TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari vrt Kyberkypsyys toimialoilla - selvitys

30.9.2025

Taustaa

- Kybermittari, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto
  - Kybermittari-palvelun tarkoituksena on auttaa organisaatioita ymmärtämään ja kehittämään kyvykkyyttään suojautua kyberuhilta ja parantaa toimintansa kyberturvallisuutta.

- Kyberkypsyys toimialoilla 2025, Digipooli, Huoltovarmuuskeskus
  - Tarkoituksena määrittää toimialojen kyberturvallisuuden taso. Selvitys on tarkoitus toteuttaa säännöllisesti noin kahden-kolmen vuoden välein käynnistettyjen kehitystoimenpiteiden vaikutusten ja yleisten trendien seuraamiseksi.

Yhteenveto

- Kyberkypsyys toimialoilla selvityksessä on hyödynnetty Kybermittarista osiota (11kpl) ja tavoitetason rakennetta.
  - Tavoitteiden käytännöt, joita Kybermittarissa on tavoitetta kohden on 6 – 13 kpl, on selvityksessä korvattu yhdellä haastattelukysymyksellä ja kriteeristöllä.
  - Numeeriset tulokset eivät ole suoraan vertailukelpoisia Kybermittarilla saatavien tavoitetason tulosten kanssa.
- Tulosten tarkastelu Kybermittarin avulla
  - Kyberkypsyys toimialoilla selvityksen havaintoja voi tarkentaa ja työstää hyödyntämällä Kybermittarin osioon, tavoitteeseen, kehityskohteeseen liitettyjä Kybermittarin käytäntöjä.
  - Esimerkkinä valitse suosituksissa oleva teema ja katso Kybermittarista vastaava osio. Alateema voi löytyä tavoitteista, kehityspoluista tai yksittäisistä käytännöistä.
  - Vastaavasti, jos organisaatio on käyttänyt Kybermittaria niin havaintoja voi verrata osioittain.

Toimialaraportin sisältö (noin 22 sivua)

Sisällysluettelo

Selvityksissä on osa-alueet eri järjestyksessä raportoinnissa. (2025)

KM järj.	Kybermittari osio	Kyberselvitys toimialoilla	Osa-alueen kuvaus
11	PROGRAM	Kyberturvallisuuden hallinta	Kyberturvallisuuden hallinta osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuista kyberturvallisuusohjelmaa.
10	ARCHITECTURE	Kyberturvallisuusarkkitehtuuri	Kyberturvallisuusarkkitehtuuri osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää kyberturvallisuustoimintaansa.
4	RISK	Riskienhallinta	Riskienhallinta osa-alueessa arvioidaan organisaation tieto- ja kyberturvallisuuteen liittyvien riskien (kyberriskit) tunnistamisen ja hallinnan valmiuksia.
1	CRITICAL	Kriittisten palveluiden suojaaminen	Kriittisten palveluiden suojaaminen osa-alueessa arvioidaan organisaation kykyä tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja sen myötä suojaamisessa.
3	THREAT	Uhkien ja haavoittuvuuksien hallinta	Uhkien ja haavoittuvuuksien hallinta osa-alueessa arvioidaan organisaation kykyä määritellä ja ylläpitää suunnitelmia, prosesseja ja tekniikoita kyberuhkien ja -haavoittuvuuksien havainnointiin, tunnistamiseen, analysointiin, hallintaan ja niihin puuttumiseen.
2	ASSET	Omaisuuden, muutosten ja konfiguraation hallinta	Omaisuuden, muutosten ja konfiguraation hallinta osa-alueessa arvioidaan organisaation kykyä hallita laite-, ohjelmisto- ja tieto-omaisuuttaan suhteessa organisaatioon kohdistuviin riskeihin ja organisaation tavoitteisiin.
9	WORKFORCE	Henkilöstön johtaminen ja kehittäminen	Henkilöstön johtaminen ja kehittäminen osa-alueessa henkilöstön johtaminen ja kehittäminen arvioidaan henkilöstön kyberturvallisuustietoisuutta, -osaamista, sekä valmiutta reagoida erilaisiin kyberhäiriötilanteisiin
8	THIRD-PARTIES	Kumppaniverkoston riskienhallinta	Kolmansien osapuolten riskienhallinta osa-alueessa arvioidaan organisaation kykyä tunnistaa sekä hallinnoida toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä.
6	SITUATION	Tilannekuva	Tilannekuva osa-alueessa arvioidaan organisaation kykyä ylläpitää kyberturvallisuuden tilannekuvaa.
7	RESPONSE	Tapahtumien ja poikkeamien hallinta	Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus osa-alueessa arvioidaan organisaatioiden kykyjä hallinnoida, reagoida sekä palautua kyberhäiriötilanteista.
5	ACCESS	Identiteetin- ja pääsynhallinta	Identiteetin- ja pääsynhallinta osa-alueessa arvioidaan organisaation kykyä hallinnoida ja rajoittaa loogisia ja fyysisiä pääsyoikeuksia yrityksen suojattavaan omaisuuteen.

