberturvallisuuden tilannekuvan viestimiseksi on määritetty menetelmät, joita päivitetään säännöllisesti.		3

Keskinäisriippuvuudet

- Oman raportin sovellus, jonka avulla voidaan tarkistaa arvioinnin vastausten loogisuus
  - Listaus arvioitavista käytännöistä, joilla on selkeitä riippuvuuksia toisista käytännöistä eli käytäntö ei voi esimerkiksi toteutua ellei toinen käytäntö ole toteutettu.
  - Esimerkki: jos kyberturvallisuus-vaatimuksia ei ole määritelty (ARCHITECTURE-1f) niin perusasetukset eivät voi sisältää niitä. (ASSET-3c)
  - Kybermittarissa välilehdellä ”Riippuvuudet”

Taso	Avain	Käytäntö	Riippuvuus	Vastaus
2	ARCHITECTURE-1f	Kyberarkkitehtuuri määrittää kyberturvallisuusvaatimukset toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille.		1
2	ASSET-3c	Vakioidut perusasetukset sisältävät soveltuvilta osin organisaation kyberarkkitehtuurissa määritellyt vaatimukset [kts. ARCHITECTURE-1f].	ARCHITECTURE-1f (cybersecurity requirements)	3
2	PROGRAM-1b	Kyberturvallisuusstrategia määrittelee organisaation kyberturvallisuustavoitteet.		2
2	ARCHITECTURE-1b	Kyberarkkitehtuurin kehittämiseksi on määritetty suunnitelma tai strategia, jota ylläpidetään. Kyberarkkitehtuurin kehittämissuunnitelma tukee organisaation kyberturvallisuusstrategiaa [kts. PROGRAM-1b] ja yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri") sekä noudattaa niiden periaatteita ja vaatimuksia.	PROGRAM-1b (cybersecurity program strategy)	2
2	RISK-1b	Organisaation kyberriskienhallintaa ohjaa järjestelmällinen toimintasuunnitelma, jota ylläpidetään säännöllisesti ja joka tukee organisaation laajempaa kyberturvallisuuden kehittämisen suunnitelmaa [kts. PROGRAM-1b) ja organisaation yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri").	PROGRAM-1b (cybersecurity program strategy)	2
2	RISK-3b	Määriteltyjä kriteerejä käytetään kyberriskien priorisoinnissa (esimerkiksi vaikutus organisaatioon, yhteiskunnallinen vaikutus, todennäköisyys, alttius, riskinsietokyky).		2
3	RESPONSE-2h	Kyberpoikkeamien määrittämisen kriteeristö on linjassa kyberriskien priorisoinnin kriteereiden kanssa [kts. RISK-3b].	RISK-3b (cyber risk prioritization criteria)	2

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toteuta arviointi

Osiot ja tavoitteet

CRITICAL Kriittisten palveluiden suojaaminen

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

Tavoitteet:

1. Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
2. Kriittisten palveluiden hallinta
3. Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

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

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

1. Laitteiden ja ohjelmistojen hallinta
2. Tietovarantojen hallinta
3. Konfiguraation hallinta
4. Muutoksenhallinta
5. 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

1. Haavoittuvuuksien vähentäminen
2. Uhkien torjunta ja uhkatiedon jakaminen
3. Yleisiä hallintatoimia

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:

1. Kyberriskienhallinnan suunnitelma
2. Kyberriskien tunnistaminen
3. Riskien analysointi
4. Riskeihin reagointi
5. 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. Heikko pääsynhallinta voi johtaa laitteiden, ohjelmistojen tai tiedon luvattomaan käyttöön, julkistamiseen, tuhoamiseen tai peukalointiin. Lisäksi se nostaa tarpeettomasti organisaation riskitaso.a

Tavoitteet

1. Identiteettien luominen ja hallinta
2. Loogisten käyttöoikeuksien hallinta
3. Fyysinen pääsynhallinta
4. 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

1. Lokienhallinta
2. Ympäristöjen valvonta
3. Tilannekuvan ylläpito
4. 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

1. Tapahtumien havainnointi
2. Tapahtumien analysointi ja häiriötilanteiden määrittäminen
3. Tapahtumiin ja häiriöihin reagoiminen
4. Kyberturvallisuus osana toiminnan jatkuvuutta
5. Yleisiä hallintatoimia

THIRD-PARTIES
Toimitusketjun ja ulkoisten riippuvuuksien hallinta

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

Riippuvuusriskien hallinta sisältää hallintatoimenpiteitä kuten riippumatonta testausta, koodikatselmointeja, haavoittuvuusskannauksia tai turvallisen ohjelmistokehityksen vaatimuksia. Toimittajien, alihankkijoiden ja muiden kolmansien osapuolten kanssa solmitut sopimukset tuotteista ja palveluista tulee tarkastaa ja hyväksyttää kyberriskien hallinnan näkökulmasta. Toimittajille ja palveluille voidaan asettaa valvonta- ja auditointivaatimuksia varmistamaan, että ne täyttävät niille asetetut kyberturvallisuus- ja toimintakykyvaatimukset.

Tavoitteet

1. Kumppaniverkoston tunnistaminen ja priorisointi
2. Kumppaniverkostoon liittyvien riskien hallinta
3. 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

1. Kyberturvallisuuden vastuiden jakaminen
2. Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen
3. Henkilöstöhallinnon prosessit
4. Koulutus ja kybertietoisuuden lisääminen
5. 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

1. Kyberarkkitehtuurin kehittäminen
2. Tietoverkkojen suojaus osana kyberarkkitehtuuria
3. Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria
4. Sovellusturvallisuus osana kyberarkkitehtuuria
5. Tietojen suojaus osana kyberarkkitehtuuria
6. 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

1. Kyberturvallisuusstrategia
2. Johdon tuki kyberturvallisuusohjelmalle
3. Yleisiä hallintatoimia

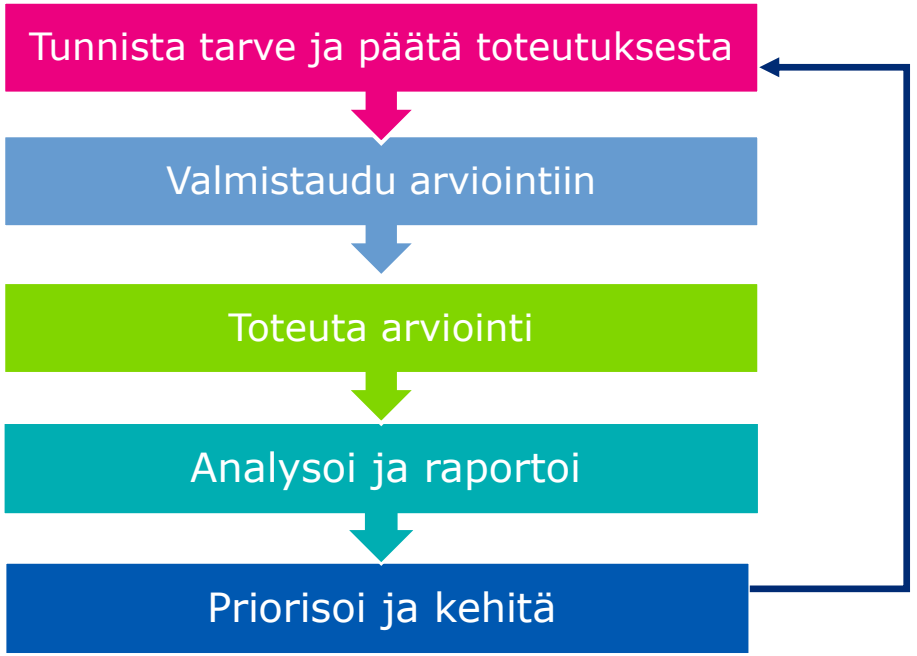
YLEISIÄ HALLINTATOIMIA
Yhteinen tavoite kaikkien osioiden arvioinnissa

- Seuraavat käytännöt arvioidaan erikseen jokaisen osion yhteydessä *(pl. osio CRITICAL)*:
  - A. Osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti. (kypsyystaso 2)
  - B. Osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut). (kypsyystaso 2)
  - C. Osion toimintaa ohjataan vaatimuksilla, jotka on asetettu organisaation johtotason politiikassa (tai vastaavassa ohjeistuksessa). (kypsyystaso 3)
  - D. Osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on osoitettu soveltuville työntekijöille. (kypsyystaso 3)
  - E. Osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen. (kypsyystaso 3)
  - F. Osion toiminnan vaikuttavuutta arvioidaan ja seurataan. (kypsyystaso 3)
- 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

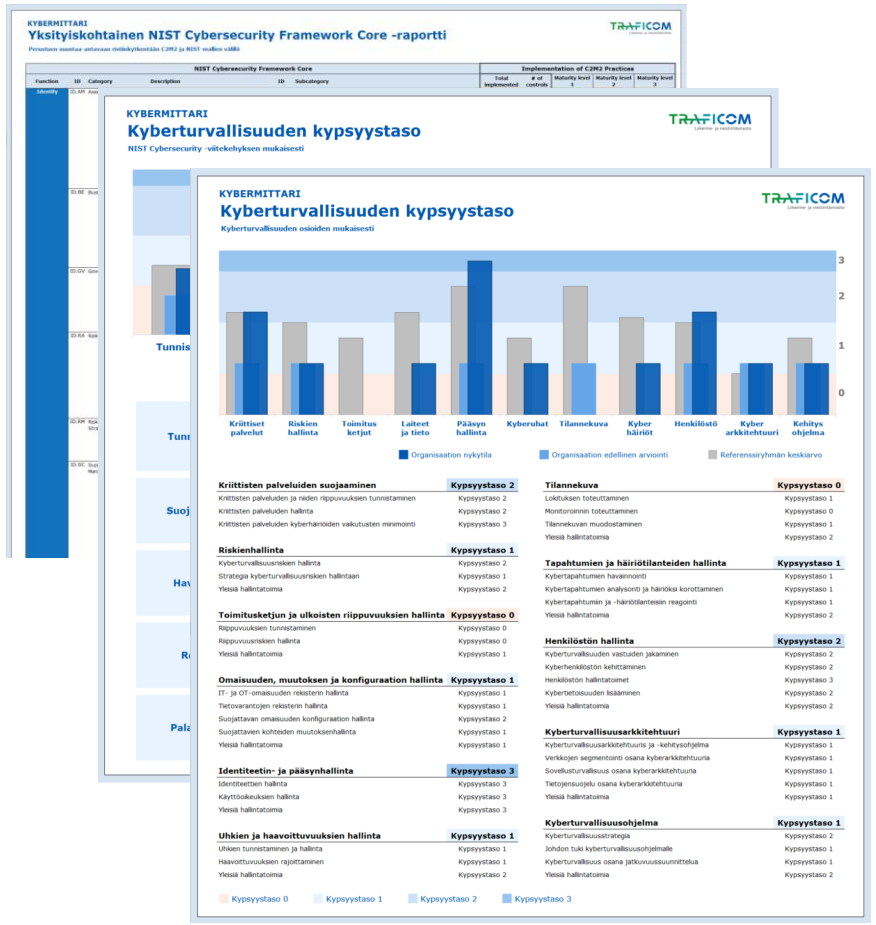
Analysoi ja raportoi

Analysoi ja raportoi



- **Osallistujat:**
  - Arvioinnin vetäjä, arvioinnin sponsori, organisaation asiantuntijat ja kehityssuunnitelmien omistajat.
- **Tehtävä:**
  - Tunnistetaan raportointia tarvitsevat sidosryhmät ja tarpeet
  - Analysoidaan arvioinnin tulokset ja ja verrataan mahdolliin aiempiin tuloksiin tai tavoitetasoon
  - Määrittää mahdollinen toiminnan tavoitetaso
  - Tunnistaa ja priorisoida tärkeimmät kehitystoimenpiteet

Arviointityökalun raportit tulosten analysoinnin ja tavoitetason asettamisen tukena



- Työkalu tuottaa automaattisesti useita erilaisia raportteja
- Kypsyystasoraportit ovat
  - Johdolle suunnattu kypsyysraportti R1 (NIST CSF)
  - Kybermittarin kypsyysraportti R2 (C2M2)
- Raportteja on mahdollista rikastaa vertailutiedolla organisaation aiemmasta arvioinnista tai esimerkiksi viiteryhmän keskiarvotuloksilla

Raporttien käyttöohjeet

Vinkit

Tarkoitus: Raportilla esitetään osiokohtaiset tulokset pylväsdiagrammina sekä taulukoinnissa listataan osioiden lisäksi myös tavoitekohtaiset kypsyystasot.

