EUROPEAN UNION AGENCY
FOR CYBERSECURITY

KANSALLISTEN VALMIUKSIEN ARVIOINTIKEHYS

JOULUKUU 2020

TIETOA ENISASTA

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka tarkoituksena on saavuttaa yhteinen korkea kyberturvataso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa sekä auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. Virasto jakaa tietoa, kehittää valmiuksia ja parantaa tietämystä sekä tekee yhteistyötä keskeisten sidosryhmiensä kanssa lujittaakseen luottamusta verkottuneeseen talouteen, parantaakseen unionin infrastruktuurin sietokykyä ja ennen kaikkea suojatakseen Euroopan yhteiskunnan ja kansalaisten digitaalista turvallisuutta. Lisätietoja virastosta on osoitteessa www.enisa.europa.eu.

OTA YHTEYTTÄ

Ota yhteyttä tekijöihin sähköpostilla team@enisa.europa.eu.
Tätä asiakirjaa koskevat tiedotusvälineiden tiedustelut sähköpostilla press@enisa.europa.eu.

TEKIJÄT

Anna Sarri, Pinelopi Kyranoudi – Euroopan unionin kyberturvallisuusvirasto (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

KIITOKSET

ENISA haluaa kiittää kaikkia asiantuntijoita, jotka ovat osallistuneet tämän raportin laatimiseen, ja erityisesti seuraavia henkilöitä (aakkosjärjestyksessä):

Central State Office for the Development of the Digital Society [digitaaliyhteiskunnan kehittämisestä vastaava valtion keskusvirasto](Kroatia), Marin Ante Pivcevic

Centre for Cyber Security [kyberturvallisuuskeskus] (Belgia)

CFCS – Center for Cybersikkerhed [kyberturvallisuuskeskus] (Tanska), Thomas Wulff

Euroopan kyberrikostorjuntakeskus – EC3, Alzofra Martinez Alvaro

Euroopan kyberrikostorjuntakeskus – EC3, Adrian-Ionut Bobeica

Liittovaltion sisäministeriö (Saksa), Sascha-Alexander Lettgen

Information Security Administration [tietoturvavirasto] (Slovenia), Marjan Kavčič

Italian hallitus (Italia)

Malta Information Technology Agency [Maltan tietotekniikkavirasto] (Malta), Katia Bonello ja Martin Camilleri

Oikeudesta ja yleisestä turvallisuudesta vastaava ministeriö (Norja), Robin Bakke

Digitaalipolitiikasta vastaava ministeriö (Kreikka), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali ja Sotiris Vasilos

Talous- ja viestintäministeriö (Viro), Anna-Liisa Pärnalaas

National Cyber and Information Security Agency [kansallinen kyber- ja tietoturvallisuusvirasto] (Tšekki), Veronika Netolická

National Security Authority [kansallinen turvallisuusvirasto] (Slovakia)

National Security Department [kansallinen turvallisuusosasto] (Espanja), Maria Mar Lopez Gil

NCTV, oikeus- ja turvallisuusministeriö (Alankomaat)

Portuguese National Cybersecurity Centre [Portugalin kansallinen kyberturvallisuuskeskus] (Portugali), Alexandre Leite ja Pedro Matos

Cyber Security Policy Division [kyberturvallisuuspolitiikasta vastaava osasto], ympäristö-, ilmasto- ja viestintäministeriö (Irlanti), James Caffrey

University of Oxford – Global Cyber Security Capacity Centre [Oxfordin yliopisto – maailmanlaajuinen kyberturvallisuusvalmiuskeskus], Carolin Weisser Harris

ENISA haluaa myös kiittää arvokkaasta panoksesta tähän tutkimukseen kaikkia niitä tutkimukseen osallistuneita asiantuntijoita, jotka haluavat pysyä nimettöminä.

OIKEUDELLISET HUOMAUTUKSET

On huomattava, että tämä julkaisu edustaa ENISAn mielipiteitä ja tulkintoja, ellei toisin mainita. Julkaisua ei tule pitää ENISAn tai ENISAn elinten oikeudellisena toimena ilman asetukseen (EU) N:o 2019/881 perustuvaa hyväksyntää.
Julkaisu ei välttämättä ole aivan ajantasainen, ja ENISA voi päivittää sitä ajoittain.

Kolmannen osapuolen lähteitä lainataan asianmukaisesti. ENISA ei ole vastuussa ulkoisten lähteiden, kuten tässä julkaisussa viitattujen ulkoisen verkkosivujen, sisällöstä.

Tämä julkaisu on tarkoitettu vain tiedoksi. Sen on oltava käytettävissä veloituksetta. ENISA ja sen nimissä toimivat henkilöt eivät ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

TEKIJÄNOIKEUSILMOITUS

ISBN: 978-92-9204-481-7

DOI: 10.2824/845928

LUETTELO: TP-02-21-253-FI-N

1. SISÄLLYSLUETTELO

SANASTO

KIRJAINLYHENNE	MÄÄRITELMÄ
AI	Tekoäly
C2M2	Kyberturvallisuusvalmiuksien kypsyysmalli
CCRA	Common criteria -sertifikaattien tunnustamisjärjestely
CCSMM	Yhteisön kyberturvallisuuden kypsyysmalli
CII	Kriittinen tietoinfrastruktuuri
CMM	Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (Cybersecurity Capacity Maturity Model for Nations)
CMMC	Kyberturvallisuuden kypsyysmallin sertifiointi (Cybersecurity Maturity Model Certification)
CPI	Kybertehoindeksi (Cyber Power Index)
CSIRT	Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat)
CVD	Koordinoitu haavoittuvuuksien julkistaminen
DPA	Tietosuoja-asetus
DSM	Digitaaliset sisämarkkinat
ECCG	Euroopan kyberturvallisuuden sertifiointiryhmä
ECSM	Euroopan kyberturvallisuuskuukausi
ECSO	Euroopan kyberturvallisuusjärjestö
EFTA	Euroopan vapaakauppaliitto
EQF	Eurooppalainen tutkintojen viitekehys
EU	Euroopan unioni
GCI	Maailmanlaajuinen kyberturvallisuusindeksi (Global Cybersecurity Index)
GDPR	Yleinen tietosuoja-asetus
GDS	Valtion digitaalipalvelu
IA-CM	Julkisen sektorin sisäisiä tarkastusvalmiuksia koskeva malli (Internal Audit Capability Model for the Public Sector)
ICT	Tieto- ja viestintätekniikka
ISMM	Tietoturvan kypsyysmalli Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin kyberturvallisuuskehystä varten (Information Security Maturity Model for NIST Cybersecurity Framework)
ITU	Kansainvälinen televiestintäliitto

LEA	Lainvalvontaviranomainen
MS	Jäsenvaltio
NCSS	Kansalliset kyberturvallisuusstrategiat
NIS	Verkko- ja tietoturva
NIST	Kansallinen standardi- ja teknologiainstituutti
NLO	Kansalliset yhteyshenkilöt
OES	Keskeisten palvelujen tarjoajat
OT	Käytännön tekniikka
PET	Yksityisyyden suojaa parantavat tekniikat
PIMS	Henkilötietojen hallintajärjestelmä
Pk-yritykset	Pienet ja keskisuuret yritykset
PPP	Julkisen ja yksityisen sektorin kumppanuudet
Q-C2M2	Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Quatar Cybersecurity Capability Maturity Model)
SOG-IS MRA	Johtavien virkamiesten tietoturvallisuusryhmä, vastavuoroista tunnustamista koskeva sopimus
T&K	Tutkimus ja kehitys

TIIVISTELMÄ

Koska kyberturvallisuuden tämänhetkiset uhkakuvat laajenevat edelleen ja kyberhyökkäysten voimakkuus ja määrä on kasvussa, EU:n jäsenvaltioiden on reagoitava niihin tehokkaasti kehittämällä edelleen ja mukauttamalla kansallisia kyberturvallisuusstrategioitaan (NCSS). Sen jälkeen kun ENISA julkaisi ensimmäiset kansallisia kyberturvallisuusstrategioita koskevat tutkimukset vuonna 2012, EU:n jäsenvaltiot ja EFTA-maat ovat edistyneet huomattavasti strategioidensa kehittämisessä ja toteuttamisessa.

Tässä raportissa esitellään ENISAn työtä, joka koskee kansallisen valmiuksien arviointikehyksen (NCAF) laatimista.

Kehyksen tarkoituksena on antaa jäsenvaltioille maturiteetin itsearviointiväline, joka perustuu kansallisen kyberturvallisuusstrategian tavoitteiden arviointiin. Välineen avulla ne voivat parantaa ja rakentaa kyberturvallisuusvalmiuksiaan sekä strategisella että toiminnallisella tasolla.

Sillä kuvaillaan jäsenvaltioiden kyberturvallisuuden kypsyystasoa yksinkertaisella ja edustavalla tavalla. Kansallisten valmiuksien arviointikehys on väline, jonka avulla jäsenvaltiot voivat

- saada hyödyllistä tietoa pitkäaikaisen strategian kehittämistä varten (esim. hyviä käytäntöjä ja suuntaviivoja);
- tunnistaa kansallisen kyberturvallisuusstrategian puutteita;
- kehittää kyberturvallisuusvalmiuksia edelleen;
- tukea poliittisten toimien vastuullisuutta;
- lisätä uskottavuutta suuren yleisön ja kansainvälisten kumppaneiden silmissä;
- tukea tiedotusta ja vahvistamaan julkista kuvaa avoimena organisaationa;
- ennakoida tulevia ongelmia;
- tunnistaa saadut kokemukset ja parhaat käytännöt;
- tarjota EU:n laajuiset perustason kyberturvallisuusvalmiudet keskustelun edistämiseksi ja
- arvioida kyberturvallisuutta koskevat kansalliset valmiudet.

Kehyksen suunnittelussa auttoivat ENISAn eri alojen asiantuntijat sekä 19 jäsenvaltion ja EFTA-maan edustajat[1]. Raportin kohdeyleisöä ovat poliittiset päättäjät, asiantuntijat ja hallituksen virkamiehet, jotka vastaavat kansallisen kyberturvallisuusstrategian ja laajemmalti kyberturvallisuusvalmiuksien suunnittelusta, täytäntöönpanosta ja arvioinnista tai osallistuvat siihen.

[1] Seuraavien jäsenvaltioiden ja EFTA-maiden edustajia haastateltiin: Alankomaat, Belgia, Espanja, Irlanti, Italia, Kreikka, Kroatia, Liechtenstein, Malta, Norja, Portugali, Ruotsi, Saksa, Slovakia, Slovenia, Tanska, Tšekki, Unkari ja Viro.

Kansallisten valmiuksien arviointikehys käsittää 17 strategista tavoitetta ja rakentuu neljästä osa-alueesta seuraavasti:

- Osa-alue 1: Kyberturvallisuuden hallinto ja standardit
    1. Kehitetään kansallinen kyberturvallisuuden jatkuvuussuunnitelma
    2. Vahvistetaan perustason turvatoimia
    3. Turvataan digitaalinen identiteetti ja lisätään luottamusta digitaalisiin julkisiin palveluihin

- Osa-alue 2: Valmiuksien kehittäminen ja tietämyksen parantaminen
    4. Järjestetään kyberturvallisuusharjoituksia
    5. Luodaan valmiudet reagoida poikkeamiin
    6. Lisätään käyttäjien tietämystä
    7. Vahvistetaan koulutus- ja opetusohjelmia
    8. Edistetään tutkimusta ja kehitystä
    9. Tarjotaan yksityiselle sektorille kannustimia investoida turvatoimiin
    10. Parannetaan toimitusketjun kyberturvallisuutta

- Osa-alue 3: Lait ja sääntely
    11. Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia
    12. Puututaan kyberrikollisuuteen
    13. Perustetaan poikkeamista raportoinnin mekanismeja
    14. Vahvistetaan yksityisyyttä ja tietosuojaa

- Osa-alue 4: Yhteistyö
    15. Perustetaan julkisen ja yksityisen sektorin kumppanuuksia
    16. Vakiinnutetaan julkisten virastojen välistä yhteistyötä
    17. Osallistutaan kansainväliseen yhteistyöhön

1. JOHDANTO

Heinäkuussa 2016 annetun verkko- ja tietoturvadirektiivin 1 ja 7 artiklassa edellytetään, että EU:n jäsenvaltiot hyväksyvät verkko- ja tietojärjestelmien turvallisuutta koskevan kansallisen strategian, jota kutsutaan myös kansalliseksi kyberturvallisuusstrategiaksi (NCSS). Tässä yhteydessä kansallinen kyberturvallisuusstrategia määritellään kehykseksi, jolla määritetään strategiset periaatteet, suuntaviivat, strategiset tavoitteet sekä asianmukaiset toimintaperiaatteet ja sääntelytoimenpiteet. Kansalliselle kyberturvallisuusstrategialle asetettuna tavoitteena on saavuttaa ja ylläpitää korkeatasoinen verkko- ja tietojärjestelmien turvallisuus ja siten antaa jäsenvaltioille mahdollisuus lieventää mahdollisia uhkia. Kansallinen kyberturvallisuusstrategia voi olla myös teollisen, taloudellisen ja sosiaalisen kehityksen katalysaattori.

EU:n kyberturvallisuusasetuksessa todetaan, että ENISAn on edistettävä kansallisen kyberturvallisuusstrategian määrittelemistä ja täytäntöönpanoa koskevien parhaiden käytäntöjen levittämistä tukemalla jäsenvaltioita verkko- ja tietoturvadirektiivin hyväksymisessä ja keräämällä näiden kokemuksiin perustuvaa arvokasta palautetta. Tältä osin ENISA on kehittänyt useita välineitä, joilla avustetaan jäsenvaltioita kansallisten kyberturvallisuusstrategioidensa kehittämisessä, täytäntöönpanossa ja arvioinnissa.

Osana toimeksiantoaan ENISA pyrkii kehittämään kansallisten valmiuksien itsearviointikehyksen, jolla mitataan eri kansallisten kyberturvallisuusstrategioiden kypsyystasoa. Tämän raportin tavoitteena on esitellä tutkimus, joka toteutettiin itsearviointikehyksen määrittelyn yhteydessä.

1.1 TUTKIMUKSEN LAAJUUS JA TAVOITTEET

Tämän tutkimuksen tärkeimpänä tavoitteena on laatia kansallisten valmiuksien itsearviointikehys, jota kutsutaan myöhemmin ’kansallisten valmiuksien arviointikehykseksi’ ja jolla mitataan jäsenvaltioiden kyberturvallisuusvalmiuksien kypsyystasoa. Tarkemmin sanottuna kehyksellä olisi annettava jäsenvaltioille mahdollisuus

- arvioida kansallisia kyberturvallisuusvalmiuksiaan;
- lisätä tietämystä maan kypsyystasosta;
- tunnistaa kehittämisalueita ja
- kehittää kyberturvallisuusvalmiuksia.

Kehyksellä on tarkoitus auttaa jäsenvaltioita ja erityisesti kansallisia poliittisia päättäjiä toteuttamaan itsearviointimenettely, jonka tavoitteena on parantaa kansallisia kyberturvallisuusvalmiuksia.

1.2 MENETTELYTAVAT

Kansallisten valmiuksien itsearviointikehyksen laatimisessa käytetty menettelytapa pohjautuu seuraaviin neljään päävaiheeseen:

1. **Aineistotutkimus**: Ensimmäisessä vaiheessa toteutettiin laaja kirjallisuuskatsaus, jonka tarkoituksena oli kerätä parhaita käytäntöjä kansallisten kyberturvallisuusstrategioiden kypsyyttä koskevan arviointikehyksen kehittämisestä. Aineistotutkimuksessa keskityttiin kyberturvallisuusvalmiuksien kehittämistä ja strategian määrittelyä koskevien asiaankuuluvien asiakirjojen järjestelmälliseen analysointiin, jäsenvaltioiden nykyisiin kyberturvallisuusstrategioihin ja nykyisten

kyberturvallisuuden kypsyysmallien vertailuun. Nykyisiä kypsyysmalleja koskeva vertailuanalyysi tehtiin käyttämällä tätä tutkimusta varten kehitettyä analysointikehystä. Analysointikehys perustuu kypsyysmallien kehittämistä koskevaan Beckerin[2] menetelmään, jolla luodaan yleinen ja yhdistetty menettelymalli kypsyysmallien suunnittelulle ja annetaan selkeät vaatimukset kypsyysmallien kehittämiselle. Analysointikehystä mukautettiin edelleen tämän tutkimuksen tarpeita vastaavaksi.

2. **Asiantuntijoiden ja sidosryhmien näkemysten kerääminen**: Aineistotutkimuksen avulla kerättyjen tietojen ja analyysin alustavien päätelmien perusteella tässä vaiheessa kartoitettiin asiantuntijoita, joilla oli kokemusta kansallisen kyberturvallisuusstrategian tai kypsyysmallien kehittämisestä ja täytäntöönpanosta, ja kutsuttiin heidät haastatteluun. ENISA otti yhteyttä omaan kansallisten kyberturvallisuusstrategioiden asiantuntijoiden ryhmään ja kansallisiin yhteyshenkilöihin löytääkseen kunkin jäsenvaltion asiaankuuluvat asiantuntijat. Joitakin kypsyysmallien kehittämiseen osallistuneita asiantuntijoita myös haastateltiin. Yhteensä tehtiin 22 haastattelua, joista 19:ssä haastateltiin eri jäsenvaltioiden (ja EFTA-maiden) kyberturvallisuusvirastojen edustajia.
3. **Saatujen tietojen analysointi:** Aineistotutkimuksen ja haastattelujen avulla kerätyt tiedot analysoitiin, jotta tunnistettaisiin kansallisten kyberturvallisuusstrategioiden maturiteetin mittaamiseen käytettävän itsearviointikehyksen suunnittelua koskevia parhaita käytäntöjä ja jotta ymmärrettäisiin jäsenvaltioiden tarpeet ja voitaisiin määrittää, mitä tietoja eri Euroopan maista[3] on mahdollista kerätä. Analyysi mahdollisti aiemmissa vaiheissa kehitetyn alustavan mallin täsmentämisen ja malliin sisältyvien indikaattorien, kypsyystasojen ja ulottuvuuksien tarkentamisen.
4. **Mallin viimeistely:** Sen jälkeen ENISAn eri alojen asiantuntijat tarkistivat kansallisten valmiuksien itsearviointikehyksen päivitetyn version. Lopuksi asiantuntijat vahvistivat kehyksen lokakuussa 2020 pidetyssä työpajassa ennen se julkistamista.

1.3 KOHDEYLEISÖ

Raportin kohdeyleisöä ovat poliittiset päättäjät, asiantuntijat ja hallituksen virkamiehet, jotka vastaavat kansallisen kyberturvallisuusstrategian ja laajemmalti kyberturvallisuusvalmiuksien suunnittelusta ja täytäntöönpanosta tai osallistuvat siihen. Tässä asiakirjassa julkaistut tulokset voivat lisäksi olla hyödyllisiä kyberturvallisuuspolitiikan asiantuntijoille ja tutkijoille sekä kansallisella että eurooppalaisella tasolla.

[2] J. Becker, R. Knackstedt ja J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application", Business & Information Systems Engineering, vol. 1, no. 3, s. 213–222, kesäkuu 2009.
[3] Tätä tutkimusta varten tässä raportissa 'Euroopan mailla' tarkoitetaan EU:n 27 jäsenvaltiota.

2. TAUSTAA

2.1 KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN ELINKAARTA KOSKEVAT AIEMMAT JULKAISUT

Kuten EU:n kyberturvallisuusasetuksessa todetaan, yksi ENISAn tärkeimmistä tavoitteista on tukea jäsenvaltioita verkko- ja tietojärjestelmien turvallisuutta koskevien kansallisten strategioiden kehittämisessä, edistää kyseisten strategioiden levittämistä ja seurata niiden täytäntöönpanoa. Osana toimeksiantoaan ENISA on laatinut useita tätä asiaa koskevia asiakirjoja edistääkseen hyvien käytäntöjen jakamista ja tukeakseen kansallisten kyberturvallisuusstrategioiden täytäntöönpanoa kaikkialla EU:ssa:

- ”Practical guide on the development and execution phase of NCSS”[4], julkaistu vuonna 2012
- ”Setting the course for national efforts to strengthen security in cyberspace”[5], julkaistu vuonna 2012
- Ensimmäinen ENISAn kehys jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden arviointia varten[6] on julkaistu vuonna 2014.
- ”Online NCSS Interactive Map”[7], julkaistu vuonna 2014.
- ”NCSS Good Practice Guide”[8], julkaistu vuonna 2016.
- ”National Cybersecurity Strategies Evaluation Tool”[9], julkaistu vuonna 2018.
- ”Good practices in innovation on Cybersecurity under the NCSS”[10], julkaistu vuonna 2019.

Liitteessä A on lyhyt yhteenveto tätä aihetta koskevista ENISAn tärkeimmistä julkaisuista.

Edellä mainittuihin oppaisiin ja asiakirjoihin tutustuttiin osana aineistotutkimusta. Erityisesti kansallisten kyberturvallisuusstrategioiden arviointivälinettä koskeva julkaisu ”National Cybersecurity Strategies Evaluation Tool”[11] on perustavanlaatuinen osa kansallisten

[4] ”NCSS: Practical Guide on Development and Execution” (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] ”NCSS: Setting the course for national efforts to strengthen security in cyberspace” (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] ”An evaluation framework for NCSS” (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] ”National Cybersecurity Strategies – Interactive Map” (ENISA, 2014, päivitetty 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Tällä asiakirjalla päivitetään vuoden 2012 opas: ”NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies” (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] ”National Cybersecurity Strategies Evaluation Tool” (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] ”National Cybersecurity Strategies Evaluation Tool” (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

valmiuksien arviointikehystä. Kansallisten valmiuksien arviointikehys perustuu kansallisten kyberturvallisuusstrategioiden verkkoarviointivälineen tavoitteisiin.

2.2 EUROOPPALAISISSA KANSALLISISSA KYBERTURVALLISUUSSTRATEGIOISSA TUNNISTETUT YLEISET TAVOITTEET

Eri jäsenvaltioiden väliset erot vaikeuttavat yhteisten toimintojen tai toimintasuunnitelmien tunnistamista erilaisissa kansallisissa yhteyksissä, oikeudellisissa kehyksissä ja toimintalinjojen asialistoilla. Jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden strategiset tavoitteet koskevat kuitenkin samoja aiheita. ENISAn aiemman työn ja jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden analysoinnin perusteella tunnistettiin 22 strategista tavoitetta. Näistä 15 oli jo tunnistettu ENISAn aiemman työn yhteydessä, kaksi lisättiin uusina tähän tutkimukseen ja viisi tavoitetta tunnistettiin tulevia keskusteluja varten.

2.2.1 Jäsenvaltioiden yhteiset strategiset tavoitteet

ENISAn aiempaan työhön eli kansallisten kyberturvallisuusstrategioiden arviointivälineeseen[12] perustuen seuraavassa taulukossa esitetään edellä mainitut 15 strategista tavoitetta, jotka ovat yhteisiä jäsenvaltioiden kansallisille kyberturvallisuusstrategioille. Tavoitteet muodostavat aihetta koskevan yleisen kansallisen filosofian ytimen. Lisätietoa alla kuvatuista tavoitteista on ENISAn raportissa ”NCSS Good Practice Guide”[13].

Taulukko 1: Jäsenvaltioiden yhteiset strategiset tavoitteet kansallisissa kyberturvallisuusstrategioissa

Nro	Kansallisen kyberturvallisuusstrategian strategiset tavoitteet	Tavoitteet
1	**Kehitetään kansallisia kyberturvallisuuden jatkuvuussuunnitelmia**	▶ Esitetään ja kuvaillaan kriteerit, joita olisi käytettävä tilanteen määrittelemiseksi kriisiksi; ▶ Määritetään tärkeimpiä kriisinhallintamenettelyjä ja -toimia; ja ▶ Määritetään selvästi eri sidosryhmien tehtävät ja vastuut kyberturvallisuuskriisissä; ▶ Esitetään ja kuvaillaan kriteerit, joiden perusteella kriisin voidaan todeta olevan ohi ja/tai kellä on valtuudet todeta asia.
2	**Vahvistetaan perustason turvatoimia**	▶ Yhdenmukaistetaan sekä julkisen että yksityisen sektorin organisaatioiden noudattamat erilaiset käytännöt; ▶ Luodaan toimivaltaisten viranomaisten ja organisaatioiden välille yhteinen kieli ja avoimet turvalliset viestintäkanavat; ▶ Annetaan eri sidosryhmille mahdollisuus tarkistaa kyberturvallisuusvalmiutensa ja vertailla niitä; ▶ Annetaan tietoa kyberturvallisuutta koskevista parhaista käytännöstä kaikilla elinkeinoelämän toimialoilla; ▶ Autetaan sidosryhmiä asettamaan turvallisuusinvestoinnit etusijalle.
3	**Järjestetään kyberturvallisuusharjoituksia**	▶ Määritellään, mitä on testattava (suunnitelmat ja käytännöt, ihmiset, infrastruktuuri, reagointivalmiudet, yhteistyövalmiudet, viestintä jne.); ▶ Perustetaan kyberturvallisuusharjoituksen suunnittelusta vastaava kansallinen työryhmä, jolla on selvä toimeksianto; ja

[12] ”National Cybersecurity Strategies Evaluation Tool” (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Tällä asiakirjalla päivitetään vuoden 2012 opas: ”NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies” (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Nro	Kansallisen kyberturvallisuusstrategian strategiset tavoitteet	Tavoitteet
		▶ Sisällytetään kyberturvallisuusharjoitukset kansalliseen kyberturvallisuusstrategiaan tai kansallisen kyberturvallisuuden jatkuvuussuunnitelmaan.
4	Luodaan valmiudet reagoida poikkeamiin	▶ Toimeksianto – tämä koskee valtuuksia, tehtäviä ja vastuita, jotka asianomaisen valtion on annettava työryhmälle; ▶ Palveluportfolio – tämä kattaa palvelut, joita työryhmä tarjoaa toiminta-alueellaan tai käyttää omassa sisäisessä toiminnassaan; ▶ Toiminnalliset valmiudet – tämä koskee teknisiä ja toiminnallisia vaatimuksia, joita työryhmän on noudatettava; ja ▶ Yhteistyövalmiudet – nämä käsittävät vaatimukset, jotka koskevat tietojenvaihtoa sellaisten muiden työryhmien kanssa, jotka eivät kuulu kolmeen edelliseen kategoriaan, esim. poliittiset päätöksentekijät, puolustusvoimat, sääntelyviranomaiset, (kriittisen tietoinfrastruktuurin) toimijat ja lainvalvontaviranomaiset.
5	Lisätään käyttäjien tietämystä	▶ Tunnistetaan puutteet kyberturvallisuus- tai tietoturvallisuusasioita koskevassa tietämyksessä; ja ▶ Korjataan puutteet lisäämällä tietämystä tai kehittämällä/vahvistamalla perustietoja.
6	Vahvistetaan koulutus- ja opetusohjelmia	▶ Vahvistetaan nykyisen tietoturvahenkilöstön toiminnallisia valmiuksia; ▶ Kannustetaan opiskelijoita mukaan ja tuetaan heitä valitsemaan kyberturvallisuusala; ▶ Edistetään ja kehitetään akateemisten tietoturvaympäristöjen ja tietoturva-alan välisiä suhteita; ja ▶ Kohdistetaan kyberturvallisuuskoulutus yrityksen tarpeisiin.
7	Edistetään tutkimusta ja kehitystä	▶ Tunnistetaan haavoittuvuuden todellisia syistä sen sijaan, että korjattaisiin niiden vaikutuksia; ▶ Tuodaan yhteen eri alojen tutkijoita, jotta saadaan ratkaistuksi monitahoisia ja monimutkaisia ongelmia, esimerkiksi fyysisiä kyberuhkia; ▶ Yhdistetään elinkeinoelämän tarpeet ja tutkimuksen tulokset ja edistetään siirtymistä teoriasta käytäntöön; ja ▶ Etsitään tapoja ylläpitää ja lisätä tuotteiden ja palvelujen kyberturvallisuuden tasoa tukemalla nykyisiä kyberturvallisuuden infrastruktuureja.
8	Tarjotaan yksityiselle sektorille kannustimia investoida turvatoimiin	▶ Määritetään yksityisten yritysten mahdollisia kannustimia investoida turvatoimiin; ja ▶ Tarjotaan yrityksille kannustimia, joilla rohkaistaan investoimaan turvallisuuteen.
9	Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia	▶ Määritetään kriittinen tietoinfrastruktuuri; ja ▶ Määritetään mahdolliset kriittisen tietoinfrastruktuurin riskit ja lievennetään niitä.
10	Puututaan kyberrikollisuuteen	▶ Laaditaan kyberrikollisuutta koskevia lakeja; ja ▶ Lisätään lainvalvontaviranomaisten tehokkuutta.
11	Perustetaan poikkeamista raportoinnin mekanismeja	▶ Hankitaan tietoa yleisestä uhkaympäristöstä; ▶ Arvioidaan poikkeamien (esim. tietoturvaloukkausten, verkkovikojen, palvelunkeskeytysten) vaikutusta; ▶ Hankitaan tietoa nykyisistä ja uusista haavoittuvuuksista ja hyökkäysten tyypeistä; ▶ Päivitetään turvatoimia vastaavasti; ja ▶ Pannaan täytäntöön poikkeamista raportointia koskevat verkko- ja tietoturvadirektiivin säännökset.
12	Vahvistetaan yksityisyyttä ja tietosuojaa	▶ Edistetään yksityisyyttä ja tietosuojaa koskevien perusoikeuksien vahvistamista.
13	Perustetaan julkisen ja yksityisen sektorin kumppanuuksia	▶ Estäminen (estetään hyökkäykset);

Nro	Kansallisen kyberturvallisuusstrategian strategiset tavoitteet	Tavoitteet
		▶ Suojaaminen (tutkitaan uusia tietoturvauhkia); ▶ Havaitseminen (puututaan uusiin tietoturvauhkiin jakamalla tietoa); ▶ Reagointi (valmiudet selvitä poikkeaman alustavasta vaikutuksesta); ja ▶ Palautuminen (valmiudet korjata poikkeaman lopullinen vaikutus).
14	Vakiinnutetaan julkisten virastojen välistä yhteistyötä	▶ Lisätään sellaisten julkisten virastojen välistä yhteistyötä, joilla on kyberturvallisuutta koskevaa vastuuta ja pätevyyttä; ▶ Vältetään osaamisen ja resurssien päällekkäisyyttä julkisten virastojen välillä ▶ Parannetaan ja vakiinnutetaan yhteistyötä julkisten virastojen välillä kyberturvallisuuden eri aloilla.
15	Osallistutaan kansainväliseen yhteistyöhön (myös muiden kuin EU:n jäsenvaltioiden kanssa)	▶ Saadaan hyötyä EU:n jäsenvaltioiden välisen yhteisen tietopohjan luomisesta; ▶ Luodaan synergiaetuja kansallisten kyberturvallisuusviranomaisten välille; ja ▶ Mahdollistetaan rajat ylittävän rikollisuuden torjuminen ja lisätään sitä.

2.2.2 Muita strategisia tavoitteita

ENISAn tekemien aineistotutkimuksen ja haastattelujen perusteella määritettiin muita strategisia tavoitteita. Jäsenvaltiot käsittelevät näitä aiheita yhä enemmän kansallisissa kyberturvallisuusstrategioissaan tai laativat samaa aihetta koskevia toimintasuunnitelmia. Esimerkkejä jäsenvaltioiden toteuttamista toimista on myös annettu. Jos esimerkki on peräisin julkisesti saatavilla olevasta lähteestä, siihen on viitattu. Jos esimerkit perustuvat EU:n jäsenvaltioiden virkamiesten luottamuksellisiin haastatteluihin, viitteitä ei ole annettu.

Seuraavat muut strategiset tavoitteet määritettiin:

- Parannetaan toimitusketjun kyberturvallisuutta; ja
- Turvataan digitaalinen identiteetti ja lisätään luottamusta digitaalisiin julkisiin palveluihin.

Parannetaan toimitusketjun kyberturvallisuutta

Pienet ja keskisuuret yritykset (pk-yritykset) ovat Euroopan talouden selkäranka. Ne edustavat 99:ää prosenttia EU:n kaikista yrityksistä[14], ja vuonna 2015 arvioitiin, että pk-yritykset ovat luoneet noin 85 prosenttia uusista työpaikoista ja tarjonneet kaksi kolmasosaa kaikista yksityisen sektorin työpaikoista EU:ssa. Koska pk-yritykset tarjoavat palveluja suuremmille yrityksille ja tekevät yhä enemmän yhteistyötä julkishallinnon kanssa[15], on syytä huomata, että nykyisessä yhteenliitetyssä verkossa pk-yritykset ovat kyberhyökkäysten heikko lenkki. Pk-yritykset ovat kaikkein alttiimpia kyberhyökkäyksille, mutta niillä ei useinkaan ole varaa investoida riittävään kyberturvallisuuteen[16]. Toimitusketjun kyberturvallisuuden parantaminen olisi siksi toteutettava keskittymällä pk-yrityksiin.

[14] https://ec.europa.eu/growth/smes_fi
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/fi/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Tämän järjestelmällisen lähestymistavan lisäksi jäsenvaltiot voivat myös korostaa tiettyjen tieto- ja viestintätekniikkapalvelujen ja olennaisiksi katsottujen tuotteiden kyberturvallisuutta koskevia toimia. Tällaisia palveluja ja tuotteita ovat kriittisessä tietoinfrastruktuurissa käytetty tieto- ja viestintätekniikka, teleliikennealalla täytäntöön pannut turvamekanismit (valvonta ISP-tasolla), eIDAS-asetuksessa määritellyt luottamuspalvelut ja pilvipalvelun tarjoajat. Esimerkiksi Puola sitoutui vuosien 2019–2024 kansallisessa kyberturvallisuusstrategiassaan[17] kehittämään kansallisen kyberturvallisuusarviointi- ja sertifiointijärjestelmän, joka toimisi toimitusketjun laadunvarmistusmekanismina. Tämä sertifiointijärjestelmä yhdenmukaistetaan EU:n kyberturvallisuusasetuksessa (2019/881) säädetyn tieto- ja viestintätekniikan digitaalisten tuotteiden, palvelujen ja prosessien EU:n sertifiointikehyksen kanssa.

Toimitusketjun kyberturvallisuuden parantaminen on siis ensiarvoisen tärkeää. Se voidaan saavuttaa muun muassa toteuttamalla vahvaa politiikkaa pk-yritysten hyväksi, tarjoamalla kyberturvallisuusvaatimuksia koskevia ohjeita julkishallinnon hankintamenettelyissä, edistämällä yksityisen sektiorin kanssa tehtävää yhteistyötä, perustamalla julkisen ja yksityisen sektorin kumppanuuksia, edistämällä koordinoituja haavoittuvuuksien julkistamismekanismeja[18], rakentamalla tuotteiden sertifiointijärjestelmä, joka koskee myös pk-yritysten digitaalisten aloitteiden kyberturvallisuusosia, ja rahoittamalla osaamisen kehittämistä.

Turvataan digitaalinen identiteetti ja lisätään luottamusta digitaalisiin julkisiin palveluihin

Helmikuussa 2020 komissio esitti näkemyksensä EU:n digitaalisesta muutoksesta tiedonannossaan Euroopan digitaalista tulevaisuutta rakentamassa[19]. Tavoitteena on tuottaa osallistavia teknologioita, jotka toimivat ihmisten eduksi ja kunnioittavat EU:n perusarvoja. Tiedonannossa todetaan erityisesti, että on ratkaisevan tärkeää edistää julkishallintojen digitalisaatiota kaikkialla Euroopassa. Tältä osin on ensiarvoisen tärkeää kehittää luottamusta hallintoon digitaalisen identiteetin ja julkisten palvelujen osalta. Se on vieläkin tärkeämpää, kun otetaan huomioon, että julkisen sektorin tapahtumat ja tietojen vaihto ovat usein arkaluonteisia.

