ISO/IEC 27001

CERTIFIED BY

huld | Certification

NIS2
-
laki kyberturvallisuuden riskienhallinnasta

Mika Lindberg
Opsec Oy

Yleisesti

Laajentaa aiempaa NIS-direktiiviä ilmoittamisesta aktiiviseen tekemiseen.

- Riskienhallinta
- Tietoturvakontrollit

Tuo mukanaan uusia toimialoja.

- Energia, liikenne, pankki ja finanssi, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkihallinto, avaruus
- Uusia toimialoja kuten jätehuolto, elintarviketeollisuus ja valmistavaa teollisuutta.

Sovelletaan seuraavasti:

- Keskisuuret ja suuret toimialan perusteella
- koosta riippumatta kriittisiä toimijoita (artikla 2 kohta 2) ja direktiivin 2022/2557 liite 1

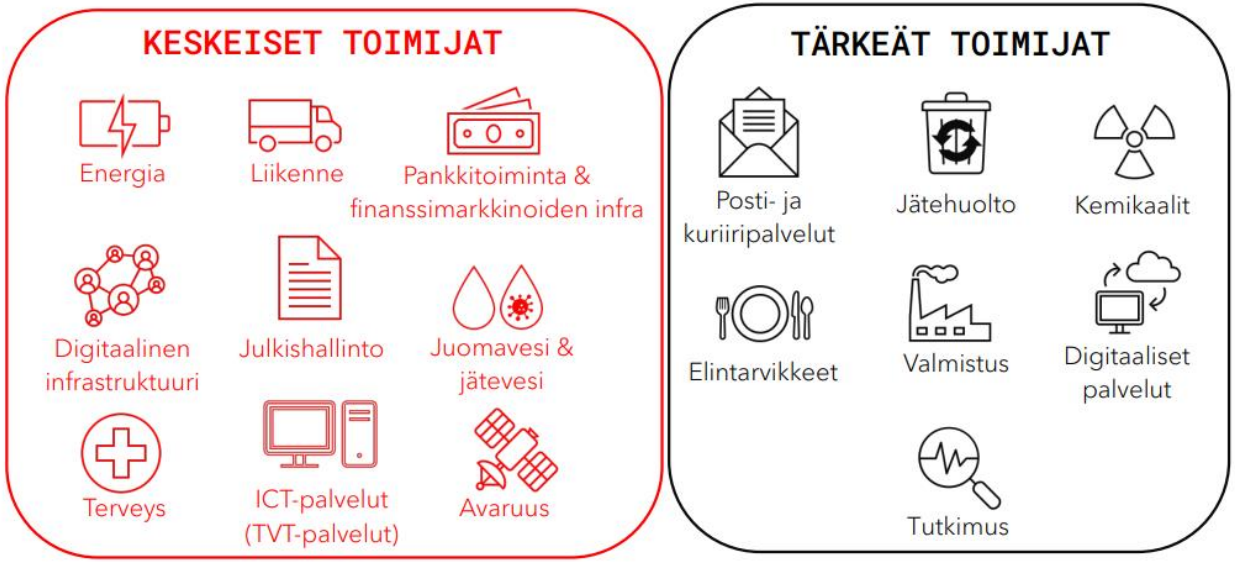
Valvontamekanismi

- Keskeiset (erittäin kriittiset) toimijat ennakoiva valvonta
- Tärkeät toimijat jälkikäteen valvonta

Seuraamusmaksut

- Enimmäismäärä 10 000 000 euroa tai 2 prosenttia kokonaisliikevaihdosta
- Enimmäismäärä 7 000 000 euroa tai 1,4 prosenttia kokonaisliikevaihdosta

- Johdon henkilökohtaiset vastuut ja toimintakiellot



Lainsäädännön soveltamisalat toimialoittain jaoteltuna keskeisiin ja tärkeisiin toimijoihin.

Vaatimukset toimitusketjuun tuovat välillisiä vaatimuksia

Kyberala ry 23.9.2024
https://www.fisc.fi/sites/fisc/files/inline-files/KYBERALA_NIS2_OPAS_0.9_BETA.pdf

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	●	◐	○
Pankkiala	Luottolaitokset	●	◐	○
Finanssimarkkinoiden infrastruktuurit	Kauppapaikkojen ylläpitäjät ja keskusvastapuolet	●	◐	○
Terveys	Terveydenhuoltopalvelujen tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimus ja kehitys, farmaseuttisten perustuotteiden ja -valmisteiden 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*		◐	

* katso ehdotus tiedonhallintalain muuttamisesta 4a luku 18 a §

NIS2 Liite II

Muut 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
Posti- ja kuriiripalvelut		◐	◐	○
Jätehuolto		◐	◐	○
Kemikaalit	Valmistus, tuotanto ja jakelu	◐	◐	○
Elintarvikkeet	Teollinen tuotanto, jalostus ja tukkukauppa	◐	◐	○
Valmistus	Lääkinnälliset laitteet, tietokoneet sekä elektroniset ja optiset tuotteet, sähkölaitteet, muut koneet ja laitteet, moottoriajoneuvot ja perävaunut sekä puoliperävaunut, muut kulkuneuvot	◐	◐	○
Digitaalisen palvelun tarjoajat	Verkossa toimivien markkinapaikkojen, hakukoneiden ja verkkoyhteisöalustojen tarjoajat	◐	◐	○
Tutkimustoiminta	Tutkimusorganisaatiot	◐	◐	○
Verkkotunnusten rekisteröintipalveluja tarjoavat toimijat	Kaikenkokoiset toimijat, mutta vain toimijaluetteloon ilmoittautumisen ja verkkotunnusten rekisteröintitietoja koskevien velvoitteiden osalta.			

Suuret toimijat
Yritys, jonka palveluksessa on vähintään 250 työntekijää tai jonka vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa

Keskisuuret toimijat
50–249 työntekijää tai vuosiliikevaihto ja taseen loppusumma ylittävät 10 miljoonaa euroa

Koosta riippumattomat toimijat
Taulukossa kuvatun lisäksi NIS2-direktiiviä sovelletaan liitteessä I tai II tarkoitettua toimijatyyppiä oleviin toimijoihin niiden koosta riippumatta, kun:

- Toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen.
- Häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen.
- Häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia.
- Toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Lisäksi NIS2-direktiiviä sovelletaan CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta. CER-kriittisten toimijoiden tunnistaminen tapahtuu arviolta vuoden 2026 aikana.

Sekä yllä mainitut ns. koosta riippumattomat poikkeusperusteiset toimijat että ns. CER-kriittiset toimijat ovat keskeisiä toimijoita.

Soveltamisessa huomioitava myös organisaatioiden omistussuhteet ja toimintahäiriöiden vaikutukset yhteiskunnan toimintaan.

Traficom 23.9.2024
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_230424.pdf