Tulkinta: Tulokset esitetään yhdentoista Kybermittarin kypsyystasoa esittävän osion mukaisesti. Jokaisen osion kypsyystaso esitetään tasoille nollasta kolmeen. Osiokohtaisen kuvaajan lisäksi, raportti esittää jokaisen tavoitteen kypsyystason.

Kypsyysmalli. Kypsyystasojen laskentamalli noudattaa Kybermittarin laskentamallia. Huomionarvoista on, että C2M2-mallin pisteytykseen verrattuna Kybermittari käyttää kevennettyä arviointia kypsyystasoilla 2 ja 3. Tason voi saavuttaa, kun vähintään 50% kyseisen tason käytännöistä on täytetty kunkin tavoitteen osalta. C2M2-viitekehyksen käytäntöjen lisäksi Kybermittarissa on Kriittisten palveluiden suojaamista arvioiva CRITICAL-välilehti.

Taso 0: Toiminta ei täytä perustavanlaatuisia vaatimuksia;
Taso 1: Toiminta täyttää perustavanlaatuiset vaatimukset, mutta voi olla vielä ajoittaista ja toiminnan taso voi vaihdella tapauskohtaisesti;
Taso 2: Toiminta on edistyneempää ja kattavampaa kuin alemmalla tasolla, minkä lisäksi kyberturvallisuuden hallintaa kuvaavat:
- Dokumentoidut prosessit ja käytänteet;
- Riittävä resursointi ja osaaminen; sekä
- Määritetyt roolit ja vastuut.

Taso 3: Toiminta on edistynyttä ja kattavaa, minkä lisäksi kyberturvallisuuden hallintaa kuvaavat:
- Toimintaa ohjaa organisaation politiikka (tai vastaava ohjeistus);
- Toiminnalle on asetettu suoritustavoitteet, joita seurataan; sekä
- Dokumentoidut prosessit ja käytänteet ovat organisaation normien mukaisia ja niiden kehitys on jatkuvaa.

- Raportti-välilehtien oikeassa laidassa on vinkit
  - Raportin tarkoituksen kuvaus
  - Tulkintaohjeet
  - Vinkit ovat tällä hetkellä vain suomenkielellä

Vertailutiedot

Aiemmat arviointitulokset
Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa.

Johdon kypsyysraportti (R1)

(ENG) Domain	(ENG) Answer
Identify	40 %
Protect	50 %
Detect	34 %
Respond	33 %
Recover	45 %

Kybermittarin kypsyysraportti (R2)

(ENG) Domain	(ENG) Answer
CRITICAL	0
ASSET	1
THREAT	0
RISK	0
ACCESS	1
SITUATION	1
RESPONSE	0
THIRD-PARTIES	0
WORKFORCE	1
ARCHITECTURE	0
PROGRAM	0

R1_V20

(ENG) Domain	(ENG) Answer
Govern	35 %
Identify	40 %
Protect	44 %
Detect	56 %
Respond	55 %
Recover	58 %

Vertailutulokset (raporteille)
Tähän taulukkoon syötetyt vertailutiedot esitetään raporteissa.

Johdon kypsyysraportti (R1)

(ENG) Domain	(ENG) Answer
Identify	45 %
Protect	55 %
Detect	50 %
Respond	60 %
Recover	65 %

Kybermittarin kypsyysraportti (R2)

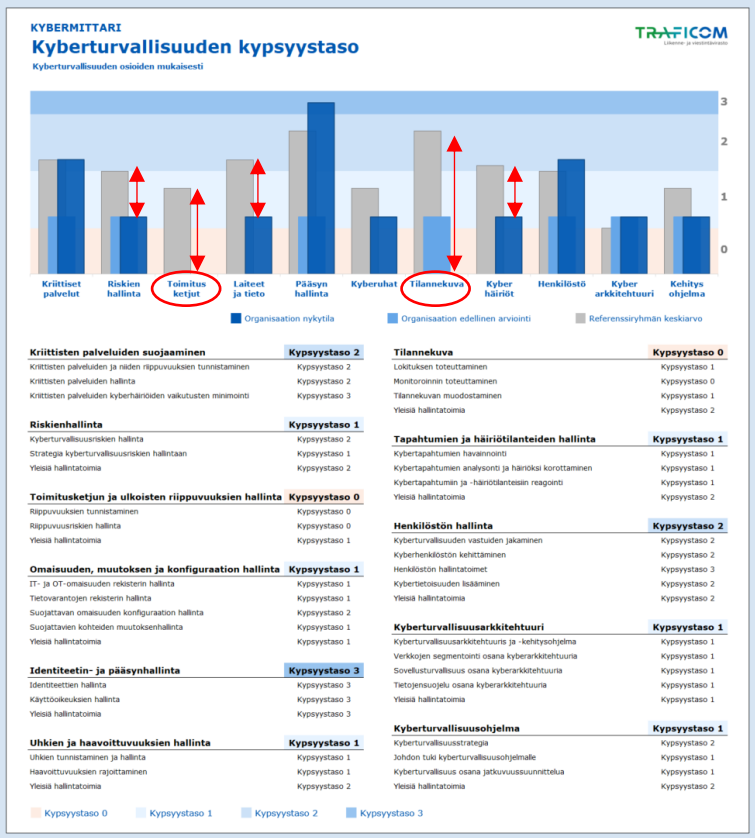
(ENG) Domain	(ENG) Answer
CRITICAL	0,5
ASSET	1,2
THREAT	0,9
RISK	0,7
ACCESS	1,2
SITUATION	1,3
RESPONSE	1,5
THIRD-PARTIES	0,6
WORKFORCE	1
ARCHITECTURE	0,4
PROGRAM	0,8

R1_V20

(ENG) Domain	(ENG) Answer
Govern	50 %
Identify	45 %
Protect	38 %
Detect	44 %
Respond	60 %
Recover	65 %

- Vertailutiedot
  - Työkalun raportteja voi rikastaa lisäämällä vertailutietoa Import-välilehden kautta
  - Tiedot luetaan automaattisesti työkalun tuottamiin raportteihin
  - Vertailutieto voi perustua esimerkiksi edellisiin tuloksiin, toimialan keskiarvoihin tai organisaation itselleen asettamaan tavoitetasoon

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
Kyberturvallisuusarkkitehtuurin 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

Keskinäisriippuvuudet

- Oman raportin sovellus, jonka avulla voidaan tarkistaa arvioinnin vastausten loogisuus
  - Listaus arvioitavista käytännöistä, joilla on selkeitä riippuvuuksia toisista käytännöistä eli käytäntö ei voi esimerkiksi toteutua ellei toinen käytäntö ole toteutettu.
  - Esimerkki: jos kyberturvallisuus-vaatimuksia ei ole määritelty (ARCHITECTURE-1f) niin perusasetukset eivät voi sisältää niitä. (ASSET-3c)
  - Kybermittarissa välilehdellä ”Riippuvuudet”

Taso	Avain	Käytäntö	Riippuvuus	Vastaus
2	ARCHITECTURE-1f	Kyberarkkitehtuuri määrittää kyberturvallisuusvaatimukset toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille.		1
2	ASSET-3c	Vakioidut perusasetukset sisältävät soveltuvilta osin organisaation kyberarkkitehtuurissa määritellyt vaatimukset [kts. ARCHITECTURE-1f].	ARCHITECTURE-1f (cybersecurity requirements)	3
2	PROGRAM-1b	Kyberturvallisuusstrategia määrittelee organisaation kyberturvallisuustavoitteet.		2
2	ARCHITECTURE-1b	Kyberarkkitehtuurin kehittämiseksi on määritetty suunnitelma tai strategia, jota ylläpidetään. Kyberarkkitehtuurin kehittämissuunnitelma tukee organisaation kyberturvallisuusstrategiaa [kts. PROGRAM-1b] ja yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri") sekä noudattaa niiden periaatteita ja vaatimuksia.	PROGRAM-1b (cybersecurity program strategy)	2
2	RISK-1b	Organisaation kyberriskienhallintaa ohjaa järjestelmällinen toimintasuunnitelma, jota ylläpidetään säännöllisesti ja joka tukee organisaation laajempaa kyberturvallisuuden kehittämisen suunnitelmaa [kts. PROGRAM-1b) ja organisaation yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri").	PROGRAM-1b (cybersecurity program strategy)	2
2	RISK-3b	Määriteltyjä kriteerejä käytetään kyberriskien priorisoinnissa (esimerkiksi vaikutus organisaatioon, yhteiskunnallinen vaikutus, todennäköisyys, alttius, riskinsietokyky).		2
3	RESPONSE-2h	Kyberpoikkeamien määrittämisen kriteeristö on linjassa kyberriskien priorisoinnin kriteereiden kanssa [kts. RISK-3b].	RISK-3b (cyber risk prioritization criteria)	2

Kehityspolut 1/2

- Kehityspolut auttavat löytämään toisiinsa liittyvät, eri kypsyystason käytännöt ja suunnittelemaan tavoitetason riskiperustaisesti ja valitsemaan kehitystoimenpiteitä
- Helpottavat ja nopeuttavat arviointia, koska voi käydä kehityspolun kerrallaan
- Kehityspolut on numeroitu käytäntöriville kypsyystason viereen
  - Lista kehityspoluista ja taulukointi löytyvät Kybermittarin ”Ohje Kehitys” ja ”Kehitys”-välilehdiltä

1		Haavoittuvuuksien vähentäminen	
Taso			Vastaus
1	9	1a	1 - Ei toteutettu tai ei tietoa
	10	1b Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	1 - Ei toteutettu tai ei tietoa
	11	1c Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
	12	1d Toiminnon kannalta olennaisiin haavoittuvuuksiin puututaan (esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
2	9	1e Haavoittuvuustiedon lähteet kattavat korkean prioriteetin laitteet ja ohjelmistot ja näitä tietolähteitä seurataan säännöllisesti.	3 - Enimmäkseen toteutettu
	11	1f Haavoittuvuusarviointeja suoritetaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.	3 - Enimmäkseen toteutettu
	12	1g Tunnistetut haavoittuvuudet analysoidaan, priorisoidaan ja niihin puututaan tilanteen edellyttämin keinoin.	3 - Enimmäkseen toteutettu
		1h Ohjelmistokorjausten vaikutus toiminnon operatiiviseen toimintaan arvioidaan ennen korjausten asentamista tai rajoitustoimia (mitigation).	3 - Enimmäkseen toteutettu
	10	1i Tietoa löydetyistä kyberturvallisuushaavoittuvuuksista jaetaan organisaation määrittelemille sidosryhmille.	3 - Enimmäkseen toteutettu
3	9	1j Kaikkille toimintoon kuuluvien IT- ja OT-omaisuuserille (laitteet, ohjelmistot ja tietovarannot) on tunnistettu haavoittuvuustietolähteet, joita myös seurataan.	2 - Osittain toteutettu
	11	1k	2 - Osittain toteutettu
	12	1l katselmus, jolla varmistetaan, että haavoittuvuuksia rajaavat tai korjaavat toimenpiteet ovat olleet tehokkaita.	2 - Osittain toteutettu
	10	1m Organisaatiolla on prosessit vastaanottaa ja käsitellä ulkoisien sidosryhmien lähettämiä raportteja mahdollisista haavoittuvuuksista (esim Bug Bounty), jotka koskevat organisaation IT- tai OT-laitteita.	3 - Enimmäkseen toteutettu

Kehityspolut 2/2

- Kybermittarin käytännöistä noin 280kpl voidaan ryhmitellä kehityspoluille (73kpl)

Kypsyysmalli sisältää kehityspolkuja, joiden numero on merkitty jokaisen käytännön kohdalle osiovälilehtien D-sarakkeeseen. (muut paitsi CRITICAL)

