TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari vrt toimialojen kyberselvitys

16.2.2023

Taustaa

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

- Toimialojen kyberselvitys 2022, 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

- Vaikka Kybermittarin ylätason rakennetta on hyödynnetty Digipoolin toimialojen kyberselvityksessä niin käytetyllä mallilla saadut tulokset eivät ole vertailukelpoisia Kybermittarilla saatavien tulosten kanssa
  - Tavoitteiden käytännöt korvattu yksittäisillä kysymyksillä
  - Arviointien kypsyysmallit ovat erilaiset
- Toimialojen kyberselvityksessä on mitattu kypsyystasoa Kybermittarin tavoitetasolla, mutta siitä puuttua tietoa konkreettisista käytännöistä. (ks. seuraava sivu)
  - Havaintoja voi tarkentaa hyödyntämällä valittuun kehityskohteeseen / tavoitteeseen liitettyjä Kybermittarin käytäntöjä. (ks seuraava sivu)

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

Kybermittari

Osio

PROGRAM

Kyberturvallisuuden hallinta (PROGRAM)

Kokonaisarvio
Kypsyystaso 1

Tiedon luokittelu

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.

- Kyberturvallisuusstrategia — Kypsyystaso 1
- Johdon tuki kyberturvallisuusohjelmalle — Kypsyystaso 2
- Yleisiä hallintatoimia — Kypsyystaso 1

Päivämäärä

Osallistujat

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 organisaatiorakenteen 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 ylimmän johdon näkyvän osallistumisen sekä vastuiden määrittelyn ja valtuutukset kyberturvallisuusohjelmalle. Lisäksi tuki kattaa organisatorisen tuen, jota vaaditaan poliitikkojen tai vastaavien ohjeistusten määrittämiseksi ja ylläpitämiseksi.

3 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 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				
2	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				
	1e	Kyberturvallisuusstrategia määrittelee kyberturvallisuuden hallinta- ja organisaatiorakenteen.	2 - Osittain toteutettu				
	1f	Kyberturvallisuusstrategia nimeää ne standardit ja ohjeet, joita tulee noudattaa.	3 - Enimmäkseen toteutettu				
	1g	Kyberturvallisuusstra… …laiki olennaiset vaatimusten… …GS), joita tule…	2 - Osittain toteutettu				
3	1h	Kyberturvallisuusstrategia päivitetään tarvittaessa muutoksia organisaation liiketoiminnassa, toimintaympäristössä tai uhkaprofiilissa [kts. THREAT-2d].	2 - Osittain toteutettu				

Käytäntö

Kypsyystasot

Kypsyystao määritellään käytäntöjen toteutumisen kautta

Hienojakoisempi analyysi

Toimialojen kyberselvitys

Osio

PROGRAM

Kyberturvallisuuden hallinta (PROGRAM)

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

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 organisaatiorakenteen ja ylemmän johdon vahvemman osallistumisen ohjelmaan suunnitteluun. Kyberturvallisuusstrategia voi olla oma dokumenttinsa, mutta usein se on kirjattu

Taso	Käytäntö	Kysymys	Vastaus	Osakohdan kypsyys
1	1a	Oletteko asettaneet tietoturvan/kyberturvan osalta strategian tai suunnan joka ohjaa kehitystoimia? Onko strategia sidoksissa muuhun strategiaanne, kuten esimerkiksi liiketoiminnan?	3 - Mallinnettu ja dokumentoitu, mutta ei seurata tai mitata kauttaaltaan	0

Kypsyystaso CMM

Yksittäiset käytännöt korvattu yhdellä kokonaisarviolla

NIST Cybersecurity Framework (CSF)- ja Cybersecurity Capability Maturity Model (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

Selvityksissä on osa-alueet eri järjestyksessä raportoinnissa.

