TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2.0 verrattuna versioon 1.0

04.10.2022

Sisältö

- Yleistä Kybermittarista
- Muutokset Kybermittarin rakenteeseen
- Muutokset osioittain
- Muutokset raportointiin
- Käytettävyys

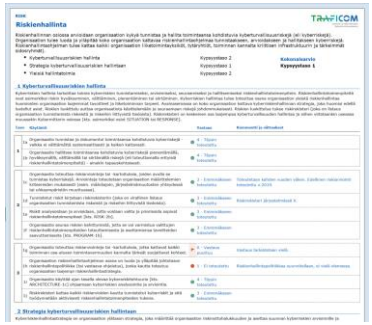
Yleistä Kybermittarista

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

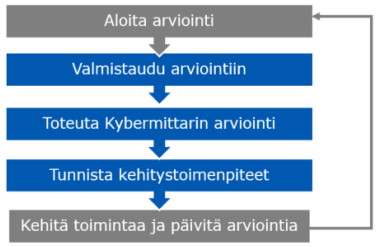
Kybermittari

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

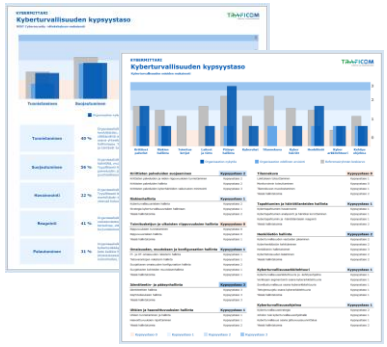
Kybermittarin materiaalit



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



- Ohjeistus ja tuki arviointiprosessiin
  - Organisaation itse toteuttamana tai ulkoisen palveluntarjoajan tukemana.



- Automaattisesti tuotetut raportit
  - Tuloksena organisaation kyberturvallisuuden kypsyystaso eri näkökulmista.

Kybermittarin taustalla olevat viitekehykset

- Kybermittarin 10 osiota ja osioiden käytännöt perustuvat suurelta osin C2M2-malliin. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
  - Kybermittari V1 pohjautui C2M2 V2 luonnokseen.
  - Kybermittari V2.0:n pohjana on C2M2 V2.0.
  - C2M2 version V2.1 vaikutuksia analysoidaan parhaillaan. Suuria rakenteellisia muutoksia ei tullut. https://c2m2.doe.gov/resources
- Lisäksi kehitetty kriittisten palveluiden suojaamisen osio (CRITICAL)
- Tulokset on ristiin kytketty soveltuvin osin NIST-malliin ja tulokset voidaan täten raportoida myös NIST CSF-mallin kyvykkyyksien näkökulmasta. Ristiinkytkentä on viitteellinen ja se on tehty Liikenne- ja viestintävirastossa.

Muutokset Kybermittarin rakenteeseen

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Muutokset käyttäjän näkökulmasta

Rakenne	Mallin rakenne ja laskentamalli säilyvät käytännössä ennallaan
Osiot	Yksi osio nimetty uudelleen DEPENDENCIES->THIRDPARTY. Sisällöllisesti suurehkoja muutoksia kolmessa osiossa.
Tavoitteet	Tavoitteisiin suurimmat muutokset mm. RISK-osiossa. Yksi tavoitteista siirretty osiosta toiseen.
Käytännöt	Uusi käytäntöjä erityisesti kypsyystasoille 2 ja 3.
Raportointi	C2M2-laskentamalli säilyy ennallaan, mutta raportoinnin on lisätty elementtejä, joita lisätään soveltuvin osin Kybermittariin. Kybermittarin laskentamalli ei ole yhtä vaativa vaan nousu tasolle 2 vaatii vain >50%

! Versiolla 1 tehdyn arvioinnin tulokset on mahdollista siirtää versioon 2. Tästä saa pyytämällä erillisen ohjeen. Numeeristen tulosten migraatioon on ohje ja välineet työkalussa, välilehdellä MIGRATION. !

NIST Cybersecurity Framework V1.1

- Ristiinviittaukset Kybermittari/C2M2 - NIST Cybersecurity Framework on viitteellinen ja toteutettu Liikenne- ja viestintävirastossa. Toteutus on näkyvillä Kybermittarin NISTmap-välilehdellä.