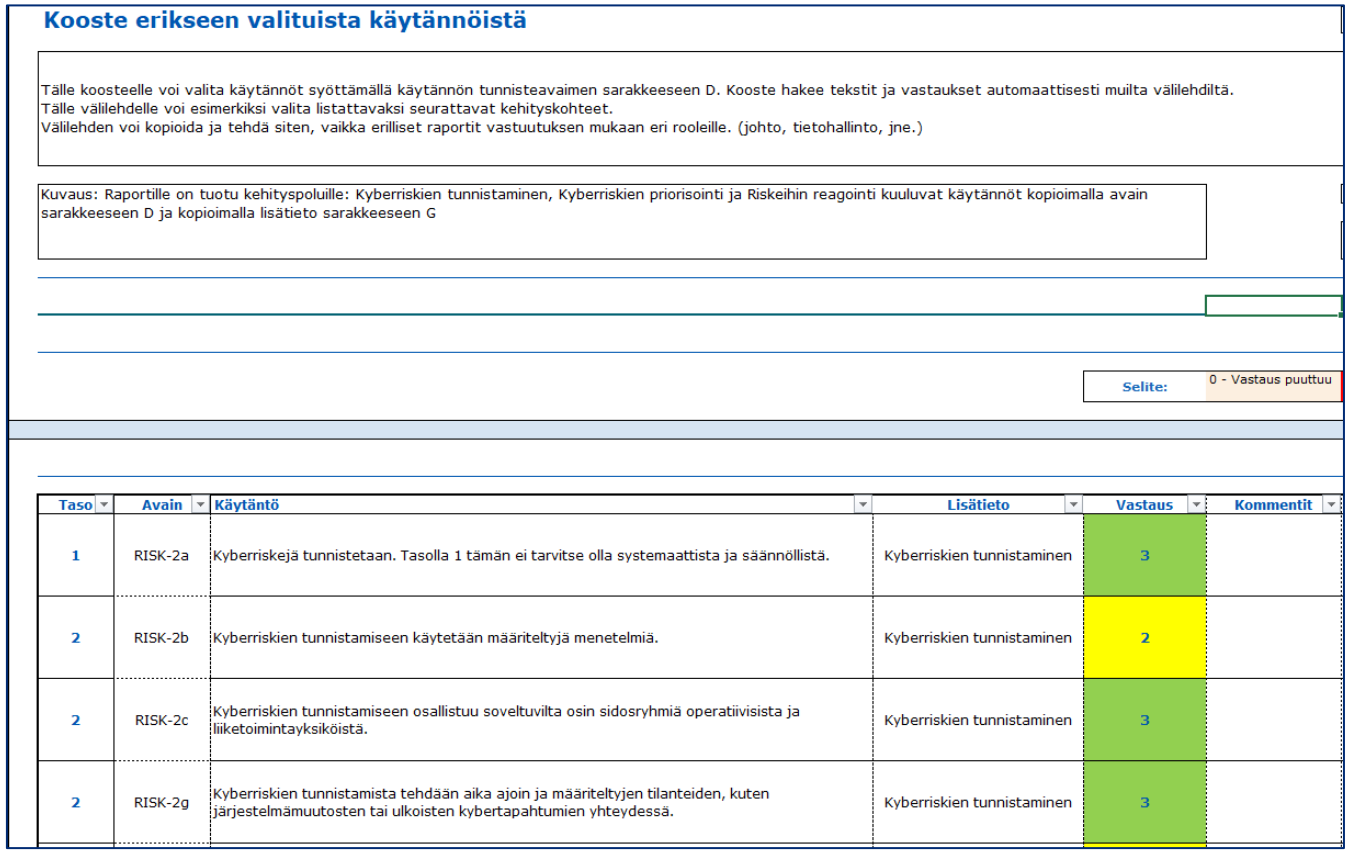
Kehitys-välilehdellä voit suodatustoiminnolla myös tutkia eri polkuja ja vastauksia yksittäisiin käytäntöihin.
Kuvaus kehityspoluista:
https://c2m2.doe.gov/C2M2%20Self-Evaluation%20Guide.pdf Appendix C:Related practices, Table 7: Practice progression

Tavoitteena jatkossa sisällyttää tiedot myös koulutusmateriaaleihin. (31.10.2024)

nro	Välilehti	Kehityspolut	Subject of Progression
1	ASSET	IT- ja OT-omaisuuden rekisteri	IT and OT asset inventory
2	ASSET	Omaisuuserien priorisointi	Prioritization of inventoried assets
3	ASSET	Tietovarantojen hallinta	Information asset inventory
4	ASSET	Luetteloidun omaisuuden luokittelu	Categorization of inventoried assets
5	ASSET	Vakioitujen perusasetusten määritys ja ylläpito	Creating and maintaining configuration baselines
6	ASSET	Vakioitujen perusasetusten käyttö	Using configuration baselines
7	ASSET	Muutosten ja päivitysten tekeminen turvallisesti	Making changes to assets in a secure manner
8	ASSET	Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtyjen muutosten dokumentointi	Documentation of changes to assets

Uudet, muokattavat raportit

- Oma raportti – ominaisuuden tarkoitus on helposti luoda listauksia halutuista käytännöistä vastauksineen
- Käyttökohde-esimerkit
  - Kehityskohteiden seuranta
  - Tavoitteenasettelu ja vastuuttaminen tiimeille
  - Tietyn aiheen käytännöt (vrt. kehityspolut),
- Kybermittarissa välilehdellä ”Oma raportti”



Kooste erikseen valituista käytännöistä

Tälle koosteelle voi valita käytännöt syöttämällä käytännön tunnisteavaimen sarakkeeseen D. Kooste hakee tekstit ja vastaukset automaattisesti muilta välilehdiltä.
Tälle välilehdelle voi esimerkiksi valita listattavaksi seurattavat kehityskohteet.
Välilehden voi kopioida ja tehdä siten, vaikka erilliset raportit vastuutuksen mukaan eri rooleille. (johto, tietohallinto, jne.)

Kuvaus: Raportille on tuotu kehityspoluille: Kyberriskien tunnistaminen, Kyberriskien priorisointi ja Riskeihin reagointi kuuluvat käytännöt kopioimalla avain sarakkeeseen D ja kopioimalla lisätieto sarakkeeseen G

Selite: 0 - Vastaus puuttuu

Taso	Avain	Käytäntö	Lisätieto	Vastaus	Kommentit
1	RISK-2a	Kyberriskejä tunnistetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	Kyberriskien tunnistaminen	3	
2	RISK-2b	Kyberriskien tunnistamiseen käytetään määriteltyjä menetelmiä.	Kyberriskien tunnistaminen	2	
2	RISK-2c	Kyberriskien tunnistamiseen osallistuu soveltuvilta osin sidosryhmiä operatiivisista ja liiketoimintayksiköistä.	Kyberriskien tunnistaminen	3	
2	RISK-2g	Kyberriskien tunnistamista tehdään aika ajoin ja määriteltyjen tilanteiden, kuten järjestelmämuutosten tai ulkoisten kybertapahtumien yhteydessä.	Kyberriskien tunnistaminen	3	

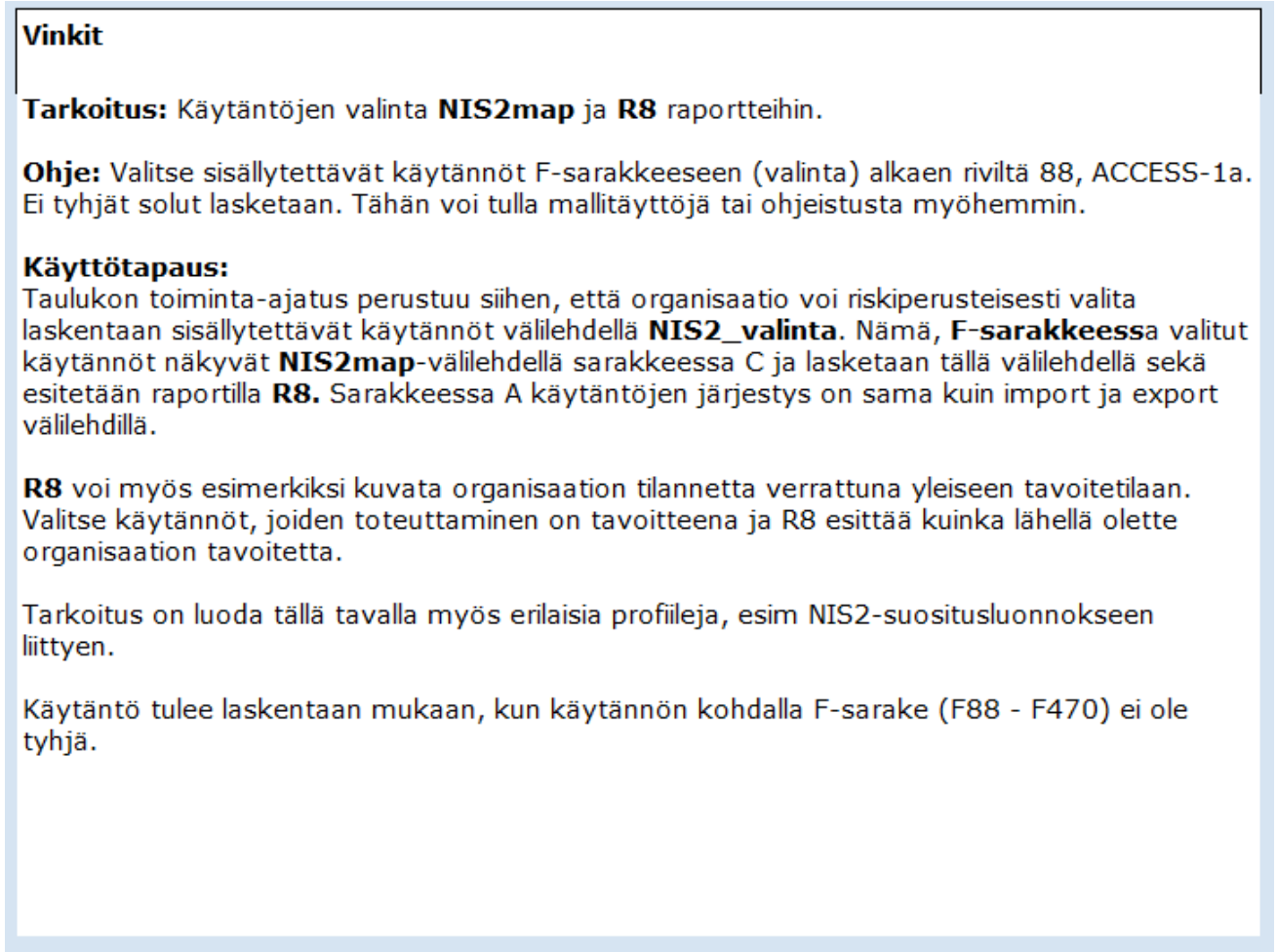
Tiedonvaihdon oleellisimmat käytännöt (10 kpl)

- Oman raportin sovellus, johon on valittu olennaisimmat tiedonvaihtoon liittyvät käytännöt
  - Listaus arvioiduista käytännöistä, jotka liittyvät tiedonvaihtoon. Tulokset haetaan automaattisesti välilehdiltä.
  - Esimerkki: Organisaatio saa arvioinnissa kerralla yleiskuvan vastauksistaan tiedonvaihdon käytäntöihin
  - Kybermittarissa välilehdellä ”Tiedonvaihto”

Taso	Avain	Käytäntö	Lisätieto	Vastaus
2	RESPONSE-2g	Sisäiset ja ulkoiset sidosryhmät (esimerkiksi johtajat, lakimiehet, viranomaiset, kumppanit, palveluntoimittajat, toimialan muut organisaatiot, ISAC-ryhmät tai organisaation muut sisäiset ja ulkoiset sidosryhmät) on tunnistettu ja näitä informoidaan kyberturvallisuustapahtumista ja -poikkeamista tilannekuva-osiossa määritettyjen raportointivaatimusten mukaisesti [kts. SITUATION-3d].		3
1	RESPONSE-3c	Kyberpoikkeamista tuotetaan raportointia (esimerkiksi sisäisesti, CERT-FI tai soveltuville ISAC-ryhmille). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.		3
2	RESPONSE-3f	Kyberpoikkeamien hallintasuunnitelma sisältää viestintäsuunnitelman, joka kattaa sekä sisäiset että ulkoiset sidosryhmät		2
2	RISK-1d	Kyberriskienhallinnan toimenpiteistä jaetaan tietoa soveltuville sidosryhmille.		3
2	SITUATION-3a	Toiminnon kyberturvallisuuden tilannekuvan viestimiseksi on määritetty menetelmät, joita päivitetään säännöllisesti.		3

Organisaation oma raportti – riskiperustainen 1/2

- NIS2-nimetty raportti antaa organisaation valita riskiperusteisesti raportointiin haluamansa käytännöt
- Käyttökohde-esimerkit
  - Organisaation oma tavoitteenasettelu ja raportit
  - Voidaan antaa myös pohjia, kuten kyberturvallisuuden perustason tietoturvakäytännöt
  - Kybermittarissa välilehdellä ”R8” ja ”NIS2”-alkuiset



Vinkit

Tarkoitus: Käytäntöjen valinta **NIS2map** ja **R8** raportteihin.