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

Kypsyystasomäärittelyt Kybermittari vrt toimialakartoitus

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)**

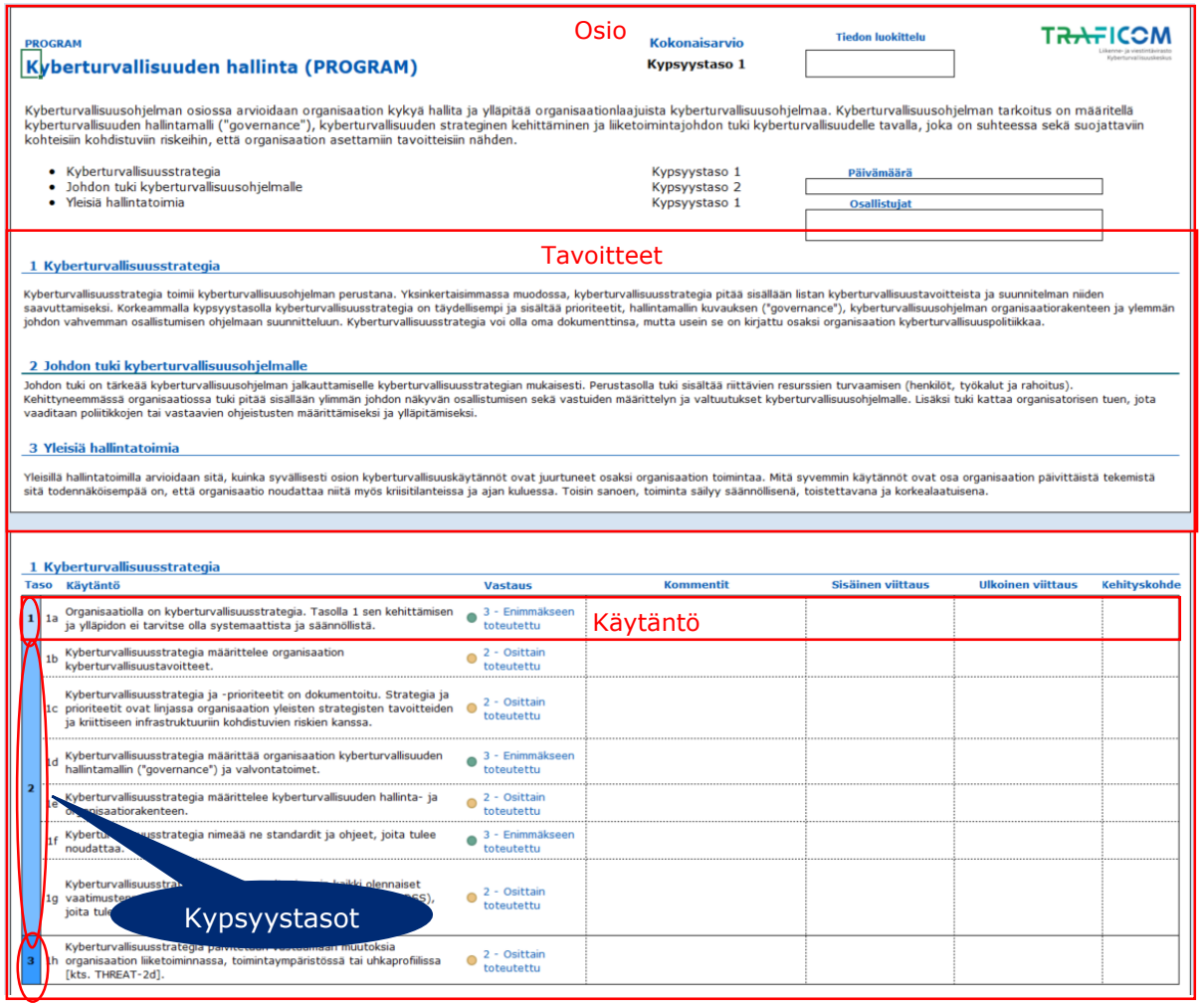
Kypsyystaso	CMM Kuvaus / yleisvaatimukset tasolle
1	Toiminta reaktiivista, prosesseja ei kuvattu tai ne ovat vakiintumattomia.
2	Prosessit ovat suunniteltuja, valvottuja ja ne toteutuvat sovittujen menettelytapojen mukaisesti. Dokumentaatio ei ole kattavaa, eikä prosessien taustalla ole johtamisjärjestelmää.
3	Johtamisjärjestelmä määritelty ja käytössä, prosessit perustuvat organisaation yhteisiin standardeihin ja linjauksiin. Ei jatkuvaa arviointia/auditointia, dokumentaation päivittäminen on puutteellista.
4	Johtamisjärjestelmä toteuttaa jatkuvan parantamisen mallia, prosessien laadulle ja suorituskyvylle on asetettu vaatimukset, joita seurataan. Toiminta on systemaattista.
5	Jatkuvan parantamisen malli, jota tuetaan teknologisilla kyvykkyyksillä ja niiden kehittämisellä (mm. automatisointi, modernit ratkaisut). Prosessit kattavat koko organisaation ja linkittyvät organisaation strategiseen tasoon.

Vertailua

- Kybermittari
  - Avoin, vapaasti saatavilla oleva välineistö
  - Asiakkaan toistettavissa oleva menetelmä
  - Hienojakoinen, useita käytäntöjä per tavoite – konkreettisemmat kehityskohteet ja hienojakoisempi GAP-analyysi
  - Kielet: suomi, ruotsi, englanti
  - Itsearviointi tarvittaessa tuettuna
- Toimialaselvitys
  - Suljettu menetelmä
  - Pdf-raportointi asiakkaalle. Ei työvälineistöä.
  - Yksi, koostava kysymys per tavoite
  - Vain suomenkielinen
  - Haastattelututkimus
  - Sisältää toimialakohtaisen riskiarvion

Kybermittarin perusrakenne

Kybermittarin rakenne



- Kybermittari koostuu
  - **Osioista** (yhteensä 11)
  - **Tavoitteista**, joita on osioilla yhteensä (46, hallintatoimia näistä 10)
  - **Käytännöistä**, joiden avulla mitataan tavoitteiden täyttymistä (yhteensä 367 jaettuna kolmelle tasolle)
- 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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

https://www.kybermittari.fi

kybermittari@traficom.fi