	Osa-alue	viittaukset
ID	Tunnistaminen	304
PR	Suojautuminen	315
DE	Havannointi	131
RS	Reagointi	74
RC	Palautuminen	21

- NIST Cybersecurity Framework V1.1 (https://www.nist.gov/cyberframework)
  - Viitekehyksestä ei ole saatavilla virallista, suomenkielistä käännöstä.
  - NIST CSF 2.0 kehitystyö on jo aloitettu

Versioiden välinen, tilastollinen vertailu.

	Kybermittari 1.0	Kybermittari 2.0
Osiot	11 (10 + CRITICAL)	11 (10 + CRITICAL)
Tavoitteet	42 (hallintatoimia 10)	46 (hallintatoimia 10)
Käytännöt yht.	325	369
Käytännöt 1 taso	60	64
Käytännöt 2 taso	147	162
Käytännöt 3 taso	118	143

Muutokset osioittain

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Critical Service Protection (CRITICAL)

Vanha

Kriittisten palveluiden suojaaminen

- Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
- Kriittisten palveluiden hallinta
- Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

Uusi

Kriittisten palveluiden suojaaminen

- Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
- Kriittisten palveluiden hallinta
- Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

Merkittäviä muutoksia | Kohtalaisia muutoksia | Vähän muutoksia

Muutokset C2M2 malliin

- Arviolta puolet C2M2-mallin kymmenestä osiosta säilyy pitkälti ennallaan.

Asset, Change, and Configuration Management (ASSET)	→	Asset, Change, and Configuration Management (ASSET)
Threat and Vulnerability Management (THREAT)	→	Threat and Vulnerability Management (THREAT)
Risk Management (RISK)	⇢	Risk Management (RISK)
Identity and Access Management (ACCESS)	⇢	Identity and Access Management (ACCESS)
Situational Awareness (SITUATION)	→	Situational Awareness (SITUATION)
Event and Incident Response (RESPONSE)	⇢	Event and Incident Resp., Continuity of Operations (RESP...)
Supply Chain and Ext. Dependencies... (DEPENDENCIES)	⇢	Third-Party Risk Management (THIRDPARTY)
Workforce Management (WORKFORCE)	→	Workforce Management (WORKFORCE)
Cybersecurity Architecture (ARCHITECTURE)	⇢	Cybersecurity Architecture (ARCHITECTURE)
Cybersecurity Program Management (PROGRAM)	→	Cybersecurity Program Management (PROGRAM)

		Vastaava	Muuttunut	Uusi	Yhteensä	Poistunut
Omaisuuden, muutosten ja konfiguraation hallinta	ASSET	27	3	6	36	1
Uhkien ja haavoittuvuuksien hallinta	THREAT	26	4	0	30	2
Riskienhallinta	**RISK**	**5**	**14**	**18**	**37**	**4**
Identiteetin- ja pääsynhallinta	ACCESS	15	7	9	31	1
Tilannekuva	SITUATION	25	3	1	29	1
Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus	RESPONSE	42	2	5	49	1
Kumppaniverkoston riskien hallinta	**THIRDPARTY**	**12**	**6**	**4**	**22**	**10**
Henkilöstön johtaminen ja kehittäminen	WORKFORCE	27	2	1	30	1
Kyberturvallisuus-arkkitehtuuri	**ARCHITECTURE**	**25**	**7**	**22**	**54**	**3**
Kyberturvallisuuden hallinta	PROGRAM	24	2	0	26	2

Vähän muutoksia

Asset, Change, and Configuration Management (ASSET)

Vanha

Omaisuuden, muutoksen ja konfiguraation hallinta

- IT- ja OT-omaisuuden rekisterin hallinta
- Tietovarantojen rekisterin hallinta
- Suojattavan omaisuuden konfiguraation hallinta
- Suojattavien kohteiden muutoksenhallinta
- Yleisiä hallintatoimia

Uusi

Omaisuuden, muutosten ja konfiguraation hallinta

- Laitteiden ja ohjelmistojen hallinta
- Tietovarantojen hallinta
- Konfiguraation hallinta
- Muutoksenhallinta
- Yleisiä hallintatoimia

Vähän muutoksia

Threat and Vulnerability Management (THREAT)

Vanha

Uhkien ja haavoittuvuuksien hallinta

- Uhkien tunnistaminen ja hallinta
- Haavoittuvuuksien rajoittaminen
- Yleisiä hallintatoimia

