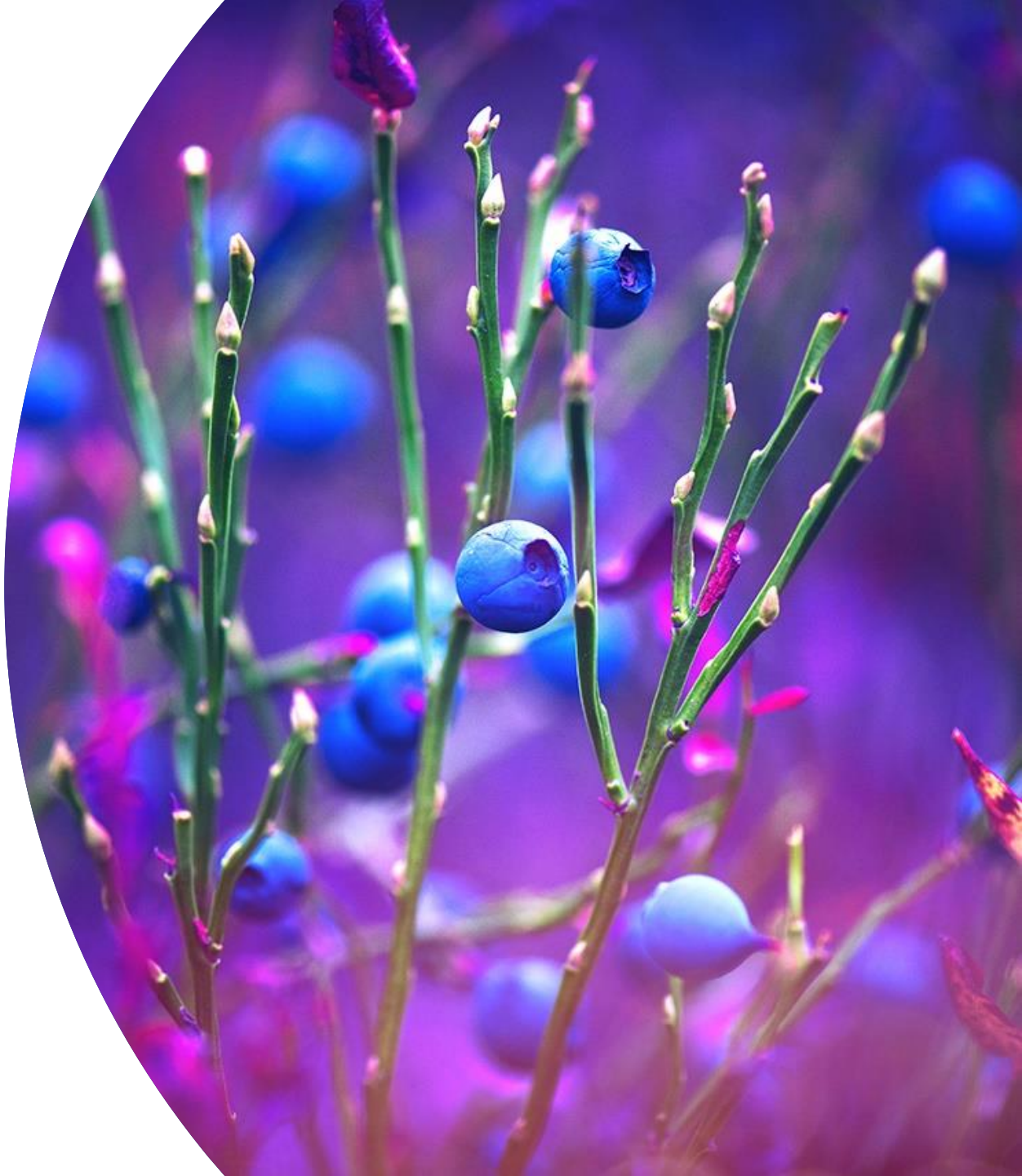
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Viranomaisen käytännön näkemyksiä NIS2 -direktiivin soveltamiseen Suomessa

Digipoolin vuosiseminaari
15.11.2024



Energia

Liikenne

Pankkitoiminta

Finanssimarkkinoiden infrastruktuuri

Terveys

Juomavesi

Jätevesi

Digitaalinen infrastruktuuri

TVT-palvelujen hallinta (yritysten välinen)

Julkishallinto

Avaruus

Posti- ja kuriiripalvelut

Jätehuolto

Kemikaalien valmistus, tuotanto ja jakelu

Elintarvikkeiden tuotanto, jalostus ja jakelu

Valmistus

Digitaalisen palvelun tarjoajat

Tutkimustoiminta

NIS2-toimialat ja valvovat viranomaiset

Valvovat viranomaiset
Traficom
Energiavirasto
Finanssivalvonta
Valvira
Tukes
Fimea
Ruokavirasto
Etelä-Savon ELY-keskus

Ks. tarkemmin: https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Toimijaluetteloon ilmoittautuminen

- Jokainen valvova viranomainen pitää omalla toimialallaan toimijaluetteloa.
- Traficomin osalta toimijaluetteloon ilmoittautuminen avataan kyberturvallisuuslain tullessa voimaan.
- Ilmoittautumisvelvollisuus luetteloon direktiivin mukaisten toimialojen keskeisillä ja tärkeillä toimijoilla.
- Tarkoituksena parantaa tilannekuvaa sääntelyn piiriin kuuluvien toimialojen osalta niin kansallisesti kuin koko Euroopan osalta.

NIS2-ilmoitussovelluksen käyttö

- Toimijat voivat tehdä ilmoitukset merkittävistä poikkeamista **keskitetysti** tätä kautta.
- Traficom julkaisee ilmoitussovelluksen, kun kyberturvallisuuslaki tulee voimaan.
- Sovellus välittää ilmoituksen oikealle valvovalle viranomaiselle ja Kyberturvallisuuskeskuksen CSIRT-yksikölle, jolta toimija voi myös halutessaan pyytää apua ns. lisälomakkeella.

Valvonnan nostoja 1/2

- KTK painottaa ennakko-ohjauksen ja neuvonnan merkitystä NIS2-toimijoille vuonna 2025
- Uutta sääntelyä ja monia uusia valvottavia toimijoita
  - Komission NIS2 täytäntöönpanoasetus vasta julkaistu ja soveltamisohjeistus vielä tulossa
  - Komission asetuksen osalta tavoitteena mahd. yhdenmukainen tulkintakäytäntö EU:n sisällä
    - Huom. komission asetus ja mainittu ohjeistus koskevat vain tiettyjä digitaalisen infran toimijoita, TVT-palvelujen tarjoajia ja digitaalisia palveluita
- Toiveena luottamuksen rakentaminen uusien valvottavien toimijoiden ja valvovan viranomaisen välillä.

Valvonnan nostoja 2/2

- ENISA on julkaissut julkisille kommenteille teknisen ohjeistuksen Komission NIS2 täytäntöönpano-asetuksen kyberturvallisuusvaatimuksista.
  - Ohjeistuksessa on viitteet myös Traficomin Kybermittariin, ja tuleva viimeistelty versio Traficomin suosituksesta NIS-valvoville viranomaisille tulee sisältämään viitteet myös tähän ohjeistukseen.
  - Lausuntoaikaa 9.12.2024, klo 18.00 CET asti.
    - ks. https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act

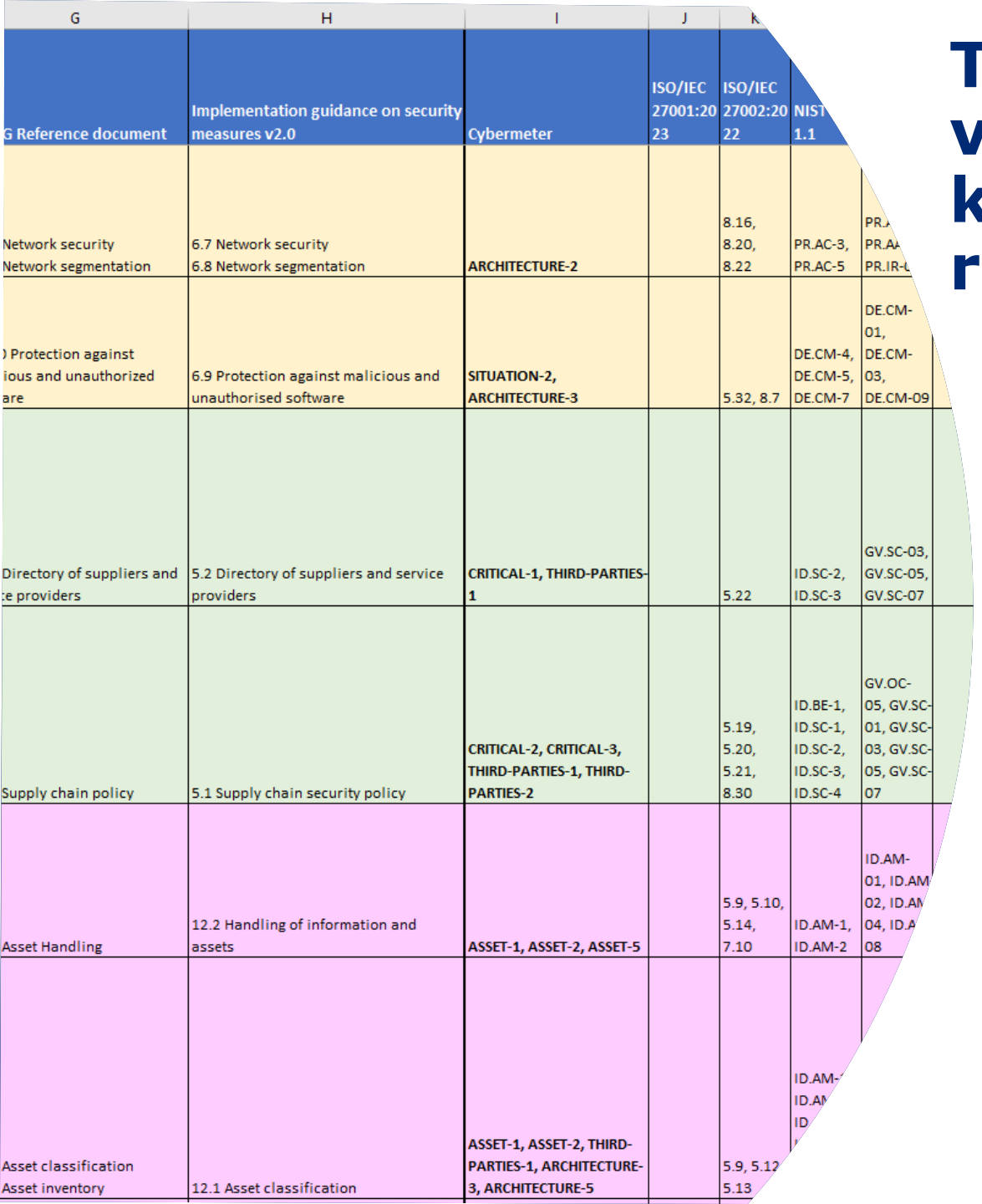
Traficomin suositus NIS valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

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**.



G Reference document	Implementation guidance on security measures v2.0	Cybermeter	ISO/IEC 27001:2023	ISO/IEC 27002:2022	NIST 1.1	
Network security Network segmentation	6.7 Network security 6.8 Network segmentation	ARCHITECTURE-2		8.16, 8.20, 8.22	PR.AC-3, PR.AC-5	PR.A PR.AA PR.IR-L
) Protection against ious and unauthorized are	6.9 Protection against malicious and unauthorised software	SITUATION-2, ARCHITECTURE-3		5.32, 8.7	DE.CM-4, DE.CM-5, DE.CM-7	DE.CM-01, DE.CM-03, DE.CM-09
Directory of suppliers and :e providers	5.2 Directory of suppliers and service providers	CRITICAL-1, THIRD-PARTIES-1		5.22	ID.SC-2, ID.SC-3	GV.SC-03, GV.SC-05, GV.SC-07
Supply chain policy	5.1 Supply chain security policy	CRITICAL-2, CRITICAL-3, THIRD-PARTIES-1, THIRD-PARTIES-2		5.19, 5.20, 5.21, 8.30	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4	GV.OC-05, GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07
Asset Handling	12.2 Handling of information and assets	ASSET-1, ASSET-2, ASSET-5		5.9, 5.10, 5.14, 7.10	ID.AM-1, ID.AM-2	ID.AM-01, ID.AM-02, ID.AM-04, ID.A-08
Asset classification Asset inventory	12.1 Asset classification	ASSET-1, ASSET-2, THIRD-PARTIES-1, ARCHITECTURE-3, ARCHITECTURE-5		5.9, 5.12 5.13	ID.AM- ID.AM ID	

Traficomin suositus NIS valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

- Lausunnot on käsitelty. Yhteenveto luettavissa KTK:n verkkosivuilta.
- Suosituksen laajennettuja ohjeita on tarkennettu täytäntöönpano-asetuksen (EU) 2024/2690 osalta.
- Suositus julkaistaan kun kyberturvallisuuslaki tulee voimaan.
- Suosituksen liitteenä julkaistaan ristiinviittaustaulukko.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos

Kalle Varjola

etunimi.sukunimi@traficom.fi