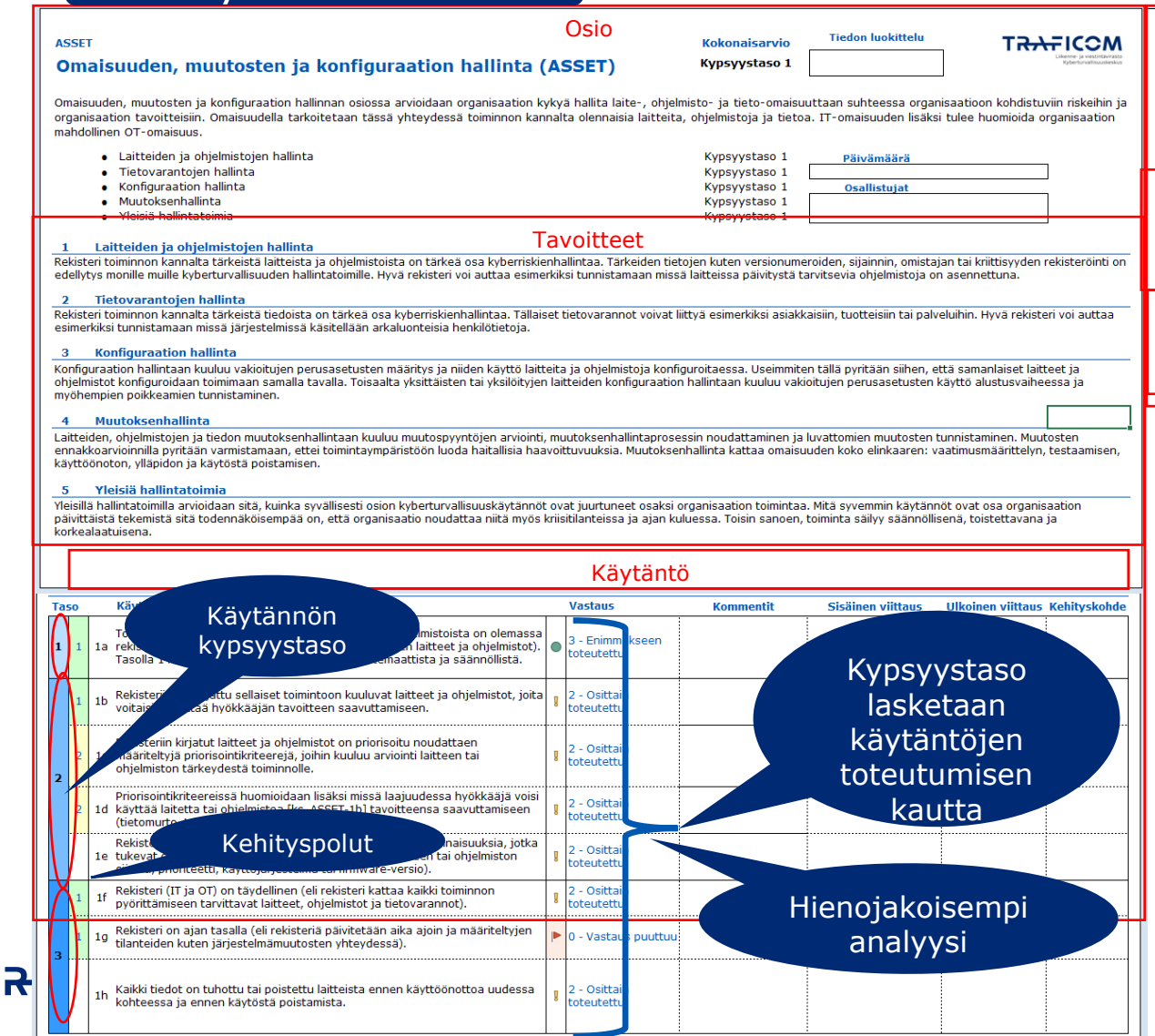
Kypsyystasomäärittelyt Kybermittari vrt kyberturvallisuus toimialoilla -selvitys (2025)