Useat maat, kuten Alankomaat, Espanja, Luxemburg, Malta, Ranska, Tanska, Viro ja Yhdistynyt kuningaskunta, ovat kertoneet, että aikovat puuttua tähän asiaan kansallisissa kyberturvallisuusstrategioissaan. Jotkin näistä valtioista ovat myös todenneet, että tätä strategista tavoitetta saatetaan käsitellä osana laajempaa suunnitelmaa:

- Viro liittää asiaa koskevan toimintasuunnitelman The security of electronic identity and electronic authentication capability laajempaan Viron digitaalistrategiaan vuodelle 2020.
- Ranskan kansallisessa kyberturvallisuusstrategiassa todetaan, että digitaaliteknologiasta vastaava ministeri valvoo sellaisen etenemissuunnitelman laatimista, jonka tarkoituksena on suojella ranskalaisten internetin käyttöä, yksityisyyttä ja henkilötietoja.
- Alankomaiden kansallisessa kyberturvallisuusstrategiassa todetaan, että julkishallinnon ja kansalaisille ja yrityksille tarjottavia julkisten palvelujen kyberturvallisuutta käsitellään tarkemmin digitaalista hallintoa koskevissa laajoissa suuntaviivoissa.
- Samalla kun Yhdistynyt kuningaskunta jatkaa palvelujensa siirtämistä verkkoon, se on nimittänyt valtion digitaalipalvelun (Government Digital Service, GDS) varmistamaan, että kaikki valtion kehittämät tai hankkimat uudet digitaaliset palvelut ovat myös

[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Euroopan digitaalista tulevaisuutta rakentamassa, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

lähtökohtaisesti turvallisia. Tehtävässä avustaa Britannian kansallinen kyberturvallisuuskeskus (British National Cybersecurity Centre, NCSC).

2.2.3 Muita harkittuja strategisia tavoitteita

Aineistotutkimusvaiheessa ja osana ENISAn tekemiä haastatteluja tutkittiin myös muita strategisia tavoitteita. Päätettiin kuitenkin, että nämä tavoitteet eivät ole osa itsearviointikehystä. Liitteessä C – Muut tutkitut tavoitteet määritellään nämä tavoitteet, joita voidaan käyttää edistämään tulevia keskusteluja mahdollisista kansallisten kyberturvallisuusstrategioiden kehityskohteista.

Tulevia pohdintoja varten tutkittiin seuraavia strategisia tavoitteita:

- Kehitetään alakohtaisia kyberturvallisuusstrategioita;
- Torjutaan väärän tiedon levityskampanjoita;
- Turvataan huipputeknologioita (5G, tekoäly, kvanttilaskenta jne.);
- Varmistetaan datasuvereniteetti; ja
- Tarjotaan kannustimia kybervakuutusalan kehittämiseen.

2.3 VERTAILUANALYYSIN TÄRKEIMMÄT HAVAINNOT

Kyberturvallisuutta koskevien nykyisten kypsyysmallien työpöytätutkimus toteutettiin keräämällä tietoja ja todisteita, joilla tuettiin kansallisten valmiuksien itsearviointikehyksen suunnittelua kansallisten kyberturvallisuusstrategioiden alalla. Tässä yhteydessä toteutettiin laaja kirjallisuuskatsaus nykyisistä malleista täydentämään 2.1 ja 2.2 kohdassa kehitettyjen kyberturvallisuuden kypsyysmallien ja nykyisten kansallisten kyberturvallisuusstrategioiden alustavan kartoitustutkimuksen tuloksia. Tällä järjestelmällisellä arvioinnilla tuetaan arviointikehyksen kypsyystasojen valintaa ja perustelua sekä eri ulottuvuuksien ja indikaattorien määrittelemistä.

Kypsyysmallien järjestelmällisessä arvioinnissa tarkasteltiin kymmentä mallia, joita analysoitiin niiden keskeisten ominaisuuksien perusteella. Taulukko 2: Yleiskatsaus analysoituihin kypsyysmalleihin: yleiskatsaus jokaisen tämän tutkimuksen yhteydessä arvioidun mallin keskeisiin ominaisuuksiin; LIITE A: tarkempaa tietoa.

Taulukko 2: Yleiskatsaus analysoituihin kypsyysmalleihin

Mallin nimi	Kypsyystasojen määrä	Määritteet	Arviointimenetelmä	Tulosten kuvaus
Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (Cybersecurity Capacity Maturity Model for Nations, CMM)	5	Viisi pääulottuvuutta	Yhteistyö paikallisen organisaation kanssa mallin hienosäätämiseksi ennen sen soveltamista kansallisesti	Viisiosainen tutka
Kyberturvallisuusvalmiuksien kypsyysmalli (Cybersecurity Capability Maturity Model, C2M2)	4	10 pääalaa	Itsearviointimenetelmä ja -välineet	Mittaristo ja ympyräkaaviot
Kriittisen infrastruktuurin kyberturvallisuuden parantamiskehys (Framework for Improving Critical Infrastructure Cybersecurity)	Ei sovelleta (neljä tasoa)	Viisi ydintehtävää	Itsearviointi	Ei sovelleta

Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Quatar Cybersecurity Capability Maturity Model, Q-C2M2)	5	Viisi pääalaa	Ei sovelleta	Ei sovelleta
Kyberturvallisuuden kypsyysmallin sertifiointi (Cybersecurity Maturity Model Certification, CMMC)	5	17 pääalaa	Kolmannen osapuolen tarkastajien tekemä arviointi	Ei sovelleta
Yhteisön kyberturvallisuuden kypsyysmalli (Community Cybersecurity Maturity Model, CCSMM)	5	Kuusi pääulottuvuutta	Yhteisöissä toteutettava arviointi, johon valtion ja liittovaltion lainvalvontaviranomaiset osallistuvat	Ei sovelleta
Tietoturvan kypsyysmalli Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin kyberturvallisuuskehystä varten (Information Security Maturity Model for NIST Cybersecurity Framework, ISMM)	5	23 arvioitua alaa	Ei sovelleta	Ei sovelleta
Julkisen sektorin sisäisiä tarkastusvalmiuksia koskeva malli (Internal Audit Capability Model (IA-CM) for the Public Sector)	5	Kuusi osaa	Itsearviointi	Ei sovelleta
Maailmanlaajuinen kyberturvallisuusindeksi (Global Cybersecurity Index, GCI)	Ei sovelleta	Viisi pilaria	Itsearviointi	Luokitustaulukko
Kybervoimaindeksi (CPI)	Ei sovelleta	Neljä luokkaa	Economist Intelligence Unitin tekemä vertailu	Luokitustaulukko

Järjestelmällisen arvioinnin perusteella oli mahdollista tehdä päätelmiä nykyisissä malleissa käytetyistä parhaista käytännöistä ja tukea nykyisen kypsyysmallin käsitteellisen mallin kehittämistä. Vertailuanalyysillä tuettiin erityisesti kypsyystasojen määrittämistä, ulottuvuuksien ryhmien luomista ja indikaattorien valintaa sekä mallin tulosten sopivan havainnollistamismenetelmän laatimista. Osien tärkeimmät havainnot esitetään yksityiskohtaisemmin taulukossa 3 .

Taulukko 3: Vertailuanalyysin tärkeimmät havainnot

Ominaisuus	Tärkein havainto
Kypsyystasot	Kyberturvallisuusvalmiuksien arviointikehysten viisitasoinen kypsyysasteikko on yleisesti hyväksytty, ja sillä pystytään saamaan rakeisia arviointituloksia (ks. tyhjentävä selvitys kunkin mallin kypsyystasojen määritelmästä taulukosta 6 Kypsyystasojen vertailu taulukosta 6 Kypsyystasojen vertailu); ▶ Kaikki mallit tuottavat kustakin kypsyystasosta korkeatasoisen määritelmän, jota mukautetaan sitten eri ulottuvuuksiin tai niiden ryhmiin; ▶ Kyberturvallisuusvalmiuksien maturiteetin mittauksessa arvioidaan tavallisesti kahta päätekijää: strategioiden kypsyyttä ja strategioiden täytäntöönpanoa varten käyttöönotettujen menetelmien kypsyyttä.
Määritteet	▶ Nykyisten kypsyysmallien määritteiden vertailuanalyysista saatiin heterogeenisiä tuloksia, ja mallikohtaisten määritteiden keskimääräinen määrä on neljästä viiteen; Neljästä viiteen määritteeseen perustuva malli antaa maille oikean datan rakeisuuden tason ryhmittämällä asiaankuuluvia ulottuvuuksia yhteen ja varmistamalla tulosten luettavuuden (ks. kunkin mallin kuvaus taulukosta 7 Määritteiden ja ulottuvuuksien vertaileminen taulukosta 6 Kypsyystasojen vertailu); ▶ Kaikissa malleissa käytetty osa-alueiden määrittelyn pääperiaate perustuu kunkin osa-alueen sisällä ryhmitellyn osan johdonmukaisuuteen.
Arviointimenetelmä	▶ Analysoiduissa eri malleissa käytetyt arviointimenetelmät vaihtelevat; ▶ Yleisin arviointimenetelmä perustuu itsearviointiin.
Tulosten kuvaus	▶ On tärkeää esittää tulokset rakeisuuden eri tasoilla; ▶ Havainnollistamismenetelmän olisi oltava itsestään selvä ja helppolukuinen.

Käsitteellinen malli laadittiin eri kypsyysmallien vertailuanalyysin sekä ENISAn aiemman työn perusteella. Kutakin määritettä varten käytettävien kypsyysindikaattorien kehittämisessä päätettiin lisäksi hyödyntää *ENISAn interaktiivista verkkotyökalua*.

2.4 HAASTEET KANSALLISTEN KYBERTURVALLISUUSSTRATEGIOIDEN ARVIOINNISSA

Jäsenvaltiot kohtaavat monenlaisia haasteita kehittäessään kyberturvallisuusvalmiuksia ja erityisesti varmistaessaan, että niiden valmiudet ovat ajan tasalla uusimman kehityksen kanssa. Alla on yhteenveto haasteista, joita jäsenvaltiot havaitsivat ja joista keskusteltiin jäsenvaltioiden kanssa tämän tutkimuksen aikana:

- **Koordinointia ja yhteistyötä koskevat vaikeudet:** Kyberturvallisuustoimien koordinointi kansallisella tasolla, jotta kyberturvallisuusongelmiin vastataan tehokkaasti, saattaa osoittautua haasteelliseksi siihen osallistuvien sidosryhmien suuren määrän vuoksi.
- **Arvioinnin toteuttamiseen osallistuvien resurssien puute:** Paikallisista olosuhteista ja kyberturvallisuutta koskevasta kansallisesta hallintorakenteesta johtuen kansallisen kyberturvallisuusstrategian ja sen tavoitteiden arviointi voi kestää jopa yli 15 henkilötyöpäivää.
- **Kyberturvallisuusvalmiuksien kehittämistä koskevan tuen puute:** Jotkin jäsenvaltiot totesivat, että kyberturvallisuusvalmiuksien kehittämistä koskevan talousarvion puolustamiseksi ja sitä koskevan tuen saamiseksi niiden on ensin toteutettava arviointivaihe havaitakseen puutteita ja rajoituksia.
- **Vaikeudet strategian saavutuksia tai muutoksia koskevien vastuiden osoittamisessa:** Koska uhkia esiintyy joka päivä ja teknologia kehittyy, toimintasuunnitelmia on jatkuvasti mukautettava vastaavasti. Kansallisen

kyberturvallisuusstrategian arviointi ja muuttaminen on kuitenkin edelleen vaivalloinen tehtävä. Tämä puolestaan tekee kansallisen kyberturvallisuusstrategian rajoitusten ja puutteiden havaitsemisen vaikeaksi.

- **Vaikeudet kansallisen kyberturvallisuusstrategian tehokkuuden mittaamisessa:** Mittareita voidaan kerätä eri alueiden, kuten edistymisen, täytäntöönpanon, maturiteetin ja tehokkuuden, mittaamista varten. Vaikka edistymisen ja täytäntöönpanon mittaaminen on varsin helppoa tehokkuuden mittaamiseen verrattuna, viimeksi mainitulla on enemmän merkitystä arvioitaessa kansallisen kyberturvallisuusstrategian tuloksia ja vaikutuksia. ENISAn tekemissä haastatteluissa useat jäsenvaltiot totesivat, että kansallisen kyberturvallisuusstrategian tehokkuuden määrällinen mittaaminen on tärkeää mutta myös erittäin vaativa tehtävä, joka on joissain tapauksissa mahdoton toteuttaa.
- **Vaikeudet yhteisen kehyksen hyväksymisessä:** EU:n jäsenvaltiot toimivat erilaisissa yhteyksissä politiikan, organisaatioiden, kulttuurin, yhteiskuntarakenteen ja kansallisen kyberturvallisuusstrategian kypsyyden osalta. Jotkin tutkimuksen aikana haastatellut jäsenvaltiot totesivat, että kaikille sopivan itsearviointikehyksen puolustaminen ja käyttö voi osoittautua vaikeaksi.

2.5 KANSALLISTEN VALMIUKSIEN ARVIOINNIN EDUT

Vuodesta 2017 lähtien kaikilla jäsenvaltioilla on ollut kansallinen kyberturvallisuusstrategia[20]. Vaikka kehitys on myönteistä, on myös tärkeää, että jäsenvaltiot pystyvät arvioimaan kansallisia kyberturvallisuusstrategioitaan kunnolla ja siten tuomaan lisäarvoa niiden strategiseen suunnitteluun ja täytäntöönpanoon.

Yksi kansallisten valmiuksien arviointikehyksen tavoitteista on arvioida kyberturvallisuusvalmiuksia useissa kansallisissa kyberturvallisuusstrategioissa asetettujen prioriteettien perusteella. Pohjimmiltaan kehyksen avulla arvioidaan jäsenvaltioiden kyberturvallisuusvalmiuksien kypsyyttä kansallisen kyberturvallisuusstrategian tavoitteissa määritellyillä aloilla. Näin kehyksen tulokset tukevat jäsenvaltioiden poliittisia päätöksentekijöitä kansallisen kyberturvallisuusstrategian määrittämisessä antamalla heille nykytilannetta koskevia maakohtaisia tietoja[21]. Kansallisten valmiuksien arviointikehyksen perimmäisenä tavoitteena on auttaa jäsenvaltioita tunnistamaan kehitysalueita ja kehittämään valmiuksia.

Kehyksen tarkoituksena on antaa jäsenvaltioille maturiteetin itsearviointiväline, joka perustuu kansallisen kyberturvallisuusstrategian tavoitteiden arviointiin. Välineen avulla ne voivat parantaa ja rakentaa kyberturvallisuusvalmiuksiaan sekä strategisella että toiminnallisella tasolla.

Sellaisen käytännönläheisemmän toimintatavan avulla, joka perustuu ENISAn tekemiin eri jäsenvaltioiden kyberturvallisuudesta vastaavien useiden virastojen haastatteluihin, havaittiin ja nousi esiin seuraavat etunäkökohdat kansallisten valmiuksien arviointikehyksessä:

- saadaan hyödyllistä tietoa pitkäaikaisen strategian kehittämistä varten (esim. hyviä käytäntöjä ja suuntaviivoja);
- tunnistetaan kansallisen kyberturvallisuusstrategian puutteita;
- kehitetään kyberturvallisuusvalmiuksia edelleen;
- tuetaan poliittisten toimien vastuullisuutta;
- lisätään uskottavuutta suuren yleisön ja kansainvälisten kumppaneiden keskuudessa;

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468–486.

- tuetaan tiedotusta ja vahvistetaan julkista kuvaa avoimena organisaationa;
- ennakoidaan tulevia ongelmia;
- tunnistetaan kokemuksia ja parhaita käytäntöjä;
- tarjotaan EU:n laajuiset perustason kyberturvallisuusvalmiudet keskustelujen edistämistä varten; ja
- arvioidaan kyberturvallisuutta koskevia kansallisia valmiuksia.

3. KANSALLISTEN VALMIUKSIEN ARVIOINTIKEHYKSEN METODOLOGIA

3.1 TARKOITUS

Kansallisten valmiuksien arviointikehyksen **päätavoitteena** on mitata **jäsenvaltioiden** kyberturvallisuusvalmiuksien kypsyystaso ja tukea jäsenvaltioita kansallisten kyberturvallisuusvalmiuksien arvioinnissa, maan kypsyystasoa koskevan tietämyksen parantamisessa, kehitysalueiden tunnistamisessa ja kyberturvallisuusvalmiuksien kehittämisessä.

3.2 KYPSYYSTASOT

Kehys perustuu **viiteen kypsyystasoon**, joilla määritellään vaiheet, jotka jäsenvaltiot läpikäyvät kehittäessään kyberturvallisuusvalmiuksia kansallisen kyberturvallisuusstrategian tavoitteiden kattamilla aloilla. Tasot edustavat maturiteetin lisääntymistä alkaen **tasosta 1**, jolla jäsenvaltioilla ei ole selvästi määritettyä kyberturvallisuusvalmiuksien kehittämistä koskevaa lähestymistapaa kansallisen kyberturvallisuusstrategian tavoitteiden kattamilla aloilla, ja päättyen **tasoon 5**, jolla kyberturvallisuusvalmiuksien kehittämisstrategia on dynaaminen ja mukautettavissa ympäristön kehitykseen. Taulukossa 4 esitetään kypsyysasteikko ja kunkin kypsyystason kuvaus.

Taulukko 4: ENISAn kansallisten valmiuksien arviointikehyksen viisitasoinen kypsyysasteikko

TASO 1 – ALKU- / AD HOC -VAIHE	TASO 2 – ALUSTAVA MÄÄRITTELY	TASO 3 – PERUSTAMINEN	TASO 4 – OPTIMOINTI	TASO 5 – MUKAUTTAMINEN
Jäsenvaltiolla ei ole selvästi määritettyä lähestymistapaa kehittää kyberturvallisuusvalmiuksia kansallisen kyberturvallisuusstrategian tavoitteiden kattamilla aloilla. Se saattaa kuitenkin olla asettanut yleisiä tavoitteita ja tehnyt joitakin (teknisiä, poliittisia tai menettelytapaa koskevia) tutkimuksia kansallisten valmiuksien parantamiseksi.	Kansallinen lähestymistapa valmiuksien kehittämiseksi kansallisen kyberturvallisuusstrategian tavoitteiden kattamilla aloilla on määritetty. Toimintasuunnitelmat tai toimet tulosten saavuttamiseksi ovat olemassa, mutta ne ovat alkuvaiheessa. Aktiivisia sidosryhmiä on saatettu myös määrittää ja/tai nämä osallistuvat toimintaan.	Toimintasuunnitelma valmiuksien kehittämiseksi kansallisen kyberturvallisuusstrategian tavoitteiden kattamilla aloilla on selkeästi määritetty, ja asiaankuuluvat sidosryhmät tukevat sitä. Käytännöt ja toimet on pantu täytäntöön ja niitä toteutetaan yhdenmukaisesti kansallisella tasolla. Toimet on määritetty ja dokumentoitu, jaetut resurssit ja hallinto on määritetty selvästi ja määräajat on asetettu.	Toimintasuunnitelma a arvioidaan säännöllisesti: se on asetettu etusijalle, optimoitu ja kestävä. Kyberturvallisuusvalmiuksien kehittämistoimien suorituskykyä mitataan säännöllisesti. Toimien toteuttamiseen liittyviä menestystekijöitä, haasteita ja puutteita tunnistetaan.	Kyberturvallisuusvalmiuksien kehittämisstrategia on dynaaminen ja mukautumiskykyinen. Ympäristön kehityksen (teknologinen kehitys, maailmanlaajuiset konfliktit, uudet uhkat jne.) jatkuva huomioiminen edistää kykyä tehdä nopeita päätöksiä ja toimia nopeasti tilanteen parantamiseksi.

3.3 ITSEARVIOINTIKEHYKSEN OSA-ALUEET JA YLEISRAKENNE

Itsearviointikehyksessä on **neljä osa-aluetta**: I) kyberturvallisuuden hallinto ja standardit, II) valmiuksien kehittäminen ja tietämyksen parantaminen, III) lait ja sääntely ja IV) yhteistyö. Kukin osa-alue kattaa valtion kyberturvallisuusvalmiuksien kehittämisen keskeisen aihealueen ja sisältää joukon eri tavoitteita, joita jäsenvaltiot voivat ottaa osaksi kansallisia kyberturvallisuusstrategioitaan. Näitä ovat erityisesti seuraavat:

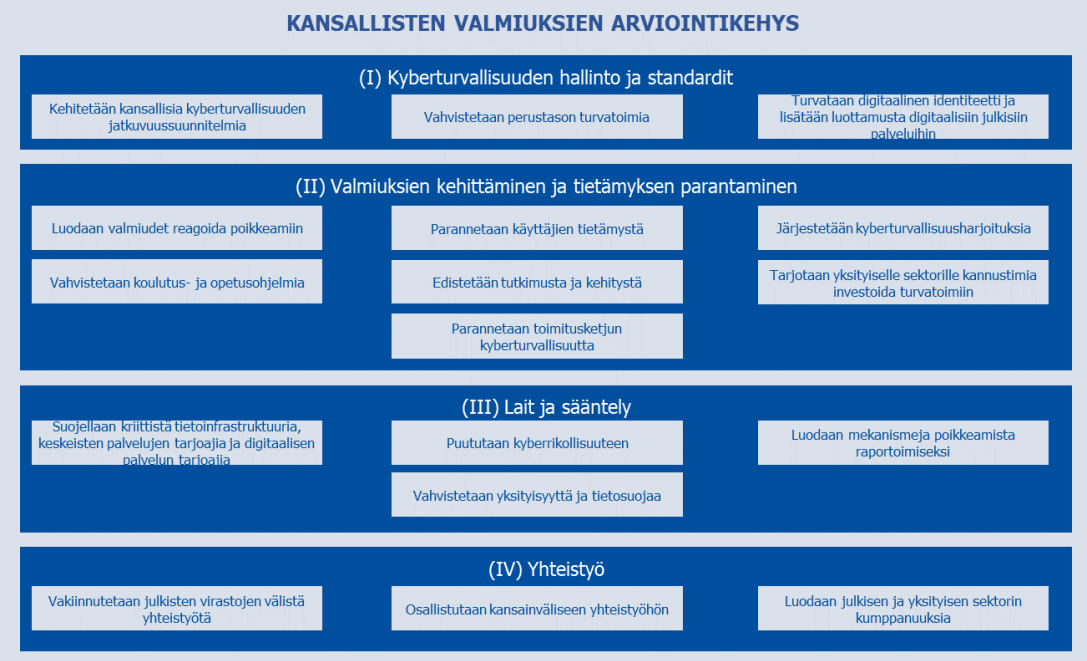
- **(I) Kyberturvallisuuden hallinto ja standardit**: tässä osa-alueessa mitataan jäsenvaltion valmiuksia perustaa kyberturvallisuusalan hyvä hallinto, standardit ja hyvät käytännöt. Tässä ulottuvuudessa tarkastellaan kyberpuolustuksen ja -resilienssin eri näkökulmia ja tuetaan kansallisen kyberturvallisuusalan kehitystä ja lisätään luottamusta hallintoon.
- **(II) Valmiuksien kehittäminen ja tietämyksen lisääminen**: tässä osa-alueessa arvioidaan jäsenvaltioiden valmiuksia lisätä tietämystä kyberriskeistä ja -uhista ja siitä, miten niihin puututaan. Tässä ulottuvuudessa arvioidaan myös maan kykyä kehittää jatkuvasti kyberturvallisuusvalmiuksiaan ja lisätä yleisiä tietoja ja taitoja tällä alalla. Siinä keskitytään kehitykseen kyberturvallisuusmarkkinoilla sekä edistysaskeliin kyberturvallisuuden tutkimuksessa ja kehityksessä **.** Tässä osa-alueessa kootaan yhteen kaikki tavoitteet ja luodaan perusta valmiuksien kehittämisen edistämiselle.
- **(III) Lait ja sääntely**: tässä osa-alueessa mitataan jäsenvaltioiden valmiuksia panna täytäntöön tarvittavat lait ja sääntelyvälineet, joilla puututaan kyberrikollisuuden ja siihen liittyvien kyberpoikkeamien lisääntymiseen ja torjutaan niitä ja suojellaan kriittistä tietoinfrastruktuuria. Tässä ulottuvuudessa arvioidaan myös jäsenvaltioiden valmiuksia laatia oikeudellinen kehys kansalaisten ja yritysten suojelemiseksi esimerkiksi turvallisuuden tasapainottamiseksi yksityisyyden osalta.
- **(IV) Yhteistyö:** tässä osa-alueessa arvioidaan eri kansallisten ja kansainvälisten sidosryhmien yhteistyötä ja tietojenvaihtoa tärkeänä välineenä, jonka avulla voidaan ymmärtää jatkuvasti muuttuvaa uhkaympäristöä entistä paremmin ja vastata siihen.

Malliin sisällytetyt tavoitteet ovat sellaisia, joita jäsenvaltiot ovat yleisesti ottaneet käyttöön, ja ne on valittu 2.2 kohdassa luetelluista tavoitteista. Mallissa arvioidaan erityisesti seuraavia tavoitteita:

- 1. Kehitetään kansallisia kyberturvallisuuden jatkuvuussuunnitelmia (I)
- 2. Vahvistetaan perustason turvatoimia (I)
- 3. Turvataan digitaalinen identiteetti ja kehitetään luottamusta digitaalisiin julkisiin palveluihin (I)
- 4. Luodaan valmiudet reagoida poikkeamiin (II)
- 5. Lisätään käyttäjien tietämystä(II)
- 6. Järjestetään kyberturvallisuusharjoituksia (II)
- 7. Vahvistetaan koulutus- ja opetusohjelmia (II)
- 8. Edistetään tutkimusta ja kehitystä (II)
- 9. Tarjotaan yksityiselle sektorille kannustimia investoida turvatoimiin (II)
- 10. Parannetaan toimitusketjun kyberturvallisuutta (II)
- 11. Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia (III)
- 12. Puututaan kyberrikollisuuteen (III)
- 13. Perustetaan poikkeamista raportoinnin mekanismeja (III)
- 14. Vahvistetaan yksityisyyttä ja tietosuojaa (III)
- 15. Vakiinnutetaan julkisten virastojen välistä yhteistyötä (IV)
- 16. Osallistutaan kansainväliseen yhteistyöhön (IV)
- 17. Perustetaan julkisen ja yksityisen sektorin kumppanuuksia (IV)

Mallissa yhdistetään neljä osa-aluetta ja niiden tavoitteet, jotta saadaan kokonaisvaltainen näkemys jäsenvaltioiden kyberturvallisuusvalmiuksien maturiteetista. Kaaviossa 1 esitetään itsearviointikehyksen yleisrakenne ja se, miten nämä osat, eli tavoitteet, osa-alueet ja itsearviointikehys, liittyvät maan suorituskyvyn arviointiin.

Kaavio 1: Itsearviointikehyksen rakenne



Jokaiselle itsearviointikehyksen tavoitteelle on indikaattoreja, jotka on jaettu viidelle kypsyystasolle. Jokainen indikaattori perustuu dikotomiseen (kyllä/ei) kysymykseen. Indikaattori voi olla ehto, jonka tulee tietyllä tasolla täyttyä.

3.4 ARVIOINTIMEKANISMI

Itsearviointikehyksen **arviointimekanismissa** otetaan huomioon edellä mainitut osat ja 3.5 kohdassa luetellut periaatteet. Itseasiassa malli antaa pistemäärän, joka perustuu kahden parametrin eli **kypsyystason** ja **kattavuuden** arvoon. Kumpikin parametri voidaan laskea eri tasoilla: i) tavoitetta kohti, ii) tavoitteiden osa-aluetta kohti tai iii) yleisesti.

Tavoitetason pistemäärät

Kypsyystason pistemäärä antaa yleiskuvan kypsyystasosta osoittamalla, mitä valmiuksia ja käytäntöjä on otettu käyttöön. Kypsyystason pistemäärä lasketaan korkeimpana tasona, jolla vastaaja täyttää kaikki vaatimukset (eli KYLLÄ-vastaus kaikkiin vaatimus-kysymyksiin) sen lisäksi, että kaikki edellisten kypsyystasojen vaatimukset täyttyvät.

Kattavuudella osoitetaan kaikkien sellaisten indikaattorien kattavuus, joita koskeva vastaus on myönteinen tasoon katsomatta. Se on täydentävä arvo, jossa otetaan huomioon kaikki tavoitteen mittausindikaattorit. Kattavuus lasketaan tavoitetta koskevien kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välisenä suhteena.

On tärkeää selventää, että tästä eteenpäin termillä ***pistemäärä*** tarkoitetaan sekä kypsyystason että kattavuuden arvoja.

Kaavio 2 – Tavoitekohtaisella arviointimekanismilla havainnollistetaan 3.1 kohdassa kuvailtua arviointimenetelmää, jota kehitetään edelleen jäljempänä.

Kaavio 2: Tavoitekohtainen arviointimekanismi

Kaaviossa 2 on esimerkki siitä, miten kypsyystaso lasketaan tavoitteen osalta. On hyvä huomata, että vastaaja täytti kaikki kolmen ensimmäisen kypsyystason vaatimukset ja täytti vain osin tason 4 vaatimukset. Näin ollen pistemäärästä käy ilmi, että ***vastaajan kypsyystaso on tavoitteen "järjestetään kyberturvallisuusharjoituksia" osalta taso 3****.*

Kaaviossa 2 esitetyssä esimerkissä tavoitteen kypsyystasossa ei kuitenkaan pystytä ottamaan huomioon sellaisten indikaattorien antamia tietoja, joiden pistemäärä on positiivinen ja jotka ovat kypsyystason 3 yläpuolella. Siinä tapauksessa kattavuus voi antaa yleiskuvan kaikista osista, joita vastaaja käytti saavuttaakseen kyseisen tavoitteen todellisesta kypsyystasosta huolimatta. Tässä tapauksessa tavoitetta koskevien kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välinen suhde on 19/27 eli ***kattavuusarvo on 70 prosenttia.***

Jotta voitaisiin mukautua jäsenvaltioiden erityispiirteisiin ja samalla saadaan johdonmukainen kuva, pistemäärä lasketaan myös kahdesta eri otannasta osa-alueen tasolla ja yleisellä tasolla:

- **Yleinen pistemäärä:** yksi kokonainen otanta, joka kattaa kaikki osa-alueen tai koko kehyksen tavoitteet (1–17);
- **Erityinen pistemäärä:** yksi erityinen näyte, joka kattaa vain jäsenvaltion valitsemat osa-alueen tai koko kehyksen tavoitteet (vastaavat yleensä kyseisen maan kansallisen kyberturvallisuusstrategian tavoitteita).

Osa-alueen pistemäärät

Kunkin osa-alueen yleinen kypsyystaso lasketaan kyseisen osa-alueen kaikkien tavoitteiden kypsyystason aritmeettisena keskiarvona.

Kunkin osa-alueen erityinen kypsyystaso lasketaan jäsenvaltion arvioitavaksi valitsemien osa-alueen tavoitteiden (vastaavat yleensä kyseisen maan kansallisessa kyberturvallisuussuunnitelmassa olevia tavoitteita) kypsyystason aritmeettisena keskiarvona.

Esimerkiksi kaaviosta 1 käy ilmi, että osa-alueella (I) ”kyberturvallisuuden hallinto ja standardit” on kolme tavoitetta. Jos oletetaan, että vastaaja valitsi arvioitaviksi vain kaksi ensimmäistä tavoitetta mutta ei kolmatta, ja jos oletetaan, että kahden ensimmäisen tavoitteen kypsyystasot ovat 2 ja 4, osa-alueen kypsyystaso kaikki tavoitteet huomioiden on taso 2 (osa-alueen (I) yleinen kypsyystaso = (2+4)/3. Osa-alueen kypsyystaso, kun huomioon otetaan vain arvioijan valitsemat erityistavoitteet, on taso 3 (osa-alueen (I) erityinen kypsyystaso = (2+4)/2).

Kunkin osa-alueen yleinen kattavuus lasketaan osa-alueen kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välisenä suhteena.

Kunkin osa-alueen erityinen kattavuus lasketaan jäsenvaltion arvioitaviksi valitsemia tavoitteita (vastaavat yleensä kyseisen maan kansallisessa kyberturvallisuusstrategiassa olevia tavoitteita) koskevien osa-alueen kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välisenä suhteena.

Yleiset pistemäärät

Maan yleinen kokonaiskypsyystaso lasketaan kehyksen kaikkien tavoitteiden (1–17) kypsyystason aritmeettisena keskiarvona.

Maan erityinen kokonaiskypsyystaso lasketaan jäsenvaltion arvioitaviksi valitsemien kehyksen tavoitteiden (vastaavat yleensä kyseisen maan kansallisessa kyberturvallisuussuunnitelmassa olevia tavoitteita) kypsyystason aritmeettisena keskiarvona.

Maan yleinen kokonaiskattavuus lasketaan kehyksen kaikkia tavoitteita (1–17) koskevien kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välisenä suhteena.

Maan erityinen kokonaiskattavuus lasketaan jäsenvaltion arvioitaviksi valitsemia tavoitteita (vastaavat yleensä kyseisen maan kansallisessa kyberturvallisuusstrategiassa olevia tavoitteita) koskevan kehyksen kysymysten kokonaismäärän ja myönteisen vastauksen saaneiden kysymysten määrän välisenä suhteena.

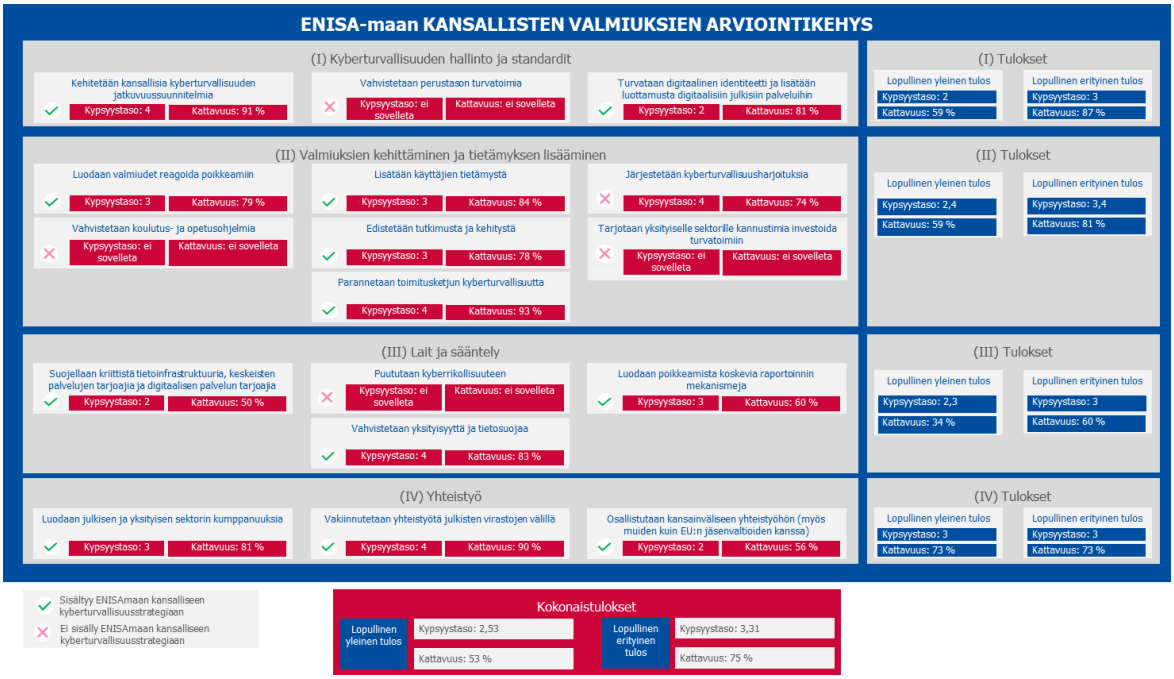
Kunkin indikaattorin osalta vastaajien on mahdollista valita vastauksessaan kolmas vaihtoehto ”en osaa sanoa / ei sovelleta”. Tässä tapauksessa indikaattoria ei huomioida tulosten kokonaislaskelmassa.

Osa-alueen ja yleisen tason kypsyystasot lasketaan keskiarvona, jotta nähdään kahden arvioinnin välinen edistyminen. Vaihtoehtoisella laskentatavalla, jossa osa-alueen ja yleisen tason kypsyystasot lasketaan vähiten kypsän tavoitteen kypsyystasona, ei pystytä kuvaamaan edistystä muiden tavoitteiden kattamilla alueilla, vaikka tulos on maturiteetin kannalta tärkeä.

Koska osa-alue ja yleinen taso yhdistetään raportointia varten, käyttöön on valittu keskiarvo. Tarkempien tulosten saamiseksi raportoinnissa käytetään tavoitetason pistemääriä.

Kaaviossa 3 esitetään yhteenveto arviointimekanismeista mallin eri tasoilla (tavoite, osa-alue ja yleinen).

Kaavio 3: Yleinen arviointimekanismi



3.5 ITSEARVIOINTIKEHYSTÄ KOSKEVAT VAATIMUKSET

Tässä osassa kuvailtu kansallisten valmiuksien arviointikehys perustuu jäsenvaltioiden esiin tuomiin tarpeisiin ja rakentuu seuraavassa lueteltujen vaatimusten ympärille:

- Jäsenvaltio käyttää kansallisten valmiuksien arviointikehystä vapaaehtoisesti itsearviointikehyksenä;
- Kansallisten valmiuksien arviointikehyksen tarkoituksena on mitata jäsenvaltioiden kyberturvallisuusvalmiuksia 17 tavoitteen osalta. Jäsenvaltio voi kuitenkin valita tavoitteet, joita se haluaa arvioida, ja arvioida vain osan 17:stä tavoitteesta;
- Itsearviointikehyksen tarkoituksena on mitata jäsenvaltion kyberturvallisuusvalmiuksien kypsyyttä;
- Arvioinnin tuloksia ei julkaista, ellei jäsenvaltio päätä julkaista niitä omasta aloitteestaan;
- Jäsenvaltio voi esittää arvioinnin tulokset esittämällä maan kyberturvallisuusvalmiuksien, tavoitteiden osa-alueen tai jopa yksittäisen tavoitteen kypsyystason;
- Kaikki arvioitavat tavoitteet ovat yhtä merkityksellisiä arviointikehyksessä, joten ne ovat yhtä tärkeitä. Sama koskee kehyksessä käytettyjä indikaattoreja; ja
- Jäsenvaltio pystyy seuraamaan edistymistään ajan kuluessa.

Itsearviointikehyksen tarkoituksena on tukea jäsenvaltioita kyberturvallisuusvalmiuksien kehittämisessä, minkä vuoksi siihen sisältyy myös suosituksia tai suuntaviivoja, joilla eurooppalaisia maita ohjataan kypsyystason parantamisessa.

On huomattava, että suositukset tai suuntaviivat ovat yleisiä ja perustuvat ENISAn julkaisuihin ja muista maista saatuihin kokemuksiin ja itsearvioinnin tulokseen.

4. KANSALLISTEN VALMIUKSIEN ARVIOINTIKEHYKSEN INDIKAATTORIT

4.1 KEHYKSEN INDIKAATTORIT

Tässä osassa käsitellään ENISAn kansallisten valmiuksien arviointikehyksen indikaattoreja. Seuraavat kohdat on järjestetty osa-alueittain.

Kunkin osa-alueen osalta taulukossa esitetään kattavasti kaikki indikaattorit kyseistä kypsyystasoa vastaavien kysymysten muodossa. Kyselylomake on itsearvioinnin tärkein väline. Kullekin tavoitteelle on kahdenlaisia indikaattoreja:

- yleiset strategian kypsyyttä koskevat kysymykset (yhdeksän yleistä kysymystä), jotka on merkitty kirjaimilla a–c kunkin kypsyystason osalta ja jotka toistuvat jokaisen tavoitteen kohdalla
- kyberturvallisuusvalmiuksia koskevat kysymykset (319 kyberturvallisuusvalmiuksia koskevaa kysymystä), jotka on merkitty numeroilla 1–10 kunkin kypsyystason osalta ja jotka ovat erityisiä tavoitteen kattamalle alueelle.

Jokainen kysymys on merkitty merkillä (0–1), jolla ilmaistaan, onko kysymys kypsyystason osalta vaatimusindikaattori (1) vai ei-vaatimusindikaattori (0).

Jokainen kysymys voidaan tunnistaa tunnistenumerolla, joka koostuu

- tavoitteen numerosta
- kypsyystasosta
- kysymyksen numerosta.

Esimerkiksi kysymys numero 1.2.4 on strategisen tavoitteen (I) ”kehitetään kansallisia kyberturvallisuuden jatkuvuussuunnitelmia” kypsyystason 2 neljäs kysymys.

On syytä huomata, että kaikki kysymykset koskevat kansallista tasoa, ellei toisin mainita. Kaikki kysymykset osoitetaan jäsenvaltiolle yleisesti eikä arvioinnin suorittavalle yksittäiselle elimelle tai hallintoelimelle.

Tavoitteiden määritelmät esitetään 2.2 luvussa - Eurooppalaisissa kansallisissa kyberturvallisuusstrategioissa tunnistetut yleiset tavoitteet.

4.1.1 Osa-alue 1: Kyberturvallisuuden hallinto ja standardit

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
1 – Kehitetään kansallisia kyberturvallisuuden jatkuvuussuunnitelmia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko kansallisten kyberturvallisuuden jatkuvuussuunnitelmien laatiminen aloitettu? Esim. jatkuvuussuunnitelmien yleisten tavoitteiden, laajuuden ja/tai periaatteiden suunnittelu.	1	Onko teillä periaatetta / kansallista strategiaa, johon kyberturvallisuus sisältyy kriisitekijänä (esim. suunnitelmaa, politiikkaa jne.)?	1	Onko teillä kansallisen tason kyberturvallisuuskriisien hallintasuunnitelmaa?	1	Oletteko tyytyväinen kansalliseen kyberturvallisuuden jatkuvuussuunnitelmaan kuuluvien kriittisten alojen määrään tai prosenttiosuuteen?	1	Onko teillä kyberturvallisuusharjoituksia tai varsinaisia kansallisen tason kriisejä koskevaa kokemusten analysointimenettelyä?	1
	2	Onko yleisesti tiedossa, että kyberhäiriöt ovat kriisitekijä, joka saattaa uhata kansallista turvallisuutta?	0	Onko teillä keskusta, jolta voi saada tietoa ja joka tiedottaa asioista päätöksentekijöille? Esim. menetelmiä, foorumeita tai paikkoja, joilla varmistetaan, että kaikilla kriisinhallintaan osallistuvilla toimijoilla on kyberturvallisuuskriisistä samat, reaaliaikaiset tiedot.	1	Onko teillä kansallisen tason kyberturvallisuuskriisiä koskevia menettelyjä?	1	Järjestättekö kansalliseen kyberturvallisuuden jatkuvuuden suunnitteluun liittyviä toimia (esim. harjoituksia) tarpeeksi usein?	1	Onko teillä menettelyä, jolla kansallista suunnitelmaa testataan säännöllisesti?	1
	3	Oletteko toteuttaneet (teknisiä, operationaalisia tai poliittisia) tutkimuksia kyberturvallisuuden jatkuvuuden suunnittelun alalla?	0	Onko teillä asiaankuuluvia resursseja, jotka osallistuvat kansallisten kyberturvallisuuden jatkuvuussuunnitelmien kehittämisen ja toteuttamisen valvontaan?	1	Onko teillä viestintäryhmää, joka on koulutettu erityisesti vastaamaan kyberturvallisuuskriiseihin ja kertomaan niistä suurelle yleisölle?	1	Onko kriisiratkaisun suunniteluun, kokemusten tutkimiseen ja muutosten toteuttamiseen nimitetty tarpeeksi henkilöitä?	1	Onko teillä riittävät välineet ja alustat tilannetietämyksen lisäämiseksi?	1

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	
1 – Kehitetään kansallisia kyberturvallisuuden jatkuvuussuunnitelmia	4	-		Onko teillä kansallisen tason kyberturvallisuusuhkien arviointimenetelmiä, joihin sisältyy vaikutusarviointimenettelyjä?	0	Osallistuvatko kaikki asiaankuuluvat kansalliset sidosryhmät (kansallinen turvallisuus, puolustus, pelastuspalvelu, lainvalvonta, ministeriöt, viranomaiset jne.) suunnitteluun?	1	Onko teillä riittävästi henkilöitä, jotka on koulutettu vastaamaan kansallisen tason kyberturvallisuuskriiseihin?	1	Noudatatteko kyberturvallisuuden jatkuvuussuunnitelman seurannassa ja parantamisessa jotakin tiettyä kypsyysmallia?	0
	5	-		-		Onko teillä riittävästi kriisinhallintatiloja ja tilannekeskuksia?	1	-		Onko teillä resursseja, jotka ovat erikoistuneet joko uhkien ennakointiin tai kyberturvallisuutta koskevien tulevien kriisien tai haasteiden ratkaisemiseen?	0
	6	-		-		Kuuletteko tarvittaessa EU:ssa olevia kansainvälisiä sidosryhmiä?	0	-		-	
	7	-		-		Kuuletteko tarvittaessa EU:n ulkopuolisia kansainvälisiä sidosryhmiä?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	
2 – Vahvistetaan perustason turvatoimia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	
2 – Vahvistetaan perustason turvatoimia	1	Oletteko tehneet tutkimusta, jossa määritetään **julkisia** organisaatioita koskevia vaatimuksia ja puutteita kansainvälisesti tunnustettuihin standardeihin perustuen? Esim. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC tai CIS.	1	Onko turvatoimet laadittu kansainvälisten/kansallisten standardien mukaisesti?	1	Ovatko perustason turvatoimet pakollisia?	1	Onko teillä menettelyä, jolla perustason turvatoimia päivitetään usein?	1	Onko teillä menettelyä, jolla tieto- ja viestintätekniikka voidaan turvata, kun toimilla ei pystytä puuttumaan poikkeamiin?	1
	2	Oletteko tehneet tutkimusta, jossa määritetään **yksityisiä** organisaatioita koskevia vaatimuksia ja puutteita kansainvälisesti tunnustettuihin standardeihin perustuen? Esim. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC tai CIS.	1	Onko yksityisen sektorin sidosryhmiä ja muita sidosryhmiä kuultu perustason turvatoimien määrittämisessä?	1	Sovellatteko horisontaalisia turvatoimia kriittisillä aloilla?	1	Onko teillä valvontamenettelyä, jolla perustason turvatoimien käyttöä voidaan tutkia?	1	Arvioitteko uhkaympäristön uuden kehityksen mukaisesti laadittujen uusien standardien tarkoituksenmukaisuutta?	1
	3	-		-		Sovellatteko alakohtaisia turvatoimia kriittisillä aloilla?	1	Onko teillä kansallista viranomaista, joka tarkastaa, että perustason turvatoimet on pantu täytäntöön?	1	Onko teillä kansallista koordinoitua haavoittuvuuksien julkistamismenettelyä tai edistättekö tällaisen menettelyn käyttöä?	1
	4	-				Ovatko perustason turvatoimet asiaankuuluvien sertifiointijärjestelmien mukaisia?	1	Onko teillä menettelyä, jolla tunnistetaan vaatimuksia noudattamattomia organisaatioita tietyn ajanjakson aikana?	1	-	
	5	-		-		Onko teillä perustason turvatoimia koskevien riskien itsearviointimenettelyä?	1	Onko teillä tarkastusmenettelyä, jolla varmistetaan, että turvatoimia sovelletaan asianmukaisesti?	1	-	
	6	-		-		Arvioitteko pakollisia perustason turvatoimia hallintoelinten hankintamenettelyissä?	0	Määritteletteköturvallisuusstandardit kriittisten tietotekniikan / käytännön tekniikan tuotteiden (lääketieteellisten laitteiden, kytkettyjen ja itseohjautuvien ajoneuvojen, ammattikäytössä olevien radiolaitteiden, raskaan teollisuuden laitteiden ym.) kehittämiselle tai rohkaisetteko aktiivisesti tällaisten standardien käyttöönottoon?	0	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
3 – Turvataan digitaalinen identiteetti ja lisätään luottamusta digitaalisiin julkisiin palveluihin	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Oletteko tehneet tutkimuksia tai puuteanalyyseja, joiden on tarkoitus määrittää tarpeet varmistaa digitaaliset julkiset palvelut kansalaisille ja yrityksille?	1	Teettekö riskianalyyseja varojen tai palvelujen riskiprofiilin määrittämiseksi ennen kuin siirrätte ne pilveen tai liitätte ne osaksi digitaalista muuntamista koskevia hankkeita?	1	Edistättekö sisäänrakennettua yksityisyyden suojaa koskevia menetelmiä kaikissa sähköisen hallinnon hankkeissa?	1	Keräättekö indikaattoreja digitaalisten julkisten palvelujen järjestelmämurtoja koskevista kyberpoikkeamista?	1	Osallistutteko eurooppalaisiin työryhmiin, joissa ylläpidetään luottamuspalvelujen (sähköisten allekirjoitusten, sähköisten leimojen, sähköisesti rekisteröityjen toimituspalvelujen, aikaleimojen ja verkkosivustojen todentamisen) laatua ja/tai suunnitellaan niille uusia vaatimuksia? Esim. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU jne.	1
	2	-		Onko teillä kansalaisia ja yrityksiä koskevien, kansallisten sähköisen tunnistamisen järjestelmien rakentamista tai edistämistä koskeva strategia?	1	Osallistuvatko yksityiset sidosryhmät turvallisten digitaalisten julkisten palvelujen suunnitteluun ja tarjoamiseen?	1	Sovellatteko sähköisen tunnistamisen tapojen vastavuoroista tunnustamista muiden jäsenvaltioiden kanssa?	1	Osallistutteko aktiivisesti vertaisarviointeihin osana Euroopan komissiolle tehtäviä sähköisen tunnistamisen järjestelmiä koskevia ilmoituksia?	1
	3	-		Onko teillä kansalaisia ja yrityksiä koskevien turvallisten kansallisten luottamuspalvelujen (sähköisten allekirjoitusten, sähköisten leimojen, sähköisesti rekisteröityjen toimituspalvelujen, aikaleimojen ja verkkosivujen todentamisen) rakentamista tai edistämistä koskeva strategia?	1	Sovellatteko turvallisuutta koskevia vähimmäisvaatimuksia kaikissa digitaalisissa julkisissa palveluissa?	1	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
3 – Turvataan digitaalinen identiteetti ja lisätään luottamusta digitaalisiin julkisiin palveluihin	4	-		Onko teillä hallintopilveä koskeva strategia (pilvipalvelustrategia, joka koskee hallintoelimiä ja julkisia elimiä kuten ministeriöitä, hallituksen virastoja ja julkishallintoa), jossa otetaan huomioon turvallisuuteen kohdistuvat vaikutukset?	0	Onko kansalaisten ja yritysten käytössä sähköisen tunnistamisen järjestelmiä, joiden varmuustaso on korotettu tai korkea eIDAS-asetuksen (EU) N:o 910/2014 liitteessä määritellyn mukaisesti?	1	-		-	
	5	-		-		Onko teillä digitaalisia julkisia palveluja, joissa vaaditaan sähköisen tunnistamisen järjestelmiä, joiden varmuustaso on korotettu tai korkea eIDAS-asetuksen (EU) N:o 910/2014 liitteessä määritellyn mukaisesti?	1	-		-	
	6	-		-		Onko teillä luottamuspalveluja (sähköisiä allekirjoituksia, sähköisiä leimoja, sähköisesti rekisteröityjä toimituspalveluja, aikaleimoja ja verkkosivujen todentamista) kansalaisille ja yrityksille tarjoavia tahoja?	1	-		-	
	7	-		-		Edistättekö perustason turvatoimien käyttöönottoa kaikissa pilvipalvelumalleissa (esim. yksityisessä, julkisessa, yhdistelmässä, infrastruktuuripalvelussa, alustapalvelussa ja sovelluspalvelussa)?	0	-		-	

4.1.2 Osa-alue 2: Valmiuksien kehittäminen ja tietämyksen parantaminen

Kansallisen kyberturvallisuusstrategian tavoite	nro	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
4 – Luodaan valmiudet reagoida poikkeamiin	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko teillä epävirallisia reagointivalmiuksia, joita hallitaan julkisella ja yksityisellä sektorilla tai näiden yhteistyönä?	1	Onko teillä vähintään yksi virallinen kansallinen tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö (CSIRT-toimija)?	1	Onko teillä reagointivalmiuksia verkko- ja tietoturvadirektiivin liitteessä II mainituilla aloilla?	1	Oletteko määrittäneet poikkeamiin reagoimisen menetelmiä ja poikkeamien luokittelujärjestelmiä koskevia standardoituja menettelyjä ja edistäneet niiden käyttöä?	1	Onko teillä mekanismeja nollapäivähaavoittuvuuden aikaista havaitsemista, tunnistamista, ehkäisemistä, torjumista ja lieventämistä varten?	1
	2	-		Onko kansallisilla CSIRT-toimijoilla selvästi määritetty toiminta-ala? Esim. kohteena olevan sektorin, poikkeaman tyyppien ja vaikutusten mukaan.	1	Onko maassanne CSIRT-toimijoiden yhteistyömekanismia poikkeamiin reagoimista varten?	1	Arvioitteko reagointivalmiuksianne, jotta varmistatte, että teillä on riittävät resurssit ja ammattitaito verkko- ja tietoturvadirektiivin liitteessä I olevassa 2 kohdassa tarkoitettujen tehtävien toteuttamiseksi?	1	-	
	3	-		Onko kansallisilla CSIRT-toimijoilla selvästi määritetyt suhteet muihin kansallisiin sidosryhmiin (esim. lainvalvontaviranomaisiin, puolustusvoimiin, internetpalveluntarjoajiin ja kansalliseen kyberturvallisuuskeskukseen) kansallisen kyberturvallisuusympäristön ja reagointimenettelyjen osalta?	0	Onko kansallisilla CSIRT-toimijoilla verkko- ja tietoturvadirektiivin liitteen I mukaisia reagointivalmiuksia? Esim. saatavuus, fyysinen turvallisuus, toiminnan jatkuvuus, kansainvälinen yhteistyö, poikkeamien seuranta, ennakkovaroitus- ja varoitusvalmiudet, poikkeamiin reagointi, riskianalyysi ja tilannetietoisuus, yhteistyö yksityisen sektorin kanssa, standardoidut toimintatavat jne.	1	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
4 – Luodaan valmiudet reagoida poikkeamiin	4	-				Onko teillä poikkeamia koskeva yhteistyömekanismi naapurimaiden kanssa?	1	-		-	
	5	-		-		Oletteko määrittäneet virallisesti selkeät poikkeamien käsittelytavat ja -menettelyt?	1	-		-	
	6	-		-		Osallistuvatko kansalliset CSIRT-toimijat sekä kansallisiin että kansainvälisiin kyberturvallisuusharjoituksiin?	1	-		-	
	7	-		-		Ovatko kansalliset CSIRT-toimijat yhteydessä FIRSTiin (poikkeamiin reagoivien työryhmien ja turvallisuustyöryhmien foorumiin)?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
5 – Parannetaan käyttäjien tietämystä	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
5 – Lisätään käyttäjien tietämystä	1	Ovatko hallitus, yksityinen sektori ja tavalliset käyttäjät ainakin hivenen sitä mieltä, että kyberturvallisuutta ja yksityisyyttä koskevaa tietämystä olisi tarpeen lisätä?	1	Onko kohdeyleisö käyttäjien tietämyksen parantamiseksi määritetty? Esim. tavalliset käyttäjät, nuoret, yrityskäyttäjät (jotka voidaan jakaa edelleen seuraaviin: pk-yritykset, keskeisten palvelujen tarjoajat, digitaalisen palvelun tarjoajat jne.).	1	Onko kampanjoita koskevia viestintäsuunnitelmia/-strategioita kehitetty?	1	Laaditteko suunnitteluvaiheessa mittareita kampanjan arviointia varten?	1	Onko käytössänne mekanismeja, joilla varmistetaan, että valistuskampanjat vastaavat aina teknistä kehitystä, uhkaympäristön muutoksia, säädöksiä ja kansallisia turvallisuusmääräyksiä?	1
	2	Toteuttavatko julkiset virastot kyberturvallisuutta koskevia valistuskampanjoita organisaationsa sisällä tarpeen mukaan? Esim. kyberturvallisuuden häiriötilanteessa.	0	Laaditteko hankesuunnitelman tietämyksen lisäämiseksi tietoturvaa ja yksityisyyttä koskevista asioista?	1	Onko teillä menetelmä sisällön laatimiseksi hallituksen tasolla?	1	Arvioitteko kampanjoitanne toteutuksen jälkeen?	1	Arvioitteko säännöllisesti tai tutkitteko asenteen tai käyttäytymisen muutoksia kyberturvallisuutta ja yksityisyyttä koskevien asioiden osalta yksityisellä ja julkisella sektorilla?	1
	3	Toteuttavatko julkiset virastot suurelle yleisölle suunnattuja kyberturvallisuutta koskevia valistuskampanjoita tarpeen mukaan? Esim. kyberturvallisuuspoikkeaman esiintyessä.	0	Onko teillä käytettävissä olevia ja helposti tunnistettavia resursseja (esim. yksi verkkoportaali ja tietojen lisäämistä koskevat välineet) käyttäjille, jotka haluavat perehtyä kyberturvallisuutta ja yksityisyyttä koskeviin tietoihin?	1	Onko teillä mekanismeja, joilla tunnistetaan tietämyksen parantamisen kohdealueet (esim. ENISAn Threat Landscape -raportti, kansalliset ympäristöt, kansainväliset ympäristöt, kansallisten kyberrikostorjuntakeskusten antama palaute jne.)?	1	Onko käytössä mekanismeja, joilla tunnistetaan kohdeyleisölle tarkoituksenmukaisin tiedotusväline tai viestintäkanava, jotta saavutettavuus ja osallistuminen olisi mahdollisimman suurta? Esim. erityyppiset digitaaliset mediat, esitteet, sähköpostit, opetusmateriaali, julisteet vilkkailla alueilla, televisio, radio jne.	1	Pyydättekö neuvoja käyttäytymisen asiantuntijoilta räätälöidäksenne kampanjan kohdeyleisölle sopivaksi?	1
	4	-		-		Tekevätkö asiantuntija- ja viestintätyöryhmät yhteistyötä sidosryhmien kanssa sisällön laatimisessa?	1			-	
	5	-		-		Osallistuuko yksityinen sektori tietämystä lisääviin toimiinne sanoman edistämiseksi ja saattamiseksi laajemman yleisön tietoon?	1	-		-	
	6	-		-		Laaditteko erityisiä tietämystä lisääviä aloitteita julkisen sektorin, yksityisen sektorin, akateemisen alan tai kansalaisyhteiskunnan johtotasolle?	1	-		-	
	7	-		-		Osallistutteko ENISAn Euroopan kyberturvallisuuskuukauden (ECSM) kampanjoihin?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
6 – Järjestetään kyberturvallisuusharjoituksia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Järjestättekö kriisiharjoituksia muilla aloilla (kuin kyberturvallisuuden alalla) kansallisella tai yleiseurooppalaisella tasolla?	1	Onko teillä kansallisen tason kyberturvallisuusharjoitusohjelmaa ?	1	Osallistuvatko kaikki julkishallinnon asiaankuuluvat virkamiehet toimiin? (vaikka skenaario on alakohtainen)	1	Laaditteko toiminnan jälkeen raportteja/arviointiraportteja?	1	Onko teillä valmiuksia kyberturvallisuutta koskevien kokemusten analysointiin (raportointiprosessit, analyysi, lieventäminen)?	1
	2	Oletteko osoittaneet resursseja kriisinhallintaharjoitusten suunnitteluun?	1	Järjestättekö tai asetatteko etusijalle yhteiskunnan välttämättömiä toimintoja ja kriittistä infrastruktuuria koskevien kyberturvallisuuskriisien hallintaharjoituksia?	1	Osallistuuko yksityinen sektori harjoitusten suunnitteluun ja toteuttamiseen?	1	Testaatteko kansallisen tason suunnitelmia ja menetelmiä?	1	Onko teillä vakiintunut kokemuksia koskeva menettely?	1
	3	-		Oletteko nimenneet koordinointielimen valvomaan kyberturvallisuusharjoitusten suunnittelua (julkisen viraston, konsulttiyrityksen jne.)?	0	Järjestättekö alakohtaisia harjoituksia kansallisella ja/tai kansainvälisellä tasolla?	1	Osallistutteko yleiseurooppalaisiin kyberturvallisuusharjoituksiin?	1	Mukautatteko harjoitusskenaarioita uusimman kehityksen (teknologisen kehityksen, maailmalaajuisten konfliktien, uhkaympäristön jne.) mukaan?	1
	4	-		-		Järjestättekö harjoituksia kaikilla verkko- ja tietoturvadirektiivin liitteessä II mainituilla kriittisillä aloilla?	1	-		Yhdenmukaistatteko kriisinhallintamenettelyjänne muiden jäsenvaltioiden kanssa tehokkaan yleiseurooppalaisen kriisihallinnan varmistamiseksi?	1
	5	-		-		Järjestättekö alan sisäisiä ja/tai alojen välisiä kyberturvallisuusharjoituksia?	1	-		Onko käytössänne menettelyä, jolla strategiaa, suunnitelmia ja menetelmiä voidaan muuttaa nopeasti kokemusten perusteella harjoitusten aikana?	0
	6	-		-		Järjestättekö useita tasoja koskevia kyberturvallisuusharjoituksia? (tekninen ja operationaalinen taso, menettelytaso, päätöksentekotaso, poliittinen taso jne.)	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Level 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
7 – Vahvistetaan koulutus- ja opetusohjelmia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Harkitsetteko kyberturvallisuuskoulutus- ja -opetusohjelmien laatimista?	1	Suunnitteletteko kyberturvallisuuskursseja?	1	Sisältyykö kyberturvallisuuskulttuuri maassanne opiskelijoiden koulutuspolkuun sen aikaisessa vaiheessa? Suositteko kyberturvallisuutta esimerkiksi ala- ja yläkoulussa?	1	Rohkaistaanko yksityisen ja julkisen sektorin työntekijöitä hankkimaan akkreditointi tai sertifiointi?	1	Onko käytössänne mekanismeja, joilla varmistetaan, että koulutukset ja koulutusohjelmat vastaavat aina nykyistä ja tulevaa teknistä kehitystä, uhkaympäristön muutoksia, säädöksiä ja kansallisia turvallisuusmääräyksiä?	1
	2	-		Tarjoavatko maanne yliopistot kyberturvallisuusalan tohtorin tutkintoja omana tieteenalanaan eikä osana tietojenkäsittelytiedettä?	1	Onko teillä kyberturvallisuuteen erikoistuneita kansallisia tutkimuslaboratorioita ja koulutuslaitoksia?	1	Onko maanne kehittänyt kyberturvallisuuden koulutus- tai mentorointiohjelmia, joilla tuetaan uusien kotimaisten yritysten perustamista ja kotimaisia pk-yrityksiä?	1	Perustatteko akateemisia kyberturvallisuusalan huippuyksiköitä, jotka toimivat tutkimus- ja koulutuskeskuksina?	1
	3	-		Suunnitteletteko valmentavanne kouluttajia eri aloilta tietoturvallisuutta ja yksityisyyden suojaa koskevissa asioissa? Esim. verkkoturvallisuudessa, henkilötietojen suojassa ja kyberkiusaamisessa.	1	Edistättekö/rahoitatteko kyberturvallisuuskursseja ja -koulutusohjelmia, jotka on tarkoitettu jäsenvaltion työvoimatoimistojen työntekijöille?	1	Edistättekö aktiivisesti tietoturvakurssien lisäämistä korkeakoulutukseen – ei ainoastaan tietojenkäsittelytieteen opiskelijoille vaan myös muiden alojen opiskelijoille? Esim. kyseisen ammatin tarpeita vastaaviksi räätälöidyt kurssit.	1	Osallistuvatko akateemiset laitokset kyberturvallisuuskoulutusta ja -tutkimusta koskevien kansainvälisten keskustelujen johtamiseen?	0
	4	-		-		Tarjotaanko eurooppalaisen tutkintojen viitekehyksen tasoilla 5–8 kyberturvallisuuskursseja ja/tai erikoistuneita opetussuunnitelmia?	1	Arvioitteko tietoturva-alan osaamisvajetta (kyberturvallisuustyöntekijöiden puutetta) säännöllisesti?	1	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
7 - Vahvistetaan koulutus- ja opetusohjelmia	5	-		-		Edistättekö ja/tai tuetteko aloitteita, joilla verkkoturvallisuuskurssit pyritään sisällyttämään osaksi perusasteen ja toisen asteen koulutusta?	1	Edistättekö akateemisten laitosten välistä verkostoitumista ja tietojenvaihtoa sekä kansallisella että kansainvälisellä tasolla?	1		
	6	-		-		Rahoitatteko kansalaisille suunnattua kyberturvallisuusalan peruskoulutusta tai tarjoatteko sitä ilmaiseksi?	0	Osallistuuko yksityinen sektori millään tavalla kyberturvallisuuskoulutusta koskeviin aloitteisiin? Esim. kurssien suunnitteluun ja järjestämiseen, harjoitteluun, työharjoitteluun jne.	1	-	
	7	-		-		Järjestättekö vuotuisia tietoturvatapahtumia (esim. hakkerointikilpailuja tai hackathon-tapahtumia)?	0	Onko teillä rahoitusmekanismeja, joilla edistetään kyberturvallisuustutkintojen suorittamista? Esim. apurahoja, taattuja harjoittelujaksoja, taattuja työpaikkoja tietyllä toimialalla tai tehtäviä julkisella sektorilla.	0	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
8 – Edistetään tutkimusta ja kehitystä	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
8 – Edistetään tutkimusta ja kehitystä											
	1	Oletteko tehneet tutkimuksia tai analyyseja kyberturvallisuutta koskevan tutkimuksen ja kehityksen ensisijaisten tavoitteiden tunnistamiseksi?	1	Onko käytössänne menettely, jolla tutkimuksen ja kehityksen ensisijaisia tavoitteita (esim. uudenlaisten kyberhyökkäysten estämistä, torjumista, havaitsemista ja niihin mukautumista koskevia uusia aihealueita) määritetään?	1	Onko teillä suunnitelma, jolla tutkimus- ja kehitysaloitteet yhdistetään reaalitalouteen?	1	Vastaavatko kyberturvallisuutta koskevat tutkimus- ja kehitysaloitteet asiaa koskevia strategisia tavoitteita, joita ovat esim. digitaaliset sisämarkkinat, Horisontti 2020, Digitaalinen Eurooppa, EU:n kyberturvallisuusstrategia?	1	Tavoitteletteko kansallisella tasolla yhteistyötä kyberturvallisuutta koskevien kansainvälisten tutkimus- ja kehitysaloitteiden kanssa?	1
	2	-		Osallistuuko yksityinen sektori tutkimusta ja kehitystä koskevien ensisijaisten tavoitteiden asettamiseen?	1	Onko teillä kyberturvallisuutta koskevia kansallisia hankkeita?	1	Onko teillä tutkimus- ja kehitysaloitteiden arviointijärjestelmää?	1	Ovatko tutkimusta ja kehitystä koskevat ensisijaiset tavoitteet yhdenmukaisia nykyisen tai tulevan (kansallisen tason) sääntelyn kanssa?	1
	3	-		Osallistuuko akateeminen maailma tutkimusta ja kehitystä koskevien ensisijaisten tavoitteiden asettamiseen?	1	Onko teillä paikallisia/alueellisia uusien yritysten ekosysteemejä tai muita verkostoitumiskanavia (esim. teknologiapuistoja, innovointiklustereita, verkostoitumistapahtumia/-alustoja), joilla edistetään innovointia (myös uusien kyberturvallisuusyritysten keskuudessa)?	1	Onko yliopistojen ja muiden tutkimuslaitosten kanssa tehty yhteistyösopimuksia?	1	Osallistutteko yhtä tai useaa huipputason tutkimusta ja kehitystä koskevien keskustelujen johtamiseen kansainvälisellä tasolla?	0
	4	-		Onko teillä kyberturvallisuuteen liittyviä kansallisia tutkimus- ja kehitysaloitteita?	0	Investoitteko akateemisen maailman ja yksityisen sektorin kyberturvallisuuden tutkimus- ja kehitysohjelmiin?	1	Onko teillä tunnustettu laitos, joka valvoo kyberturvallisuutta koskevia tutkimus- ja kehitystoimia?	0	-	
	5	-		-		Onko yliopistoissanne teollisuustutkimuksen professuureja tutkimusaiheiden ja markkinoiden tarpeiden yhdistämiseksi?	1	-		-	
	6	-		-		Onko teillä kyberturvallisuuden tutkimusta ja kehitystä koskevia rahoitusohjelmia?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Level 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
9 – Tarjotaan yksityiselle sektorille kannustimia investoida turvatoimiin	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko teillä teollisuuspolitiikkaa tai poliittista tahtoa edistää kyberturvallisuusalan kehitystä?	1	Osallistuuko yksityinen sektori kannustimien suunnitteluun?	1	Onko teillä taloudellisia tai sääntelyyn liittyviä tai muunlaisia kannustimia, joilla edistetään kyberturvallisuusinvestointeja?	1	Onko yksityisissä toimijoissa jokin taho, jota reagoi kannustimiin investoimalla turvatoimiin? Esim. kyberturvallisuuteen erikoistuneet sijoittajat ja muut sijoittajat.	1	Keskitättekö kannustimia kyberturvallisuusseikkoihin uhkien viimeisen kehityksen mukaan?	1
	2	-		Oletteko havainneet erityisiä kyberturvallisuusaiheita, joita olisi kehitettävä? Esim. kryptografia, yksityisyys, uusi todentamismuoto, kyberturvallisuutta koskeva tekoäly jne.	0	Tuetteko (esim. verokannustimilla) kyberturvallisuusalan uusia yrityksiä ja pk-yrityksiä?	1	Tarjoatteko kannustimia yksityiselle sektorille, jotta tämä keskittyisi huipputeknologian turvallisuuteen? Esim. 5G, tekoäly, esineiden internet, kvanttilaskenta jne.	1	-	
	3	-		-		Tarjoatteko verokannustimia tai muita taloudellisia motiiveja yksityisen sektorin sijoittajille, jotta nämä investoisivat kyberturvallisuusalan uusiin yrityksiin?	1	–		-	
	4	-		-		Helpotatteko kyberturvallisuusalan uusien yritysten ja pk-yritysten pääsyä julkisiin hankintamenettelyihin?	0	-		-	
	5	-		-		Onko käytettävissänne määrärahoja kannustimien tarjoamiseksi yksityiselle sektorille?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
10 – Parannetaan toimitusketjun kyberturvallisuutta	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Oletteko tehneet tutkimuksen toimitusketjun hallinnan turvallisuutta koskevista hyvistä käytännöistä, joita on käytetty hankinnoissa useilla elinkeinoelämän toimialoilla ja/tai julkisella sektorilla?	1	Arvioitteko (verkko- ja tietoturvadirektiivin (2016/1148) liitteessä II määritettyjen) kriittisten alojen tieto- ja viestintätekniikkapalvelujen ja -tuotteiden koko toimitusketjun kyberturvallisuutta?	1	Onko käytössänne turvallisuussertifiointijärjestelmä tieto- ja viestintätekniikkaan perustuville tuotteille ja palveluille? Esim. SOG-ISia koskeva MRA-sopimus Euroopassa (johtavien virkamiesten tietoturvallisuusryhmä, vastavuoroista tunnustamista koskeva sopimus), common criteria -sertifikaattien tunnustamisjärjestely (CCRA), kansalliset aloitteet, alakohtaiset aloitteet jne.	1	Onko käytössänne menettely, jolla päivitätte (verkko- ja tietoturvadirektiivin (2016/1148) liitteessä II määritettyjen) kriittisten alojen tieto- ja viestintätekniikkapalvelujen ja -tuotteiden koko toimitusketjun kyberturvallisuuden arviointeja?	1	Onko käytössänne välineitä, joilla tutkitte toimitusketjun tärkeimpiä osia havaitaksenne viitteet heikkouksista varhaisessa vaiheessa? Esim. ISP-tason turvavalvontatoimenpiteet, tärkeimpien infrastruktuuriosien turvallisuusvälineet jne.	1
	2	-		Sovellettako standardeja julkishallinnon hankintapolitiikassa, jotta varmistatte, että tieto- ja viestintätekniikkatuotteiden tai -palvelujen tarjoajat noudattavat perustason tietoturvavaatimuksia? Esim. ISO/IEC 27001 ja 27002, ISO/IEC 27036 jne.	1	Edistättekö aktiivisesti turvallisuutta ja sisäänrakennettua yksityisyyden suojaa koskevia parhaita käytäntöjä tieto- ja viestintätekniikkatuotteiden ja -palvelujen kehityksessä? Esim. turvallinen ohjelmistokehityksen elinkaari ja esineiden internetin elinkaari.	1	Onko käytössänne menettely, jolla havaitsette (verkko- ja tietoturvadirektiivin (2016/1148) liitteessä II määritettyjen) kriittisten alojen toimitusketjun heikkouksia?	1	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
10 – Parannetaan toimitusketjun kyberturvallisuutta	3	-		-		Kehitättekö ja tarjoatteko keskitettyjä luetteloja, joissa on laajennettua tietoa pk-yrityksiin skaalattavista ja näiden soveltamista nykyisistä tietoturvaa ja yksityisyyttä koskevista standardeista?	1	Onko käytössänne mekanismeja, joilla varmistatte, että keskeisten palvelujen tarjoajille kriittiset tieto- ja viestintätekniikkatuotteet ja -palvelut ovat kyberkestäviä (esim. pystyvät pitämään yllä käytettävyyttä ja turvallisuutta kyberhäiriötilanteissa)? Esim. testaamalla, säännöllisillä arvioinneilla, vaarantuneiden osien havaitsemisella jne.	1	-	
	4	-				Osallistutteko aktiivisesti tieto- ja viestintätekniikkatuotteiden, -palvelujen ja -prosessien EU:n sertifiointikehyksen suunnitteluun EU:n kyberturvallisuusasetuksen (asetus (EU) 2019/881) mukaisesti? Esim. osallistumalla Euroopan kyberturvallisuuden sertifiointiryhmään (ECCG) ja edistämällä tieto- ja viestintätekniikkatuotteiden/-palvelujen turvallisuutta koskevia teknisiä standardeja ja menettelyjä.	0	Edistättekö sellaisten pk-yrityksille suunnattujen sertifiointijärjestelmien kehittämistä, joiden tarkoituksena on lisätä tietoturvaa ja yksityisyyttä koskevien standardien käyttöönottoa?	0	-	
	5	-		-		Tarjoatteko jonkinlaisia kannustimia pk-yrityksille, jotta nämä ottaisivat käyttöön turvallisuus- ja yksityisyysstandardeja?	0	Onko teillä säännöksiä, joilla suuria yrityksiä rohkaistaan lisäämään toimitusketjuihinsa kuuluvien pienten yritysten kyberturvallisuutta? Esim. kyberturvallisuuskeskus, koulutus ja valistuskampanjat jne.	0	-	
	6	-		-		Rohkaisetteko ohjelmistotoimittajia tukemaan pk-yrityksiä varmistamalla pienille organisaatioille tarkoitettujen tuotteiden turvalliset oletuskokoonpanot?	0	-		-	

4.1.3 Osa-alue 3: Lait ja sääntely

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
11 – Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko yleisesti tiedossa, että kriittisen tietoinfrastruktuurin toimijat edistävät kansallista turvallisuutta?	1	Onko teillä menetelmä olennaisten palvelujen määrittämiseksi?	1	Oletteko panneet täytäntöön verkko- ja tietoturvadirektiivin (2016/1148)?	1	Onko teillä menettely riskirekisterin päivittämiseksi?	1	Laaditteko uhkaympäristöraportteja ja pidättekö ne ajan tasalla?	1
	2	-		Onko teillä menetelmä kriittisten tietoinfrastruktuurien määrittämiseksi?	1	Oletteko panneet täytäntöön Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista annetun direktiivin (2008/114) (Euroopan elintärkeää infrastruktuuria koskevan direktiivin)?	1	Onko käytössänne muita mekanismeja, joilla mitataan sitä, että keskeisten palvelujen tarjoajien toteuttamat tekniset ja organisatoriset toimenpiteet sopivat verkko- ja tietoturvajärjestelmien turvallisuusriskien hallintaan? Esim. säännölliset kyberturvallisuustarkastukset, vakiotoimenpiteiden toteuttaminen, hallituksen antamat tekniset välineet, kuten havainnointivälineet tai järjestelmäkohtainen konfiguraation arviointi jne.	1	Uhkaympäristön viimeinen kehitys huomioiden, voitteko lisätä uuden alan kriittisen tietoinfrastruktuurin suojaamista koskevaan toimintasuunnitelmaanne?	1
	3	-		Onko teillä menetelmä keskeisten palvelujen tarjoajien määrittämiseksi?	1	Onko teillä kriittisten alojen mukaan määritettyjen keskeisten palvelujen tarjoajien kansallinen rekisteri?	1	Arvioitteko ja päivitättekö määritettyjen keskeisten palvelujen tarjoajien luetteloa vähintään kahden vuoden välein?	1	Uhkaympäristön viimeinen kehitys huomioiden, voitteko mukauttaa kriittisen tietoinfrastruktuurin suojaamista koskevaa toimintasuunnitelmaanne vastaamaan uusia vaatimuksia?	1

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
11 – Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia	4	-		Onko teillä menetelmä digitaalisen palvelun tarjoajien määrittämiseksi?	1	Onko teillä määritettyjen digitalisen palvelun tarjoajien kansallinen rekisteri?	1	Onko käytössänne muita mekanismeja, joilla mitataan sitä, että digitaalisen palvelun tarjoajien toteuttamat tekniset ja organisatoriset toimenpiteet sopivat verkko- ja tietoturvajärjestelmien turvallisuusriskien hallintaan? Esim. säännölliset kyberturvallisuustarkastukset, vakiotoimenpiteiden toteuttaminen, hallituksen antamat tekniset välineet, kuten havainnointivälineet tai järjestelmäkohtainen konfiguraation arviointi jne.	1	-	
	5	-		Onko teillä yksi tai useampi kansallinen viranomainen, joka valvoo kriittisen tietoinfrastruktuurin suojaamista ja verkko- ja tietojärjestelmien turvallisuutta? Esim. verkko- ja tietoturvadirektiivissä (2016/1148) vaaditun mukaisesti.	1	Onko teillä määritettyjen tai tunnettujen riskien kansallinen riskirekisteri?	1	Arvioitteko ja päivittättekö määritettyjen digitaalisen palvelun tarjoajien luetteloa vähintään kahden vuoden välein?	1	-	
	6	-		Laaditteko alakohtaisia suojelusuunnitelmia? Esim. perustason kyberturvallisuusmenetelmien (pakollisten tai suuntaviivojen) osalta.	0	Onko teillä menetelmä kriittisen tietoinfrastruktuurin riippuvuuksien kartoittamiseksi?	1	Onko käytössänne (kansallinen tai kansainvälinen) turvallisuussertifiointijärjestelmä, jonka avulla keskeisten palvelujen tarjoajat ja digitaalisen palvelun tarjoajat voivat tunnistaa turvalliset tieto- ja viestintätekniikkatuotteet? Esim. SOG-ISia koskeva MRA-sopimus Euroopassa, kansalliset aloitteet jne.	1	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
11 – Suojellaan kriittistä tietoinfrastruktuuria, keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia	7	-		-		Sovellatteko riskinhallintamenettelyjä kriittisiin tietoinfrastruktuureihin liittyvien riskien tunnistamisessa, kvantifioinnissa ja hallinnassa kansallisella tasolla?	1	Käytättekö turvallisuussertifiointijärjestelmää tai laadunvarmistusmenettelyä, kun arvioitte keskeisten palvelujen tarjoajien kanssa työskenteleviä palveluntarjoajia? Esim. poikkeamien havaitsemisen, poikkeamiin reagoinnin, kyberturvallisuustarkastusten, pilvipalvelujen, älykorttien ym. alalla toimivia palveluntarjoajia.	1	-	
	8	-		-		Osallistutteko rajat ylittävien riippuvuuksien määrittämistä koskevaan kuulemismenettelyyn?	1	Onko teillä mekanismeja, joilla mitataan keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien vaatimusten mukaisuutta perustason kyberturvallisuustoimenpiteiden osalta?	0	-	
	9					Onko teillä yksi yhteyspiste, joka vastaa verkko- ja tietojärjestelmien turvallisuuteen liittyvien asioiden koordinoinnista kansallisella tasolla ja rajat ylittävästä yhteistyöstä unionin tasolla?	1	Onko teillä määräyksiä, joilla varmistetaan kriittisten tietoinfrastruktuurien tarjoamien palvelujen jatkuvuus? Esim. kriisin ennakointi, kriittisten tietoinfrastruktuurien jälleenrakennusmenettelyt, liiketoiminnan jatkuminen ilman tieto- ja viestintätekniikkaa, ilmavälin varmistusmenettelyt jne.	0		
	10					Määritättekö perustason kyberturvallisuusmenetelmät (pakolliset tai suuntaviivat) digitaalisen palvelun tarjoajille ja kaikille verkko- ja tietoturvadirektiivin (2016/1148) liitteessä II tarkoitetuille aloille?	1				
	11	-		-		Tarjoatteko välineitä tai menetelmiä kyberturvallisuuden häiriöiden havaitsemista varten?	1	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
12 – Torjutaan kyberrikollisuutta	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Oletteko tehneet tutkimuksen, jolla määritellään lainvalvontavaatimukset (oikeusperusta, resurssit, ammattitaito jne.), jotta kyberrikollisuuteen voidaan puuttua tehokkaasti?	1	Vastaako kansallinen oikeudellinen kehyksenne täysin asiaankuuluvaa EU:n oikeudellista kehystä, mukaan lukien tietojärjestelmiin kohdistuvista hyökkäyksistä annettua direktiiviä 2013/40/EU? Esim. laittomat tunkeutumiset tietojärjestelmiin, laiton järjestelmän häirintä, laiton datan vahingoittaminen, viestintäsalaisuuden loukkaaminen, rikoksissa käytetyt välineet jne.	1	Onko teillä yksiköitä, joiden tehtävänä on käsitellä kyberrikollisuutta syyttäjänvirastoissa?	1	Keräättekö tilastoja direktiivin 2013/40/EU (tietojärjestelmiin kohdistuvista hyökkäyksistä annetun direktiivin) 14 artiklan 1 kohdan säännösten mukaisesti?	1	Onko teillä lainvalvontaviranomaisille, tuomareille, syyttäjille ja kansallisille/valtion CSIRT-toimijoille tarkoitettua toimielinten välistä koulutusta tai koulutustyöpajoja kansallisella tasolla ja/tai monenvälisellä tasolla?	1
	2	Oletteko tehneet tutkimuksen, jolla syyttäjiä ja tuomareita koskevat vaatimukset (oikeusperusta, resurssit, ammattitaito jne.) määritellään, jotta kyberrikollisuuteen voidaan puuttua tehokkaasti?	1	Onko teillä säädöstä, jolla puututaan verkossa tapahtuviin henkilöllisyyden varastamisiin ja henkilötietovarkauksiin?	1	Oletteko osoittaneet määrärahoja kyberrikoksia tutkiville yksiköille?	1	Keräättekö erillisiä tilastoja kyberrikollisuudesta? Esim. operationaalisia tilastoja, kyberrikollisuuden suuntauksia koskevia tilastoja, kyberrikollisuuden tuottoja ja sen aiheuttamia vahinkoja koskevia tilastoja jne.	1	Osallistutteko kansainvälisen tason koordinointitoimiin rikollisen toiminnan häiritsemiseksi? Esim. soluttautuminen rikollisille hakkerointialustoille, järjestäytyneen kyberrikollisuuden ryhmiin, pimeän verkon markkinoille ja bottiverkkojen alasajoon.	1

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
12 – Torjutaan kyberrikollisuutta	3	Onko maanne allekirjoittanut Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen?	1	Onko teillä säädöstä, jolla puututaan verkossa tapahtuviin henkisen omaisuuden ja tekijänoikeuksien loukkauksiin?	1	Oletteko perustaneet keskuselimen, joka koordinoi kyberrikollisuuden torjuntaa koskevan alan toimintaa?	1	Arvioitteko lainvalvontaviranomaisten, oikeuslaitoksen ja kansallisten CSIRT-toimijoiden henkilöstölle tarjotun koulutuksen riittävyyttä kyberrikollisuuden torjunnassa?	1	Onko CSIRT-toimijoiden, lainvalvontaviranomaisten ja oikeuslaitoksen (syyttäjien ja tuomarien) tehtävät erotettu selvästi, kun he tekevät yhteistyötä kyberrikollisuuden torjunnassa?	1
	4			Onko teillä säädöstä, jolla puututaan verkossa tapahtuvaan häirintään tai kyberkiusaamiseen?	1	Oletteko perustaneet yhteistyömekanismeja kyberrikollisuuden torjuntaan osallistuvien kansallisten laitosten, mukaan lukien lainvalvontaan osallistuvien kansallisten CSIRT-toimijoiden, välille?	1	Teettekö säännöllisiä arviointeja, jotta voitte varmistaa, että olette antaneet riittävästi resursseja (henkilöstöä, määrärahoja ja välineitä) lainvalvontaviranomaisten alaisille kyberrikoksia tutkiville yksiköille?	1	Edistetäänkö sääntelykehyksellä CSIRT-toimijoiden/lainvalvonnan ja oikeuslaitoksen (syyttäjien ja tuomarien) välistä yhteistyötä?	1
	5			Onko teillä säädöstä, jolla puututaan tietokoneisiin liittyviin petoksiin? Esim. Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen määräysten mukaisesti.	1	Teettekö yhteistyötä ja jaatteko tietoja toisten jäsenvaltioiden kanssa kyberrikollisuuden torjunnan alalla?	1	Teettekö säännöllisiä arviointeja, jotta voitte varmistaa, että olette antaneet riittävästi resursseja (henkilöstöä, määrärahoja ja välineitä) syyttäjäviranomaisten alaisille kyberrikoksia tutkiville yksiköille?	1	Osallistutteko EU:n sidosryhmien (lainvalvontaviranomaisten, CSIRT-toimijoiden, ENISAn, Europolin Euroopan kyberrikostorjuntakeskuksen ym.) kanssa jaettavien standardoitujen välineiden ja menetelmien, mallien ja menettelyjen rakentamiseen ja ylläpitämiseen?	1
	6	-		Onko teillä säädöstä, jolla puututaan lasten suojeluun verkossa? Esim. direktiivin 2011/93/EU säännösten ja Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen määräysten mukaisesti.	1	Teettekö yhteistyötä ja jaatteko tietoja EU:n virastojen (esim. Europolin Euroopan kyberrikostorjuntakeskuksen, Eurojustin ja ENISAn) kanssa kyberrikollisuuden torjunnan alalla?	1	Onko teillä kyberrikollisuustapausten käsittelyyn erikoistuneita yksiköitä, tuomioistuimia tai tuomareita?	1	Onko teillä kehittyneitä mekanismeja, joilla estetään henkilöiden kiinnostuminen kyberrikollisuudesta tai osallistuminen siihen?	0

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
12 – Torjutaan kyberrikollisuutta	7	-		Oletteko määrittäneet toiminnallisen kansallisen yhteyspisteen, joka vaihtaa direktiivissä 2013/40/EU (tietojärjestelmiin kohdistuvista hyökkäyksistä annetussa direktiivissä) säädettyjä rikoksia koskevia tietoja muiden jäsenvaltioiden kanssa tai vastaa muiden jäsenvaltioiden tekemiin asiaa koskeviin kiireellisiin tietopyyntöihin?	1	Onko teillä riittävät välineet kyberrikollisuuteen puuttumista varten? Esim. kyberrikollisuuden taksonomia ja luokitus, välineet sähköisen todistusaineiston keräämistä varten, tietokonetutkintavälineet, luotetut alustat tietojen jakamista varten jne.	1	Onko teillä järjestelyjä, joilla tarjotaan tukea ja apua kyberrikollisuuden uhreille (tavallisille käyttäjille, pk-yrityksille ja suurille yrityksille)?	1	Soveltaako maanne EU:n suunnitelmaa ja/tai lainvalvonnan valmiusprotokollaa (EU LE ERP) vastatakseen tehokkaasti suuriin kyberturvallisuuden häiriötilanteisiin?	0
	8			Toimiiko lainvalvontaviranomaisenne alaisuudessa erityinen kyberrikoksia tutkiva yksikkö?	1	Onko teillä menettelyohjeet sähköisen todistusaineiston käsittelyä varten?	1	Oletteko perustaneet toimielinten välisen kehyksen ja yhteistyömekanismin kaikkien asiaankuuluvien sidosryhmien (esim. lainvalvontaviranomaisen, kansallisen CSIRT-toimijan ja oikeuslaitoksen) sekä yksityisen sektorin (esim. olennaisten palvelujen tarjoajien ja palveluntarjoajien) välille kyberhyökkäyksiin vastaamista varten?	1	-	
	9			Oletteko nimittäneet Budapestin yleissopimuksen 35 artiklassa tarkoitetun yhteyspisteen, joka on auki joka päivä 24 tuntia vuorokaudessa?	1	Osallistutteko EU:n virastojen (esim. Europolin, Eurojustin, OLAFin, Cepolin ja ENISAn) tarjoamiin ja/tai tukemiin koulutusmahdollisuuksiin?	0	Edistetäänkö sääntelykehyksellänne CSIRT-toimijoiden ja lainvalvonnan välistä yhteistyötä?	1	-	
	10	-		Oletteko nimittäneet EU:n lainvalvonnan valmiusprotokollan (EU LE ERP) mukaisen toiminnallisen kansallisen yhteyspisteen, joka on avoinna joka päivä 24 tuntia vuorokaudessa, suuriin kyberhyökkäyksiin vastaamista varten?	1	Harkitsetteko Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen toisen lisäpöytäkirjan hyväksymistä?	0	Onko teillä mekanismeja (esim. välineitä tai menettelyjä), joilla edistetään CSIRT-toimijoiden/lainvalvontaviranomaisten ja mahdollisesti oikeuslaitoksen (syyttäjien ja tuomarien) välistä tietojen vaihtoa ja yhteistyötä kyberrikollisuuden torjunnan alalla?	1	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
	11			Tarjoatteko säännöllistä erityiskoulutusta kyberrikollisuuden torjuntaan osallistuville sidosryhmille (lainvalvontaviranomaisille, oikeuslaitokselle ja CSIRT-toimijoille)? Esim. kyberympäristöä hyväksi käyttäen tehtäviä rikoksia koskevien kanteiden/syytteiden nostamista koskevat koulutukset, sähköisen todistusaineiston keräämistä ja koskemattomuuden varmistamista digitaalisessa käsittelyketjussa ja tietokonetutkintaa koskevat koulutukset.	1						
	12			Onko maanne ratifioinut Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen tai liittynyt siihen?	1			-	-	-	
	13	-		Onko maanne allekirjoittanut ja ratifioinut Budapestissä tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen lisäpöytäkirjan (joka koskee tietojärjestelmien avulla tehtyjen rasististen ja muukalaisvastaisten rikosten säätämistä rangaistaviksi teoiksi)?	0	-	-	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
13 – Perustetaan poikkeamista raportoinnin mekanismeja	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko teillä epävirallisia yksityisten organisaatioiden ja kansallisten viranomaisten välisiä kyberturvallisuuspoikkeamia koskevien tietojen vaihtamisen mekanismeja?	1	Onko teillä poikkeamista raportoinnin järjestelmä kaikilla verkko- ja tietoturvadirektiivin liitteessä II mainituilla aloilla?	1	Onko käytössänne pakollinen poikkeamista raportoiva järjestelmä, joka toimii käytännössä?	1	Onko teillä yhdenmukaistettu menettely alakohtaisille poikkeamista raportoinnin järjestelmille?	1	Laaditteko vuotuisia poikkeusraportteja?	1
	2	-		Oletteko panneet täytäntöön direktiivin (EU) 2018/1972 40 artiklassa tarkoitetut televiestintäpalvelujen tarjoajia koskevat ilmoitusvaatimukset? Direktiivissä vaaditaan, että jäsenvaltioiden on varmistettava, että yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat ilmoittavat toimivaltaiselle viranomaiselle viipymättä kaikki sellaiset turvapoikkeamat, joilla on ollut huomattava vaikutus verkkojen tai palvelujen toimintaan.	1	Onko käytössänne koordinointi-/yhteistyömekanismi yleistä tietosuoja-asetusta, verkko- ja tietoturvadirektiiviä, 40 artiklaa (entinen 13a artikla) ja eIDAS-asetusta koskevien poikkeamista raportoinnin velvoitteita varten?	1	Onko teillä poikkeamista raportoinnin järjestelmä kaikilla muilla kuin verkko- ja tietoturvadirektiivissä tarkoitetuilla aloilla?	1	Onko käytössänne kyberturvallisuusympäristöä koskevia raportteja tai muita poikkeamaraportit vastaanottavan tahon laatimia analyyseja?	1

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
13 – Perustetaan poikkeamista raportoinnin mekanismeja	3	-		Oletteko panneet täytäntöön eIDAS-asetuksen (asetus (EU) N:o 910/2014) 19 artiklassa tarkoitetut luottamuspalvelujen tarjoajia koskevat ilmoitusvaatimukset? Asetuksen 19 artiklassa vaaditaan muun muassa, että luottamuspalvelujen tarjoajien on ilmoitettava valvontaelimelle merkittävistä poikkeamista/loukkauksista.	1	Onko teillä riittävät välineet useiden ilmoituskanavien kautta jaettujen tietojen luottamuksellisuuden ja koskemattomuuden varmistamiseksi?	1	Mittaatteko poikkeamista raportoinnin menettelyjen tehokkuutta? Esim. asiaankuuluvien kanavien kautta ilmoitettuja poikkeamia koskevat indikaattorit, poikkeamaraportin ajoitus jne.	1	-	
	4	-		Oletteko panneet täytäntöön verkko- ja tietoturvadirektiivin 16 artiklassa tarkoitetut digitalisen palvelun tarjoajia koskevat ilmoitusvaatimukset? Direktiivin 16 artiklassa vaaditaan, että digitaalisen palvelun tarjoajat ilmoittavat toimivaltaiselle viranomaiselle tai CSIRT-toimijalle ilman aiheetonta viivytystä kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen liitteessä III tarkoitetun palvelun tarjoamiseen, jota ne tarjoavat unionissa.	1	Onko käytössänne alusta/väline ilmoitusprosessin helpottamiseksi?	0	Onko teillä kansallisen tason yhteinen taksonomia poikkeamien luokitusta ja perussyiden luokkia varten?	0	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
14 – Vahvistetaan yksityisyyttä ja tietosuojaa	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Oletteko tehneet tutkimuksia tai analyysejä kehittämisalueiden tunnistamiseksi, jotta kansalaisten oikeuksia yksityisyyteen voidaan suojella entistä paremmin?	1	Osallistuuko kansallinen tietosuojaviranomainen kyberturvallisuustapahtumia koskevien alojen toimintaan (esim. uusien kyberturvallisuuslakien ja -määräysten laatimiseen tai vähimmäistason turvatoimien määrittämiseen)?	1	Edistättekö turvatoimia ja sisäänrakennettua tietosuojaa koskevia parhaita käytäntöjä suuren yleisön keskuudessa ja/tai yksityisellä sektorilla?	1	Teettekö säännöllisiä arviointeja sen varmistamiseksi, että olette antaneet riittävät resurssit (henkilöstöä, määrärahoja ja välineitä) tietosuojaviranomaiselle?	1	Onko käytössä mekanismeja, joilla seurataan viimeisintä teknistä kehityksiä, jotta asiaankuuluvia ohjeita ja säädöksiä/velvoitteita voidaan mukauttaa niitä vastaaviksi?	1
	2	Oletteko kehittäneet kansallisen tason oikeusperustan, jolla yleinen tietosuoja-asetus (asetus (EU) N:o 2016/679) pannaan täytäntöön? Esim. asetuksen säännöksiä tarkempien säännösten tai niitä koskevien rajoitusten ylläpitäminen tai käyttöönotto.	0	-		Järjestättekö tätä aihetta koskevia tiedotus- ja koulutusohjelmia?	1	Rohkaisetteko organisaatioita ja yrityksiä hankkimaan henkilötietojen hallintajärjestelmää koskevan standardin ISO/IEC 27701:2019 mukaisen sertifioinnin?	1	Osallistutteko aktiivisesti yksityisyyden suojaa parantavien tekniikoiden tutkimusta ja kehitystä koskeviin aloitteisiin tai edistättekö niitä aktiivisesti?	0
	3	-		-		Koordinoitteko poikkeamista raportoinnin menettelyjä tietosuojaviranomaisen kanssa?	1	-		-	
	4	-		-		Edistättekö ja tuetteko tietoturvaa ja yksityisyyttä koskevien teknisten standardien kehittämistä? Onko niitä räätälöity erityisesti pienille ja keskisuurille yrityksille (pk-yrityksille)?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
14 – Vahvistetaan yksityisyyttä ja tietosuojaa	5	-		-		Tarjoatteko käytännönläheisiä ja skaalattavia suuntaviivoja, joilla tuetaan erilaisia rekisterinpitäjiä, jotta nämä noudattavat yksityisyyttä ja tietosuojaa koskevia lakisääteisiä vaatimuksia ja velvoitteita?	0	-		-	

4.1.4 Osa-alue 4: Yhteistyö

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
15 – Perustetaan julkisen ja yksityisen sektorin kumppanuuksia	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko yleisesti tiedossa, että julkisen ja yksityisen sektorin kumppanuuksilla edistetään valtion kyberturvallisuustason nostamista eri tavoin? Esim. kyberturvallisuusalan kasvusta syntyvien etujen jakaminen, asianmukaisen kyberturvallisuusalan sääntelykehyksen laatimista koskeva yhteistyö, tutkimuksen ja kehityksen edistäminen jne.	1	Onko teillä julkisen ja yksityisen sektorin kumppanuuksien perustamista koskeva kansallinen toimintasuunnitelma?	1	Oletteko perustaneet kansallisia julkisen ja yksityisen sektorin kumppanuuksia?	1	Oletteko perustaneet monialaisia julkisen ja yksityisen sektorin kumppanuuksia?	1	Pystyttekö mukauttamaan tai luomaan julkisen ja yksityisen sektorin kumppanuuksia tekniikan ja sääntelyn uusimman kehityksen mukaan?	1
	2	-		Laaditteko oikeus- tai sopimusperustan (erityiset lait, salassapitosopimukset ja teollis- ja tekijänoikeudet), jota sovelletaan julkisen ja yksityisen sektorin kumppanuuksiin?	1	Oletteko perustaneet alakohtaisia julkisen ja yksityisen sektorin kumppanuuksia?	1	Keskitytäänkö jo perustetuissa julkisen ja yksityisen sektorin kumppanuuksissa myös julkisten toimijoiden väliseen yhteistyöhön ja yksityisten toimijoiden väliseen yhteistyöhön?	1		
	3	-		-		Tarjoatteko rahoitusta julkisen ja yksityisen sektorin kumppanuuksien perustamista varten?	1	Edistättekö julkisen ja yksityisen sektorin kumppanuuksia pk-yritysten keskuudessa?	1	-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
15 – Perustetaan julkisen ja yksityisen sektorin kumppanuuksia	4	-		-		Johtavatko julkiset laitokset yleisesti julkisen ja yksityisen sektorin kumppanuuksia? Eli julkisen sektorin yksi yhteyspiste, joka hallinnoi ja koordinoi julkisen ja yksityisen sektorin kumppanuutta; julkiset elimet sopivat ennakkoon, mitä ne haluavat saavuttaa; julkishallinnon antamat selvät ohjeet niiden tarpeista ja rajoituksista yksityiselle sektorille jne.	1	Mittaatteko julkisen ja yksityisen sektorin kumppanuuksien tuloksia?	1	-	
	5	-		-		Oletteko julkisen ja yksityisen sektorin kyberturvallisuuskumppanuutta koskevan Euroopan kyberturvallisuusjärjestön (ECSO) sopimuksen osapuoli?	0	-		-	
	6	-		-		Työskenteleekö yksi tai useampi julkisen ja yksityisen sektorin kumppanuuksistanne CSIRT-toiminnan parissa?	0	-		-	
	7					Työskenteleekö yksi tai useampi julkisen ja yksityisen sektorin kumppanuuksistanne kriittisen tietoinfrastruktuurin suojaamisen parissa?	0				
	8	-		-		Työskenteleekö yksi tai useampi julkisen ja yksityisen sektorin kumppaninne kybertietoisuuden lisäämisen ja kyberturvallisuusvalmiuksien kehittämisen parissa?	0	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	nro	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
16 – Vakiinnutetaan julkisten virastojen välistä yhteistyötä	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko teillä julkisten virastojen välisiä epävirallisia yhteistyökanavia?	1	Onko teillä kyberturvallisuuteen keskittyvää kansallista yhteistyöjärjestelmää? Esim. neuvoa-antavat elimet, ohjausryhmät, foorumit, neuvostot, kyberkeskukset tai asiantuntijaryhmät.	1	Osallistuvatko viranomaiset yhteistyöjärjestelmään?	1	Varmistatteko, että kyberturvallisuutta koskevia yhteistyökanavia on käytössä vähintään seuraavien julkisten elinten välillä: tiedustelupalvelut, kansallinen lainvalvonta, syyttäjäviranomaiset, hallinnon toimijat, kansalliset CSIRT-toimijat ja puolustusvoimat?	1	Annetaanko julkisille virastoille yhdenmukaiset vähimmäistiedot uhkaympäristön ja kyberturvallisuutta koskevan tilannetietoisuuden uudesta kehityksestä?	1
	2	-		-		Oletteko perustaneet yhteistyöalustoja tietojen vaihtamista varten?	1	Mittaatteko erilaisten yhteistyöjärjestelmien menestystä ja rajoituksia tehokkaan yhteistyön edistämisessä?	1	-	
	3	-		-		Oletteko määrittäneet yhteistyöalustojen laajuuden (esim. tehtävät ja vastuualueet ja asiakokonaisuuksien määrä)?	1	-		-	
	4	-		-		Järjestättekö vuotuisia tapaamisia?	1	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	nro	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
16 – Vakiinnutetaan julkisten virastojen välistä yhteistyötä	5	-		-		Onko teillä eri maantieteellisten alueiden toimivaltaisten viranomaisten välisiä yhteistyömekanismeja? Esim. alueellisten turvallisuusyhteishenkilöiden verkostoa, kyberturvallisuusasioista vastaavaa virkailijaa alueellisissa kauppakamareissa jne.	1	-		-	

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
17 – Osallistutaan kansainväliseen yhteistyöhön (myös muiden kuin EU:n jäsenvaltioiden kanssa)	a	Sisältyykö tavoite nykyiseen kansalliseen kyberturvallisuussuunnitelmaanne tai aiotteko sisällyttää sen suunnitelman seuraavaan versioon?	1	Onko teillä epävirallisia menettelyjä tai toimia, joilla tavoite pyritään saavuttamaan koordinoimattomalla tavalla?	1	Onko teillä virallisesti määritettyä ja dokumentoitua toimintasuunnitelmaa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen suorituskyvyn testaamiseksi?	1	Onko teillä mekanismeja, joilla varmistetaan, että toimintasuunnitelmaa mukautetaan dynaamisesti ympäristön kehitystä vastaavaksi?	1
	b			Onko halutut tulokset, suuntaa-antavat periaatteet ja keskeiset toimet määritetty toimintasuunnitelmassa?	1	Onko resurssit ja hallinto määritetty selvästi toimintasuunnitelmassa?	1	Onko toimintasuunnitelmaa tarkistettu tavoitteen osalta sen varmistamiseksi, että se on asetettu etusijalle ja optimoitu oikein?	1		
	c			Onko mahdollinen toimintasuunnitelmanne pantu täytäntöön ja jo voimassa rajoitetusti?	0						
	1	Onko teillä kansainväliseen toimintaan osallistumista koskevaa strategiaa?	1	Oletteko tehneet (kahdenvälisiä tai monenvälisiä) yhteistyösopimuksia muiden maiden tai muissa maissa olevien kumppaneiden kanssa? Esim. tietojenvaihdosta, valmiuksien kehittämisestä, avustamisesta jne.	1	Vaihdatteko strategisen tason tietoja? Esim. korkean tason politiikasta, riskien havainnoinnista jne.	1	Osallistuvatko maanne kansalliset kyberturvallisuusvirastot kansainvälisiin yhteistyöjärjestelmiin?	1	Johdatteko monenvälisten sopimusten aiheita koskevia keskusteluja?	1

Kansallisen kyberturvallisuusstrategian tavoite	#	Taso 1	R	Taso 2	R	Taso 3	R	Taso 4	R	Taso 5	R
17 – Osallistutaan kansainväliseen yhteistyöhön (myös muiden kuin EU:n jäsenvaltioiden kanssa)	2	Onko teillä epävirallisia yhteistyökanavia muiden maiden kanssa?	1	Onko teillä yksi yhteyspiste, joka voi toimia yhteystahona ja varmistaa rajatylittävän yhteistyön jäsenvaltion viranomaisten kanssa (esim. yhteistyöryhmä tai CSIRT-toimijoiden verkosto)?	1	Vaihdatteko taktisen tason tietoja? Esim. uhkatoimijoiden tiedotuslehti, tietojen jakamisen ja analysoinnin keskukset, luotetut kolmannet osapuolet jne.	1	Arvioitteko säännöllisesti kansainvälisen yhteistyön aloitteiden tuloksia?	1	Johdatteko kansainvälisten yleissopimusten aiheita koskevia keskusteluja?	1
	3	Onko julkisen puolen johto tuonut esiin aikomuksensa osallistua kyberturvallisuusalan kansainväliseen yhteistyöhön?	1	Oletteko nimittäneet kansainväliseen yhteistyöhön osallistuvia henkilöitä?	1	Vaihdatteko operationaalisen tason tietoja? Esim. operationaalisia toimintatietoja, tietoja käynnissä olevista poikkeamista, vaarantumisindikaattoreista jne.	1	-		Johdatteko yhtä tai useampaa aihetta koskevaa keskustelua tai neuvottelua kansainvälisissä asiantuntijaryhmissä? Esim. kyberavaruuden vakautta koskevassa maailmanlaajuisessa komissiossa (Global Commission on the Stability of Cyberspace, GCSC), ENISAn NIS-yhteistyöryhmässä, YK:n alaisessa tietoturvallisuutta käsittelevässä hallitusten asiantuntijoiden ryhmässä jne.	1
	4	-		-		Osallistutteko kansainvälisiin kyberturvallisuusharjoituksiin?	1	-		-	
	5	-		-		Osallistutteko kansainvälisiin valmiuksien kehittämisaloitteisiin? Esim. koulutuksiin, osaamisen kehittämiseen, vakiomenettelyjen laatimiseen jne.	0	-		-	
	6	-		-		Oletteko tehneet keskinäisiä avunantosopimuksia muiden maiden kanssa? Esim. lainvalvontatoimista, oikeudenkäynneistä, poikkeamiin vastaamista koskevien valmiuksien jakamisesta, kyberturvallisuusomaisuuden jakamisesta jne.	0	-		-	
	7	-		-		Oletteko allekirjoittaneet tai ratifioineet kyberturvallisuusalan sopimuksia tai yleissopimuksia? Esim. tietoturvallisuutta koskevat kansainväliset käytännesäännöt, tietoverkkorikollisuutta koskevan yleissopimuksen.	0	-		-	

4.2 KEHYKSEN KÄYTTÖOHJEET

Tämän osan tarkoituksena on antaa jäsenvaltioille kehyksen käyttöönottoa ja kyselylomakkeen täyttämistä koskevia ohjeita ja suosituksia. Seuraavassa luetellut suositukset perustuvat pääasiassa jäsenvaltioiden edustajien haastatteluista kerättyyn palautteeseen:

- **Tiedon keräämistä ja yhdistämistä koskevien koordinointitoimien ennakointi.** Useimmat jäsenvaltiot toteavat, että itsearviointimenettelyn tekeminen kestää noin 15 henkilötyöpäivää. Itsearvioinnin suorittamiseksi on kuultava useita ja monenlaisia sidosryhmiä. Siksi on suositeltavaa, että valmisteluvaiheessa varataan aikaa kaikkien hallintoelinten, julkisten virastojen ja yksityisen sektorin asiaankuuluvien sidosryhmien tunnistamiseen.
- **Itsearvioinnin toteuttamisesta kansallisella tasolla vastaavan keskuselimen nimeäminen.** Koska kansallisten valmiuksien arviointikehyksen kaikkia indikaattoreja koskevan aineiston keräämiseen saattaa osallistua useita sidosryhmiä, on suositeltavaa nimetä keskuselin tai -virasto, joka vastaa itsearvioinnin toteuttamisesta toimimalla yhteystahona kaikille asiaankuuluville sidosryhmille ja koordinoimalla näitä.
- **Arviointimenettelyn käyttö tapana jakaa tietoa ja viestiä kyberturvallisuusaiheista.** Jäsenvaltioiden jakamista kokemuksista kävi ilmi, että keskustelut (joko henkilökohtaiset haastattelut tai yhteiset työpajat) ovat hyvä mahdollisuus edistää kyberturvallisuutta koskevaa vuoropuhelua, jakaa yhteisiä näkemyksiä ja keskustella kehitysalueista. Tärkeimpien saavutusten esiin nostamisen lisäksi myös tulosten jakaminen voi auttaa edistämään kyberturvallisuutta.
- **Kansallisen kyberturvallisuusstrategian käyttäminen arvioitavien tavoitteiden valinnassa.** Kansallisten valmiuksien arviointikehykseen kuuluvat 17 tavoitetta perustuvat tavoitteisiin, jotka yleisesti sisältyvät jäsenvaltioiden kansallisiin kyberturvallisuusstrategioihin. Kansalliseen kyberturvallisuusstrategiaan kuuluvia tavoitteita on käytettävä arvioinnin laajuuden määrittämisessä. Kansallisella kyberturvallisuusstrategialla ei kuitenkaan pidä rajoittaa arviointia. Koska kansallisissa kyberturvallisuussuunnitelmissa luonnollisesti keskitytään ensisijaisiin tavoitteisiin, tietyt alueet on jätetty siitä tarkoituksella pois. Se ei kuitenkaan tarkoita, että tiettyä valmiutta ei olisi. Esimerkiksi, jos tietty tavoite on jätetty pois kansallisesta kyberturvallisuussuunnitelmasta mutta maalla on kyseistä tavoitetta koskevia kyberturvallisuusvalmiuksia, tavoite voidaan arvioida.
- **Sen varmistaminen, että pisteiden tulkinta muuttuu samalla, kun kansallisen kyberturvallisuusstrategian soveltamisala muuttuu.** Kansallisen kyberturvallisuusstrategian elinkaari on monivuotinen prosessi. Joidenkin jäsenvaltioiden kansalliset kyberturvallisuusstrategiat pannaan tavallisesti täytäntöön 3–5 vuoden etenemissuunnitelmalla, ja soveltamisala muuttuu kahdessa peräkkäisessä kansallisen kyberturvallisuusstrategian versiossa. Näin ollen on kiinnitettävä erityistä huomiota, kun kansallisen kyberturvallisuusstrategian kahden eri version itsearvioinnin tuloksia esitellään: soveltamisalan muutokset saattavat vaikuttaa lopulliseen kypsyyspistemäärään. On suositeltavaa vertailla strategisten tavoitteiden täyttä laajuutta koskevia pistemääriä eri vuosina (eli yleistä kokonaispistemäärää).

Arviointimekanismia koskeva muistutus – esimerkki kattavuudesta

Arviointimekanismissa on kaksi pistetasoa:
(i) **yleinen kokonaiskattavuus**, joka perustuu itsearviointikehyksen strategisten tavoitteiden kattavaan luetteloon; ja
(ii) **erityinen kokonaiskattavuus**, joka perustuu jäsenvaltion valitsemiin strategisiin tavoitteisiin (vastaavat yleensä kyseisen maan kansallisessa kyberturvallisuusstrategiassa olevia tavoitteita).

Erityinen kokonaiskattavuus on tarkoituksellisesti (ks. arviointimekanismia koskeva 3.1 kohta) sama tai korkeampi kuin yleinen kokonaiskattavuus, sillä viimeksi mainittu saattaa sisältää tavoitteita, joita jäsenvaltio ei ole valinnut, mikä alentaa yleistä kokonaiskattavuutta. Kun

jäsenvaltio lisää uuden tavoitteen, kokonaiskattavuus nousee (eli katetaan useampia kypsyysindikaattoreja) mutta erityinen kokonaiskypsyys saattaa laskea (jos uusi lisätty tavoite on alkuvaiheessa ja sen kypsyystaso on alhainen).

- **Itsearviointikyselylomakkeen täyttämisessä on syytä muistaa, että ensisijaisena tavoitteena on tukea jäsenvaltioiden kyberturvallisuusvalmiuksien kehittämistä.** Sen vuoksi itsearviointiin vastattaessa on suositeltavaa valita lähinnä hyväksyttävä vastaus, vaikka kysymykseen vastaaminen täsmällisesti olisi vaikeaa joissain tilanteissa. Jos esimerkiksi vastaus kysymykseen on joissain tilanteissa KYLLÄ mutta toisissa tilanteissa EI, jäsenvaltion on hyvä muistaa, että EI-vastaus edellyttää toimintaa: joko parantamissuunnitelmaa tai kehitysalaa koskevaa toimintasuunnitelmaa, joka on otettava huomioon tulevissa kehitystoimissa.

5. SEURAAVAT VAIHEET

5.1 TULEVAT PARANNUKSET

Jäsenvaltioiden edustajien haastattelujen ja aineistotutkimusvaiheen aikana määritettiin seuraavat suositukset, joiden avulla nykyistä kansallisten valmiuksien arviointikehystä voidaan parantaa ja kehittää tulevaisuudessa:

- **Pisteytysjärjestelmän kehittäminen entistä tarkemmaksi.** Käyttöön voitaisiin ottaa esimerkiksi kattavuuden prosenttiosuus kaksiosaisen KYLLÄ/EI-vastauksen sijaan, jotta kansallisen tason valmiuksien vahvistamisen monimutkaisuus voitaisiin ottaa paremmin huomioon. Yksinkertainen lähestymistapa ja KYLLÄ/EI-vastaukset valittiin alkuvaiheessa.
- **Määrällisten mittareiden käyttöönotto jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden tehokkuuden mittaamisessa.** Kansallisten valmiuksien arviointikehyksessä keskitytään jäsenvaltioiden kyberturvallisuusvalmiuksien kypsyystason arviointiin. Sitä voitaisiin täydentää mittareilla, joilla mitataan niiden toimien ja toimintasuunnitelmien tehokkuutta, joita jäsenvaltiot ovat panneet täytäntöön valmiuksien vahvistamista varten. Tällaisten tehokkuusmittareiden laatiminen tässä vaiheessa ei vaikuttanut realistiselta, sillä alalta saatua palautetta on vähän, on vaikeaa löytää merkityksellisiä indikaattoreja, jotka liittävät tulokset kansallisen kyberturvallisuusstrategian täytäntöönpanoon, ja on vaikeaa laatia realistisia indikaattoreja, jotka voidaan myöhemmin yhdistää. Tätä työtä voidaan kuitenkin jatkaa tulevaisuudessa.
- **Siirtyminen itsearviointimenettelystä arviointiin.** Kehystä voidaan mahdollisesti kehittää tulevaisuudessa niin, että siirrytään kohti arvioinnin lähestymistapaa ja jäsenvaltioiden kyberturvallisuusvalmiuksien kypsyyttä arvioidaan entistä yhdenmukaisemmalla tavalla. Mahdollista puolueellisuutta voitaisiin todennäköisesti vähentää niin, että arvioinnin suorittaisi kolmas osapuoli.

LIITE A – YLEISKATSAUS AINEISTOTUTKIMUKSEN TULOKSIIN

Liitteessä A kerrotaan lyhyesti ENISAn aikaisemmasta kansallisia kyberturvallisuusstrategioita koskevasta työstä sekä arvioidaan asiaankuuluvia kyberturvallisuusvalmiuksiin liittyviä kypsyysmalleja, jotka ovat julkisesti saatavilla. Mallien valinnassa ja arvioinnissa on huomioitu seuraavat olettamukset:

- Kaikki mallit eivät perustu tarkkoihin tutkimusmenetelmiin.
- Mallien rakennetta ja tuloksia ei aina selitetä kattavasti siten, että kullekin mallille ominaisten eri elementtien välillä olisi selkeät yhteydet.
- Joissain malleissa ei anneta tarkkoja tietoja kehitysprosessista, rakenteesta tai arviointimenetelmistä.
- Muissa löytämissämme malleissa ja työkaluissa ei anneta mitään tietoja rakenteesta tai sisällöstä, eikä niitä ole siksi lueteltu.
- Arvioitavat mallit on valittu maantieteellisen kattavuuden perusteella. Ensisijaisena painopisteenä ovat kyberturvallisuusvalmiuksia koskevat kypsyysmallit, jotka on kehitetty Euroopan maiden suorituksen arvioimiseksi. Maantieteellistä kattavuutta on kuitenkin syytä laajentaa siten, että voidaan analysoida kypsyysmallien kehittämisen hyviä käytäntöjä eri puolilta maailmaa.

Tämä asiaankuuluvien, julkisesti saatavilla olevien kyberturvallisuusvalmiuksiin liittyvien kypsyysmallien järjestelmällinen arviointi toteutettiin käyttämällä mukautettua analyysikehystä, joka perustuu Beckerin määrittämiin menetelmiin kypsyysmallien kehittämiseksi[22]. Kunkin olemassa olevan kypsyysmallin osalta analysoitiin seuraavat elementit:

- **Kypsyysmallin nimi:** nimi ja tärkeimmät viitteet.
- **Alkuperä:** mallin suunnittelusta vastaava julkinen tai yksityinen laitos.
- **Yleinen tarkoitus ja kohderyhmä:** mallin yleinen soveltamisala ja aiotut kohderyhmät.
- **Tasojen määrä ja määritelmä:** mallin kypsyystasojen lukumäärä sekä niiden yleinen määritelmä.
- **Määritteiden määrä ja nimet:** Kypsyysmallissa käytettyjen määritteiden lukumäärä ja nimet. Määritteiden analyysillä on kolmiosainen tavoite:
  - kypsyysmallin jakaminen helposti ymmärrettäviin osioihin
  - useiden määritteiden kokoaminen samaa tavoitetta palvelevien määritteiden ryhmiksi sekä
  - erilaisten näkökohtien tarjoaminen kypsyystason kohteesta.
- **Arviointimenetelmä:** kypsyysmallin arviointimenetelmä.
- **Tulosten kuvaus:** Kypsyysmallin tulosten visualisointimenetelmän määrittäminen. Tämän vaiheen taustalla on se tosiseikka, että usein liian monimutkaiset kypsyysmallit epäonnistuvat. Näin ollen kuvaustavan on vastattava käytännön tarpeita.

[22] J. Becker, R. Knackstedt, J. Pöppelbuß. ”Developing Maturity Models for IT Management: A Procedure Model and its Application”. Business & Information Systems Engineering. Vuosikerta 1, nro 3, s. 213–222, kesäkuu 2009.

Aikaisempi kansallisia kyberturvallisuusstrategioita koskeva työ

ENISA julkaisi vuonna 2012 osana varhaisia toimiaan kaksi kansallisiin kyberturvallisuusstrategioihin liittyvää asiakirjaa. Ensiksi kansallisten kyberturvallisuusstrategioiden kehittämis- ja toteuttamisvaiheeseen liittyvässä käytännön oppaassa[23] esitettiin joukko konkreettisia toimia kansallisen kyberturvallisuusstrategian tehokasta toimeenpanoa varten ja kuvattiin kansallisen kyberturvallisuusstrategian elinkaari neljässä vaiheessa: strategian kehittäminen, strategian toteuttaminen, strategian arviointi ja strategian ylläpito. Toiseksi kyberavaruuden turvallisuuden vahvistamiseksi toteutettavien kansallisten toimien suunnan asettamisesta laaditussa asiakirjassa[24] määritettiin kyberturvallisuusstrategioiden tila EU:ssa ja sen ulkopuolella vuonna 2012 ja esitettiin, että jäsenvaltioiden tulisi määrittää yhteisiä teemoja ja eroja kansallisten kyberturvallisuusstrategioidensa välillä.

Vuonna 2014 julkaistiin ENISAn ensimmäinen jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden arviointikehys[25]. Kyseiseen kehykseen sisältyy suosituksia ja hyviä käytäntöjä sekä joukko valmiuksien kehittämistyökaluja kansallisten kyberturvallisuusstrategioiden arviointiin (*esim.* määritellyt tavoitteet, panokset, tulokset, keskeiset suorituskykyindikaattorit…). Nämä työkalut mukautetaan strategisessa suunnittelussaan kypsyyden eri tasoilla olevien maiden erilaisiin tarpeisiin. Samana vuonna ENISA julkaisi verkossa toimivan kansallisia kyberturvallisuusstrategioita koskevan interaktiivisen kartan[26], jonka avulla käyttäjät saavat nopeasti selvitettyä kaikkien EU:n jäsenvaltioiden ja EFTA-maiden kansalliset kyberturvallisuusstrategiat sekä niiden strategiset tavoitteet ja hyviä esimerkkejä toteutuksesta. Kartta kehitettiin alun perin vuonna 2014 kansallisten kyberturvallisuusstrategioiden kuvauskannaksi, ja vuonna 2018 sitä päivitettiin esimerkeillä toteutuksesta. Vuodesta 2019 lähtien kartta on toiminut *tietokeskuksena* sellaisten tietojen keskittämiseksi, joita jäsenvaltiot ovat toimittaneet kansallisen kyberturvallisuuden parantamiseksi suorittamistaan toimista.

Vuonna 2016 julkaistussa kansallisten kyberturvallisuusstrategioiden hyviä käytäntöjä koskevassa oppaassa[27] määritetään 15 strategista tavoitetta. Lisäksi kyseisessä oppaassa analysoidaan kunkin jäsenvaltion kansallisen kyberturvallisuusstrategian täytäntöönpanon tila sekä määritetään erilaisia kyseiseen täytäntöönpanoon liittyviä puutteita ja haasteita.

Vuonna 2018 ENISA julkaisi kansallisten kyberturvallisuusstrategioiden arviointityökalun[28]. Kyseessä on interaktiivinen itsearviointityökalu, jolla on tarkoitus auttaa jäsenvaltioita arvioimaan kansalliseen kyberturvallisuusstrategiaansa liittyviä strategisia prioriteettejaan ja tavoitteitaan. Työkalussa on joukko yksinkertaisia kysymyksiä, joiden avulla jäsenvaltioille annetaan täsmällisiä suosituksia kunkin tavoitteen toteuttamiseksi. Lisäksi vuonna 2019 julkaistussa asiakirjassa hyvistä käytännöistä kyberturvallisuuteen liittyvissä innovaatioissa kansallisten kyberturvallisuusstrategioiden yhteydessä[29] käsitellään kyberturvallisuuteen liittyviä

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, päivitetty vuonna 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Tällä asiakirjalla päivitetään vuoden 2012 opas: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

innovaatioita kansallisten kyberturvallisuusstrategioiden yhteydessä. Kyseisessä asiakirjassa määritetään eri innovaatioulottuvuuksiin liittyviä, alan asiantuntijoiden näkemysten mukaisia haasteita ja hyviä käytäntöjä, jotta edistetään tulevien innovatiivisten strategisten tavoitteiden kehittämistä.

A.1 Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (CMM)

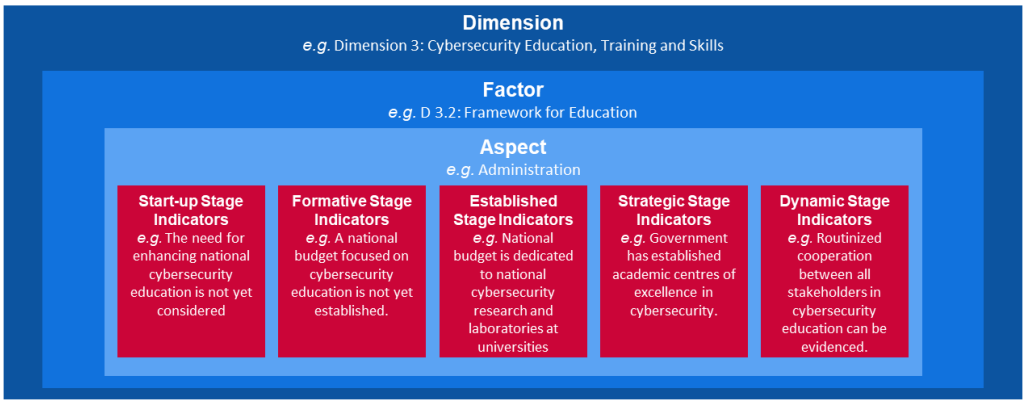
Valtioiden kyberturvallisuusvalmiuksien kypsyysmallin (Cybersecurity Capacity Maturity Model for Nations – CMM) on kehittänyt Global Cyber Security Capacity Centre -osaamiskeskus, joka on osa Oxfordin yliopistoon kuuluvaa Oxford Martin School -laitosta. Osaamiskeskuksen tavoitteena on laajentaa ja tehostaa kyberturvallisuusvalmiuksien kehittämistä sekä Yhdistyneessä kuningaskunnassa että kansainvälisesti kyberturvallisuusvalmiuksien kypsyysmallia (CMM) hyödyntämällä. CMM on kohdistettu suoraan valtioille, jotka haluavat kehittää kansallisia kyberturvallisuusvalmiuksiaan. CMM otettiin alun perin käyttöön vuonna 2014. Mallia muutettiin vuonna 2016 sen jälkeen, kun sitä oli käytetty yhdentoista kansallisen kyberturvallisuusvalmiuden arvioinnissa.

Määritteet/ulottuvuudet

CMM-mallin mukaan kyberturvallisuusvalmiudet käsittävät **viisi ulottuvuutta**, jotka edustavat kyberturvallisuusvalmiuksien ryhmiä. Kukin ryhmä edustaa erilaista tutkimusnäkökulmaa, josta käsin kyberturvallisuusvalmiuksia voidaan tutkia ja jonka avulla niitä voidaan ymmärtää. Viiden ulottuvuuden sisäisillä **tekijöillä** kuvataan kyberturvallisuusvalmiuksien hallinnan yksityiskohtia. Kyseiset yksityiskohdat ovat elementtejä, joilla edistetään kyberturvallisuusvalmiuksiin liittyvän kypsyyden lisäämistä kunkin ulottuvuuden sisällä. Kuhunkin tekijään sisältyvät eri **näkökohdat** edustavat tekijän eri komponentteja. Näkökohdat edustavat organisatorista menetelmää jakaa indikaattorit pienempiin, helpommin ymmärrettäviin ryhmiin. Kutakin näkökohtaa arvioidaan sitten **indikaattorien** avulla sellaisten vaiheiden, toimien tai rakenneosien kuvaamiseksi, jotka ilmaisevat tiettyä kypsyyden astetta (määritetään seuraavassa osiossa) tietyn näkökohdan, tekijän ja ulottuvuuden sisällä.

Edellä mainitut termit voidaan esittää kerroksittain alla olevan kuvan mukaisesti.

Kuva 4: Esimerkki CMM-indikaattoreista



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills
Factor
e.g. D 3.2: Framework for Education
Aspect
e.g. Administration

Start-up Stage Indicators
e.g. The for enhancing national cybersecurity education is not yet considered

Formative Stage Indictors
e.g. A national budget focused on cybersecurity education is not yet established

Ulottuvuus
Esim. ulottuvuus 3: kyberturvallisuuskoulutus ja -osaaminen
Tekijä
Esim. D 3.2: koulutuksen puitteet
Näkökohta
Esim. hallinto
Käynnistysvaiheen indikaattorit
Esim. tarvetta kansallisen kyberturvallisuuskoulutuksen parantamiseen ei ole vielä käsitelty
Kehitysvaiheet indikaattorit
Esim. kyberturvallisuuskoulutukseen kohdistettua kansallista budjettia ei ole vielä perustettu

Established Stage Indicators
e.g. National budget is dedicated to national cybersecurity research and laboratories at universities
Strategic Stage Indicators
e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.
Dynamic Stage Indicators
e.g. Routinized cooperation between all stakeholder

Vakiintuneen vaiheen indikaattorit
Esim. kansalliseen kyberturvallisuustutkimukseen ja -laboratorioihin yliopistoissa on varattu kansallinen budjetti
Strategisen vaiheen indikaattorit
Esim. hallitus on perustanut kyberturvallisuuskoulutukseen liittyviä akateemisia asiantuntijakeskuksia
Dynaamisen vaiheen indikaattorit
Esim. kaikkien kyberturvallisuuskoulutukseen liittyvien sidosryhmien välillä on rutiininomaista yhteistyötä

Viisi ulottuvuutta määritellään seuraavasti:

i kyberturvallisuuspolitiikan ja -strategian laatiminen (kuusi tekijää)
ii yhteiskunnan vastuullisen kyberturvallisuuskulttuurin edistäminen (viisi tekijää)
iii kyberturvallisuustietämyksen kehittäminen (kolme tekijää)
iv tehokkaiden oikeudellisten kehysten ja sääntelykehysten luominen (kolme tekijää) sekä
v riskien hallinta standardien, organisaatioiden ja teknologioiden avulla (seitsemän tekijää).

Kypsyystasot

CMM-mallissa käytetään **viittä kypsyystasoa** määrittämään, mille asteelle maa on edennyt tietyn kyberturvallisuusvalmiuksiin liittyvän tekijän tai näkökohdan suhteen. Kyseiset seuraavassa esitellyt tasot antavat kuvan senhetkisistä kyberturvallisuusvalmiuksista:

- **Käynnistys:** Tässä vaiheessa kyberturvallisuuskypsyyttä ei vielä ole tai se on luonteeltaan hyvin kehittymätöntä. Kyberturvallisuusvalmiuksien kehittämisestä saatetaan käydä alustavia keskusteluja, mutta konkreettisiin toimiin ei ole vielä ryhdytty. Havaittavaa näyttöä ei tässä vaiheessa vielä ole.
- **Kehitys:** Joidenkin näkökohtien osa-alueet ovat alkaneet kasvaa ja muotoutua; ne voivat olla tilapäisiä, sekavia, huonosti määriteltyjä – tai uusia. Toimintaa koskevaa näyttöä on kuitenkin jo selvästi osoitettavissa.
- **Vakiintunut**: Näkökohdan elementit ovat paikallaan ja toiminnassa. Tarkkaa harkintaa resurssien suhteellisesta kohdentamisesta ei ole kuitenkaan tehty. Näkökohdan eri elementteihin kohdistuvan ”suhteellisen” investoinnin jakamisesta on tehty vain vähän päätöksiä. Näkökohta on kuitenkin toimiva ja määritetty.
- **Strateginen:** On tehty päätöksiä siitä, mitkä näkökohdan osat ovat kyseessä olevalle organisaatiolle tai valtiolle tärkeitä ja mitkä vähemmän tärkeitä. Strateginen vaihe kuvastaa sitä, että kyseiset päätökset on tehty – valtion tai organisaation erityisten olosuhteiden mukaisesti.
- **Dynaaminen:** Tässä vaiheessa käytössä on selkeitä mekanismeja strategian muuttamiseksi vastaamaan vallitsevia olosuhteita, kuten uhkaympäristön teknologiaa, globaalia konfliktia tai jossakin huolenaiheessa (*esim.* kyberrikollisuus tai tietosuoja) tapahtunutta merkittävää muutosta. Dynaamiset organisaatiot ovat kehittäneet menetelmiä strategioiden joustavaa muuttamista varten. Tälle vaiheelle ominaisia ovat nopea päätöksenteko, resurssien uudelleen kohdentaminen sekä muuttuvan ympäristön jatkuva huomiointi.

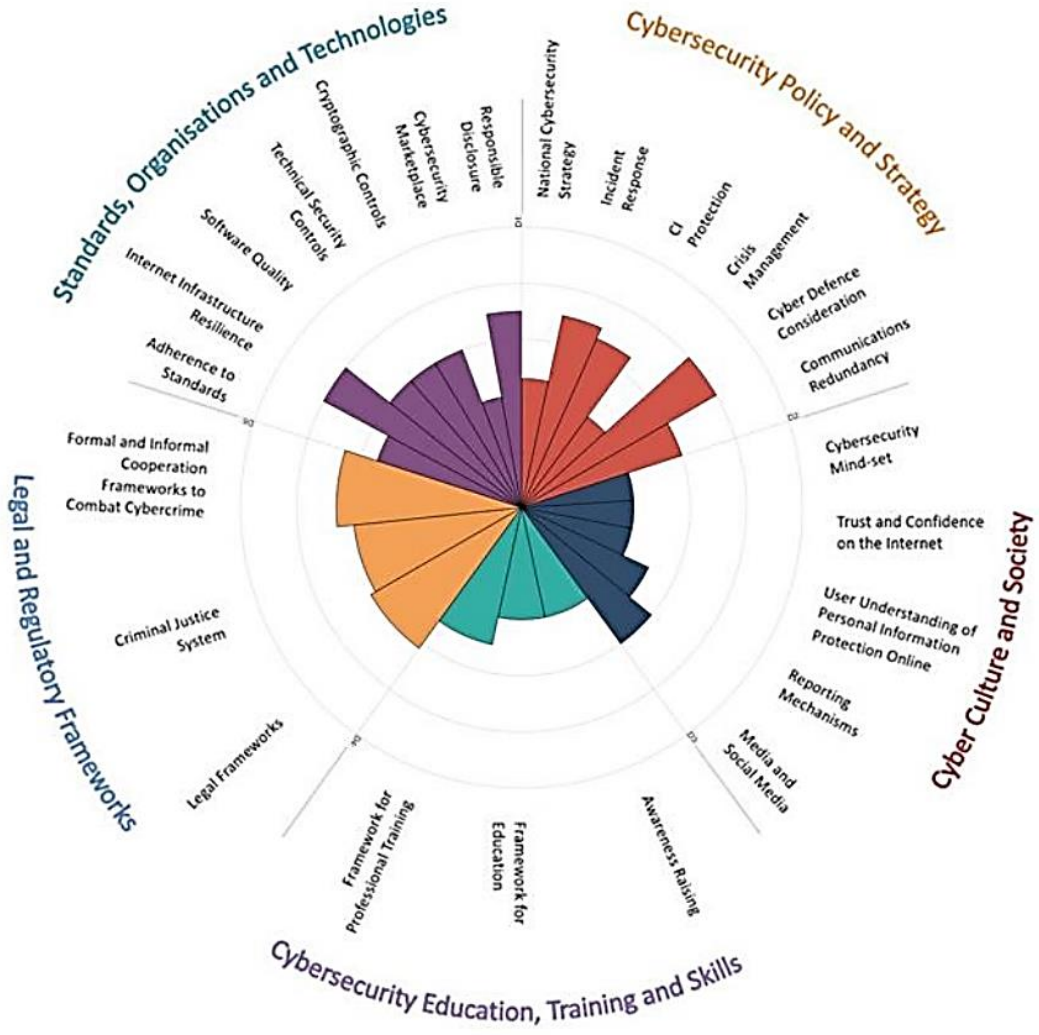
Arviointimenetelmä

Osaamiskeskuksella ei ole kattavaa ja syvällistä ymmärrystä kaikista kansallisista konteksteista, joissa mallia käytetään, joten se toimii yhdessä kansainvälisten organisaatioiden, isännöivien ministeriöiden tai organisaatioiden kanssa kyseessä olevassa maassa arvioidakseen kyberturvallisuusvalmiuksien kypsyyttä. CMM-malliin sisältyvien viiden ulottuvuuden kypsyystason arvioimiseksi osaamiskeskus ja isäntäorganisaatio tapaavat 2–3 päivän ajanjaksolla asiaankuuluvia kansallisia sidosryhmiä julkiselta ja yksityiseltä sektorilta sekä toteuttavat täsmäryhmähaastatteluja CMM-mallin ulottuvuuksista. Kutakin ulottuvuutta käsitellään erilaisissa sidosryhmäkokoonpanoissa vähintään kahdesti. Näin saadaan aikaan alustava tietovaranto myöhempää arviointia varten.

Tulosten kuvaustapa

CMM-mallissa annetaan yleiskuva kunkin maan kypsyystasosta tutkakaaviolla, joka koostuu viidestä sektorista (yksi kutakin ulottuvuutta kohden). Jokainen ulottuvuus on yksi viidesosa kaaviosta, ja kunkin tekijän viisi kypsyystasoa ulottuvat kaavion keskikohdasta reunoja kohden alla esitetyn mukaisesti. Käynnistysvaihe on lähimpänä kaavion keskikohtaa ja dynaaminen vaihe sen ulkokehällä.

Kuva 5 CMM: yleiskuva tuloksista



Standards, Organisations and Technologies	Standardit, organisaatiot ja teknologiat
Legal Regulatory Frameworks	Oikeudelliset sääntelykehykset
Cybersecurity Education, Training and Skills	Kyberturvallisuuskoulutus ja -osaaminen
Cybersecurity Policy and Strategy	Kyberturvallisuuspolitiikka ja -strategia
Cyber Culture and Society	Kyberkulttuuri ja yhteiskunta
Responsible Disclosure	Vastuullinen tiedonanto
Cybersecurity market place	Kyberturvallisuusmarkkinat
Cryptographic Controls	Salaustekniset hallintakeinot
Technical Security Controls	Tekniset turvatoimet
Software Quality	Ohjelmistojen laatu
Internet Infrastructure Resilience	Internetinfrastruktuurin häiriönsietokyky
Adherence to Standards	Standardien noudattaminen
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Viralliset ja epäviralliset yhteistyörakenteet kyberrikollisuuden torjumiseksi

Criminal Justice System	Rikosoikeusjärjestelmä
Legal Frameworks	Oikeudelliset kehykset
Framework for Professional Training	Ammatillisen koulutuksen puitteet
Framework for Education	Koulutuksen puitteet
Awareness Raising	Tietämyksen lisääminen
Media and Social Medai	Media ja sosiaalinen media
Reporting Mechanisms	Raportointimekanismit
User Understanding of Personal Information Protection Online	Käyttäjien ymmärrys henkilötietojen suojaamisesta verkossa
Trust and Confidence on the Internet	Luottamus internetiin
Cybersecurity Mind-set	Kyberturvallisuutta koskeva ajattelutapa
Communications Redundancy	Viestinnän varajärjestelmät
Cyber Defence Consideration	Kyberpuolustuksen huomioonottaminen
Crisis Management	Kriisinhallinta
CI Protection	Kriittisen infrastruktuurin suojelu
Incident Response	Kybertapahtumiin reagointi
National Cybersecurity Strategy	Kansallinen kyberturvallisuusstrategia

Global Cyber Security Capacity Centre -osaamiskeskus, Oxford Martin School, Oxfordin yliopisto, 2017.

A.2 Kyberturvallisuusvalmiuksien kypsyysmalli (C2M2)

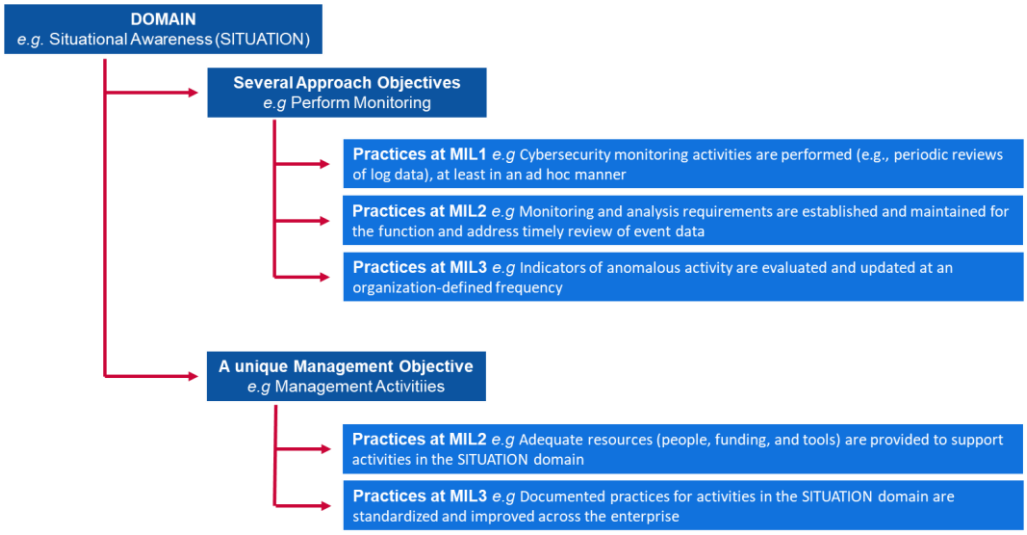
Kyberturvallisuusvalmiuksien kypsyysmallin (Cybersecurity Capacity Maturity Model – C2M2) on kehittänyt Yhdysvaltain energiaministeriö yhdessä yksityisen ja julkisen sektorin asiantuntijoiden kanssa. Osaamiskeskuksen tavoitteena on auttaa kaikkien alojen kaikentyyppisiä ja kaikenkokoisia organisaatioita arvioimaan ja parantamaan kyberturvallisuusohjelmiaan sekä vahvistamaan toimintansa häiriönsietokykyä. C2M2-mallissa keskitytään tietoa, tietotekniikkaa (IT) sekä operatiivista teknologiaa (OT) koskeviin resursseihin liittyvien kyberturvallisuuskäytäntöjen sekä niiden toimintaympäristöjen toteutukseen ja hallintaan. C2M2-mallissa kypsyysmallit määritellään seuraavasti: joukko ominaisuuksia, määritteitä, indikaattoreita tai malleja, jotka kuvaavat valmiuksia ja edistymistä tietyllä alalla. C2M2 otettiin alun perin käyttöön vuonna 2014, ja se on tarkistettu vuonna 2019.

Määritteet/ulottuvuudet

C2M2-mallissa on **kymmenen kohdealuetta**, jotka edustavat kyberturvallisuuskäytäntöjen loogista ryhmittelyä. Kukin käytäntöjen ryhmä kuvaa toimia, joihin organisaatio voi ryhtyä luodakseen ja kypsyttääkseen valmiuksia kyseisellä kohdealueella. Kuhunkin kohdealueeseen liittyy **ainutlaatuinen hallintatavoite** ja **useita menettelytapatavoitteita**. Sekä menettelytapatavoitteiden että hallintatavoitteiden osalta eritellään **useita käytäntöjä** institutionaalisten toimien kuvaamiseksi.

Mainittujen käsitteiden väliset yhteydet tiivistetään seuraavassa:

Kuva 6: Esimerkki C2M2-indikaattorista



Domain eg Situational Awareness (SITUATION)	**Kohdealue** Esim. tilannetietoisuus (TILANNE)
Several Approaches Objectives e.g. Perform Monitoring	**Useat menettelytapatavoitteet** Esim. valvonnan toteuttaminen
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Käytännöt tasolla MIL1** Esim. kyberturvallisuuden valvontatoimia toteutetaan (esim. lokitietojen määräajoin toistuvat arvioinnit) vähintään tilapäisesti
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Käytännöt tasolla MIL2** Esim. toimintoa koskevat valvonta- ja analyysivaatimukset on määritetty, niitä ylläpidetään ja niissä otetaan kantaa tapahtumatietojen oikea-aikaiseen arviointiin
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Käytännöt tasolla MIL3** Esim. epänormaalin toiminnan indikaattoreita arvioidaan ja päivitetään organisaation määrittämin aikavälein
A unique Management Objectve e.g. Management Activities	Ainutlaatuinen hallintatavoite esim. hallintatoimet
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Käytännöt tasolla MIL2** Esim. tarjotaan riittävät resurssit (henkilöstö, rahoitus ja työkalut) TILANNE-kohdealueella tapahtuvan toiminnan tukemiseksi
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Käytännöt tasolla MIL3** Esim. TILANNE-kohdealueella tapahtuvaa toimintaa koskevia dokumentoituja käytäntöjä standardoidaan ja parannetaan toimijan laajuisesti

Kymmenen kohdealuetta määritellään seuraavasti:

i riskinhallinta (RISKI)
ii resurssien, muutoksen ja kokoonpanon hallinta (RESURSSI)
iii identiteetin ja pääsyn hallinta (PÄÄSY)
iv uhkien ja haavoittuvuuksien hallinta (UHKA)
v tilannetietoisuus (TILANNE)
vi kybertapahtumiin ja -häiriöihin reagointi (REAGOINTI)
vii toimitusketjun ja ulkoisten riippuvuuksien hallinta (RIIPPUVUUDET)
viii työvoiman hallinta (TYÖVOIMA)
ix kyberturvallisuusarkkitehtuuri (ARKKITEHTUURI) sekä
x kyberturvallisuusohjelman hallinta (OHJELMA).

Kypsyyden tasot

C2M2-mallissa käytetään **neljää kypsyyden tasoa** (joita kutsutaan kypsyysindikaattoritasoiksi, Maturity Indicator Level – MIL) kypsyyden kahtalaisen eli menettelytapoihin ja hallintaan liittyvän edistymisen määrittämiseksi. MIL-tasot ulottuvat tasolta MIL0 tasolle MIL3, ja niitä on tarkoitus soveltaa erikseen kullekin kohdealueelle.

- **MIL0**: Käytäntöjä ei sovelleta.
- **MIL1**: Alustavia käytäntöjä sovelletaan, mutta ne voivat olla tilapäisiä.
- **MIL2**: Hallintaominaisuudet:
  - käytännöt on dokumentoitu
  - prosessin tukemiseksi tarjotaan riittävät resurssit
  - käytäntöjä soveltavalla henkilöstöllä on riittävä osaaminen ja tietämys
  - käytäntöjen soveltamista koskevat vastuut ja valtuudet on jaettu.

  Menettelytapaominaisuus:
  - käytännöt ovat valmiimpia tai edistyneempiä kuin tasolla MIL1.

- **MIL3**: Hallintaominaisuudet:
  - toiminta on periaatteiden (tai muiden organisatoristen suuntaviivojen) ohjaamaa
  - kohdealueen toiminnan suorituskykytavoitteet on määritetty, ja niitä valvotaan saavutusten seuraamiseksi
  - kohdealueen toiminnan dokumentoituja käytäntöjä standardoidaan ja parannetaan toimijan laajuisesti.

  Menettelytapaominaisuus:
  - käytännöt ovat valmiimpia tai edistyneempiä kuin tasolla MIL2.

Arviointimenetelmä

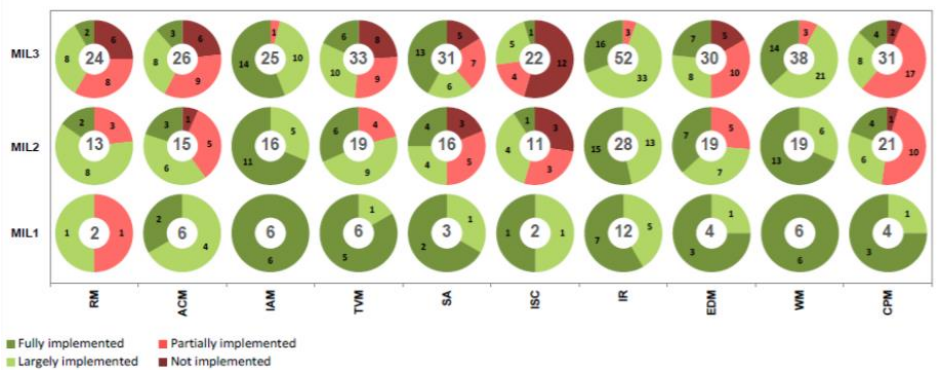
C2M2 on suunniteltu käytettäväksi **itsearviointimenetelmän** ja työkalusarjan (saatavana pyynnöstä) kanssa, joiden avulla organisaatio voi mitata ja parantaa kyberturvallisuusohjelmaansa. Työkalusarjan avulla toteutettavan itsearvioinnin voi tehdä yhdessä päivässä, mutta työkalusarjaa voi myös mukauttaa tarkempaan arviointiin. Lisäksi C2M2-mallia voi käyttää uuden kyberturvallisuusohjelman kehityksen ohjaamiseen.

Mallin sisältö esitetään hyvin abstraktilla tasolla, joten sitä voivat tulkita tyyppinsä, rakenteensa, kokonsa ja alansa puolesta erilaiset organisaatiot. Mallin laaja käyttö jollakin alalla voi tukea alan kyberturvallisuusvalmiuksien vertailua.

Tulosten kuvaustapa

C2M2-mallissa annetaan selvityksen tuloksista tuotettu arviointiraportti. Tulokset esitetään raportissa kahdessa näkymässä: tavoitenäkymässä, jossa esitetään vastaukset käytännön kysymyksiin kunkin kohdealueen ja sen tavoitteiden osalta, sekä kohdealuenäkymässä, jossa esitetään vastaukset kaikilta kohdealueilta ja MIL-tasoilta. Kummassakin näkymässä käytetään kuvausjärjestelmää, jolle ovat ominaisia piirakkakaaviot (yksi vastausta kohden) sekä liikennevalojärjestelmää hyödyntävä pisteytysmekanismi. Kuten kaavio 7 osoittaa, piirakkakaavion punaiset osiot ilmaisevat niiden kysymysten lukumäärää, joihin on saatu selvityksessä vastaukset ”ei toteutettu” (tummanpunainen) tai ”osin toteutettu” (vaaleanpunainen). Vihreät osiot ilmaisevat niiden kysymysten lukumäärää, joihin saatiin vastaukset ”suurelta osin toteutettu” (vaaleanvihreä) tai ”täysin toteutettu” (tummanvihreä).
Kaavio 7 alla on esimerkki pisteytyskortista kypsyysarvioinnin päätteeksi. X-akselilla ovat C2M2-mallin kymmenen kohdealuetta ja Y-akselilla kypsyyden tasot (MIL-tasot). Kuvassa on kolme riskinhallinnan (RM) kohdealueeseen liittyvää piirakkakaaviota, joista kukin vastaa yhtä kypsyyden tasoa (MIL1, MIL2 ja MIL3). RM-kohdealueen osalta kaaviosta käy ilmi, että ensimmäisen kypsyystason (MIL1) saavuttamiseksi on arvioitava kaksi kohdetta. Tässä tapauksessa yhden tuloksena on ”suurelta osin toteutettu” ja yhden ”osin toteutettu”. Toisen kypsyystason (MIL2) osalta mallissa määritetään 13 arvioitavaa kohdetta. Kaksi näistä 13 kohteesta kuuluu ensimmäiselle tasolle (MIL1) ja 11 toiselle tasolle (MIL2). Samaa sovelletaan kolmanteen tasoon (MIL3).

Kuva 7: C2M2 – esimerkki kohdealuenäkymästä



Fully implemented	Täysin toteutettu
Largely implemented	Suurelta osin toteutettu
Partially implemented	Osin toteutettu
Not implemented	Ei toteutettu
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	RM

ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Lähde: Yhdysvaltain energiaministeriö, sähkönjakelusta ja energiavarmuudesta vastaava osasto, 2015.

A.3 Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi

Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi kehitettiin Yhdysvaltain kansallisessa standardi- ja teknologiainstituutissa (NIST). Kehyksen painopiste on organisaation kyberturvallisuustoimien ohjaamisessa ja riskien hallinnassa. Se on tarkoitettu kaikentyyppisille organisaatioille niiden koosta, kyberriskin asteesta ja kyberturvallisuuden kehittyneisyydestä riippumatta. Kyseessä on kehys eikä malli, joten se on rakennettu eri tavalla kuin edellä analysoidut mallit.

Kehys koostuu seuraavista kolmesta osasta: kehyksen ydin, toteutuksen tasot sekä kehyksen profiilit:

- **Kehyksen ytimellä** tarkoitetaan kyberturvallisuustoimien joukkoa, toivottuja lopputuloksia sekä sovellettavia referenssejä, jotka ovat kriittisen infrastruktuurin aloille yhteisiä. Ne vastaavat kyberturvallisuusvalmiuksien kypsyysmalleihin sisältyviä määritteitä tai ulottuvuuksia.
- **Kehyksen toteutuksen tasoilla** (”tasot”) tarjotaan kontekstia siitä, miten organisaatiossa suhtaudutaan kyberriskiin ja millaisia prosesseja siellä käytetään kyseisen riskin hallitsemiseksi. Osittaisesta (taso 1) mukautuvaan (taso 4) ulottuvilla tasoilla kuvataan kasvavaa tarkkuuden ja edistyneisyyden astetta kyberriskin hallintakäytännöissä. Tasot eivät vastaa kypsyystasoja, vaan ne on pikemminkin tarkoitettu tukemaan organisaatioiden päätöksentekoa siitä, miten kyberriskiä hallitaan ja mitkä organisaation ulottuvuudet ovat prioriteetiltaan korkeammalla ja voisivat saada lisäresursseja.
- **Kehyksen profiililla** (”profiili”) kuvataan liiketoimintatarpeisiin perustuvia tuloksia, jotka organisaatio on valinnut kehyksen kategorioiden ja alakategorioiden joukosta. Profiilia voidaan luonnehtia suhteessa standardien, suuntaviivojen ja käytäntöjen yhdenmukaisuuteen kehyksen ytimen kanssa jossakin tietyssä toteutusskenaariossa. Profiilien avulla voidaan tunnistaa kyberturvallisuuden tason parantamismahdollisuuksia vertaamalla ”nykyprofiilia” (tosiasiallinen tila) ”kohdeprofiiliin” (tavoitetila).

Kehyksen ydin

Kehyksen ydin koostuu viidestä **toiminnosta**. Kokonaisuudessaan näistä toiminnoista saa korkean tason strategisen näkymän organisaation toteuttamaan kyberriskin hallinnan elinkaareen. Kehyksen ytimestä voidaan sitten eritellä kunkin toiminnon taustalla olevat keskeiset **kategoriat** ja **alakategoriat** ja yhdistää ne esimerkkeihin informatiivisista referensseistä, kuten kutakin alakategoriaa koskevista olemassa olevista standardeista, suuntaviivoista ja käytännöistä.

Toiminnot ja kategoriat määritellään seuraavasti:

i **Tunnistus**: Järjestelmiä, ihmisiä, resursseja, dataa ja valmiuksia koskevien kyberriskien hallintaan liittyvän organisatorisen ymmärryksen kehittäminen.
- Alakategoriat: resurssien hallinta, liiketoimintaympäristö, hallinto, riskinarviointi sekä riskinhallintastrategia.

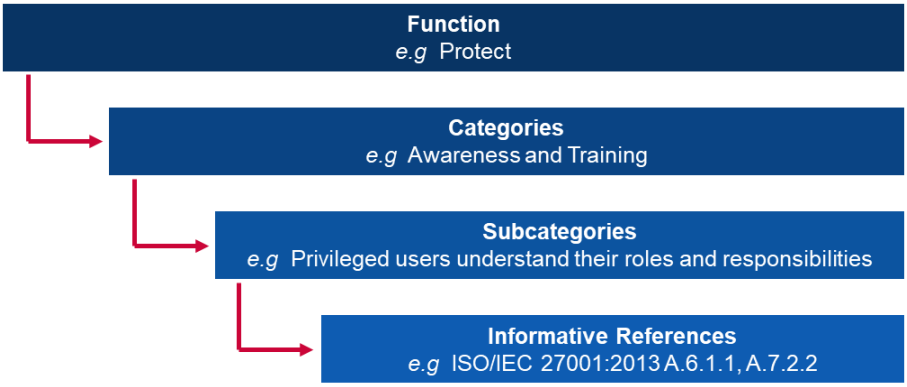
ii **Suojaus**: Asianmukaisten suojatoimien kehittäminen ja toteuttaminen kriittisten palvelujen toimittamisen varmistamiseksi.
- Alakategoriat: identiteetin hallinta ja käyttöoikeuksien hallinta, tietämys ja koulutus, tietoturva, tietosuojaprosessit ja -menettelyt, ylläpito ja suojaustekniikka.

iii **Havaitseminen**: asianmukaisten toimien kehittäminen ja toteuttaminen kyberturvallisuustapahtumien tunnistamiseksi.
- Alakategoriat: poikkeamat ja tapahtumat, jatkuva turvallisuuden valvonta sekä havaitsemisprosessit.

iv **Reagointi**: asianmukaisten toimien kehittäminen ja toteuttaminen toimeen ryhtymiseksi havaitun kybertapahtuman yhteydessä.
- Alakategoriat: reagoinnin suunnittelu, viestintä, analyysi, lievennystoimet sekä parannukset.

v **Toipuminen**: asianmukaisten toimien kehittäminen ja toteuttaminen häiriönsietokykyä koskevien suunnitelmien ylläpitämiseksi sekä kybertapahtuman heikentämien valmiuksien tai palvelujen palauttamiseksi.
- Alakategoriat: toipumisen suunnittelu, parannukset ja viestintä.

Kuva 8: Esimerkki kehyksestä kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi



Function e.g Project	**Toiminto** Esim. suojaus
Categories e.g Awarness and Training	**Kategoriat** Esim. tietämys ja koulutus
Subcategories e.g Privileged useres understand their roles and responsibilities	**Alakategoriat** Esim. etuoikeutetut käyttäjät ymmärtävät roolinsa ja vastuunsa
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informatiiviset referenssit** Esim. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Tasot

Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi perustuu **neljään tasoon**, joista kukin määritetään seuraavilla kolmella akselilla: riskinhallintaprosessi, integroitu riskinhallintaohjelma sekä ulkoinen osallistuminen. Tasoja ei tule pitää kypsyystasoina vaan kehyksenä, jonka avulla organisaatiot saavat kontekstia kyberriskiä koskeville näkemyksilleen sekä kyseisen riskin hallitsemiseksi käyttämilleen prosesseille.

- **Taso 1: Osittainen**
  - **Riskinhallintaprosessi**: organisaation kyberriskin hallintakäytäntöjä ei ole virallistettu, ja riskien hallinta on tilapäistä ja toisinaan reaktiivista.
  - **Integroitu riskinhallintaohjelma**: tietämys kyberturvallisuusriskeistä organisaation tasolla on rajallista. Kyberturvallisuusriskien hallinta organisaatiossa on epäsäännöllistä ja tapauskohtaista, eikä käytössä välttämättä ole prosesseja, jotka mahdollistaisivat kyberturvallisuutta koskevien tietojen jakamisen organisaation sisällä.
  - **Ulkoinen osallistuminen**: organisaatio ei ymmärrä rooliaan suuremmassa ekosysteemissä riippuvuuksiensa tai siitä riippuvaisten tahojen osalta.

Organisaatiossa ollaan yleisesti tietämättömiä sen tarjoamien ja käyttämien tuotteiden ja palvelujen kybertoimitusketjuun liittyvistä riskeistä.

- **Taso 2: Riskitietoinen**
  - **Riskinhallintaprosessi**: riskinhallintakäytännöt ovat johdon hyväksymiä mutta eivät välttämättä vakiintuneet organisaation laajuisiksi.
  - **Integroitu riskinhallintaohjelma**: kyberturvallisuusriski tunnetaan organisaation tasolla, mutta organisaation laajuista lähestymistapaa sen hallintaan ei ole määritetty. Organisaation resurssien ja ulkoisten resurssien kyberriskejä arvioidaan, mutta arviointi ei yleensä ole toistettavaa tai toistuvaa.
  - **Ulkoinen osallistuminen**: organisaatiossa ymmärretään yleisesti sen rooli suuremmassa ekosysteemissä joko sen omien riippuvuussuhteiden tai siitä riippuvaisten tahojen mutta ei molempien osalta. Lisäksi organisaatiossa ollaan tietoisia sen tarjoamien ja käyttämien tuotteiden ja palvelujen kybertoimitusketjuun liittyvistä riskeistä, mutta kyseisiin riskeihin ei puututa johdonmukaisesti tai virallisesti.
- **Taso 3: Toistettava**
  - **Riskinhallintaprosessi**: organisaation riskinhallintakäytännöt on hyväksytty ja tuotu julki virallisesti. Organisaation kyberturvallisuuskäytäntöjä päivitetään säännöllisesti sen mukaan, miten riskinhallintaprosesseja sovelletaan muutoksiin liiketoiminnan tai tehtävän vaatimuksissa sekä muuttuvaan uhka- ja teknologiaympäristöön.
  - **Integroitu riskinhallintaohjelma**: kyberriskin hallintaan on organisaation laajuinen lähestymistapa. Riskitietoiset periaatteet, prosessit ja menetelmät on määritetty, toteutettu tarkoitetulla tavalla sekä arvioitu. Ylempi johto varmistaa, että kyberturvallisuus otetaan huomioon organisaation kaikilla toimintalinjoilla.
  - **Ulkoinen osallistuminen**: organisaatiossa ymmärretään sen rooli ja riippuvuussuhteet sekä siitä riippuvaiset tahot suuremmassa ekosysteemissä ja voidaan edistää yhteisön laajempaa ymmärrystä riskeistä. Organisaatio on selvillä sen tarjoamien ja käyttämien tuotteiden ja palvelujen kybertoimitusketjuun liittyvistä riskeistä.
- **Taso 4: Mukautuva**
  - **Riskinhallintaprosessi**: organisaation kyberturvallisuuskäytäntöjä mukautetaan aikaisempien ja nykyisten kyberturvallisuustoimien, kuten saatujen kokemusten ja ennakoivien indikaattorien, mukaan.
  - **Integroitu riskinhallintaohjelma**: kyberriskin hallintaan on organisaation laajuinen lähestymistapa, jossa käytetään riskitietoisia periaatteita, prosesseja ja menetelmiä mahdollisiin kyberturvallisuustapahtumiin puuttumiseksi.
  - **Ulkoinen osallistuminen**: organisaatiossa ymmärretään sen rooli ja riippuvuussuhteet sekä siitä riippuvaiset tahot suuremmassa ekosysteemissä ja edistetään yhteisön laajempaa ymmärrystä riskeistä.

Arviointimenetelmä

Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi on tarkoitettu organisaatioille itsearvioinnin tekemiseksi riskeistään, jotta ne voisivat kehittää kyberturvallisuutteen liittyviä menettelytapojaan ja investointejaan järkiperäisemmiksi, tehokkaammiksi ja arvokkaammiksi. Investointien tehokkuuden arvioimiseksi organisaatiolla on ensinnä oltava selkeä käsitys organisatorisista tavoitteistaan, kyseisten tavoitteiden välisistä yhteyksistä ja niitä tukevista kyberturvallisuustuloksista. Kehyksen ytimen kyberturvallisuustulokset tukevat investointien tehokkuuden ja kyberturvallisuustoimien itsearvioinnissa.

A.4 Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Q-C2M2)

Qatarin kyberturvallisuusvalmiuksien kypsyysmallin (Qatar Cybersecurity Capability Maturity Model – Q-C2M2) on kehittänyt Qatarin yliopiston oikeustieteellinen korkeakoulu vuonna 2018. Q-C2M2 perustuu useisiin olemassa oleviin malleihin, ja sillä on tarkoitus luoda kattava arviointimenetelmä Qatarin kyberturvallisuuskehyksen parantamiseksi.

Määritteet/ulottuvuudet

Q-C2M2-mallissa hyödynnetään Yhdysvaltain kansallisen standardi- ja teknologiainstituutin (NIST) kehyksessä sovellettua lähestymistapaa, jossa viittä ydintoimintoa käytetään mallin

pääkohdealueina. Viisi ydintoimintoa soveltuvat Qatarin kontekstiin, sillä ne ovat kriittisen infrastruktuurin aloille yhteisiä, mikä on Qatarin kyberturvallisuuskehyksessä tärkeä elementti. Q-C2M2 perustuu **viiteen kohdealueeseen**, joista kukin jaetaan useisiin **osakohdealueisiin** kyberturvallisuusvalmiuksien kypsyyden koko alan kattamiseksi.

Viisi kohdealuetta määritellään seuraavasti:

i **Ymmärrä-kohdealueeseen** sisältyy neljä osakohdealuetta: kyberhallinto, resurssit, riskit ja koulutus.
ii **Turvaa-kohdealueeseen** kuuluvat osakohdealueet tietoturvallisuus, tekniikkaturvallisuus, käyttöoikeuksien hallinnan turvallisuus, viestinnän turvallisuus sekä henkilöstöturvallisuus.
iii **Paljasta-kohdealueeseen** kuuluvat osakohdealueet valvonta, kybertapahtumien hallinta, havaitseminen, analyysi ja paljastaminen.
iv **Reagoi-kohdealueeseen** kuuluvat reagoinnin suunnittelu, lievennystoimet sekä reagointia koskeva viestintä.
v **Säilytä-kohdealueeseen** kuuluvat toipumisen suunnittelu, jatkuvuuden hallinta, parannukset sekä ulkoiset riippuvuudet.

Kypsyyden tasot

Q-C2M2-mallissa käytetään **viittä kypsyyden tasoa** mittaamaan valtiollisen yksikön tai valtiosta riippumattoman organisaation valmiuksien kypsyyttä ydintoimintojen tasolla. Tasot on tarkoitettu kypsyyden arviointiin edellisessä osiossa määritellyillä kohdealueilla.

- **Alustus**: tilapäisiä kyberturvallisuuskäytäntöjä ja -prosesseja käytetään joillakin kohdealueilla.
- **Toteutus**: periaatteet kaikkien kohdealueille kuuluvien kyberturvallisuustoimien toteuttamiseksi on hyväksytty, ja tavoitteena on saattaa toteutus päätökseen tietyssä ajassa.
- **Kehitys**: periaatteet ja käytännöt kohdealueille kuuluvien kyberturvallisuustoimien kehittämiseksi ja parantamiseksi on pantu täytäntöön, ja tavoitteena on esittää toteutettaviksi uusia toimia.
- **Mukautuva**: kyberturvallisuustoimia tarkastellaan ja arvioidaan, ja käytäntöjä otetaan käyttöön aikaisemmista kokemuksista ja toimenpiteistä saatujen ennakoivien indikaattorien perusteella.
- **Ketterä**: mukautuvaa vaihetta jatketaan kiinnittämällä entistä enemmän huomiota ketteryyteen ja nopeuteen kohdealueilla toteutettavien toimien yhteydessä.

Arviointimenetelmä

Q-C2M2 on varhaisessa tutkimusvaiheessa, eikä se ole vielä valmis otettavaksi käyttöön. Kyseessä on kehys, jota voitaisiin tulevaisuudessa käyttää yksityiskohtaisena arviointimallina qatarilaisia organisaatioita varten.

A.5 Kyberturvallisuuden kypsyysmallisertifiointi (CMMC)

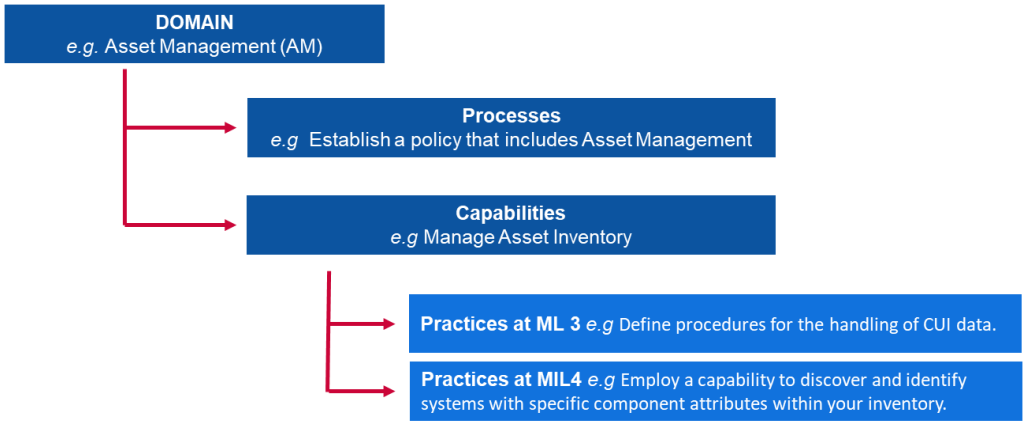
Kyberturvallisuuden kypsyysmallisertifioinnin (Cybersecurity Maturity Model Certification – CMMC) on kehittänyt Yhdysvaltain puolustusministeriö yhteistyössä Carnegie Mellon -yliopiston ja Johns Hopkinsin yliopiston Applied Physics Laboratory -tutkimuskeskuksen kanssa. Puolustusministeriön pääasiallinen tavoite tämän mallin suunnittelussa on puolustusteollisen perustan alalta peräisin olevien tietojen suojaaminen. CMMC-mallin kohteena olevat tiedot on luokiteltu joko liittovaltion sopimustiedoiksi eli tiedoiksi, jotka hallitus on toimittanut tai tuottanut sopimuksen mukaisesti ja joita ei ole tarkoitettu julkaistaviksi, tai valvotuiksi luokittelemattomiksi tiedoiksi eli tiedoiksi, jotka edellyttävät suojatoimia tai levityksen valvontaa lakien, määräysten ja hallinnonlaajuisten periaatteiden mukaisesti. CMMC-mallilla mitataan kyberturvallisuuden kypsyyttä, ja se tarjoaa parhaita käytäntöjä sekä sertifiointielementin sen varmistamiseksi, että kuhunkin kypsyystasoon liittyvät käytännöt pannaan täytäntöön. CMMC-mallin viimeisin versio julkaistiin vuonna 2020.

Määritteet/ulottuvuudet

CMMC-mallissa on **17 kohdealuetta**, jotka edustavat kyberturvallisuusprosessien ja -valmiuksien ryhmiä. Kukin kohdealue jakautuu useaan **prosessiin**, jotka ovat samanlaisia eri kohdealueilla, sekä yhteen tai useampaan **valmiuteen** viidellä kypsyyden tasolla. Valmiudet (tai valmius) eritellään vielä **käytäntöihin** kullakin asiaankuuluvalla kypsyyden tasolla.

Mainittujen käsitteiden välillä on seuraava yhteys:

Kuva 9: esimerkki CMMC-indikaattoreista



DOMAIN e.g. Asset Management (AM)	**KOHDEALUE** esim. resurssien hallinta (AM)
Processes e.g Establish a policy that includes Asset Management	**Prosessit** Esim. resurssien hallinnan käsittävien periaatteiden luominen
Capabilities e.g Manage Asset Inventory	**Valmiudet** Esim. resurssivarannon hallinta
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Käytännöt tasolla MIL 3** Esim. menetelmien määrittely valvotun luokittelemattoman tiedon käsittelyyn
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Käytännöt tasolla ML 4** Esim. valmiuden käyttö tietyillä attribuuteilla varustettujen järjestelmien löytämiseen ja tunnistamiseen varannosta

17 kohdealuetta ovat seuraavat:

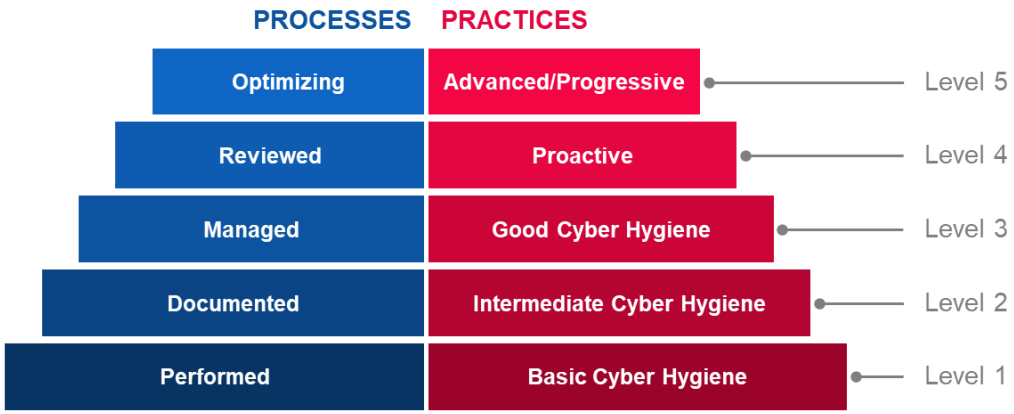
i käyttöoikeuksien hallinta (AC)
ii resurssien hallinta (AM)
iii tarkastus ja vastuuvelvollisuus (AU)
iv tietämys ja koulutus (AT)
v kokoonpanon hallinta (CM)
vi tunnistus ja todentaminen (IA)
vii kybertapahtumiin reagointi (IR)
viii ylläpito (MA)
ix median suojaus (MP)
x henkilöstöturvallisuus (PS)
xi fyysinen suojaus (PE)
xii toipuminen (RE)
xiii riskinhallinta (RM)
xiv turvallisuusarviointi (CA)
xv tilannetietoisuus (SA)

xvi järjestelmien ja viestinnän suojaaminen (SC) sekä
xvii järjestelmien ja tietojen eheys (SI).

Kypsyyden tasot

CMMC-mallissa käytetään **viittä kypsyyden tasoa**, jotka on määritelty prosessien ja käytäntöjen perusteella. Saavuttaakseen CMMC-mallissa tietyn kypsyystason organisaationon täytettävä kyseisen tason prosesseja ja käytäntöjä koskevat vaatimukset. Sen on täytettävä myös kaikkien edellisten tasojen vaatimukset.

Kuva 10: CMMC-mallin kypsyystasot



PROCESSES	PROSESSIT
Optimizing	Optimointi
Reviewed	Tarkastettu
Managed	Hallittu
Documented	Dokumentoitu
Performed	Suoritettu
PRACTICES	KÄYTÄNNÖT
Advanced/Progressive	Edennyt/etenevä
Proactive	Ennakoiva
Good Cyber Hygiene	Hyvä kyberhygienia
Intermediate Cyber Hygiene	Keskitason kyberhygienia
Basic Cyber Hygiene	Perustason kyberhygienia
Level 5	Taso 5
Level 4	Taso 4
Level 3	Taso 3
Level 2	Taso 2
Level 1	Taso 1

- **Taso 1**
  - **Prosessit – suoritettu**: organisaatio saattaa pystyä suorittamaan kyseiset käytännöt ainoastaan tilapäisesti ja voi turvautua tai olla turvautumatta dokumentaatioon. Tasolla 1 ei arvioida prosessien kypsyyttä.
  - **Käytännöt – perustason kyberhygienia**: taso 1 koskee erityisesti liittovaltion sopimustietojen suojaamista ja koostuu vain perustason suojausvaatimuksia vastaavista käytännöistä.
- **Taso 2**
  - **Prosessit – dokumentoitu**: päästäkseen tasolle 2 organisaation on määritettävä ja dokumentoitava käytännöt ja periaatteet CMMC-pyrkimystensä toteutuksen

ohjaamiseksi. Käytäntöjen dokumentoinnin ansiosta ne ovat yksilöiden toteutettavissa toistettavalla tavalla. Organisaatiot kehittävät kypsiä valmiuksia dokumentoimalla prosessinsa ja panemalla ne sitten täytäntöön dokumentoinnin mukaisesti.
    - **Käytännöt – keskitason kyberhygienia**: taso 2 on siirtymävaihe tasolta 1 tasolle 3 ja koostuu joukosta turvavaatimuksia, jotka on määritelty julkaisussa NIST SP 800-171, ja käytännöistä, jotka ovat peräisin muista standardeista ja referensseistä.

- **Taso 3**
    - **Prosessit – hallittu**: päästäkseen tasolle 3 organisaation on laadittava suunnitelma, jossa osoitetaan käytäntöjen toteuttamiseksi suoritettavien toimien hallinta, ylläpidettävä kyseistä suunnitelmaa ja annettava resurssit sitä varten. Suunnitelma voi sisältää tietoa tehtävistä, tavoitteista, projektisuunnitelmista, resursoinnista, tarvittavasta koulutuksesta sekä asiaankuuluvien sidosryhmien osallistamisesta.
    - **Käytännöt – hyvä kyberhygienia**: taso 3 koskee erityisesti valvotun luokittelemattoman tiedon suojaamista ja kattaa kaikki julkaisussa NIST SP 800-171 määritellyt turvavaatimukset sekä muista standardeista ja referensseistä peräisin olevat lisäkäytännöt uhkien lieventämiseksi.
- **Taso 4**
    - **Prosessit – tarkastettu**: tasolle 4 päästäkseen organisaation on tarkastettava ja mitattava käytäntöjensä tehokkuus. Käytäntöjen tehokkuuden mittaamisen lisäksi tällä tasolla olevat organisaatiot voivat ryhtyä tarvittaessa korjaaviin toimenpiteisiin. Ne myös huolehtivat toistuvasta tiedottamisesta ylemmälle johdolle tilanteesta tai ongelmista.
    - **Käytännöt – proaktiivinen**: taso 4 koskee erityisesti valvotun luokittelemattoman tiedon suojaamista ja kattaa joukon korotettuja turvavaatimuksia. Näillä käytännöillä parannetaan organisaation havaitsemis- ja reagointivalmiuksia, joiden avulla se voi puuttua ja mukautua muuttuviin taktiikoihin, tekniikoihin ja menetelmiin.
- **Taso 5**
    - **Prosessit – optimointi**: päästäkseen tasolle 5 organisaation on standardoitava ja optimoitava prosessien toteutus organisaation laajuisesti.
    - **Käytännöt – edennyt/etenevä**: taso 5 koskee erityisesti valvotun luokittelemattoman tiedon suojaamista. Lisäkäytännöt kasvattavat kyberturvallisuusvalmiuksien syvyyttä ja kehittyneisyyttä.

Arviointimenetelmä

CMMC on melko tuore malli, sillä se valmistui vuoden 2020 ensimmäisellä neljänneksellä. Tähän mennessä sitä ei ole otettu käyttöön missään organisaatiossa. Puolustusministeriön toimeksisaajat odottavat kuitenkin tukevansa sertifioituja ulkopuolisia tarkastajia tarkastusten tekemiseksi. Puolustusministeriö odottaa toimeksisaajiensa toteuttavan parhaat käytännöt kyberturvallisuuden sekä arkaluonteisten tietojen suojaamisen edistämiseksi.

A.6 Yhteisön kyberturvallisuuden kypsyysmalli (CCSMM)

Yhteisön kyberturvallisuuden kypsyysmalli (Community Cyber Security Maturity Model – CCSMM) on kehitetty Texasin yliopistoon kuuluvassa Center for Infrastructure Assurance and Security -keskuksessa. CCSMM-mallin tavoitteena on määritellä entistä paremmin menetelmät, joiden avulla saadaan selville yhteisön kybervalmiuksien kulloinenkin tila, sekä tarjota etenemissuunnitelma, jota yhteisöt voivat valmisteluissaan seurata. Yhteisöt, joille CCSMM-malli on kohdistettu, ovat pääasiassa paikallis- tai osavaltiotason hallintoja. CCSMM suunniteltiin vuonna 2007.

Määritteet/ulottuvuudet

Kypsyyden tasot perustuvat **kuuteen pääasialliseen ulottuvuuteen**, jotka kattavat kyberturvallisuuden eri näkökohdat yhteisöissä ja organisaatioissa. Kyseiset ulottuvuudet on määritelty tarkasti kunkin kypsyystason osalta (eritellään kaaviossa 31: Yhteenveto CCSMM mallin). Kuusi ulottuvuutta ovat seuraavat:

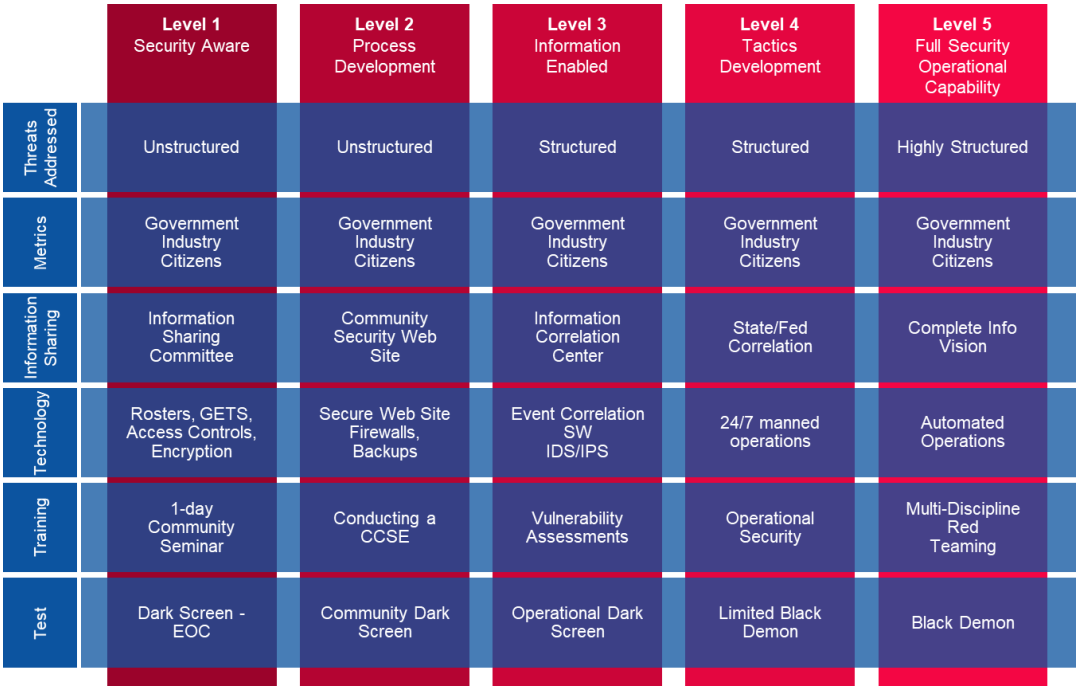
i uhat, joihin puututaan
ii mittarit
iii tietojen jakaminen
iv teknologia
v koulutus sekä
vi testaus.

Kypsyyden tasot

CCSMM-mallissa on seuraavat **viisi kypsyystasoa**. Ne perustuvat uhkien ja toimien pääasiallisiin tyyppeihin, joihin kyseisellä tasolla puututaan:

- **Taso 1: turvallisuustietoisuus**
  Tällä tasolla toiminnan pääasiallisena teemana on tehdä yksilöistä ja organisaatioista tietoisia kyberturvallisuuteen liittyvistä uhista, ongelmista ja kysymyksistä.
- **Taso 2: prosessin kehittäminen**
  Taso on suunniteltu auttamaan yhteisöjä luomaan ja parantamaan turvallisuusprosesseja, joita kyberturvallisuuskysymysten tehokas käsittely edellyttää.
- **Taso 3: tietojen käyttäminen**
  Taso on suunniteltu parantamaan yhteisön sisäisiä tiedonjakomekanismeja, jotta yhteisössä voidaan tehokkaasti yhdistellä näennäisesti erillisiä tiedonpalasia.
- **Taso 4: taktiikan kehittäminen**
  Tämän tason elementit on suunniteltu entistä parempien ja ennakoivampien menetelmien kehittämiseen hyökkäysten havaitsemiseksi ja niihin reagoimiseksi. Tähän tasoon mennessä suurimman osan ennaltaehkäisevistä menetelmistä pitäisi olla käytössä.
- **Taso 5: täysi turvallisuuteen liittyvä toimintavalmius**
  Taso edustaa kaikkia niitä osatekijöitä, jotka organisaatiolla pitäisi olla käytössään, jotta sen voi katsoa olevan täysin toimintavalmis puuttumaan mihin tahansa kyberuhkaan.

Kuva 31: yhteenveto CCSMM-mallin ulottuvuuksista tasoittain



Level 1 Security Aware	Taso 1 turvallisuustietoisuus
Level 2 Process Development	Taso 2 prosessin kehittäminen
Level 3 Information Enabled	Taso 3 tietojen käyttäminen
Level 4 Tactics Development	Taso 4 taktiikan kehittäminen
Level 5 Full Security Operational Capability	Taso 5 täysi turvallisuuteen liittyvä toimintavalmius
Threats Addressed	Uhat, joihin puututaan
Metrics	Mittarit
Information sharing	Tietojen jakaminen
Technology	Teknologia
Training	Koulutus
Test	Testaus
Unstructured	Jäsentymätön
Governement Industry Citizens	Hallinto, elinkeinoelämä, kansalaiset
Information Sharing Committee	Tiedonjakokomitea
Rosters, GETS, Assess Controls, Encryption	Yhteystietoluettelot, hallinnon hätätietoliikennepalvelu (GETS), pääsynvalvonta, salaus
1-dat Community Seminar	Yksipäiväinen yhteisöseminaari
Dark Screen – EOC	Dark Screen – hätätilannekeskus (EOC)
Unstructured	Jäsentymätön
Governement Industry Citizens	Hallinto, elinkeinoelämä, kansalaiset
Community Security Web site	Yhteisön turvallisuusverkkosivusto
Secure Web Site Firewalls, Backups	Turvalliset verkkosivustojen palomuurit, varmuuskopiot
Conudcting a CCSE	CCSE-sertifioinnin suorittaminen
Community Dark Screen	Yhteisön Dark Screen
Structured	Jäsentynyt
Governement Industry Citizens	Hallinto, elinkeinoelämä, kansalaiset
Information Correlation Center	Tiedon yhdistämiskeskus
Event Correlation SW IDS/IPS	Tapahtumien yhdistäminen, IDS/IPS-ohjelmistot

Vulnerability Assessment	Haavoittuvuusarvioinnit
Operational Dark Screen	Operatiivinen Dark Screen
Structured	Jäsentynyt
Governement Industry Citizens	Hallinto, elinkeinoelämä, kansalaiset
State/Fed Correlation	Osa-/liittovaltioyhteistyö
24/7 manned operations	24/7 miehitetyt toiminnot
Operational Security	Käyttövarmuus
Limited Black Demon	Rajattu Black Demon
Highly Structured	Erittäin jäsentynyt
Complete Info Vision	Kattavat tiedot, Visio
Automated Operations	Automaattiset toiminnat
Multi-Discipline Red Teaming	Monialainen, Red team -toiminta
Black Demon	Black demon -toiminta

Arviointimenetelmä

CCSMM-malli arviointimenetelmänä on tarkoitettu yhteisöjen käyttöön osavaltion ja liittovaltion lainvalvontaviranomaisten avustuksella. Sen tarkoituksena on auttaa yhteisöä määrittämään, mikä on kaikista tärkeintä, mitkä ovat todennäköisimmät kohteet ja mitä on suojattava (ja missä määrin). Kyseiset tavoitteet huomioimalla voidaan kehittää suunnitelmia, joilla saadaan yhteisön kaikki näkökohdat kyberturvallisuuskypsyyden vaaditulle tasolle. CCSMM-mallista tuotetun erityisen tiedon avulla voidaan määrittää tavoitteet erilaisille testeille ja harjoituksille, joita on mahdollista käyttää perustettujen ohjelmien tehokkuuden mittaamiseen.

A.7 Tietoturvan kypsyysmalli NIST-kyberturvallisuuskehystä varten (ISMM)

Tietoturvan kypsyysmalli (Information Security Maturity Model – ISMM) on kehitetty King Fahd University of Petroleum and Minerals -yliopiston tietojenkäsittelytieteiden ja tietokonetekniikan korkeakoulussa Saudi-Arabiassa. Se tarjoaa uuden valmiuksien kypsyysmallin kyberturvallisuustoimien toteutuksen mittaamiseen. ISMM-mallin tavoitteena on, että organisaatiot voivat mitata toteuttamisen edistymistä ajan myötä käyttämällä samaa mittaustyökalua säännöllisesti sen varmistamiseksi, että haluttu turvallisuustaso pidetään yllä. ISMM kehitettiin vuonna 2017.

Määritteet/ulottuvuudet

ISMM pohjautuu NIST-kehyksen olemassa oleviin arvioituihin alueisiin ja täydentää niitä vaatimustenmukaisuuden arviointia koskevalla ulottuvuudella. Näin ollen malliin sisältyy **23 arvioitavaa aluetta** organisaation turvallisuustasosta. 23 arvioitavaa aluetta ovat seuraavat:

i resurssien hallinta
ii toimintaympäristö
iii hallinto
iv riskinarviointi
v riskinhallintastrategia
vi vaatimustenmukaisuuden arviointi
vii käyttöoikeuksien hallinta
viii tietämys ja koulutus
ix tietoturva
x tietosuojaprosessit ja -menettelyt
xi ylläpito
xii suojaustekniikka
xiii poikkeamat ja tapahtumat

xiv jatkuva turvallisuuden valvonta
xv havaitsemisprosessit
xvi reagoinnin suunnittelu
xvii reagointia koskeva viestintä
xviii reagoinnin analyysi
xix reagoinnin lievennystoimet
xx reagoinnin kehittäminen
xxi toipumisen suunnittelu
xxii toipumisen kehittäminen sekä
xxiii toipumista koskeva viestintä.

Kypsyyden tasot

ISMM-malli perustuu **viiteen kypsyyden tasoon**, joita ei valitettavasti ole määritelty saatavilla olevassa dokumentaatiossa.

- **Taso 1:** suoritettu prosessi
- **Taso 2:** hallittu prosessi
- **Taso 3:** vakiintunut prosessi
- **Taso 4:** ennakoitava prosessi
- **Taso 5:** optimointiprosessi

Arviointimenetelmä

ISMM-mallissa ei esitetä organisaatioille mitään tiettyjä menetelmiä arvioinnin suorittamiseksi.

A.8 Sisäisen tarkastuksen valmiusmalli (IA-CM) julkiselle sektorille

Sisäisen tarkastuksen valmiusmallin (Internal Audit Capability Model – IA-CM) on kehittänyt sisäisten tarkastajien järjestön tutkimussäätiö IIARF tarkoituksenaan kehittää valmiuksia ja edunvalvontaa julkisen sektorin itsearvioinnin avulla. IA-CM on tarkoitettu tarkastusammattilaisille, ja se tarjoaa yleiskuvan itse mallista sekä soveltamisoppaan mallin käytöstä itsearvioinnin työkaluna.

Vaikka IA-CM koskee erityisesti sisäiseen tarkastukseen liittyviä valmiuksia eikä niinkään kyberturvallisuusvalmiuksien kehittämistä, malli on tehty kypsyyden itsearviointityökaluksi julkisen sektorin yksiköille, ja sitä voidaan soveltaa yleisesti prosessien ja tehokkuuden parantamista varten. Mallin soveltamisala ei keskity kyberturvallisuuteen, joten sen määritteitä ei analysoida. IA-CM valmistui vuonna 2009.

Kypsyyden tasot

Sisäisen tarkastuksen valmiusmalliin (IA-CM) sisältyy **viisi kypsyyden tasoa**, joista kukin kuvaa sisäisen tarkastustoiminnan ominaisuuksia ja valmiuksia kyseisellä tasolla. Mallin valmiustasot tarjoavat etenemissuunnitelman jatkuvaa kehittymistä varten.

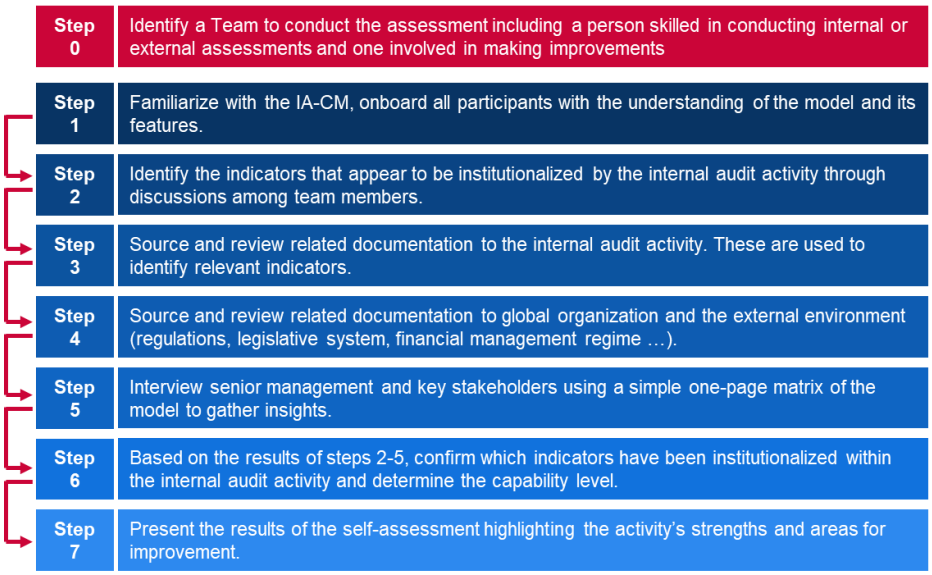
- **Taso 1: alustava**
  Ei kestäviä, toistettavia valmiuksia – yksittäisistä ponnisteluista riippuvainen.
  - Tilapäinen tai jäsentymätön.
  - Yksittäisiä asiakirjojen ja tapahtumien tarkkuutta ja vaatimustenmukaisuutta koskevia yhtenäisiä tarkastuksia tai arviointeja.
  - Tulokset riippuvat tietyn asemassa toimivan henkilön osaamisesta.
  - Ammattikäytäntöjä ei ole vahvistettu ammattijärjestöjen määrittämiä käytäntöjä lukuun ottamatta.
  - Johto hyväksyy rahoituksen tarpeen perusteella.
  - Infrastruktuuria ei ole.
  - Tarkastajat ovat todennäköisesti osa suurempaa organisaatioyksikköä.
  - Institutionaaliset valmiudet eivät ole kehittyneet.

- **Taso 2: infrastruktuuri**
  Kestävät ja toistettavat käytännöt ja menettelyt.
  - Tason 2 keskeinen kysymys tai haaste on, miten luodaan ja ylläpidetään prosessien toistettavuutta ja siten toistettavia valmiuksia.
  - Sisäisen tarkastuksen raportointiyhteyksiä, johtamis- ja hallintainfrastruktuureja sekä ammattikäytäntöjä ja -prosesseja muodostetaan (sisäisen tarkastuksen suuntaviivat, prosessit ja menettelyt).
  - Tarkastuksen suunnittelu perustuu pääasiassa johdon prioriteetteihin.
  - Tiettyjen henkilöiden taidoista ja osaamisesta ollaan edelleen huomattavan riippuvaisia.
  - Standardeja noudatetaan osittain.
- **Taso 3: integroitu**
  Hallinta- ja ammattikäytäntöjä sovelletaan yhdenmukaisesti.
  - Sisäisen tarkastuksen periaatteet, prosessit ja menettelyt on määritetty, dokumentoitu ja integroitu toisiinsa sekä organisaation infrastruktuuriin.
  - Sisäisen tarkastuksen hallinta- ja ammattikäytännöt ovat vakiintuneita, ja niitä sovelletaan yhdenmukaisesti sisäisen tarkastustoimen laajuisesti.
  - Sisäinen tarkastus alkaa olla linjassa organisaation liiketoiminnan ja sen kohtaamien riskien kanssa.
  - Sisäinen tarkastus kehittyy pelkästä perinteisten sisäisten tarkastusten suorittamisesta ja integroituu ryhmään sekä tarjoaa neuvoa suorituksiin ja riskien hallintaan.
  - Keskiössä ovat sisäisen tarkastustoimen ryhmän luominen ja sen valmiudet, riippumattomuus ja objektiivisuus.
  - Standardeja noudatetaan yleisesti.
- **Taso 4: hallittu**
  Eri puolilta organisaatiota peräisin olevaa tietoa integroidaan hallinnon ja riskinhallinnan parantamiseksi.
  - Sisäisen tarkastuksen ja keskeisten sidosryhmien odotukset ovat yhdenmukaisia.
  - Suorituskykymittareita käytetään sisäisen tarkastuksen prosessien ja tulosten mittaamiseksi ja seuraamiseksi.
  - Sisäisen tarkastuksen tunnustetaan tuovan organisaatiolle merkittävää lisäarvoa.
  - Sisäinen tarkastus toimii erottamattomana osana organisaation hallintoa ja riskinhallintaa.
  - Sisäinen tarkastus on hyvin hoidettu liiketoimintayksikkö.
  - Riskejä mitataan ja hallitaan kvantitatiivisesti.
  - Käytössä on tarvittavat taidot ja osaaminen, ja uudistumiseen ja tietojen jakamiseen on valmiudet (sisäisen tarkastuksen sisällä ja organisaation laajuisesti).
- **Taso 5: Optimointi**
  Organisaation sisältä ja ulkopuolelta lähtöisin oleva oppiminen jatkuvaa kehittymistä varten.
  - Sisäiseen tarkastukseen liittyy käsitys oppivasta organisaatiosta, jossa prosesseja parannetaan ja innovoidaan jatkuvasti.
  - Sisäinen tarkastus käyttää tietoa organisaation sisältä ja ulkoa edistääkseen strategisten tavoitteiden saavuttamista.
  - Suorituskyky on maailmanluokkaa ja/tai suositusten / parhaiden käytäntöjen mukainen.
  - Sisäinen tarkastus on kriittinen osa organisaation hallintorakennetta.
  - Ammatti- ja erikoisosaaminen on huipputasoa.
  - Yksilöiden, yksikön ja organisaation suorituskyvyn mittaukset on täysin integroitu
  - suoritusparannusten edistämiseksi.

Arviointimenetelmä

Sisäisen tarkastuksen valmiusmalli on kehitetty selkeästi itsearviointia varten Siinä on yksityiskohtaiset vaiheet IA-CM-mallin käyttämiseen sekä mukautettavat otantakalvot. Ennen itsearvioinnin aloittamista on määritettävä erityinen tiimi, johon kuuluu vähintään yksi sisäisiä tarkastuksia koskevien sisäisten tai ulkoisten arviointien suorittamisen osaava henkilö sekä yksi kyseistä alaa koskevien parannusten tekemiseen osallistuva henkilö.

Kuva 12: IC-AM-mallin itsearviointivaiheet



Step 0	Vaihe 0
Step 1	Vaihe 1
Step 2	Vaihe 2
Step 3	Vaihe 3
Step 4	Vaihe 4
Step 5	Vaihe 5
Step 6	Vaihe 6
Step 7	Vaihe 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Määritetään arvioinnin suorittava tiimi, johon kuuluu yksi sisäisten tai ulkoisten arviointien suorittamisen osaava henkilö sekä yksi parannusten tekemiseen osallistuva henkilö.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Tutustutaan IA-CM-malliin, perehdytetään kaikki osallistujat malliin ja sen ominaisuuksiin.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Tunnistetaan sisäisessä tarkastustoimessa institutionaalistuneilta vaikuttavat indikaattorit tiimin jäsenten välisillä keskusteluilla.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Hankitaan ja arvioidaan sisäiseen tarkastustoimeen liittyvää dokumentaatiota. Sitä käytetään merkityksellisten indikaattorien tunnistukseen.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Hankitaan ja arvioidaan yleisesti organisaatioon ja ulkoiseen ympäristöön liittyvää dokumentaatiota (säädökset, lainsäädäntöjärjestelmä, varainhoitojärjestelmä jne.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Haastatellaan ylempää johtoa ja keskeisiä sidosryhmiä käyttämällä mallista yksinkertaista yhden sivun matriisia näkemysten keräämiseksi.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the	Vahvistetaan vaiheiden 2–5 tulosten perusteella, mitkä indikaattorit ovat sisäisessä

internal audit activity and determine the capacity level.	tarkastustoimessa institutionalisoituneita, ja määritetään valmiuksien taso.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Esitellään itsearvioinnin tulokset tuomalla erityisesti esiin toiminnan vahvuuksia ja kehittämiskohteita.

A.9 Globaali kyberturvallisuusindeksi (GCI)

Globaali kyberturvallisuusindeksi (Global Cybersecurity Index – GCI) on Kansainvälisen televiestintäliiton (ITU) aloite, jonka tarkoituksena on arvioida kyberturvallisuuteen liittyvää sitoutumista ja tilannetta kaikilla ITU:n alueilla eli Afrikassa, Amerikoissa, arabimaissa, Aasian ja Tyynenmeren alueella, IVY-maissa ja Euroopassa ja jossa tuodaan esiin maita, joiden sitoutumisen taso on korkea ja joissa sovelletaan suositeltuja käytäntöjä. GCI-indeksin tavoitteena on auttaa maita tunnistamaan kyberturvallisuuteen liittyviä kehittämiskohteita sekä motivoida niitä ryhtymään toimiin sijoituksensa parantamiseksi eli auttaa nostamaan kyberturvallisuuden yleistä tasoa maailmanlaajuisesti.

GCI on indeksi eikä kypsyysmalli, joten siinä ei käytetä kypsyyden tasoja vaan pisteytystä maiden ja alueiden kyberturvallisuuteen liittyvän yleisen sitoutumisen arvioimiseksi ja vertailemiseksi.

Määritteet/ulottuvuudet

Globaali kyberturvallisuusindeksi (GCI) perustuu globaalin kyberturvallisuusagendan (Global Cybersecurity Agenda – GCA) viiteen pilariin. Pilarit muodostavat GCI-indeksin viisi alaindeksiä, joista kuhunkin sisältyy joukko indikaattoreita. Viisi pilaria ja niiden indikaattorit ovat seuraavat:

i **Oikeudellinen**: toimenpiteet, jotka perustuvat kyberturvallisuutta ja kyberrikollisuutta käsittelevien oikeudellisten instituutioiden ja kehysten olemassaoloon:
- kyberrikollisuutta koskeva lainsäädäntö
- kyberturvallisuutta koskeva sääntely ja
- roskapostin torjuntaa/hillitsemistä koskeva lainsäädäntö.

ii **Tekninen**: toimenpiteet, jotka perustuvat kyberturvallisuutta käsittelevien teknisten instituutioiden ja kehysten olemassaoloon:
- CERT/CIRT/CSRIT
- standardien täytäntöönpanokehys
- standardointielin
- tekniset mekanismit ja valmiudet, joita käytetään roskapostin torjumiseksi
- pilvipalvelujen käyttö kyberturvallisuustarkoituksiin ja
- mekanismit lasten suojelemiseksi verkossa.

iii **Organisatorinen**: toimenpiteet, jotka perustuvat kyberturvallisuuden kehittämistä koskevien politiikkaa koordinoivien instituutioiden ja strategioiden olemassaoloon kansallisella tasolla:
- kansallinen kyberturvallisuusstrategia
- vastaava virasto ja
- kyberturvallisuus.

iv **Valmiuksien kehittäminen**: toimenpiteet, jotka perustuvat valmiuksien kehittämistä edistävien tutkimus- ja kehitysohjelmien, koulutusohjelmien, sertifioitujen ammattilaisten ja julkisen sektorin laitosten olemassaoloon:
- julkiset tiedotuskampanjat
- kyberturvallisuusammattilaisten sertifiointia ja akkreditointia koskeva kehys
- ammatillisen koulutuksen kurssit kyberturvallisuuden alalla
- koulutusohjelmat tai akateemiset opetussuunnitelmat kyberturvallisuuden alalla
- kyberturvallisuutta koskevat tutkimus- ja kehitysohjelmat sekä
- kannustinmekanismit.

v **Yhteistyö**: toimenpiteet, jotka perustuvat kumppanuuksien, yhteistyökehysten ja tiedonjakoverkostojen olemassaoloon:
- kahdenväliset sopimukset
- monenväliset sopimukset

- osallistuminen foorumeihin/järjestöihin kansainvälisesti
- julkisen ja yksityisen sektorin kumppanuudet
- virastojen väliset/sisäiset kumppanuudet ja
- parhaat käytännöt.

Arviointimenetelmä

GCI on itsearviointityökalu, joka on kehitetty kahden vaihtoehdon kysymyksistä, esikoodatuista kysymyksistä sekä avoimista kysymyksistä koostuvasta kyselystä[30]. Kahden vastausvaihtoehdon käyttö ehkäisee mielipiteisiin perustuvaa arviointia ja mahdollista tietynlaisten vastausten suosimista. Esikoodatut vastaukset säästävät aikaa ja mahdollistavat tarkemman data-analyysin. Lisäksi yksinkertainen dikotominen asteikko mahdollistaa nopeamman ja monipuolisemman arvioinnin, sillä se ei edellytä pitkiä vastauksia. Tämä nopeuttaa ja tehostaa vastausten antamiseen ja muuhun arviointiin liittyvää prosessia. Vastaajan kuuluu vain vahvistaa, että tietyt ennalta määritetyt kyberturvallisuusratkaisut ovat tai eivät ole käytössä. Verkossa toimiva kyselymekanismi, jota käytetään vastausten keräämiseen ja asiaankuuluvan materiaalin lataamiseen verkkoon, mahdollistaa asiantuntijapaneelille hyvien käytäntöjen sekä temaattisten laadullisten arviointien erottelun.

GCI-prosessi toteutetaan kokonaisuudessaan seuraavasti:

- Kaikille osallistujille lähetetään kutsukirje, jossa tiedotetaan aloitteesta ja pyydetään yhteyspistevastaavaa keräämään kaikki asiaankuuluvat tiedot ja täyttämään verkossa toimiva GCI-kyselylomake. Verkkokyselyn aikana ITU kutsuu hyväksytyn yhteyspisteen virallisesti vastaamaan kyselylomakkeeseen.
- Perustietojen kerääminen (niiden maiden osalta, jotka eivät vastaa kyselylomakkeeseen):
  - ITU laatii kyselylomakkeeseen alustavan vastausluonnoksen käyttämällä julkisesti saatavilla olevia tietoja ja verkkotutkimusta.
  - Kyselylomakkeen luonnos lähetetään yhteyspisteisiin tarkastettavaksi.
  - Yhteyspisteet tarkentavat kyselylomakkeen luonnosta ja palauttavat sen sitten.
  - Korjattu kyselylomakkeen luonnos lähetetään kaikkiin yhteyspisteisiin lopullista hyväksyntää varten.
  - Validoitua kyselylomaketta käytetään analyysiin, pisteytykseen ja sijoituksen määrittämiseen.
- Toissijaisten tietojen kerääminen (niiden maiden osalta, jotka vastaavat kyselylomakkeeseen):
  - ITU määrittää mahdolliset puuttuvat vastaukset, täydentävät asiakirjat, linkit jne.
  - Yhteyspiste tarkentaa vastauksia tarvittaessa.
  - Korjattu kyselylomakkeen luonnos lähetetään kaikkiin yhteyspisteisiin lopullista hyväksyntää varten.
  - Validoitua kyselylomaketta käytetään analyysiin, pisteytykseen ja sijoituksen määrittämiseen.

A.10 Kybervoimaindeksi (CPI)

Kybervoimaindeksi (Cyber Power Index – CPI) luotiin Booz Allen Hamilton -yhtiön rahoittamassa Economist Intelligence Unit -tutkimusohjelmassa vuonna 2011. CPI on dynaaminen määrällinen ja laadullinen malli, […] jolla mitataan kyberympäristön erityisiä määritteitä seuraavien neljän kybervoimatekijän osalta: oikeudellinen kehys ja sääntelykehys, taloudellinen ja sosiaalinen konteksti, tekninen infrastruktuuri sekä keskeisillä aloilla tapahtuvaa digitaalista edistymistä koskeva soveltaminen teollisuudessa[31]. Kybervoimaindeksin tavoitteena on vertailla G20-maiden valmiuksia kestää kyberhyökkäyksiä ja hyödyntää menestyvältä ja turvalliselta taloudelta vaadittavaa digitaalista infrastruktuuria. CPI-indeksin vertailussa

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf
[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

keskitytään 19 G20-maahan (pois luettuna EU). Maiden sijoitus määritetään indeksissä kunkin indikaattorin suhteen.

Määritteet/ulottuvuudet

Kybervoimaindeksi (CPI) perustuu neljään kybervoimatekijään. Kutakin kategoriaa mitataan useiden indikaattorien avulla, jotta kaikille maille saadaan oma pisteytys. Kategoriat ja niiden pilarit ovat seuraavat:

i **Oikeudellinen kehys ja sääntelykehys**
- Hallinnon sitoutuminen kyberkehitykseen
- Kybersuojausperiaatteet
- Kybersensuuri (tai sen puuttuminen)
- Politiikan tehokkuus
- Teollis- ja tekijänoikeuksien suojelu

ii **Taloudellinen ja sosiaalinen konteksti**
- Koulutustaso
- Tekninen osaaminen
- Kaupan avoimuus
- Liiketoimintaympäristön innovatiivisuus

iii **Tekninen infrastruktuuri**
- Tieto- ja viestintätekniikan saavutettavuus
- Tieto- ja viestintätekniikan laatu
- Tieto- ja viestintätekniikan edullisuus
- Tietotekniikkaan kohdistuvat menot
- Suojattujen palvelimien määrä

iv **Soveltaminen elinkeinoelämässä**
- Älykkäät verkot
- Sähköinen terveydenhuolto
- Sähköinen kaupankäynti
- Älykäs liikenne
- Sähköinen hallinto

Arviointimenetelmä

CPI on määrällinen ja laadullinen pisteytysmalli. Economist Intelligence Unit suoritti arvioinnin käyttämällä kvantitatiivisia indikaattoreita saatavilla olevista tilastollisista lähteistä sekä tekemällä arvioita, kun tiedot olivat puutteelliset. Pääasialliset lähteet ovat Economist Intelligence Unit, YK:n kasvatus-, tiede- ja kulttuurijärjestö (Unesco), Kansainvälinen televiestintäliitto (ITU) sekä Maailmanpankki.

A.11 Kybervoimaindeksi (CPI)

Tässä osiossa tiivistetään tämänhetkisiä kypsyysmalleja koskevan analyysin tärkeimmät havainnot. Taulukko 5: Yleiskatsaus analysoituihin kypsyysmalleihin antaa yleiskuvan kunkin mallin tärkeimmistä ominaisuuksista muokatun Beckerin mallin mukaan. Taulukko 6: Kypsyystasojen vertailu sisältää analysoitujen mallien kypsyystasoja koskevat korkean tason määritelmät. Taulukko 7 antaa yleiskuvan kussakin mallissa käytetyistä ulottuvuuksista tai määritteistä.

Taulukko 5: yleiskatsaus analysoituihin kypsyysmalleihin

Mallin nimi	Alkuperä	Tarkoitus	Kohderyhmä	Tasojen määrä	Määritteiden määrä	Arviointimenetelmä	Tulosten kuvaus
Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (CMM)	Global Cybersecurity Capacity Centre, Oxfordin yliopisto	Kyberturvallisuusvalmiuksien kehittämisen laajentaminen ja tehostaminen kansainvälisesti	Maat	5	5 pääasiallista ulottuvuutta	Yhteistyö paikallisen organisaation kanssa mallin hienosäätämiseksi ennen sen soveltamista kansalliseen kontekstiin	Viisisektorinen tutkakaavio
Kyberturvallisuusvalmiuksien kypsyysmalli (C2M2)	Yhdysvaltain energiaministeriö (DOE)	Organisaatioiden auttaminen kyberturvallisuusohjelmiensa arvioimisessa ja parantamisessa sekä toimintansa häiriönsietokyvyn vahvistamisessa	Kaikkien alojen kaikentyyppiset ja kaikenkokoiset organisaatiot	4	10 pääasiallista kohdealuetta	Itsearviointimenetelmä ja työkalusarja	Pisteytyskortti piirakkakaavioilla
Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi	Yhdysvaltain kansallinen standardi- ja teknologiainstituutti (NIST)	Kehyksen tarkoituksena on organisaatioiden kyberturvallisuustoimien ohjaaminen ja riskien hallinta	Organisaatiot	N/A (4 tasoa)	5 ydintoimintoa	Itsearviointi	-
Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Q-C2M2)	Qatarin yliopiston oikeustieteellinen korkeakoulu	Sellaisen toimivan mallin tarjoaminen, jota voidaan käyttää Qatarin kyberturvallisuuskehyksen vertailemiseen, mittaamiseen ja kehittämiseen	Qatarilaiset organisaatiot	5	5 pääasiallista kohdealuetta	–	-
Kyberturvallisuuden kypsyysmallisertifiointi (CMMC)	Yhdysvaltain puolustusministeriö (DOD)	Parhaiden kyberturvallisuuskäytäntöjen edistäminen tietojen suojaamiseksi	Puolustusteollisen perustan (DIB) alan organisaatiot	5	17 pääasiallista kohdealuetta	Ulkopuolisten tarkastajien suorittama arviointi	-
Yhteisön kyberturvallisuuden kypsyysmalli (CCSMM)	Center for Infrastructure Assurance and Security, Texasin yliopisto	Yhteisön kybervalmiuksien kulloisenkin tilan määrittäminen sekä sellaisen etenemissuunnitelman tarjoaminen, jota yhteisöt voivat seurata valmisteluissaan	Yhteisöt (paikallis- tai osavaltiohallinnot)	5	6 pääasiallista ulottuvuutta	Yhteisöjen sisäinen arviointi osavaltion ja liittovaltion lainvalvontaviranomaisten avustuksella	-
Tietoturvan kypsyysmalli NIST-kyberturvallisuuskehystä varten (ISMM)	Tietojenkäsittelytieteiden ja tietokonetekniikan korkeakoulu, King Fahd University of Petroleum and Minerals -yliopisto, Dhahran, Saudi-Arabia	Sen mahdollistaminen, että organisaatiot voivat mitata toteutuksensa edistymistä ajan myötä varmistaakseen halutun turvallisuustason ylläpitämisen	Organisaatiot	5	23 arvioitavaa aluetta	–	-
Sisäisen tarkastuksen valmiusmalli (IA-CM) julkiselle sektorille	Sisäisten tarkastajien järjestön tutkimussäätiö IIARF	Sisäisen tarkastuksen valmiuksien ja edunvalvonnan kehittäminen julkisen sektorin itsearvioinnin avulla	Julkisen sektorin organisaatiot	5	6 elementtiä	Itsearviointi	-

Globaali kyberturvallisuusindeksi (GCI)	Kansainvälinen televiestintäliitto (ITU)	Kyberturvallisuuteen liittyvän sitoutumisen arviointi sekä maiden auttaminen tunnistamaan kyberturvallisuuteen liittyviä kehittämiskohteita	Maat	N/A	5 pilaria	Itsearviointi	Sijoitustaulukko
Kybervoimaindeksi (CPI)	Economist Intelligence Unit ja Booz Allen Hamilton	Vertailu, joka koskee G20-maiden valmiuksia kestää kyberhyökkäyksiä ja hyödyntää vaadittavaa menestyvän ja turvallisen talouden digitaalista infrastruktuuria	G20-maat	N/A	4 kategoriaa	Economist Intelligence Unitin suorittama vertailu	Sijoitustaulukko

Taulukko 6: kypsyystasojen vertailu

Malli	Taso 1	Taso 2	Taso 3	Taso 4	Taso 5
Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (CMM)	**Käynnistys** Kyberturvallisuuskypsyyttä ei vielä ole tai se on luonteeltaan hyvin kehittymätöntä. Kyberturvallisuusvalmiuksien kehittämisestä saatetaan käydä alustavia keskusteluja, mutta konkreettisiin toimiin ei ole vielä ryhdytty. Havaittavaa näyttöä ei tässä vaiheessa vielä ole.	**Kehitys** Jotkut näkökohtien osat ovat alkaneet kasvaa ja muotoutua, mutta ne voivat olla tilapäisiä, sekavia, huonosti määriteltyjä – tai yksinkertaisesti uusia. Toimintaa koskevaa näyttöä on kuitenkin jo selvästi osoitettavissa.	**Vakiintunut** Näkökohdan elementit ovat paikallaan ja toiminnassa. Tarkkaa harkintaa resurssien suhteellisesta kohdentamisesta ei ole kuitenkaan tehty. Näkökohdan eri elementteihin kohdistuvan ”suhteellisen” investoinnin jakamisesta on tehty vain vähän päätöksiä. Näkökohta on kuitenkin toimiva ja määritetty.	**Strateginen** On tehty päätöksiä siitä, mitkä näkökohdan osat ovat kyseessä olevalle organisaatiolle tai valtiolle tärkeitä ja mitkä vähemmän tärkeitä. Strateginen vaihe kuvastaa sitä, että kyseiset päätökset on tehty – valtion tai organisaation olosuhteiden mukaisesti.	**Dynaaminen** Käytössä on selkeitä mekanismeja strategian muuttamiseksi vastaamaan vallitsevia olosuhteita, kuten uhkaympäristön teknologiaa, globaalia konfliktia tai jossakin huolenaiheessa (esim. kyberrikollisuus tai tietosuoja) tapahtunutta merkittävää muutosta. Dynaamiset organisaatiot ovat kehittäneet menetelmiä strategioiden joustavaa muuttamista varten. Tälle vaiheelle ominaisia ovat nopea päätöksenteko, resurssien uudelleen kohdentaminen sekä muuttuvan ympäristön jatkuva huomiointi.
Kyberturvallisuusvalmiuksien kypsyysmalli (C2M2)	**MIL0** Käytäntöjä ei sovelleta.	**MIL1** Alustavia käytäntöjä sovelletaan, mutta ne voivat olla tilapäisiä.	**MIL2** Hallintaominaisuudet: käytännöt on dokumentoitu, prosessin tukemiseksi tarjotaan riittävät resurssit, käytäntöjä soveltavalla henkilöstöllä on riittävä osaaminen ja tietämys, käytäntöjen soveltamista koskevat vastuut ja valtuudet on jaettu. Menettelytapaominaisuus: käytännöt ovat valmiimpia tai edistyneempiä kuin tasolla MIL1.	**MIL3** Hallintaominaisuudet: toiminta on periaatteiden (tai muiden organisatoristen suuntaviivojen) ohjaamaa, kohdealueen toiminnan suorituskykytavoitteet on määritetty, ja niitä valvotaan saavutusten seuraamiseksi, kohdealueen toiminnan dokumentoituja käytäntöjä standardoidaan ja parannetaan toimijan laajuisesti.	–

				Menettelytapaominaisuus: käytännöt ovat valmiimpia tai edistyneempiä kuin tasolla MIL2.	
Tietoturvan kypsyysmalli NIST-kyberturvallisuuskeskeistä varten (ISMM)	**Suoritettu prosessi**	**Hallittu prosessi**	**Vakiintunut prosessi**	**Ennakoitava prosessi**	**Optimointiprosessi**
Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Q-C2M2)	**Alustus** Tilapäisiä kyberturvallisuuskäytäntöjä ja -prosesseja käytetään joillakin kohdealueilla.	**Kehitys** Periaatteet ja käytännöt kohdealueille kuuluvien kyberturvallisuustoimien kehittämiseksi ja parantamiseksi on pantu täytäntöön, ja tavoitteena on esittää toteutettaviksi uusia toimia.	**Toteutus** Periaatteet kaikkien kohdealueille kuuluvien kyberturvallisuustoimien toteuttamiseksi on hyväksytty, ja tavoitteena on saattaa toteutus päätökseen tietyssä ajassa.	**Mukautuva** Kyberturvallisuustoimia tarkastellaan ja arvioidaan ja käytäntöjä otetaan käyttöön aikaisemmista kokemuksista ja toimenpiteistä saatujen ennakoivien indikaattorien perusteella.	**Ketterä** Mukautuvaa vaihetta jatketaan kiinnittämällä entistä enemmän huomiota ketteryyteen ja nopeuteen kohdealueilla toteutettavien toimien yhteydessä.
Kyberturvallisuuden kypsyysmallisertifiointi (CMMC)	**Prosessit: suoritettu** Organisaatio saattaa pystyä suorittamaan kyseiset käytännöt ainoastaan tilapäisesti ja voi turvautua tai olla turvautumatta dokumentaatioon. Tasolla 1 ei arvioida prosessien kypsyyttä. **Käytännöt: perustason kyberhygienia** Taso 1 koskee erityisesti liittovaltion sopimustietojen suojaamista ja koostuu vain perustason suojausvaatimuksia vastaavista käytännöistä.	**Prosessit: dokumentoitu** Tasolle 2 päästäkseen organisaation on määritettävä ja dokumentoitava käytännöt ja periaatteet CMMC-pyrkimystensä toteutuksen ohjaamiseksi. Käytäntöjen dokumentoinnin ansiosta yksilöt voivat toteuttaa niitä toistettavalla tavalla. Organisaatiot kehittävät kypsiä valmiuksia dokumentoimalla prosessinsa ja panemalla ne sitten täytäntöön dokumentoinnin mukaisesti. **Käytännöt: keskitason kyberhygienia** Taso 2 on siirtymävaihe tasolta 1 tasolle 3 ja koostuu joukosta julkaisussa NIST SP 800-171 määriteltyjä turvavaatimuksia sekä muista standardeista ja referensseistä peräisin olevista käytännöistä.	**Prosessit: hallittu** Tasolle 3 päästäkseen organisaation on laadittava suunnitelma, jossa osoitetaan käytäntöjen toteuttamiseksi suoritettavien toimien hallinta, ylläpidettävä kyseistä suunnitelmaa ja annettava resurssit sitä varten. Suunnitelma voi sisältää tietoa tehtävistä, tavoitteista, projektisuunnitelmista, resursoinnista, tarvittavasta koulutuksesta sekä asiaankuuluvien sidosryhmien osallistamisesta. **Käytännöt: hyvä kyberhygienia** Taso 3 koskee erityisesti valvotun luokittelemattoman tiedon (CUI) suojaamista ja kattaa kaikki julkaisussa NIST SP 800-171 määritellyt turvavaatimukset sekä muista standardeista ja referensseistä peräisin olevat lisäkäytännöt uhkien lieventämiseksi.	**Prosessit: tarkastettu** Tasolle 4 päästäkseen organisaation on tarkastettava ja mitattava käytäntöjensä tehokkuus. Käytäntöjen tehokkuuden mittaamisen lisäksi tällä tasolla olevat organisaatiot voivat ryhtyä tarvittaessa korjaustoimenpiteisiin. Ja ne tiedottavat ylemmän tason johdolle tilasta tai ongelmista toistuvasti. **Käytännöt: proaktiivinen** Taso 4 koskee erityisesti valvotun luokittelemattoman tiedon (CUI) suojaamista ja kattaa joukon korotettuja turvavaatimuksia. Näillä käytännöillä parannetaan organisaation havaitsemis- ja reagointivalmiuksia, joiden avulla se voi puuttua ja mukautua muuttuviin taktiikoihin, tekniikoihin ja menetelmiin.	**Prosessit: optimointi** Tasolle 5 päästäkseen organisaation on standardoitava ja optimoitava prosessien toteutus organisaation laajuisesti. **Käytännöt: edennyt/etenevä** Taso 5 koskee erityisesti valvotun luokittelemattoman tiedon (CUI) suojaamista. Lisäkäytännöt kasvattavat kyberturvallisuusvalmiuksien syvyyttä ja kehittyneisyyttä.
Yhteisön kyberturvallisuuden kypsyysmalli (CCSMM)	**Turvallisuustietoinen** Tällä tasolla toiminnan pääasiallisena teemana on tehdä yksilöistä ja organisaatioista tietoisia kyberturvallisuuteen	**Prosessin kehittäminen** Taso on suunniteltu auttamaan yhteisöjä luomaan ja parantamaan turvallisuusprosesseja, joita	**Tiedot käytössä** Taso on suunniteltu parantamaan yhteisön sisäisiä tiedonjakomekanismeja, jotta yhteisössä voidaan tehokkaasti	**Taktiikan kehittäminen** Tämän tason elementit on suunniteltu entistä parempien ja proaktiivisempien menetelmien kehittämiseen hyökkäysten havaitsemista ja niihin reagointia	**Täysi turvallisuuteen liittyvä toimintavalmius** Tämä taso kuvastaa elementtejä, jotka organisaatiolla pitäisi olla käytössään voidakseen pitää itseään täysin toimintavalmiina

	liittyvistä uhista, ongelmista ja kysymyksistä.	kyberturvallisuuskysymysten tehokas käsittely edellyttää.	yhdistää näennäisesti erillisiä tiedonpalasia.	varten. Tähän tasoon mennessä suurimman osan ennaltaehkäisevistä menetelmistä pitäisi olla käytössä.	puuttumaan mihin tahansa kyberuhkaan.
Sisäisen tarkastuksen valmiusmalli (IA-CM) julkiselle sektorille	**Alustava** Ei kestäviä, toistettavia valmiuksia – yksittäisistä ponnisteluista riippuvainen.	**Infrastruktuuri** Kestävät ja toistettavat käytännöt ja menettelyt.	**Integroitu** Hallinta- ja ammattikäytäntöjä sovelletaan yhdenmukaisesti.	**Hallittu** Eri puolilta organisaatiota peräisin olevaa tietoa integroidaan hallinnon ja riskinhallinnan parantamiseksi.	**Optimointi** Oppiminen organisaation sisältä ja ulkoa jatkuvaa kehittymistä varten.

Taulukko 7: Ulottuvuuksien ja määritteiden vertaileminen

	Valtioiden kyberturvallisuusvalmiuksien kypsyysmalli (CMM)	Kyberturvallisuusvalmiuksien kypsyysmalli (C2M2)	Qatarin kyberturvallisuusvalmiuksien kypsyysmalli (Q-C2M2)	Kyberturvallisuuden kypsyysmallisertifiointi (CMMC)	Kyberturvallisuuden kypsyysmallisertifiointi (CMMC)	Tietoturvan kypsyysmalli NIST-kyberturvallisuuskehystä varten (ISMM)	Kehys kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi	Globaali kyberturvallisuusindeksi (GCI)	Kybervoimaindeksi (CPI)
Tasot	Viisi ulottuvuutta jaettuna useisiin tekijöihin, jotka puolestaan sisältävät useita näkökohtia ja indikaattoreita (Kuva 4)	Kymmenen kohdealuetta, joihin sisältyy ainutlaatuinen hallintatavoite ja useita menettelytapatavoitteita (Kuva 6)	Viisi kohdealuetta, jotka on jaettu alikohdealueisiin	17 kohdealuetta jaettuna prosesseihin sekä yhteen tai useampaan valmiuteen, jotka puolestaan eritellään käytäntöihin (Kuva 9)	Kuusi pääasiallista ulottuvuutta	23 arvioitavaa aluetta	Viisi toimintoa, joiden taustalla on keskeiset kategoriat ja alakategoriat (Kuva 8)	Viisi pilaria, joihin sisältyy useita indikaattoreita	Neljä kategoriaa, joihin sisältyy useita indikaattoreita
Määritteet/ulottuvuudet	i Kyberturvallisuuspolitiikan ja -strategian laatiminen ii Yhteiskunnan vastuullisen kyberturvallisuuskulttuurin edistäminen iii Kyberturvallisuustietämyksen kehittäminen iv Tehokkaiden oikeudellisten kehysten ja sääntelykehysten luominen v Riskien hallinta standardien, organisaatioiden ja teknologioiden avulla	i Riskinhallinta ii Resurssien, muutoksen ja kokoonpanon hallinta iii Identiteetin ja pääsyn hallinta iv Uhkien ja haavoittuvuuksien hallinta v Tilannetietoisuus vi Kybertapahtumiin ja -häiriöihin reagointi vii Toimitusketjun ja ulkoisten riippuvuuksien hallinta viii Työvoiman hallinta ix Kyberturvallisuusarkkitehtuuri x Kyberturvallisuusohjelman hallinta	i Ymmärrä (kyberhallinto, resurssit, riskit ja koulutus) ii Turvaa (tietoturvallisuus, tekniikkaturvallisuus, käyttöoikeuksien hallinnan turvallisuus, viestinnän turvallisuus sekä henkilöstöturvallisuus) iii Paljasta (valvonta, kybertapahtumien hallinta, havaitseminen, analyysi ja paljastaminen) iv Reagoi (reagoinnin suunnittelu, lievennystoimet sekä reagointia koskeva viestintä) v Säilytä (toipumisen suunnittelu, jatkuvuuden hallinta, parannukset sekä ulkoiset riippuvuudet)	i Käyttöoikeuksien hallinta ii Resurssien hallinta iii Tarkastus ja vastuuvelvollisuus iv Tietoisuus ja koulutus v Kokoonpanon hallinta vi Tunnistus ja todentaminen vii Kybertapahtumiin reagointi viii Ylläpito ix Median suojaus x Henkilöstöturvallisuus xi Fyysinen suojaus xii Toipuminen xiii Riskinhallinta xiv Turvallisuusarviointi xv Tilannetietoisuus xvi Järjestelmien ja viestinnän suojaaminen xvii Järjestelmien ja tietojen eheys	i Uhat, joihin puututaan ii Mittarit iii Tietojen jakaminen iv Teknologia v Koulutus vi Testaus	i Resurssien hallinta ii Liiketoimintaympäristö iii Hallinto iv Riskinarviointi v Riskinhallintastrategia vi Vaatimustenmukaisuuden arviointi vii Käyttöoikeuksien hallinta viii Tietoisuus ja koulutus ix Tietoturva x Tietosuojaprosessit ja -menettelyt xi Ylläpito xii Suojaustekniikka xiii Poikkeamat ja tapahtumat xiv Jatkuva turvallisuuden valvonta xv Havaitsemisprosessit xvi Reagoinnin suunnittelu xvii Reagointia koskeva viestintä xviii Reagoinnin analyysi xix Reagoinnin lievennystoimet xx Reagoinnin parannukset xxi Toipumisen suunnittelu xxii Toipumisen parannukset xxiii Toipumista koskeva viestintä	i Tunnistus ii Suojaus iii Havaitseminen iv Reagointi v Toipuminen	i Oikeudellinen ii Tekninen iii Organisatorinen iv Valmiuksien kehittäminen v Yhteistyö	i Oikeudellinen kehys ja sääntelykehys ii Taloudellinen ja sosiaalinen konteksti iii Tekninen infrastruktuuri iv Soveltaminen elinkeinoelämässä

LIITE B – AINEISTOTUTKIMUKSEN LÄHDELUETTELO

Almuhammadi, S. ja Alsaleh, M. (2017). ”Information Security Maturity Model for Nist Cyber Security Framework”. Sarjassa Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. ja Alsaleh, M. (2017). ”Information Security Maturity Model for Nist Cyber Security Framework”. Sarjassa Computer Science & Information Technology (CS & IT). Saatavilla osoitteessa https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016). Stocktaking, analysis and recommendations on the protection of CIIs. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. Saatavilla osoitteessa https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgian hallitus (2012). Cyber Security Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018). Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Saatavilla osoitteessa https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012). ”Introduction to Return on Security Investment”.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019). ”Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Saatavilla osoitteessa https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019). National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Saatavilla osoitteessa https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Portugalin ministerineuvosto (2019). Portugalin virallinen lehti, 1 sarja – N:o 108 – Ministerineuvoston päätös N:o 92/2019. Saatavilla osoitteessa https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016). Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity – Self-assessment Tool (ei päivämäärää). Saatavilla osoitteessa https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Euroopan neuvoston ja Euroopan unionin CyberCrime@IPA-hanke, Euroopan neuvoston Global Project on Cybercrime -hanke ja kyberrikollisuutta käsittelevä Euroopan unionin erityisryhmä (2011). Specialised cybercrime units – Good practice study. Saatavilla osoitteessa https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (ei päivämäärää). Saatavilla osoitteessa https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017). Public Private Partnerships (PPP).

Darra, E. (ei päivämäärää). ”Welcome to the NCSS Training Tool”.

Dekker, M. A. C. (2014). Technical Guideline on Incident Reporting. Saatavilla osoitteessa https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014). Technical Guideline on Security Measures. Saatavilla osoitteessa https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015). Guideline on Threats and Assets. Saatavilla osoitteessa https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016). Cybersecurity Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014). *Privacy and data protection by design – from policy to engineering.* Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Euroopan komissio (2012). Euroopan parlamentin ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla. Saatavilla osoitteessa https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Euroopan unionin verkko- ja tietoturvavirasto (2012). NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

Euroopan unionin verkko- ja tietoturvavirasto (2012). NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

Euroopan unionin verkko- ja tietoturvavirasto (2016). Guidelines for SMEs on the security of personal data processing.

Euroopan unionin verkko- ja tietoturvavirasto (2016). NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

Euroopan unioni ja Euroopan unionin verkko- ja tietoturvavirasto (2017). Handbook on security of personal data processing. Saatavilla osoitteessa http://dx.publications.europa.eu/10.2824/569768

Euroopan unioni ja Euroopan unionin verkko- ja tietoturvavirasto (2014). *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Saatavilla osoitteessa http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015). Memorandum for Heads of Executive Departments and Agencies. Saatavilla osoitteessa https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Itävallan liittokanslerin virasto (2013). Austrian Cyber Security Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Saksan liittotasavallan sisäasiainministeriö (2011). Cyber Security Strategy for Germany. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016). NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Euroopan unioni ja Euroopan unionin verkko- ja tietoturvavirasto (2015). The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Ranskan pääministerin kanslia (2014). French National Digital Security Strategy. Saatavilla osoitteessa https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015). Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017). ”Evaluating Business Process Maturity Models”. Journal of the Association for Information Systems. Saatavilla osoitteessa https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Bulgarian hallitus (2015). National Cyber Security Strategy – Cyber-resistant Bulgaria 2020.

Kroatian hallitus (2015). The National Cyber Security Strategy of The Republic of Croatia. Saatavilla osoitteessa https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Kreikan hallitus (2017). National Cyber Security Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Unkarin hallitus (2018). Strategy for the Security of Network and Information Systems. Saatavilla osoitteessa https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Irlannin hallitus (2019). National Cyber Security Strategy. Saatavilla osoitteessa https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Espanjan hallitus (2019). National Cyber Security Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Institute of Internal Auditors (toim.) (2009). Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Kansainvälinen televiestintäliitto (ITU) (2018). The Global Cybersecurity Index. Saatavilla osoitteessa https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Kansainvälinen televiestintäliitto (ITU) (2018). Guide to developing a national cybersecurity strategy. Saatavilla osoitteessa https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019). ”Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework”. International Review of Law.

Latvian hallitus (2014). Cyber Security Strategy of Latvia. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014). An evaluation framework for national cyber security strategies. Heraklion: ENISA. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014). *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Maltan kilpailukyvystä ja digitaali-, meri- ja palvelutaloudesta vastaava ministeriö (2016). Malta Cyber Security Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Viron talous- ja viestintäministeriö (2019). Cybersecurity Strategy – Republic of Estonia. Saatavilla osoitteessa https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Liettuan tasavallan puolustusministeriö (2018). National Cyber Security Strategy

Tšekin tasavallan kansallinen kyberturvallisuuskeskus (2015). National Cyber Security Strategy of the Czech Republic. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cyber Security Strategies – Interactive Map (ei päivämäärää). Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018). Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Yhdysvaltojen kansallinen standardi- ja teknologiainstituutti (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Saatavilla osoitteessa http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008). Business Process Maturity Model. Saatavilla osoitteessa https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Euroopan unioni ja yhteinen tutkimuskeskus – Euroopan komissio (2008). Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Saatavilla osoitteessa https://www.oecd.org/sdd/42495745.pdf.

Kyproksen sähköisestä viestinnästä ja postisäännöistä vastaavan komissaarin toimisto (2012). Cybersecurity Strategy of the Republic of Cyprus.

Euroopan unionin virallinen lehti (2008). NEUVOSTON DIREKTIIVI 2008/114/EY, annettu 8 päivänä joulukuuta 2008, Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista. Saatavilla osoitteessa https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Taloudellisen yhteistyön ja kehityksen järjestö (OECD) (2012). Cybersecurity policy making at a turning point. Saatavilla osoitteessa http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012). ”National Cyber Security Strategies – Practical Guide on Development and Execution”.

Ouzounis, E. (2012). Good Practice Guide on National Exercises.

Portesi, S. (2017). Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Italian pääministerin kanslia (2017). The Italian Cybersecurity Action Plan. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019). Dziennik Urzędowy Rzeczypospolitej Polskiej. Saatavilla osoitteessa http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Romanian hallitus (2013). Cyber security strategy of Romania. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. ja Euroopan unionin kyberturvallisuusvirasto (2019). Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Saatavilla osoitteessa https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Suomen turvallisuuskomitean sihteeristö (2019). Finland’s Cyber Security Strategy 2019. Saatavilla osoitteessa https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovakian hallitus (2015). Cyber Security Concept of the Slovak Republic. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015). Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016). ”Directive (EU) 2016/1148/EU of the European Parliament and of the Council of 7 July 2010”. Teoksessa Smith, R., Core EU Legislation. London: Macmillan Education. Saatavilla osoitteessa https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017). European Cyber Security Month 2017.

Ruotsin hallitus (2017). Nationell strategi för samhällets informations- och cybersäkerhet. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Tanskan hallitus – valtiovarainministeriö (2018). Danish Cyber and Information Security Strategy. Saatavilla osoitteessa https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Sveitsin liittoneuvosto (2018). National strategy for the protection of Switzerland against cyber risks.

Luxemburgin valtioneuvosto (2018). National Cybersecurity Strategy. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Alankomaiden hallitus (2018). National Cyber Security Agenda. Saatavilla osoitteessa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Valkoinen talo (2018). National Cyber Strategy of the United States of America. Saatavilla osoitteessa https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011). Cyber Europe Report. Saatavilla osoitteessa https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. ja Euroopan unionin verkko- ja tietoturvavirasto (2013). *National-level risk assessments: an analysis report.* Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015). Report on cyber-crisis cooperation and management. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015). Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Saatavilla osoitteessa http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016–2021 (2016). Saatavilla osoitteessa https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck et al. (2009). Understanding Maturity Models.

Wamala, D. F. (2011). ITU National Cybersecurity Strategy Guide. Saatavilla osoitteessa https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007). ”The Community Cyber Security Maturity Model”. Teoksessa 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07).

LIITE C – MUUT TUTKITUT TAVOITTEET

Jäljempänä tarkemmin kuvattuja tavoitteita tutkittiin osana aineistotutkimusvaihetta ja ENISAn suorittamia haastatteluja. Seuraavat tavoitteet eivät ole osa kansallisten valmiuksien arviointikehystä, mutta niiden avulla voidaan valottaa aiheita, joita on syytä pohtia. Kaikissa seuraavissa alaluvuissa annetaan selvitys tavoitteen hylkäämisen syistä.

- Kehitetään alakohtaisia kyberturvallisuusstrategioita;
- Torjutaan väärää tietoa levittäviä kampanjoita
- Turvataan huipputeknologioita (5G, tekoäly, kvanttilaskenta jne.)
- Varmistetaan datasuvereniteetti
- Tarjotaan kannustimia kybervakuutusalan kehittämiseen.

Kehitetään alakohtaisia kyberturvallisuusstrategioita

Sellaisten alakohtaisten strategioiden hyväksymisellä, jotka kohdistuvat alan interventioihin ja kannustimiin, korostetaan vahvempaa hajautettua osaamista. Tämä soveltuu hyvin jäsenvaltioille, joiden keskeisten palvelujen tarjoajat joutuvat toimimaan eri puitteiden ja määräysten mukaisesti ja joissa on useita riippuvuuksia kyberturvallisuuden monialaisen luonteen vuoksi. Useissa jäsenvaltioissa on tavanomaista, että on useita kansallisia viranomaisia ja sääntelyelimiä, joilla on tietämystä kunkin alan erityispiirteistä ja joilla on valtuudet valvoa erityisen sääntelyn noudattamista kullakin alalla.

Tanskassa käynnistettiin esimerkiksi kuusi kohdennettua strategiaa, jotka liittyvät kriittisimpien alojen kyber- ja tietoturvatöihin, vahvemman hajautetun osaamisen kehittämiseksi kyber- ja tietoturvallisuudessa. Kukin alakohtainen yksikkö edistää muun muassa uhkien arviointia alakohtaisella tasolla, valvontaa, valmiusharjoituksia, turvajärjestelmien perustamista, tietämyksen jakamista ja ohjeistusta. Alakohtaiset strategiat kattavat seuraavat alat:

- Energia
- Terveydenhuolto
- Liikenne
- Tietoliikenne
- Talous
- Merenkulku.

Muut jäsenvaltiot ovat ilmaisseet olevansa kiinnostuneita harkitsemaan alakohtaisia kyberturvallisuusstrategioita kaikkien sääntelyvaatimusten ilmentämiseksi. On kuitenkin huomattava, että kyseinen tavoite ei välttämättä sovellu kaikille jäsenvaltioille niiden koon, kansallisten toimintalinjojen ja maturiteetin perusteella. Koska on varsin vaikea varmistaa, että kehyksessä voidaan huomioida kaikki erityispiirteet, ENISA päätti jättää kyseisen tavoitteen pois kehyksestä.

Torjutaan väärän tiedon levityskampanjoita

Jäsenvaltiot sisällyttävät perusperiaatteiden, kuten ihmisoikeuksien, avoimuuden ja julkisen luottamuksen, suojelun kansallisiin kyberturvallisuusstrategioihinsa. Tämä on erityisen tärkeää, kun on kyse disinformaatiosta, jota levitetään perinteisten tiedotusvälineiden tai sosiaalisen median alustojen kautta. Kyberturvallisuus on lisäksi yksi suurimmista vaaleihin liittyvistä

haasteista tällä hetkellä. Toimia, kuten väärän tiedon tai kielteisen propagandan levittämistä, on havaittu useissa maissa ennen tärkeitä vaaleja. Tämä uhka voi heikentää EU:n demokraattista prosessia. Euroopan tasolla komissio on laatinut toimintasuunnitelman[32] tehostaakseen toimia disinformaation torjumiseksi Euroopassa. Kyseisessä suunnitelmassa keskitytään neljään keskeiseen alueeseen (tunnistaminen, yhteistoiminta verkkoalustayhteistyö ja tietämys), ja sen tavoitteena on EU:n valmiuksien kehittäminen ja jäsenvaltioiden välisen yhteistyön vahvistaminen.

Haastatelluista 19 maasta neljä on ilmaissut aikomuksensa ratkaista disinformaatiota ja propagandaa koskevan kysymyksen kansallisessa kyberturvallisuusstrategiassaan.

Esimerkiksi Ranskan kansallisessa kyberturvallisuusstrategiassa[33] todetaan, että on valtion velvollisuus tiedottaa kansalaisille internetissä toimivien ilkivaltaisten tahojen käyttämien manipulointi- ja propagandatekniikoiden riskeistä. Esimerkiksi tammikuussa 2015 Ranskaa vastaan tehtyjen terroristi-iskujen jälkeen hallitus perusti tietofoorumin viestintäverkkojen kautta tapahtuvaan islamistiseen radikalisoitumiseen liittyvistä riskeistä (Stop-djihadisme.gouv.fr). Tätä lähestymistapaa voidaan laajentaa vastaamaan muihin propagandaan tai epävakauteen liittyviin ilmiöihin.

Toinen esimerkki on Puolan kansallinen kyberturvallisuusstrategia vuosille 2019–2024[34], jossa todetaan, että manipuloivia toimia, kuten disinformaatiokampanjoita, vastaan tarvitaan järjestelmällisiä toimia, jotta voidaan parantaa kansalaisten tietoisuutta tietojen todenmukaisuuden vahvistamisen ja niiden vääristämisyrityksiin vastaamisen yhteydessä.

ENISAn suorittamien haastattelujen aikana useat jäsenvaltiot kuitenkin kertoivat, että kyseistä kysymystä ei käsitellä osana kansallista kyberturvallisuusstrategiaa vaan laajemmalla yhteiskunnallisella tasolla esimerkiksi poliittisten aloitteiden avulla.

Turvataan huipputeknologioita (5G, tekoäly, kvanttilaskenta jne.)

Kun nykyinen kyberturvallisuuden uhkaympäristö laajenee, uusien teknologioiden kehitys johtaa todennäköisesti kyberhyökkäysten voimakkuuden ja määrän kasvuun ja uhkatoimijoiden käyttämien menetelmien, keinojen ja kohteiden monipuolistumiseen. Samanaikaisesti näistä uusista teknologisista ratkaisuista huipputeknologioiden muodossa voi tulla eurooppalaisten digitaalisten markkinoiden tärkeitä rakenneosia. Jäsenvaltioiden kasvavan digitaalisen riippuvuuden ja uusien teknologioiden synnyn turvaamiseksi on laadittava kannustimia ja kattavia toimintalinjoja kyseisten teknologioiden turvallisen ja luotettavan kehityksen ja käyttöönoton tukemiseksi EU:ssa.

Aineistotutkimuksen aikana, jolloin tutkittiin jäsenvaltioiden kansallisia kyberturvallisuusstrategioita, seuraavat huipputeknologiat esiteltiin jäsenvaltioita kiinnostavina: 5G, tekoäly, kvanttilaskenta, kryptografia, reunalaskenta, verkottuneet ja itseohjautuvat ajoneuvot, iso ja älykäs data, lohkoketju, robotiikka ja esineiden internet.

Euroopan komissio julkaisi alkuvuodesta 2020 tiedonannon, jossa pyydettiin jäsenvaltioita ryhtymään toimiin sellaisten toimenpiteiden toteuttamiseksi, joita suositeltiin 5G-välineistöä koskevissa päätelmissä[35]. Kyseinen 5G-välineistö on jatkoa komission vuonna 2019

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

hyväksymälle 5G-verkkojen kyberturvallisuudesta annetulle suositukselle (EU) 2019/534, jossa esitetään vaatimus yhdenmukaisesta eurooppalaisesta lähestymistavasta 5G-verkkojen turvallisuuteen[36].

ENISAn suorittamien haastatteluiden aikana korostui se, että tämä aihe on ennemminkin monialainen aihe, jota käsitellään yleisesti kansallisissa kyberturvallisuusstrategioissa, kuin erityinen tavoite itsessään.

Varmistetaan datasuvereniteetti

Yhtäältä kyberavaruus voidaan katsoa valtavaksi globaaliksi yhteiseksi tilaksi, joka on helposti saatavilla ja tarjoaa korkeatasoisen yhdistettävyyden ja jossa voidaan tuottaa erinomaisia tilaisuuksia sosiaalis-taloudelliseen kasvuun. Toisaalta kyberavaruutta luonnehtii heikko lainkäyttövalta, vaikeus määrittää toimia, rajojen puute ja toisiinsa yhteydessä olevat järjestelmät, joissa voi olla puutteita ja joista voidaan varastaa tietoa tai joihin vieraat valtiot voivat päästä käsiksi. Kahden edellä mainitun näkökannan lisäksi digitaalista ekosysteemiä kuvaa verkkopalvelualustojen ja -infrastruktuurien keskittyminen ainoastaan muutamille sidosryhmille. Kaikkia edellä mainitut näkökohdat johtavat digitaalisen suvereniteetin edistämiseen jäsenvaltioissa. Digitaalinen suvereniteetti merkitsee sitä, että kansalaisten ja yritysten on mahdollista menestyä hyödyntämällä luotettavia digitaalisia palveluja sekä tieto- ja viestintätekniikan tuotteita pelkäämättä henkilökohtaisten tietojensa tai digitaalisen omaisuutensa, taloudellisen riippumattomuutensa tai poliittisen vaikutusvaltansa puolesta.

Jäsenvaltiot vaalivat datasuvereniteettia tai digitaalista suvereniteettia kansallisella ja eurooppalaisella tasolla. Vaikka jäsenvaltiot eivät näytä käsittelevän kysymystä erityisenä tavoitteena suoraan kansallisissa kyberturvallisuusstrategioissaan, ne käsittelevät sitä joko monialaisena periaatteena tai hahmottelevat aikomusta varmistaa digitaalinen suvereniteetti kansallisella tasolla yksittäisissä julkaisuissa keskittymällä keskeisiin teknologioihin. Esimerkiksi Ranskan kyberpuolustusta koskevassa vuoden 2018 strategisessa katsauksessa todetaan, että seuraavien teknologioiden valvonta on ehdottoman tärkeää digitaalisen suvereniteetin varmistamiseksi: viestinnän salaus, kyberhyökkäysten havaitseminen, ammattikäyttöön tarkoitetut matkaviestimet, pilvipalvelut ja tekoäly[37].

Euroopan tasolla jäsenvaltiot osallistuvat aktiivisesti Euroopan datastrategian määrittämiseen (COM(2020) 66 final) ja EU:n kyberturvallisuusasetuksella (2019/881) perustetun digitaalisille tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille tarkoitetun EU:n sertifiointikehyksen kehittämiseen, jotta voitaisiin varmistaa digitaalinen autonomia Euroopan tasolla.

Jäsenvaltioiden haastatteluvaiheessa osoittautui, että digitaalinen suvereniteetti katsotaan usein laajemmaksi kysymykseksi, joka ei rajoitu ainoastaan kyberturvallisuuteen. Näin ollen jäsenvaltiot eivät käsittele aihetta kansallisissa kyberturvallisuusstrategioissaan, ja ne, jotka näin tekevät, eivät käsittele sitä erityisenä tavoitteena.

Kannustinten tarjoaminen kybervakuutusalan kehittämiseen

Kybervakuutusalan nykyinen tilanne osoittaa, että maailmanmarkkinat ovat kiistämättä kasvaneet. Ollaan kuitenkin vasta alkuvaiheessa, sillä tietoja on kerättävä ja monia ennakkopäätöksiä on vielä ratkaistava (esimerkiksi hiljainen kattavuus, systeemiset kyberriskit jne.). Lisäksi arvioidut menetykset, jotka johtuvat maailmanlaajuisista kyberhyökkäyksistä, ovat useita kertaluokkia suuremmat kuin nykyinen kybervakuutusalan kattavuuskyky (IMF Working

[36] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Paper – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Kybervakuutusalan kehittämisestä saadaan kuitenkin varmasti etuja ja samalla luodaan pohja positiivisille mekanismeille. Kybervakuutukseen liittyvistä mekanismeista voi olla hyötyä seuraavissa:

- Kyberturvallisuusriskejä koskevan tietoisuuden lisääminen yrityksissä;
- Kyberriskeille altistumisen arviointi kvantitatiivisesti;
- Kyberturvallisuusriskien hallinnan parantaminen;
- Kyberhyökkäysten uhreiksi joutuneiden organisaatioiden tukeminen; ja
- Kyberhyökkäyksestä aiheutuneiden (aineellisten tai muiden) vahinkojen korvaaminen.

Tietyissä jäsenvaltioissa aihetta on alettu työstää, ja esimerkiksi

- Viro hyväksyi kansallisessa kyberturvallisuusstrategiassaan seuraavanlaisen odottavan ja seuraavan lähestymistavan: Kyberriskien vähentämiseksi yleisesti yksityisellä sektorilla Viron kybervakuutuspalvelujen kysyntä ja tarjonta analysoidaan, minkä perusteella asianosaisten osapuolten kanssa sovitaan yhteistyön periaatteet, mukaan luettuina tiedonjako, riskinarvioinnin valmistelu jne. Tällä hetkellä kybervakuutuspalvelujen tarjoajia on Viron markkinoilla vain muutama, ja aluksi on tärkeää kartoittaa, kuka tarjoaa mitäkin. Vakuutussuojan monimutkaisuus katsotaan usein kybervakuutusmarkkinoiden kehittämisen esteeksi.
- Luxemburg tukee erityisesti kybervakuutusalan kehittämistä kansallisessa kyberturvallisuusstrategiassaan seuraavasti: Tavoite 1: Uusien tuotteiden ja palvelujen luominen. Riskien yhdistäminen ja digitaalisten kyberhäiriöiden uhrien kannustaminen hakemaan asiantuntevaa apua häiriön saamiseksi hallintaan ja ilkivallan kohteeksi joutuneen järjestelmän palauttamiseksi; vakuutusyhtiöiden kannustaminen luomaan erityisiä tuotteita kybervakuutusalalle.

Haastatelluilta saadut palautteet olivat melko vaihtelevia tämän aiheen osalta: jotkin jäsenvaltiot ilmoittivat, että kybervakuutus on vasta viime aikoina noussut keskustelun aiheeksi, kun taas toiset jäsenvaltiot sanoivat, että vaikka aihe on lupaava, ala ei ole vielä riittävän kypsä. Moni haastateltava totesi kuitenkin, että aihetta ei käsitellä osana kansallista kyberturvallisuusstrategiaa joko sen takia, että sen katsotaan olevan liian erityinen, tai siksi, että se ei kuulu kansallisen kyberturvallisuusstrategian soveltamisalaan.

TP-06-20-047-EN-N

Tietoa Euroopan unionin kyberturvallisuusvirastosta

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka tarkoituksena on saavuttaa korkea kyberturvallisuuden taso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa ja auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. Virasto jakaa tietoa, kehittää valmiuksia ja lisää tietämystä sekä tekee yhteistyötä keskeisten sidosryhmiensä kanssa lujittaakseen luottamusta verkottuneeseen talouteen, parantaakseen unionin infrastruktuurin sietokykyä ja ennen kaikkea suojatakseen eurooppalaisen yhteiskunnan ja kansalaisten digitaalista turvallisuutta. Lisätietoja virastosta on osoitteessa www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-481-7
DOI: 10.2824/845928