



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari

Perusperiaatteet
10.10.2022

Sisältö ja tavoite

- ▶ Kybermittari 2021-2022
- ▶ Johdanto aiheeseen
- ▶ Kybermittarin arviointimalli
- ▶ Kybermittarin arviointiprosessi
- ▶ Kybermittari-työkalu





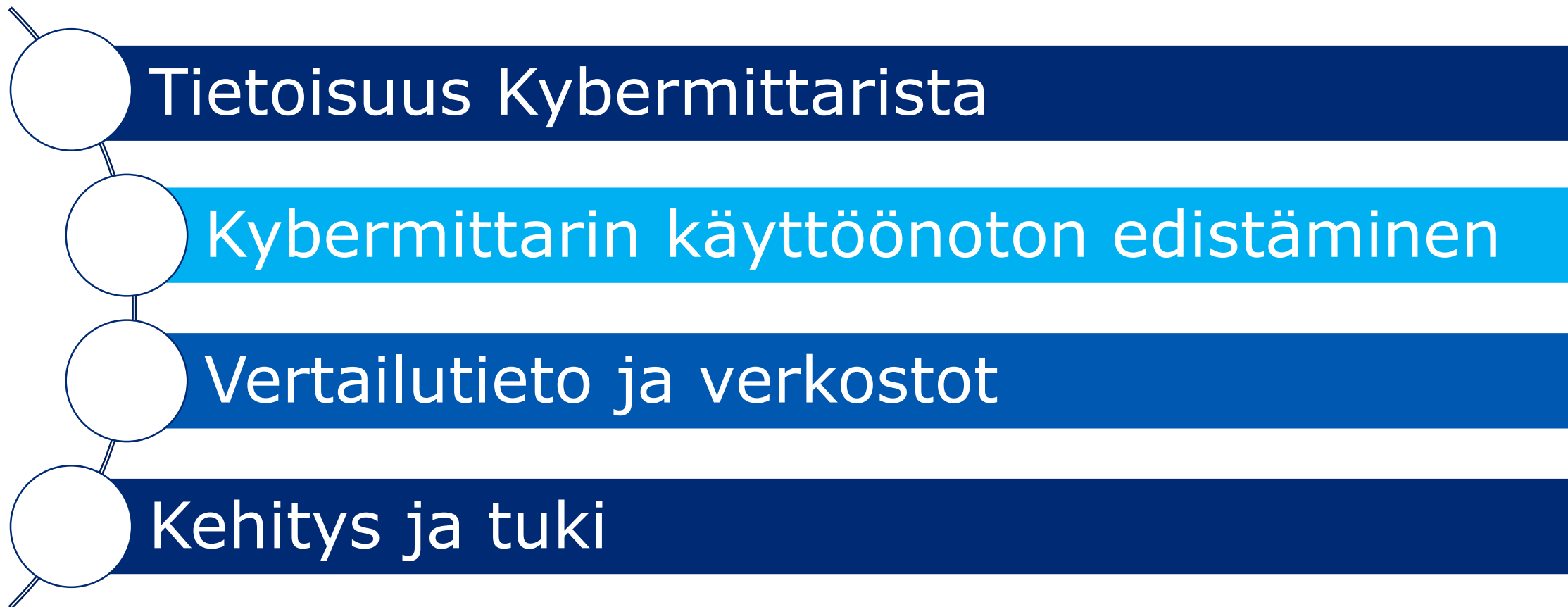
TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2022-

Kybermittari 2022->

Pääteemat





TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Johdanto aiheeseen

Kybermittarin tausta ja
tarkoitus

Kybermittari-palvelu lyhyesti

- ▶ Kybermittari auttaa
 - ▶ tunnistamaan yrityksen ja yhteiskunnan kannalta kriittiset palvelut ja riskit
 - ▶ muodostamaan tilannekuvan kyberturvallisuuskyykyksistä ja potentiaaliset kehityskohteet
 - ▶ mahdollistaa yritysten ja toimialojen vertailun ja parhaiden käytäntöjen jakamisen
- ▶ Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen julkaisema kansallinen kyberturvallisuuden arviointimalli
 - ▶ Yhtenäinen lähestymistavan kyberturvallisuuden arviointiin ja kehittämiseen
 - ▶ Koottu kansallisista ja kansainvälisistä käytänteistä
 - ▶ Vapaasti saatavilla suomen, ruotsin ja englannin kielisenä
 - ▶ Kybermittari on Traficomin omistama tavaramerkki.
 - ▶ Lisenssi: Creative Commons Nimeä 4.0 (CC BY 4.0)

Kybermittari

- ▶ Kansallinen kyberturvallisuuskyykyksien **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



Kybermittarin

- ▶ Kyberturvallisuuskeskus
 - ▶ Omistaa Kybermittari-tuotenimen (tavaramerkki) ja vastaa Kybermittarin ylläpidosta ja jatkokehityksestä
 - ▶ Toimii kansallisena luottamuspisteenä anonyymien vertailutiedon keräämisessä, säilyttämisessä ja jakamisessa
 - ▶ Tarjoaa Kybermittarin yksityisten ja julkisten organisaatioiden, kaupallisten palveluntarjoajien ja viranomaisten vapaasti käytettäväksi, muokattavaksi ja levitettäväksi.
 - ▶ Käyttöehdot verkkosivuilla
 - ▶ Lisenssiehdot: Creative Commons Nimeä 4.0 -lisenssillä (CC BY 4.0)
- ▶ Yksityiset ja julkiset organisaatiot
 - ▶ Voivat hyödyntää Kybermittaria vapaasti joko itse tai kaupallisen palveluntarjoajan tukemana
 - ▶ Halutessaan jakaa arviointituloksensa luottamuksellisesti Kyberturvallisuuskeskukselle ja hyötyä toimialansa anonyymien vertailutiedon rakentumisesta
- ▶ Kaupalliset palveluntarjoajat voivat käyttää, muokata ja levittää Kybermittaria käyttöehtojen, markkinointiehtojen ja lisenssiehtojen puitteissa.

Kybermittarin käytön ehdot, tarkemmin

► Cybersecurity Capability Maturity Model (C2M2) ehdot:

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

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

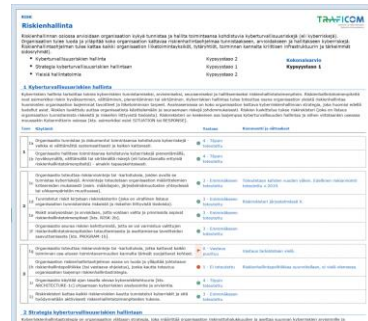
► Kybermittarin ehdot:

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

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

- Nimeä - Sinun on mainittava lähde asianmukaisesti, tarjottava linkki lisenssiin sekä merkittävä, mikäli olet tehnyt muutoksia. Voit tehdä yllä olevan millä tahansa kohtuullisella tavalla, mutta et siten, että annat ymmärtää lisenssiantajan suosittelavan 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 materiaalit



► Arviointityökalu

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

► Ohjeistus ja tuki arviointiprosessiin

- Organisaation itse toteuttamana tai ulkoisen palveluntarjoajan tukemana.

► Automaattisesti tuotetut raportit

- Tuloksena organisaation kyberturvallisuuden kypsyystaso eri näkökulmista.

Yhteystiedot ja turvallinen viestintä

- ▶ Materiaalit: <https://www.kybermittari.fi>
- ▶ Kysymykset ja palaute: kybermittari@traficom.fi
 - ▶ Halutessasi voit lähettää palvelullamme salatun viestin osoitteeseen kybermittari@traficom.fi
 - ▶ <https://www.traficom.fi/fi/traficom/yhteystiedot/salatun-viestin-lahettaminen-traficomiin>
- ▶ Tulosten lähettäminen ja vertailutietojen vastaanottaminen
 1. Ilmoittaudu ja sovi tietojen vaihdosta Kyberturvallisuuskeskuksen kanssa, joko Kybermittarin osoitteen (kybermittari@traficom.fi) tai yhteistyöverkostosi kautta
 2. Sovi Kyberturvallisuuskeskuksen kanssa tietojenvaihtokanavasta (esim. Traficom turvaposti tai muu vastaava suojattu palvelu)
 3. Kyberturvallisuuskeskus lähettää tarkemmat ohjeet tulosten ja vertailutietojen käsittelystä.

HUOM! Käytä aina salattua sähköpostia tulosten lähettämiseen Kyberturvallisuuskeskukselle!

Hyödynnä Kyberturvallisuuskeskuksen ilmaiset ohjeet ja oppaat



”Tavanomaiset torjuntatoimenpiteet” käytännössä

1. Ottakaa kaikkialla käyttöön **monivaiheinen tunnistautuminen**.
2. Asentakaa **tietoturvapäivitykset** viipymättä.
3. Huolehtikaa **varmuuskopioista**.
4. Varmistakaa **etäyhteyksien** turvallisuus.
5. Tehkää **henkilöstöstä** tietoturvan vahvin lenkki (koulutus, tietoisuus ja poikkeamista ilmoittamisen kulttuuri).



Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa

Ohje johdolle ja asiantuntijoille

Kyberturvallisuuskeskus



<https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatioissa-ohje-johdolle-ja-asiantuntijoille>



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointimalli

Kybermittarin rakenne ja
laskentamalli

Tärkeimmät käsitteet

- ▶ **Kyvykkyys** tarkoittaa kykyä toimia tarkoituksenmukaisella tavalla tietyllä osa-alueella ja hyödyntää osaamistaan sekä resurssejaan, jotta tavoitteet saavutettaisiin.
- ▶ **Kypsyysmalli** tarkoittaa mallia, jossa toimintaa tarkastellaan tasoina tai askelmina, joita kiivetään ylöspäin kohti järjestelmällisempää ja kehittyneempää toimintaa.
- ▶ **Toiminnan osa-alue** on Kybermittarin yhteydessä käytetty käsite, jolla tarkoitetaan niitä organisaation tai yhteiskunnan kannalta kriittisiä palveluita tai toimintoja, joiden kyberturvallisuutta arvioinnissa tarkastellaan.

Kybermittarin taustalla olevat viitekehykset

Kybermaturiteetin mittaminen

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

Muut osa-alueet

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

NIST- ja C2M2-dimensiot

Tunnistaminen	Suojautuminen	Havainnointi	Reagointi	Palautuminen
Uhkien, haavoittuvuuksien ja riskien tunnistaminen	Hyökkäyksiltä suojautuminen	Onnistuneiden hyökkäyksien havainnointi	Onnistuneisiin hyökkäyksiin reagointi	Hyökkäyksistä 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				
THIRDPARTY – 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

PROGRAM

Kyberturvallisuuden hallinta (PROGRAM)

Osio

Kokonaisarvio

Tiedon luokittelu

TRAFFICOM

Lähteen ja vastikkeen
Kyberturvallisuus

Kypsyystaso 1

Kypsyystaso 2

Kypsyystaso 1

Päivämäärä

Osallistajat

Kyberturvallisuusohjelman osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuisia kyberturvallisuusohjelmia. 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.

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Yleisiä hallintatoimia

Tavoitteet

1 Kyberturvallisuusstrategia

Kyberturvallisuusstrategia toimii kyberturvallisuusohjelman perustana. Yksinkertaisimmassa muodossa, kyberturvallisuusstrategia pitää sisällään listan kyberturvallisuustavoitteista ja suunnitelman niiden saavuttamiseksi. Korkeammalla kypsyystasolla kyberturvallisuusstrategia on täydellisempi ja sisältää prioriteetit, hallintamallin kuvauksen ("governance"), kyberturvallisuusohjelman organisaatorakenteen ja ylempään johdon vahvemman osallistumisen ohjelmaan suunnitteluun. Kyberturvallisuusstrategia voi olla oma dokumenttinsa, mutta usein se on kirjattu osaksi organisaation kyberturvallisuuspolitiikkaa.

2 Johdon tuki kyberturvallisuusohjelmalle

Johdon tuki on tärkeää kyberturvallisuusohjelman jalkauttamiselle kyberturvallisuusstrategian mukaisesti. Perustasolla tuki sisältää riittävien resurssien turvaamisen (henkilöt, työkalut ja rahoitus). Kehittyneemmässä organisaatiossa tuki pitää sisällään ylempään johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset kyberturvallisuusohjelmalle. Lisäksi tuki kattaa organisatorisen tuen, jota vaaditaan poliittikojen tai vastaavien ohjeistusten määrittämiseksi ja ylläpitämiseksi.

3 Yleisiä hallintatoimia

Yleisillä hallintatoimilla arvioidaan sitä, kuinka syvästi 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 Kyberturvallisuusstrategia

Taso	Käytäntö	Vastaus	Kommentit	Sisäinen viittaus	Ulkoinen viittaus	Kehityskohde
1	1a Organisaatiolla on kyberturvallisuusstrategia. Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu	Käytäntö			
1b	Kyberturvallisuusstrategia määrittelee organisaation kyberturvallisuustavoitteet.	2 - Osittain toteutettu				
1c	Kyberturvallisuusstrategia ja -prioriteetit on dokumentoitu. Strategia ja prioriteetit ovat linjassa organisaation yleisten strategisten tavoitteiden ja kriittiseen infrastruktuuriin kohdistuvien riskien kanssa.	2 - Osittain toteutettu				
1d	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	3 - Enimmäkseen toteutettu				
2	2a Kyberturvallisuusstrategia määrittelee kyberturvallisuuden hallinta- ja organisaatorakenteen.	2 - Osittain toteutettu				
2b	Kyberturvallisuusstrategia nimeää ne standardit ja ohjeet, joita tulee noudattaa.	3 - Enimmäkseen toteutettu				
2c	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2d	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2e	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2f	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2g	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2h	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2i	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2j	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2k	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2l	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2m	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2n	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2o	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2p	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2q	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2r	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2s	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2t	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2u	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2v	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2w	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2x	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2y	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
2z	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3	3a Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3b	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3c	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3d	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3e	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3f	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3g	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3h	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3i	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3j	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3k	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3l	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3m	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3n	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3o	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3p	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3q	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3r	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3s	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3t	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3u	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3v	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3w	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3x	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3y	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				
3z	Kyberturvallisuusstrategia määrittää organisaation kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.	2 - Osittain toteutettu				

► Kybermittari koostuu

► Osioista (yhteensä 11)

► Tavoitteista, joita on osioilla yhteensä (46, hallintatoimia näistä 10)

► Käytännöistä, joiden avulla mitataan tavoitteiden täyttymistä (yhteensä 367)

► 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 toteutettu ja 1) Ei toteutettu

Kybermittarin laskentamalli

RISK

Riskienhallinta

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

- Kyberturvallisuusriskien hallinta
- Strategia kyberturvallisuusriskien hallintaan
- Yleisiä hallintatoimia

Kypsyystaso 2
Kypsyystaso 1
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 laajemmät tavoitteet ja liiketoiminnan tarpeet. Avalaimesessa on koko organisaation kattava kyberriskienhallinnan strategia, joka huomioi edellä luellut 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 viitataan usein muussakin Kybermittarin osiossa [kts. esimerkiksi osiot SITUATION tai RESPONSE].

Taso	Käytäntö	Vastaus	Kommentti ja viittaukset
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	
1c	Organisaatio toteuttaa riskiarviointia tai -kartoituksia, joiden avulla se tunnistaa kyberriskejä. Arviointia toteutetaan organisaation määrittelemien kriteerien mukaisesti (esim. määräjain, järjestelmämuutosten yhteydessä tai uhkaympäristön muuttuessa).	3 - Enimmäkseen toteutettu	Toteutetaan kahden vuoden välein. Edellinen riskiarviointi toteutettu v.2019.
1d	Tunnistetut riskit kirjataan riskirekisteriin (joka on virallinen listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista).	3 - Enimmäkseen toteutettu	Riskirekisteri järjestelmässä X.
1e	Riskit analysoidaan ja arvioidaan, jotta voidaan valita ja priorisoida sopivat riskienhallintatoimenpiteet [kts. RISK-2b].	3 - Enimmäkseen toteutettu	>50%
1f	Organisaatio seuraa riskien kehittymistä, jotta se voi varmistua valittujen riskienhallintatoimenpiteiden toteuttamisesta ja asettamiensa tavoitteiden saavuttamisesta [kts. PROGRAM-1b].	3 - Enimmäkseen toteutettu	
1g	Organisaatio toteuttaa riskiarviointia tai -kartoituksia, jotka kattavat kaikki toiminnan osa-alueen toimintavarmuuden kannalta tärkeät suojattavat kohteet.	0 - Vastaus puuttuu	Vastaus tarkistetaan vielä.
1h	Organisaation riskienhallintaohjelman osana on luoda ja ylläpitää johtotason riskienhallintapolitiikka (tai vastaava ohjeistus), jonka kautta toteutuu organisaation laajempi riskienhallintastrategia.	1 - Ei toteutettu	Riskienhallintapolitiikkaa suunnitellaan, ei vielä olemassa.
1i	Organisaatio käyttää ajan tasalla olevaa kyberarkkitehtuuria [kts. ARCHITECTURE-1c] ohjaamaan kyberriskien analysointia ja arviointia.	4 - Täysin toteutettu	<50%
1j	Riskirekisteri kattaa kaikki riskiarvioiden kautta tunnistetut kyberriskit ja sitä hyödynnetään aktiivisesti riskienhallintatoimenpiteiden tukena.	3 - Enimmäkseen toteutettu	

2 Strategia kyberturvallisuusriskien hallintaan

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

► Kypsyystaso lasketaan kolmessa vaiheessa:

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

► Lopputuloksena muodostuu jokaisen yhdentoista osion kypsyystaso asteikolla 0-3

- Taso perustuu toteutettuihin käytäntöihin ja saavutettuihin tavoitteisiin
- Jokaisen osion kypsyystaso on sama kuin heikoimman tavoitteen kypsyystaso