Kypsyystaso	Kybermittari / yleisvaatimukset tasolle
0	Organisaatio ei toteuta kyberturvallisuuden hallintaan liittyviä käytäntöjä
1	Organisaatio toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä
2	Organisaatiolla **dokumentoidut säännöllisesti toistettavat ja ylläpidettävät** kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet kyberturvallisuuden toteuttamiseksi on määritetty.
3	Organisaatio toteuttaa kyberturvallisuutta **riskilähtöisesti**, koko organisaation kattavia **toimintamalleja ylläpidetään jatkuvasti** ja kyberturvallisuudelle on määritetty tavoitteet, joita mitataan säännöllisesti.
info	**Jokainen yksittäinen käytäntö on liitetty jollekin kypsyystasoista 1, 2 tai 3. Käytännöt arvioidaan asteikolla 1-4 (ei toteutettu – täysin toteutettu)**

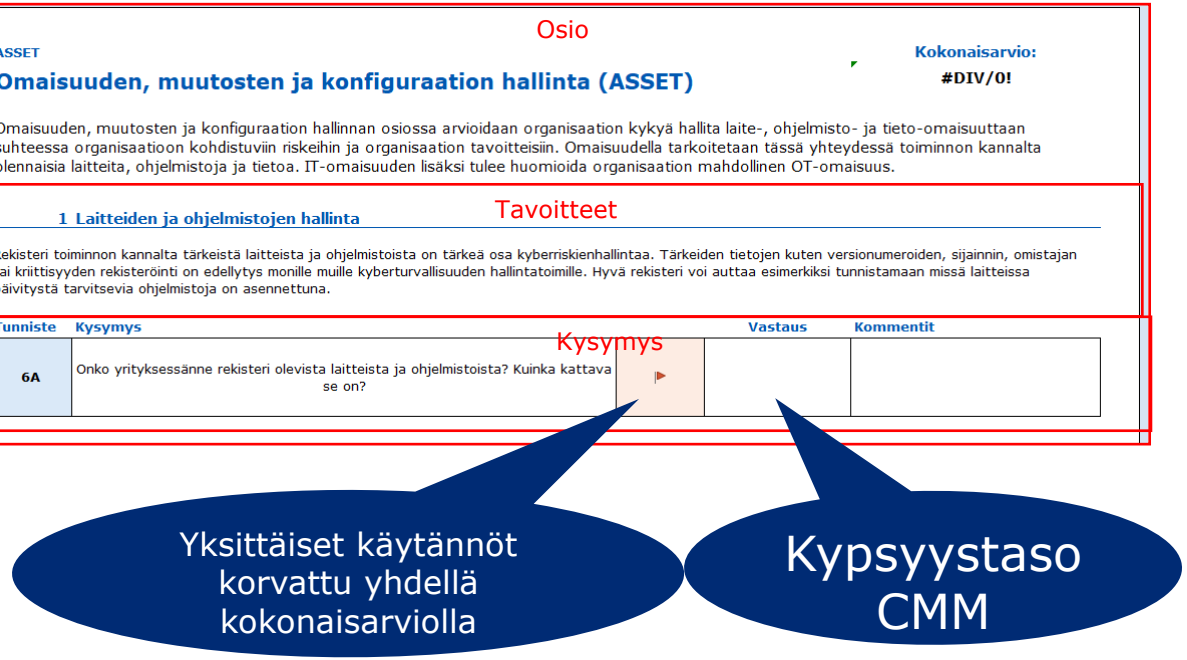
Kypsyystaso	CMM Kuvaus / yleisvaatimukset tasolle
1	Ei määritelty. Organisaatio ei toteuta osa-alueeseen liittyviä käytäntöjä. Käytäntöjen mahdollinen toteuttaminen reaktiivista ja suunnittelematonta.
2	Organisaatio **toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä**. Esimerkiksi joitain prosesseja on olemassa, mutta niitä ei ole dokumentoitu. Kehittämisen ja ylläpidon ei tarvitse olla systemaattista.
3	Toiminta systemaattista, esim. regulaatiolähtöistä. Toimintatavat ja prosessit dokumentoitu, mutta koskevat vain osaa toiminnoista, vaativat päivitystä tai niitä ei ole jalkautettu kauttaaltaan. Ei jatkuvaa arviointia / auditointia.
4	Organisaatiolla on **dokumentoidut säännöllisesti toistettavat** ja **ylläpidettävät** kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet käytäntöjen toteuttamiseksi. Selkeät prosessit ja toimintatavat, joita noudatetaan ja niiden toteutumista valvotaan. Priorisointia tehty kriittisyyden ja riskiarvion perusteella..
5	Organisaatio toteuttaa käytäntöjä **riskilähtöisesti**, koko organisaation kattavia **toimintamalleja ylläpidetään jatkuvasti** ja kyberturvallisuudelle on määritetty **tavoitteet**, joita **mitataan säännöllisesti**. Toimintaa johdetaan strategisesti, organisaation johto on sitoutunut toimintaan. Käytössä toimintaa tukevat modernit teknologiset kyvykkyydet.