Ohje: Valitse sisällytettävät käytännöt F-sarakkeeseen (valinta) alkaen riviltä 88, ACCESS-1a. Ei tyhjät solut lasketaan. Tähän voi tulla mallitäyttöjä tai ohjeistusta myöhemmin.

Käyttötapaus:
Taulukon toiminta-ajatus perustuu siihen, että organisaatio voi riskiperusteisesti valita laskentaan sisällytettävät käytännöt välilehdellä **NIS2_valinta**. Nämä, **F-sarakkeessa** valitut käytännöt näkyvät **NIS2map**-välilehdellä sarakkeessa C ja lasketaan tällä välilehdellä sekä esitetään raportilla **R8.** Sarakkeessa A käytäntöjen järjestys on sama kuin import ja export välilehdillä.

R8 voi myös esimerkiksi kuvata organisaation tilannetta verrattuna yleiseen tavoitetilaan. Valitse käytännöt, joiden toteuttaminen on tavoitteena ja R8 esittää kuinka lähellä olette organisaation tavoitetta.

Tarkoitus on luoda tällä tavalla myös erilaisia profiileja, esim NIS2-suositusluonnokseen liittyen.

Käytäntö tulee laskentaan mukaan, kun käytännön kohdalla F-sarake (F88 - F470) ei ole tyhjä.

Organisaation oma raportti – riskiperustainen 2/2

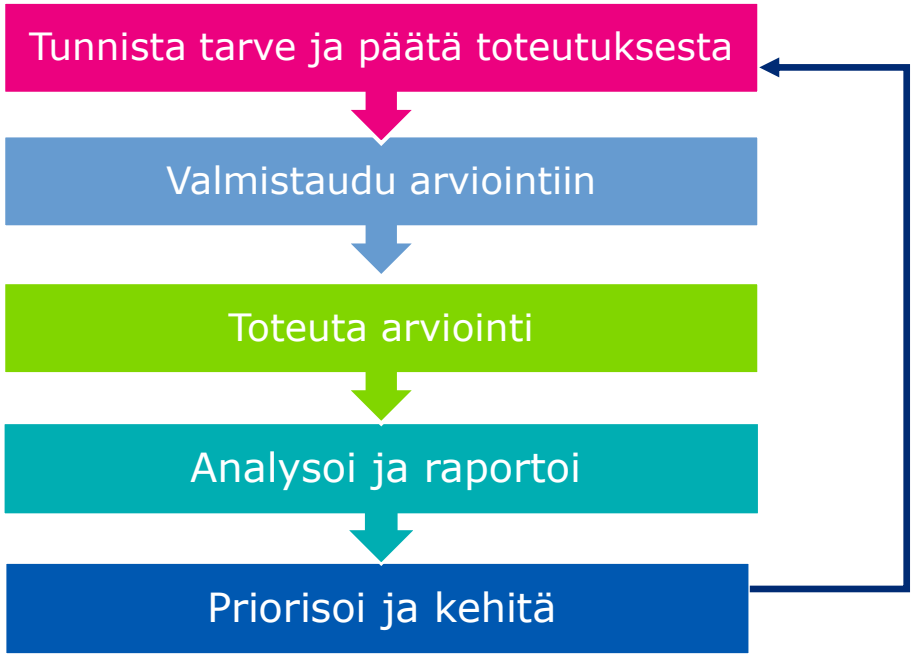
- ”NIS2_valinta” –välilehti
  - Vapaa käytäntöjen valinta
  - Tukee myös erilaisia pohjia
    - Perustason käytännöt
    - Toimialan suositukset

ACCESS-1a	1	Työntekijöille ja muille entiteeteille (kuten prosesseille tai laitteille, jotka tarvitsevat pääsyn toimintoon kuuluviin laitteisiin, ohjelmistoihin tai tietovarantoihin) osoitetaan erilliset identiteetit. (Huom. tällä vaatimuksella ei kuitenkaan rajoiteta jaettujen identiteettien käyttöä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	valittu
ACCESS-1b	1	Työntekijöille ja muille entiteeteille jaetaan pääsyvaltuustiedot (kuten salasanat, älykortit tai avaimet). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	suositus
ACCESS-1c	1	Identiteetit poistetaan käytöstä, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	ISO27001 Ax.x
ACCESS-1d	2	Salasanojen vahvuusvaatimukset ja uudelleenkäytön rajoitukset on määritelty ja niiden noudattaminen on pakollista.	
ACCESS-1e	2	Identiteettien ajantasaisuudesta huolehditaan tarkastamalla ja päivittämällä ne määrätellyin väliajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä tai organisaatiorakenteen muuttuessa.	toimialan riskiprofiili
ACCESS-1f	2	Identiteetit poistetaan käytöstä organisaation määrittelemien enimmäismääräaikojen puitteissa, kun niitä ei enää tarvita.	sääntely

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Priorisoi ja kehitä

Ymmärrä nykytaso ja määritä tavoitetaso, priorisoi ja kehitä



- **Osallistujat:**
  - Kehityssuunnitelmien omistajat, organisaation asiantuntijat sekä organisaation johtoryhmä tai muu päätöksentekoelin.
- **Tehtävä:**
  - Käydään läpi nykytaso ja määritä tavoitetaso
  - Tunnistetaan priorisoitavat kehitystoimet
  - Toteutetaan priorisoidut kehitystoimenpiteet
  - Päätetään arvioinnin päivittämisen ajankohdasta

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

Kehityspolut 1/2

- Kehityspolut auttavat löytämään toisiinsa liittyvät, eri kypsyystason käytännöt ja suunnittelemaan tavoitetason riskiperustaisesti ja valitsemaan kehitystoimenpiteitä
- Helpottavat ja nopeuttavat arviointia, koska voi käydä kehityspolun kerrallaan
- Kehityspolut on numeroitu käytäntöriville kypsyystason viereen
  - Lista kehityspoluista ja taulukointi löytyvät Kybermittarin ”Ohje Kehitys” ja ”Kehitys”-välilehdiltä

1		Haavoittuvuuksien vähentäminen	
Taso			Vastaus
1	9	1a	1 - Ei toteutettu tai ei tietoa
	10	1b Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	1 - Ei toteutettu tai ei tietoa
	11	1c Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
	12	1d Toiminnon kannalta olennaisiin haavoittuvuuksiin puututaan (esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu
2	9	1e Haavoittuvuustiedon lähteet kattavat korkean prioriteetin laitteet ja ohjelmistot ja näitä tietolähteitä seurataan säännöllisesti.	3 - Enimmäkseen toteutettu
	11	1f Haavoittuvuusarviointeja suoritetaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.	3 - Enimmäkseen toteutettu
	12	1g Tunnistetut haavoittuvuudet analysoidaan, priorisoidaan ja niihin puututaan tilanteen edellyttämin keinoin.	3 - Enimmäkseen toteutettu
		1h Ohjelmistokorjausten vaikutus toiminnon operatiiviseen toimintaan arvioidaan ennen korjausten asentamista tai rajoitustoimia (mitigation).	3 - Enimmäkseen toteutettu
	10	1i Tietoa löydetyistä kyberturvallisuushaavoittuvuuksista jaetaan organisaation määrittelemille sidosryhmille.	3 - Enimmäkseen toteutettu
3	9	1j Kaikkille toimintoon kuuluvien IT- ja OT-omaisuuserille (laitteet, ohjelmistot ja tietovarannot) on tunnistettu haavoittuvuustietolähteet, joita myös seurataan.	2 - Osittain toteutettu
	11	1k	2 - Osittain toteutettu
	12	1l katselmus, jolla varmistetaan, että haavoittuvuuksia rajaavat tai korjaavat toimenpiteet ovat olleet tehokkaita.	2 - Osittain toteutettu
	10	1m Organisaatiolla on prosessit vastaanottaa ja käsitellä ulkoisien sidosryhmien lähettämiä raportteja mahdollisista haavoittuvuuksista (esim Bug Bounty), jotka koskevat organisaation IT- tai OT-laitteita.	3 - Enimmäkseen toteutettu

Kehityspolut 2/2

- Kybermittarin käytännöistä noin 280kpl voidaan ryhmitellä kehityspoluille (73kpl)

Kypsyysmalli sisältää kehityspolkuja, joiden numero on merkitty jokaisen käytännön kohdalle osiovälilehtien D-sarakkeeseen. (muut paitsi CRITICAL)

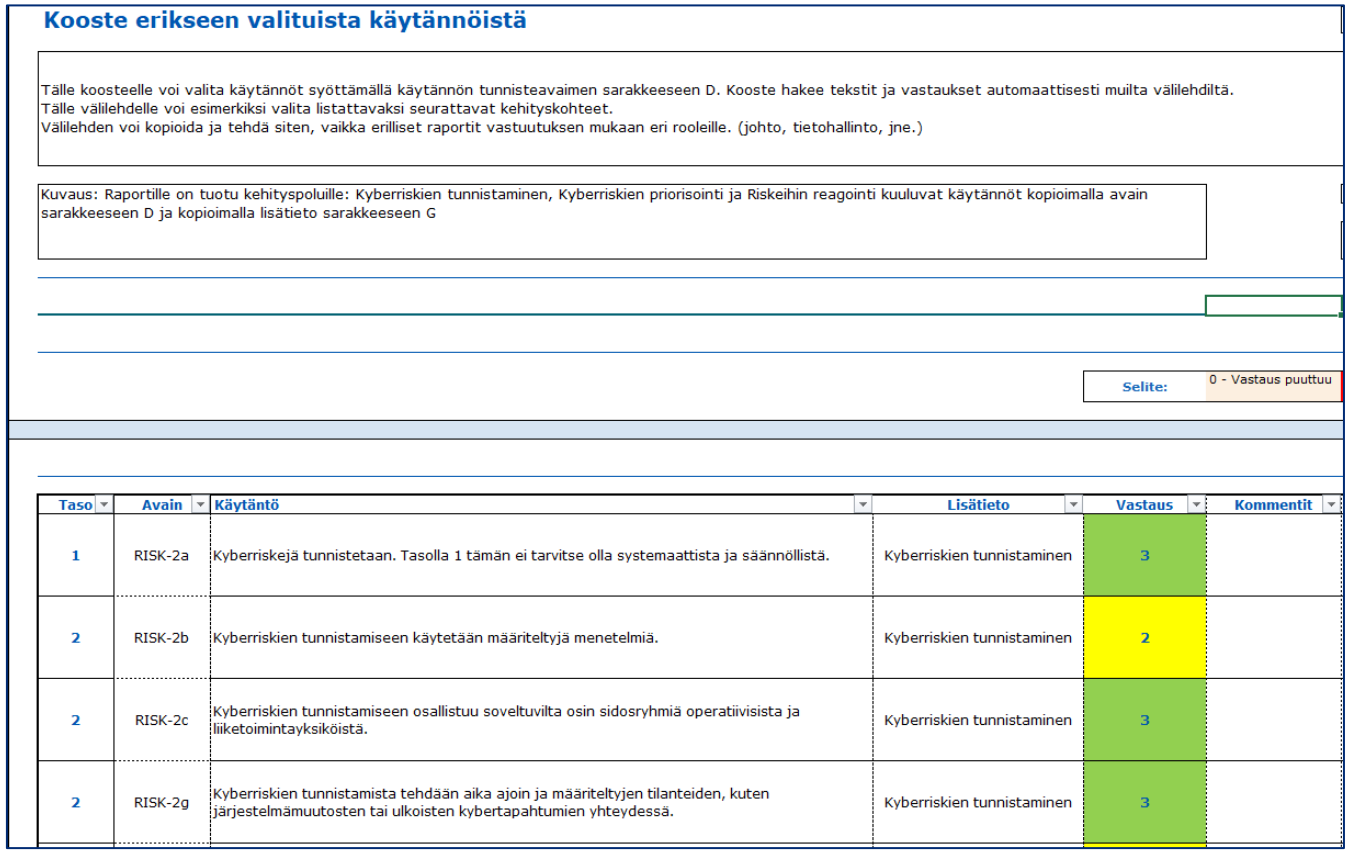
Kehitys-välilehdellä voit suodatustoiminnolla myös tutkia eri polkuja ja vastauksia yksittäisiin käytäntöihin.
Kuvaus kehityspoluista:
https://c2m2.doe.gov/C2M2%20Self-Evaluation%20Guide.pdf Appendix C:Related practices, Table 7: Practice progression

Tavoitteena jatkossa sisällyttää tiedot myös koulutusmateriaaleihin. (31.10.2024)

nro	Välilehti	Kehityspolut	Subject of Progression
1	ASSET	IT- ja OT-omaisuuden rekisteri	IT and OT asset inventory
2	ASSET	Omaisuuserien priorisointi	Prioritization of inventoried assets
3	ASSET	Tietovarantojen hallinta	Information asset inventory
4	ASSET	Luetteloidun omaisuuden luokittelu	Categorization of inventoried assets
5	ASSET	Vakioitujen perusasetusten määritys ja ylläpito	Creating and maintaining configuration baselines
6	ASSET	Vakioitujen perusasetusten käyttö	Using configuration baselines
7	ASSET	Muutosten ja päivitysten tekeminen turvallisesti	Making changes to assets in a secure manner
8	ASSET	Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtyjen muutosten dokumentointi	Documentation of changes to assets

Uudet, muokattavat raportit

- Oma raportti – ominaisuuden tarkoitus on helposti luoda listauksia halutuista käytännöistä vastauksineen
- Käyttökohde-esimerkit
  - Kehityskohteiden seuranta
  - Tavoitteenasettelu ja vastuuttaminen tiimeille
  - Tietyn aiheen käytännöt (vrt. kehityspolut),
- Kybermittarissa välilehdellä ”Oma raportti”



Kooste erikseen valituista käytännöistä

Tälle koosteelle voi valita käytännöt syöttämällä käytännön tunnisteavaimen sarakkeeseen D. Kooste hakee tekstit ja vastaukset automaattisesti muilta välilehdiltä.
Tälle välilehdelle voi esimerkiksi valita listattavaksi seurattavat kehityskohteet.
Välilehden voi kopioida ja tehdä siten, vaikka erilliset raportit vastuutuksen mukaan eri rooleille. (johto, tietohallinto, jne.)

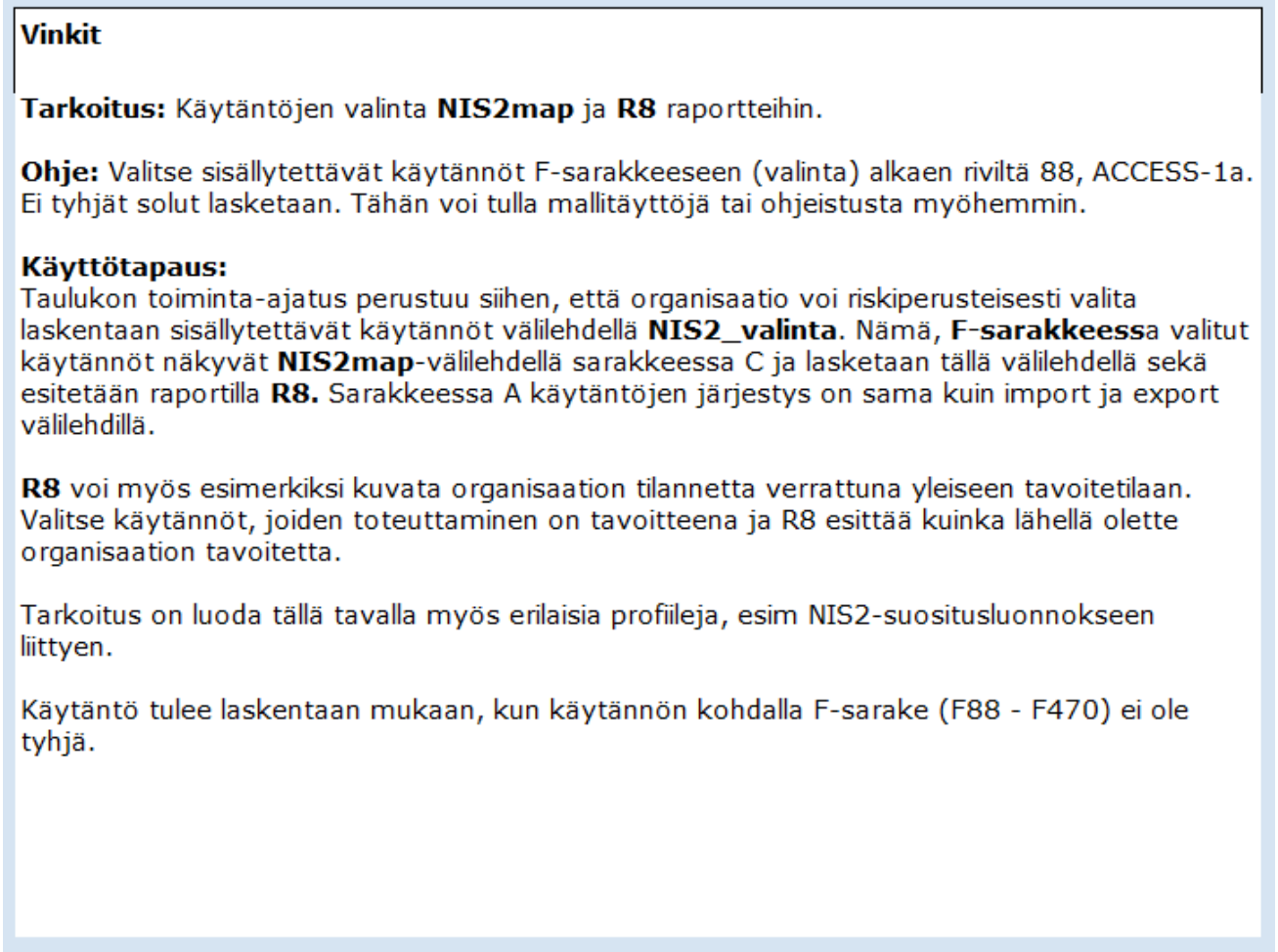
Kuvaus: Raportille on tuotu kehityspoluille: Kyberriskien tunnistaminen, Kyberriskien priorisointi ja Riskeihin reagointi kuuluvat käytännöt kopioimalla avain sarakkeeseen D ja kopioimalla lisätieto sarakkeeseen G

Selite: 0 - Vastaus puuttuu

Taso	Avain	Käytäntö	Lisätieto	Vastaus	Kommentit
1	RISK-2a	Kyberriskejä tunnistetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	Kyberriskien tunnistaminen	3	
2	RISK-2b	Kyberriskien tunnistamiseen käytetään määriteltyjä menetelmiä.	Kyberriskien tunnistaminen	2	
2	RISK-2c	Kyberriskien tunnistamiseen osallistuu soveltuvilta osin sidosryhmiä operatiivisista ja liiketoimintayksiköistä.	Kyberriskien tunnistaminen	3	
2	RISK-2g	Kyberriskien tunnistamista tehdään aika ajoin ja määriteltyjen tilanteiden, kuten järjestelmämuutosten tai ulkoisten kybertapahtumien yhteydessä.	Kyberriskien tunnistaminen	3	

Organisaation oma raportti – riskiperustainen 1/2

- NIS2-nimetty raportti antaa organisaation valita riskiperusteisesti raportointiin haluamansa käytännöt
- Käyttökohde-esimerkit
  - Organisaation oma tavoitteenasettelu ja raportit
  - Voidaan antaa myös pohjia, kuten kyberturvallisuuden perustason tietoturvakäytännöt
  - Kybermittarissa välilehdellä ”R8” ja ”NIS2”-alkuiset



Vinkit

Tarkoitus: Käytäntöjen valinta **NIS2map** ja **R8** raportteihin.

Ohje: Valitse sisällytettävät käytännöt F-sarakkeeseen (valinta) alkaen riviltä 88, ACCESS-1a. Ei tyhjät solut lasketaan. Tähän voi tulla mallitäyttöjä tai ohjeistusta myöhemmin.

Käyttötapaus:
Taulukon toiminta-ajatus perustuu siihen, että organisaatio voi riskiperusteisesti valita laskentaan sisällytettävät käytännöt välilehdellä **NIS2_valinta**. Nämä, **F-sarakkeessa** valitut käytännöt näkyvät **NIS2map**-välilehdellä sarakkeessa C ja lasketaan tällä välilehdellä sekä esitetään raportilla **R8.** Sarakkeessa A käytäntöjen järjestys on sama kuin import ja export välilehdillä.

R8 voi myös esimerkiksi kuvata organisaation tilannetta verrattuna yleiseen tavoitetilaan. Valitse käytännöt, joiden toteuttaminen on tavoitteena ja R8 esittää kuinka lähellä olette organisaation tavoitetta.

Tarkoitus on luoda tällä tavalla myös erilaisia profiileja, esim NIS2-suositusluonnokseen liittyen.

Käytäntö tulee laskentaan mukaan, kun käytännön kohdalla F-sarake (F88 - F470) ei ole tyhjä.

Organisaation oma raportti – riskiperustainen 2/2

- ”NIS2_valinta” –välilehti
  - Vapaa käytäntöjen valinta
  - Tukee myös erilaisia pohjia
    - Perustason käytännöt
    - Toimialan suositukset

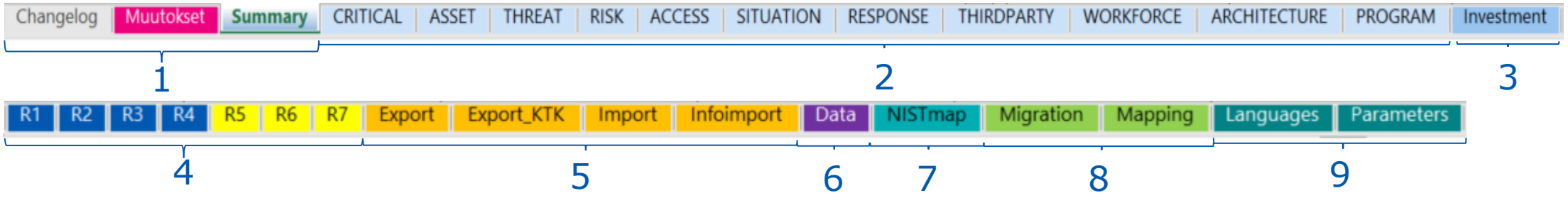
ACCESS-1a	1	Työntekijöille ja muille entiteeteille (kuten prosesseille tai laitteille, jotka tarvitsevat pääsyn toimintoon kuuluviin laitteisiin, ohjelmistoihin tai tietovarantoihin) osoitetaan erilliset identiteetit. (Huom. tällä vaatimuksella ei kuitenkaan rajoiteta jaettujen identiteettien käyttöä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	valittu
ACCESS-1b	1	Työntekijöille ja muille entiteeteille jaetaan pääsyvaltuustiedot (kuten salasanat, älykortit tai avaimet). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	suositus
ACCESS-1c	1	Identiteetit poistetaan käytöstä, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.	ISO27001 Ax.x
ACCESS-1d	2	Salasanojen vahvuusvaatimukset ja uudelleenkäytön rajoitukset on määritelty ja niiden noudattaminen on pakollista.	
ACCESS-1e	2	Identiteettien ajantasaisuudesta huolehditaan tarkastamalla ja päivittämällä ne määrätellyin väliajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä tai organisaatiorakenteen muuttuessa.	toimialan riskiprofiili
ACCESS-1f	2	Identiteetit poistetaan käytöstä organisaation määrittelemien enimmäismääräaikojen puitteissa, kun niitä ei enää tarvita.	sääntely

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointityökalu

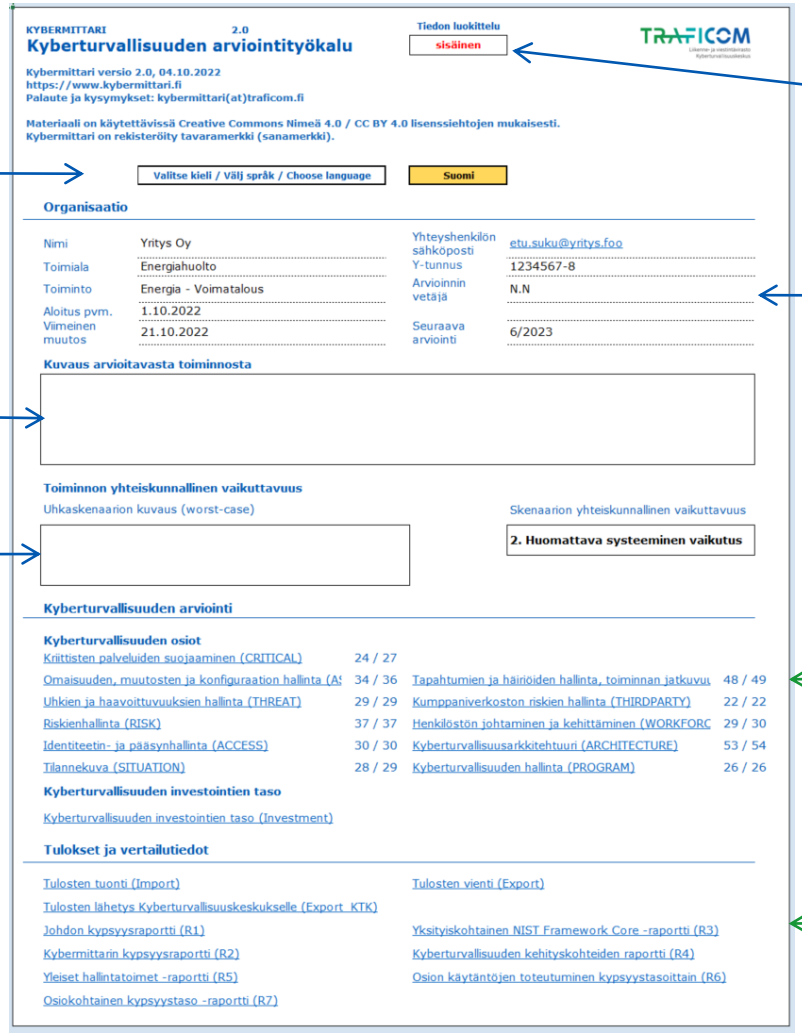
Ohjeita työkalun hyödyntämiseen

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



Kielivalinta

Toiminnan osa-alue

Yhteiskunnallinen vaikuttavuus

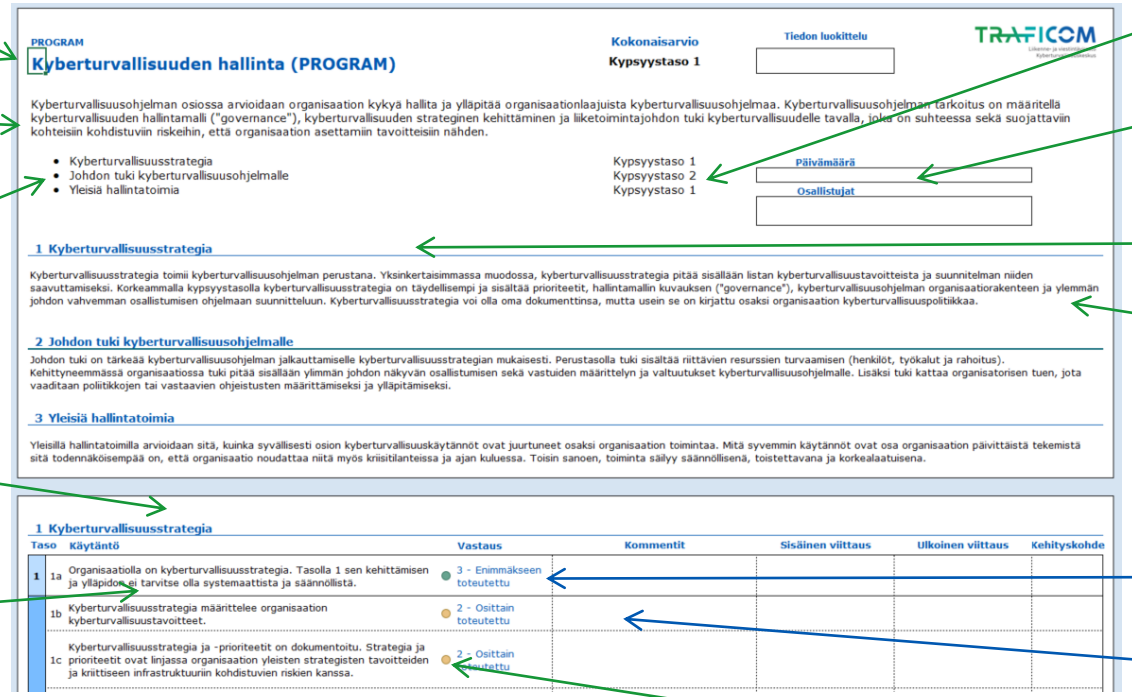
Tiedon luokittelu

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

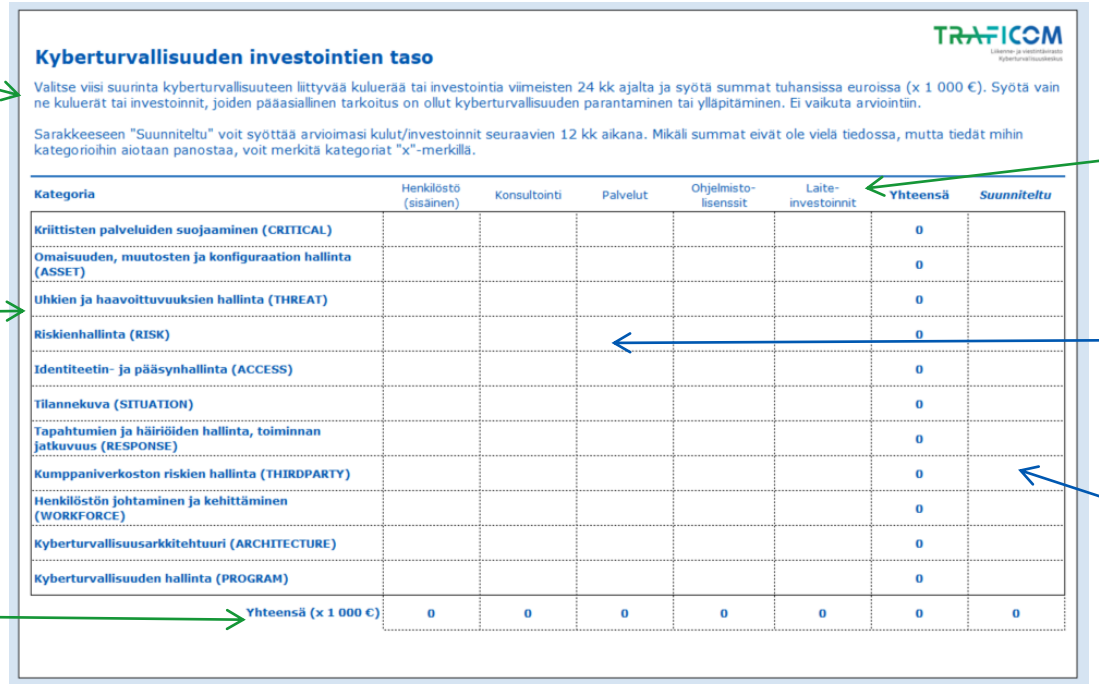
Vastauksen indikaattori

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)

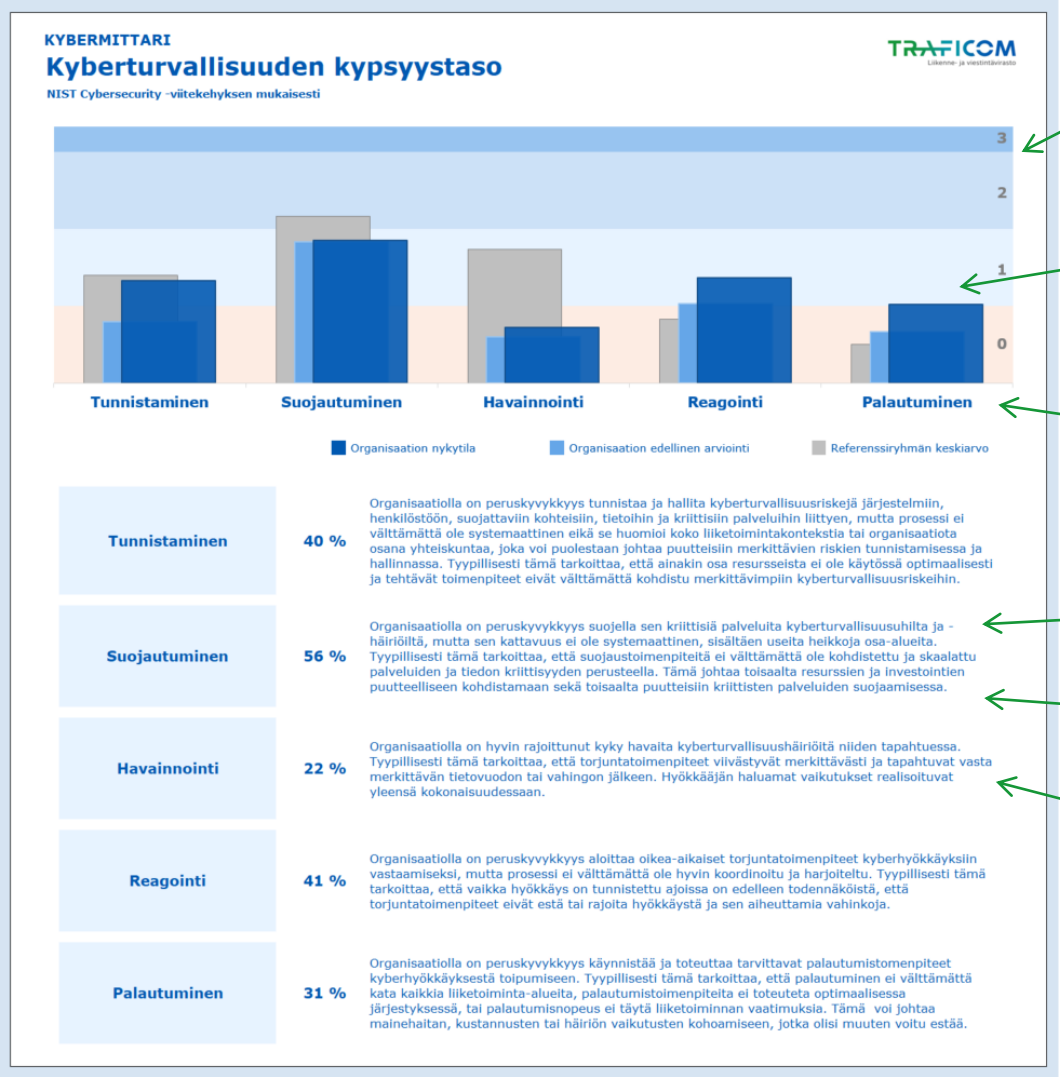
4. Raportoinnin sisältö ja merkittävät muutokset

- 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.
- 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.

4. Raportoinnin sisältö ja merkittävät muutokset

- R7: Kaaviot esittävät yhteenvedon käytäntöjen arvionnista niinkuin ne on arvioitu neliportaisella asteikolla sekä osioittain että sen mukaan, mille kypsyystasolle käytäntö on sijoitettu.
- R8: Muokattava raportti, joka perustuu NIS-osion valintoihin. Voidaan käyttää esimerkiksi organisaation tavoiteseurantaan
- Oma-raportti: Hakee tietyt käytännöt ja niihin annetut vastaukset yhdelle välilehdelle
- Jokaiseen raporttiin on lisätty ohjeita oikeaan yläkulmaan

4. R1 NIST CSF ristiinviittaus



KYBERMITTARI

Kyberturvallisuuden kypsyystaso

NIST Cybersecurity -viitekehyksen mukaisesti

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

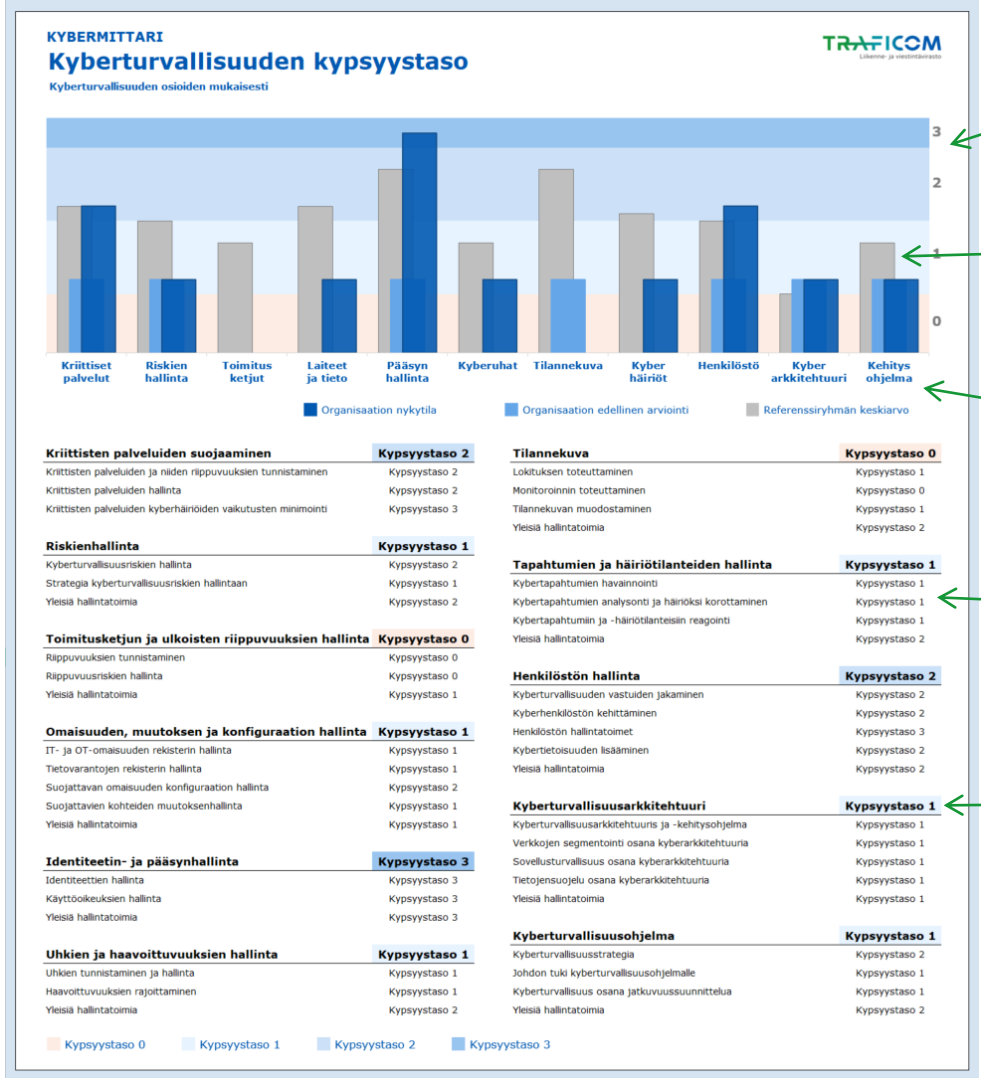
NIST CSF 5 osa-aluetta

Osa-alue

Toteutuneiden käytäntöjen osuus (%)

Sanallinen kuvaus kypsyystasosta

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

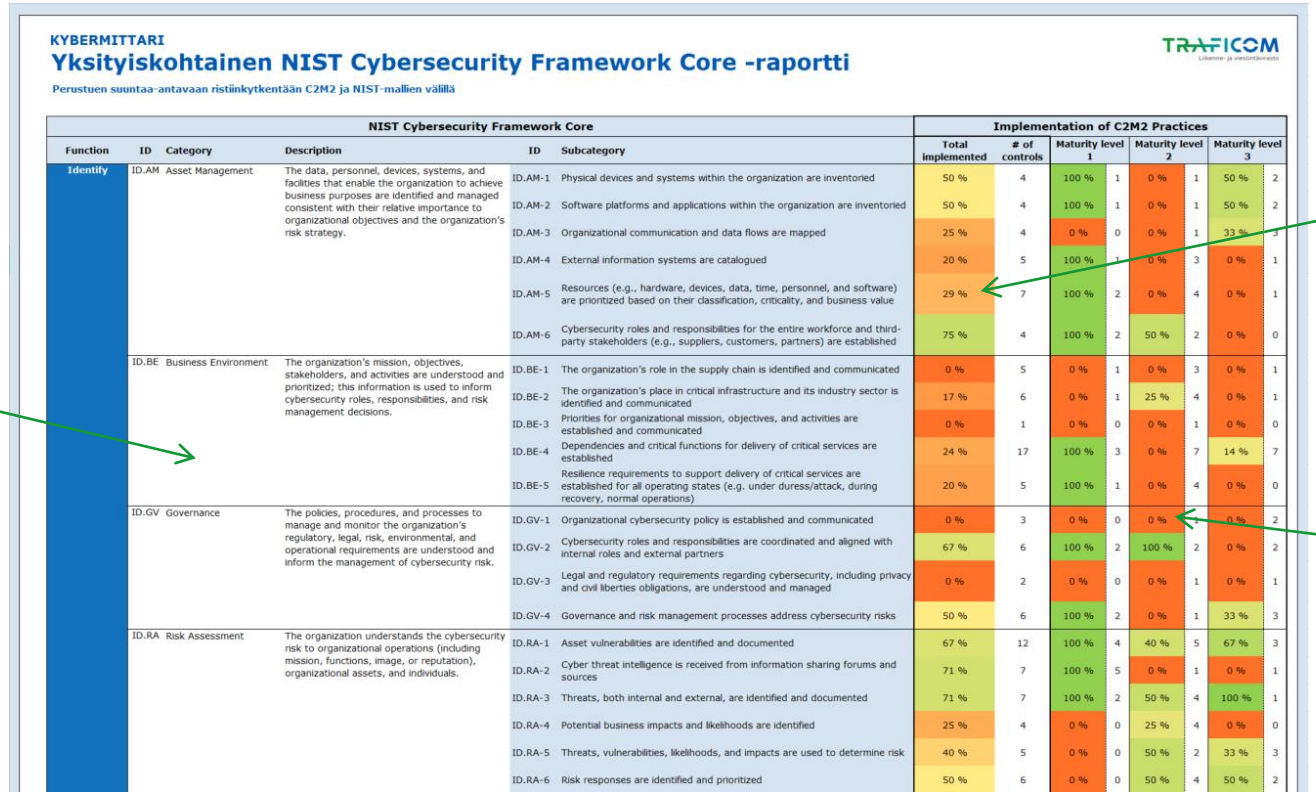
Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

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 %	1
				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

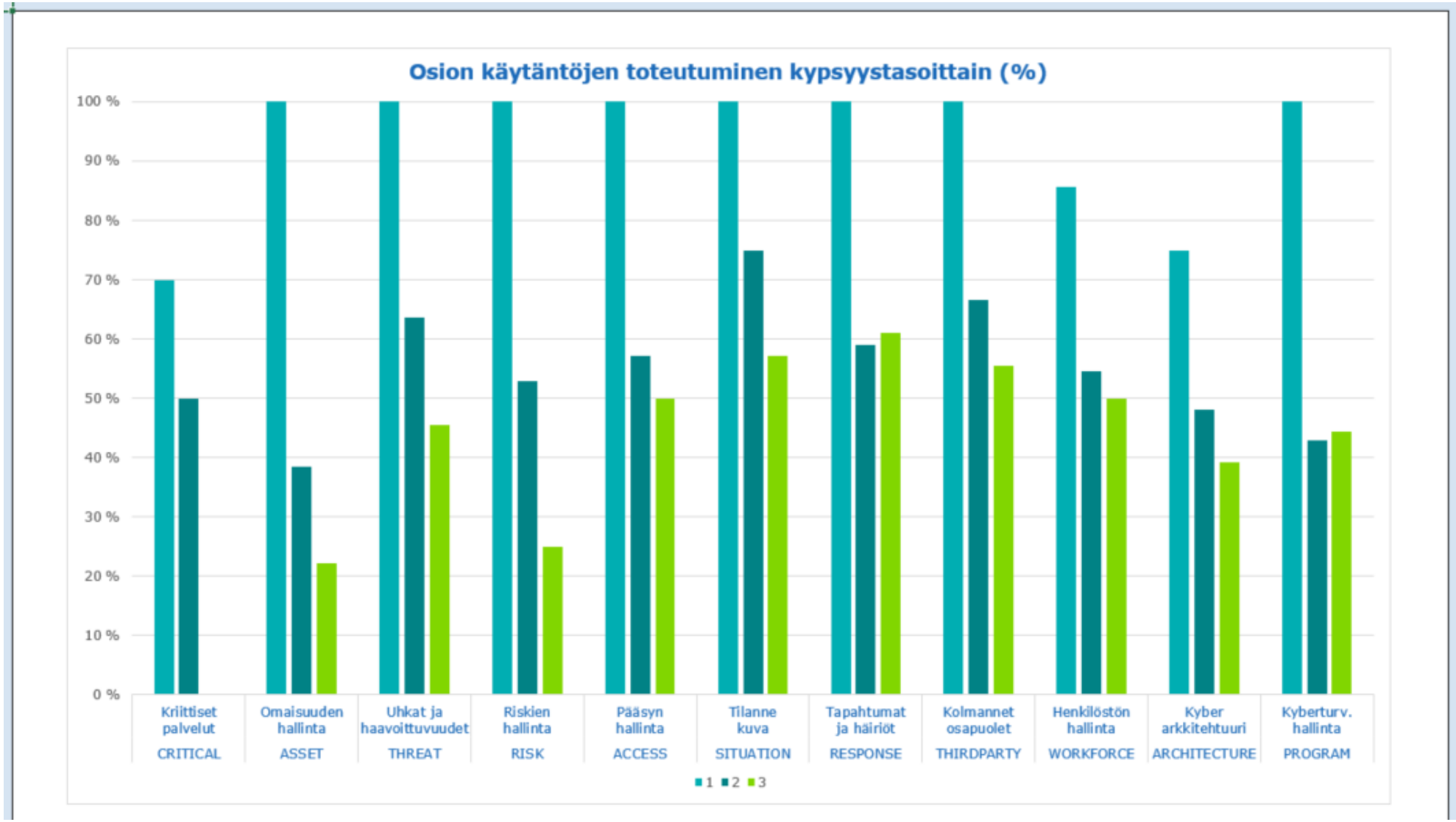
KYBERMITTARI

Yleiset hallintatoimet

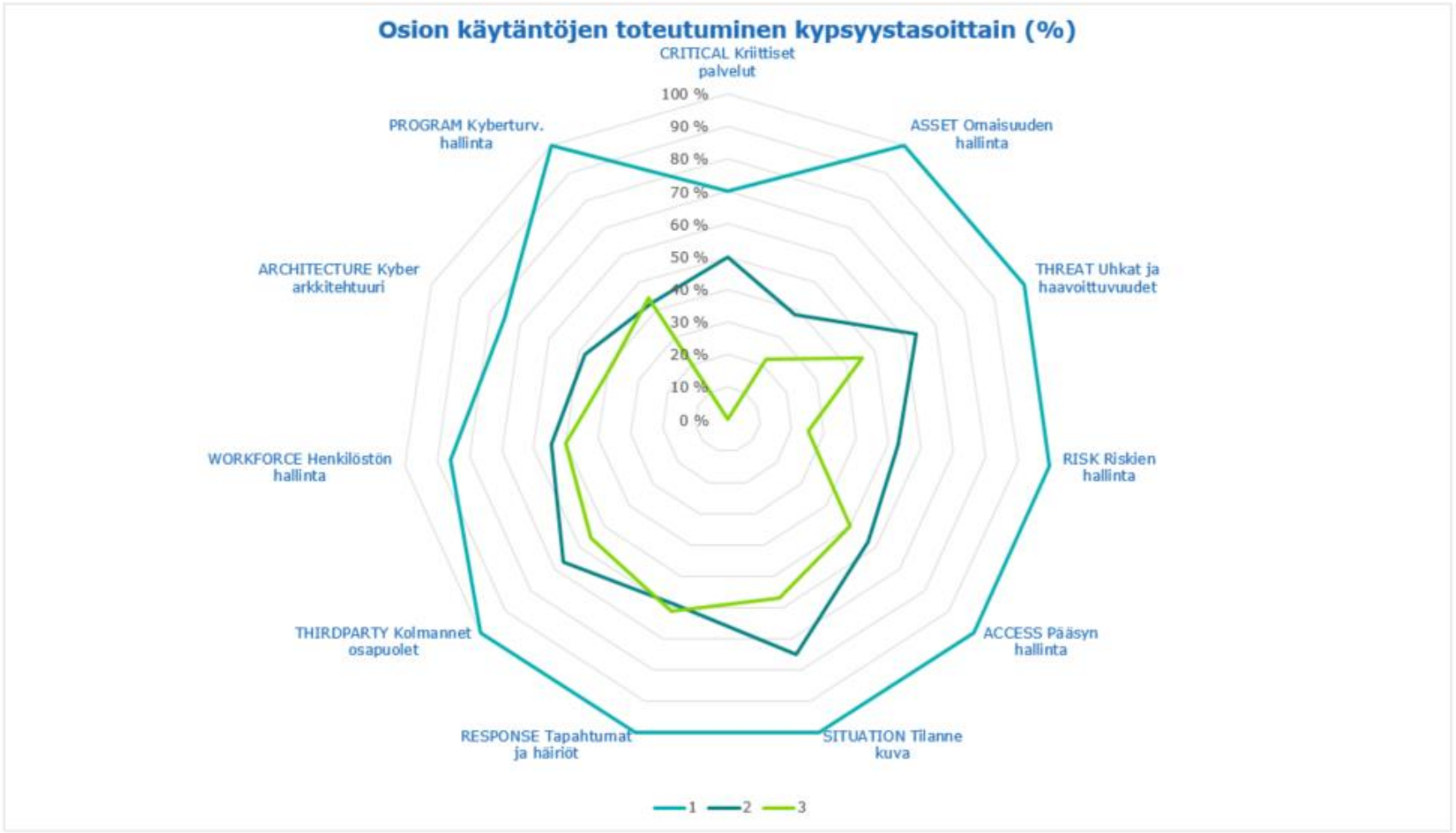
Selite:	0 - Vastaus	1 - Ei toteutettu	2 - Osittain toteutettu	3 - Enimmäkse	4 - Täysin toteutettu

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

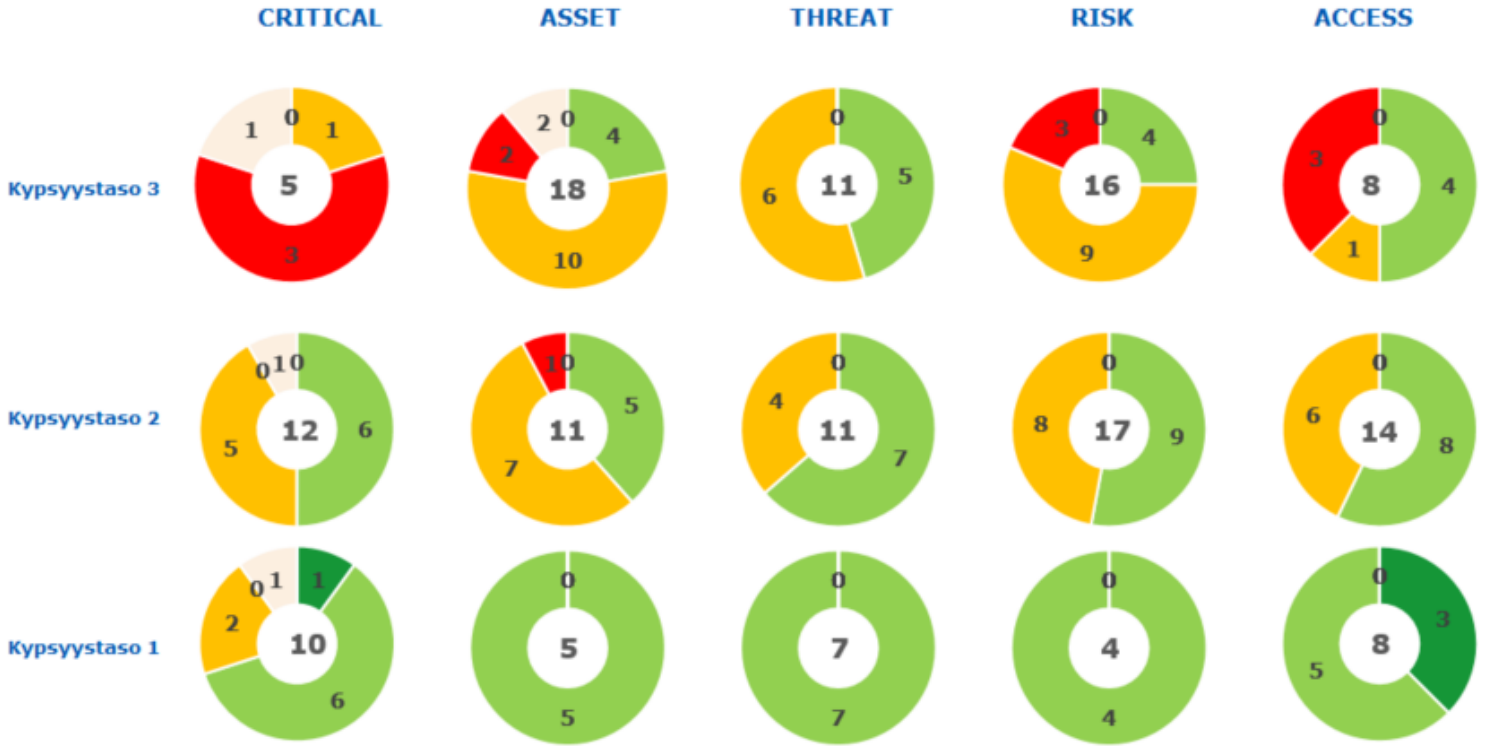

Osion käytäntöjen toteutuminen kypsyystasoittain (%)
CRITICAL Kriittiset palvelut
ASSET Omaisuuden hallinta
THREAT Uhkat ja haavoittuvuudet
RISK Riskien hallinta
ACCESS Pääsyn hallinta
SITUATION Tilanne kuva
RESPONSE Tapahtumat ja häiriöt
THIRDPARTY Kolmannet osapuolet
WORKFORCE Henkilöstön hallinta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

R7

KYBERMITTARI

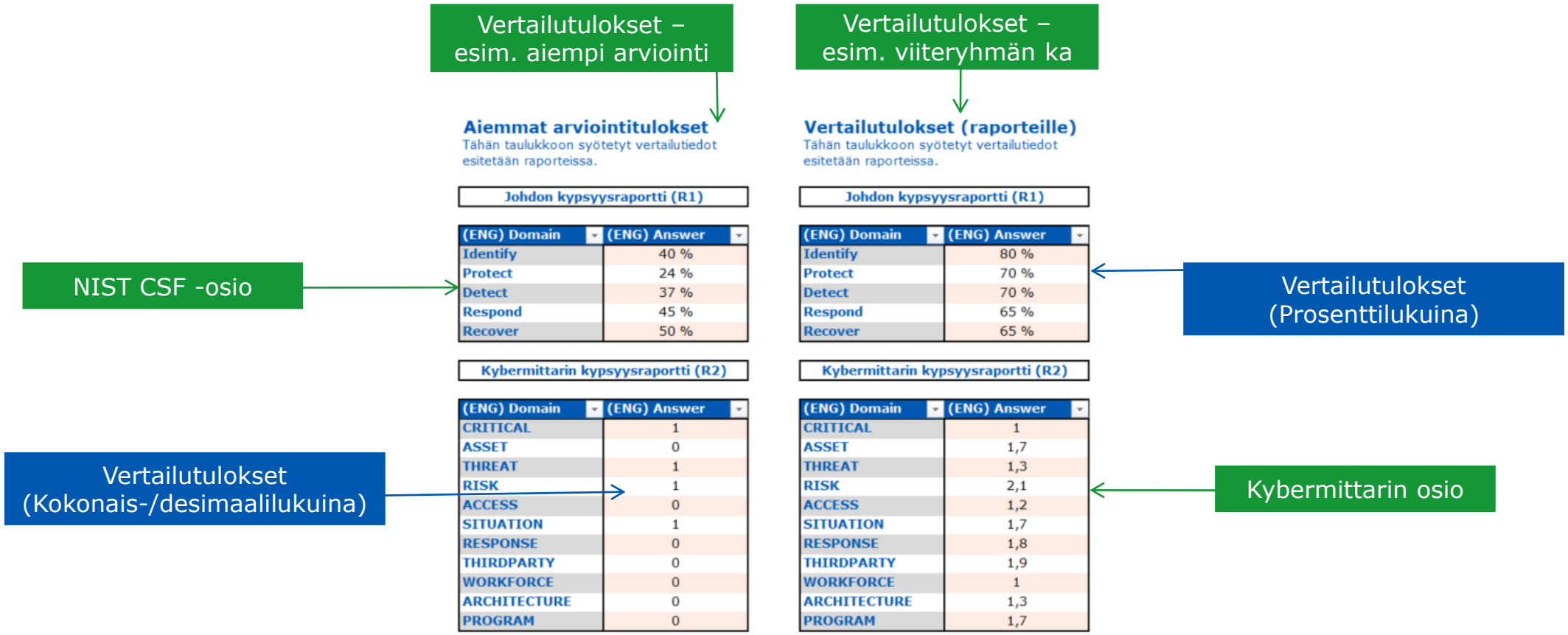
Osiokohtainen kypsyystasoraportti

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



TRAFICOM

5. Import-välilehti



Muut Kybermittarin toiminnallisuuksiin liittyvät välilehdet

- Data
  - Laskentatietojen koonti- ja laskentasivu
- NISTMap
  - Kybermittarin / C2M2 –mallien ja NIST CSF –mallien välinen ristiin kytkentä
- NIS2-alkuiset
  - Muokattava raportointi, esimerkiksi organisaation riskiperustainen käytäntöjen valinta
- Import ja Infoimport
  - Vertailutietojen ja muun oheistuksen tai rikastavan tiedon tuontiominasuudet
  - Voidaan käyttää myös migraatioon
- Export
  - Tulosten vientiominaisuudet
- Languages
  - Selitetekstien kieliversiot (FI, SE, EN)
- Parameters
  - Työkalun käyttämät vaihtoehdot ja säätöparametrit

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

https://www.kybermittari.fi