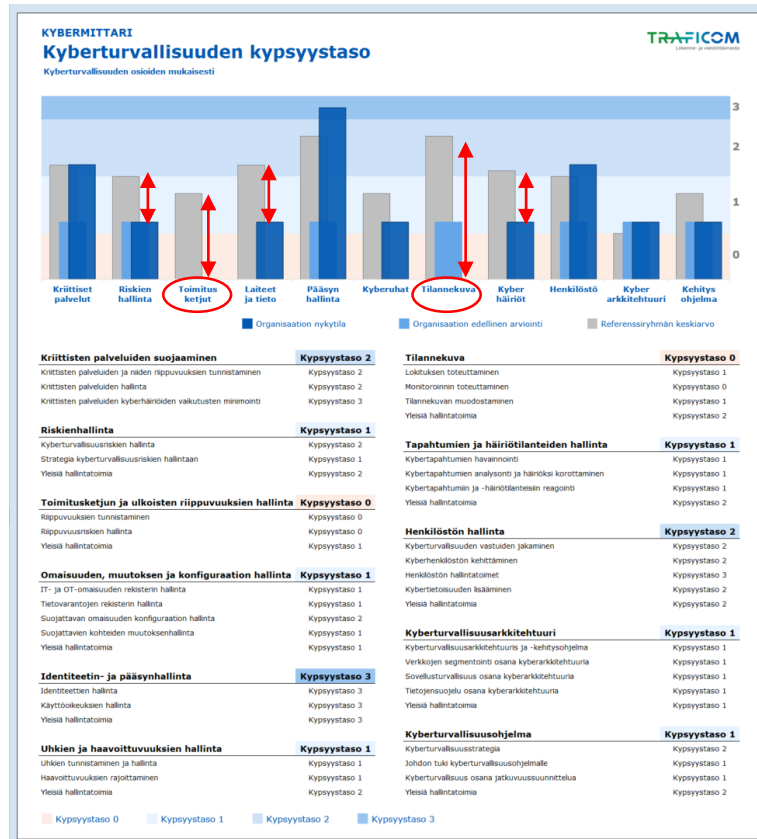
Tavoitteet ja osiot – kypsyystaso

- ▶ Osioiden ja tavoitteiden kypsyystason laskennassa käytetään seuraavia sääntöjä:
 - ▶ **Taso 0:** kaikki tason 1 käytännöt eivät toteudu kokonaan (4) Täysin tai 3) Enimmäkseen toteutettu)
 - ▶ **Taso 1:** tulee toteuttaa kaikki (100%) kyseisen tason käytännöistä
 - ▶ **Taso 2:** tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä ja kaikki (100%) tason 1 käytännöt
 - ▶ **Taso 3:** tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä ja kaikki (100%) tason 2 ja kaikki (100%) tason 1 käytännöt.

**Jokaisen osion ja tavoitteen kypsyystaso on sama kuin
heikoimman tavoitteen kypsyystaso**

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

Kehitysalueiden tunnistaminen - esimerkiksi näin



► Kybermittarin kypsyysraportista (R2), esimerkiksi:

► Osiot ja tavoitteet, joiden kypsyystaso 0

► Osiot, joiden kypsyystaso on merkittävästi toimialan referenssi- tai suositustasoa 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 - nimetyille henkilölle tai roolille, joka rekisteröi tapahtumat.

- ▶ Kybermittarin kypsyysraportista (R2):
 - ▶ Raportoin alaosasta löytyy osio, jossa on listattu kypsyystasolle 1 vaadittavat käytännöt.
 - ▶ Yksittäisen käytännön puuttuminen voi pudottaa koko osion tasolle 0, joten tässä listattujen käytäntöjen toteuttaminen voi nostaa kypsyystasoa merkittävästi.



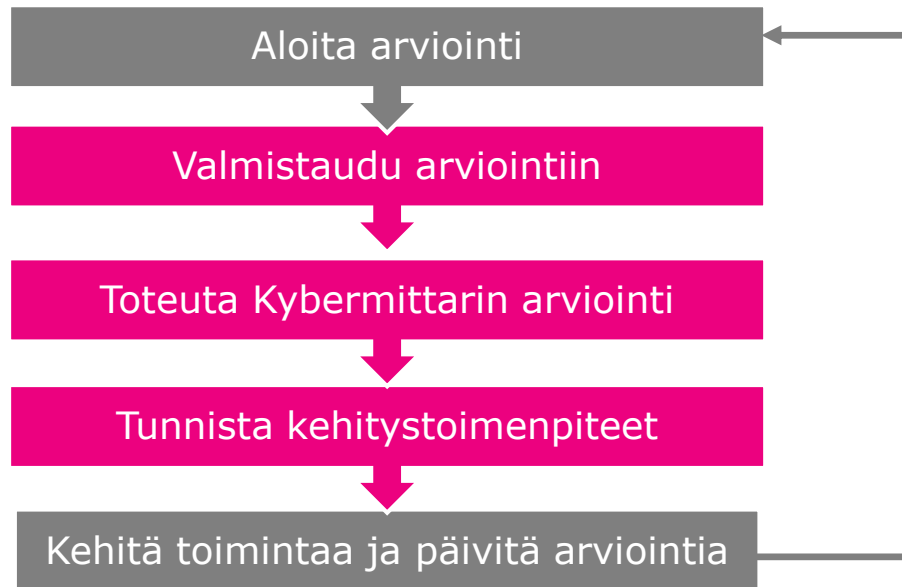
TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointiprosessi

Kybermittarin hyödyntämiseen

Kybermittarin arviointiprosessi



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

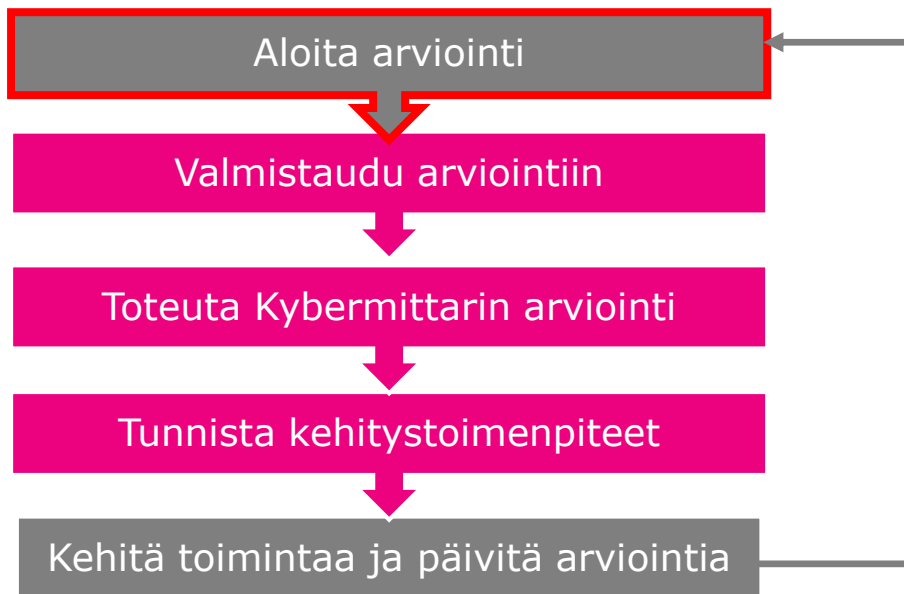


TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Aloita arviointi

Aloita arviointi



► Osallistujat:

- Organisaation johtoryhmä tai muu päätöksentekoeelin.

► Tehtävä:

- Tunnistaa tarpeen arvioinnin toteuttamiselle
- Päättää arvioinnin toteuttamisesta ja arvioinnin kohteesta; ja
- Nimittää arvioinnille sponsori ja vetäjä, jotka vastaavat jatkotoimenpiteistä.

Päätös arvioinnin toteuttamisesta ja kohteesta

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

Sponsori ja vetäjä seuraavia vaiheita varten

- ▶ Arviointia varten tulee nimetä vähintään arvioinnin sponsori ja vetäjä

Arvioinnin sponsori

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

Arvioinnin vetäjä

Organisaation oma tai ulkopuolisen palveluntarjoajan edustaja, joka vastaa arvioinnin käytännön toteutuksesta



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Valmistaudu arviointiin

Valmistaudu arviointiin



► Osallistujat:

- Arvioinnin sponsori ja vetäjä yhdessä.

► Tehtävä:

- Rajata tarkemmin arvioitavana oleva toiminnan osa-alue ja tunnistaa osa-alueen kriittiset riippuvuudet;
- Tunnistaa arviointiin tarvittavat asiantuntijat; ja
- Sopia arviointitavasta ja arvioinnin aikataulusta.

Toiminnan osa-alueen rajaaminen

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

Yhteiskunnan kannalta kriittiset palvelut

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

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

Kriittisten riippuvuuksien tunnistaminen

- ▶ Kriittisten palveluiden lisäksi arvioinnin kohteen määrittämiseksi tulee tunnistaa näiden tärkeimmät riippuvuudet
- ▶ Kriittisiä riippuvuuksia ovat:
 - ▶ Liiketoimintaprosessit ja operatiiviset prosessit;
 - ▶ Järjestelmät ja osajärjestelmät; ja
 - ▶ Tietovarannot

Palvelun toimittaminen riippuu useista tekijöistä



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

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

- ▶ Tunnista palvelun toimittamisen kannalta keskeinen suojattava omaisuus
 - ▶ Suojatta omaisuus voi olla tuotantolaitte 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 palveluntarjoajan 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 Omaisuuksien, muutosten ja konfiguraatioiden hallinta	Tietoturva- ja tietohallintojohtaja yhdessä (*OT omaisuus: lisäksi asiasta vastaavat liiketoiminnan edustajat)
PROGRAM Kyberturvallisuuden hallinta	Tietoturvajohtaja/päällikkö tai muu kyberturvallisuudesta organisaatiossa vastaava henkilö
THIRDPARTY Kumppaniverkoston riskien hallinta	Hankintapäällikkö, riskienhallintapäällikkö, Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä

Kybermittarin osio	Keskeiset roolit
ACCESS Identiteetin ja pääsynhallinta	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
RESPONSE Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus	Tietoturvajohtaja/päällikkö, tietohallintojohtaja ja riskienhallintapäällikkö yhteisesti sekä asiaa hoitavat liiketoiminnan edustajat
ARCHITECTURE Kyberturvallisuus-arkkitehtuuri	Tietoturvajohtaja/päällikkö yhdessä relevanttien arkkitehtien kanssa
SITUATION Tilannekuva	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
THREAT Uhkien ja haavoittuvuuksien hallinta	Tietoturvajohtaja ja -päällikkö yhteisesti, sekä asiaa hoitavat liiketoiminnan edustajat
WORKFORCE Henkilöstön johtaminen ja kehittäminen	Tietoturvajohtaja yhteistyössä henkilöstöjohtajan kanssa

Arvioinnin toteutustapa

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

Ohjattu työpajamuotoinen toimintamalli

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



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toteuta arviointi

Toteuta Kybermittarin arviointi



► Osallistujat:

- Arvioinnin vetäjä, arvioinnin sponsori ja organisaation asiantuntijat.