Kybermittarin rakenne vs Digipoolin toimialojen kyberselvitys
Monta käytäntöä per tavoite vs 1 arvioitava kohta per tavoite.

Kybermittari



Toimialojen kyberselvitys



Kybermittari

ASSET

Osio

Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Kokonaisarvio

Kypsyystaso 1

Tiedon luokittelu

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

Tavoitteet

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.

1 Laitteiden ja ohjelmistojen hallinta

Käytäntö

Taso		Käytäntö		Vastaus	Kommentit	Sisäinen viittaus	Ulkoinen viittaus	Kehityskohde
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 Rekist… …ohjelmistot on priorisoitu noudattaen m… …joihin kuuluu arviointi laitteen tai …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				
		1e Rekisteriin on kirjattu laitteista ja ohjelmistoista sellaisia ominaisuuksia, jotka tukevat organisaation kybertoimintaa (esimerkiksi laitteen tai ohjelmiston sijainti, prioriteetti, käyttöjärjestelmä tai firmware-versio).		2 - Osittain toteutettu				
3	1	1f Rekisteri (IT ja OT) on täydellinen (eli rekisteri kattaa kaikki toiminnon pyörittämiseen tarvittavat laitteet, ohjelmistot ja tietovarannot).		2 - Osittain toteutettu				
	1	1g Rekisteri on ajan tasalla (eli rekisteriä päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä).		0 - Vastaus puuttuu				
		1h Kaikki tiedot on tuhottu tai poistettu laitteista ennen käyttöönottoa uudessa kohteessa ja ennen käytöstä poistamista.		2 - Osittain toteutettu				

Kypsyys tasot

Kehityspolut

Kypsyystao määritellään käytäntöjen toteutumisen kautta

Hienojakoisempi analyysi

Kybermittarin rakenne vs Digipoolin toimialojen kyberselvitys
Monta käytäntöä per tavoite vs 1 arvioitava kohta per tavoite.

Toimialojen kyberselvitys

Osio

ASSET

Kokonaisarvio:

#DIV/0!

Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

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.

Tavoitteet

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.

Tunniste	Kysymys	Kysymys	Vastaus	Kommentit
6A	Onko yrityksessänne rekisteri olevista laitteista ja ohjelmistoista? Kuinka kattava se on?			

Yksittäiset käytännöt korvattu yhdellä kokonaisarviolla

Kypsyystaso 1-5

Miten löytää vastaavat käytännöt kehitystyötä ja seurantaa varten

Selvitys - suositukset

Suositukset

Teema	Alateema
01 Kyberturvallisuusarkkitehtuuri	Tietojen suojaus
	Muutostenhallinta
	Palomuurit

Kybermittari Osiot ja tavoitteet

Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

- Kyberarkkitehtuurin kehittäminen
- Tietoverkkojen suojaus osana kyberarkkitehtuuria
- Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria
- Sovellusturvallisuus osana kyberarkkitehtuuria
- Tietojen suojaus osana kyberarkkitehtuuria
- Yleisiä hallintatoimia

7	ASSET	Muutosten ja päivitysten tekeminen turvallisesti
8	ASSET	Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtyjen muutosten dokumentointi

Kybermittari Kehityspolut

60	ARCHITECTURE	Kyberturvallisuusarkkitehtuurin kehittämissuunnitelma
61	ARCHITECTURE	Kyberturvallisuusarkkitehtuuri
62	ARCHITECTURE	Kyberturvallisuusarkkitehtuurin hallintamalli ja johdon tuki
63	ARCHITECTURE	Omaisuuserien segmentointi
64	ARCHITECTURE	Verkkojen suojaus
65	ARCHITECTURE	IT- ja OT-omaisuuden sekä tietovarantojen turvaaminen
66	ARCHITECTURE	Turvalliset konfiguraatiot
67	ARCHITECTURE	Turvallinen ohjelmistokehitys käytössä talon sisällä
68	ARCHITECTURE	Turvallinen ohjelmistokehitys käytössä toimittajilla
69	ARCHITECTURE	Tietojen suojaus

Kybermittari - 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

Kybermittari – käytäntöjen 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

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus