EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NACIONALINIŲ PAJĖGUMŲ VERTINIMO SISTEMA

2020 M. GRUODŽIO MĖN.

APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra Sąjungos agentūra, kurios tikslas – pasiekti bendrą aukštą kibernetinio saugumo lygį visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įkurta 2004 m. ir sustiprinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų, kuriuose naudojamos kibernetinio saugumo sertifikavimo schemos, patikimumą, bendradarbiauja su valstybėmis narėmis ir ES įstaigomis ir padeda Europai pasirengti būsimiems kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra kartu su savo pagrindiniais suinteresuotaisiais subjektais siekia stiprinti pasitikėjimą susietąja ekonomika, didinti Sąjungos infrastruktūros atsparumą, užtikrinti Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos rasite svetainėje www.enisa.europa.eu.

KONTAKTINIAI DUOMENYS

Su dokumento rengėjais galima susisiekti adresu team@enisa.europa.eu.
Žiniasklaidos atstovų užklausas dėl šio dokumento galima teikti adresu press@enisa.europa.eu.

DOKUMENTO RENGĖJAI

Anna Sarri, Pinelopi Kyranoudi – Europos Sąjungos kibernetinio saugumo agentūra (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – „Wavestone“

PADĖKA

ENISA norėtų padėkoti visiems dalyvavusiems ekspertams, reikšmingai prisidėjusiems rengiant šią ataskaitą, visų pirma institucijoms ir asmenims, kurių sąrašas pateikiamas toliau:

Adrian-Ionut Bobeica iš Europos kovos su elektroniniu nusikalstamumu centro (EC3)

Alexandre Leite ir Pedro Matos iš Portugalijos nacionalinio kibernetinio saugumo centro

Alzofra Martinez Alvaro iš Europos kovos su elektroniniu nusikalstamumu centro (EC3)

Anna-Liisa Pärnalaas iš Estijos ekonomikos reikalų ir komunikacijos ministerijos

Belgijos kibernetinio saugumo centras

Carolin Weisser Harris iš Oksfordo universiteto Visuotinio kibernetinio saugumo gebėjimų centro

George Drivas, Nestor Chouliar, Evgenia Tsaprali ir Sotiris Vasilos iš Graikijos skaitmeninės politikos ministerijos

Italijos Vyriausybė

James Caffrey iš Airijos aplinkos, klimato ir komunikacijos departamento Kibernetinio saugumo politikos skyriaus

Katia Bonello ir Martin Camilleri iš Maltos informacinių technologijų agentūros

Maria Mar Lopez Gil iš Ispanijos nacionalinio saugumo departamento

Marin Ante Pivcevic iš Kroatijos centrinio valstybinio skaitmeninės visuomenės plėtros biuro

Marjan Kavčič iš Slovėnijos informacijos saugumo administracijos

NCTV, Nyderlandų teisingumo ir saugumo ministerija

Robin Bakke iš Norvegijos teisingumo ir visuomenės saugumo ministerijos

Sascha-Alexander Lettgen iš Vokietijos federalinės vidaus reikalų ministerijos

Slovakijos nacionalinio saugumo institucija

Thomas Wulff iš CFCS – Danijos kibernetinio saugumo centro (*Cybersikkerhed*)

Veronika Netolická iš Čekijos nacionalinės kibernetinio saugumo ir informacijos saugumo agentūros

ENISA taip pat norėtų padėkoti už vertingą indėlį į šį tyrimą visiems ekspertams, kurie pateikė savo nuomonę, tačiau pageidauja išlikti anonimiški.

TEISINIS PRANEŠIMAS

PRANEŠIMAS APIE AUTORIŲ TEISES

ISBN 978-92-9204-492-3

DOI 10.2824/588763

KATALOGAS TP-02-21-253-LT-N

1. TURINYS

SĄVOKŲ ŽODYNĖLIS

SANTRUMPA	APIBRĖŽTIS
BDAR	Bendrasis duomenų apsaugos reglamentas
BSR	Bendroji skaitmeninė rinka
C2M2	Kibernetinio saugumo pajėgumų brandos modelis
CCRA	Susitarimas dėl bendrųjų kriterijų pripažinimo
CCSMM	Bendruomenės kibernetinio saugumo brandos modelis
CII	Ypatingos svarbos informacinė infrastruktūra
CMM	Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis
CMMC	Kibernetinio saugumo brandos modelių sertifikavimas
CSIRT	Reagavimo į kompiuterinius saugumo incidentus tarnybos
DAA	Duomenų apsaugos aktas
DI	Dirbtinis intelektas
EKS	Europos kvalifikacijų sandara
EKSM	Europos kibernetinio saugumo mėnuo
EKSO	Europos kibernetinio saugumo organizacija
EKSSG	Europos kibernetinio saugumo sertifikavimo grupė
ELPA	Europos laisvosios prekybos asociacija
EPO	Esminių paslaugų operatoriai
ES	Europos Sąjunga
IA-CM	Viešojo sektoriaus vidaus audito pajėgumų modelis
IRT	Informacinės ir ryšių technologijos
ISMM	NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis
ITU	Tarptautinė telekomunikacijų sąjunga
KGI	Kibernetinės galios indeksas
MTTP	Moksliniai tyrimai ir technologinė plėtra
MVĮ	Mažosios ir vidutinės įmonės
NIST	Nacionalinis standartų ir technologijų institutas
NKSS	Nacionalinės kibernetinio saugumo strategijos

NRPP	Nacionaliniai ryšių palaikymo pareigūnai
OT	Operacijų technologija
PDT	Privatumo didinimo technologijos
PIVS	Privatumo informacijos valdymo sistema
Q-C2M2	Kataro kibernetinio saugumo pajėgumų brandos modelis
SOG-IS MRA	Vyresniųjų pareigūnų grupė informacinių sistemų saugumo klausimais, tarpusavio pripažinimo susitarimas
SPA	Suderintas pažeidžiamumų atskleidimas
TI	Teisėsaugos institucija
TIS	Tinklų ir informacijos saugumas
VKSI	Visuotinis kibernetinio saugumo indeksas
VN	Valstybė narė
VPSP	Viešojo ir privačiojo sektorių partnerystės
VST	Vyriausybės skaitmeninė tarnyba

SANTRAUKA

Kadangi dabartinė kibernetinių grėsmių aplinka ir toliau plečiasi, o kibernetinių išpuolių vis daugėja ir jie intensyvėja, ES valstybės narės turi veiksmingai reaguoti plėtodamos ir pritaikydamos savo nacionalines kibernetinio saugumo strategijas (NKSS). Nuo 2012 m., kai ENISA paskelbė pirmuosius su NKSS susijusius tyrimus, ES valstybės narės ir ELPA šalys padarė didelę pažangą rengdamos ir įgyvendindamos savo strategijas.

Šioje ataskaitoje pristatomas ENISA darbas, atliktas kuriant nacionalinių pajėgumų vertinimo sistemą (NPVS).

Sistema siekiama, kad valstybės narės, vertindamos savo NKSS tikslus, galėtų pačios įvertinti savo brandos lygį. Tai padės joms stiprinti kibernetinio saugumo pajėgumus tiek strateginiu, tiek veiklos lygmeniu.

Ataskaitoje pateikiamas paprastas valstybės narės kibernetinio saugumo brandos lygio vaizdas. NPVS yra priemonė, padedanti valstybėms narėms:

- teikti naudingą informaciją, kad būtų galima parengti ilgalaikę strategiją (pvz., geroji patirtis, gairės);
- padėti nustatyti trūkstamus NKSS elementus;
- padėti toliau stiprinti kibernetinio saugumo pajėgumus;
- remti atskaitomybę už politinius veiksmus;
- užtikrinti plačiosios visuomenės ir tarptautinių partnerių patikimumą;
- remti informavimo veiklą ir gerinti savo, kaip skaidrios organizacijos, įvaizdį visuomenėje;
- padėti numatyti būsimas problemas;
- padėti nustatyti įgytą patirtį ir gerąją patirtį;
- suteikti pagrindą diskusijoms apie kibernetinio saugumo gebėjimus visoje ES ir
- padėti įvertinti nacionalinius kibernetinio saugumo pajėgumus.

Sistema sukurta padedant šią temą išmanantiems ENISA ekspertams ir atstovams iš 19 valstybių narių bei ELPA šalių[1]. Šios ataskaitos tikslinė auditorija yra politikos formuotojai, ekspertai ir valstybės pareigūnai, atsakingi už NKSS kūrimą, įgyvendinimą ir vertinimą, o platesniu mastu – už kibernetinio saugumo pajėgumus, arba dalyvaujantys šiame procese.

[1] Apklausti atstovai iš šių valstybių narių ir ELPA šalių: Airijos, Belgijos, Čekijos, Danijos, Estijos, Graikijos, Ispanijos, Italijos, Kroatijos, Lichtenšteino, Maltos, Nyderlandų, Norvegijos, Portugalijos, Slovakijos, Slovėnijos, Švedijos, Vengrijos, Vokietijos.

Nacionalinių pajėgumų vertinimo sistema apima 17 strateginių tikslų, suskirstytų į keturias pagrindines grupes:

- 1 grupė. Kibernetinio saugumo valdymas ir standartai
  1. Parengti nacionalinį nenumatytų atvejų kibernetinėje erdvėje planą
  2. Nustatyti bazines apsaugos priemones
  3. Apsaugoti skaitmeninę tapatybę ir didinti pasitikėjimą skaitmeninėmis viešosiomis paslaugomis

- 2 grupė. Gebėjimų stiprinimas ir informuotumas
  4. Organizuoti kibernetinio saugumo pratybas
  5. Įtvirtinti reagavimo į incidentus pajėgumą
  6. Didinti naudotojų informuotumą
  7. Stiprinti mokymo ir švietimo programas
  8. Skatinti mokslinius tyrimus ir technologinę plėtrą
  9. Suteikti paskatų privačiajam sektoriui investuoti į apsaugos priemones
  10. Didinti tiekimo grandinės kibernetinį saugumą

- 3 grupė. Teisinės ir reguliavimo priemonės
  11. Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus
  12. Spręsti kibernetinių nusikaltimų problemą
  13. Nustatyti pranešimo apie incidentus mechanizmus
  14. Stiprinti privatumo ir duomenų apsaugą

- 4 grupė. Bendradarbiavimas
  15. Sukurti viešojo ir privačiojo sektorių partnerystę
  16. Įforminti viešųjų agentūrų bendradarbiavimą
  17. Dalyvauti tarptautiniame bendradarbiavime

1. ĮVADAS

2016 m. liepos mėn. paskelbtoje Tinklų ir informacijos saugumo (TIS) direktyvoje reikalaujama, kad ES valstybės narės priimtų nacionalinę tinklų ir informacinių sistemų saugumo strategiją, dar vadinamą nacionaline kibernetinio saugumo strategija (NKSS), kaip nustatyta 1 ir 7 straipsniuose. Šiomis aplinkybėmis NKSS apibrėžiama kaip sistema, kurioje nustatomi strateginiai principai, gairės, strateginiai tikslai, prioritetai, tinkamos politikos ir reguliavimo priemonės. Numatomas NKSS tikslas – pasiekti ir išlaikyti aukšto lygio tinklų ir informacinių sistemų saugumą, kad valstybės narės galėtų sušvelninti galimas grėsmes. Be to, NKSS gali būti pramonės plėtros ir ekonominės bei socialinės pažangos katalizatorius.

ES kibernetinio saugumo akte teigiama, kad ENISA skatina gerosios patirties, susijusios su NKSS apibrėžimu ir įgyvendinimu, sklaidą, remdama valstybes nares priimant TIS direktyvą ir rinkdama vertingą grįžtamąją informaciją apie jų patirtį. Šiuo tikslu ENISA parengė kelias priemones, kurių tikslas – padėti valstybėms narėms rengti, įgyvendinti ir vertinti savo nacionalines kibernetinio saugumo strategijas (NKSS).

Vykdydama savo įgaliojimus, ENISA siekia sukurti nacionalinių pajėgumų įsivertinimo sistemą, kad būtų galima įvertinti skirtingų NKSS brandos lygį. Šios ataskaitos tikslas – pristatyti tyrimą, atliktą apibrėžiant įsivertinimo sistemą.

1.1 TYRIMO APRĖPTIS IR TIKSLAI

Pagrindinis šio tyrimo tikslas – sukurti nacionalinių pajėgumų įsivertinimo sistemą (toliau – NPVS), kad būtų galima įvertinti valstybių narių kibernetinio saugumo pajėgumų brandos lygį. Kalbant konkrečiau, sistema turėtų įgalinti valstybes nares:

- atlikti savo nacionalinių kibernetinio saugumo pajėgumų vertinimą;
- didinti informuotumą apie šalies brandos lygį;
- nustatyti tobulintinas sritis;
- stiprinti kibernetinio saugumo pajėgumus.

Ši sistema turėtų padėti valstybėms narėms, visų pirma nacionalinės politikos formuotojams, vykdyti įsivertinimo procedūras, siekiant pagerinti nacionalinius kibernetinio saugumo pajėgumus.

1.2 METODIKA

Metodika, taikoma kuriant nacionalinių pajėgumų įsivertinimo sistemą, grindžiama keturiais pagrindiniais etapais:

1. **Dokumentų tyrimas.** Pirmasis etapas – išsami literatūros apžvalga, siekiant surinkti gerosios patirties pavyzdžius, susijusius su nacionalinių kibernetinio saugumo strategijų brandos vertinimo sistemos kūrimu. Atliekant dokumentų tyrimą daugiausia dėmesio skiriama sisteminei atitinkamų dokumentų dėl kibernetinio saugumo gebėjimų stiprinimo ir strategijos apibrėžimo analizei, esamų valstybių narių NKSS ir esamų kibernetinio saugumo brandos modelių palyginimui. Esamų brandos modelių lyginamoji analizė atlikta taikant šiam tyrimui parengtą analizės sistemą. Analizės sistema

grindžiama J. Beckerio[2] brandos modelių kūrimo metodika, kurioje pateikiamas bendras, suvestinis brandos modelių rengimo procedūrų modelis ir aiškūs brandos modelių kūrimo reikalavimai. Analizės sistema buvo pritaikyta šio tyrimo poreikiams.

2. **Ekspertų ir suinteresuotųjų subjektų nuomonių rinkimas.** Remiantis duomenimis, surinktais atliekant dokumentų tyrimą, ir susijusiomis preliminariomis analizės išvadomis, šiame etape nustatyti ir pakviesti į pokalbį atrinkti ekspertai, turintys patirties kuriant ir įgyvendinant NKSS arba brandos modelius. ENISA susisiekė su savo nacionalinių kibernetinio saugumo strategijų ekspertų grupe ir nacionaliniais ryšių palaikymo pareigūnais (NRPP), siekdama rasti tinkamų ekspertų kiekvienoje valstybėje narėje. Be to, apklausti keli ekspertai, dalyvaujantys kuriant brandos modelius. Iš viso surengti 22 pokalbiai, iš jų 19 – su įvairių valstybių narių (ir ELPA šalių) kibernetinio saugumo agentūrų atstovais.
3. **Apžvalgos duomenų analizė.** Vėliau buvo analizuojami duomenys, surinkti atliekant dokumentų tyrimą ir rengiant pokalbius, siekiant nustatyti, kaip geriausia kurti įsivertinimo sistemą NKSS brandai įvertinti, suprasti valstybių narių poreikius ir išsiaiškinti, kuriuos duomenis galima surinkti įvairiose Europos šalyse[3]. Ši analizė leido patikslinti ankstesniuose etapuose sukurtą preliminarų modelį ir patobulinti į modelį įtrauktų rodiklių rinkinį, brandos lygius ir jo matmenis.
4. **Modelio galutinis parengimas.** Vėliau šią temą išmanantys ENISA ekspertai peržiūrėjo atnaujintą nacionalinių pajėgumų įsivertinimo sistemos versiją. Dar vėliau, 2020 m. spalio mėn., prieš paskelbimą surengtame seminare sistemą patvirtino ekspertai.