Uusi

Uhkien ja haavoittuvuuksien hallinta

- Haavoittuvuuksien vähentäminen
- Uhkien torjunta ja uhkatiedon jakaminen
- Yleisiä hallintatoimia

Risk Management (RISK)

Vanha

Riskienhallinta

- Kyberturvallisuusriskien hallinta
- Strategia kyberturvallisuusriskien hallintaan
- Yleisiä hallintatoimia

Uusi

Riskienhallinta

- Kyberriskienhallinnan suunnitelma
- Kyberriskien tunnistaminen
- Riskien analysointi
- Riskeihin reagointi
- Yleisiä hallintatoimia

Identity and Access Management (ACCESS)

Vanha

Identiteetin- ja pääsynhallinta

- Identiteettien hallinta
- Käyttöoikeuksien hallinta
- Yleisiä hallintatoimia

Uusi

Identiteetin- ja pääsynhallinta

- Identiteettien luominen ja hallinta
- Loogisten käyttöoikeuksien hallinta
- Fyysinen pääsynhallinta
- Yleisiä hallintatoimia

Vähän muutoksia

Situational Awareness (SITUATION)

Vanha

Tilannekuva

- Lokituksen toteuttaminen
- Monitoroinnin toteuttaminen
- Tilannekuvan muodostaminen
- Yleisiä hallintatoimia

Uusi

Tilannekuva

- Lokienhallinta
- Ympäristöjen valvonta
- Tilannekuvan ylläpito
- Yleisiä hallintatoimia

Event and Incident Response, Continuity of Operations (RESPONSE)

Vanha

Tapahtumien ja häiriötilanteiden hallinta

- Kybertapahtumien havainnointi
- Kybertapahtumien analysointi ja häiriöksi korottaminen
- Kybertapahtumiin ja -häiriötilanteisiin reagointi
- Yleisiä hallintatoimia

Uusi

Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus

- Tapahtumien havainnointi
- Tapahtumien analysointi ja häiriötilanteiden määrittäminen
- Tapahtumiin ja häiriöihin reagoiminen
- Kyberturvallisuus osana toiminnan jatkuvuutta (ennen PROGRAM-osiossa)
- Yleisiä hallintatoimia

Third-Party Risk Management (THIRDPARTY)

Vanha

Toimitusketjun ja ulkoisten riippuvuuksien hallinta (DEPENDENCIES)

- Riippuvuuksien tunnistaminen
- Riippuvuusriskien hallinta
- Yleisiä hallintatoimia

Uusi

Kumppaniverkoston riskienhallinta

- Kumppanien tunnistaminen ja priorisointi
- Kumppaneihin liittyvien riskien hallinta
- Yleisiä hallintatoimia

Vähän muutoksia

Workforce Management (WORKFORCE)

Vanha

Henkilöstön hallinta

- Kyberturvallisuuden vastuiden jakaminen
- Kyberhenkilöstön kehittäminen
- Henkilöstön hallintatoimet
- Kybertietoisuuden lisääminen
- Yleisiä hallintatoimia

Uusi

Henkilöstön johtaminen ja kehittäminen

- Kyberturvallisuuden vastuiden jakaminen
- Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen
- Henkilöstöhallinnon prosessit
- Koulutus ja kybertietoisuuden lisääminen
- Yleisiä hallintatoimia

Cybersecurity Architecture (ARCHITECTURE)

Vanha

Kyberturvallisuusarkkitehtuuri

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

Uusi

Kyberturvallisuusarkkitehtuuri

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

Vähän muutoksia

Cybersecurity Program Management (PROGRAM)

Vanha

Kyberturvallisuusohjelma

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Kyberturvallisuus osana jatkuvuussuunnittelua (siirto RESPONSE-osioon)
- Yleisiä hallintatoimia

Uusi

Kyberturvallisuuden hallinta (PROGRAM)

- Kyberturvallisuusstrategia
- Johdon tuki kyberturvallisuusohjelmalle
- Yleisiä hallintatoimia

Muutokset raportointiin

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Päämuutokse raportointiin

- 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.

