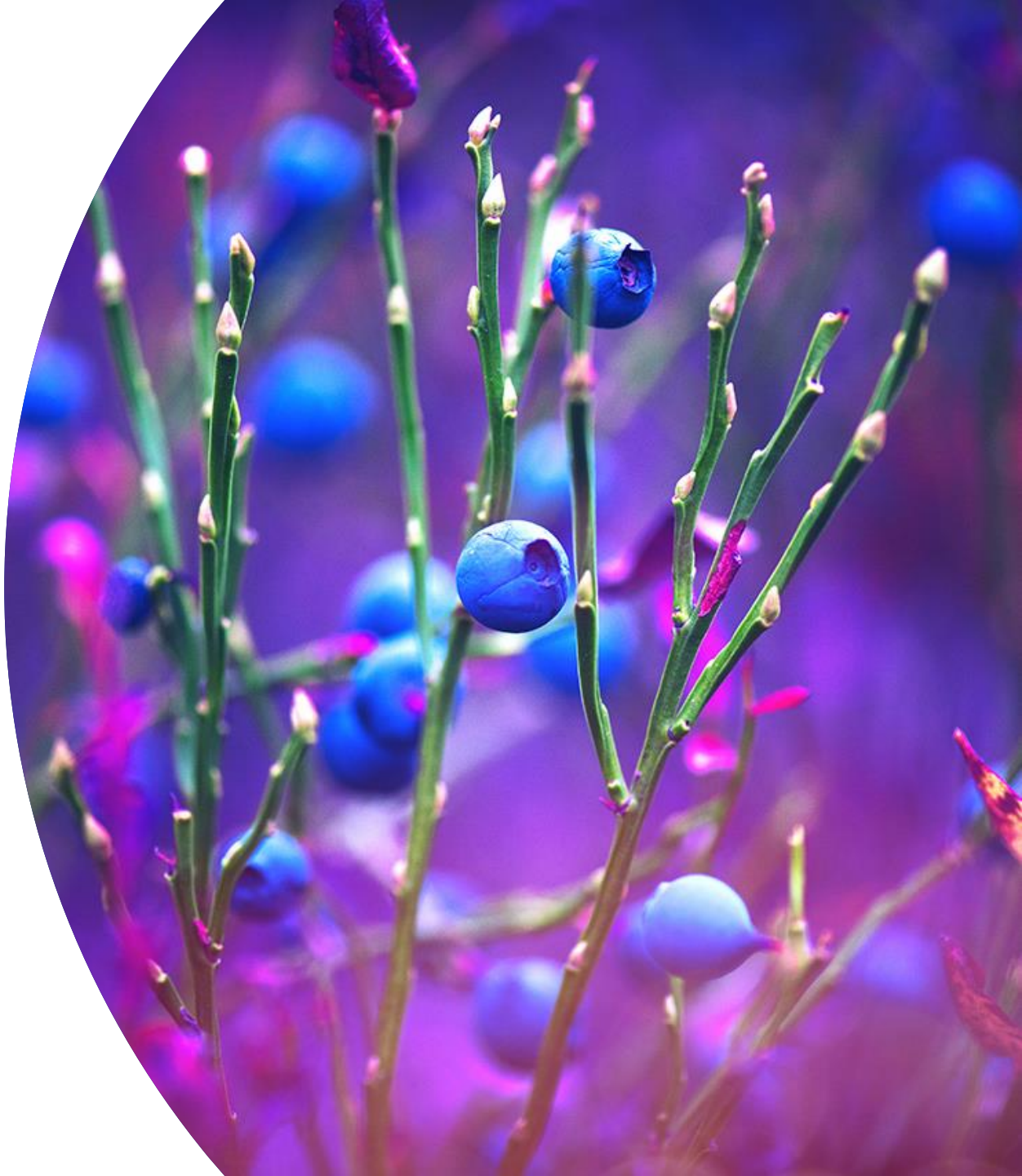
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari esittely palveluntarjoajille

11.04.2024



Agenda

- Kybermittari
  - Kybermittarin tavoitteet
  - Luottamusverkosto
  - Kybermittari 2024-
- Palveluntarjoajapaketti
  - Kybermittarin ja sen materiaalien käyttö
  - Viestintä- ja markkinointiyhteistyö
  - Tukea Kybermittarin käyttöön ja kehitykseen
- Kysymyksiä ja avointa keskustelua

Kyberturvallisuus on...

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

- Lähde: Kyberturvallisuuden sanasto, Turvallisuuskomitea

Kyberturvallisuuskeskus –tammikuun kybersää

”Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista”.

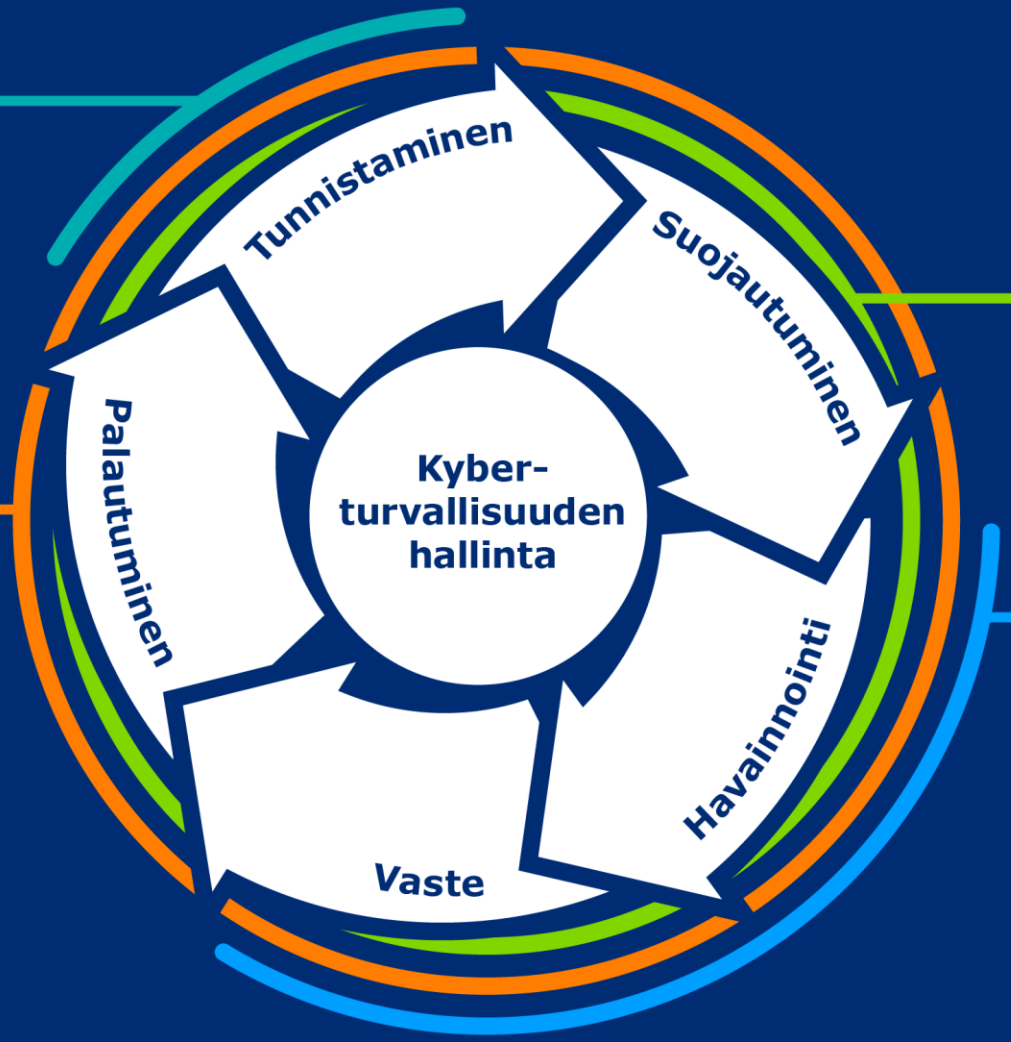
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Tärkein tietoturvateko on tiedostaa, mikä on yrityksen nykyinen tietoturvallisuuden taso. Mitä tulisi kehittää? Tämän jälkeen pitäisi myös viedä läpi tarvittavat kehitystoimet.

TRAFICOM

HYÖKY
Kansallinen hyökkäyspinnan kartoitus

HARJOITUS-TOIMINTA



KYBER-MITTARI

HAVARO
Vakavien tietoturvauhkien kansallinen havainnointipalvelu

Riskienhallinnan palvelut organisaatioille

Kybermittari

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

Organisaation tietoturvaohjelma

- Organisaatiossa tulisi hyödyntää erilaisia kyberturvallisuuden viitekehyksiä
  - Riskienhallinta
  - Tietoturvallisuuden hallinta
  - Tietoturvakontrollit
  - Liiketoiminta-arkkitehtuuri
- Kypsyysmalli auttaa seuraamaan ja todentamaan organisaation tietoturvaohjelman etenemistä ja asetettujen tavoitteiden saavuttamista
  - Tässä mm. Kybermittari voi auttaa

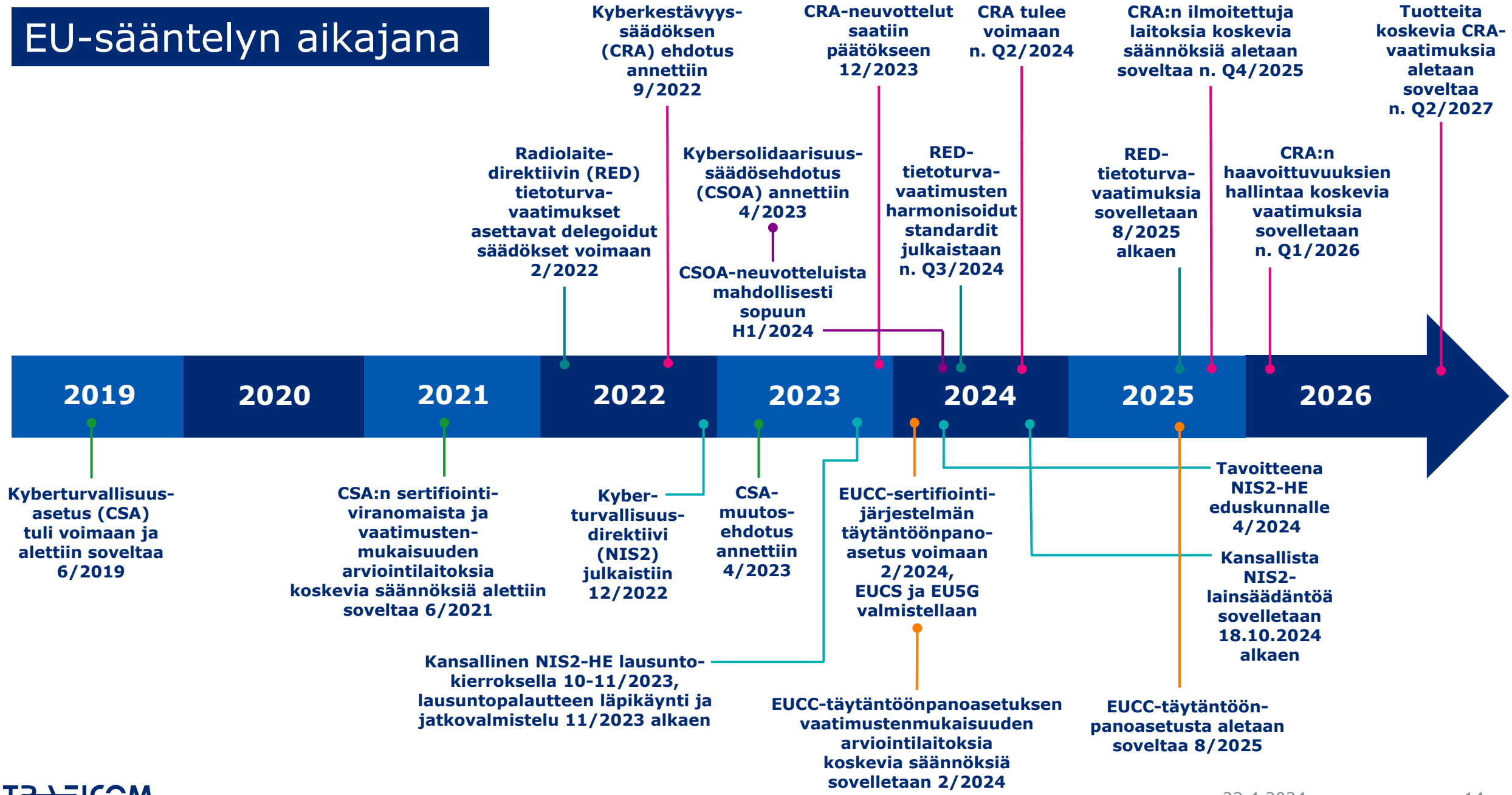
Ilmainen Kybermittari sisältää hyviä käytäntöjä riskien hallintakeinoiksi

- **Kybermittari** on organisaatioiden johdolle ja tietoturva-ammattilaisille suunnattu **ilmainen** palvelu kyberturvallisuuden hallintaan.
- Arviointityökalun avulla organisaatio **mittaa kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla**. Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat **kehitysalueet**.
- Organisaatio voi halutessaan jakaa mittaustuloksensa Kyberturvallisuuskeskukselle, joka anonymisoi tulokset ja tarjoaa organisaatiolle niiden pohjalta tuotettua **toimialan vertailutietoa ja suosituksia**.
- Tutustu kybermittariin: www.kybermittari.fi
- Ota yhteyttä: kybermittari@traficom.fi

Sääntelystä ja suosituksista

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

EU-sääntelyn aikajana



Tietoa

- NIS2 - Euroopan unionin kyberturvallisuusdirektiivi -sivusto
  - https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi
- Suositusluonnos NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä on lausuntokierroksella 5.4.-31.5.2024
  - https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4

Suositusten soveltamisesta

- Ei sido viranomaisia eikä toimijoita. Sitovat velvoitteet säädetään:
  - **Laeissa**,
  - Euroopan komission antamassa **tarkentavassa sääntelyssä** ja
  - toimialakohtaisen viranomaisen **määräyksissä**.
- Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää suosituksesta poikkeavia, tiukempia vaatimuksia.
  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.

Toteutusesimerkit

Todennus

Perustelut

Viitteet

Työkalut

11.12 Toiminta vakavissa poikkeamissa	
Toteutusesimerkit	• Toimijalla on olemassa käytännöt, joilla määritetään vastuut ja toimenpiteet erityisesti vakavia poikkeamia varten. • Toimijalla on olemassa käytännöt, joita se seuraa NIS-ilmoituksen tai muun viranomaisilmoituksen tekemiseen poikkeamissa.
Todennus	1. Valvova viranomainen todentaa, että toimijalla on kirjannut käytäntönsä poikkeamia varten. Näistä käy ilmi ilmoitusvelvollisuudet, sisäiset ja ulkoiset kontaktipisteet, vastuut ja velvollisuudet, mahdolliset hätätilanteiden käyttäjätunnukset sekä toimintaohjeet. 2. Siinä tapauksessa, että toimijalla on ollut poikkeamia, todennetaan poikkeamanhallinnan käytännöt esimerkiksi haastatteluin sekä poikkeamakäsittelyyn liittyvän dokumentaation avulla. Erityisesti tulee todentaa se, että poikkeamanhallinta on ollut riittävää, siinä on selvitetty poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi ja siinä on toteutettu lainsäädännölliset velvollisuudet, kuten poikkeamailmoitukset. Näitä voi todentaa esimerkiksi toimijan toimittamasta materiaalista, kuten poikkeaman loppuraportista.
Perustelut	Hyvin suunnitellut toimintatavat ja käytännöt poikkeamatilanteissa lyhentävät palautumisaikaa. Käytännöt ilmoitusvelvollisuuksien suhteen varmistavat sen, että lakisääteisten ilmoituksien, kuten NIS-ilmoituksen, tekeminen ei unohdu poikkeamatilanteessa.
Viitteet	Relevantit standardit ja viitekehykset: ISO27002-2022 (5.5, 5.24, 5.26) NIST CSF 1.1 (RS.RP, RC.RP, RC.CO-3) CCB CYFUN Basic (RS.RP-1, RC.RP-1, RC.CO-3) Julkri (HAL-08) IEC 62443-2-1 (4.3.4.5)
Työkalut	Kybermittari: RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-4

THL: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (20.2.2024)

- 6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset
- 6.1 Yleiset tietoturvakäytännöt
  - "Asiakastietolain 77 §:n 1 momentin kohdan 5 mukaan tietojärjestelmän käyttöympäristön on sovelluttava tietojärjestelmien asianmukaiseen ja tietoturvan sekä tietosuojan varmistavaan käyttöön. Käyttöympäristöön ja tietojärjestelmiin kohdistuvien riskien hallinnasta on huolehdittava. ISO/IEC 27000 -sarjan standardien mukainen tietoturvallisuuden hallintajärjestelmä on suositeltava esimerkki hyvästä käytännöstä etenkin isoille organisaatioille. Pienemmille palvelunantajille suositeltava menettely on esimerkiksi Traficomin Kyberturvallisuuskeskuksen **Kybermittarilla tehtävä itsearviointi**."

Suositus kyberturvallisuuden edistämisestä raideliikenteessä (30.01.2023)

- 4. Suositukset raideliikenteen kyberturvallisuuden kehittämiseksi
  - Kaikkien raideliikennejärjestelmän toimijoiden suositellaan arvioivan ja mittaavan organisaationsa kyberturvallisuuden tasoa. Olemassa olevien hallinnollisten IT-järjestelmien osalta ensisijaisesti suositellaan käytettävän ISO/IEC 27001:20228 kyberturvallisuuden hallintajärjestelmästandardia. ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmällä on mahdollista hallinnoida myös OT-ympäristöä, jossa lisäksi sovelletaan edellä mainittuja OT-ympäristöön soveltuvia standardeja. Muu vaihtoehtoinen viitekehys voi olla esimerkiksi Kyberturvallisuuskeskuksen ylläpitämä, ilmainen ja suomenkielinen Kybermittari.

1 Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

Taso	Käytäntö	Vastaus	ommentäinen viitt	Ulkoinen viittaus
1a	Organisaation tuottamat yhteiskunnalle kriittiset palvelut on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu		Traficom suositus 4.2.1
1b	(Yhteiskunnalle kriittisten) palveluiden tuottamiseen tarvittava data on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu		Traficom suositus 4.2.2

https://www.traficom.fi/fi/saadokset/suositus-kyberturvallisuuden-edistamisesta-raideliikenteessa

Kybermittari

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari 2024->
Pääteemat

- Tietoisuus Kybermittarista
- Kybermittarin käyttöönoton edistäminen
- Vertailutieto ja verkostot
- Kehitys ja tuki

Kybermittari: tilastollista analyysiä

Mittaria itsearviointiin käyttäneiden organisaatioiden tulosten perusteella seuraavissa osioissa ja niiden tavoitteissa oli eniten käytäntöjä, jotka olivat vain **osittain toteutettu**. Näistä muodostuu todennäköisesti organisaatioiden **kehityskohteita**:

- Kriittisten palvelujen suojaaminen
  - Kybertapahtumien ja –häiriöiden hallinta, vaikutusten minimointi sekä kuinka henkilöstö on sisäistänyt suunnitelmat
- Kumppaniverkoston riskien hallinta
- Omaisuuden, muutosten ja konfiguraation hallinta
  - Laitteiden ja ohjelmistojen hallinta, muutosten hallinta, tietovarantojen hallinta
- Kyberturvallisuusarkkitehtuuri
  - Kyberarkkitehtuuri ja sen kehittäminen
  - Tietojen suojaus osana kyberarkkitehtuuria
- Uhkien ja haavoittuvuuksien hallinta
  - Uhkien torjunta ja uhkatiedon jakaminen
- Tilannekuva
  - Ympäristöjen valvonta ja lokitus

Kybermittari palveluntarjoajille

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittarin käytön ehdot

- Cybersecurity Capability Maturity Model (C2M2) ehdot:

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

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

- Kybermittarin ehdot:

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

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

- *Nimeä - Sinun on mainittava lähde asianmukaisesti, tarjottava linkki lisenssiin sekä merkittävä, mikäli olet tehnyt muutoksia. Voit tehdä yllä olevan millä tahansa kohtuullisella tavalla, mutta et siten, että annat ymmärtää lisenssinantajan suosittelevan sinua tai teoksen käyttöäsi.*
- *Ei muita rajoituksia - Et voi asettaa sellaisia oikeudellisia ehtoja tai teknisiä estoja, jotka estävät oikeudellisesti muita tekemästä mitään sellaista, minkä lisenssi sallii*

Kybermittari palveluntarjoajille

- Palveluntarjoajilla on keskeinen rooli Kybermittarin käytössä ja organisaatioiden kyberturvallisuuden edistämisessä

- Kyberturvallisuuskeskus haluaa tehdä yhteistyötä palveluntarjoajien kanssa
  - Tarjoamalla Kybermittarin ja sen materiaalit **vapaasti käytettäväksi, soveltuvin ehdoin**
  - **Viestintäyhteistyötä**
  - **Rajattua tuotetukea** kipukohtien ratkaisemiseksi
  - **Yhteistyötä ja vaikuttamismahdollisuuksia Kybermittarin kehitykseen**

Viestintä- ja markkinointiyhteistyötä

- Kyberturvallisuuskeskus kannustaa organisaatioita palveluntarjoajan käyttöön, mikäli organisaatiot kaipaavat laajaa tukea mittarin läpiviemiseen.
- Kyberturvallisuuskeskus listaa Kybermittari-verkkosivulla yrityksiä, jotka tarjoavat Kybermittariin pohjautuvia arviointi- ja kehityspalveluja
- Palveluntarjoajien on mahdollista päästä listalle ja käyttää Kybermittari-sanaa markkinoinnissa sitoutumalla Kybermittarin markkinointiehtoihin ja palvelunkuvaukseen, joissa määritellään mm.
  - Miltä osin Kybermittarin käytännöt tulee toteutua ja miten muokkaukset alkuperäiseen on dokumentoitu asiakkaalle
  - Miten vertailutietoa pitää pystyä vaihtamaan

Kybermittariin pohjautuvia arviointi- tai kehittämispalveluita tarjoavat yritykset ^

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen –logo, käyttöohje

- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen logoa voi käyttää Kybermittariin liittyvää palvelua esittävällä sivulla. Logon käyttöön on seuraavat graafiset ohjeet:
  - Pääsääntöisesti tunnuksesta käytetään tummansinistä versiota. Jos tämä ei ole mahdollista, tunnusta käytetään mustana. Tummalla tai värillisellä pohjalla tunnusta käytetään aina valkoisena. Muissa väreissä tunnusta ei saa käyttää.
  - Tunnukselle on selkeän erottumisen takaamiseksi määritelty suoja-alue, joka on vähintään puolet tunnuksen t-kirjaimen korkeudesta. Tälle alueelle ei saa sijoittaa muita elementtejä.
  - KTK logo löytyy linkistä: https://www.kyberturvallisuuskeskus.fi/dist/node/svg/00e263c841093e736a4c668932ffa9a9.svg
  - Tiedustele tarvittaessa lisäohjeita tai muita versioita logosta.

Palveluntarjoajan käytössä

- *www.kybermittari.fi*
  - *Työkalu ja tukimateriaali*
  - *Tulkintaohje (C2M2, eng)*
  - *Tiedonjako-ohje*
  - *Käyttöehdot*
  - *Kybermittari V1 vs V2 vs 2.1*
  - *Esimerkkitäyttö numeroin*
  - *Versiomuunnostyökalut*
  - *Tiedon tuonnin työkalut*
  - *Jne.*
- *Markkinointiehdot*
- *Palvelukuvaus*
- *NIS2 ja Kybermittari*
- *Pyydettäessä:*
  - *Logot (myös erillinen ohje sivuilla)*
  - *Viestinnän tuki*

Kyberturvallisuuskeskuksen rooli kansallisena luottamuspisteenä

Puolueeton kumppani

Viranomaisrooli mittarin käytön tukemissa ja edistämisessä

- Kyberturvallisuuskeskus tarjoaa mittarin vapaasti käytettäväksi
- Edistää mittarin käyttöönottoa ja käyttöä verkostojensa kautta
- Tarjoaa neuvoja ja suosituksia
- Ylläpitää ja kehittää mittaria

Kansallinen luottamuspiste

Mittaustulosten koonti, säilytys ja anonymisointi

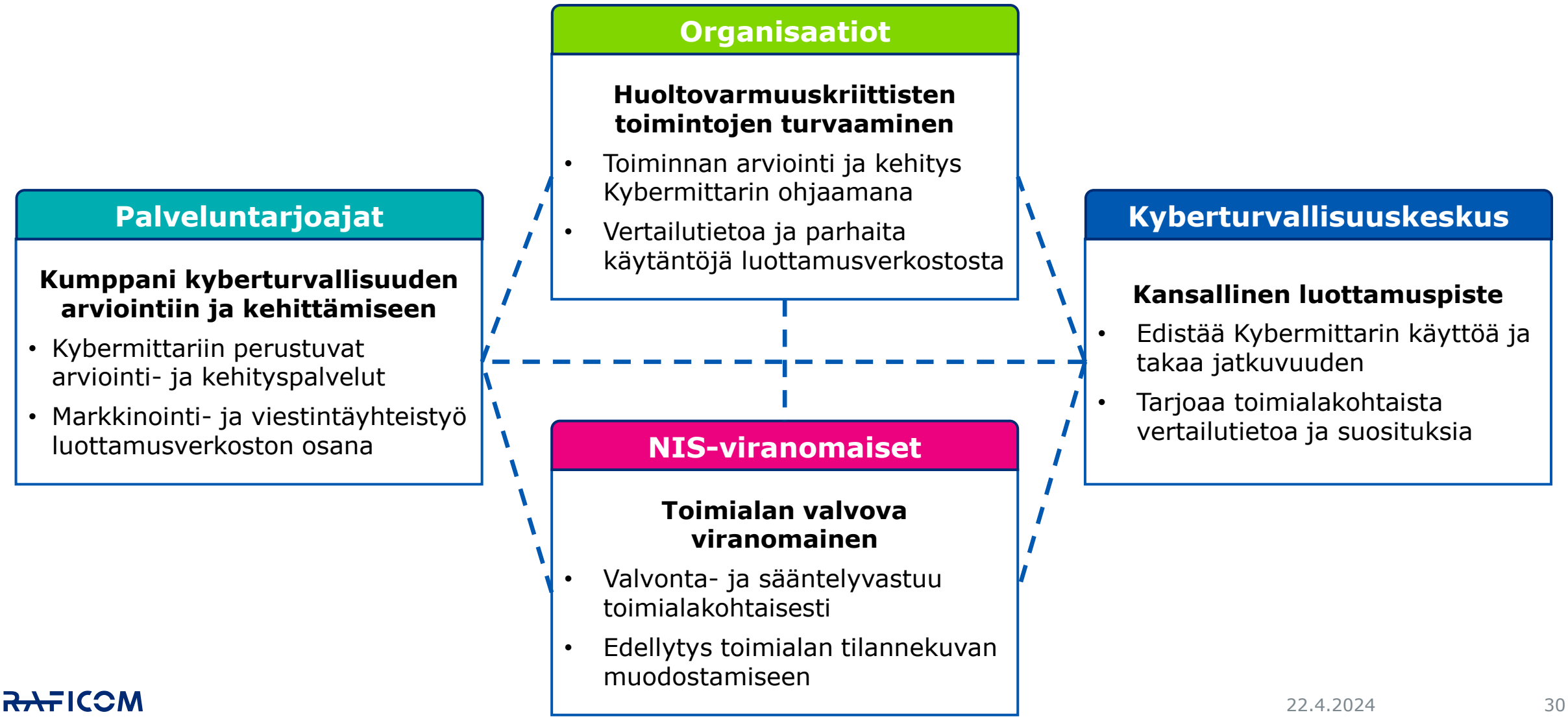
- Kyberturvallisuuskeskus kerää organisaatioilta mittaustuloksia
- Luottamuksellinen tiedonkäsittely ja tulosten anonymisointi
- Pohjana vertailutiedolle ja KTK:n tarjoamille suositustasoille

Anonyymi vertailutieto

Toimialakohtaisen vertailutiedon tarjoaminen

- Kyberturvallisuuskeskus tuottaa mittaustuloksista anonymisoitua toimialakohtaista vertailutietoa
- Lisäksi tuloksiin pohjautuvia suositustasoja ja ohjeistusta
- Jakelu suoraan osallistuville asiakasorganisaatioille

Kybermittarin luottamusverkosto



Vertailutieto ja suositukset, tarkemmin

- Kyberturvallisuuskeskus tuottaa Kybermittarin käytön tueksi vertailutietoa ja suosituksia
- Tulokset kerätään yksittäisiltä organisaatioilta ja niitä analysoidaan sekä tuotetaan mm. vertailutietoa, josta yksittäisten organisaatioiden tulokset eivät ole tunnistettavissa. (6-10)
- Tiedonvaihto tapahtuu luottamuksellisesti suoraan asiakasorganisaation ja Kyberturvallisuuskeskuksen välillä.
  - Palveluntarjoaja voi sopia asiakkaansa kanssa erikseen tulosten käsittelystä ja tulosten hyödyntämisestä
- Kyberturvallisuuskeskus ei luovuta osallistuvien organisaatioiden nimiä eikä arviointituloksia kolmansille osapuolille

KYBERMITTARI

Vertailutietotalkoot

1 Arvioi ja tallenna

2 Jaa tieto Traficomille
lomakkeella tai turvapostilla

3 Hyödynnä vertailutietoa

Kyberturvallisuuskeskus

- **kokoaa ja anonymisoi** eri organisaatioiden tulokset
- tuottaa ja **jakaa vertailu-tietoa** kansallisiin tarpeisiin

YRITYKSET JA ORGANISAATIOT

Mitattu tieto kehittämisen ja päätöksenteon tueksi

- Vertailu alan yleiseen tasoon
- Henkilöstön osaaminen
- Tukea johtamiseen
- Kehityskohteiden tunnistaminen
- Tavoitetason asettaminen
- Investointien kohdentaminen

VERKOSTOT JA SIDOSRYHMÄT

Yhteistyö ja tiedonjako

KYBERTURVALLISUUSKESKUS

Kansallinen tilannekuva

Ohje tulosten jakamiseen

Organisaation tulokset

- Täytä arviointi ja tallenna tulokset.
- Voit käyttää jakamiseen esimerkiksi .csv muotoa (työkalun välilehti Export_KTK)

Tulosten lähettäminen

- Voit käyttää tulosten lähettämiseen Kybermittari-sivuston **yhteydenottolomaketta**, omaa turvapostia tai lähetä viestin, jossa yhteystietosi (nimi ja puhelinnumero*) osoitteeseen kybermittari@traficom.fi niin saat ohjeet Traficomin turvapostin käyttöönottoon.

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.

Käyttökohteita

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Esimerkki Kybermittarin arviointiprosessista

Perustuen Kyberturvallisuuskeskuksen 2020-22 toteuttamiin pilottiarvointeihin

ITSEARVIOINTI	HAASTATTELU	TULOSTEN RAPORTOINTI

Organisaatio

Vastuuhenkilöiden nimeäminen	Vastausten täydentäminen	½ päivän työpaja	Raportointi johdolle

Arvioinnin fasilitoija

Valmistelu	Tuki, tarvittaessa	½ päivän työpaja	Loppuraportti

Esimerkki rooleista ja vastuista

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

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

Esimerkki kuvaavasta tekstistä (ASSET-2g)

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

The inventory of information assets should be updated and maintained as assets change throughout their lifecycle to ensure the inventory is complete and accurate. Ensuring that the information asset inventory is current might involve change management procedures that require inventory updates any time assets are significantly altered. The organization might also conduct inventory reviews, both periodically (such as quarterly or yearly) and based on events (such as changes in organizational structure, major changes in critical systems, and the acquisition and consolidation of another business).

Related Practices

· *Progression*: This practice is part of a practice progression. Practice progressions are groups of related practices that represent increasingly complete or more advanced implementations of an activity. The practices in this progression include: ASSET-2a, ASSET-2b, ASSET-2f, ASSET-2g.

Raideliikenteen suosituksen liite

1 Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

Taso		Käytäntö	Vastaus	ommentäinen viitt		Ulkoinen viittaus
1	1a	Organisaation tuottamat yhteiskunnalle kriittiset palvelut on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu			Traficom suositus 4.2.1
	1b	(Yhteiskunnalle kriittisten) palveluiden tuottamiseen tarvittava data on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu			Traficom suositus 4.2.2
	1c	Palveluiden tuottamiseen tarvittavat prosessit on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu			Traficom suositus 4.2.3
	1d	Palveluiden tuottamiseen tarvittavat järjestelmät (IT- ja OT-omaisuus) on tunnistettu ja dokumentoitu.	4 - Täysin toteutettu			Traficom suositus 4.2.4

https://www.traficom.fi/fi/saadokset/suositus-kyberturvallisuuden-edistamisesta-raideliikenteessa

NIS2-direktiivi	NIS2-direktiivin suomennos	Kybermittari osiot	Kybermittari tavoitteet, (es
(e) | security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	e) | verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;	**ASSET** **THREAT** **THIRD-PARTIES** **ARCHITECTURE**	**ASSET-1** **ASSET-2** **ASSET-3** **ASSET-4** **THREAT-1** **THIRD-PARTIES-2** **ARCHITECTURE-2**
(f) | policies and procedures to assess the effectiveness of cybersecurity risk-	f) | toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden		**RISK-4** **Yleisiä Hallintatoimia-f**
(g) | basic cyber hygiene practices and cybersecurity training;	g) | perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;	**WORKFORCE**	**WORKFORCE-4**
(h) | policies and procedures regarding the use of cryptography and, where	h) | toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;	**ASSET** **ARCHITECTURE**	**(ASSET-2)** **ARCHITECTURE-5**
(i) | human resources security, access control policies and asset management;	i) | henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;	**WORKFORCE** **ACCESS** **ASSET** **ARCHITECTURE**	**WORKFORCE-3** **ASSET-1** **ASSET-2** **ARCHITECTURE-3**
(j) | the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and	j) | tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.	**ACCESS** **RESPONSE** **ARCHITECTURE** **SITUATION**	**ACCESS-1** **RESPONSE-3** **ARCHITECTURE-5** **SITUATION-3**

TLP:AMBER

TRAFICOM

NIS2 Art21 (2) i) omaisuudenhallinta; (ASSET-1-2)

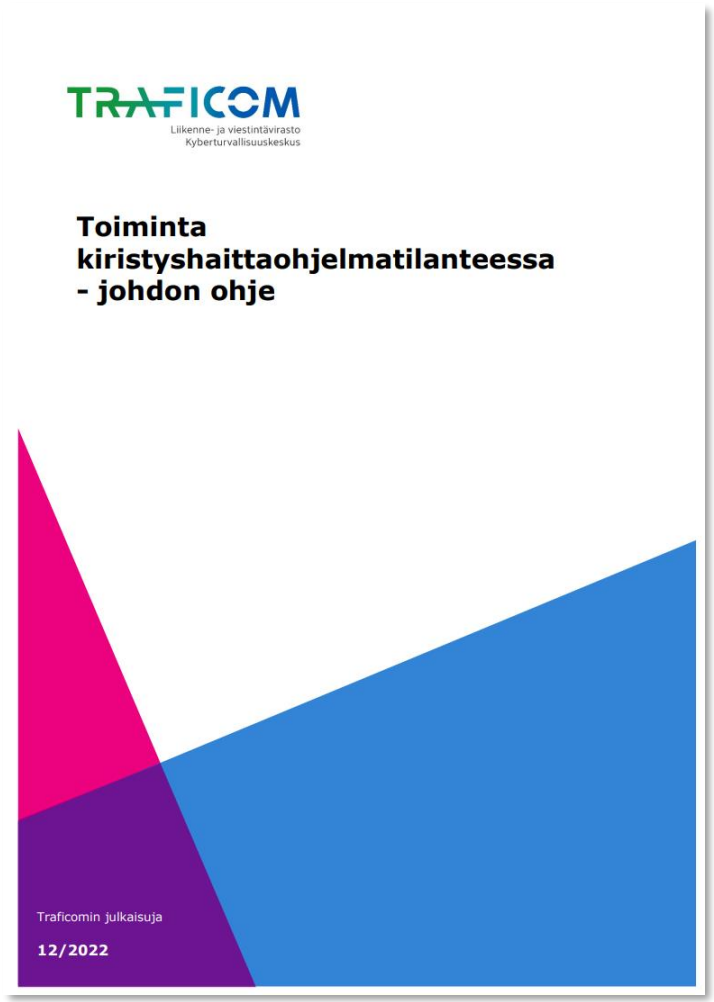
(i) | human resources security, access control policies and asset management;	i) | henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;	**WORKFORCE** **ACCESS** **ASSET** **ARCHITECTURE**	**WORKFORCE-3** **ASSET-1** **ASSET-2** **ARCHITECTURE-3**

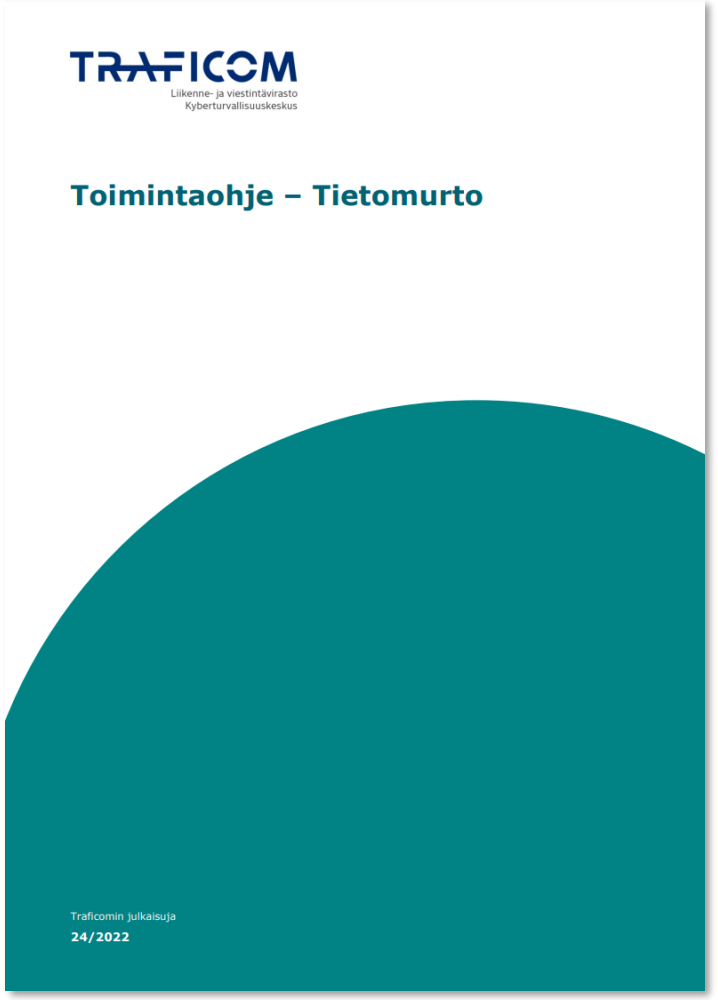
ISO27002 NIST CSF IEC62443

Kybermittari / C2M2

Asset inventory	5.9	ID.AM-1,2,3,4,5 PR.IP-1	IEC 62443-2-1:2010 4.2.3.4 IEC 62443-3-3:2013 SR 7.8	ARCHITECTURE-1c, ARCHITECTURE-3b, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3e, ARCHITECTURE-4c, ASSET-1a, ASSET-1b, ASSET-1c, ASSET-1d, ASSET-1f, ASSET-1g, ASSET-2a, ASSET-2b, ASSET-2c, ASSET-2d, ASSET-2f, ASSET-3a, ASSET-3c, ASSET-3d, SITUATION-3g, THIRD-PARTIES-1d

Response-3: Tapahtumiin ja häiriöihin reagoiminen



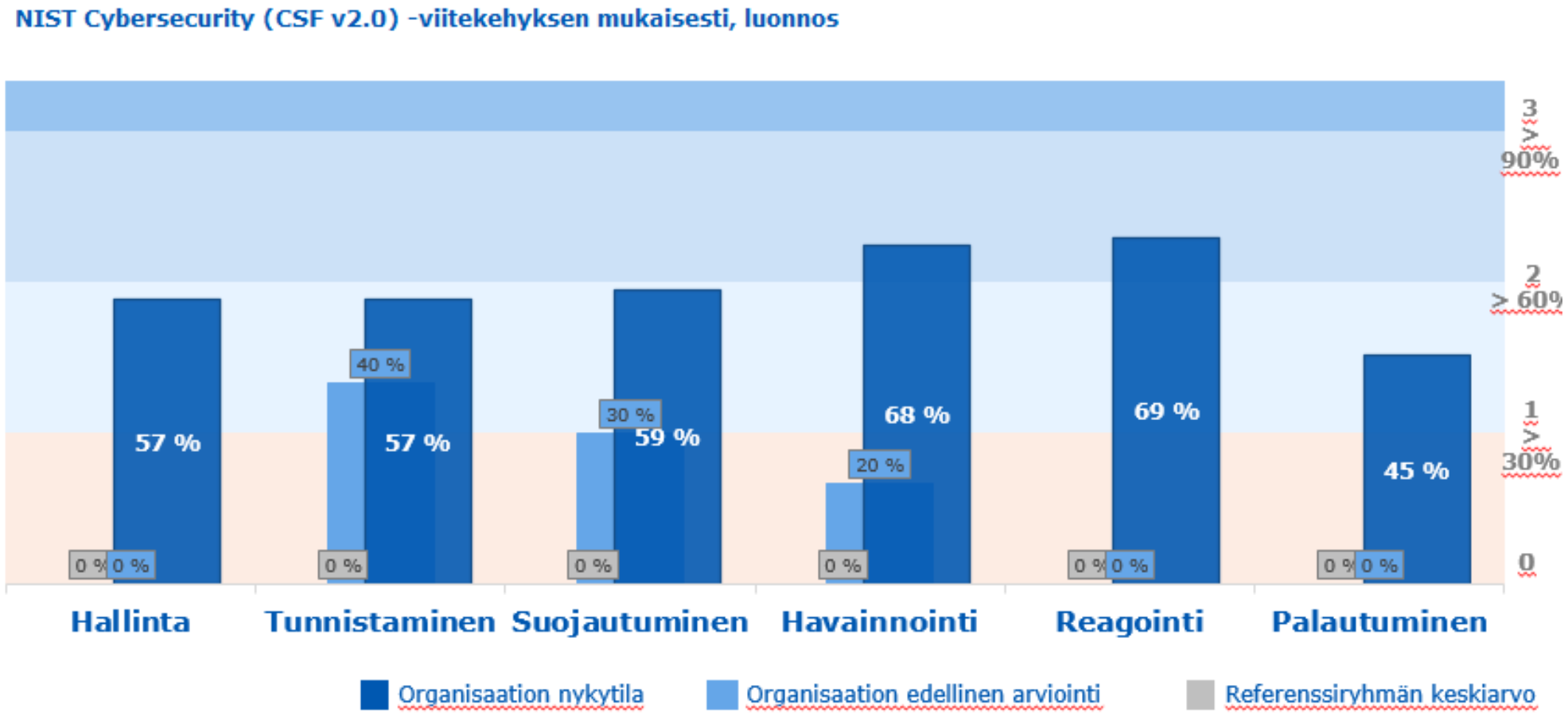


https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

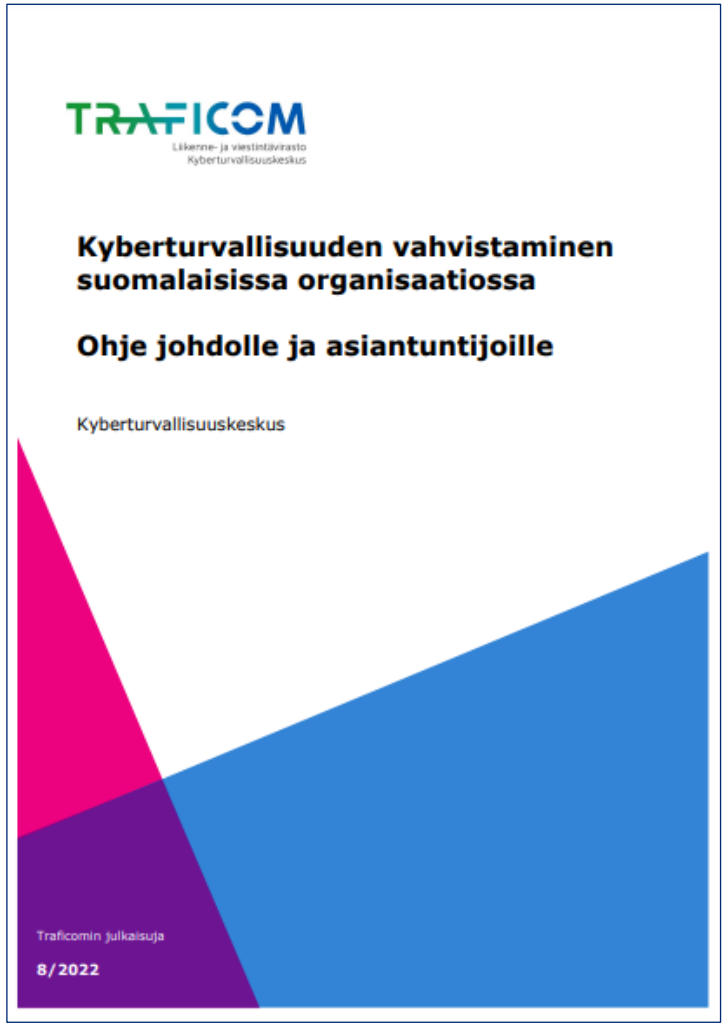
Tulevaisuus

NIST CSF 2.0


NIST Cybersecurity (CSF v2.0) -viitekehyksen mukaisesti, luonnos
3
> 90%
2
> 60%
1
> 30%
0
0 %
0 %
57 %
40 %
0 %
57 %
30 %
0 %
59 %
20 %
0 %
68 %
0 %
0 %
69 %
0 %
0 %
45 %
Hallinta
Tunnistaminen
Suojautuminen
Havainnointi
Reagointi
Palautuminen
Organisaation nykytila
Organisaation edellinen arviointi
Referenssiryhmän keskiarvo

”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).



https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille

Pohdittavaa: Asiakastarve ja tarjonta

- Paljon erilaisia asiakastarpeita
  - Eri toimialat, kypsyystasot, riskiprofiilit, uhkaympäristöt
- Useita toimijoita
  - Organisaatiot, palveluntarjoajat, viranomaiset, valtionhallinto, HVK
- Useita viitekehyksiä ja standardeja
  - NIST CSF 2.0 julkaistu
- Uutta lainsäädäntöä ja toimialakohtaisia vaatimuksia
  - NIS2, CER, CSA, NCCS, jne.
  - EU:n ja Enisan rooli

Kyberriskien 10 lakia

Onnistuminen tietoturvassa syö hyökkääjän voittoja
Täydellistä tietoturvaa on mahdoton saavuttaa, joten vaikeuta hyökkääjän toimintaa ja lisää heidän kustannuksiaan ja vähennän oman suojattavan omaisuuden kiinnostavuutta.

Kyberturvallisuus on joukkuepeli
Kukaan ei pysty tekemään kaikkea yksin. Keskity niihin tehtäviin, jotka juuri sinä voit tehdä suojataksesi organisaation tehtäviä ja anna muiden tehdä muut tehtävät.

Jos et pidä yllä, jäät jälkeen
Kyberturvallisuus on jatkuva prosessi ja kokoajan tulee liikkua eteenpäin. Hyökkäysten toteuttaminen käy koko ajan hyökkääjille edullisemmaksi.

Verkkosi ei ole niin turvallinen kuin luulet
Turvallisuusstrategia, joka nojaa luottamukseen on helposti hyökkääjien murrettavissa. Noudata organisaatiossa nollaluottamusajattelua.

Tuottavuus voittaa aina
Jos tietoturva ei ole helppoa käyttäjille, he keksivät tavan ohittaa sen. Muista aina käytettävyys turvallisuuden ohella.

Eristetyt verkot eivät ole automaattisesti turvallisia
Kunnolla eristetyt verkot voivat oikein hallittuina tarjota korkeaa tietoturvaa, mutta usein verkko ei ole täysin eristetty ulkoisilta riskeiltä.

Hyökkääjät eivät välitä
Hyökkääjät käyttävät mitä tahansa saatavilla olevia menetelmiä päästääkseen organisaatiosi ympäristöön ja tietoihin.

Salaus yksinään ei ole tiedon suojauksen ratkaisu
Salaus suojaa tietyn tyyppisiltä hyökkäyksiltä, mutta data on vain niin turvassa kuin salausavain ja muut pääsynhallinnan käytännöt sitä suojaavat.

Ankara priorisointi on selviytymiskeino
Kenelläkään ei ole riittävästi aikaa ja resursseja päästäkseen eroon kaikista riskeistä, joten aloita aina siitä, mikä organisaatiollesi on tärkeintä (”kruununjalokivet”).

Teknologia ei ratkaise ihmis- ja prosessiongelmia
Edistyneet teknologiat, kuten tekoäly ja koneoppiminen tarjoavat suuria harppauksia eteenpäin, kyberturvallisuus on yhteiskunnallinen ja ihmisiin liittyvä haaste.

Lisätietoa

Kybermittari.fi –sivusto

- **Kybermittarin työkalut ja tuki**
- **Tapahtumat**
- **Ohjeet vertailutiedon jakamiseen.**
- **Mahdollisuudet osallistua kehitykseen**
- **Palveluntarjoajat**, jotka ovat ilmoittaneet tarjoavansa tukipalveluita Kybermittarin käyttöön
- **Yhteystiedot ja palautekanavat**
  - **Kybermittari.fi**

TRAFICOM

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

kybermittari@traficom.fi