1.3 TIKSLINĖ AUDITORIJA

Šios ataskaitos tikslinė auditorija yra politikos formuotojai, ekspertai ir vyriausybės pareigūnai, atsakingi už NKSS kūrimą, įgyvendinimą ir vertinimą, o platesniu mastu – už kibernetinio saugumo pajėgumus, arba dalyvaujantys šiame procese. Be to, šiame dokumente pateiktos išvados gali būti naudingos kibernetinio saugumo politikos ekspertams ir tyrėjams nacionaliniu arba Europos lygmeniu.

[2] Becker, J., Knackstedt, R., Pöppelbuß, J. Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering*, vol. 1, no. 3, p. 213–222, Jun. 2009.
[3] Kalbant apie šį tyrimą, ataskaitoje minimos Europos šalys yra 27 ES valstybės narės.

2. BENDROJI INFORMACIJA

2.1 ANKSTESNIS DARBAS, SUSIJĘS SU NKSS GYVAVIMO CIKLU

Kaip nurodyta ES kibernetinio saugumo akte, vienas pagrindinių ENISA tikslų yra remti valstybes nares joms rengiant nacionalines tinklų ir informacinių sistemų saugumo strategijas, skatinti tų strategijų sklaidą ir stebėti jų įgyvendinimą. Vykdydama savo įgaliojimus, ENISA parengė keletą dokumentų šiuo klausimu, siekdama skatinti dalytis gerąja praktika ir remti NKSS įgyvendinimą visoje ES:

- „NKSS kūrimo ir vykdymo etapų praktinis vadovas“[4], paskelbtas 2012 m.;
- „Nacionalinių pastangų stiprinti kibernetinės erdvės saugumą krypties nustatymas“[5], paskelbtas 2012 m.;
- pirmoji ENISA sistema, skirta valstybės narės NKSS vertinti[6], paskelbta 2014 m.;
- „Internetinis NKSS interaktyvusis žemėlapis“[7], paskelbtas 2014 m.;
- „NKSS gerosios patirties vadovas“[8], paskelbtas 2016 m.;
- „Nacionalinių kibernetinio saugumo strategijų vertinimo priemonė“[9], paskelbta 2018 m.;
- „Kibernetinio saugumo inovacijų taikymo geroji patirtis pagal NKSS“[10], paskelbtas 2019 m.

A PRIEDE trumpai apibendrinami pagrindiniai ENISA leidiniai šia tema.

Pirmiau minėti vadovai ir dokumentai buvo nagrinėjami atliekant dokumentų tyrimą. Pagrindinis NPVS elementas visų pirma yra nacionalinių kibernetinio saugumo strategijų vertinimo priemonė[11]. NPVS grindžiama tikslais, įtrauktais į NKSS internetinę vertinimo priemonę.

2.2 BENDRI TIKSLAI, NUSTATYTI EUROPOS NKSS

Dėl įvairių valstybių narių skirtumų sunku nustatyti bendrą veiklą ar veiksmų planus atsižvelgiant į skirtingas nacionalines aplinkybes, teisines sistemas ir politines darbotvarkes. Vis dėlto valstybių narių NKSS strateginiai tikslai dažnai susiję su tomis pačiomis temomis. Taigi,

[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), atnaujinta 2019 m.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Šiuo dokumentu atnaujinamas 2012 m. vadovas: 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

remiantis ankstesniu ENISA darbu ir valstybių narių NKSS analize, nustatyti 22 strateginiai tikslai. 15 iš šių strateginių tikslų jau buvo nustatyti ankstesniame ENISA darbe, 2 į šį tyrimą įtraukti naujai, o 5 nustatyti atsižvelgiant į būsimus aspektus.

2.2.1 Bendri valstybių narių strateginiai tikslai

Remiantis ankstesniu ENISA darbu, t. y. nacionalinių kibernetinio saugumo strategijų vertinimo priemone[12], toliau lentelėje pateikiamas pirmiau minėtas 15 strateginių tikslų, kurie paprastai įtraukiami į valstybių narių NKSS, rinkinys. Tikslais apibrėžiama bendros nacionalinės koncepcijos šioje srityje esmė. Daugiau informacijos apie toliau aprašytus tikslus rasite ENISA ataskaitoje „NKSS gerosios patirties vadovas“[13].

1 lentelė. Bendri valstybių narių NKSS strateginiai tikslai

Nr.	NKSS strateginiai tikslai	Uždaviniai
1	**Parengti nacionalinius nenumatytų atvejų kibernetinėje erdvėje planus**	▶ Pateikti ir paaiškinti kriterijus, kurie turėtų būti naudojami, kad padėtį būtų galima įvardyti kaip krizę. ▶ Apibrėžti pagrindinius krizės valdymo procesus ir veiksmus. ▶ Aiškiai apibrėžti įvairių suinteresuotųjų subjektų vaidmenis ir atsakomybę kibernetinės krizės metu. ▶ Pateikti ir paaiškinti kriterijus, pagal kuriuos krizę galima laikyti pasibaigusia, ir (arba) nustatyti, kas turi įgaliojimus tai skelbti.
2	**Nustatyti bazines apsaugos priemones**	▶ Suderinti skirtingą viešojo ir privačiojo sektorių organizacijų praktiką. ▶ Sukurti kompetentingų valdžios institucijų ir organizacijų bendrą kalbą ir atverti saugius ryšių kanalus. ▶ Sudaryti sąlygas įvairiems suinteresuotiesiems subjektams patikrinti ir palyginti savo kibernetinio saugumo pajėgumus. ▶ Dalytis informacija apie kibernetinio saugumo srities gerąją patirtį visuose pramonės sektoriuose. ▶ Padėti suinteresuotiesiems subjektams nustatyti savo investicijų į saugumą prioritetus.
3	**Organizuoti kibernetinio saugumo pratybas**	▶ Nustatyti, ką reikia išbandyti (planai ir procesai, žmonės, infrastruktūra, reagavimo pajėgumai, bendradarbiavimo pajėgumai, komunikacija ir kt.). ▶ Sudaryti nacionalinę kibernetinio saugumo pratybų planavimo grupę, kuriai būtų suteikti aiškūs įgaliojimai. ▶ Įtraukti kibernetinio saugumo pratybas į nacionalinės kibernetinio saugumo strategijos arba nacionalinio nenumatytų atvejų kibernetinėje erdvėje plano gyvavimo ciklą.
4	**Įtvirtinti reagavimo į incidentus pajėgumą**	▶ Įgaliojimai – tai galios, vaidmenys ir atsakomybė, kuriuos grupei turi suteikti atitinkama vyriausybė. ▶ Paslaugų portfelis – tai paslaugos, kurias grupė teikia suinteresuotiesiems subjektams arba naudoja savo vidaus veikimo tikslais. ▶ Veiklos pajėgumai – tai techniniai ir veiklos reikalavimai, kurių turi laikytis grupė. ▶ Bendradarbiavimo pajėgumai – tai reikalavimai, susiję su keitimusi informacija su kitomis grupėmis, kurios nepatenka į ankstesnes tris kategorijas, pvz., politikos formuotojais, kariniais subjektais, reguliavimo institucijomis, (ypatingos svarbos informacinės infrastruktūros) operatoriais, teisėsaugos institucijomis.

[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] Šiuo dokumentu atnaujinamas 2012 m. vadovas: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Nr.	NKSS strateginiai tikslai	Uždaviniai
5	Didinti naudotojų informuotumą	▶ Nustatyti žinių apie kibernetinį saugumą arba informacijos saugumo problemas spragas. ▶ Užpildyti spragas didinant informuotumą arba plėtojant ir (arba) stiprinant žinių pagrindus.
6	Stiprinti mokymo ir švietimo programas	▶ Stiprinti esamų informacijos saugumo srities darbuotojų veiklos pajėgumus. ▶ Skatinti besimokančiuosius prisijungti ir rengti juos dalyvauti kibernetinio saugumo srities veikloje. ▶ Propaguoti ir skatinti informacijos saugumo srities akademinės aplinkos ir informacijos saugumo pramonės ryšius. ▶ Mokymą apie kibernetinį saugumą derinti su verslo poreikiais.
7	Skatinti mokslinius tyrimus ir technologinę plėtrą	▶ Nustatyti tikrąsias pažeidžiamumų priežastis, užuot šalinus jų poveikį. ▶ Suburti įvairių sričių mokslininkus, siekiant rasti daugialypių ir sudėtingų problemų, pvz., fizinių ir kibernetinių grėsmių, sprendimus. ▶ Susieti pramonės poreikius ir mokslinių tyrimų rezultatus ir taip palengvinti perėjimą nuo teorijos prie praktikos. ▶ Rasti būdų ne tik išlaikyti, bet ir padidinti produktų ir paslaugų, kuriais remiama esama kibernetinė infrastruktūra, kibernetinio saugumo lygį.
8	Suteikti paskatų privačiajam sektoriui investuoti į apsaugos priemones	▶ Nustatyti galimas paskatas privačioms įmonėms investuoti į apsaugos priemones. ▶ Suteikti paskatų įmonėms, siekiant paraginti jas investuoti į saugumą.
9	Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus	▶ Nustatyti ypatingos svarbos informacinę infrastruktūrą ▶ Nustatyti ir sušvelninti ypatingos svarbos informacinei infrastruktūrai kylančią atitinkamą riziką.
10	Spręsti kibernetinių nusikaltimų problemą	▶ Rengti kibernetinių nusikaltimų srities teisės aktus ▶ Didinti teisėsaugos institucijų veiksmingumą.
11	Nustatyti pranešimo apie incidentus mechanizmus	▶ Įgyti žinių apie bendrą grėsmių aplinką. ▶ Įvertinti incidentų (pvz., saugumo pažeidimų, tinklo gedimų, paslaugų teikimo pertrūkių) poveikį. ▶ Įgyti žinių apie esamas ir naujas silpnąsias vietas ir išpuolių rūšis. ▶ Atitinkamai atnaujinti apsaugos priemones. ▶ Įgyvendinti TIS direktyvos nuostatas dėl pranešimų apie incidentus.
12	Stiprinti privatumo ir duomenų apsaugą	▶ Padėti stiprinti pagrindines teises į privatumą ir duomenų apsaugą.
13	Sukurti viešojo ir privačiojo sektorių partnerystę (VPSP)	▶ Atgrasymas (atgrasomi išpuolių vykdytojai). ▶ Apsauga (naudojami naujų grėsmių saugumui moksliniai tyrimai). ▶ Nustatymas (dalijamasi informacija, siekiant kovoti su naujomis grėsmėmis). ▶ Reagavimas (pajėgumas susidoroti su pradiniu incidento poveikiu). ▶ Atkūrimas (pajėgumas ištaisyti galutinį incidento poveikį).
14	Įforminti viešųjų agentūrų bendradarbiavimą	▶ Stiprinti viešųjų agentūrų, turinčių su kibernetiniu saugumu susijusių pareigų ir kompetencijos, bendradarbiavimą. ▶ Vengti viešųjų agentūrų kompetencijos ir išteklių dubliavimosi. ▶ Gerinti ir įforminti viešųjų agentūrų bendradarbiavimą įvairiose kibernetinio saugumo srityse
15	Dalyvauti tarptautiniame bendradarbiavime (ne tik su ES valstybėmis narėmis)	▶ Sukurti bendrą ES valstybių narių žinių bazę. ▶ Užtikrinti nacionalinių kibernetinio saugumo institucijų sąveikos poveikį. ▶ Sudaryti sąlygas kovai su tarpvalstybiniu nusikalstamumu ir ją stiprinti.

2.2.2 Papildomi strateginiai tikslai

Remiantis ENISA atliktu dokumentų tyrimu ir pokalbiais, nustatyti papildomi strateginiai tikslai. Valstybės narės vis dažniau sprendžia šiuos klausimus savo NKSS arba rengia veiksmų planus ta pačia tema. Taip pat pateikiami valstybių narių vykdomos veiklos pavyzdžiai. Jei pavyzdys pateiktas iš viešai prieinamo šaltinio, pateikiama nuoroda. Tais atvejais, kai pavyzdžiai grindžiami konfidencialiais pokalbiais su ES valstybių narių pareigūnais, nuorodų nepateikiama.

Nustatyti šie papildomi strateginiai tikslai:

- didinti tiekimo grandinės kibernetinį saugumą;
- apsaugoti skaitmeninę tapatybę ir didinti pasitikėjimą skaitmeninėmis viešosiomis paslaugomis.

Tiekimo grandinės kibernetinio saugumo didinimas

Europos ekonomikos pagrindas yra mažosios ir vidutinės įmonės (MVĮ). Jos sudaro 99 proc. visų ES įmonių[14]. 2015 m. apskaičiuota, kad MVĮ sukūrė apie 85 proc. naujų darbo vietų ir du trečdalius visų ES privačiojo sektoriaus darbo vietų. Be to, MVĮ teikia paslaugas didelėms įmonėms ir vis dažniau bendradarbiauja su viešojo administravimo institucijomis[15], todėl reikia pažymėti, kad dabartinėmis tarpusavyje susijusiomis aplinkybėmis MVĮ yra silpna kibernetinių išpuolių grandis. Iš tiesų MVĮ patiria didžiausią kibernetinių išpuolių poveikį, tačiau dažnai jos negali sau leisti tinkamai investuoti į kibernetinį saugumą[16]. Todėl tiekimo grandinės kibernetinis saugumas turėtų būti didinamas daugiausia dėmesio skiriant MVĮ.

Be šio sisteminio požiūrio, valstybės narės taip pat gali sustiprinti pastangas, susijusias su konkrečių IRT paslaugų ir produktų, kurie laikomi esminiais, kibernetiniu saugumu: ypatingos svarbos informacinės infrastruktūros IRT technologijomis, telekomunikacijų sektoriuje taikomais saugumo mechanizmais (kontrolės priemonėmis interneto paslaugų teikėjų lygmeniu ir pan.), patikimumo užtikrinimo paslaugomis, kaip apibrėžta eIDAS reglamente, ir debesijos paslaugų teikėjais. Pavyzdžiui, Lenkija 2019–2024 m. nacionalinėje kibernetinio saugumo strategijoje[17] įsipareigojo sukurti nacionalinę kibernetinio saugumo vertinimo ir sertifikavimo sistemą kaip kokybės užtikrinimo tiekimo grandinėje mechanizmą. Ši sertifikavimo sistema bus suderinta su ES IRT skaitmeninių produktų, paslaugų ir procesų sertifikavimo sistema, nustatyta ES kibernetinio saugumo aktu (Reglamentas 2019/881).

Taigi, didinti tiekimo grandinės kibernetinį saugumą labai svarbu. Tai galima pasiekti nustatant tvirtą MVĮ skatinimo politiką, teikiant gaires dėl kibernetinio saugumo reikalavimų viešojo administravimo srities viešųjų pirkimų procedūrose, skatinant bendradarbiavimą privačiajame sektoriuje, kuriant viešojo ir privačiojo sektorių partnerystes, skatinant suderinto pažeidžiamumų atskleidimo (SPA) mechanizmus[18], kuriant produktų sertifikavimo sistemą, įskaitant kibernetinio saugumo elementus MVĮ skirtose skaitmeninėse iniciatyvose, ir, be kita ko, finansuojant įgūdžių ugdymą.