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

R5

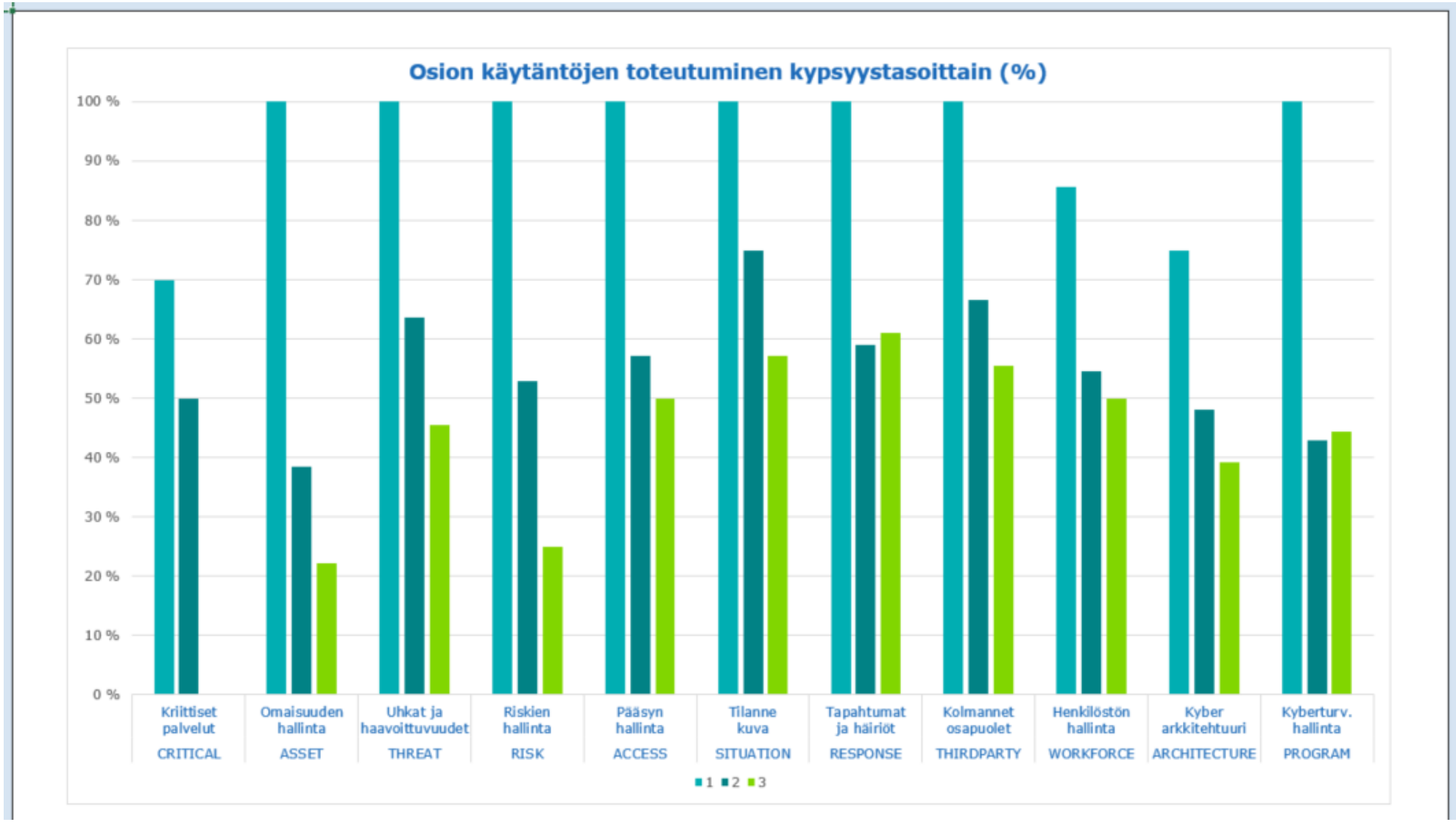
KYBERMITTARI

Yleiset hallintatoimet

