TLP:CLEAR

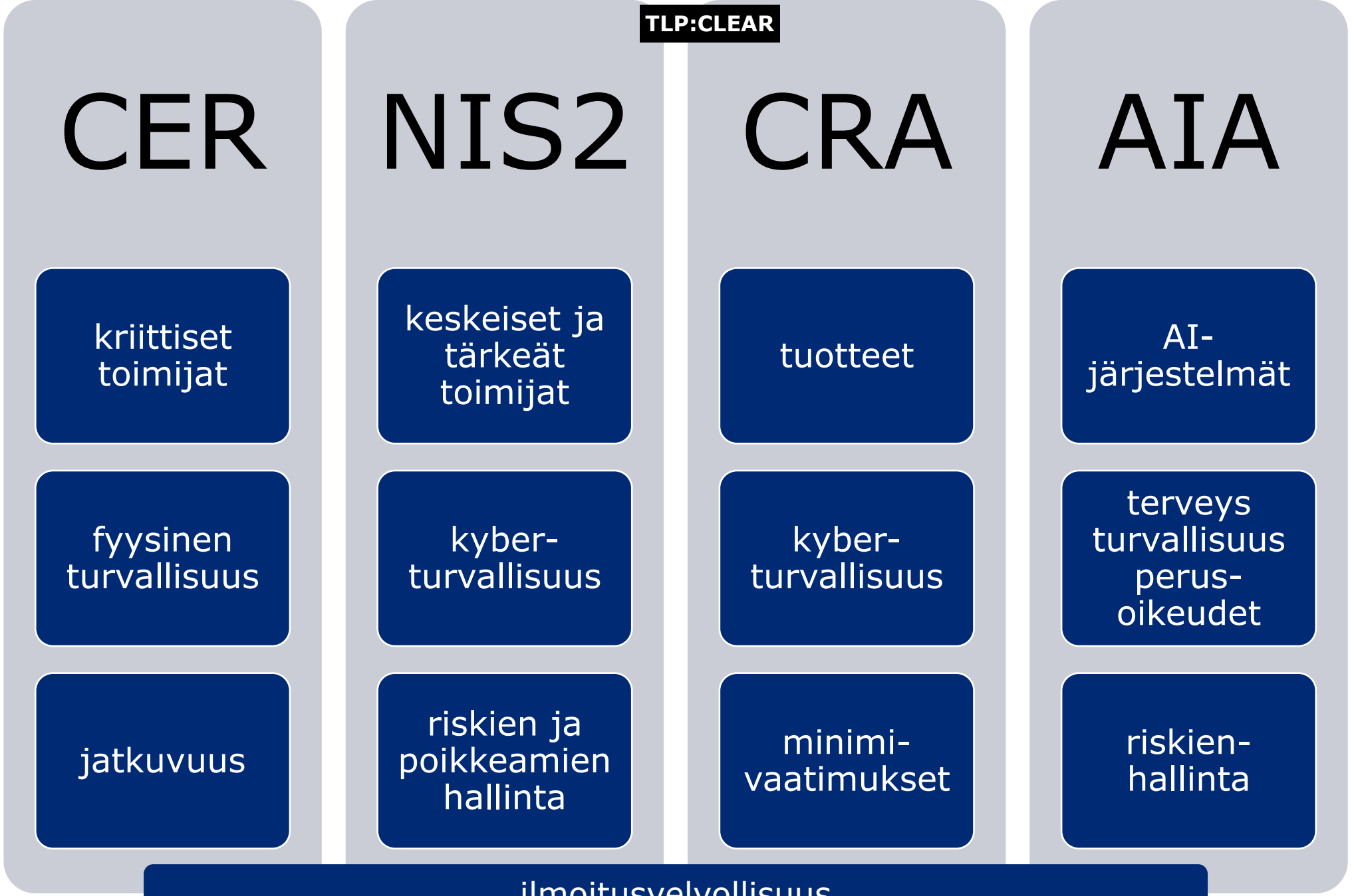
TLP:CLEAR

TRAFICOM

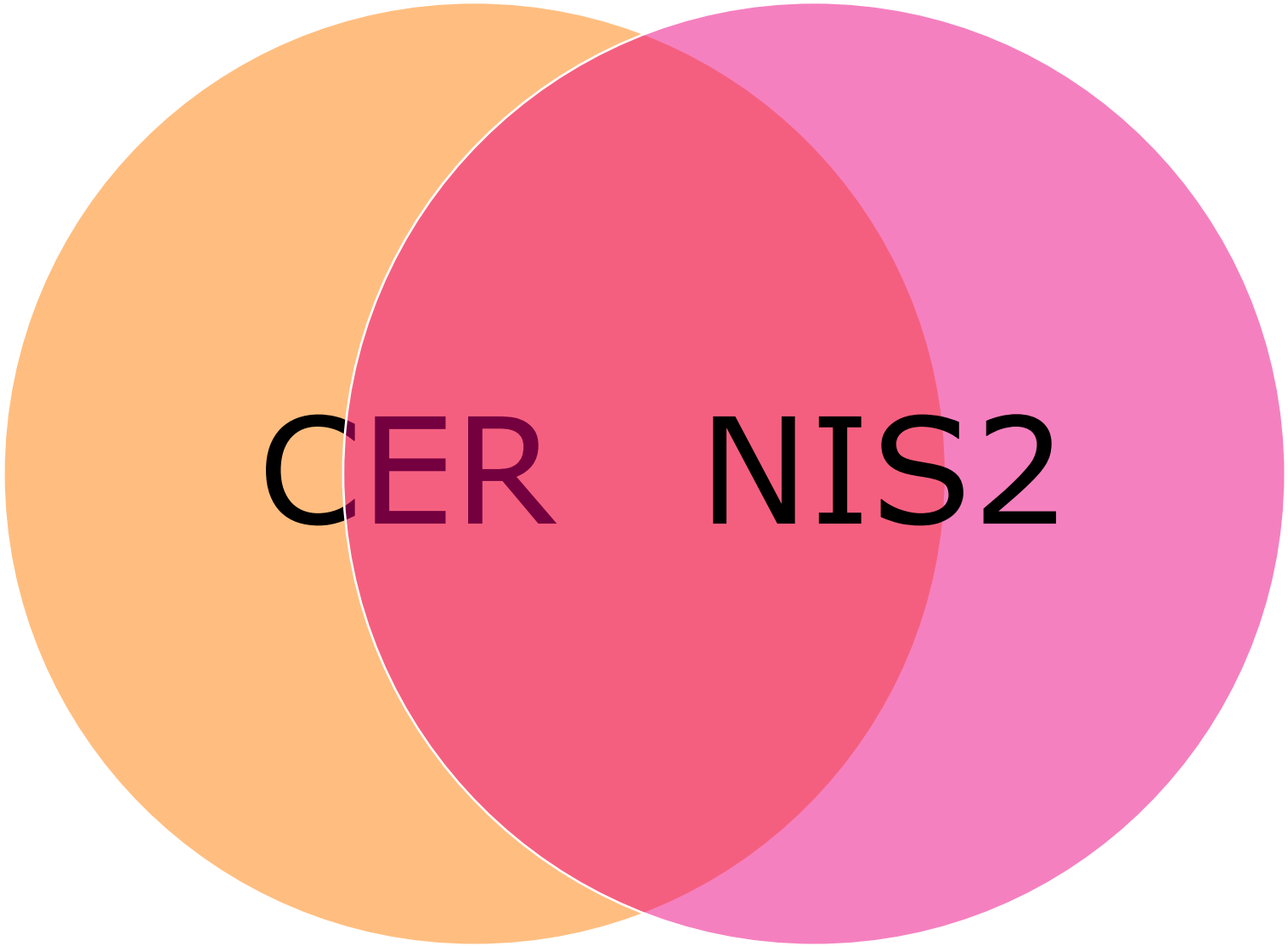
Finnish Transport and Communications Agency
National Cyber Security Centre

Uusi EU-sääntely muuttaa yritysten velvoitteita

Jussi Eronen


CER
NIS2
CRA
AIA
kriittiset toimijat
keskeiset ja tärkeät toimijat
tuotteet
AI-järjestelmät
fyysinen turvallisuus
kyber-turvallisuus
kyber-turvallisuus
terveys turvallisuus perus-oikeudet
jatkuvuus
riskien ja poikkeamien hallinta
minimi-vaatimukset
riskien-hallinta
ilmoitusvelvollisuus

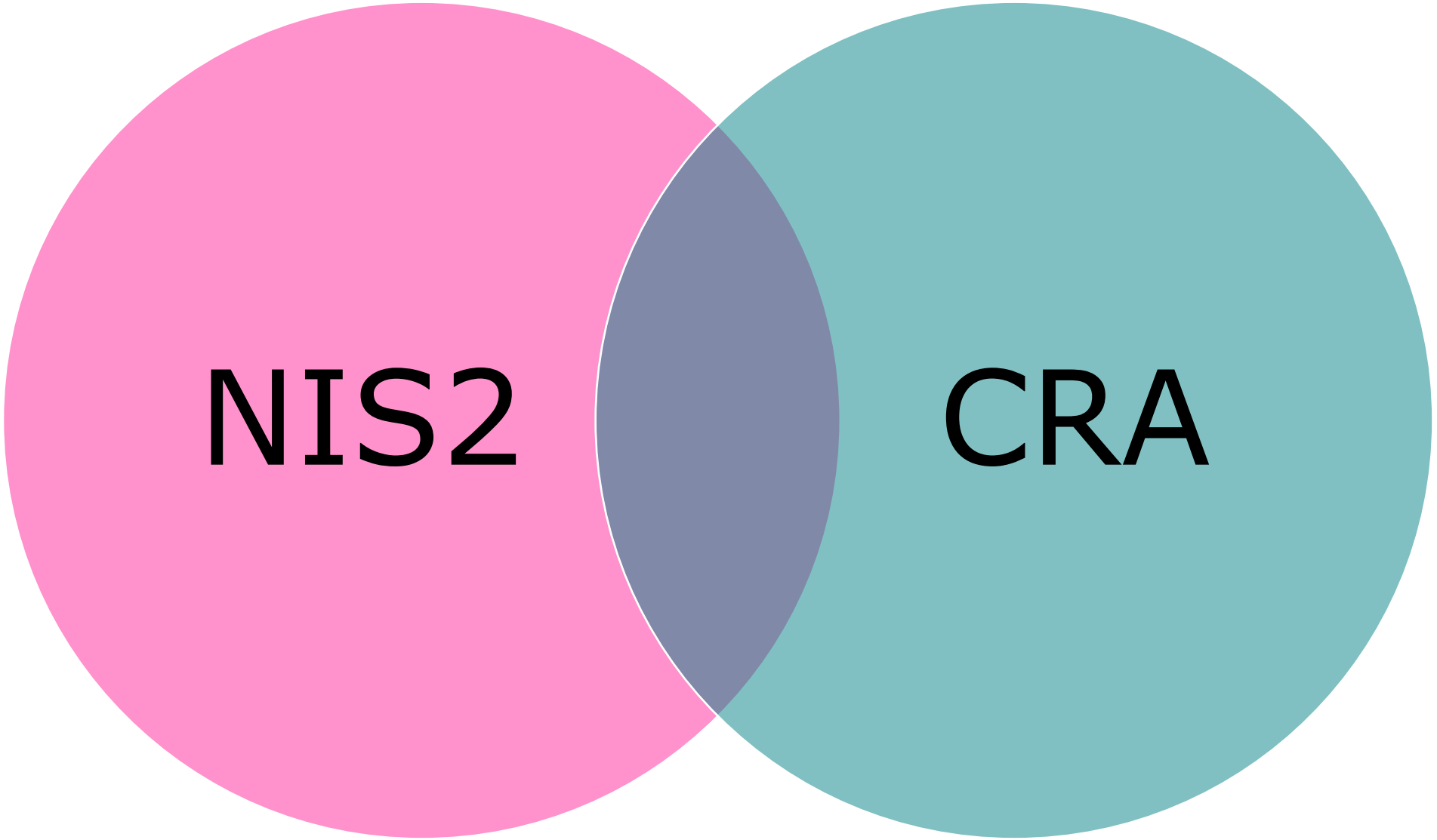
Soveltamisala - kohteet



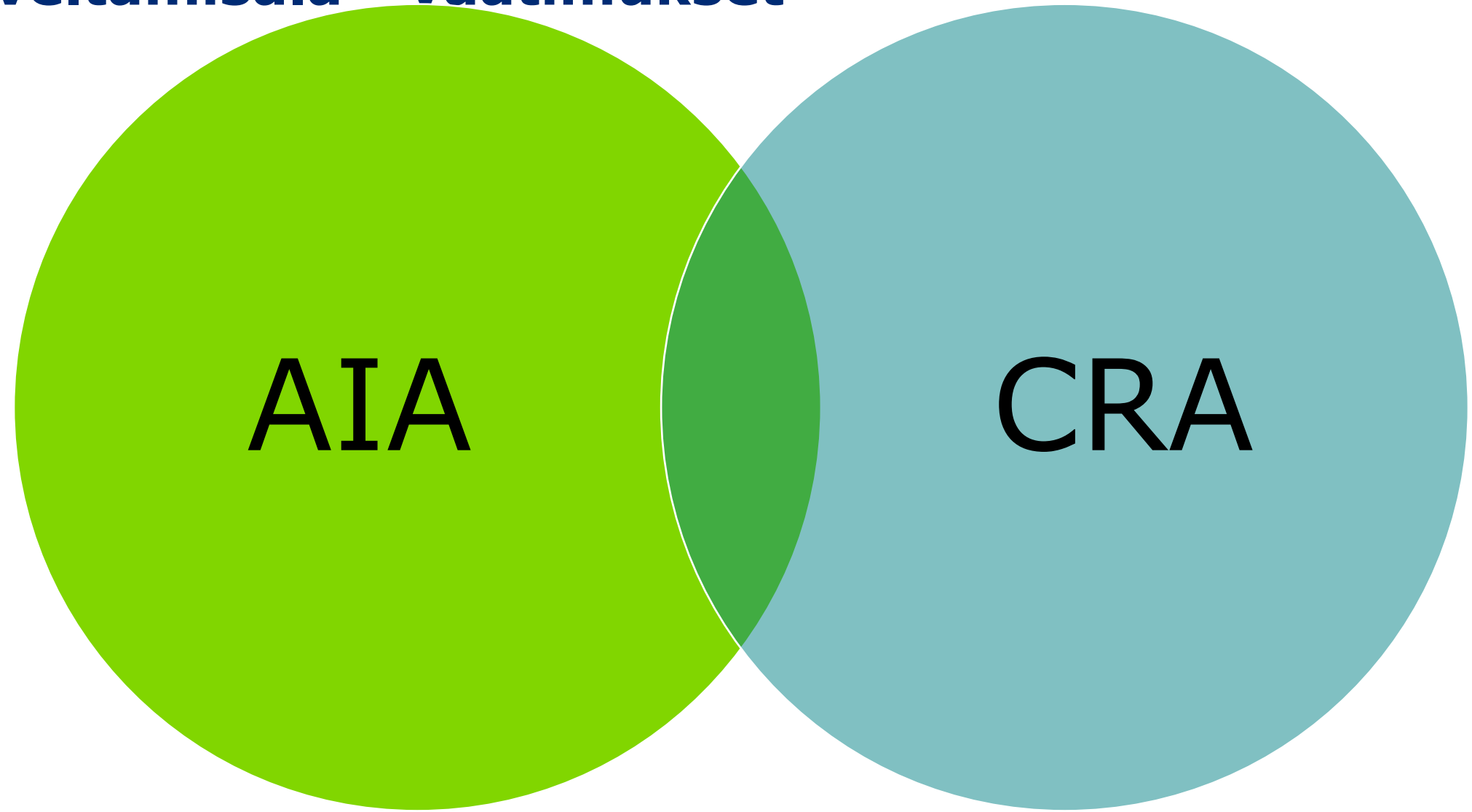
CER ja NIS2 yhteensovittaminen

- CER-kriittiset toimijat ovat suoraan NIS2 keskeisiä toimijoita, mikä ei vaikuta NIS2 velvoitteisiin, mutta mahdollistaa ennakkovalvonnan, mikäli se ei ollut aiemmin mahdollista.
- Digitaalisen infrastruktuurin kohdalla CER ei tuo lisävelvoitteita tai vaatimuksia, koska kyse on poikkeussektorista. Velvoitteiden osalta sovelletaan NIS2 vaatimuksia.
- Muiden sektoreiden kohdalla NIS2 ja CER velvoitteet myös täydentävät toisiaan, kun CER korostaa enemmän onnettomuuksia ja ympäristöriskejä, fyysisen infran ja tilojen turvallisuutta sekä henkilöstöturvallisuutta, pätevyysvaatimuksia ja turvallisuusselvityksiä.

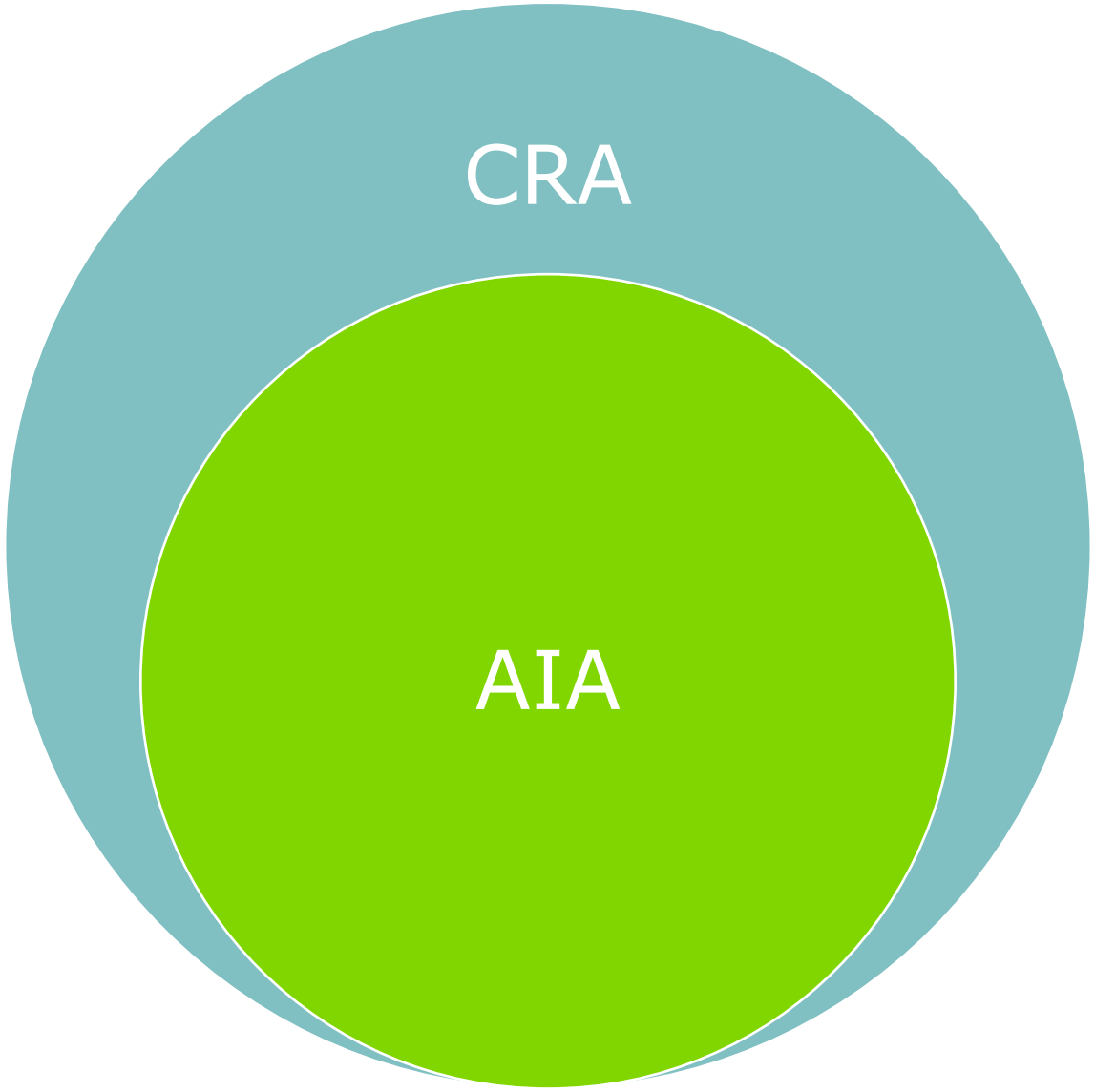
Soveltamisala - kohteet



Soveltamisala - vaatimukset



Soveltamisala - turvallisuusvaatimukset



Tapausesimerkki – Oy ÄlyEnergia Ab

- Paikallinen energiayritys
  - Sähkön siirto
  - Sähkön tuotanto
- Älykäs sähköverkon ohjausjärjestelmä ÄlyOhjaaja™
  - Hyödyntää tekoälyä
  - Tarjotaan palveluna asiakkaille kustannusten minimointiin
  - Myynnissä kaupallisena tuotteena

NIS2

TRAFICOM

NIS2: Euroopan unionin kyberturvallisuusdirektiivi

- Direktiivi edellyttää, että jäsenvaltiot asettavat sen soveltamisalassa oleville organisaatioille toimialarajat ylittäviä vähimmäistason velvoitteita kyberturvallisuuden parantamiseksi
  - Riskienhallinnan vähimmäistaso, huomioitavat osa-alueet ja riskienhallintatoimenpiteet
  - Merkittävistä poikkeamista ilmoittaminen

LÄHDE https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

TLP:CLEAR

TLP:CLEAR

NIS2 Liitteet

kyberturvallisuuskeskus.fi/files/media/file/TRAFICOM_NIS2_taulukko_08042025.pdf

NIS2 Liitteet 1 / 2 86%

NIS2 Liite I

Erittäin kriittiset toimialat

Taulukon selitteet

1 Suuret toimijat
2 Keskisuuret toimijat
3 Pienet ja mikrotoimijat

● Keskeinen
◐ Tärkeä
○ Ei kuulu soveltamisalaan

Toimiala	Toimialan osa tai toimijatyyppi	1	2	3
Energia	Sähkö, kaukolämmitys ja -jäähdytys, kaasu, vety, öljy, latauspalvelujen tarjoajat loppukäyttäjille	●	◐	○
Liikenne	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne	●	◐	○
Pankkitoiminta	Luottolaitokset	●	◐	○
Finanssimarkkinoiden infrastruktuurit	Kauppapaikkojen ylläpitäjät ja keskusvastapuolet	●	◐	○
Terveys	Terveydenhuoltopalvelujen tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimus ja kehitys, lääkeaineiden ja lääkkeiden valmistus, kansanterveyden kriittisten lääkinnällisten laitteiden valmistus hätätilanteessa	●	◐	○
Juomavesi		●	◐	○
Jätevesi		●	◐	○
Digitaalinen infrastruktuuri	Hyväksytyt luottamuspalveluntarjoajat	●	●	●
	Ei-hyväksytyt luottamuspalveluntarjoajat	●	◐	◐
	DNS-palveluntarjoajat (lukuun ottamatta juurinimipalvelimia)	●	●	●
	Aluetunnusrekisterit	●	●	●
	Yleisten sähköisten viestintäverkkojen tarjoajat	●	●	◐
	Yleisesti saatavilla olevat sähköisten viestintäpalveluiden tarjoajat	●	●	◐
	Internetin yhdysliikennepisteiden tarjoajat	●	◐	○
	Pilvipalveluntarjoajat	●	◐	○
	Datakeskuspalveluntarjoajat	●	◐	○
	Sisällönjakeluverkkojen tarjoajat	●	◐	○
Yritysten välinen TVT-palvelujenhallinta	Hallintapalveluntarjoajat, tietoturvapalveluntarjoajat	●	◐	○
Avaruus	Maanpäällisen infrastruktuurin ylläpitäjät	●	◐	○
Julkishallinto	Keskeiset toimijat: tiedonhallintalakiehdotuksessa* määritellyt toimijat		●	
	Tärkeät toimijat: hyvinvointialueet ja -yhtymät sekä Helsingin kaupunki*		◐	

* Tiedonhallintalain 4a luvun soveltamisalaan kuuluvat toimijat

TLP:CLEAR

TRAFICOM

TLP:CLEAR

NIS2 - Eri sektoreiden valvovat viranomaiset

TRAFICOM
Liikenne- ja viestintävirasto

Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

tukes

RUOKAVIRASTO
Livsmedelsverket • Finnish Food Authority

fimea

Elinkeino-, liikenne- ja ympäristökeskus

FIN-FSA
FINANSSIVALVONTA

energiavirasto

TLP:CLEAR

Tapausesimerkki – Oy ÄlyEnergia Ab

- Kriittinen toimiala: energia-ala
- Keskisuuri toimija: ”50–249 työntekijää tai vuosiliikevaihto ja taseen loppusumma ylittävät 10 miljoonaa euroa”
- Koosta riippumatta sähkön siirron osalta ”Toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen”
- -> Keskeinen toimija, valvovana viranomaisena Energiavirasto

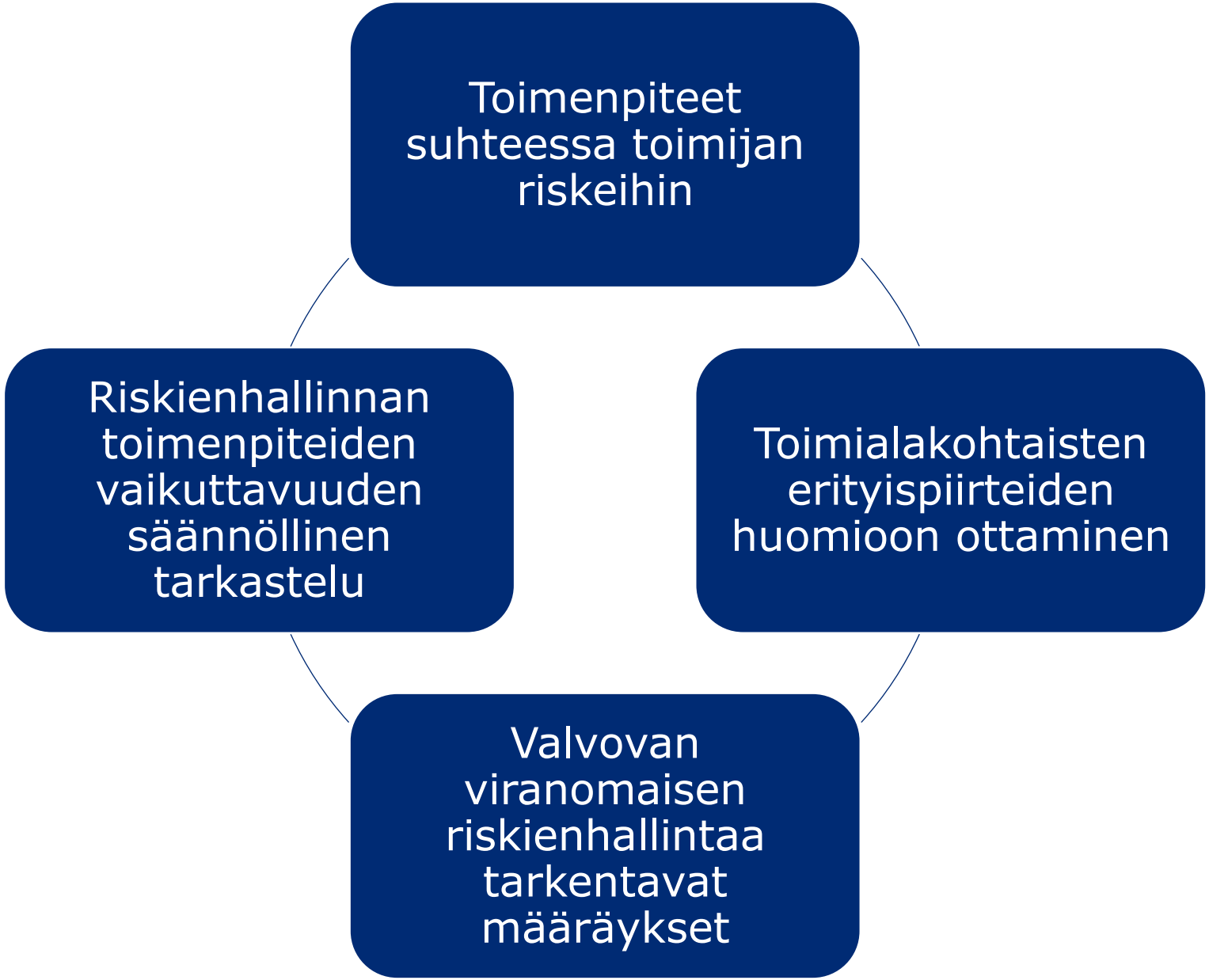
Velvoitteet

- Toimijaluetteloon ilmoittautuminen
- Kyberturvallisuuden riskienhallinnan toimintamalli
- Merkittävän poikkeaman raportointi

Riskiperustainen lähestymistapa

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

Kyberturvallisuuslaki 7 § 2 mom.
Tiedonhallintalaki 18 b § 1 mom.



Kaikki vaaratekijät huomioiden

- Riskien tunnistamisessa huomioidaan internet-välitteisen uhkan lisäksi fyysinen uhka. Tahallinen tai tahaton tapahtuma. Ulkoisen uhkan lisäksi sisäinen uhka.
- Toimijan on huomioitava riskienhallinnassaan teknisen tietoturvallisuuden lisäksi myös verkko- ja tietojärjestelmiensä fyysisen ympäristönsä suojaus.

Kyberturvallisuuden riskienhallinnan toimenpiteet

1. Kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

2. Viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet**

3. Viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon turvallisuus** sekä tarvittavat menettelyt **haavoittuvuuksien** käsittelyyn ja julkistamiseen

4. **Toimitusketjun** välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja **häiriönsietokyky**, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien **kyberturvallisuuskäytännöt**

5. **Omaisuudenhallinta** ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

6. **Henkilöstöturvallisuus ja kyberturvallisuuskoulutus**

7. **Pääsynhallinnan ja todentamisen** menettelyt

8. **Salausmenetelmien** käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

9. **Poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

10. Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan **jatkuvuuden hallinta** ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

11. **Perustason tietoturvakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

12. Toimenpiteet viestintäverkkojen ja tietojärjestelmien **fyysisen ympäristön** ja tilaturvallisuuden sekä **välttämättömien resurssien** varmistamiseksi

Kyberturvallisuuslaki 9 §
Tiedonhallintalaki 18 c §

TRAFICOM

Suositus **valvoville viranomaisille** NIS2-direktiivin mukaisista kyberturvallisuuden riskienhallinnan toimenpiteistä.

Suositus voi tukea myös **toimijoiden** kyberturvallisuuden **riskienhallinnan suunnittelua**.

Suositukseen on koottu **tietoa ja käytännön esimerkkejä** siitä, millaisia toimenpiteitä laissa säädettyihin **vaatimuksiin** voi kuulua.

Suosituksessa kuvataan myös erilaisia **keinoja**, joita valvova viranomainen voi harkintansa ja arvionsa mukaan käyttää **ohjaus- ja valvontatehtävissään**.

Esimerkki suosituksen kohdasta

10.3 Palautustestaus ja varmuuskopioiden suojaaminen

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Varmuuskopioiden palautusta ja varajärjestelmien toimivuutta tulisi testata säännöllisesti, ensisijaisesti automaattisesti. Testauksessa pitäisi tarkastaa myös varmuuskopioiden eheys. Varmuuskopioiden palautustestaus on tehtävä turvallisesti niin, ettei se vaaranna tuotantojärjestelmää.
- Varmuuskopioita on säilytettävä turvallisessa tilassa, joka on toimijan riskienhallinnan perusteella riittävän eriytettynä varmuuskopioitavasta järjestelmästä. Tämä voi tarkoittaa esimerkiksi muuta toimitilaa tai erillistä palotilaa. Varmuuskopioita voi säilyttää tarvittaessa useassa muodossa, joiden palautusnopeuksissa voi olla eroa, kuten levylle otetut varmistukset sekä erilliset pitkäaikaisarkistot.
- Varmuuskopioiden suojaamisessa voidaan ottaa huomioon niiden eheyden, saatavuuden ja luottamuksellisuuden tarpeet. Tämä tarkoittaa esimerkiksi riittävää fyysistä suojausta ja muita kontrolleja, kuten salausta.

Todennus

1. Valvova viranomainen todentaa, että toimija on mahdollisuuksien ja tarpeen mukaan määrittänyt toimenpiteet, joilla varmuuskopioiden ja varajärjestelmien toimivuutta testataan säännöllisesti, esimerkiksi kerran viikossa. Tämä voi olla automatisoitua tai manuaalista. Keskeistä on, että mekaanisen palautuksen lisäksi tarkastetaan myös se, että tieto saadaan palautettua eheänä ja käyttökelpoisena, sekä mahdollinen varajärjestelmä pystytettyä oikealla tiedolla. Valvovan viranomainen todentaa, että varmuuskopiot on suojattu riittävästi. Esimerkiksi arkkitehtuurikuvauksissa, järjestelmädokumentaatiossa tai vastaavassa pitäisi olla kuvattuna se, miten varmuuskopiojärjestelmä tai sen osa on eriytetty muusta järjestelmästä. Tämän pitäisi varmistaa se, että jos esimerkiksi viestintäverkkoon ja tietojärjestelmään pääsee hyökkääjä, ei tämä voi päästä käsiksi kaikkiin varmistuksiin.
2. Valvova viranomainen todentaa katselmoinneilla ja haastatteluilla, miten toimija testaa varmuuskopioiden toimivuutta mahdollisuuksien ja tarpeen mukaan. Tästä tulisi käydä ilmi esimerkiksi suoritetut toimenpiteet varmuuskopioiden eheyden varmistamiseksi sekä testauksen säännöllisyys. Valvova viranomainen voi tarvittaessa hyödyntää myös fyysisiä katselmointeja sen varmistamiseksi, että varmuuskopioita on eriytetty muusta järjestelmästä riittävästi. Katselmoinnissa tulisi varmistua esimerkiksi siitä, että uhkat kuten tulipalo, tulvat ja henkilöuhka, eivät koske sekä varmistettavaa järjestelmää että varmuuskopioita.
3. Jos kyseessä on fyysisen erottelun sijaan perusteltu looginen erottelu, voi valvova viranomainen hyödyntää esimerkiksi toimijan tekemiä skannauksia ja yhteydenottoyrityksiä sen varmistamiseksi, että eriytettyyn varmuuskopiointijärjestelmään ei pääse käsiksi varmistettavan viestintäverkon ja tietojärjestelmän puolelta.

Perustelut

Poikkeamatilanteista palautumisen yhteydessä tapahtuu liian usein niin, että palautus ei onnistu tai hyökkääjä onnistuu tuhoamaan sekä tietojärjestelmän että varmuuskopiot. Tämän vuoksi palautuksen kattava ja säännöllinen testaaminen sekä palautusjärjestelmän suojaaminen voivat olla toiminnan kannalta elintärkeitä.

Viitteet

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

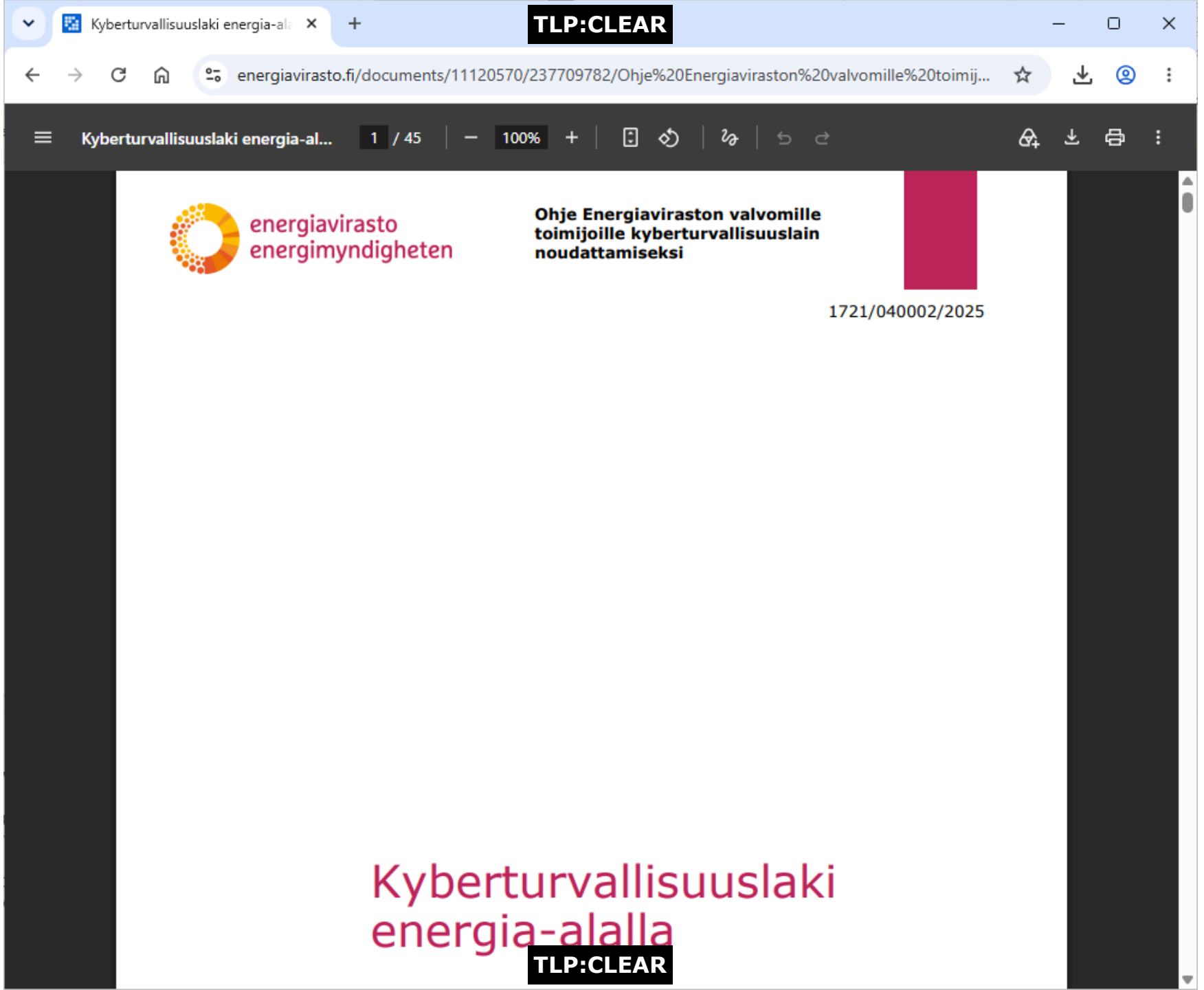
Työkalut

Julkri (TEK-20, VAR-09)

Kybermittari (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5)

TLP:CLEAR

TLP:CLEAR



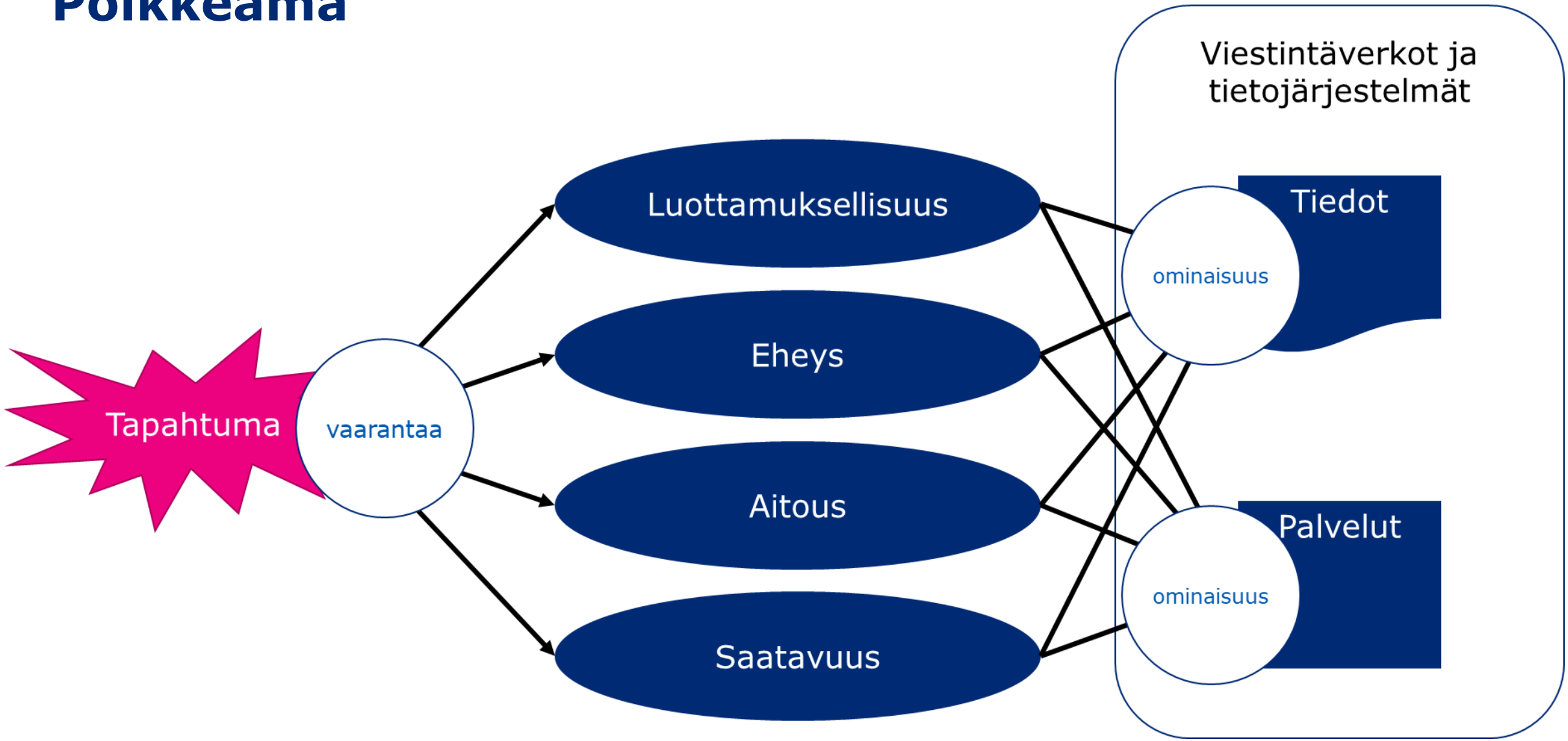
TLP:CLEAR

TRAFICOM

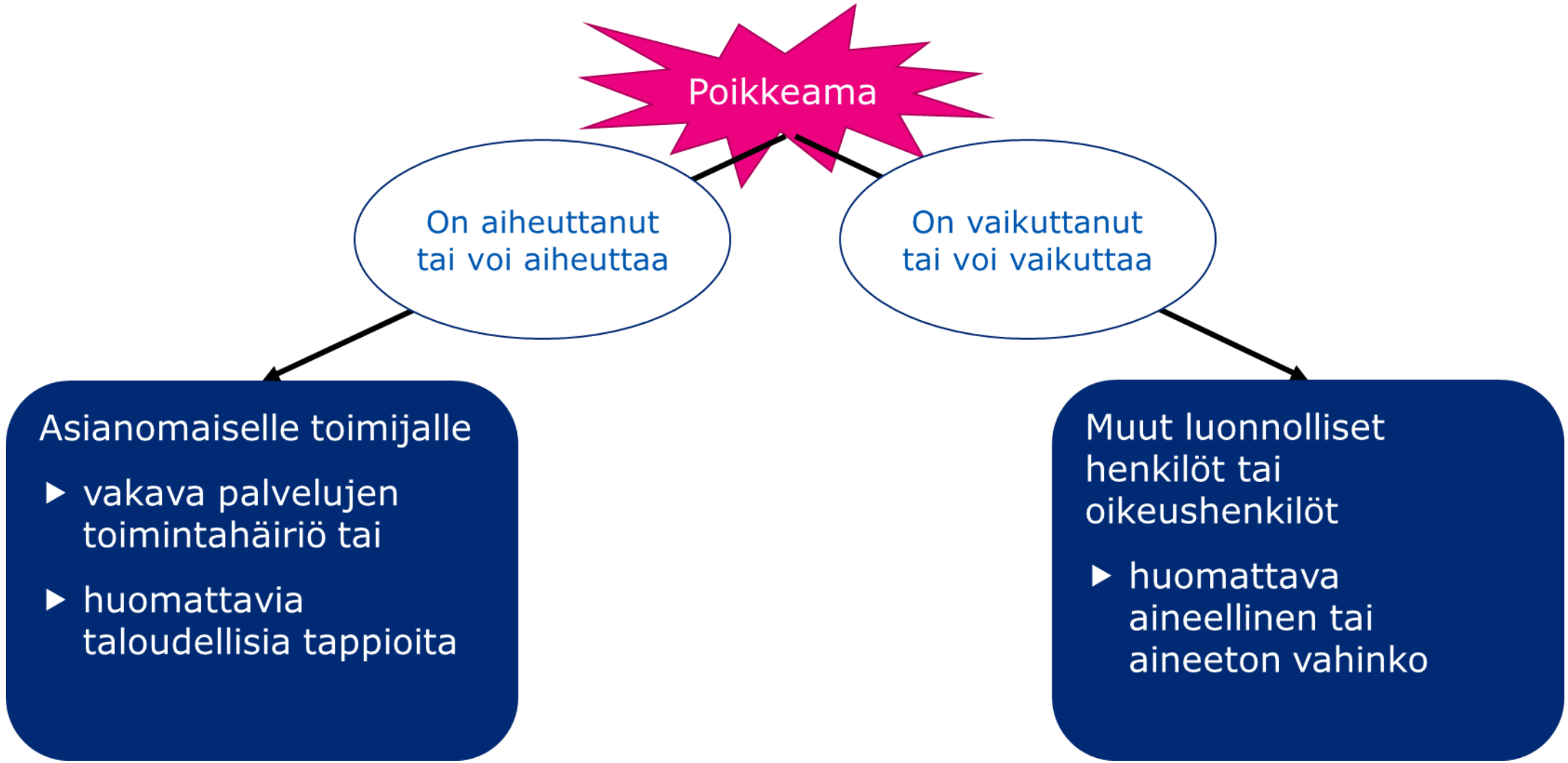
NIS2 – poikkeamien käsittely ja ilmoittaminen

TRAFICOM

Poikkeama


Viestintäverkot ja tietojärjestelmät
Tapahtuma
vaarantaa
Luottamuksellisuus
Eheys
Aitous
Saatavuus
ominaisuus
ominaisuus
Tiedot
Palvelut

Merkittävä poikkeama



Poikkeama tapahtui. Mitäs nyt?

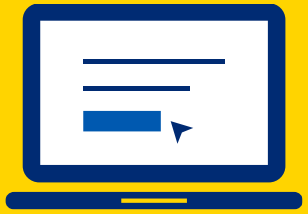
- Don't panic :-) Toimi suunnitelmallisesti
- Havaitse poikkeama
- Tee ensiarvio poikkeaman merkittävyydestä
- Käynnistä toimenpiteet turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi
- Jos merkittävä poikkeama:
  - Tee ensi-ilmoitus toimivaltaiselle viranomaiselle. Vahva suositus: Tee ilmoitus Kyberturvallisuuskeskuksen NIS2-ilmoitussovelluksen kautta.
  - Jos poikkeama todennäköisesti haittaa palveluidesi tarjoamista: Ilmoita palveluidesi vastaanottajille

Poikkeaman käsittelyn myöhempiä toimenpiteitä

- Tee muut asiaan kuuluvat ilmoitukset
  - poliisille
  - tietosuojavaltuutetulle
  - sopimuskumppaneille
- Arvioi säännöllisesti poikkeaman hallinnan tilannetta ja toimenpiteiden riittävyyttä
- Päätä, milloin olet käsitellyt poikkeaman loppuun
- Jos merkittävä poikkeama: Tee toimivaltaiselle viranomaiselle jatkoilmoitus ja loppuraportti, ja tarvittaessa myös väliraportti
- Opi poikkeamasta ja kehitä ennaltaehkäisyä ja varautumista

Miten toimijan tulee raportoida merkittävän poikkeaman sattuessa?

Kaikkien NIS2-toimijoiden on aina ilmoitettava merkittävästä poikkeamasta valvovalle viranomaiselle.



24 h kuluessa ensi-ilmoitus

- Havainto merkittävästä poikkeamasta
- Onko syytä epäillä, että kyseessä on rikos tai viha-mielinen teko
- Rajat ylittävien vaikutusten mahdollisuus

72 h kuluessa jatkoilmoitus

- Arvio poikkeaman laadusta, vakavuudesta ja vaikutuksista
- Vaarantumis-indikaattori (IOC), jos mahdollista
- Mahdolliset täydennykset

Mahdollinen väliraportti

1 kk kuluessa loppuraportti

- Yksityiskohtainen kuvaus poikkea-masta, sen vakavuudesta ja vaikutuksista
- Poikkeaman arveltu aiheuttaja
- Toimenpiteet tilanteen hoitamiseksi
- Mahdolliset rajat ylittävät vaikutukset

TRAFICOM

Miten ilmoittaa poikkeamasta?

- https://www.kyberturvallisuuskeskus.fi/fi/ilmoita → "NIS 2-direktiivin mukainen poikkeamailmoitus"
  - Suora linkki: https://eservices.traficom.fi/ContactForms/form/NIS2-Ilmoitus?langid=fi
  - Vapaaehtoinen ilmoitus, jos poikkeama ei ollut merkittävä.
  - Kyberturvallisuuskeskus saa lomakkeella tehdystä ilmoituksesta kopion itselleen
- Ilmoita toimialasi oikein, esimerkkejä:
  - Terveydenhuollon palvelutuotannossa käytetyn pilvipalvelun katkos → Terveydenhuolto, Terveydenhuollon tarjoajat
  - Haittaohjelma pelastuslaitoksen työntekijän tietokoneella → Julkishallinto.
  - Hyvinvointialueen valmistaman lääkinnällisen laitteen ohjelmistokomponentin haavoittuvuus → Valmistus, Lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus

CSIRT on tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö

- NIS2:n myötä säädetyssä kansallisessa kyberturvallisuuslaissa on oma 3 luku pelkästään CSIRT-yksiköstä (kyberturvallisuuslain 19–25 §)
- Kyberturvallisuuslaista seuraa CSIRT:lle lukuisia uusia lakisääteisiä tehtäviä ja toimivaltuuksia.
  - Mm. haavoittuvuuskartoitukset, haavoittuvuuskoordinaatio, kyberturvallisuustietojen vapaaehtoisten jakamisjärjestelyjen koordinointi jne.

CSIRTille ilmoitetaan aina vapaaehtoisesti

CSIRT-yksiköllä ei ole uudessakaan kyberturvallisuuslaissa tiedonsaantioikeuksia.

Ainoa tiedonsaantioikeuden tapainen on CSIRT:n oikeus saada valvovilta viranomaisilta tietoja toimijaluettelosta.

Lakisääteisesti luottamuksellista

Kyberturvallisuus-keskus (CSIRT)
jakaa organisaatiolle tietoa tilannekuvasta, auttaa ensivasteessa, tukee ja ohjeistaa

Organisaatio
luovuttaa tietoa vapaaehtoisesti.

Salassa pidettäviä (Julkisuuslaki (621/1999) 24.1 §) tietoja ovat mm. kansainvälisistä suhteista (2), tieto- ja viestintä-järjestelmien turvajärjestelyistä (7), varautumisesta (8) sekä liikesalaisuuksista ja muista elinkeinosalaisuuksista (20).

Käyttötarkoituspalomuuri (25 §)

[…] **CSIRT-yksikölle** tämän lain mukaisten tehtävien hoitamiseksi **vapaaehtoisesti luovutettua tietoa** ei saa ilman tiedon luovuttaneen **suostumusta** käyttää tiedon luovuttajaan kohdistuvassa **rikostutkinnassa** eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa **päätöksenteossa.**

TRAFICOM

CER


e 11
ialaa
energia
liikenne
pankkiala
rahoitus-
markkinoiden
infrastruktuuri
terveys
juomavesi
jätevesi
digitaalinen
infra
julkishallinto
avaruus
elintarvikkeiden
tuotanto, jalostus
ja jakelu

Kriittisten toimijoiden määrittäminen

Määrittämisessä huomioidaan **kriittisten toimijoiden häiriönsietokykyä koskeva valtakunnallinen suunnitelma ja kansallinen CER-riskiarvio**

- **Toimii jollakin laissa määritetyllä toimialalla** (esim. energia, liikenne, vesi tai terveys)
- **Tarjoaa CER-lain mukaista keskeistä palvelua**
- **Toimii Suomessa ja sen infrastruktuuri sijaitsee Suomessa**
- **Häiriö tai keskeytys palvelun tarjonnassa aiheuttaisi merkittäviä haitallisia vaikutuksia**

Kriittinen toimija

Toimijoita koskevat velvoitteet:

- riskiarviointi
- häiriönsietokykyä koskeva suunnitelma
- poikkeamailmoitusten tekeminen

Kriittisen toimijan suorittama riskiarviointi, CER-laki 14 § ja 30.3 §

- Kriittisen toimijan on suoritettava **riskiarviointi tarvittaessa ja vähintään neljän vuoden välein.** Riskiarviointia laadittaessa on otettava huomioon kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskeva kansallinen riskiarvio ja muut riskiarvioinnin kannalta merkittävät tietolähteet.
- Kriittisen toimijan riskiarvioinnissa on otettava **huomioon kaikki sellaiset merkitykselliset luonnon ja ihmisen aiheuttamat riskit, jotka voivat johtaa poikkeamaan.** Tällöin otetaan huomioon toimialojen tai rajat ylittävät riskit, onnettomuudet, luonnonkatastrofit, kansanterveydelliset hätätilanteet, hybridiuhat ja muut uhat sekä muut toimivaltaisen ministeriön määrittämät uhat.
- Riskiarvioinnissa on **otettava huomioon, missä määrin muut toimialat ovat riippuvaisia kriittisen toimijan tarjoamasta keskeisestä palvelusta**.
- Jos vastaavan kaltaista tarkoitusta varten laaditaan muun lain kuin tämän lain nojalla muu riskiarvio tai asiakirja, kriittinen toimija voi käyttää kyseistä arviointia tai asiakirjaa. Tästä on mainittava kyseisessä riskiarviossa tai asiakirjassa
  - CER-lain voimaan tullessa 14 §:ssä säädetty **kriittisen toimijan riskiarviointi tulee kriittiseksi toimijaksi määritetyn toimesta suorittaa ensimmäisen kerran yhdeksän kuukauden kuluessa siitä, kun vastaanottaja on saanut tiedon 13 §:ssä tarkoitetusta päätöksestä**

Häiriönsietokyvyn varmistaminen ja häiriönsietokykyä koskeva suunnitelma, CER-laki 15 § ja 30.3 §

- Kriittisen toimijan on toteutettava häiriönsietokykynsä varmistamiseksi asianmukaisia ja oikeasuhteisia teknisiä, turvallisuuteen liittyviä ja organisatorisia toimenpiteitä, jotka perustuvat 14 §:ssä tarkoitettuun riskiarviointiin ja muihin asiaan kuuluviin tietoihin. Tässä tarkoituksessa **kriittisen toimijan on laadittava** asianmukaisia ja oikeasuhtaisia teknisiä, turvallisuuteen liittyviä ja organisatorisia toimenpiteitä sisältävä **suunnitelma häiriönsietokyvyn varmistamiseksi.**
- CER-lain 15 §:n mukainen suunnitelma **on laadittava ensimmäisen kerran vuoden kuluessa 14 §:ssä tarkoitetun riskiarvioinnin laatimisesta.**

Suunnitelmassa on oltava selostus:

1) toimenpiteistä poikkeamien syntymisen estämiseksi ottaen huomioon katastrofiriskien vähentämiseen ja ilmastonmuutokseen sopeutumiseen liittyvät toimenpiteet;

2) tilojen ja niissä sijaitsevan infrastruktuurin suojaamisesta kuten aidan asentamisesta, esteiden pystyttämisestä, ilmaisulaitteista ja kulunvalvonnasta sekä muusta fyysisestä suojaamisesta;

3) toimenpiteistä poikkeamien seurauksiin ja häiriötilanteisiin vastaamiseksi, torjumiseksi ja lieventämiseksi;

4) toimenpiteistä poikkeamisista palautumiseksi ottaen huomioon liiketoiminnan jatkuvuuteen liittyvät toimenpiteet ja vaihtoehtoiset toimitusketjut;

5) henkilöstöturvallisuuden varmistamisesta kuten kriittisiä tehtäviä hoitavien henkilöstöryhmien määrittämisestä mukaan lukien ulkopuolisten palvelutarjoajien henkilöstön huomioiminen määrittämisessä, pääsyoikeuksien vahvistamisesta tiloihin, kriittiseen infrastruktuuriin ja arkaluonteisiin tietoihin sekä turvallisuusselvitysten pyytämisestä ja koulutus- ja pätevyysvaatimuksista;

6) tiedottamisesta asianomaiselle henkilöstölle; sekä

7) toteuttamisaikataulua koskevasta suunnitelmasta.

Poikkeamia koskeva ilmoitusvelvollisuus, CER-laki 16 §

- Ensi-ilmoitus
  - Kriittisen toimijan on annettava ensi-ilmoitus valvovalle viranomaiselle ja Valtioneuvoston tilannekeskukselle viimeistään 24 tunnin kuluttua siitä, kun poikkeama on tullut tietoon, jollei välttämättömästä operatiivisesta syystä muuta johdu.
- Yksityiskohtainen raportti
  - Kriittinen toimija antaa yksityiskohtaisen raportin tarvittaessa viimeistään kuukauden kuluttua siitä, kun poikkeama on tullut tietoon yhteensovittamistehtävää hoitavalle ministeriölle, toimialasta vastaavalle ministeriölle ja toimivaltaiselle valvovalle viranomaiselle.

Ensi-ilmoituksen ja yksityiskohtaisen raportin sisältö, CER-laki 17 §

Poikkeamaa koskevaan ensi-ilmoitukseen sisällytetään:

1) tieto poikkeaman havaitsemisesta ja sen luonteesta;

2) arvio mahdollisesta aiheuttajasta tai syystä;

3) arvio mahdollisista seurauksista ja arvio keskeisen palvelun käyttäjien lukumäärästä tai osuudesta, johon häiriö vaikuttaa;

4) tieto, joka on tarpeen poikkeaman mahdollisten rajat ylittävien vaikutusten määrittämiseksi.

Yksityiskohtaiseen raporttiin sisällytetään:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista sekä maantieteellisestä laajuudesta;

2) poikkeaman todennäköisesti aiheuttaneen uhkan tai syyn luonne;

3) toteutetut tai meneillään olevat toimenpiteet vaikutusten lieventämiseksi;

4) mahdolliset rajat ylittävät vaikutukset; sekä

5) muut kuin 1—4 kohdassa tarkoitetut poikkeaman hallinnan kannalta olennaiset tiedot

Velvoite	Tavoite	Kuvaus	Aikataulu
Riskinarviointi	Tunnistaa riskit ja varmistaa toiminnan jatkuvuus	-Toimintaan kohdistuvien riskien sekä niiden vaikutusten arviointi. Luonnonriskit ja katastrofit -Ihmisen aiheuttamat riskit (esim. terrorismi) -Kansanterveydelliset hätätilanteet -Hybridiuhat ja vieraan valtion toiminta	9 kk sen jälkeen, kun toimija on saanut tiedon päätöksestä, jossa toimija nimetään kriittiseksi. Tämän jälkeen päivitys aina tarvittaessa.
Suunnitelma häiriönsietokyvyn varmistamiseksi	Varmistaa, että organisaatiolla on prosessit ja resurssit häiriöiden hallintaan, liiketoiminnan jatkuvuuden turvaamiseen ja vaihtoehtoisten toimitusketjujen käyttöön	-Suunnitelma häiriönsietokyvyn varmistamiseksi ja sen ylläpito. Toimenpiteet poikkeamien syntymisen estämiseksi -Tilojen ja infrastruktuurin suojaaminen -Toimenpiteet häiriötilanteisiin vastaamiseksi -Palautuminen ja jatkuvuus -Henkilöstöturvallisuuden varmistaminen -Tiedottaminen henkilöstölle -Toteuttamisaikataulu	12 kk riskiarvion valmistumisen jälkeen eli 21 kuukauden päästä tiedon saamisesta nimeämispäätöksestä. Tämän jälkeen päivitys aina tarvittaessa.
Jatkuvuuden hallinta	Varmistaa, että organisaatio voi jatkaa toimintaansa kaikissa olosuhteissa	Jatkuvuudenhallinta sekä häiriötilanteisiin vastaaminen ja palautuminen	Osana häiriönsietokyvyn varmistamisen suunnitelmaa
Yhteyspisteen nimeäminen	Helpottaa tiedonkulkua ja koordinointia	Yhteyshenkilön nimeäminen ja yhteystietojen ilmoittaminen viranomaisille	Osana häiriönsietokyvyn varmistamisen suunnitelmaa
Fyysisen infrastruktuurin suojaaminen	Varmistaa fyysisten toimintatilojen turvallisuus	-Fyysisten tilojen riskien arviointi ja tarvittava suojaaminen. Aidat, portit ja muut rakenteelliset ratkaisut -Ilmaisulaitteet ja tekninen valvonta -Kulunvalvontajärjestelmät -Muu fyysinen suojaaminen, esim. kameravalvonta, valaistus ja lukitukset	Osana häiriönsietokyvyn varmistamisen suunnitelmaa
Henkilöstön turvallisuus, koulutus ja tiedottaminen	Hallita henkilöstöriskejä ja varmistaa henkilöstön osaaminen	Kriittisiä tehtäviä hoitavien henkilöiden luotettavuuden varmistaminen turvallisuusselvityksillä Ohjeet häiriötilanteisiin, koulutukset ja harjoittelu	Osana häiriönsietokyvyn varmistamisen suunnitelmaa
Poikkeamien ilmoittaminen	Mahdollistaa nopea reagointi	Ilmoitus merkittävistä poikkeamista viranomaisille	Ensi-ilmoitus 24 tunnin kuluessa tietoon tulosta ja yksityiskohtainen ilmoitus 1 kk tapahtumasta
Osallistuminen arviointeihin ja harjoituksiin	Osallistua viranomaisten järjestämiin harjoituksiin ja arviointeihin	Kehittää valmiuksia ja yhteistyötä	Viranomaisten ohjeistuksen mukaan

Tapausesimerkki – Oy ÄlyEnergia Ab

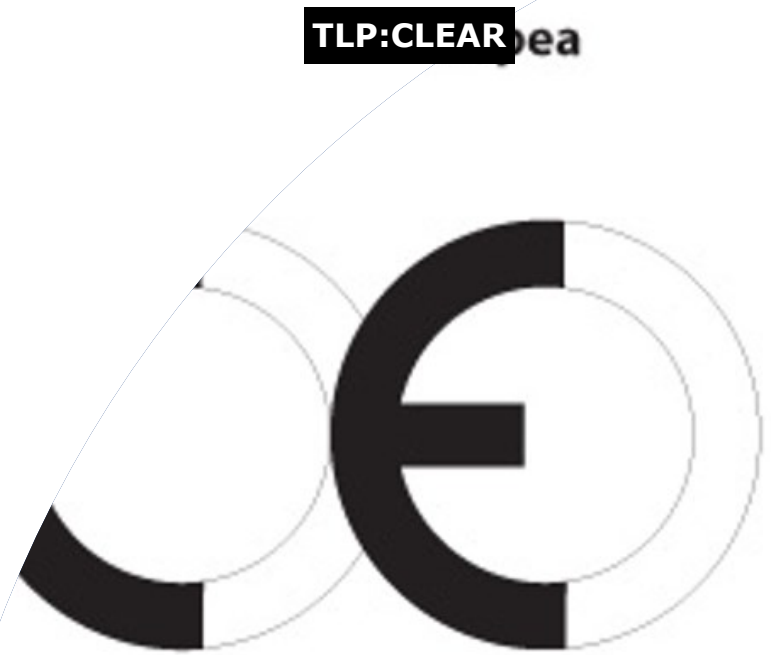
- Toimii energia-alalla
- Tarjoaa keskeistä palvelua (olennainen välttämättömien yhteiskunnallisten toimintojen kannalta)
- Toimii Suomessa
- Häiriö tai keskeytys aiheuttaisi merkittäviä haitallisia vaikutuksia
- -> CER alainen toimija

TLP:CLEAR

TLP:CLEAR

TRAFICOM

CRA



China Export

TLP:CLEAR

Mitä tuotteita CRA koskee?

Valmistajan komponentit
esim. näytöt, kamerat, käyttöjärjestelmät, ohjelmistot

Muiden valmistajien komponentit
esim. muistiyksiköt, prosessorit, mikrosirut

Sovellukset ja lisäosat
esim. etähallinta- ja muut ohjelmistot, lisämuistit, SIM-kortit

EU-markkinoille

Olennaiset vaatimukset

Haavoittuvuuksien korjaaminen

CE-merkintä

TRAFICOM

Tuotteen saattaminen markkinoille

1. Verkkoon yhdistettävä digitaalinen ohjelmisto tai laite kehitetään.

Kyberturvallisuus-ominaisuudet toteutetaan riskiperustaisesti.

CRA artikla 6 ja 13, Liite I

2. Tuotteen on läpäistävä vaatimustenmukaisuuden arviointi ja oltava kyberkestävyys-säädöksen mukainen.

CRA artikla 32

3. Joissain tilanteissa vaatimusten-mukaisuuteen edellytetään ilmoitettua laitosta tai kyberturvallisuus-sertifikaattia.

CRA artiklat 7 ja 8, Liite III ja IV

4. EU-vaatimustenmukaisuusvakuutus laaditaan. Tuotteessa on oltava CE-merkintä.

Tuotteelle ilmoitetaan tukijakso.

Tuote saatetaan markkinoille.

5. Markkinoille saattamisen jälkeinen seuranta.

Tuotteen haavoittuvuudet korjataan tukijakson ajan.

Markkinavalvonta.

Tuotteen vaatimustenmukaisuutta on arvioitava uudelleen, jos tuotteeseen tehdään merkittäviä muutoksia.

Vaikutukset toimijoihin

Valmistaja

Laitevalmistajien pitää huomioida uudet tekniset vaatimukset laitteiden suunnittelussa ja valmistuksessa sekä päivittää laitteen dokumentit mm. EU-vaatimustenmukaisuus-vakuutus.

Maahantuojat ja jakelijat

Velvollisuus varmistaa, että myynnissä on vain vaatimusten mukaisia laitteita.

! Tämä kannattaa varmistaa jo ennen tuotteen ottamista valikoimaan.

Avoimen lähdekoodin ohjelmistovastaavat

Samat säännöt koko EU-alueella

Kun tuote täyttää CRA:n ja muiden sitä koskevien tuotesäädösten vaatimukset, niin laitetta voi myydä vapaasti EU-markkinoilla.

Mitä CRA tarkoittaa laitteen ja ohjelmiston valmistajalle? (13 artikla)

Tuotteen suunnittelu, kehittäminen ja valmistus vastaamaan olennaisia kyberturvallisuus-vaatimuksia (liite I osa I)	Tuotteen kyberturvallisuus-riskien arviointi. Riskienhallinta tuotteen elinkaaren ajan.	Kolmansien osapuolten komponenttien huolellinen valinta	Haavoittuvuuksien hallinta (liite I osa II)
Tukiaika (support period)	Valmisteltava tekninen dokumentaatio & EU-vaatimusten-mukaisuus-vakuutus	Tuotteen tunniste ja valmistajan yhteystiedot	Käyttöohjeet ja tiedot käyttäjälle (liite II)

Tarkemmat velvollisuudet kannattaa tarkistaa asetuksesta

Miten valmistaja voi varmistaa, että laite täyttää CRA:n vaatimukset?