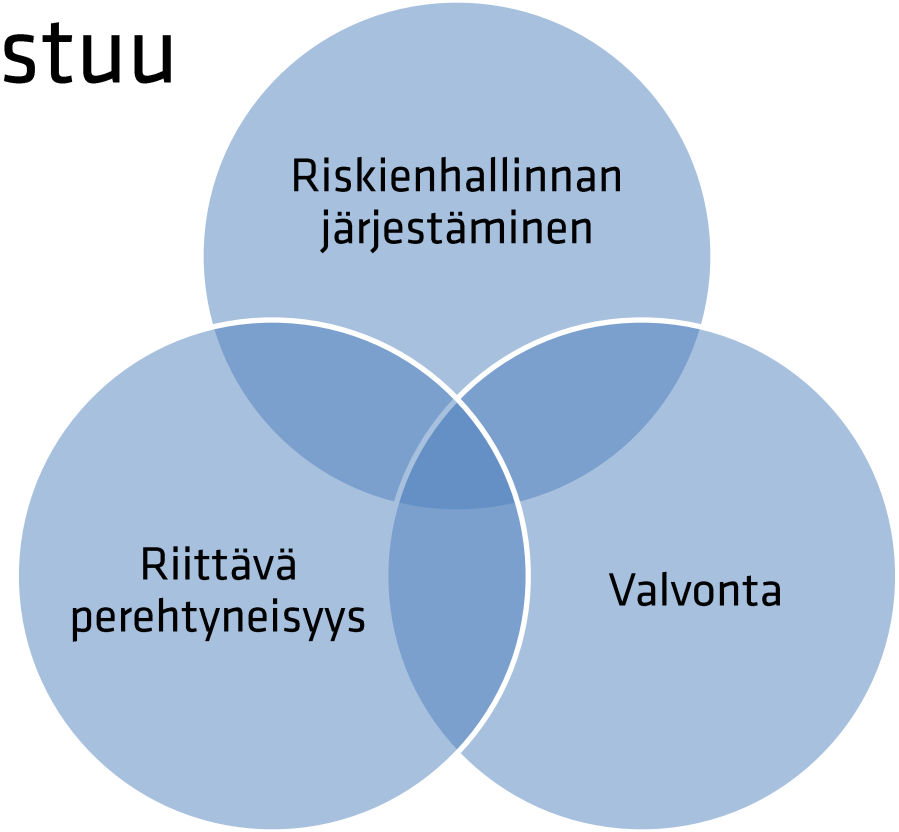
Aikataulu


Direktiivi astui voimaan 14. joulukuuta 2022
Hallituksen esitys lausunnoille Syyskuu 2023
Traficomin esitys käytännöistä lausunnoille huhtikuu 2024
Kansallinen lainsäädäntö valmistuttava 17.10.2024
Soveltaminen alkaa 18.10.2024

Vaatimukset

NIS2 korostaa johdon vastuuta ja riskien hallintaa

Johdon vastuu



Riskienhallinta

Hallituksen esitys
https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd&attachmentId=21084

Hallituksen esitys
https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd&attachmentId=21084

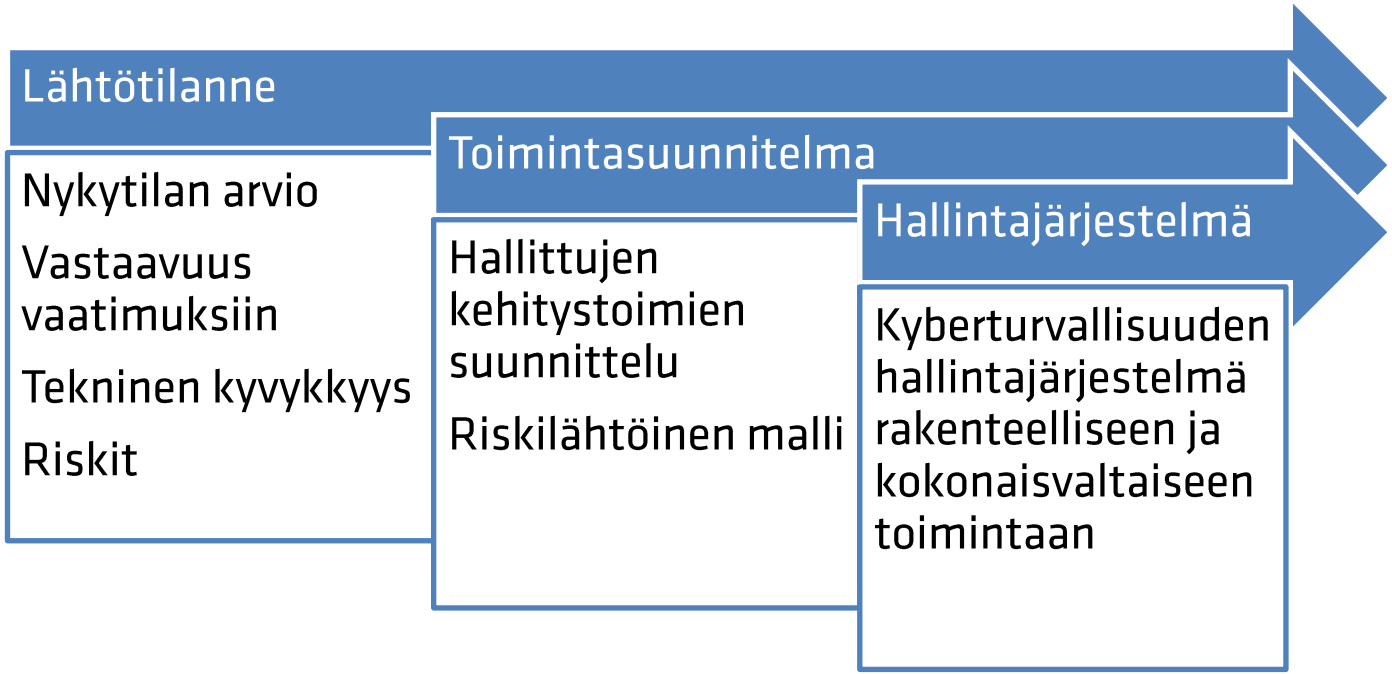
Kyberhygienia - tarkistuslista

- Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille
- Toimija on tunnistanut kriittisimmän omaisuutensa
- Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä
- Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä
- Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan
- Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti
- Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista
- Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti
- Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä
- Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu
- Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu
- Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa
- Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki)

Poikkeamailmoitukset

Vaatimus kolmiportaisella poikkeamienilmoittamisen käytännölle

Käytännön ratkaisuja



Lähtötilannekartoitus

Kartoitetaan käytännönläheisesti nykyiset kyberturvallisuuden käytännöt.

Kuvataan niiden nykyinen toteutus tiivistetysti ja tunnistetaan puutteelliset toiminnot.

Tunnistetaan kokonaan vailla toimintaa olevat osa-alueet.

Luodaan tilannekuva NIS2 -vaatimustenmukaisuudesta ja priorisoitu toimintasuunnitelma etenemisestä. Tunnistetaan myös ne osiot, mitkä vaikuttavat organisaation muihin toimintoihin, kuten kouluttaminen.

Hallintajärjestelmän perusta

Vaatimukset määrittävät, mitä ulkoisia ja sisäisiä vaatimuksia tietoturvallisuuteen kohdistuu.

Suojattava omaisuus kertoo, mitä tieto-omaisuutta hallussamme on ja mitä suojaamme toiminnassa.

Riskit ovat suojattavaan tieto-omaisuuteen kohdistuvia epävarmuustekijöitä ja uhkia. Mitä seurauksia niistä voi meille olla?

Tietoturvaperiaatteiden määrittäminen:
Mikä on tietoturvan tavoite ja rooli organisaatiossa, miten siinä organisoidutaan?

Tietoturvasuunnitelma on toimintakuvaus, jolla tietoturvaperiaatteet viedään osaksi toimintaa. Konkretisoi sitä, miten periaatteissa ilmaistuihin tavoitteisiin päästään.

Tietoturvaohje on käytännön ohjeita ja sen on oltava osa perehdytyssuunnitelmaa. Antaa keinot toimia arkipäivän tilanteissa.

Pika-analyysi

- Kuulummeko NIS2 piiriin tai onko syytä varautua sen velvoitteisiin sopimusten kautta?
- Olemmeko tunnistaneet kriittiset tietojärjestelmät, tietoaineistot, toiminnot, toimitusketjut, henkilöt ja tilat?
- Tunnistammeko, arvioimmeko ja hallitsemmeko edellä mainittuihin kohdistuvia riskejä säännöllisesti määritellyn toimintamallin mukaisesti?
- Olemmeko kuvanneet kyberturvallisuuden keskeiset menettelyt ja tekniset toteutukset?
- Valvommeko riskienhallinnan, hallinnollisten menettelyiden ja teknisten toimintojen toimintaa ja vaikuttavuutta?
- Olemmeko varautuneet riittävin keinoin kyberturvallisuuspoikkeamiin? Havaitsemmeko ne, pystymmekö rajoittamaan niitä ja palautumana niistä. Onko määritelty menettelyt niiden arviointiin ja ilmoittamiseen?

Yhteenveto

Soveltamisalan piirissä keskisuuret ja suuret organisaatiot nimetyiltä toimialoilta.

Asettaa velvoitteet kyberturvallisuuden riskienhallintaan ja toteutukseen kaikki vaaratekijät huomioivalla lähestymistavalla.

Vaatii huomioimaan nimetyt kyberturvallisuuden hallintakeinot sekä kyberhygienian perusteet.

Korostaa johdon vastuuta kyberturvallisuuden järjestämisessä ja valvonnassa.

Vaatii poikkeamien havainnointi, analysointi ja käsittely kyvykkyyttä.

Tietolähteitä

Direktiivi
https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2555

Hallituksen esitys
https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd&attachmentId=21084

Traficomin NIS2 sivusto
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Traficomin luonnos toimenpidesuosituksista
https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4&attachmentId=22133

Kyberala r.y:n opas
https://www.fisc.fi/sites/fisc/files/inline-files/KYBERALA_NIS2_OPAS_0.9_BETA.pdf

Mika Lindberg
p. 020 198 6698
mika.lindberg@opsec.fi

OPSEC OY
Tiedekatu 2, 60320 Seinäjoki
p. 020 198 6690,
info@opsec.fi
www.opsec.fi

ISO/IEC 27001
CERTIFIED BY
huld | Certification