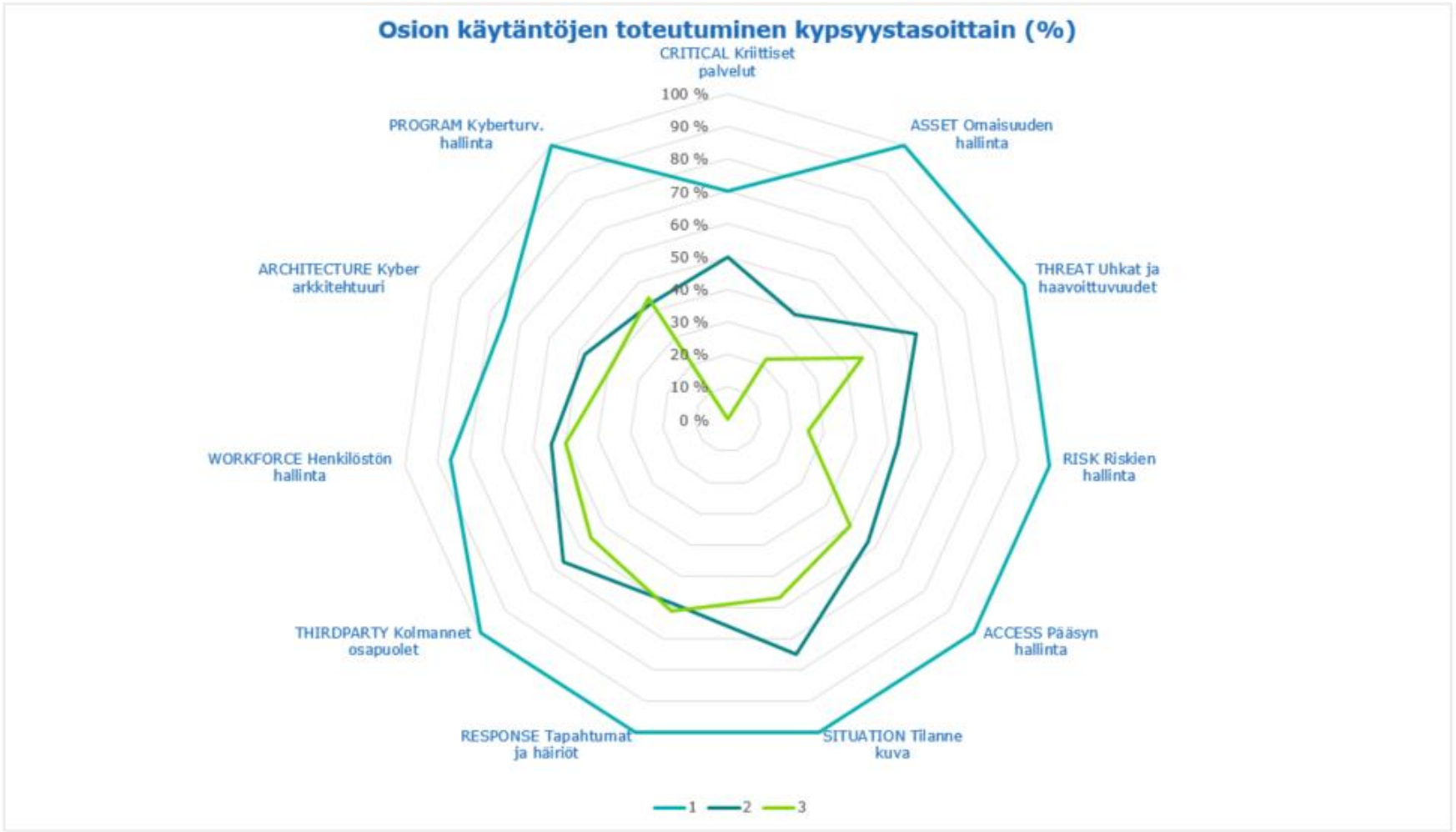
Selite:	0 - Vastaus	1 - Ei toteutettu	2 - Osittain toteutettu	3 - Enimmäkse	4 - Täysin toteutettu