► Tehtävä:

- Toteuttaa arviointi valitulla arviointitavalla Kybermittari-työkalun avulla.

Kybermittarin osiot

CRITICAL – Kriittisten palveluiden suojaaminen
--

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
--

THIRDPARTY – Kumppaniverkoston riskien hallinta

WORKFORCE – Henkilöstön johtaminen ja kehittäminen
--

ARCHITECTURE - Kyberturvallisuusarkkitehtuuri

PROGRAM – Kyberturvallisuuden hallinta
--

Yhteenvedo – Summary-välilehti

KYBERMITTARI
Kyberturvallisuuden arviointityökalu

2.0

Tiedon luokittelu
sisäinen

TRAFICOM

Kybermittari versio 2.0, 04.10.2022
https://www.kybermittari.fi
Palaute ja kysymykset: kybermittari(at)traficom.fi

Materiaali on käytettävissä Creative Commons Nimeä 4.0 / CC BY 4.0 lisenssiehtojen mukaisesti.
Kybermittari on rekisteröity tavaramerkki (sanamerkki).

Valitse kieli / Välj språk / Choose language

Suomi

Organisaatio

Nimi	Yritys Oy	Yhteyshenkilön sähköposti	etu.suku@yritys.foo
Toimiala	Energiahuolto	Y-lunnus	1234567-8
Toiminto	Energia - Voimalatous	Arvioinnin vetäjä	NN
Aloituspvm.	1.10.2022	Seuraava arvio	6/2023
Viimeinen muutos	21.10.2022		

Kuvaus arvioitavasta toiminnosta

Toiminnon yhteiskunnallinen vaikuttavuus
Uhkaskenaarion kuvaus (worst-case)

Skenaariot yhteiskunnallinen vaikuttavuus
2. Huomattava systeeminen vaikutus

Kyberturvallisuuden arviointi

Kyberturvallisuuden osiot			
Kriittisten palveluiden suojaaminen (CRITICAL)	24 / 27		
Omistuksen muutosten ja konfiguraation hallinta (ASSE)	34 / 36	Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus (	48 / 49
Uhkien ja haavoittuvuuksien hallinta (THREAT)	29 / 29	Kumppaniverkoston riskien hallinta (THIRDPARTY)	22 / 22
Riskienhallinta (RISK)	37 / 37	Henkilöstön johtaminen ja kehittäminen (WORKFORCE)	29 / 30
Identiteetti- ja pääsynhallinta (ACCESS)	30 / 30	Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)	53 / 54
Tilannekuva (SITUATION)	28 / 29	Kyberturvallisuuden hallinta (PROGRAM)	26 / 26

Kyberturvallisuuden investointien taso
Kyberturvallisuuden investointien taso (Investment)

Tulokset ja vertailutiedot

Tulosten tuonti (Import)	Tulosten vienti (Export)
Tulosten lähetyk Kyberturvallisuuskeskukselle (Export_KTK)	
Johdon kysymysraportti (R1)	Yksityiskohtainen NIST Framework Core -raportti (R3)
Kybermittarin kysymysraportti (R2)	Kyberturvallisuuden kehityskohteiden raportti (R4)
Yleiset hallintatoimet -raportti (R5)	Osion käyttäntöjen toteutuminen kysymysasetuksilla (R6)
Osiokohtainen kysymysasetus -raportti (R7)	

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

Osiokohtaiset välilehdet

PROGRAM

Kyberturvallisuuden hallinta (PROGRAM)

Kokonaisarvio

Kypsyystaso 1

Tiedon luokittelu

TRAFICOM

Liikenne- ja viestikeskus

Kyberturvallisuuskeskus

Kyberturvallisuusohjelman osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuisia kyberturvallisuusohjelmia. Kyberturvallisuusohjelman tarkoitus on määrittää kyberturvallisuuden hallintamalli ("governance"), kyberturvallisuuden strategien kehittäminen ja liiketoimintajohdon tuki kyberturvallisuudelle tavalla, joka on suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin nähden.

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Yleisiä hallintatoimia

Kypsyystaso 1

Kypsyystaso 2

Kypsyystaso 1

Päivämäärä

Osallistajat

1 Kyberturvallisuusstrategia

Kyberturvallisuusstrategia toimii kyberturvallisuusohjelman perustana. Yksinkertaisimmassa muodossa, kyberturvallisuusstrategia pitää sisällään listan kyberturvallisuustavoitteista ja suunnitelman niiden saavuttamiseksi. Korkeammalla kypsyystasolla kyberturvallisuusstrategia on täydellisempi ja sisältää prioriteetit, hallintamallin kuvauksen ("governance"), kyberturvallisuusohjelman organisaatorakenteen ja ylemmän johdon vahvemman osallistumisen ohjelmaan suunnitteluun. Kyberturvallisuusstrategia voi olla oma dokumenttinsa, mutta usein se on kirjattu osaksi organisaation kyberturvallisuuspolitiikkaa.

2 Johdon tuki kyberturvallisuusohjelmalle

Johdon tuki on tärkeä kyberturvallisuusohjelman jalkauttamiselle kyberturvallisuusstrategian mukaisesti. Perustasolla tuki sisältää riittävien resurssien turvaamisen (henkilöt, työkalut ja rahoitus). Kehittyneemässä organisaatiossa tuki pitää sisällään yllmän johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset kyberturvallisuusohjelmalle. Lisäksi tuki kattaa organisatorisen tuen, jota vaaditaan poliittikkojen tai vastaavien ohjeistusten määrittämiseksi ja ylläpitämiseksi.

3 Yleisiä hallintatoimia

Yleisillä hallintatoimilla arvioidaan sitä, kuinka syväisesti 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 Kyberturvallisuusstrategia

Taso	Käytäntö	Vastaus	Kommentit	Sisäinen viittaus	Ulkoinen viittaus	Kehityskohde
1	1a	Organisaatiolla on kyberturvallisuusstrategia. Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.	3 - Enimmäkseen toteutettu			
	1b	Kyberturvallisuusstrategia määrittelee organisaation kyberturvallisuustavoitteet.	2 - Osittain toteutettu			
	1c	Kyberturvallisuusstrategia ja -prioriteetit on dokumentoitu. Strategia ja prioriteetit ovat linjassa organisaation yleisten strategisten tavoitteiden ja kriittiseen infrastruktuuriin kohdistuvien riskien kanssa.	2 - Osittain toteutettu			

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

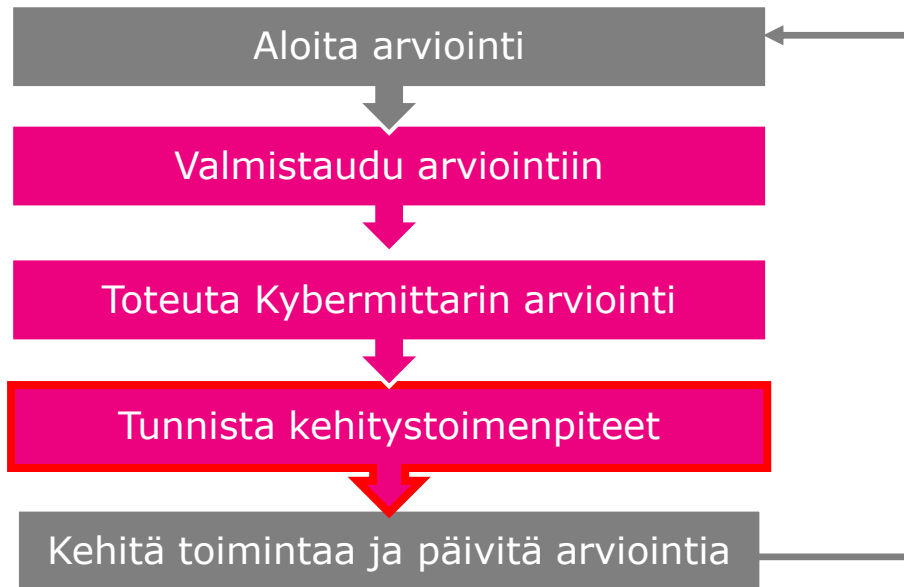


TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tunnista kehitystoimen- piteet

Tunnista kehitystoimenpiteet



► Osallistujat:

- Arvioinnin vetäjä, arvioinnin sponsori, organisaation asiantuntijat ja kehityssuunnitelmien omistajat.

► Tehtävä:

- Analysoida arvioinnin tulokset;
- Määrittää mahdollinen toiminnan tavoitetaso; sekä
- Tunnistaa ja priorisoida tärkeimmät kehitystoimenpiteet.

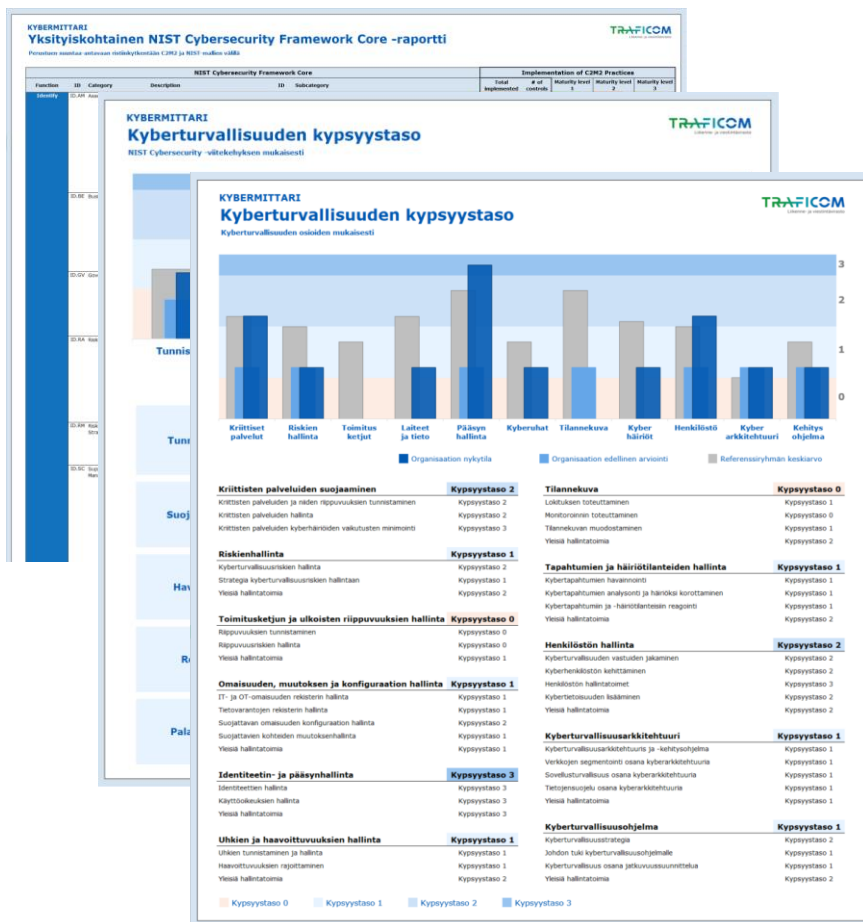
Arviointityökalun raportit tulosten analysoinnin ja tavoitetasen asettamisen tukena

- Työkalu tuottaa automaattisesti kolme erilaista raporttia kyberturvallisuuden kypsyystasosta

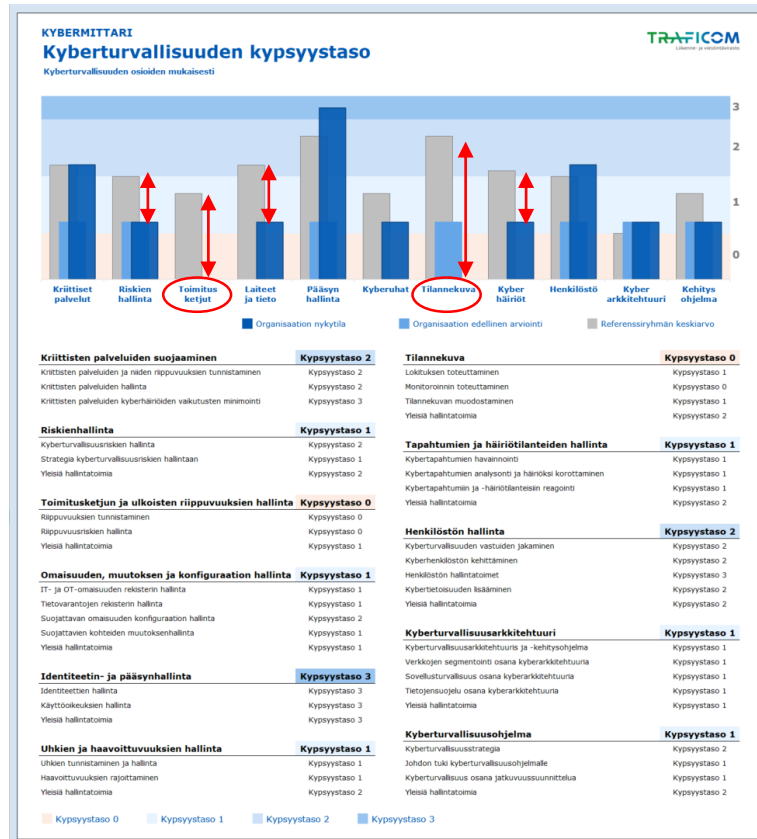
- Raportit ovat

- Johdolle suunnattu kypsyysraportti
- Kybermittarin kypsyysraportti
- Yksityiskohtainen NIST CSF -raportti

- Raportteja on mahdollista rikastaa vertailutiedolla organisaation aiemmasta arvioinnista tai esimerkiksi viiteryhmän keskiarvotuloksilla



Esimerkkejä kehitystoimenpiteiden tunnistamiseen



► Kybermittarin kypsyysraportista, esimerkiksi:

► Osiot ja tavoitteet, joiden kypsyystaso 0

► Osiot, joiden kypsyystaso on merkittävästi toimialan referenssi- tai suositustasoa matalampi

► Alhaisimmin suoriutuneet osiot

► Alhaisimmin suoriutuneet osiot suhteessa aihealueen muihin tavoitteisiin



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

**Kehitä toimintaa
ja päivitä
arviointia**

Kehitä toimintaa ja päivitä arviointia



► Osallistujat:

- Kehityssuunnitelmien omistajat, organisaation asiantuntijat sekä organisaation johtoryhmä tai muu päätöksenteköelin.

► Tehtävä:

- Toteuttaa suunniteltuja kehitystoimenpiteitä, päivittää arviointia ja käynnistää tarvittaessa uusi arviointiprosessi.

Kehityssuunnitelman toteuttaminen

- ▶ Kehityssuunnitelmien omistajat koordinoivat suunnitelmien toteutusta ja ylläpitävät kokonaiskuvaa toimenpiteiden etenemisestä.
- ▶ Tavoitteena on varmistaa päätettyjen toimenpiteiden toteutuminen ja tunnistaa oikea aika arvioinnin päivittämiselle.
- ▶ Kybermittarin käyttäminen tulee nähdä prosessina, jossa arviointi ja kehystoimenpiteiden 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 seuranta 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



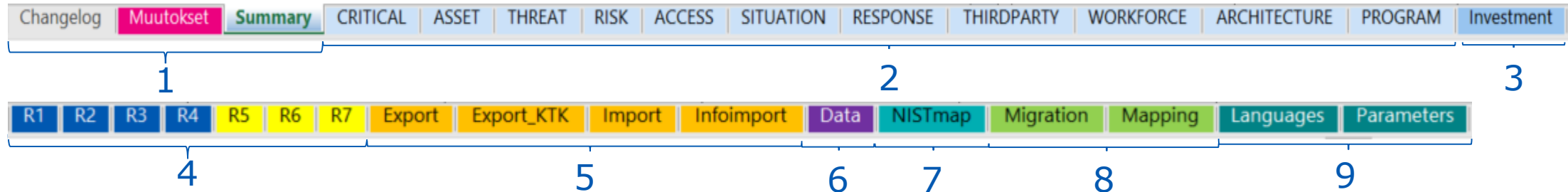
TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin arviointityökalu

Ohjeita teknisen työkalun
hyödyntämiseen

Kybermittarin arviointityökalun rakenne



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

1. Kybermittari-välilehti – yhteenveto

Kielivalinta

Valitse kieli / Välj språk / Choose language

Suomi

Tiedon luokittelu

Tiedon luokittelu
sisäinen

Organisaation tiedot

Organisaatio

Nimi	Yntys Oy	Yhteyshenkilön sähköposti	etu.suku@yntys.fo
Toimiala	Energiahuolto	Y-tunnus	1234567-8
Toiminto	Energia - Voimatalous	Arvioinnin vetäjä	N.N
Aloituspvm.	1.10.2022	Seuraava arviointi	6/2023
Viimeinen muutos	21.10.2022		

Toiminnan osa-alue

Kuvaus arvioitavasta toiminnosta

Yhteiskunnallinen vaikuttavuus

Toiminnan yhteiskunnallinen vaikuttavuus
Uhkaskenaarion kuvaus (worst-case)

Skenaariion yhteiskunnallinen vaikuttavuus
2. Huomattava systeeminen vaikutus

Linkit arvioitaviin osioihin

Kyberturvallisuuden arviointi

Kyberturvallisuuden osiot		
Kriittisten palveluiden suojaaminen (CRITICAL)	24 / 27	
Omaisuuksien, muutosten ja konfiguraation hallinta (ASSET)	34 / 36	Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus
Uhkien ja haavoittuvuuksien hallinta (THREAT)	29 / 29	Kumppaniverkoston riskien hallinta (THIRDPARTY)
Riskienhallinta (RISK)	37 / 37	Henkilöstön johtaminen ja kehittäminen (WORKFORCE)
Identiteetti- ja pääsynhallinta (ACCESS)	30 / 30	Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)
Tilannekuva (SITUATION)	28 / 29	Kyberturvallisuuden hallinta (PROGRAM)

Linkit raportteihin ja vertailutietoihin

Kyberturvallisuuden investointien taso
Kyberturvallisuuden investointien taso (Investment)

Tulokset ja vertailutiedot

Tulosten tuonti (Import)	Tulosten vienti (Export)
Tulosten lähetyksen Kyberturvallisuuskeskukselle (Export_KTK)	
Johdon kypsyysraportti (R1)	Yksityiskohtainen NIST Framework Core -raportti (R3)
Kybermittarin kypsyysraportti (R2)	Kyberturvallisuuden kehityskohteiden raportti (R4)
Yleiset hallintatoimet -raportti (R5)	Osion käytäntöjen toteutuminen kypsyystasoin (R6)
Osiokohtainen kypsyystaso -raportti (R7)	

2. Osiokohtaiset välilehdet (11 kpl)

Osion tunniste ja nimi

Osion kuvaus

Osion tavoitteet

Käytäntö
(tunniste ja kuvaus)

Käytännön kypsyystaso

PROGRAM

Kyberturvallisuuden hallinta (PROGRAM)

Kyberturvallisuusohjelman osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuisuutta 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.

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Yleisiä hallintatoimia

Kokonaisarvio

Kypsyystaso 1

Kypsyystaso 1

Kypsyystaso 2

Kypsyystaso 1

Tiedon luokittelu

Päivämäärä

Osallistujat

TRAFICOM

Liikenne ja viestintä

1 Kyberturvallisuusstrategia

Kyberturvallisuusstrategia toimii kyberturvallisuusohjelman perustana. Yksinkertaisimmassa muodossa, kyberturvallisuusstrategia pitää sisällään listan kyberturvallisuustavoitteista ja suunnitelman niiden saavuttamiseksi. Korkeammalla kypsyystasolla kyberturvallisuusstrategia on täydellisempi ja sisältää prioriteetit, hallintamallin kuvauksen ("governance"), kyberturvallisuusohjelman organisaatorakenteen ja ylemmän johdon vahvemman osallistumisen ohjelmaan suunnitteluun. Kyberturvallisuusstrategia voi olla oma dokumenttinsa, mutta usein se on kirjattu osaksi organisaation kyberturvallisuuspolitiikkaa.

2 Johdon tuki kyberturvallisuusohjelmalle

Johdon tuki on tärkeää kyberturvallisuusohjelman jalkauttamiselle kyberturvallisuusstrategian mukaisesti. Perustasolla tuki sisältää riittävien resurssien turvaamisen (henkilöt, työkalut ja rahoitus). Kehittyneemmässä organisaatiossa tuki pitää sisällään ylemmän johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset kyberturvallisuusohjelmalle. Lisäksi tuki kattaa organisatorisen tuen, jota vaaditaan poliittikkojen tai vastaavien ohjeistusten määrittämiseksi ja ylläpitämiseksi.

3 Yleisiä hallintatoimia

Yleisillä hallintatoimilla arvioidaan sitä, kuinka syvästi 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.

Taso	Käytäntö	Vastaus	Kommentit	Sisäinen viittaus	Ulkoinen viittaus	Kehityskohde
1	1a	3 - Enimmäkseen toteutettu				
	1b	2 - Osittain toteutettu				
	1c	2 - Osittain toteutettu				

Tavoitteiden kypsyystasot

Osion kypsyystaso

Tavoitteen nimi

Tavoitteen kuvaus

Vastaus (1-4 tai 0)

Kommentti ja viittaus

Vastauksen indikaattori

3. Kyberturvallisuuden investoinnit -välilehdet

Kyberturvallisuuden investointien taso

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

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

Kategoria	Henkilöstö (sisäinen)	Konsultointi	Palvelut	Ohjelmisto- lisenssit	Laitte- investoinnit	Yhteensä	Suunniteltu
Kriittisten palveluiden suojaaminen (CRITICAL)						0	
Omaisuuksien, 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

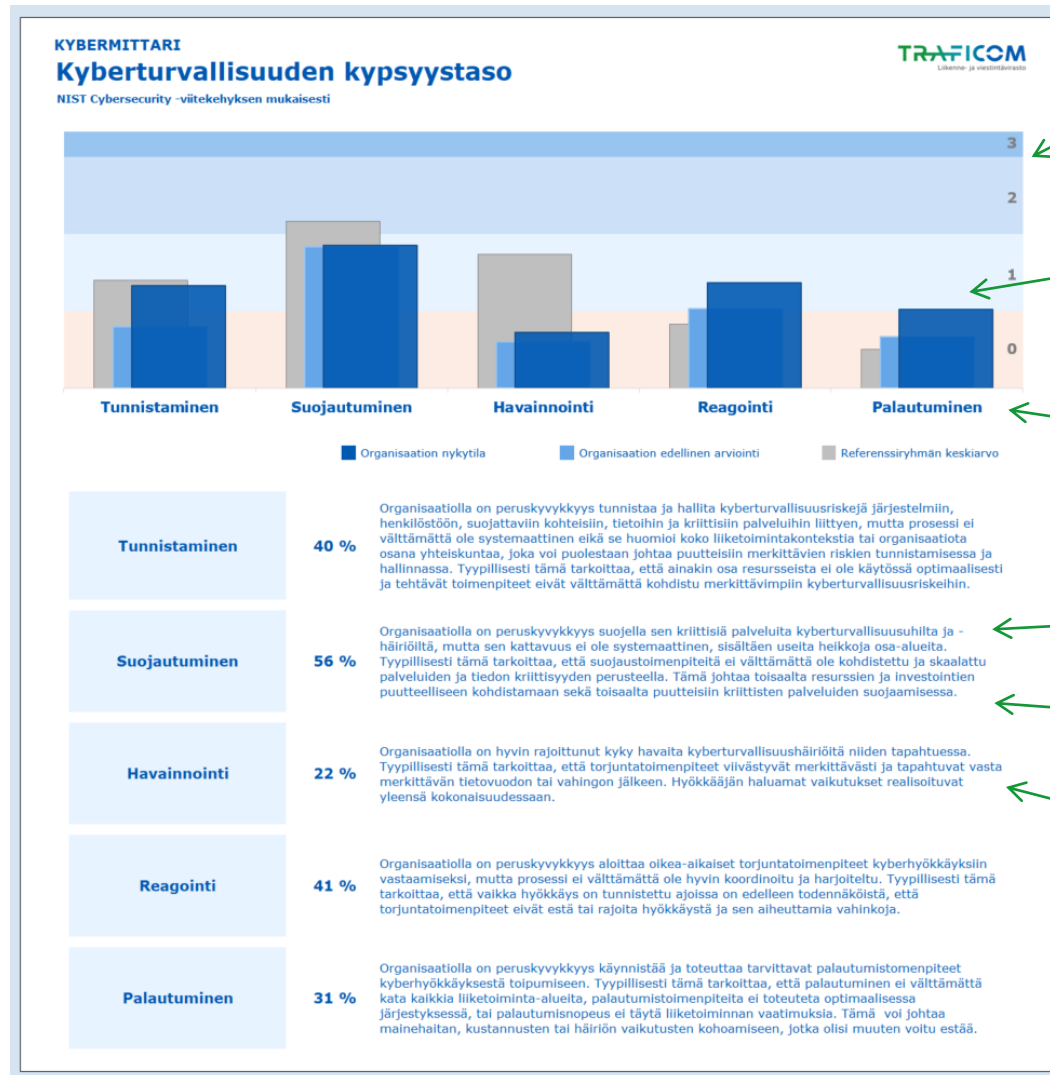
4. Raportoinnin sisältö ja merkittävät muutokset

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

4. Raportointi, uudet

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

4. R1 NIST CSF ristiinviittaus



Kypsyysasteikko 0-3

Kolmet arviointitulokset

- Nykyinen
- Edellinen
- Referenssi

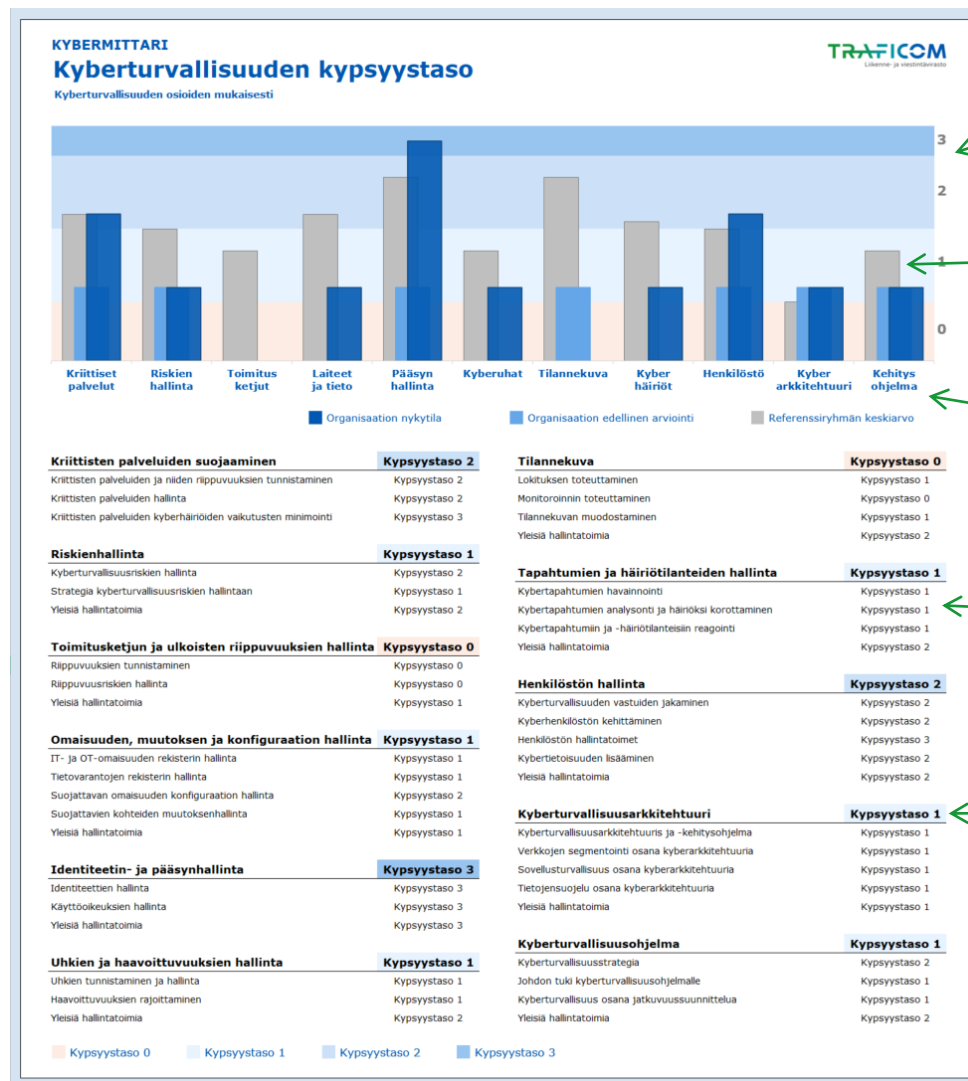
NIST CSF 5 osa-aluea

Osa-alue

Toteutuneiden käytäntöjen osuus (%)

Sanallinen kuvaus kypsyystasosta

4. R2 Kyberturvallisuuden kypsyystaso



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

Perustuen suuntaa-antavaan ristiinkytöntään 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	Maturity level 4	Maturity level 5	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-3	Organizational communication and data flows are mapped	25 %	4	0 %	0	0 %	1	33 %	3
				ID.AM-4	External information systems are catalogued	20 %	5	100 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	29 %	7	100 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	17 %	6	0 %	1	25 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	24 %	17	100 %	3	0 %	7	14 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	100 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	0	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

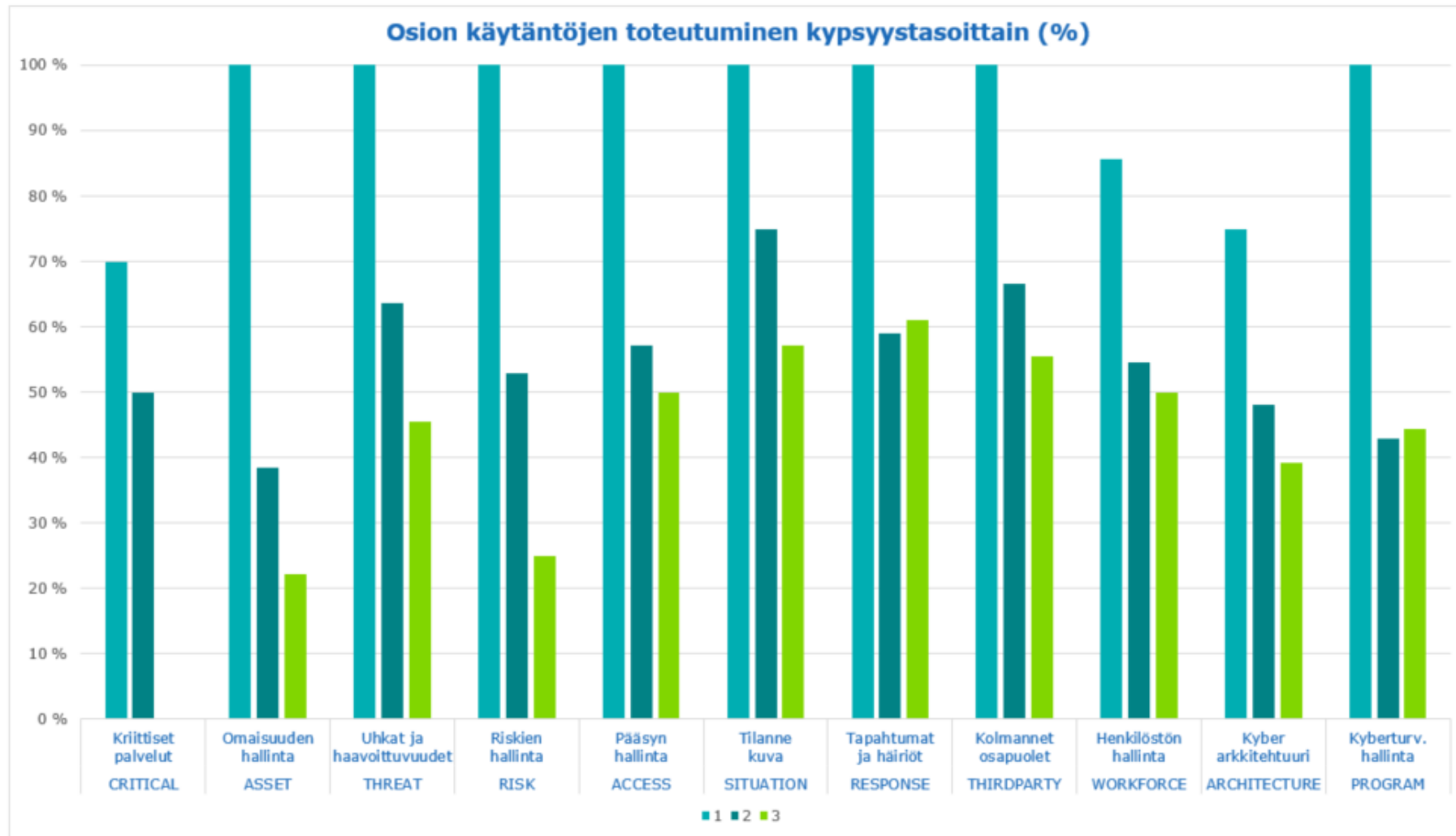
Käytäntöjen määrä ja toteutumisprosentti
(kokonaisuudessaan)

Käytäntöjen määrä ja toteutumisprosentti
(jaettuna kypsyystasojen mukaisesti)

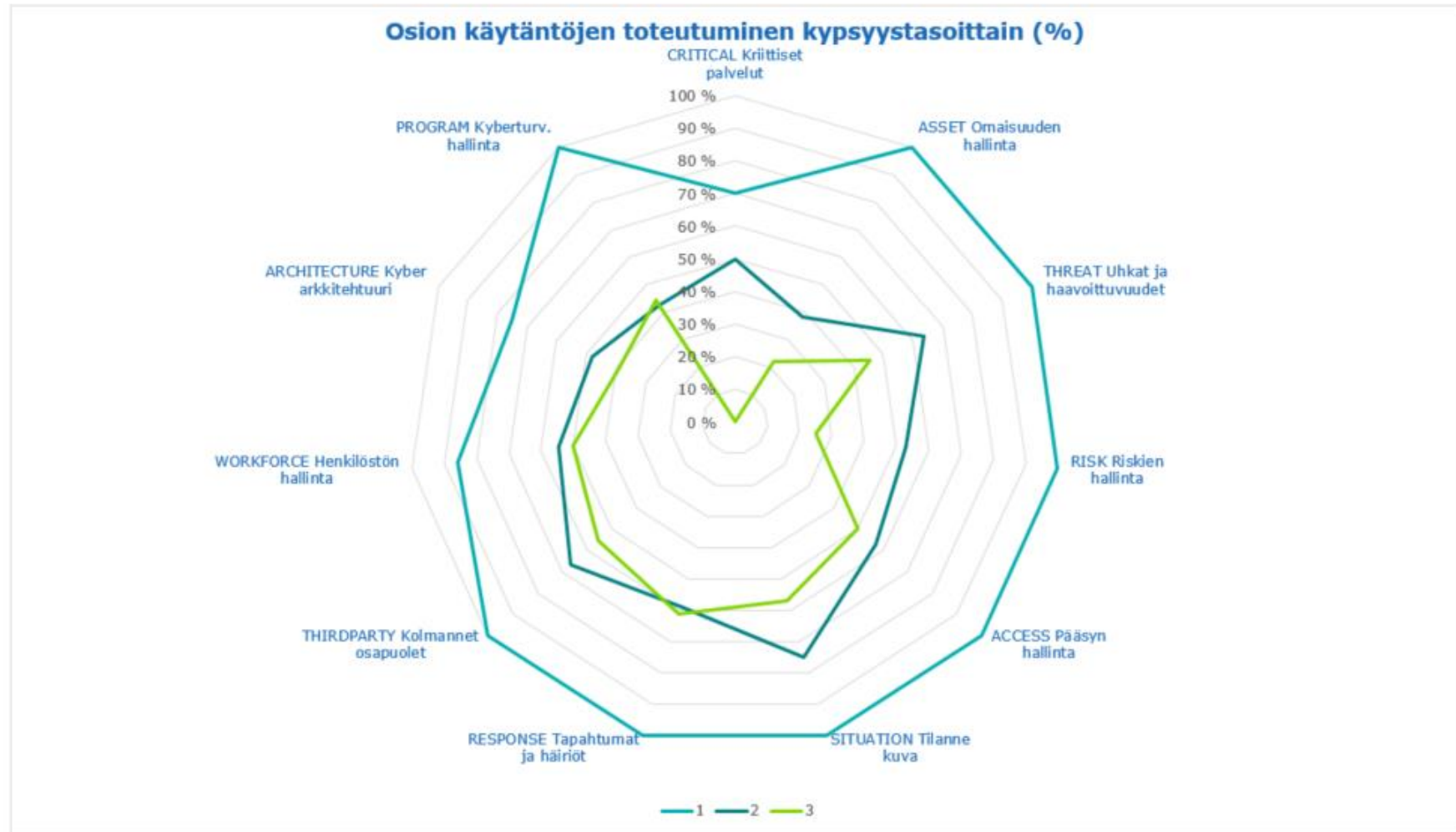
4. R5 Yleiset hallintatoimet, yhteenveto

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



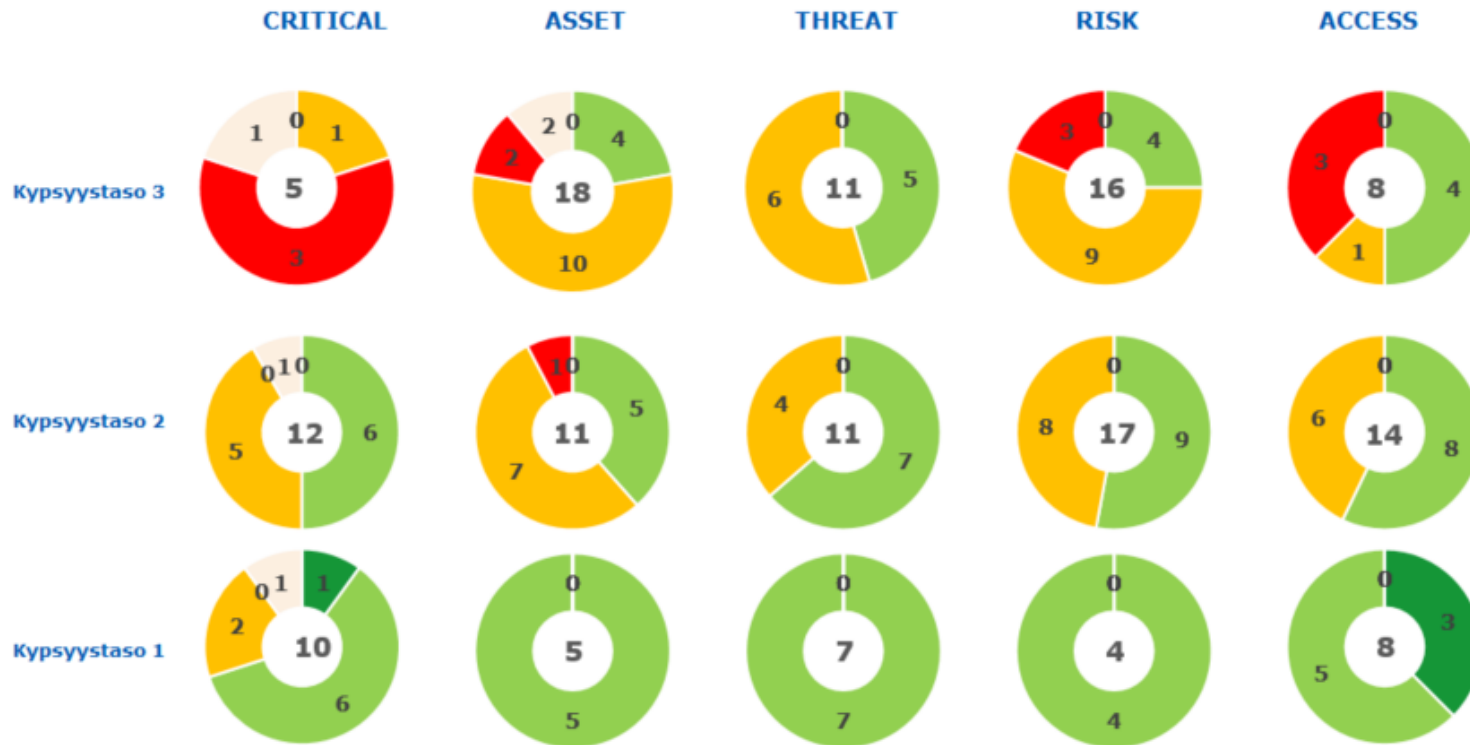
R6



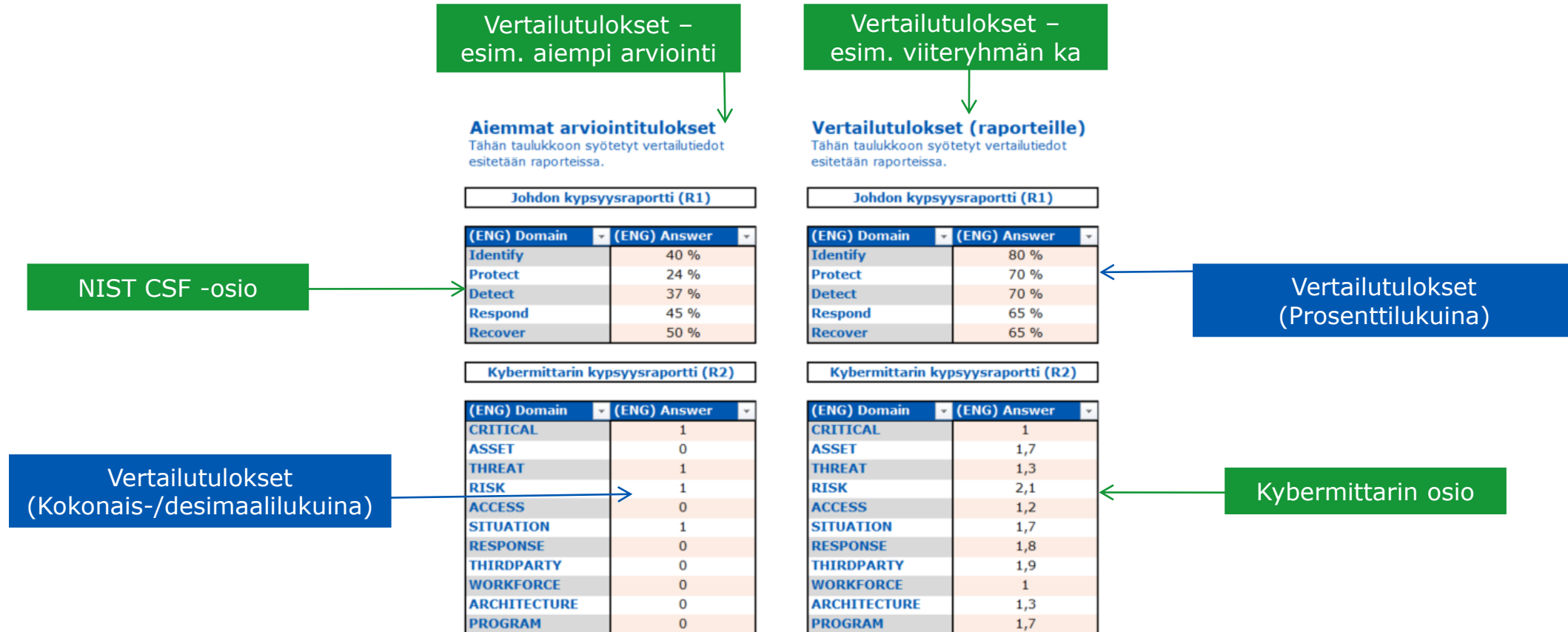
KYBERMITTARI

Osiokohtainen kypsyystasoraportti

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



5. Import-välilehti



Muut Kybermittarin toiminnallisuuksiin liittyvät välilehdet

▶ Data

- ▶ Kypsyystasojen koonti- ja laskentasisu

▶ NISTMap

- ▶ Kybermittarin / C2M2 –mallien ja NIST CSF –mallien välinen ristiin kytkentä

▶ Migration ja Mapping

- ▶ V1 -> V2 siirto

▶ Languages

- ▶ Selitetekstien kieliversiot (FI, SE, EN)

▶ Parameters

- ▶ Työkalun käyttämät vaihtoehdot ja säätöparametrit



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Lähteitä

Lähteitä

- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ohjeet>
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta>
- ▶ <https://c2m2.doe.gov/>
- ▶ <https://www.nist.gov/cyberframework>

Kiitos!

<https://www.kybermittari.fi>

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ohje tulosten jakamiseen

Organisaation tulokset

- Täytä arviointi ja tallenna tulokset.
- Voit käyttää jakamiseen joko .xlsx tai .xml-muotoa (tarkemmat ohjeet löytyvät työkalun DataExport-välilehdeltä)

Tulosten lähettäminen

- Voit käyttää tulosten lähettämiseen omaa turvapostia tai lähetä viestin, jossa yhteystietosi (nimi ja puhelinnumero*) osoitteeseen kybermittari@traficom.fi niin saat ohjeet.
- Lähetä tulokset turvapostilla Traficomiin osoitteeseen kybermittari@traficom.fi

Tulosten käsittely

- Kyberturvallisuuskeskus käsittelee ja anonymisoi tulokset
- Tuottaa tulosten pohjalta toimialakohtaista vertailutietoa
- Kun riittävä määrä tietoa on saatavilla, jakaa tapauskohtaisesti vertailutietoa organisaatiolle turvasähköpostilla

*Puhelinnumero vaaditaan, jotta Traficom pystyy toimittamaan toimialan vertailutiedot varmennetulle vastaanottajalle.