Soveltamalla harmonisoitua standardia	Ilmoitetun laitoksen avulla	Kyberturvallisuus-asetuksen (EU) Kyberturvallisuus-sertifikaatilla

- Kyberkestävyyssäädöksessä on määritelty tavat, joilla valmistaja voi varmistaa laitteen vaatimustenmukaisuuden. (32 artikla)
- Tietyiltä tuoteryhmiltä edellytetään korkeampaa varmuustasoa niihin kohdistuvan kyberturvallisuusriskin ja häiriön vaikutusten laajuuden vuoksi. (7 ja 8 artikla, liite III ja IV)

Tärkeät tuotteet – luokka I

1. Identiteetinhallintajärjestelmät ja korotettujen käyttöoikeuksien hallintaohjelmistot ja -laitteistot
2. Erilliset ja sulautetut selaimet
3. Salasanojen hallinnointityökalut
4. Ohjelmistot, jotka etsivät, poistavat tai asettavat karanteeniin haittaohjelmistoja
5. VPN-ratkaisut
6. Verkonhallintajärjestelmät
7. Tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)
8. Käynnistysohjelmat
9. Julkisen avaimen infrastruktuuri ja digitaalisen varmenteen luomiseen käytettävät ohjelmistot
10. Fyysiset ja virtuaaliset verkkorajapinnat
11. Käyttöjärjestelmät
12. Reitittimet, modeemit ja kytkimet
13. Mikroprosessorit, joissa on turvallisuustoimintoja
14. Mikro-ohjaimet, joissa on turvallisuustoimintoja
15. Sovelluskohtaiset integroidut piirit (ASIC) ja kenttäohjelmoitavat porttimatriisit (FPGA), joissa on turvallisuustoimintoja
16. Älykodin yleiskäyttöiset virtuaaliavustajat
17. Älykodin tuotteet, joissa on turvallisuustoimintoja, mukaan lukien ovien älylukot, turvakamerat, itkuhälyttimet ja hälytysjärjestelmät
18. Internetyhteydellä varustetut lelut
19. Terveyttä seuraavat tai lapsille tarkoitetut puettavat laitteet

TLP:CLEAR

Tärkeät tuotteet – luokka II kriittiset tuotteet

Liite III - Luokka II

1. Virtualisointialustat (hypervisorit ja konttialustat)

2. Palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät (IDS ja IPS)

3. Väärinkäytöltä suojatut mikroprosessorit

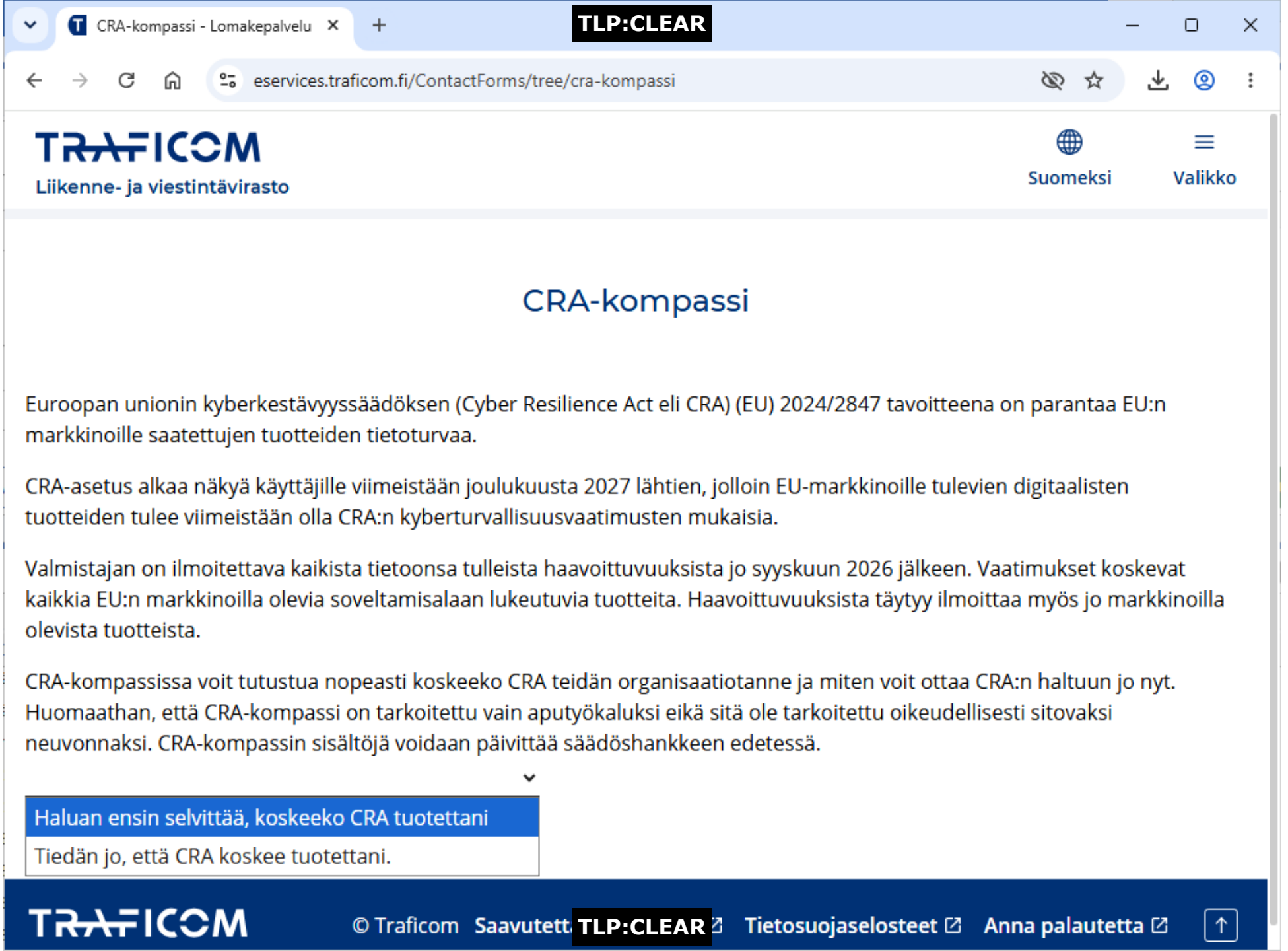
4. Väärinkäytöltä suojatut mikro-ohjaimet

LIITE IV - KRIITTISET TUOTTEET

1. Fyysiset laitteet, joissa on peukaloinnilta suojaavia turvamekanismeja

2. Älymittareiden yhdyskäytävät ja kryptolaskentaan käytettävät laitteet

3. Älykortit ja turvaelementit



Laitteiden ja ohjelmistojen valmistajien raportointivelvollisuus (14 artikla)

Valmistajalla on velvollisuus raportoida ENISA:lle ja kansalliselle CSIRT-yksikölle

- aktiivisesti hyödynnetyistä **haavoittuvuuksista** ja
- tuotteidensa tietoturvaan vaikuttavista vakavista **poikkeamista**.

Valmistajan on lisäksi oikea-aikaisesti **tiedotettava** niitä **käyttäjiä, joihin vaikutukset kohdistuvat** ja tarvittaessa kaikkia käyttäjiä.

Ennakkovaroitus-ilmoitus

24 h kuluessa

- Tieto vakavasta poikkeamasta tai aktiivisesti hyödynnettävästä haavoittuvuudesta
- Minkä EU-jäsenvaltioiden alueella valmistaja tietää tuotteen olevan saatavilla?

Haavoittuvuus- tai poikkeama-ilmoitus

72 h kuluessa

- Tarkemmat tiedot haavoittuvuudesta tai tapahtumasta, sen vaikutuksista ja tehdyistä korjauksista tai lieventävistä toimista
- Mitä korjaavia tai lieventäviä toimenpiteitä **käyttäjät** voivat itse toteuttaa?

Loppuraportti

14 vrk kuluessa, kun haavoittuvuuden korjaava tai lieventävä toimenpide on käytettävissä

1 kk kuluessa poikkeamailmoituksen jättämisestä

- Puuttuvat tiedot, ellei kaikkia tietoja ole jo annettu

Tapausesimerkki – Oy ÄlyEnergia Ab

- ÄlyOhjaaja™ on digitaalisia elementtejä sisältävä tuote ja siten CRA alainen
- Tuote ei ole kategorioissa tärkeä tai kriittinen tuote, joten valmistaja voi varmistua turvallisuudesta omavalvonnalla harmonisoituja standardeja noudattaen.

AIA

AI Act pätee aina kun AI:ta käytetään EU:ssa, paitsi

kansallinen turvallisuus

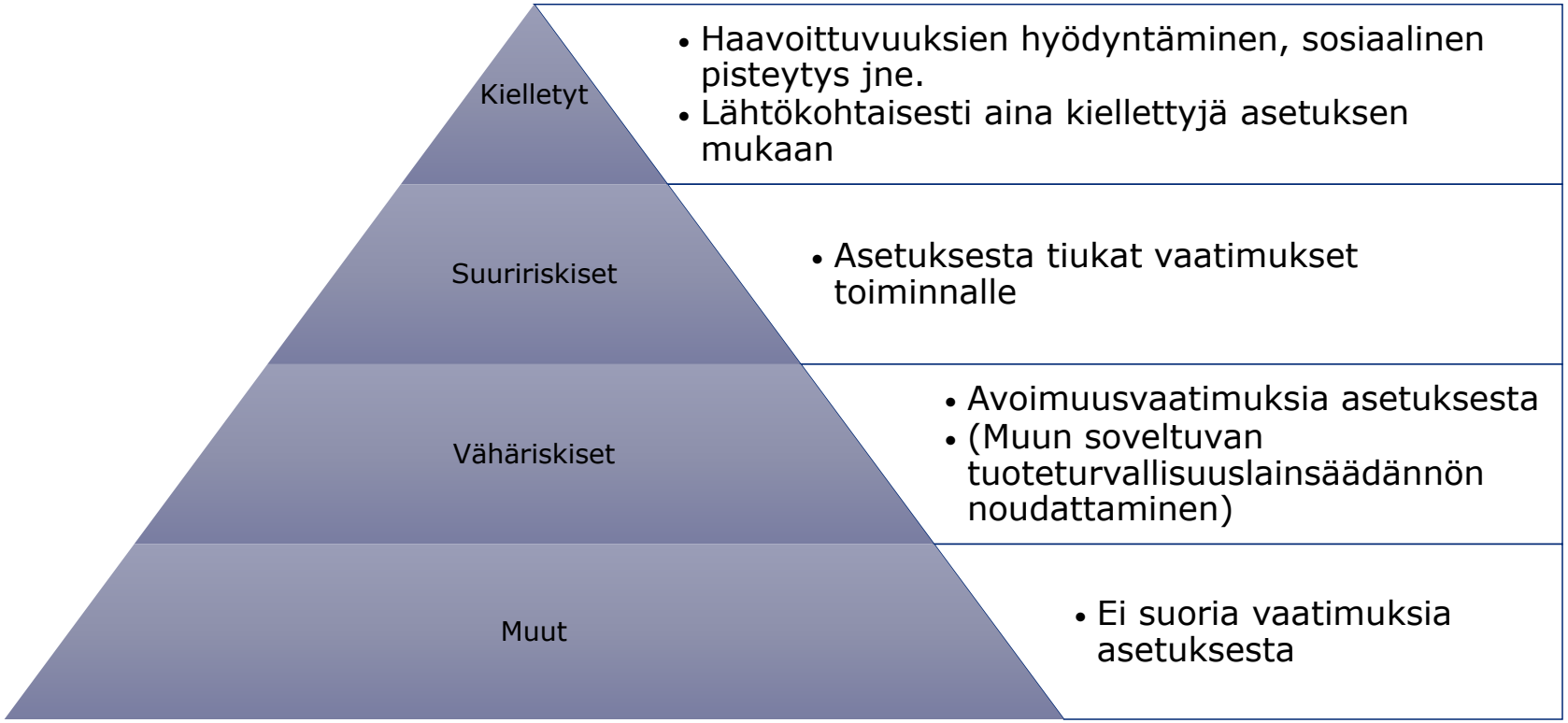
tieteellinen tutkimus

muu tutkimus, testaus ja kehitys

henkilökohtainen käyttö

avoin lähdekoodi (jos ei kielletty tai suuririskinen)

Tekoälyasetuksen riskiperustainen jaottelu



Lisäksi ns. Yleiskäyttöiset tekoälymallit, joiden toiminnalle omat vaatimuksensa

TLP:CLEAR

Suuririskiset tekoälyjärjestelmät suomeksi

“merkittävä haitallinen vaikutus EU:n kansalaisten terveyteen, turvallisuuteen ja perusoikeuksiin.”

Suuririskiset tekoälyjärjestelmät juristiksi

Tekoälyasetuksen sääntely koskee pääosin suuririskisiä tekoälyjärjestelmiä. Näillä tarkoitetaan tekoälyjärjestelmiä, joilla voi olla merkittävä haitallinen vaikutus EU:n kansalaisten terveyteen, turvallisuuteen ja perusoikeuksiin.

Tekoälyjärjestelmät ovat ’suuririskisiä’ järjestelmiä, jos niitä on tarkoitus käyttää

1. tuotteina tai tuotteiden turvallisuusosina, joiden on läpäistävä kolmannen osapuolen vaatimustenmukaisuuden arviointi asetuksen **liitteessä I** tarkoitetun lainsäädännön mukaisesti:

   Koneet, lelut, huvikäyttöiset alukset ja vesiskootterit, hissit, laitteet ja suojajärjestelmät, jotka on tarkoitettu mahdollisesti räjähdysvaarallisiin ympäristöihin, radiolaitteet, painelaitteet, köysirata-asennukset, henkilönsuojaimet, kaasua polttavat laitteet, lääkinnälliset laitteet, in vitro -diagnostiikkaan tarkoitetut lääkinnälliset laitteet, siviili-ilmailu, 2/3-pyöräiset ajoneuvot, maatalous- ja metsäkoneet, merivarusteet, rautatiejärjestelmät, moottoriajoneuvot ja niiden perävaunut, miehittämättömät ilma-alukset

   Liitteessä I listattu lainsäädäntö kattaa yllä olevat kategoriat, mutta voi kattaa myös niihin liittyviä tuotteita, kuten robotiikkaa.

2 johonkin asetuksen **liitteessä III** kuvattuun tarkoitukseen:

   Biometria (henkilöiden biometrinen tunnistaminen tai luokittelu ja/tai henkilöiden tunnetilojen tunnistaminen), Kriittisen infrastruktuurin hallinta ja toiminta, Koulutus ja ammatillinen koulutus, Rekrytointi ja henkilöstöhallinto, Välttämättömät palvelut (esimerkiksi yksilöiden tukikelpoisuuden arviointi julkisiin avustuksiin, kuten terveydenhuoltopalveluihin, sosiaaliturvaan, vammaisetuuksiin; luottokelpoisuuden arviointi; hätäpuheluiden arviointi ja luokittelu), Rikollisuusanalytiikka, todisteiden kerääminen ja arviointi, Maahanmuuttajien tunnistaminen, maahanmuuton riskinarviointi ja maahanmuuttohakemusten arviointi, Oikeudenhoito ja demokraattiset prosessit

Liitteen III tekoälyjärjestelmiä, ei kuitenkaan pidetä suuririskisinä järjestelminä, jos ne eivät aiheuta merkittävää riskiä luonnollisten henkilöiden terveydelle, turvallisuudelle tai perusoikeuksille; neljä kriteeriä, joista vähintään yhden on täytyttävä: Tekoälyjärjestelmä ei ole suuririskinen, jos sen tarkoituksena on:

A) suorittaa suppea menettelyllinen tehtävä
B) parantaa aiemmin suoritetun ihmisen toiminnan tulosta
C) havaita päätöksentekotapoja tai poikkeamia aiemmista päätöksentekotavoista, eikä sen tarkoituksena ole korvata aiemmin tehtyä ihmisen tekemää arviota tai vaikuttaa siihen ilman asianmukaista ihmisen suorittamaa arviota
D) Suorittaa valmisteleva tehtävä, joka koskee liitteessä III lueteltujen käyttötapausten kannalta merkityksellistä arviointia

HUOM! Jos tekoälyjärjestelmä suorittaa luonnollisten henkilöiden profilointia, sitä pidetään aina suuririskisenä tekoälyjärjestelmänä, eikä siihen voi soveltua mikään edellä mainituista neljästä poikkeuksesta.

Tiukoista vaatimuksista (suuririskiset)

Laadunhallintajärjestelmä

Riskienhallinta

Tekninen dokumentaatio

Tiedonhallinta

Lokitus

Valvontavelvoitteet ihmisille

Itsearviointi (tai riippumaton arviointi biometriikassa)

Rekisteröinti

Viranomaiskommunikaatio

Avoimmuusvelvoite: kerro käyttäjälle että sisältö on tekoälyllä tehty tämä vuorovaikuttaa tekoälyn kanssa

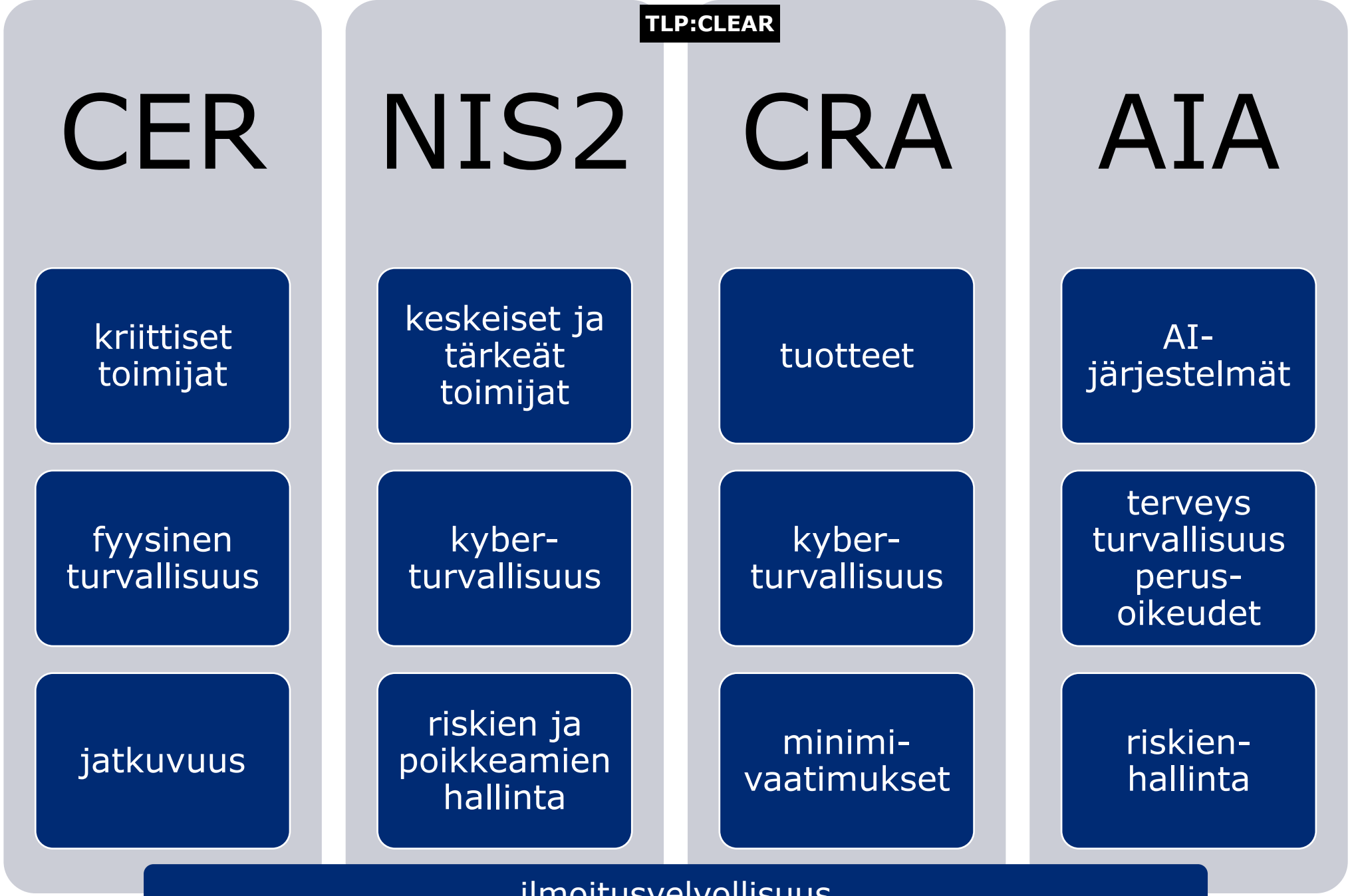
AIA ilmoitusvelvollisuus

- Korkean riskin tekoälyjärjestelmän vakavat vaaratilanteet
  - esimerkiksi vakava terveyshaitta, vakava perusoikeusloukkaus, vakava tai peruuttamaton häiriö kriittisen infrastruktuurin hallinnassa ja toiminnassa, vakava omaisuus- tai ympäristövahinko
- Käyttöönottajan on ilmoitettava tilanteesta välittömästi järjestelmän tarjoajalle ja asianomaiselle markkinavalvontaviranomaiselle sekä tarvittaessa keskeytettävä käyttö
- Ilmoitus pääsääntöisesti viimeistään 15 päivässä, laajamittaisesta rikkomuksesta tai kriittisen infrastruktuurin häiriöstä 2 päivässä.

TLP:CLEAR

Tapausesimerkki – Oy ÄlyEnergia Ab

- ÄlyOhjaaja™ on markkinoilla tarjolla oleva tekoälyjärjestelmä ja siten AIA alainen
- Oy ÄlyEnergia Ab käyttää tuotetta optimointiin, ja tässä käyttötarkoituksessa se on vähäriskinen järjestelmä
- Teleoperaattori-asiakas käyttää tuotetta tukiasemien virransyötön varmistamiseen. Tässä tilanteessa tekoälyratkaisu onkin kriittisen digitaalisen infrastruktuurin turvakomponentti ja siitä tulee suuririskinen tekoälyjärjestelmä.


CER
NIS2
CRA
AIA
kriittiset toimijat
keskeiset ja tärkeät toimijat
tuotteet
AI-järjestelmät
fyysinen turvallisuus
kyber-turvallisuus
kyber-turvallisuus
terveys turvallisuus perus-oikeudet
jatkuvuus
riskien ja poikkeamien hallinta
minimi-vaatimukset
riskien-hallinta
ilmoitusvelvollisuus