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

R6


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

R6

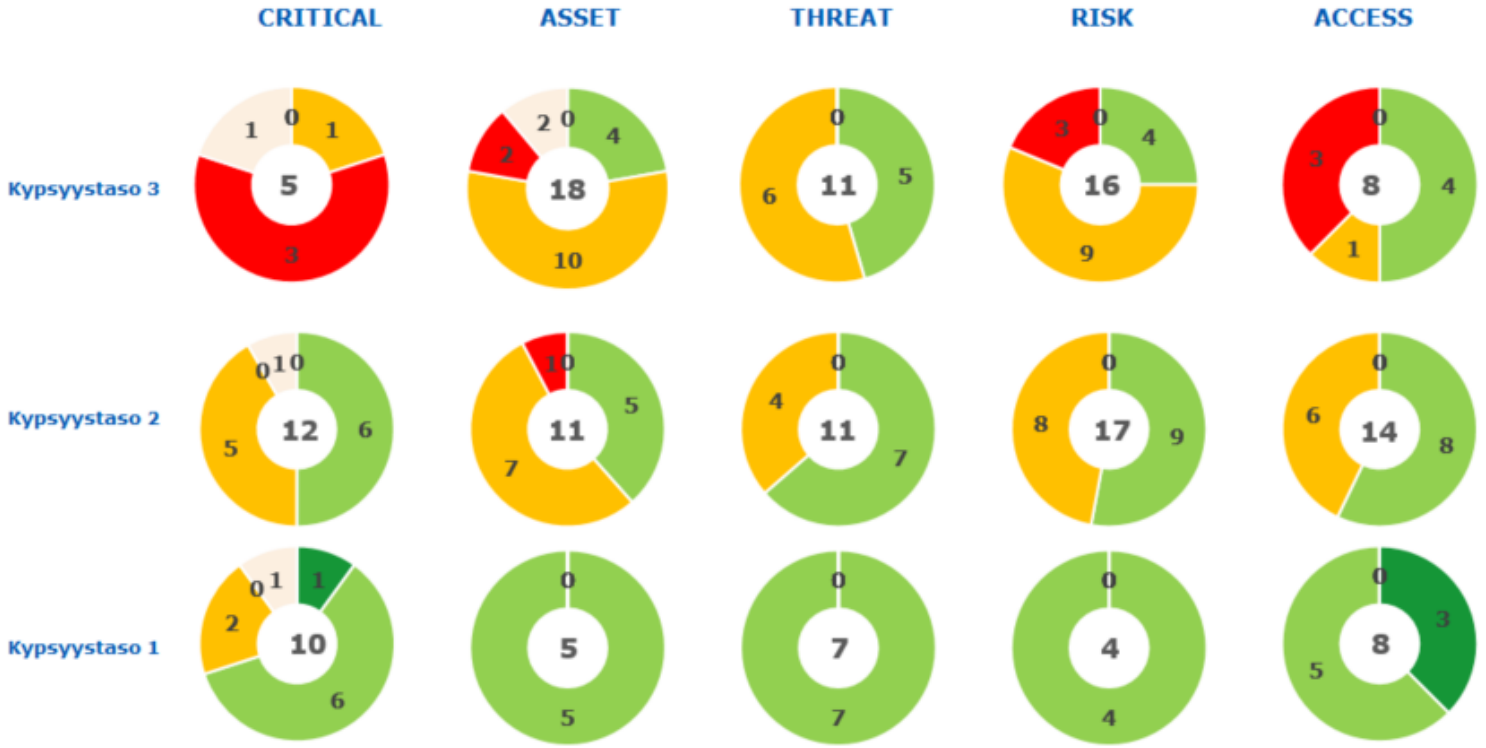

Osion käytäntöjen toteutuminen kypsyystasoittain (%)
CRITICAL Kriittiset palvelut
ASSET Omaisuuden hallinta
THREAT Uhkat ja haavoittuvuudet
RISK Riskien hallinta
ACCESS Pääsyn hallinta
SITUATION Tilanne kuva
RESPONSE Tapahtumat ja häiriöt
THIRDPARTY Kolmannet osapuolet
WORKFORCE Henkilöstön hallinta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

R8

KYBERMITTARI

Osiokohtainen kypsyystasoraportti

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



TRAFICOM

Käytettävyys

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Muutoksia

- Lisätty ohjeistusta ja vinkkejä välilehdille
- Lisätty tietokenttiä palautteen perusteella
  - Toimialoihin enemmän valintoja - pohjautuu toimialaluokitukseen
  - MUUTOKSET-välilehti organisaation sisäiseen käyttöön
  - Käytäntöjen kohdalle uusia sarakkeita vastausten dokumentointia varten
- XML-export tulosten viennissä poistettu, jotta työstäminen mahdollista myös O365-ympäristössä

Import - Export

- Import-Export toiminnallisuuden parannukset
  - Edelliset tulokset tai muuta tietoa jokaiselle välilehdelle
  - Erillinen ohjeistus tulosten siirtämiselle / kopioinnille
- Migraatio ja Mapping välilehti
  - Lisätyökalut ja ohje version 1 ja version 2 välille
  - Migration-välilehden avulla siirretään vastaukset ja kommentit versioiden välillä
  - Mapping kertoo viittaukset ja arvion muutoksesta versioiden välillä

https://www.kybermittari.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus