TIS2 direktyvos tiesioji: naujausios žinios, veiksmų planas ir sprendimai

Evaldas Valūnas
Grupės vadovas, Saugumo sprendimų kompetencijos centras, Atea

TIS2. Kas tai ?

Direktyvos

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2016/1148
... dėl priemonių aukštam bendram **Tinklų ir Informacinių Sistemų** saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555
... dėl priemonių aukštam bendram **kibernetinio saugumo lygiui** visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas ... ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)

Tikslai

- Padidinti Europos Sąjungoje veikiančių įmonių visuose atitinkamuose sektoriuose kibernetinio atsparumo lygį.

- Sumažinti atsparumo nenuoseklumą visoje vidaus rinkoje, sektoriuose, kuriems jau taikoma direktyva.

Teisės aktai

- Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428
- Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo Nr. 818
- Lietuvos Respublikos administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas Nr. XII-1869

Šaltinis: NIS Directive tool — ENISA (europa.eu)

Pozicija

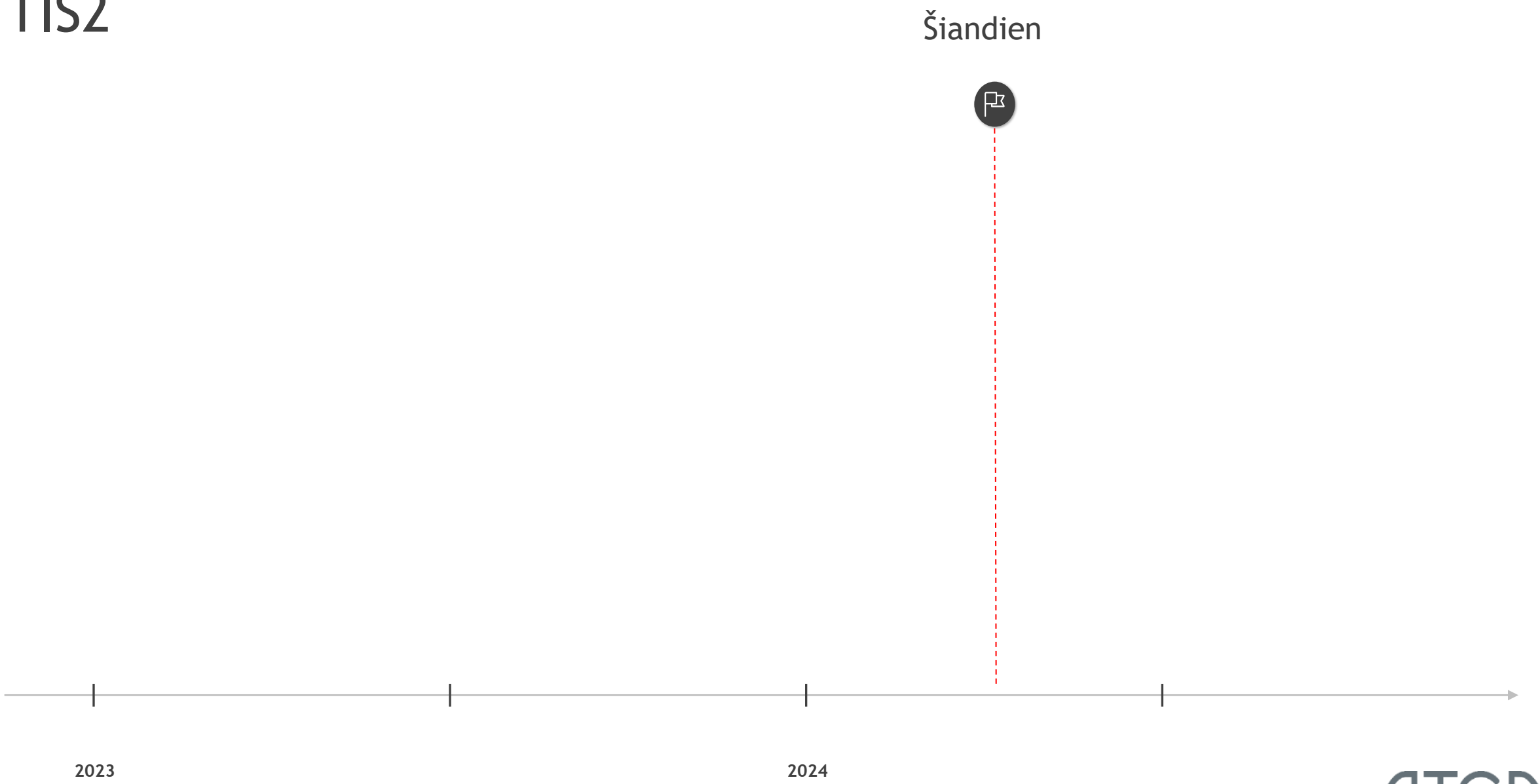
- KAM, bendradarbiaudama su kitomis suinteresuotomis Lietuvos institucijomis ir organizacijomis, derybose išlaikė ambicingus NIS2 direktyvos tikslus dėl taikymo srities išplėtimo, aukštesnio lygio rizikos valdymo ir aiškių kriterijų nustatymo, kartu užtikrinant šių nuostatų proporcingumą.

- Šiuo metu atliekamas NIS2 direktyvos nuostatų ir jų atitikties teisės aktams vertinimas, jų aptarimas su susijusiomis Lietuvos institucijomis. Preliminariai nustatyta, kad dėl įsigaliojusios NIS2 direktyvos gali reikėti keisti 11 teisės aktų ir įtraukti kitas institucijas (pagal kompetencijas elektroninių ryšių, asmens duomenų apsaugos, krizių valdymo, finansų sektoriaus srityje ir pan.).

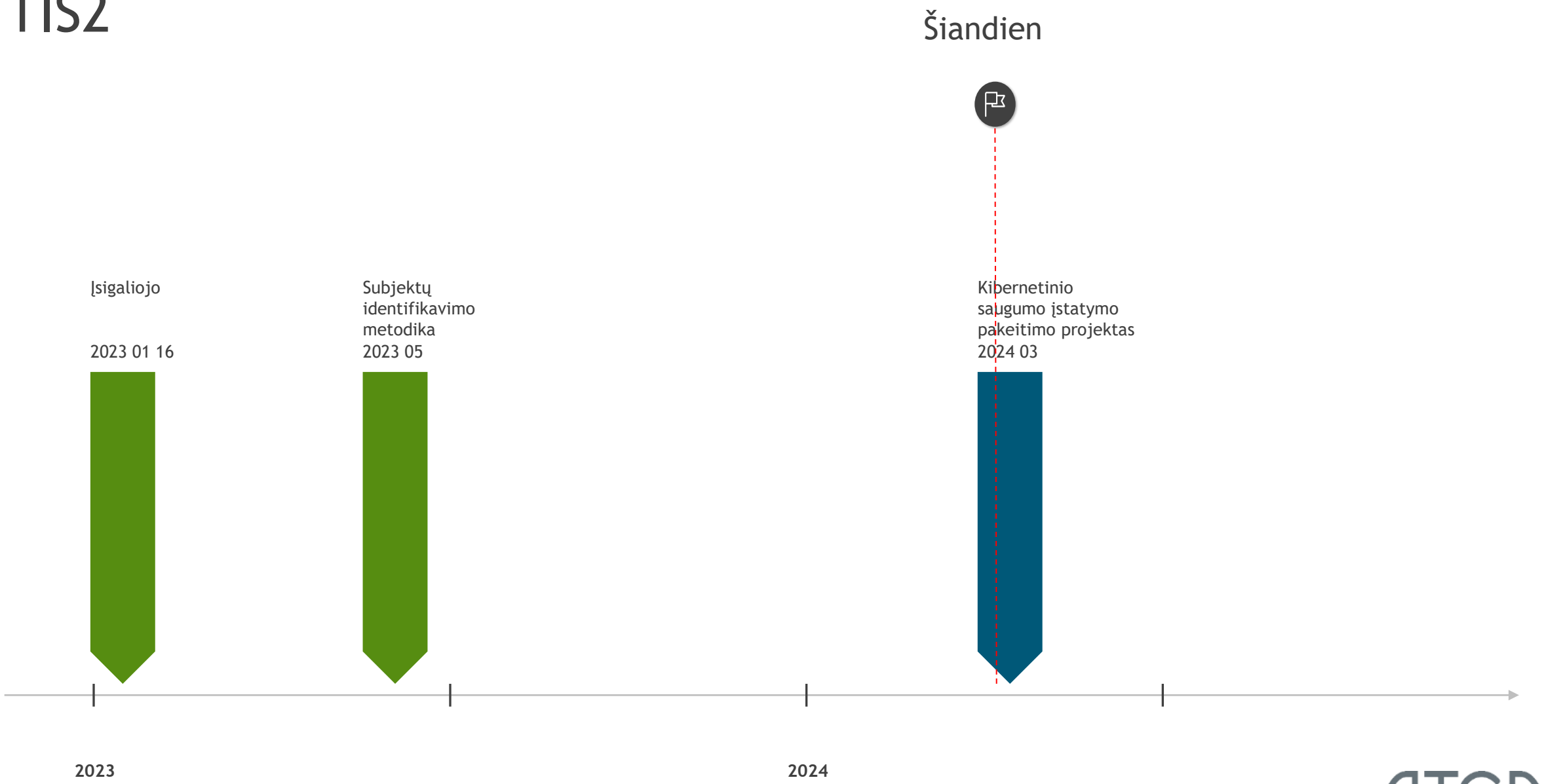
Šaltinis: Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf (nksc.lt)

TIS2 evoliucija

TIS2

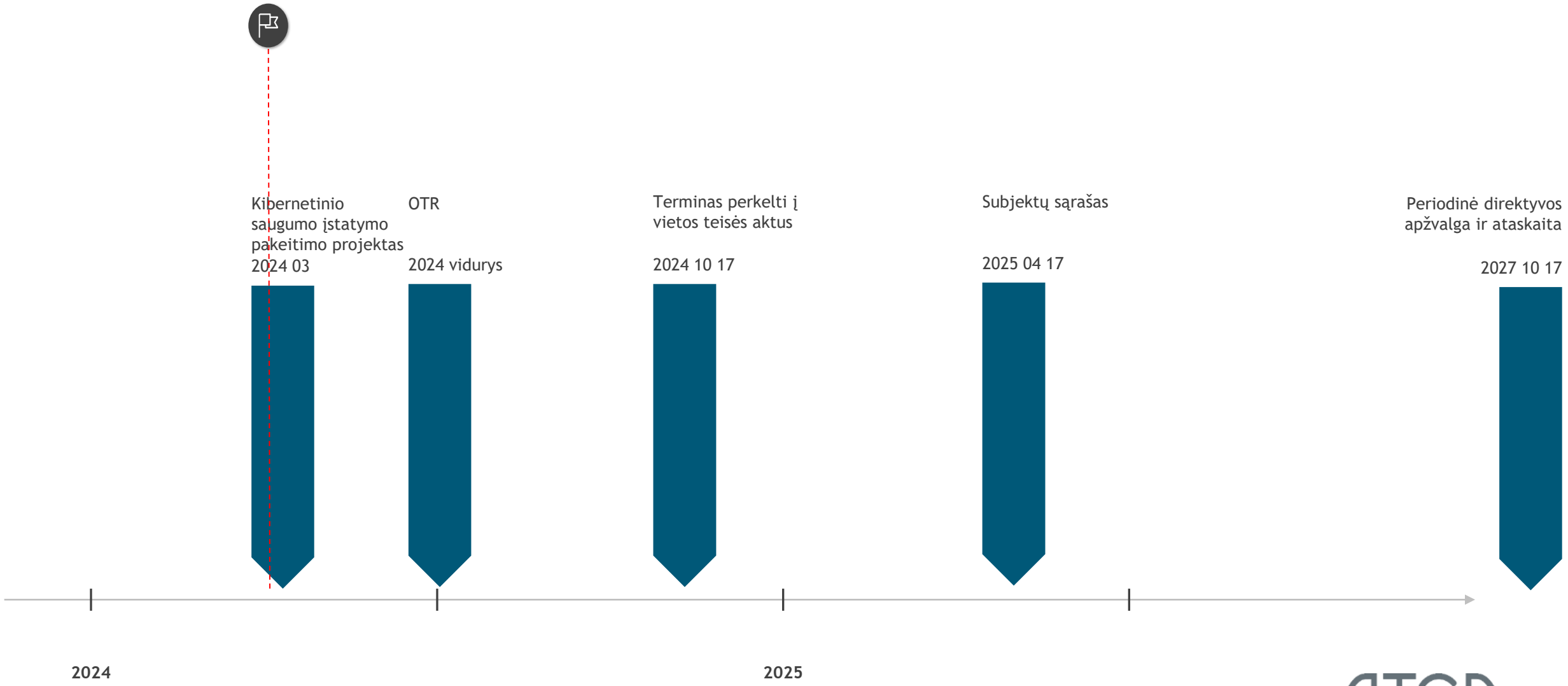


TIS2


Šiandien
Įsigaliojo
2023 01 16
Subjektų identifikavimo metodika
2023 05
Kibernetinio saugumo įstatymo pakeitimo projektas
2024 03
2023
2024

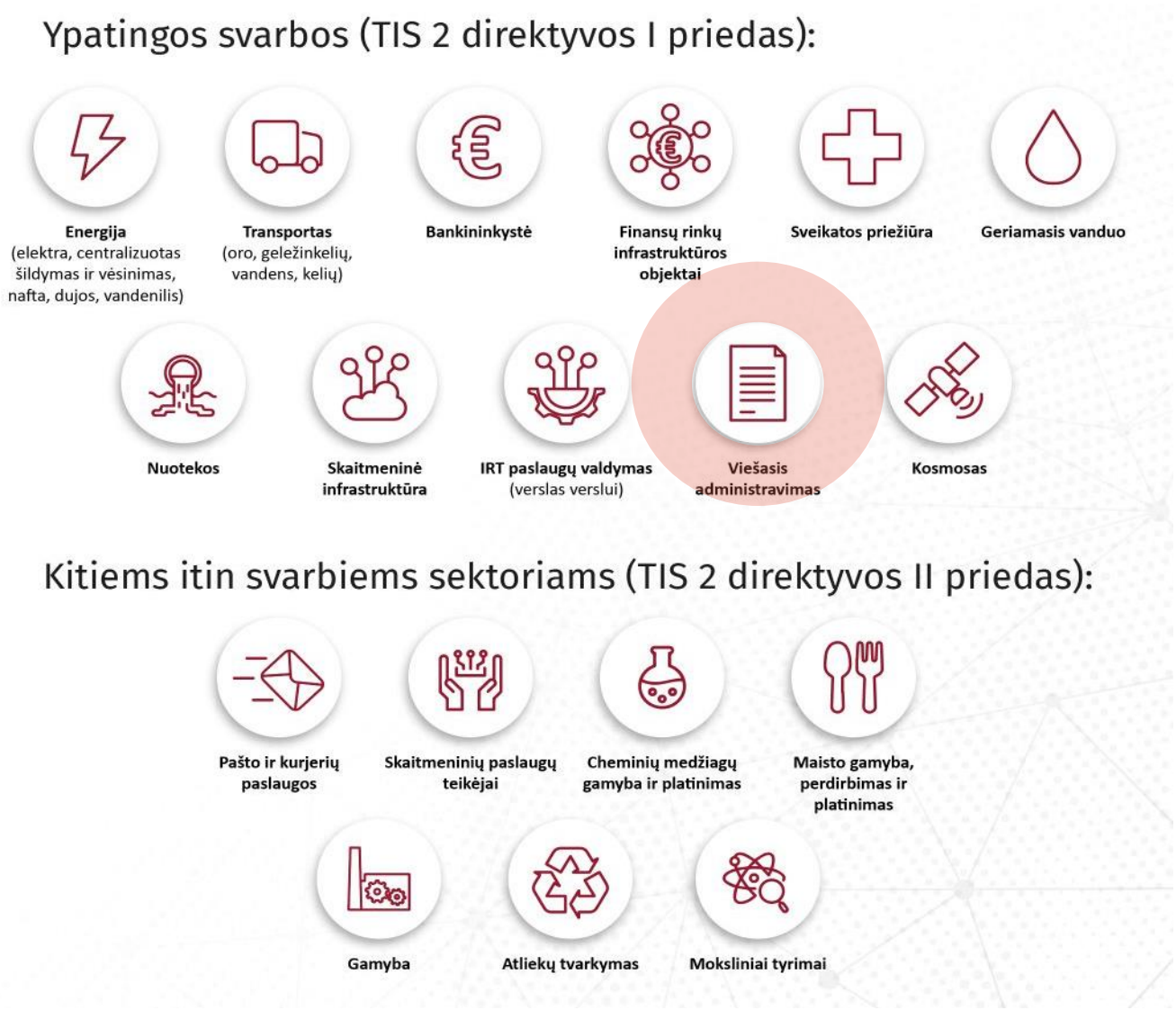
TIS2

Šiandien



TIS2 taikymo sritis

Sektoriai



Šaltinis: https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/

Sektoriai

Nepaisant subjektų **dydžio**, ši direktyva taip pat **taikoma** I ar II priede nurodytos rūšies subjektams, kai:

...

f) subjektas yra:

i) centrinės valdžios ... viešojo administravimo subjektas, arba

ii) regioninio lygmens ... viešojo administravimo subjektas.

Sektorius	Subsektorius	Atsakinga institucija	Subjekto rūšis	Jurisdikcija
I priedas: YPATINGOS SVARBOS SEKTORIAI				
10. Viešasis administravimas		VRM, Ministerijos	Centrinės valdžios viešojo administravimo subjektai (išskyrus nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas)	VN, kuri juos įsteigė
		VRM, Ministerijos	Regioninio lygmens viešojo administravimo subjektai | Viešojo administravimo subjektai vietos lygmeniu	

Šaltinis: https://kam.lt/wp-content/uploads/2023/05/NIS2_Identifikavimo-kriterijai.pdf

TIS2 reikalavimai

Priemonės

Kibernetinio saugumo rizikos valdymo priemonės turi apimti:

a. rizikos analizės ir informacinių sistemų saugumo politiką;
b. incidentų valdymą;
c. veiklos tęstinumą (pvz., Atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą);
d. tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;
e. tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;
f. politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;
g. pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus;
h. kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras;
i. žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;
j. kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.

Šaltinis: NIS2 direktyva, 21 straipsnis; *Publications Office (europa.eu)

ISO27001:2022

Organizacinius ir techninius kibernetinio saugumo reikalavimus (numatytus TIS2 direktyvos 21 str.), kurie bus tvirtinami Lietuvos Respublikos Vyriausybės nutarimu, planuojama grįsti tarptautiniu standartu ISO/IEC 27001:2022.

Šaltinis: https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/

Tiekimo grandinė

Esminių ir svarbių subjektų **tiekimo grandinėje** esantiems tiekėjams **bus taikomi** kibernetinio saugumo **reikalavimai**, pvz., bus reikalaujama sutartyse numatyti, kad **rangovai** laikytųsi perkančiosios organizacijos nustatytų informacijos saugumo bei kibernetinio saugumo reikalavimų **visą sutarties** vykdymo **laikotarpį**...

Šaltinis: https://kam.lt/duk_kategorijos/tis-2-direktyva/

Pareigos pranešti

... pateikiama ši informacija:

- **išsamus** incidento, įskaitant jo sunkumą ir poveikį, **aprašymas**;
- grėsmės arba pagrindinės **priežasties**, dėl kurios incidentas galėjo būti sukeltas, rūšis;
- taikomos ir įgyvendinamos poveikio mažinimo **priemonės**;
- ...

Šaltinis: L_2022333LT.01008001.xml (europa.eu)

Atsakomybė

Valstybės narės užtikrina, kad esminių ir svarbių subjektų **valdymo organai** patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis 21 straipsnio, prižiūrėtų jo įgyvendinimą ir galėtų būti **patraukti atsakomybėn** už tai, kad subjektai pažeidžia tą straipsnį.

Šaltinis: L_2022333LT.01008001.xml (europa.eu)

Baudos

- **Esminiams subjektams** 10 000 000 EUR arba 2 proc. (kuris didesnis)
- **Svarbiems subjektams** 7 000 000 EUR arba 1,4 proc. (kuris didesnis)

Kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos viešojo administravimo subjektams.

Šaltinis: *Publications Office (europa.eu)

Nuo ko pradėti?

Ką daryti, jau dabar?

- **Atlikti rizikų analizę** ir atsižvelgiant į gautus rezultatus, susidėlioti rizikų valdymo politiką ir nusimatyti priemones, tiek organizacines tiek ir technines, kuriomis tos rizikos bus valdomos.

- Pasirengti ir/ar atnaujinti **dokumentaciją,** tai, ko tikrai reikės ir nuo ko verta pradėti:
  - **IS saugumo politika**
  - **Veikos tęstinumo planas**
  - **Incidentų valdymo planas**
- **Planuoti** kibernetinio saugumo **priemonių diegimą** ir naudojimą atsižvelgianti į rizikų valdymo plane numatytas priemones.

Klausimai?

Turite klausimų apie TIS2 direktyvos taikymą Jūsų organizacijai ?

Susisiekime:

evaldas.valunas@atea.lt

+370 682 55171


Kuriame Lietuvą su IT
ATEA