Skaitmeninės tapatybės apsaugojimas ir pasitikėjimo skaitmeninėmis viešosiomis paslaugomis didinimas

2020 m. vasario mėn. Komisija išdėstė savo ES skaitmeninės transformacijos viziją komunikate „Europos skaitmeninės ateities formavimas“[19], kad būtų kuriamos tokios įtraukiosios

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[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] Europos skaitmeninės ateities formavimas, COM(2020) 67 *final:* https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0067&qid=1612073418779&from=LT

technologijos, kurios būtų naudingos žmonėms ir atitinkančios pagrindines ES vertybes. Visų pirma komunikate teigiama, kad labai svarbu skatinti skaitmeninę viešojo administravimo institucijų transformaciją visoje Europoje. Šiuo požiūriu itin svarbu didinti pasitikėjimą vyriausybe, kiek tai susiję su skaitmenine tapatybe, ir viešosiomis paslaugomis. Tai dar svarbiau atsižvelgiant į tai, kad viešojo sektoriaus sandoriai ir keitimasis duomenimis dažnai yra slapto pobūdžio.

Nemažai šalių pareiškė ketinančios spręsti šią problemą savo NKSS, kaip antai Danija, Estija, Ispanija, Jungtinė Karalystė, Liuksemburgas, Malta, Nyderlandai ir Prancūzija. Kai kurios iš šių šalių taip pat pareiškė, kad šis strateginis tikslas galėtų būti įtrauktas į platesnio masto planą:

- Estija atitinkamą savo veiksmų planą „Elektroninės tapatybės saugumas ir elektroninio tapatumo nustatymo pajėgumas“ sieja su platesnio masto 2020 m. Estijos skaitmenine darbotvarke.
- Prancūzijos NKSS nurodyta, kad už skaitmenines technologijas atsakingas valstybės sekretorius prižiūri, kaip rengiamos veiksmų gairės „Prancūzijos žmonių skaitmeninio gyvenimo, privatumo ir asmens duomenų apsaugai užtikrinti“.
- Nyderlandų NKSS teigiama, kad kibernetinis saugumas viešojo administravimo institucijose, taip pat piliečiams ir įmonėms teikiamos viešosios paslaugos išsamiau aptariami bendrojoje skaitmeninės valdžios darbotvarkėje.
- Kadangi Jungtinės Karalystės vyriausybė vis daugiau savo paslaugų teikia internetu, ji įsteigė Vyriausybės skaitmeninę tarnybą (VST), kuri, Jungtinės Karalystės nacionalinio kibernetinio saugumo centro (NKSC) padedama, turi užtikrinti, kad visos vyriausybės sukurtos ar įsigytos naujos skaitmeninės paslaugos taip pat būtų saugios.

2.2.3 Kiti svarstyti strateginiai tikslai

Dokumentų tyrimo etape ir ENISA rengiamuose pokalbiuose buvo nagrinėjami ir kiti strateginiai tikslai. Vis dėlto nuspręsta, kad šie tikslai nebus įtraukti į įsivertinimo sistemą. C PRIEDAS. Kiti nagrinėti tikslai

pateikiamas kiekvieno iš tikslų, kurie gali būti naudojami būsimoms diskusijoms dėl galimų NKSS patobulinimų, apibūdinimas.

Ateityje bus svarstomi šie strateginiai tikslai:

- Parengti konkretiems sektoriams skirtas kibernetinio saugumo strategijas.
- Kovoti su dezinformacijos kampanijomis.
- Saugios pažangiosios technologijos (5G, dirbtinis intelektas, kvantinė kompiuterija ir kt.).
- Užtikrinti duomenų suverenumą.
- Teikti paskatas plėtoti kibernetinių rizikų draudimo sektorių.

2.3 PAGRINDINĖS LYGINAMOSIOS ANALIZĖS IŠVADOS

Siekiant surinkti informaciją ir įrodymus, kuriais būtų galima pagrįsti nacionalinių pajėgumų įsivertinimo sistemos NKSS srityje kūrimą, buvo vykdomas esamų brandos modelių, susijusių su kibernetiniu saugumu, dokumentų tyrimas. Atlikta išsami esamų modelių literatūros apžvalga, siekiant papildyti kibernetinio saugumo brandos modelių ir esamų NKSS, aprašytų 2.1 ir 2.2 skirsniuose, taikymo srities tyrimo išvadas. Ši sisteminė apžvalga padeda pasirinkti ir pagrįsti vertinimo sistemos brandos lygius ir apibrėžti skirtingus matmenis bei rodiklius.

Rengiant brandos modelių sisteminę apžvalgą apsvarstyta ir išnagrinėta 10 modelių, remiantis jų pagrindiniais požymiais. Bendra pagrindinių kiekvieno modelio, kuris apžvelgiamas šiame

tyrime, požymių apžvalga pateikiama 2 lentelėje. Nagrinėtų brandos modelių apžvalga, o išsamesnę analizę galima rasti A PRIEDE.

2 lentelė. Nagrinėtų brandos modelių apžvalga

Modelio pavadinimas	Brandos lygių skaičius	Požymių skaičius	Vertinimo metodas	Rezultatų pateikimas
Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis (CMM)	5	5 pagrindiniai matmenys	Bendradarbiavimas su vietos organizacija siekiant patobulinti modelį prieš jį taikant nacionaliniu lygmeniu	5 dalių radaras
Kibernetinio saugumo pajėgumų brandos modelis (C2M2)	4	10 pagrindinių sričių	Įsivertinimo metodika ir priemonių rinkinys	Rezultatų lentelė su skritulinėmis diagramomis
Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistema	Netaikoma (4 pakopos)	5 pagrindinės funkcijos	Įsivertinimas	Netaikoma
Kataro kibernetinio saugumo pajėgumų brandos modelis (Q-C2M2)	5	5 pagrindinės sritys	Netaikoma	Netaikoma
Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)	5	17 pagrindinių sričių	Trečiųjų šalių auditorių atliekamas vertinimas	Netaikoma
Bendruomenės kibernetinio saugumo brandos modelis (CCSMM)	5	6 pagrindiniai matmenys	Vertinimas bendruomenėse, dalyvaujant valstybinėms ir federalinėms teisėsaugos institucijoms	Netaikoma
NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis (ISMM)	5	23 vertinamos sritys	Netaikoma	Netaikoma
Viešojo sektoriaus vidaus audito pajėgumų modelis (IA-CM)	5	6 elementai	Įsivertinimas	Netaikoma
Visuotinis kibernetinio saugumo indeksas (VKSI)	Netaikoma	5 ramsčiai	Įsivertinimas	Reitingų lentelė
Kibernetinės galios indeksas (KGI)	Netaikoma	4 kategorijos	„Economist Intelligence Unit“ atliekama lyginamoji analizė	Reitingų lentelė

Ši sisteminė apžvalga leido padaryti išvadas apie esamų modelių taikymo gerąją patirtį ir paremti dabartinio brandos modelio koncepcijos kūrimą. Visų pirma, lyginamoji analizė padėjo apibrėžti brandos lygius, sukurti matmenų grupes ir pasirinkti rodiklius, taip pat tinkamą modelio rezultatų pateikimo metodiką. Svarbiausios išvados apie kiekvieną iš šių elementų išsamiai išdėstytos 3 lentelėje.

3 lentelė. Pagrindinės lyginamosios analizės išvados

Požymis	Pagrindinės išvados
Brandos lygiai	▶ Kibernetinio saugumo pajėgumų vertinimo sistemų penkių lygių brandos skalė yra visuotinai priimta ir ją taikant galima pateikti išsamius vertinimo rezultatus (išsamią kiekvieno modelio brandos lygių apibrėžtį žr. 6 lentelę. Brandos lygių palyginimas). ▶ Visuose modeliuose pateikiama kiekvieno brandos lygio aukšto lygio apibrėžtis, vėliau pritaikoma skirtingiems matmenims ar matmenų grupėms. ▶ Vertinant kibernetinio saugumo pajėgumų brandą paprastai vertinami du pagrindiniai aspektai: strategijų ir strategijų įgyvendinimo procesų branda.
Požymiai	▶ Iš esamų brandos modelių požymių lyginamosios analizės matyti, kad rezultatai nevienodi, o vidutinis kiekvieno modelio požymių skaičius – nuo keturių iki penkių. ▶ Modelis, grindžiamas maždaug keturiais arba penkiais požymiais, suteikia šalims tinkamo išsamumo lygio duomenis sugrupuojant atitinkamus matmenis ir užtikrinant rezultatų aiškumą (kiekvieno modelio požymių aprašymą žr. 7 lentelėje. Požymių ir (arba) **matmenų** palyginimas). ▶ Pagrindinis principas, taikomas visuose modeliuose apibrėžiant grupes, grindžiamas kiekvienoje grupėje esančių elementų nuoseklumu.
Vertinimo metodas	▶ Įvairiuose nagrinėjamuose modeliuose taikomi skirtingi vertinimo metodai. ▶ Dažniausias vertinimo metodas grindžiamas įsivertinimu.
Rezultatų pateikimas	▶ Rezultatus svarbu pateikti skirtingais išsamumo lygiais. ▶ Vaizdavimo metodas turėtų būti savaime aiškus ir lengvai skaitomas.

Koncepcija buvo grindžiama lyginamąja įvairių brandos modelių analize ir ankstesniu ENISA darbu. Be to, nuspręsta naudojantis *ENISA internetine interaktyviąja priemone* parengti kiekvienam požymiui naudojamus brandos rodiklius.

2.4 NKSS VERTINIMO SUNKUMAI

Valstybės narės, stiprindamos kibernetinio saugumo pajėgumus, o ypač siekdamos užtikrinti, kad jų pajėgumai atitiktų naujausias aplinkybes, susiduria su daugybe sunkumų. Toliau pateikiama šiame tyrime valstybių narių nustatytų ir su jomis aptartų sunkumų santrauka.

- **Koordinavimo ir bendradarbiavimo sunkumai.** Su kibernetiniu saugumu susijusių pastangų koordinavimas nacionaliniu lygmeniu, siekiant efektyviai reaguoti į kibernetinio saugumo problemas, gali kelti sunkumų, nes šiame procese dalyvauja daug suinteresuotųjų subjektų.
- **Nepakankami ištekliai vertinimui atlikti.** Atsižvelgiant į vietos aplinkybes ir kibernetinio saugumo nacionalinę valdymo struktūrą, NKSS ir jos tikslų vertinimas gali užtrukti iki 15 asmens darbo dienų.
- **Nepakankama parama kibernetinio saugumo pajėgumams plėtoti.** Kai kurios valstybės narės pritarė, kad, siekdamos apsaugoti biudžetą ir gauti paramą kibernetinio saugumo pajėgumams plėtoti, jos pirmiausia turėtų užbaigti vertinimo etapą, kuriame būtų nustatytos spragos ir trūkumai.
- **Sunkumai, susiję su strategijos pasiekimų ar pakeitimų priskyrimu.** Kasdien kintant grėsmėms ir tobulėjant technologijoms, veiksmų planus reikia nuolat koreguoti. Vis dėlto įvertinti NKSS ir priskirti pačios strategijos pakeitimus tebėra sunki užduotis. Tai savo ruožtu sunkina NKSS ribotumų ir trūkumų nustatymą.
- **NKSS veiksmingumo vertinimo sunkumai.** Siekiant įvertinti įvairias sritis, pvz., pažangą, įgyvendinimą, brandą ir veiksmingumą, galima kaupti metriką. Nors vertinti pažangą ir įgyvendinimą gana lengva, palyginti su veiksmingumo vertinimu, pastarasis tebėra prasmingesnis vertinant NKSS rezultatus ir poveikį. Remdamosi ENISA

surengtais pokalbiais, daugelis valstybių narių pareiškė, kad svarbu kiekybiškai įvertinti NKSS veiksmingumą, tačiau tai labai sudėtinga, kai kuriais atvejais kažin ar įmanoma užduotis.

- **Nelengva nustatyti bendrą sistemą.** ES valstybės narės veikia skirtingomis politikos, organizacijų, kultūros, visuomenės struktūros ir NKSS brandos aplinkybėmis. Kai kurios valstybės narės, apklaustos atliekant šį tyrimą, pareiškė, kad gali būti sunku apginti ir taikyti vieną visiems tinkančią įsivertinimo sistemą.

2.5 NACIONALINIŲ PAJĖGUMŲ VERTINIMO PRIVALUMAI

Nuo 2017 m. NKSS turi visos ES valstybės narės[20]. Nors tai ir teigiamas pokytis, taip pat svarbu, kad valstybės narės galėtų tinkamai įvertinti šias NKSS ir taip suteikti pridėtinės vertės savo strateginiam planavimui ir įgyvendinimui.

Vienas iš nacionalinių pajėgumų vertinimo sistemos tikslų – įvertinti kibernetinio saugumo pajėgumus remiantis įvairiose NKSS nustatytais prioritetais. Iš esmės taikant sistemą vertinamas valstybių narių kibernetinio saugumo pajėgumų NKSS tiksluose apibrėžtose srityse brandos lygis. Taigi šios sistemos rezultatai padeda valstybių narių politikos formuotojams parengti nacionalinę kibernetinio saugumo strategiją, suteikdami jiems informacijos apie esamą padėtį šalyje[21]. Galiausiai NPVS skirta padėti valstybėms narėms nustatyti tobulintinas sritis ir stiprinti pajėgumus.

Sistema siekiama, kad valstybės narės, vertindamos savo NKSS tikslus, galėtų pačios įvertinti savo brandos lygį – tai padės joms stiprinti kibernetinio saugumo pajėgumus tiek strateginiu, tiek veiklos lygmeniu.

Taikant praktiškesnį požiūrį, remiantis ENISA pokalbiais su keliomis agentūromis, atsakingomis už kibernetinio saugumo sritį skirtingose valstybėse narėse, nustatyti ir pabrėžti šie nacionalinių pajėgumų vertinimo sistemos privalumai:

- suteikia naudingos informacijos ilgalaikei strategijai rengti (pvz., geroji patirtis, gairės);
- padeda nustatyti trūkstamus NKSS elementus;
- padeda toliau stiprinti kibernetinio saugumo pajėgumus;
- padeda užtikrinti atskaitomybę už politinius veiksmus;
- ugdo plačiosios visuomenės ir tarptautinių partnerių pasitikėjimą;
- remia informavimo veiklą ir gerina skaidrios organizacijos įvaizdį visuomenėje;
- padeda numatyti būsimas problemas;
- padeda nustatyti įgytą ir gerąją patirtį;
- suteikti pagrindą diskusijoms apie kibernetinio saugumo gebėjimus visoje ES ir
- padeda įvertinti nacionalinius kibernetinio saugumo pajėgumus.

[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), p. 468–486.

3. NACIONALINIŲ PAJĖGUMŲ VERTINIMO SISTEMOS METODIKA

3.1 BENDRASIS TIKSLAS

NPVS **pagrindinis tikslas** – įvertinti **valstybių narių** kibernetinio saugumo pajėgumų brandos lygį, siekiant padėti joms atlikti savo nacionalinių kibernetinio saugumo pajėgumų vertinimą, didinti informuotumą apie šalies brandos lygį, nustatyti tobulintinas sritis ir stiprinti kibernetinio saugumo pajėgumus.

3.2 BRANDOS LYGIAI

Sistema grindžiama **penkiais brandos lygiais**, kuriais apibrėžiami valstybių narių kibernetinio saugumo pajėgumų stiprinimo etapai kiekvieno NKSS tikslo aprėpiamoje srityje. Kiekvienas lygis atspindi vis aukštesnį brandos lygį, pradedant pradiniu – **1 lygiu**, kai valstybės narės neturi aiškiai apibrėžto kibernetinio saugumo gebėjimų stiprinimo metodo NKSS tikslų apimamose srityse, ir baigiant **5 lygiu**, kai kibernetinio saugumo gebėjimų stiprinimo strategija yra dinamiška ir pritaikoma prie kintančių aplinkybių. 4 lentelėje pateikiama brandos lygių skalė, kurioje apibūdinamas kiekvienas brandos lygis.

4 lentelė. ENISA nacionalinių pajėgumų vertinimo sistemos penkių lygių brandos skalė

1 LYGIS. PRADINIS / *AD HOC*	2 LYGIS. PIRMINIS APIBRĖŽIMAS	3 LYGIS. ĮTVIRTINIMAS	4 LYGIS. OPTIMIZAVIMAS	5 LYGIS. PRITAIKOMUMAS
Valstybė narė neturi aiškiai apibrėžto kibernetinio saugumo gebėjimų stiprinimo metodo NKSS tikslų apimamose srityse. Nepaisant to, šalyje gali būti nustatyti kai kurie bendrieji tikslai ir atlikti tam tikri tyrimai (techniniai, politiniai, politikos), kad būtų pagerinti nacionaliniai pajėgumai.	Nustatytas nacionalinis gebėjimų stiprinimo metodas NKSS tikslų apimamoje srityje. Veiksmų planai arba veikla, kuriais siekiama rezultatų, yra parengti, bet tik pirminio etapo. Be to, galbūt nustatyti ir (arba) įtraukti aktyvūs suinteresuotieji subjektai.	NKSS tikslų apimamoje srityje gebėjimų stiprinimo veiksmų planas yra aiškiai apibrėžtas ir remiamas susijusių suinteresuotųjų subjektų. Praktikos ir veiklos vykdymas užtikrinamas ir vienodai įgyvendinamas nacionaliniu lygmeniu. Veikla apibrėžta ir dokumentuojama, ištekliai aiškiai paskirstyti, valdymas užtikrinamas ir terminai nustatyti.	Veiksmų planas reguliariai vertinamas: nustatyti prioritetai, planas optimalus ir tvarus. Reguliariai vertinami kibernetinio saugumo gebėjimų stiprinimo rezultatai. Veiklos įgyvendinimo sėkmės veiksniai, uždaviniai ir spragos nustatyti.	Kibernetinio saugumo gebėjimų stiprinimo strategija yra dinamiška ir pritaikoma. Nuolatinis dėmesys aplinkos pokyčiams (technologiniams pokyčiams, pasauliniams konfliktams, naujoms grėsmėms ir kt.) skatina greito sprendimų priėmimo pajėgumus ir gebėjimą imtis skubių veiksmų, kad padėtis pagerėtų.

3.3 GRUPĖS IR VISA APIMANTI ĮSIVERTINIMO SISTEMOS STRUKTŪRA

Įsivertinimo sistemai būdingos **keturios grupės**: I) kibernetinio saugumo valdymas ir standartai; II) gebėjimų stiprinimas ir informuotumas; III) teisinės ir reguliavimo priemonės; IV)

bendradarbiavimas. Kiekviena iš šių grupių apima pagrindinę teminę sritį, susijusią su šalies kibernetinio saugumo pajėgumų stiprinimu, ir įvairius tikslus, kuriuos valstybės narės gali įtraukti į savo NKSS. Būtent:

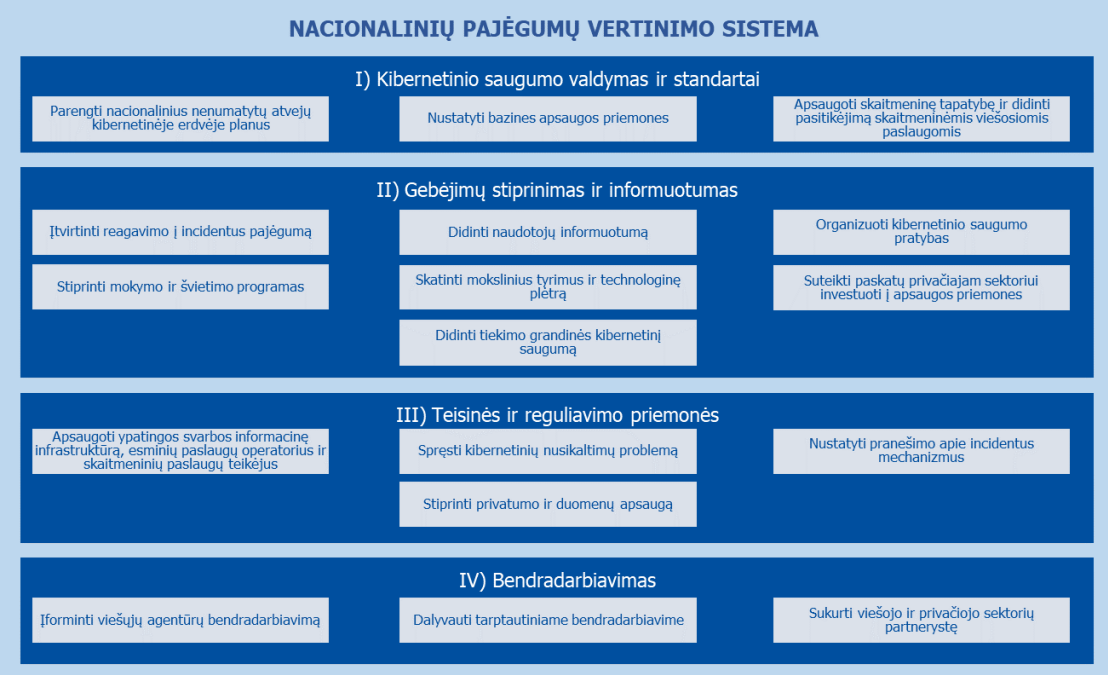
- **(I) Kibernetinio saugumo valdymas ir standartai.** Šioje grupėje vertinamas valstybių narių gebėjimas nustatyti tinkamą valdymą, standartus ir gerąją patirtį kibernetinio saugumo srityje. Šiuo aspektu atsižvelgiama į įvairius kibernetinės gynybos ir atsparumo veiksnius, kartu remiant nacionalinės kibernetinio saugumo pramonės plėtrą ir didinant pasitikėjimą vyriausybėmis.
- **(II) Gebėjimų stiprinimas ir informuotumas.** Šioje grupėje vertinami valstybių narių gebėjimai didinti informuotumą apie kibernetiniam saugumui kylančią riziką, grėsmes ir apie tai, kaip su jomis kovoti. Be to, atsižvelgiant į šį aspektą vertinamas šalies gebėjimas nuolat stiprinti kibernetinio saugumo pajėgumus ir didinti bendrą šios srities žinių ir įgūdžių lygį. Taip pat atsižvelgiama į kibernetinio saugumo rinkos plėtrą ir pažangą kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros srityje. Į šią grupę įtraukiami visi tikslai, suteikiantys pagrindą stiprinti gebėjimus.
- **(III) Teisinės ir reguliavimo priemonės.** Šioje grupėje vertinamas valstybių narių gebėjimas nustatyti būtinas teisines ir reguliavimo priemones, skirtas kovai su kibernetinių nusikaltimų ir susijusių kibernetinių incidentų plitimu, taip pat ypatingos svarbos informacinės infrastruktūros apsaugai. Be to, atsižvelgiant į šį aspektą taip pat vertinamas valstybių narių gebėjimas sukurti teisinę sistemą piliečiams ir įmonėms apsaugoti, pvz., saugumo ir privatumo pusiausvyros užtikrinimo atveju.
- **(IV) Bendradarbiavimas.** Šioje grupėje vertinamas įvairių suinteresuotųjų subjektų grupių bendradarbiavimas ir dalijimasis informacija nacionaliniu ir tarptautiniu lygmenimis, nes tai svarbi priemonė siekiant geriau suprasti nuolat kintančią grėsmių aplinką ir į ją reaguoti.

Į modelį įtraukti tie tikslai, kuriuos bendrai nustato valstybės narės ir kurie atrinkti iš 2.2 skirsnyje išvardytų tikslų. Visų pirma taikant šį modelį įvertinami toliau išvardyti tikslai:

- 1. Parengti nacionalinius nenumatytų atvejų kibernetinėje erdvėje planus (I)
- 2. Nustatyti bazines apsaugos priemones (I)
- 3. Apsaugoti skaitmeninę tapatybę ir didinti pasitikėjimą skaitmeninėmis viešosiomis paslaugomis (I)
- 4. Įsteigti reagavimo į incidentus pajėgumą (II)
- 5. Didinti naudotojų informuotumą (II)
- 6. Organizuoti kibernetinio saugumo pratybas (II)
- 7. Stiprinti mokymo ir švietimo programas (II)
- 8. Skatinti mokslinius tyrimus ir technologinę plėtrą (II)
- 9. Suteikti paskatų privačiajam sektoriui investuoti į apsaugos priemones (II)
- 10. Didinti tiekimo grandinės kibernetinį saugumą (II)
- 11. Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus (III)
- 12. Spręsti kibernetinių nusikaltimų problemą (III)
- 13. Nustatyti pranešimo apie incidentus mechanizmus (III)
- 14. Stiprinti privatumo ir duomenų apsaugą (III)
- 15. Įforminti viešųjų agentūrų bendradarbiavimą (IV)
- 16. Dalyvauti tarptautiniame bendradarbiavime (IV)
- 17. Sukurti viešojo ir privačiojo sektorių partnerystę (IV)

Keturios grupės ir pagrindiniai tikslai sujungiami į modelį, kad būtų galima visapusiškai įvertinti valstybių narių kibernetinio saugumo pajėgumų brandą. 1 pav. pateikiama visa apimanti įsivertinimo sistemos struktūra ir parodoma, kaip šie elementai, t. y. tikslai, grupės ir įsivertinimo sistema, yra susiję su šalies veiklos rezultatų vertinimu.

1 pav. Įsivertinimo sistemos struktūra



Kiekvienam į įsivertinimo sistemą įtrauktam tikslui pateikiami rodikliai, paskirstyti tarp penkių brandos lygių. Kiekvienas rodiklis grindžiamas dichotominiu klausimu (taip / ne). Rodiklis gali būti būtinas arba nebūtinas.

3.4 VERTINIMO BALAIS MECHANIZMAS

Įsivertinimo sistemos **vertinimo balais mechanizme** atsižvelgiama į pirmiau nurodytus elementus ir principus, išvardytus 3.5 skirsnyje. Tiesą sakant, taikant modelį pateikiamas balas, grindžiamas dviejų parametrų – **brandos lygio** ir **aprėpties koeficiento** – verte. Kiekvienas iš šių parametrų gali būti apskaičiuojamas skirtingais lygmenimis: i) pagal tikslą; ii) pagal tikslų grupę; iii) bendrai.

Balai pagal tikslus

Brandos lygio balas suteikia galimybę susidaryti įspūdį apie brandos lygį, nes atskleidžia, kokie pajėgumai ir praktika buvo taikomi. Brandos lygio balas apskaičiuojamas kaip aukščiausias lygis, kurio visus reikalavimus respondentas tenkina (t. y. atsakė TAIP į visus būtinus klausimus), neskaitant to, kad jis tenkina ir visus žemesnių brandos lygių reikalavimus.

Aprėpties koeficientu išreiškiamas visų rodiklių, kurių atžvilgiu atsakymas teigiamas, aprėpties mastas, neatsižvelgiant į jų lygį. Tai yra papildoma vertė, kuria atsižvelgiama į visus rodiklius, pagal kuriuos įvertinamas tikslas. Aprėpties koeficientas apskaičiuojamas kaip visų su tikslu susijusių klausimų skaičiaus ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis.

Svarbu patikslinti, kad toliau šiame dokumente, nurodant tiek brandos lygio vertes, tiek aprėpties koeficientą, vartojamas terminas ***balas***.

2 pav. vertinimo pagal tikslą mechanizmas leidžia pavaizduoti 3.1 skirsnyje aprašytą vertinimo mechanizmą, kuris išsamiau apibūdinamas toliau.

2 pav. Vertinimo pagal tikslą mechanizmas

2 pav. pateikiamas pavyzdys, kaip pagal tikslą nustatomas brandos lygis. Verta pažymėti, kad respondentas tenkina visus pirmų trijų brandos lygių reikalavimus ir tik iš dalies tenkina 4 lygio reikalavimus. Taigi balu nurodoma, kad ***respondento brandos lygis pagal tikslą „Organizuoti kibernetinio saugumo pratybas“ yra trečias****.*

Vis dėlto 2 pav. pateiktame pavyzdyje tikslo brandos lygis negali apimti informacijos, kuri teikiama atsižvelgiant į rodiklius, kurių balas yra teigiamas ir kurie viršija 3 brandos lygį. Tokiu atveju aprėpties koeficientas gali padėti apžvelgti visus elementus, kuriuos respondentas įgyvendino siekdamas šio tikslo, nepaisant faktinio jo brandos lygio. Šiuo atveju visų su tikslu susijusių klausimų skaičiaus ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis yra 19/27, t. y. ***aprėpties koeficiento vertė yra 70 proc.***

Be to, siekiant prisitaikyti prie valstybių narių ypatumų ir kartu sudaryti sąlygas atlikti nuoseklią apžvalgą, balai apskaičiuojami remiantis dviem skirtingomis imtimis grupių lygmeniu ir bendruoju lygmeniu:

- **bendrieji balai:** viena išsami imtis, apimanti visus grupės arba visos sistemos tikslus (nuo 1 iki 17);
- **konkretūs balai:** viena konkreti imtis, apimanti tik valstybės narės atrinktus tikslus (paprastai atitinkančius konkrečios šalies NKSS nustatytus tikslus) grupėje arba visoje sistemoje.

Balai pagal grupes

Bendras kiekvienos grupės brandos lygis apskaičiuojamas kaip visų tos grupės tikslų įgyvendinimo lygio aritmetinis vidurkis.

Konkretus kiekvienos grupės brandos lygis apskaičiuojamas kaip tos grupės tikslų, kuriuos valstybė narė nusprendė vertinti (paprastai atitinkančių konkrečios šalies NKSS nustatytus tikslus), brandos lygio aritmetinis vidurkis.

Pavyzdžiui, 1 pav. parodyta, kad I grupę „Kibernetinio saugumo valdymas ir standartai“ sudaro trys tikslai. Darant prielaidą, kad respondentas nusprendė vertinti tik pirmuosius du tikslus, o trečio – ne, ir darant prielaidą, kad pirmųjų dviejų tikslų brandos lygis yra atitinkamai 2 ir 4, grupės brandos lygis, atsižvelgiant į visus tikslus, yra 2 (I grupės bendras brandos lygis = (2 + 4) / 3), o grupės brandos lygis, atsižvelgiant tik į konkrečius vertintojo pasirinktus tikslus, yra 3 (I grupės konkretus brandos lygis = (2 + 4) / 2).

Bendras kiekvienos grupės aprėpties koeficientas apskaičiuojamas kaip visų grupės klausimų skaičiaus ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis.

Konkretus kiekvienos grupės aprėpties koeficientas apskaičiuojamas kaip visų grupės klausimų, susijusių su tikslais, kuriuos valstybė narė nusprendė vertinti (paprastai atitinkančiais konkrečios šalies NKSS nustatytus tikslus), skaičiaus ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis.

Bendrieji balai

Bendras šalies brandos lygis apskaičiuojamas kaip visų sistemoje numatytų tikslų, nuo 1 iki 17, brandos lygio aritmetinis vidurkis.

Bendras konkretus šalies brandos lygis apskaičiuojamas kaip sistemoje numatytų tikslų, kuriuos valstybė narė nusprendė vertinti (paprastai atitinkančių konkrečios šalies NKSS nustatytus tikslus), brandos lygio aritmetinis vidurkis.

Bendras šalies aprėpties koeficientas apskaičiuojamas kaip visų klausimų, susijusių su visais sistemoje numatytais tikslais, skaičiaus (nuo 1 iki 17) ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis.

Bendras konkretus šalies aprėpties koeficientas apskaičiuojamas kaip visų klausimų, susijusių su sistemoje numatytais tikslais, kuriuos valstybė narė nusprendė vertinti (paprastai atitinkančiais konkrečios šalies NKSS nustatytus tikslus), skaičiaus ir klausimų, į kuriuos atsakyta teigiamai, skaičiaus santykis.

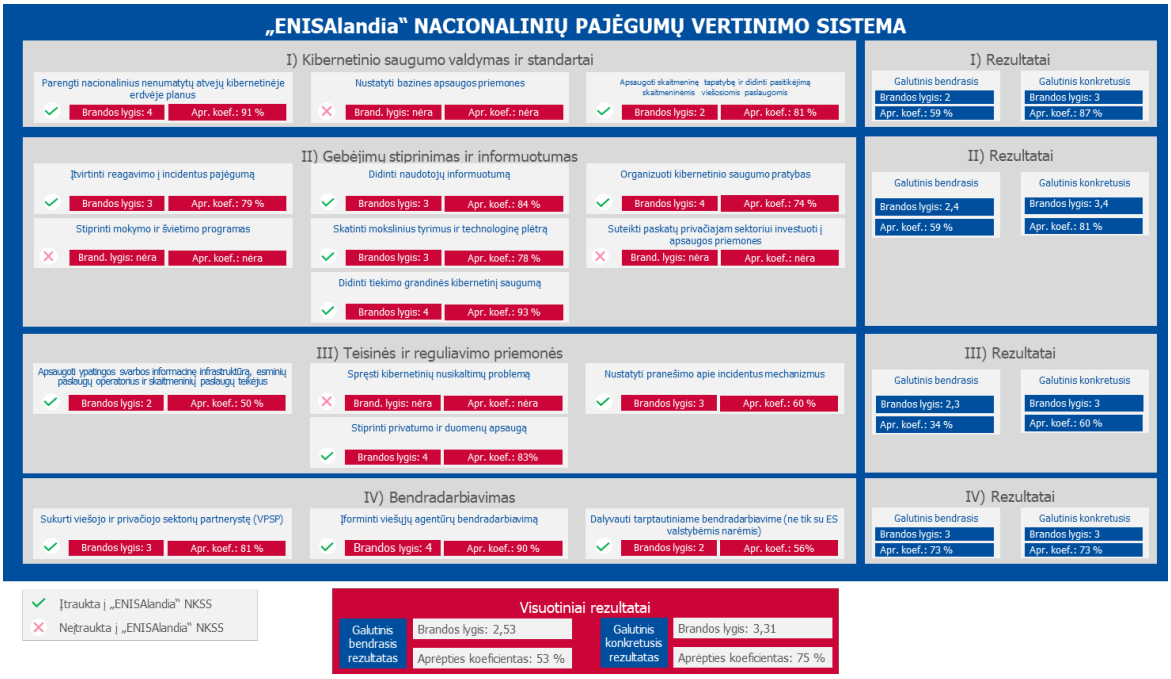
Kiekvienam rodikliui respondentai savo atsakymuose gali pasirinkti trečią variantą „nežinau / netaikoma“. Tuomet rodiklis neįtraukiamas į bendrą rezultatų skaičiavimą.

Siekiant atskleisti pažangą tarp dviejų vertinimų, grupės ir bendro lygmenų brandos lygiai apskaičiuojami kaip aritmetinis vidurkis. Iš tiesų nors alternatyva, kurią sudaro grupės ir bendras brandos lygių skaičiavimas kaip mažiausiai brandaus tikslo brandos lygis, svarbi brandos požiūriu, ji negali atspindėti pažangos, padarytos srityse, kuriose numatyti kiti tikslai.

Kadangi grupės ir bendrasis lygmenys ataskaitų teikimo tikslais sujungiami, nuspręsta naudoti aritmetinį vidurkį. Siekdami didesnio tikslumo, ataskaitų teikimo tikslais naudokite objektyvaus lygmens balus.

Toliau pateiktame 3 pav. apibendrinami vertinimo balais mechanizmai pagal įvairius modelio lygmenis (tikslas, grupė, visuma).

3 pav. Bendras vertinimo balais mechanizmas



3.5 ĮSIVERTINIMO SISTEMOS REIKALAVIMAI

Šiame skirsnyje aprašoma nacionalinių pajėgumų vertinimo sistema grindžiama valstybių narių nurodytais poreikiais ir šiais reikalavimais:

- valstybė narė savanoriškai naudoja NPVS kaip įsivertinimo sistemą;
- NPVS tikslas – įvertinti valstybių narių kibernetinio saugumo pajėgumus atsižvelgiant į 17 tikslų. Vis dėlto valstybė narė gali pasirinkti tikslus, kuriuos ji nori vertinti, ir įvertinti tik 17 tikslų poaibį;
- įsivertinimo sistema siekiama įvertinti valstybės narės kibernetinio saugumo pajėgumų brandos lygį;
- vertinimo rezultatai neskelbiami, išskyrus atvejus, kai valstybė narė nusprendžia tai daryti savo iniciatyva;
- valstybė narė gali parodyti vertinimo rezultatus pristatydama šalies kibernetinio saugumo pajėgumų, tikslų grupės ar net vieno tikslo brandos lygį;
- visi įvertinti tikslai yra lygiaverčiai vertinimo sistemoje, todėl vienodai svarbūs. Tas pats pasakytina apie joje naudojamus rodiklius;
- valstybė narė gali stebėti savo ilgainiui daromą pažangą.

Įsivertinimo sistema siekiama padėti valstybėms narėms stiprinti kibernetinio saugumo pajėgumus. Taigi ji taip pat apima rekomendacijų arba gairių rinkinį, kuriuo Europos šalys galėtų vadovautis gerindamos savo brandos lygį.

Pastaba. Šios rekomendacijos arba gairės yra bendrojo pobūdžio, pagrįstos ENISA leidiniais ir kitų šalių įgyta patirtimi, ir priklausys nuo įsivertinimo rezultatų.

4. NPVS RODIKLIAI

4.1 SISTEMOS RODIKLIAI

Šiame skirsnyje aprašomi ENISA nacionalinių pajėgumų vertinimo sistemos rodikliai. Toliau skirsniai suskirstyti pagal grupes.

Lentelėse pateikiamas išsamus kiekvienos grupės rodiklių rinkinys klausimų, atspindinčių tam tikrą brandos lygį, forma. Klausimynas yra pagrindinė įsivertinimo priemonė. Vertinant kiekvieną tikslą reikia atkreipti dėmesį į du rodiklių rinkinius:

- bendrųjų klausimų apie strategijos brandą rinkinį (9 bendrieji klausimai), kuriame kiekvieno brandos lygio klausimai žymimi raidėmis nuo a iki c ir tai pakartota prie kiekvieno tikslo;
- klausimų apie kibernetinio saugumo pajėgumą rinkinį (319 klausimų apie kibernetinio saugumo pajėgumą), kuriame kiekvienas brandos lygis, būdingas su tikslu susijusiai sričiai, žymimas skaičiais nuo 1 iki 10.

Kiekvienas klausimas pateikiamas su žymeniu (0–1), kuriuo nurodoma, ar klausimas yra būtinas (1), ar nebūtinas brandos lygio rodiklis (0).

Kiekvieną klausimą galima identifikuoti pagal identifikacinį numerį, kurį sudaro:

- tikslo numeris;
- brandos lygis;
- klausimo numeris.

Pavyzdžiui, 1.2.4 klausimas yra ketvirtas klausimas, susijęs su I strateginio tikslo „Parengti nacionalinius nenumatytų atvejų kibernetinėje erdvėje planus“ 2 brandos lygiu.

Reikia pažymėti, kad visame klausimyne klausimai yra nacionalinio lygio, nebent būtų nurodyta kitaip. Visuose klausimuose įvardis „jūs“ bendrai reiškia valstybę narę, o ne vertinimą atliekantį asmenį ar vyriausybinę įstaigą.

Kiekvieno tikslo apibrėžtis pateikiama 2.2 skyriuje – Bendri tikslai, nustatyti Europos NKSS.

4.1.1 1 grupė. Kibernetinio saugumo valdymas ir standartai

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
1. Parengti nacionalinius nenumatytų atvejų kibernetinėje erdvėje planus	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar pradėjote rengti nacionalinius nenumatytų atvejų kibernetinėje erdvėje planus, pvz., nustatėte nenumatytų atvejų planų bendruosius tikslus, taikymo sritį ir (arba) principus ir pan.?	1	Ar turite doktriną ir (arba) nacionalinę strategiją, kurioje kibernetinis saugumas apibrėžiamas kaip krizės veiksnys (t. y. projektą, politiką ir kt.)?	1	Ar turite nacionalinio lygio kibernetinių krizių valdymo planą?	1	Ar esate patenkinti į nacionalinį nenumatytų atvejų kibernetinėje erdvėje planą įtrauktų ypatingos svarbos sektorių skaičiumi arba procentine dalimi?	1	Ar po kibernetinių pratybų arba faktinių krizių nacionaliniu lygmeniu vykdomas patirties įsisavinimo procesas?	1
	2	Ar visuotinai suprantama, kad kibernetiniai incidentai yra krizės veiksnys, galintis kelti grėsmę nacionaliniam saugumui?	0	Ar turite informacijos ir sprendimų priėmėjų informavimo centrą, t. y. kokį nors metodą, platformą ar vietą, padedančią užtikrinti, kad visi reagavimo į krizes subjektai gautų tą pačią tikralaikę informaciją apie kibernetinę krizę?	1	Ar vykdote su kibernetinėmis krizėmis susijusias nacionalinio lygio procedūras?	1	Ar pakankamai dažnai organizuojate su nacionaliniu nenumatytų atvejų kibernetinėje erdvėje planavimu susijusią veiklą (t. y. pratybas)?	1	Ar vykdote reguliaraus nacionalinio plano tikrinimo procesą?	1
	3	Ar atlikta tyrimų (techninių, veiklos, politinių), susijusių su nenumatytų atvejų kibernetinėje erdvėje planavimu?	0	Ar naudojami atitinkami ištekliai siekiant prižiūrėti nacionalinių nenumatytų atvejų kibernetinėje erdvėje planų rengimą ir vykdymą?	1	Ar turite komunikacijos grupę, specialiai išmokytą reaguoti į kibernetines krizes ir informuoti visuomenę?	1	Ar turite pakankamai žmonių, atsakingų už krizių planavimą, analizuojate įgytą patirtį ir diegiate pokyčius?	1	Ar turite tinkamų priemonių ir platformų informuotumui apie padėtį didinti?	1
	4	-		Ar turite nacionalinio lygio kibernetinių grėsmių vertinimo metodiką, apimančią poveikio vertinimo procedūras?	0	Ar įtraukiate visus susijusius nacionalinius suinteresuotuosius subjektus (nacionalinio saugumo, gynybos, civilinės saugos, teisėsaugos institucijas, ministerijas, valdžios institucijas ir kt.)?	1	Ar turite pakankamai žmonių, išmokytų reaguoti į kibernetines krizes nacionaliniu lygmeniu?	1	Ar laikotės konkretaus brandos modelio, kad galėtumėte stebėti ir tobulinti nenumatytų atvejų kibernetinėje erdvėje planą?	0
	5	-		-		Ar turite krizei valdyti tinkamą infrastruktūrą ir situacijų centrą?	1	-		Ar turite išteklius, kurių darbo sritis – numatyti grėsmes arba ruošti ateities kibernetinio saugumo priemones, padėsiančias įveikti būsimas krizes ar ateities uždavinius?	0

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
	6	-		-		Ar prireikus bendradarbiaujate su tarptautiniais suinteresuotaisiais subjektais ES šalyse?	0	-		-	
	7	-		-		Ar prireikus bendradarbiaujate su tarptautiniais suinteresuotaisiais subjektais trečiosiose šalyse?	0	-		-	
2. Nustatyti bazines apsaugos priemones	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar atlikote tyrimą, kad nustatytumėte **viešosioms** organizacijoms taikytinus reikalavimus ir būdingas spragas pagal tarptautiniu mastu pripažintus standartus (pvz., ISO 27001, ISO 27002, BS 15000, EN ISO 27799, PCI-DSS, „CobiT“, ITIL, „BSI IT-Grundschutz“, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, RIS ir pan.)?	1	Ar apsaugos priemonės parengtos laikantis tarptautinių ir (arba) nacionalinių standartų?	1	Ar bazinės apsaugos priemonės yra privalomos?	1	Ar vykdomas procesas, kuriuo siekiama dažnai atnaujinti bazines apsaugos priemones?	1	Ar taikote procesą, kuriuo siekiama sustiprinti IRT, kai incidentų klausimo nepavyksta išspręsti priemonėmis?	1
	2	Ar atlikote tyrimą, kad nustatytumėte **privačioms** organizacijoms taikytinus reikalavimus ir būdingas spragas pagal tarptautiniu mastu pripažintus standartus (pvz., ISO 27001, ISO 27002, BS 15000, EN ISO 27799, PCI-DSS, „CobiT“, ITIL, „BSI IT-Grundschutz“, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, RIS ir pan.)?	1	Ar nustatant bazines apsaugos priemones konsultuojamasi su privačiuoju sektoriumi ir kitais suinteresuotaisiais subjektais?	1	Ar įgyvendinate horizontaliąsias apsaugos priemones visuose ypatingos svarbos sektoriuose?	1	Ar įdiegtas stebėsenos mechanizmas, skirtas bazinių apsaugos priemonių taikymui tirti?	1	Ar vertinate naujų standartų, parengtų reaguojant į naujausius įvykius grėsmių aplinkoje, aktualumą?	1
	3	-		-		Ar įgyvendinate konkretiems sektoriams skirtas apsaugos priemones visuose ypatingos svarbos sektoriuose?	1	Ar yra nacionalinė institucija, kuri tikrina, ar bazinės apsaugos priemonės vykdomos, ar ne?	1	Ar taikote arba skatinate nacionalinį suderinto pažeidžiamumų atskleidimo (SPA) procesą?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
	4	-				Ar bazinės apsaugos priemonės atitinka atitinkamas sertifikavimo sistemas?	1	Ar vykdomas reikalavimų neatitinkančių organizacijų nustatymo per tam tikrą laikotarpį procesas?	1	-	
	5	-		-		Ar vykdomas bazinių apsaugos priemonių rizikos įsivertinimo procesas?	1	Ar vykdomas auditas, siekiant užtikrinti, kad apsaugos priemonės būtų taikomos tinkamai?	1	-	
2. Nustatyti bazines apsaugos priemones	6	-		-		Ar peržiūrite privalomas bazines apsaugos priemones vyriausybinių institucijų viešųjų pirkimų procese?	0	Ar apibrėžiate arba aktyviai skatinate priimti saugius ypatingos svarbos IT ir (arba) OT produktų (medicininės įrangos, susietųjų ir autonominių transporto priemonių, profesionalų radijo ryšio, sunkiosios pramonės įrangos ir kt.) kūrimo standartus?	0	-	
3. Apsaugoti skaitmeninę tapatybę ir didinti pasitikėjimą skaitmeninėmis viešosiomis paslaugomis	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar atlikote tyrimus arba trūkumų analizes, kad nustatytumėte poreikį užtikrinti skaitmenines viešąsias paslaugas piliečiams ir įmonėms?	1	Ar atliekate rizikos analizes, kad nustatytumėte išteklių ar paslaugų rizikos profilį prieš perkeldami juos į debesiją, ar įgyvendinate kokius nors skaitmeninės transformacijos projektus?	1	Ar visuose e. valdžios projektuose propaguojate integruotosios privatumo apsaugos metodiką?	1	Ar renkate kibernetinių incidentų, susijusių su skaitmeninių viešųjų paslaugų pažeidimu, rodiklius?	1	Ar dalyvaujate Europos darbo grupių veikloje, kuria siekiama išlaikyti elektroninių patikimumo užtikrinimo paslaugų (e. parašų, e. antspaudų, e. registruoto pristatymo paslaugų, laiko žymėjimo, interneto svetainių tapatumo nustatymo) standartus ir (arba) parengti naujus reikalavimus (pvz., ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU ir kt.)?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
3. Apsaugoti skaitmeninę tapatybę ir didinti pasitikėjimą skaitmeninėmis viešosiomis paslaugomis	2	-		Ar turite strategiją, kaip kurti arba skatinti piliečiams ir įmonėms skirtas saugias nacionalines elektroninės atpažinties schemas („eID“)?	1	Ar į saugių skaitmeninių viešųjų paslaugų kūrimą ir teikimą įtraukiate privačius suinteresuotuosius subjektus?	1	Ar užtikrinote e. atpažinties priemonių tarpusavio pripažinimą su kitomis valstybėmis narėmis?	1	Ar aktyviai dalyvaujate tarpusavio vertinimuose, teikdami pranešimus Europos Komisijai pagal „eID“ sistemas?	1
	3	-		Ar turite strategiją, kaip kurti arba skatinti piliečiams ir įmonėms skirtas saugias nacionalines elektronines patikimumo užtikrinimo paslaugas (e. parašus, e. antspaudus, e. registruoto pristatymo paslaugas, laiko žymėjimą, interneto svetainių tapatumo nustatymą)?	1	Ar taikote būtinąjį saugumo bazinį lygį visoms skaitmeninėms viešosioms paslaugoms?	1	-		-	
	4	-		Ar turite valstybinę debesijos strategiją (debesijos kompiuterijos strategiją, skirtą vyriausybei ir viešosioms įstaigoms, pvz., ministerijoms, vyriausybinėms agentūroms ir viešojo administravimo institucijoms ir kt.), kurioje atsižvelgiama į poveikį saugumui?	0	Ar piliečiai ir įmonės gali naudotis kokiomis nors elektroninės atpažinties schemomis, kurių saugumo užtikrinimo lygis yra pakankamas arba aukštas, kaip apibrėžta eIDAS reglamento (ES) Nr. 910/2014 priede?	1	-		-	
	5	-		-		Ar turite skaitmeninių viešųjų paslaugų, kurioms reikia pakankamo arba aukšto lygio elektroninės atpažinties schemų, kaip apibrėžta eIDAS reglamento (ES) Nr. 910/2014 priede?	1	-		-	
	6	-		-		Ar turite piliečiams ir įmonėms skirtų patikimumo užtikrinimo paslaugų (e. parašo, e. antspaudo, e. registruoto pristatymo paslaugų, laiko žymėjimo, interneto svetainių tapatumo nustatymo) teikėjų?	1	-		-	
	7	-		-		Ar skatinate priimti bazines apsaugos priemones visiems debesijos diegimo modeliams (pvz., privatiems, viešiesiems, mišriems, „IaaS“, „PaaS“, „SaaS“)?	0	-		-	

4.1.2 2 grupė. Gebėjimų stiprinimas ir informuotumas

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
4. Įtvirtinti reagavimo į incidentus pajėgumą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar turite neoficialių reagavimo į incidentus pajėgumų, valdomų viešajame ir privačiajame sektoriuose arba tarp jų?	1	Ar turite bent vieną oficialią nacionalinę CSIRT?	1	Ar turite reagavimo į incidentus pajėgumų TIS direktyvos II priede nurodytuose sektoriuose?	1	Ar apibrėžėte ir skatinate standartizuotą reagavimo į incidentus procedūrų ir incidentų klasifikavimo sistemų praktiką?	1	Ar turite ką tik nustatytų (angl. *zero-day*) pažeidžiamumų ankstyvo aptikimo, nustatymo, prevencijos, švelninimo ir reagavimo į juos mechanizmų?	1
	2	-		Ar jūsų nacionalinė(s) CSIRT turi aiškiai apibrėžtą intervencinių veiksmų taikymo sritį, pvz., atsižvelgiant į tikslinį sektorių, incidentų rūšis, poveikį?	1	Ar jūsų šalyje taikomas CSIRT bendradarbiavimo mechanizmas, skirtas reaguoti į incidentus?	1	Ar vertinate reagavimo į incidentus pajėgumus, siekdami užtikrinti, kad turėtumėte pakankamai išteklių ir įgūdžių TIS direktyvos I priedo 2 punkte nurodytoms užduotims atlikti?	1	-	
	3	-		Ar jūsų nacionalinė(s) CSIRT palaiko aiškiai apibrėžtus santykius su kitais nacionaliniais suinteresuotaisiais subjektais, kalbant apie nacionalinę kibernetinio saugumo aplinką ir reagavimo į incidentus praktiką (pvz., teisėsaugos institucijomis, kariniais subjektais, IPT, NKSC)?	0	Ar jūsų nacionalinė(s) CSIRT turi reagavimo į incidentus pajėgumų pagal TIS direktyvos I priedą, t. y. kalbant apie prieinamumą, fizinį saugumą, veiklos tęstinumą, tarptautinį bendradarbiavimą, incidentų stebėseną, ankstyvojo perspėjimo ir įspėjimo pajėgumą, reagavimą į incidentus, rizikos analizę ir informuotumą apie padėtį, bendradarbiavimą su privačiuoju sektoriumi, standartinę praktiką ir kt.?	1	-		-	
	4	-				Ar yra sukurtas su incidentais susijusio bendradarbiavimo su kitomis kaimyninėmis šalimis mechanizmas?	1	-		-	

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
4. Įtvirtinti reagavimo į incidentus pajėgumą	5	-		-		Ar oficialiai apibrėžėte aiškią incidentų valdymo politiką ir procedūras?	1	-		-	
	6	-		-		Ar jūsų nacionalinė(s) CSIRT dalyvauja kibernetinio saugumo pratybose tiek nacionaliniu, tiek tarptautiniu lygmeniu?	1	-		-	
	7	-		-		Ar jūsų nacionalinė(s) CSIRT priklauso FIRST (Reagavimo į incidentus ir saugumo tarnybų forumui)?	0	-		-	
5. Didinti naudotojų informuotumą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar vyriausybė, privatusis sektorius arba bendrieji naudotojai bent kiek pripažįsta, kad reikia didinti informuotumą kibernetinio saugumo ir privatumo klausimais?	1	Ar nustatėte konkrečią tikslinę auditoriją naudotojų informuotumo didinimo srityje, pvz., bendruosius naudotojus, jaunimą, verslo klientus (šią auditoriją galima skirstyti toliau: MVĮ, esminių paslaugų operatoriai, skaitmeninių paslaugų teikėjai ir kt.)?	1	Ar esate parengę kampanijų komunikacijos planus ir (arba) strategiją?	1	Ar rengiate savo kampanijos vertinimo planavimo etape metriką?	1	Ar turite mechanizmus, užtikrinančius, kad informuotumo didinimo kampanijos būtų nuolat aktualios technologijų pažangos, grėsmių aplinkos pokyčių, teisinių reglamentų ir nacionalinio saugumo direktyvų aspektais?	1
	2	Ar viešosios agentūros savo organizacijoje vykdo *ad hoc* informuotumo apie kibernetinį saugumą didinimo kampanijas, pvz., įvykus kibernetiniam incidentui?	0	Ar rengiate projektą, kuriuo siekiama didinti informuotumą informacijos saugumo ir privatumo klausimais?	1	Ar vykdote turinio kūrimo procesą vyriausybės lygmeniu?	1	Ar vertinate savo kampanijas jas užbaigę?	1	Ar atliekate reguliarų vertinimą arba tyrimą, kad nustatytumėte su kibernetinio saugumo ir privatumo klausimais susijusį požiūrio pokytį arba elgesio pokyčius privačiajame ir viešajame sektoriuose?	1

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
5. Didinti naudotojų informuotumą	3	Ar viešosios agentūros vykdo *ad hoc* visuomenės informavimo apie kibernetinį saugumą kampanijas, pvz., įvykus kibernetiniam incidentui?	0	Ar turite išteklių, kuriuos lengva atpažinti (pvz., bendrą interneto portalą, informuotumo didinimo priemonių) ir kurie būtų prieinami visiems naudotojams, norintiems įgyti žinių apie kibernetinį saugumą ir privatumą?	1	Ar turite kokių nors mechanizmų, kaip nustatyti tikslines informuotumo didinimo sritis (pvz., ENISA grėsmių žemėlapis, nacionalinis kraštovaizdis, tarptautinis kraštovaizdis, nacionalinių kovos su elektroniniu nusikalstamumu centrų grįžtamoji informacija ir kt.)?	1	Ar turite kokių nors mechanizmų tinkamiausiai žiniasklaidos priemonei ar komunikacijos kanalui nustatyti atsižvelgiant į tikslinę auditoriją, kad būtų galima kuo labiau padidinti aprėptį ir dalyvavimą (pvz., įvairių rūšių skaitmeninė žiniasklaida, brošiūros, e. laiškai, mokomoji medžiaga, plakatai lankomose vietose, televizija, radijas ir kt.)?	1	Ar konsultuojatės su elgesio ekspertais, kad priderintumėte savo kampaniją prie tikslinės auditorijos?	1
	4	-		-		Ar buriate suinteresuotuosius subjektus, ekspertus ir komunikacijos grupes turiniui kurti?	1			-	
	5	-		-		Ar į savo informuotumo didinimo veiksmus įtraukiate privatųjį sektorių, siekdami viešinti ir skleisti informaciją platesnei auditorijai?	1	-		-	
	6	-		-		Ar rengiate konkrečias viešojo, privačiojo, akademinio arba pilietinės visuomenės sektorių vadovams skirtas informuotumo didinimo iniciatyvas?	1	-		-	
	7	-		-		Ar dalyvaujate ENISA Europos kibernetinio saugumo mėnesio (EKSM) kampanijose?	0	-		-	
6. Organizuoti kibernetinio saugumo pratybas	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
6. Organizuoti kibernetinio saugumo pratybas	1	Ar vykdote krizių valdymo pratybas kituose sektoriuose (ne kibernetinio saugumo) nacionaliniu arba visos Europos lygmeniu?	1	Ar turite nacionalinio lygio kibernetinio saugumo pratybų programą?	1	Ar įtraukiate visas susijusias viešojo administravimo institucijas (net jei scenarijus susijęs su konkrečiu sektoriumi)?	1	Ar rengiate veiksmų įgyvendinimo ir (arba) vertinimo ataskaitas?	1	Ar turite kibernetinėje erdvėje įgytos patirties analizės pajėgumą (ataskaitų teikimas, analizė, poveikio švelninimas)?	1
	2	Ar turite išteklius krizių valdymo pratyboms rengti ir planuoti?	1	Ar vykdote arba teikiate pirmenybę kibernetinių krizių valdymo pratyboms, susijusioms su esminėmis visuomenės funkcijomis ir ypatingos svarbos informacine infrastruktūra?	1	Ar į pratybų planavimą ir vykdymą įtraukiate privatųjį sektorių?	1	Ar išbandote nacionalinio lygio planus ir procedūras?	1	Ar turite nusistovėjusį įgytos patirties vertinimo procesą?	1
	3	-		Ar nustatėte, kuri koordinavimo įstaiga (viešoji, konsultacinė ar pan. įstaiga) prižiūrės kibernetinio saugumo pratybų rengimą ir planavimą?	0	Ar organizuojate konkretiems sektoriams skirtas pratybas nacionaliniu ir (arba) tarptautiniu lygmeniu?	1	Ar dalyvaujate kibernetinio saugumo pratybose visos Europos lygmeniu?	1	Ar pritaikote pratybų scenarijus atsižvelgdami į naujausias aplinkybes (technologinę pažangą, pasaulinius konfliktus, grėsmių aplinką ir kt.)?	1
	4	-		-		Ar organizuojate pratybas visuose ypatingos svarbos sektoriuose, nurodytuose TIS direktyvos II priede?	1	-		Ar derinate savo krizių valdymo procedūras su kitomis valstybėmis narėmis, kad krizės būtų veiksmingai valdomos visos Europos mastu?	1
	5	-		-		Ar organizuojate sektorių ir (arba) tarpsektorines kibernetinio saugumo pratybas?	1	-		Ar turite mechanizmą, užtikrinantį, kad strategija, planai ir procedūros būtų greitai pritaikomi atsižvelgiant į pratybose įgytą patirtį?	0
	6	-		-		Ar organizuojate kibernetinio saugumo pratybas, skirtas įvairiems lygmenims (techniniam ir veiklos lygmeniui, procedūrų lygmeniui, sprendimų priėmimo lygmeniui, politiniam lygmeniui ir kt.)?	0	-		-	
7. Stiprinti mokymo ir švietimo programas	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar svarstote galimybę rengti kibernetinio saugumo mokymo ir švietimo programas?	1	Ar rengiate kibernetinio saugumo kursus?	1	Ar jūsų šalis įtraukusi kibernetinio saugumo kultūros mokymą į ankstyvąjį moksleivių ugdymo etapą? Pavyzdžiui, ar pritariate kibernetinio saugumo mokymui pagrindinėje ir vidurinėje mokyklose?	1	Ar primygtinai raginate užtikrinti, kad privačiojo ir viešojo sektorių darbuotojai būtų akredituoti arba sertifikuoti?	1	Ar turite mechanizmus, užtikrinančius, kad mokymai ir švietimo programos būtų nuolat aktualios esamų ir besiformuojančių technologinių pokyčių, grėsmių aplinkos pokyčių, teisinių reglamentų ir nacionalinio saugumo direktyvų aspektais?	1
	2	-		Ar jūsų šalies universitetai siūlo kibernetinio saugumo doktorantūros studijas kaip nepriklausomą discipliną, o ne kaip informatikos dalyką?	1	Ar turite nacionalinių mokslinių tyrimų laboratorijų ir švietimo įstaigų, kurios specializuojasi kibernetinio saugumo srityje?	1	Ar jūsų šalis yra parengusi kibernetinio saugumo mokymo arba mentorystės programų, skirtų šalies startuoliams ir MVĮ remti?	1	Ar steigiate akademinius kibernetinio saugumo kompetencijos centrus, kurie veiktų kaip mokslinių tyrimų ir švietimo centrai?	1
	3	-		Ar planuojate mokyti pedagogus, neatsižvelgiant į jų specializaciją, apie informacijos saugumą ir privatumą (pvz., saugumą internete, asmens duomenų apsaugą, patyčias kibernetinėje erdvėje)?	1	Ar skatinate ir (arba) finansuojate specialius kibernetinio saugumo kursus ir mokymo planus, skirtus valstybių narių įdarbinimo agentūrų darbuotojams?	1	Ar aktyviai skatinate į aukštojo mokslo programas įtraukti informacijos saugumo kursus ne tik informatikos studentams, bet ir kitų specialybių studentams (pvz., tos profesijos poreikiams pritaikytus kursus)?	1	Ar akademinės institucijos dalyvauja svarbiose tarptautinėse diskusijose, susijusiose su švietimu kibernetinio saugumo klausimais ir moksliniais tyrimais?	0
	4	-		-		Ar turite kibernetinio saugumo kursus ir (arba) specializuotą EKS (Europos kvalifikacijų sandara) 5–8 lygių mokymo programą?	1	Ar reguliariai vertinate įgūdžių trūkumą (kibernetinio saugumo darbuotojų trūkumą) informacijos saugumo srityje?	1	-	
	5	-		-		Ar skatinate ir (arba) remiate iniciatyvas įtraukti saugumo internete kursus į pradinio ir vidurinio ugdymo programas?	1	Ar skatinate akademinių institucijų tinklaveiką ir dalijimąsi informacija tiek nacionaliniu, tiek tarptautiniu lygmeniu?	1		

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
7. Stiprinti mokymo ir švietimo programas	6	-		-		Ar finansuojate arba siūlote nemokamus kibernetinio saugumo pagrindų mokymus piliečiams?	0	Ar kokiu nors būdu įtraukiate privatųjį sektorių į švietimo kibernetinio saugumo klausimais iniciatyvas, pvz., kursų kūrimą ir organizavimą, stažuotes, mokomąją praktiką ir kt.?	1	-	
	7	-		-		Ar organizuojate kasmetinius informacijos saugumo renginius (pvz., įsilaužimo konkursus arba programuotojų maratonus)?	0	Ar įgyvendinate finansavimo mechanizmus, kuriais skatinama siekti diplomų kibernetinio saugumo srityje (pvz., stipendijos, užtikrintos pameistrystės ir (arba) stažuotės vietos, užtikrintos darbo vietos tam tikrame sektoriuje arba pareigos viešajame sektoriuje)?	0	-	
8. Skatinti mokslinius tyrimus ir technologinę plėtrą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar atlikote tyrimus arba analizes, kad nustatytumėte mokslinių tyrimų ir technologinės plėtros kibernetinio saugumo srityje prioritetus?	1	Ar taikote mokslinių tyrimų ir technologinės plėtros prioritetų nustatymo procesą (pvz., naujų temų, susijusių su atgrasymu nuo naujų kibernetinių išpuolių, jų apsauga, aptikimu ir prisitaikymu prie jų)?	1	Ar planuojama mokslinių tyrimų ir technologinės plėtros iniciatyvas susieti su realiąja ekonomika?	1	Ar mokslinių tyrimų ir technologinės plėtros kibernetinio saugumo srityje iniciatyvos suderintos su atitinkamais strateginiais tikslais, pvz., bendrąja skaitmenine rinka, programa „Horizontas 2020“, Skaitmeninės Europos programa, ES kibernetinio saugumo strategija?	1	Ar nacionaliniu lygmeniu bendradarbiaujate įgyvendinant kokias nors tarptautines mokslinių tyrimų ir plėtros iniciatyvas, susijusias su kibernetiniu saugumu?	1
	2	-		Ar nustatant mokslinių tyrimų ir technologinės plėtros prioritetus dalyvauja privatusis sektorius?	1	Ar vykdomi nacionaliniai projektai, susiję su kibernetiniu saugumu?	1	Ar įdiegta mokslinių tyrimų ir technologinės plėtros iniciatyvų vertinimo sistema?	1	Ar mokslinių tyrimų ir technologinės plėtros prioritetai suderinti su esamais ar būsimais reguliavimo aktais (nacionaliniu lygmeniu)?	1

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
8. Skatinti mokslinius tyrimus ir technologinę plėtrą	3	-		Ar nustatant mokslinių tyrimų ir technologinės plėtros prioritetus dalyvauja akademinė bendruomenė?	1	Ar turite vietos ir (arba) regionų startuolių ekosistemų ir kitų tinklaveikos kanalų (pvz., technologijų parkų, inovacijų grupių, tinklaveikos renginių ir platformų), kad būtų skatinamos inovacijos (įskaitant kibernetinio saugumo startuolius)?	1	Ar yra sudaryta bendradarbiavimo susitarimų su universitetais ir kitomis mokslinių tyrimų įstaigomis?	1	Ar dalyvaujate pagrindinėse diskusijose viena ar keliomis pažangiųjų mokslinių tyrimų ir technologinės plėtros temomis tarptautiniu lygmeniu?	0
	4	-		Ar yra kokių nors nacionalinių mokslinių tyrimų ir technologinės plėtros iniciatyvų, susijusių su kibernetiniu saugumu?	0	Ar investuojama į kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros programas akademinėje bendruomenėje ir privačiajame sektoriuje?	1	Ar yra pripažintas institucinis organas, prižiūrintis veiklą kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros srityje?	0	-	
	5	-		-		Ar universitetuose yra pramoninių mokslinių tyrimų katedros, kad būtų galima susieti mokslinių tyrimų srities dalykus ir rinkos poreikius?	1	-		-	
	6	-		-		Ar turite specialių su kibernetiniu saugumu susijusių mokslinių tyrimų ir technologinės plėtros finansavimo programų?	0	-		-	
9. Suteikti paskatų privačiajam sektoriui investuoti į apsaugos priemones	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar yra pramonės politika arba politinė valia skatinti kibernetinio saugumo pramonės plėtrą?	1	Ar rengiant paskatas dalyvauja privatusis sektorius?	1	Ar yra ekonominių arba reguliavimo ar kitokių rūšių paskatų investicijoms į kibernetinį saugumą skatinti?	1	Ar yra kokių nors privačių subjektų, kurie reaguoja į paskatas investuodami į apsaugos priemones, pvz., investuotojų, kurių specializacija – kibernetinis saugumas, ir nespecializuotų investuotojų?	1	Ar numatydami paskatas, susijusias su kibernetinio saugumo temomis, atsižvelgiate į naujausius grėsmių pokyčius?	1

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
9. Suteikti paskatų privačiajam sektoriui investuoti į apsaugos priemones	2	–		Ar esate nustatę konkrečias kibernetinio saugumo temas, kurias reikia plėtoti, pvz., kriptografija, privatumas, nauja tapatumo nustatymo forma, dirbtinis intelektas kibernetinio saugumo srityje ir pan.?	0	Ar teikiate paramą (pvz., mokesčių paskatas) kibernetinio saugumo startuoliams ir MVĮ?	1	Ar teikiate paskatas privačiajam sektoriui, kad daugiausia dėmesio būtų skiriama pažangiųjų technologijų, pvz., 5G, dirbtinio intelekto, daiktų interneto, kvantinės kompiuterijos ir kt., saugumui?	1	–	
	3	–		–		Ar teikiate mokestines arba kitas finansines paskatas privačiojo sektoriaus investuotojams, investuojantiems į kibernetinio saugumo startuolius?	1	–		–	
	4	–		–		Ar kibernetinio saugumo startuoliams ir MVĮ sudarote palankesnes sąlygas dalyvauti viešųjų pirkimų procese?	0	–		–	
	5	–		–		Ar skirtas biudžetas paskatoms privačiajam sektoriui teikti?	0	–		–	
10. Didinti tiekimo grandinės kibernetinį saugumą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar atlikote tyrimą dėl tiekimo grandinės valdymo saugumo gerosios patirties, kuri taikoma viešuosiuose pirkimuose įvairiuose pramonės segmentuose ir (arba) viešajame sektoriuje?	1	Ar atliekate kibernetinio saugumo vertinimus visoje IRT paslaugų ir produktų tiekimo grandinėje ypatingos svarbos sektoriuose (kaip nurodyta TIS direktyvos (2016/1148) II priede)?	1	Ar naudojate IRT pagrįstų produktų ir paslaugų saugumo sertifikavimo sistemą, pvz., SOG-IS MRA Europoje (Vyresniųjų pareigūnų grupė informacinių sistemų saugumo klausimais, tarpusavio pripažinimo susitarimas) susitarimą dėl bendrųjų kriterijų pripažinimo (CCRA), nacionalines iniciatyvas, sektorių iniciatyvas ir pan.?	1	Ar vykdomas IRT paslaugų ir produktų tiekimo grandinės kibernetinio saugumo vertinimų ypatingos svarbos sektoriuose atnaujinimo procesas (kaip nurodyta TIS direktyvos (2016/1148) II priede)?	1	Ar taikote aptikimo priemones pagrindiniuose tiekimo grandinės elementuose, kad būtų galima anksti nustatyti neteisėto atskleidimo požymius (pvz., saugumo kontrolę IPS lygmeniu, apsaugos priemones pagrindiniuose infrastruktūros komponentuose ir kt.)?	1

NKSS tikslas	Nr.	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
10. Didinti tiekimo grandinės kibernetinį saugumą	2	-		Ar taikote viešojo administravimo viešųjų pirkimų politikos standartus siekdami užtikrinti, kad IRT produktų ar paslaugų teikėjai atitiktų pagrindinius informacijos saugumo reikalavimus, pvz., ISO/IEC 27001 ir 27002, ISO/IEC 27036 ir kt.?	1	Ar aktyviai skatinate IRT produktų ir paslaugų kūrimo gerąją patirtį, susijusią su integruotąja privatumo apsauga, pvz., saugios programinės įrangos kūrimo gyvavimo ciklą, daiktų interneto gyvavimo ciklą?	1	Ar taikote procesą silpnoms kibernetinio saugumo grandims nustatyti ypatingos svarbos sektorių tiekimo grandinėje (kaip nurodyta TIS direktyvos (2016/1148) II priede)?	1	-	
	3	-		-		Ar rengiate ir teikiate centralizuotus katalogus, kuriuose pateikiama išsami informacija apie esamus informacijos saugumo ir privatumo standartus, kurie gali būti pritaikyti MVĮ ir kuriuos jos gali taikyti?	1	Ar esate įdiegę mechanizmus, kuriais užtikrinama, kad esminių paslaugų operatoriams itin svarbūs IRT produktai ir paslaugos būtų atsparūs kibernetiniu požiūriu (t. y. gebėtų išlaikyti prieinamumą ir apsisaugoti nuo kibernetinio incidento), pvz., atliekant bandymus, reguliarius vertinimus, aptinkant pažeistus elementus ir pan.?	1	-	
	4	-				Ar aktyviai dalyvaujate kuriant IRT skaitmeninių produktų, paslaugų ir procesų ES sertifikavimo sistemą, kaip nustatyta ES kibernetinio saugumo akte (Reglamentas (ES) 2019/881) (pvz., dalyvaujate Europos kibernetinio saugumo sertifikavimo grupės (EKSSG) veikloje, propaguojate IRT produktų ir (arba) paslaugų saugumo techninius standartus ir procedūras)?	0	Ar skatinate kurti MVĮ skirtas sertifikavimo sistemas, kad būtų didinamas informacijos saugumas ir skatinamas privatumo standartų taikymas?	0	-	
	5	-		-		Ar teikiate kokias nors paskatas MVĮ priimti saugumo ir privatumo standartus?	0	Ar taikote kokias nors nuostatas, kuriomis didelės įmonės skatinamos didinti mažųjų įmonių kibernetinį saugumą jų tiekimo grandinėse (pvz., kibernetinio saugumo centras, mokymo ir informuotumo didinimo kampanijos ir kt.)?	0	-	
	6	-		-		Ar skatinate programinės įrangos pardavėjus remti MVĮ užtikrinant saugias standartines produktų, skirtų mažoms organizacijoms, konfigūracijas?	0	-		-	

4.1.3 3 grupė. Teisinės ir reguliavimo priemonės

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
11. Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar visuotinai suprantama, kad ypatingos svarbos informacinės infrastruktūros operatoriai prisideda prie nacionalinio saugumo?	1	Ar turite esminių paslaugų nustatymo metodiką?	1	Ar įgyvendinote TIS direktyvą (2016/1148)?	1	Ar turite rizikos registro atnaujinimo procedūrą?	1	Ar rengiate ir atnaujinate grėsmių padėties ataskaitas?	1
	2	-		Ar turite ypatingos svarbos informacinės infrastruktūros objektų nustatymo metodiką?	1	Ar įgyvendinote ESI direktyvą (2008/114) dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo?	1	Ar turite kitų mechanizmų, skirtų įvertinti, ar esminių paslaugų operatorių įgyvendinamos techninės ir organizacinės priemonės yra tinkamos tinklų ir informacinių sistemų saugumui kylančiai rizikai valdyti (pvz., reguliarus kibernetinio saugumo auditas, nacionalinė standartinių priemonių įgyvendinimo sistema, vyriausybės teikiamos techninės priemonės, kaip antai aptikimo priemonės arba sistemos konfigūracijos peržiūra ir kt.)?	1	Ar atsižvelgdami į naujausius įvykius grėsmių aplinkoje galite įtraukti naują sektorių į savo ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planą?	1
	3	-		Ar turite esminių paslaugų operatorių nustatymo metodiką?	1	Ar turite pagal ypatingos svarbos sektorių nustatytų esminių paslaugų operatorių nacionalinį registrą?	1	Ar bent kas dvejus metus peržiūrite ir atitinkamai atnaujinate nustatytų esminių paslaugų operatorių sąrašą?	1	Ar atsižvelgdami į naujausius įvykius grėsmių aplinkoje galite pritaikyti naujus reikalavimus savo ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų plane?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
11. Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus	4	-		Ar turite skaitmeninių paslaugų teikėjų nustatymo metodiką?	1	Ar turite nustatytų skaitmeninių paslaugų teikėjų nacionalinį registrą?	1	Ar turite kitų mechanizmų, skirtų įvertinti, ar skaitmeninių paslaugų teikėjų įgyvendinamos techninės ir organizacinės priemonės yra tinkamos tinklų ir informacinių sistemų saugumui kylančiai rizikai valdyti (pvz., reguliarus kibernetinio saugumo auditas, nacionalinė standartinių priemonių įgyvendinimo sistema, vyriausybės teikiamos techninės priemonės, kaip antai aptikimo priemonės arba sistemos konfigūracijos peržiūra ir kt.)?	1	-	
	5	-		Ar turite vieną ar daugiau nacionalinių institucijų, prižiūrinčių ypatingos svarbos informacinės infrastruktūros apsaugą ir tinklų bei informacinių sistemų saugumą, pvz., kaip reikalaujama pagal TIS direktyvą (2016/1148)?	1	Ar turite nustatomos arba žinomos rizikos nacionalinį registrą?	1	Ar bent kas dvejus metus peržiūrite ir atitinkamai atnaujinate nustatytų skaitmeninių paslaugų teikėjų sąrašą?	1	-	
	6	-		Ar rengiate konkretiems sektoriams skirtus apsaugos planus, pvz., apimančius bazines kibernetinio saugumo priemones (privalomas arba rekomendacinio pobūdžio)?	0	Ar turite ypatingos svarbos informacinės infrastruktūros priklausomybės nustatymo metodiką?	1	Ar naudojate saugumo sertifikavimo sistemą (nacionalinę arba tarptautinę), kad esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams padėtumėte nustatyti saugius IRT produktus (pvz., SOG-IS MRA Europoje, nacionalines iniciatyvas ir kt.)?	1	-	
	7	-		-		Ar taikote rizikos valdymo praktiką, kad nacionaliniu lygmeniu nustatytumėte, kiekybiškai įvertintumėte ir valdytumėte su ypatingos svarbos informacinės infrastruktūros objektais susijusią riziką?	1	Ar taikote saugumo sertifikavimo sistemą arba kvalifikacijos vertinimo procedūrą siekdami įvertinti su esminių paslaugų operatoriais dirbančius paslaugų teikėjus, pvz., paslaugų teikėjus incidentų nustatymo, reagavimo į incidentus, kibernetinio saugumo audito, debesijos paslaugų, lustinių kortelių ir kt. srityse?	1	-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
11. Apsaugoti ypatingos svarbos informacinę infrastruktūrą, esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus	8	-		-		Ar dalyvaujate konsultacijų, skirtų nustatyti tarpvalstybinę priklausomybę, procese?	1	Ar taikote mechanizmus, kuriais nustatomas esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų atitikties bazinėms kibernetinio saugumo priemonėms lygis?	0	-	
	9					Ar turite vieną bendrą informacinį punktą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu nacionaliniu lygmeniu ir tarpvalstybiniu bendradarbiavimu Sąjungos lygmeniu, koordinavimą?	1	Ar taikote kokias nors priemones, kad užtikrintumėte ypatingos svarbos informacinės infrastruktūros teikiamų paslaugų tęstinumą (pvz., krizių numatymas, ypatingos svarbos informacinių sistemų atkūrimo procedūros, veiklos tęstinumas be IT, atsarginės oro tarpo procedūros ir kt.)?	0		
	10					Ar nustatote bazines kibernetinio saugumo priemones (privalomas arba rekomendacinio pobūdžio), skirtas skaitmeninių paslaugų teikėjams ir visiems sektoriams, nurodytiems TIS direktyvos (2016/1148) II priede?	1				
	11	-		-		Ar teikiate priemones arba metodiką kibernetiniams incidentams nustatyti?	1	-		-	
12. Spręsti kibernetinių nusikaltimų problemą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
12. Spręsti kibernetinių nusikaltimų problemą	1	Ar atlikote tyrimą, siekdami išsiaiškinti teisėsaugos reikalavimus (teisinį pagrindą, išteklius, įgūdžius ir kt.), kad būtų galima veiksmingai kovoti su kibernetiniais nusikaltimais?	1	Ar jūsų nacionalinė teisinė sistema visiškai atitinka susijusią ES teisinę sistemą, įskaitant Direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, pvz., kalbant apie neteisėtą prieigą prie informacinių sistemų, neteisėtą poveikį sistemai, neteisėtą poveikį duomenims, neteisėtą duomenų perėmimą, nusikalstamai veikai vykdyti naudojamas priemones ir pan.?	1	Ar prokuratūrose yra skyriai, atsakingi už kovą su kibernetiniais nusikaltimais?	1	Ar renkate statistinius duomenis pagal Direktyvos 2013/40/ES (Direktyva dėl atakų prieš informacines sistemas) 14 straipsnio 1 dalies nuostatas?	1	Ar rengiate tarpinstitucinius mokymus arba mokymo seminarus teisėsaugos institucijoms, teisėjams, prokurorams ir nacionalinėms ir (arba) vyriausybinėms CSIRT nacionaliniu lygmeniu ir (arba) daugiašaliu lygmeniu?	1
	2	Ar atlikote tyrimą, siekdami išsiaiškinti prokurorams ir teisėjams taikomus reikalavimus (teisinį pagrindą, išteklius, įgūdžius ir kt.), kad būtų galima veiksmingai kovoti su kibernetiniais nusikaltimais?	1	Ar taikote kokias nors teisės nuostatas dėl tapatybės vagysčių internete ir asmens duomenų vagysčių?	1	Ar turite specialų kovos su kibernetiniais nusikaltimais skyriams skirtą biudžetą?	1	Ar renkate atskirus statistinius duomenis apie kibernetinius nusikaltimus, pvz., veiklos statistiką, kibernetinių nusikaltimų tendencijų statistiką, iš kibernetinių nusikaltimų gautų pajamų ir padarytos žalos statistiką ir pan.?	1	Ar dalyvaujate koordinuotoje tarptautinėje veikloje, kuria siekiama sužlugdyti nusikalstamą veiklą (pvz., įsiskverbimas į nusikalstamų įsilaužėlių forumus, organizuotas kibernetinių nusikaltimų grupes, „tamsiojo tinklo“ rinkos ir botnetų išardymas ir kt.)?	1
	3	Ar jūsų šalis pasirašė Europos Tarybos Budapešto konvenciją dėl elektroninių nusikaltimų?	1	Ar taikote kokias nors teisės nuostatas dėl intelektinės nuosavybės ir autorių teisių pažeidimų internete?	1	Ar įsteigėte centrinę įstaigą (subjektą), kuri koordinuoja veiksmus kovos su kibernetiniais nusikaltimais srityje?	1	Ar vertinate teisėsaugos institucijoms, teisminėms institucijoms ir nacionalinių CSIRT darbuotojams rengiamų kovos su kibernetiniais nusikaltimais mokymų tinkamumą?	1	Ar CSIRT, teisėsaugos institucijų ir teisminių institucijų (prokurorų ir teisėjų) pareigos yra aiškiai atskirtos joms bendradarbiaujant kovoje su kibernetiniais nusikaltimais?	1
	4			Ar taikote kokias nors teisės nuostatas, kuriomis būtų kovojama su priekabiavimu internete ar patyčiomis kibernetinėje erdvėje?	1	Ar sukūrėte atitinkamų nacionalinių institucijų, dalyvaujančių kovoje su kibernetiniais nusikaltimais, įskaitant teisėsaugos institucijas, nacionalines CSIRT, bendradarbiavimo mechanizmus?	1	Ar reguliariai vertinate, ar turite pakankamai išteklių (žmogiškųjų išteklių, biudžeto ir priemonių) teisėsaugos institucijų kovos su kibernetiniais nusikaltimais skyriams?	1	Ar jūsų reguliavimo sistema sudaromos palankios sąlygos CSIRT, teisėsaugos institucijų ir teisminių institucijų (prokurorų ir teisėjų) bendradarbiavimui?	1
	5			Ar taikote kokias nors teisės nuostatas dėl su kompiuteriais susijusio sukčiavimo, pvz., ar laikomasi Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų nuostatų?	1	Ar bendradarbiaujate su kitomis valstybėmis narėmis kovos su kibernetiniais nusikaltimais srityje ir dalijatės su jomis informacija?	1	Ar reguliariai vertinate, ar turite pakankamai išteklių (žmogiškųjų išteklių, biudžeto ir priemonių) baudžiamojo persekiojimo institucijų kovos su kibernetiniais nusikaltimais skyriams?	1	Ar dalyvaujate kuriant ir prižiūrint standartizuotas priemones ir metodikas, formas ir procedūras, kuriomis turi būti dalijamasi su ES suinteresuotaisiais subjektais (TI, CSIRT, ENISA, Europolo EC3 ir kt.)?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
12. Spręsti kibernetinių nusikaltimų problemą	6	-		Ar taikote kokias nors teisės nuostatas dėl vaikų apsaugos internete, pvz., ar laikomasi Direktyvos 2011/93/ES ir Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų ir kt. nuostatų?	1	Ar bendradarbiaujate su ES agentūromis (pvz., Europolo EC3, Eurojustu, ENISA) ir dalijatės su jomis informacija kovos su kibernetiniais nusikaltimais srityje?	1	Ar turite specializuotus teismus arba specializuotus teisėjus kibernetinių nusikaltimų byloms nagrinėti?	1	Ar turite kokių nors pažangių mechanizmų, kuriais asmenys būtų atgrasomi nuo polinkio į kibernetinius nusikaltimus ar dalyvavimo juos vykdant?	0
	7	-		Ar nustatėte veikiantį nacionalinį kontaktinį centrą, kuris keistųsi informacija ir atsakytų į kitų valstybių narių skubius prašymus suteikti informaciją, susijusią su Direktyvoje 2013/40/ES (Direktyva dėl atakų prieš informacines sistemas) numatytais teisės pažeidimais?	1	Ar turite tinkamų priemonių kovai su kibernetiniais nusikaltimais (pvz., kibernetinių nusikaltimų taksonomija ir klasifikavimas, elektroninių įrodymų rinkimo priemonės, kompiuterinės ekspertizės priemonės, patikimos dalijimosi platformos ir kt.)?	1	Ar taikote kokias nors nuostatas, kuriomis siekiama suteikti paramą ir pagalbą nuo kibernetinių nusikaltimų nukentėjusiems asmenims (bendriesiems naudotojams, MVĮ, didelėms įmonėms)?	1	Ar jūsų šalis naudoja ES metmenis ir (arba) Teisėsaugos institucijų reagavimo į ekstremaliąsias situacijas protokolą, kad veiksmingai reaguotų į didelio masto kibernetinius incidentus?	0
	8			Ar jūsų teisėsaugos institucijoje yra specialus kovos su kibernetiniais nusikaltimais skyrius?	1	Ar taikote standartines veiklos procedūras elektroniniams įrodymams tvarkyti?	1	Ar esate parengę visų susijusių suinteresuotųjų subjektų (pvz., teisėsaugos institucijų, nacionalinių CSIRT, teisminių institucijų bendruomenių), įskaitant privatųjį sektorių (pvz., esminių paslaugų operatorius, paslaugų teikėjus), tarpinstitucinę sistemą ir bendradarbiavimo mechanizmus, kad prireikus būtų reaguojama į kibernetinius išpuolius?	1	-	
	9			Ar, remdamiesi Budapešto konvencijos 35 straipsniu, paskyrėte visą parą 7 dienas per savaitę veikiantį kontaktinį centrą?	1	Ar jūsų šalis dalyvauja ES agentūrų (pvz., Europolo, Eurojusto, OLAF, CEPOL, ENISA) siūlomose ir (arba) remiamose mokymo programose?	0	Ar jūsų reguliavimo sistema sudaromos palankios sąlygos CSIRT ir teisėsaugos institucijų bendradarbiavimui?	1	-	
	10	-		Ar paskyrėte visą parą 7 dienas per savaitę veikiantį nacionalinį kontaktinį centrą, atsakingą už ES teisėsaugos institucijų reagavimo į ekstremaliąsias situacijas protokolą, kad būtų reaguojama į didelio masto kibernetinius išpuolius?	1	Ar jūsų šalis ketina priimti Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų 2 papildomą protokolą?	0	Ar taikote mechanizmus (pvz., priemones, procedūras), skirtus CSIRT ar teisėsaugos institucijų ir galbūt teisminių institucijų (prokurorų ir teisėjų) keitimuisi informacija ir bendradarbiavimui kovos su kibernetiniais nusikaltimais srityje palengvinti?	1	-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
	11			Ar reguliariai rengiate specializuotus mokymus su kibernetiniais nusikaltimais kovojantiems suinteresuotiesiems subjektams (TI, teisminėms institucijoms, CSIRT), pvz., mokymo kursus, susijusius su bylomis dėl kibernetinių nusikaltimų ir (arba) baudžiamuoju persekiojimu, elektroninių įrodymų rinkimu ir vientisumo užtikrinimu visoje skaitmeninėje kilmės grandinėje ir kompiuterinėje ekspertizėje ir kt.?	1						
	12			Ar jūsų šalis ratifikavo Europos Tarybos Budapešto konvenciją dėl elektroninių nusikaltimų arba prie jos prisijungė?	1			-	-	-	
	13	-		Ar jūsų šalis pasirašė ir ratifikavo Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų papildomą protokolą (dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo)?	0	-	-	-		-	
13. Nustatyti pranešimo apie incidentus mechanizmus	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar taikote neoficialius privačių organizacijų ir nacionalinių institucijų dalijimosi informacija apie kibernetinius incidentus mechanizmus?	1	Ar turite pranešimo apie incidentus sistemą, taikomą visiems TIS direktyvos II priede nurodytiems sektoriams?	1	Ar turite privalomą pranešimo apie incidentus sistemą, kuri veikia praktiškai?	1	Ar turite suderintą pranešimų apie atskirų sektorių incidentus teikimo tvarką?	1	Ar rengiate metinę incidentų ataskaitą?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
13. Nustatyti pranešimo apie incidentus mechanizmus	2	-		Ar įgyvendinote telekomunikacijų paslaugų teikėjams taikomus pranešimo reikalavimus pagal Direktyvos (ES) 2018/1972 40 straipsnį? Direktyvoje reikalaujama, kad valstybės narės užtikrintų, kad viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjai nedelsdami praneštų kompetentingai institucijai apie saugumo incidentą, kuris turėjo didelės įtakos tinklų veikimui arba paslaugų teikimui.	1	Ar esama koordinavimo ir (arba) bendradarbiavimo mechanizmo, skirto pranešimo apie incidentus įpareigojimams, susijusiems su BDAR, TIS direktyvos 40 straipsniu (buvęs 13a straipsnis) ir eIDAS reglamentu, vykdyti?	1	Ar turite pranešimo apie incidentus sistemą, skirtą ne tik numatytiems TIS direktyvoje, bet ir kitiems sektoriams?	1	Ar pranešimus apie incidentus gaunantis subjektas yra parengęs ataskaitą apie kibernetinį saugumą arba kitų rūšių analizę?	1
	3	-		Ar įgyvendinote elektroninių patikimumo užtikrinimo paslaugų teikėjams taikomus pranešimo reikalavimus pagal eIDAS reglamento (Reglamentas (ES) Nr. 910/2014) 19 straipsnį? 19 straipsnyje, be kitų reikalavimų, nustatyta, kad patikimumo užtikrinimo paslaugų teikėjai turi pranešti priežiūros įstaigai apie reikšmingus incidentus ir (arba) pažeidimus.	1	Ar turite tinkamų priemonių informacijos, kuria dalijamasi įvairiais pranešimų teikimo kanalais, konfidencialumui ir vientisumui užtikrinti?	1	Ar vertinate pranešimo apie incidentus procedūrų veiksmingumą (pvz., incidentų, apie kuriuos pranešta atitinkamais kanalais, rodikliai, pranešimo apie incidentus pateikimo laikas ir kt.)?	1	-	
	4	-		Ar įgyvendinote skaitmeninių paslaugų teikėjams taikomus pranešimo reikalavimus pagal TIS direktyvos 16 straipsnį? 16 straipsnyje reikalaujama, kad skaitmeninių paslaugų teikėjai nepagrįstai nedelsdami praneštų kompetentingai institucijai arba nacionalinei CSIRT apie bet kokį incidentą, turintį didelį poveikį III priede nurodytos paslaugos, kurią jie siūlo Sąjungoje, teikimui.	1	Ar turite platformą ir (arba) priemonę ataskaitų teikimo procesui palengvinti?	0	Ar turite bendrą nacionalinio lygio taksonomiją incidentams klasifikuoti ir priežastims kategorizuoti?	0	-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
14. Stiprinti privatumo ir duomenų apsaugą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar atlikote tyrimus arba analizes, siekdami nustatyti tobulintinas sritis, kad būtų geriau apsaugomos piliečių teisės į privatumą?	1	Ar nacionalinė duomenų apsaugos institucija dalyvauja su kibernetiniu saugumu susijusiose probleminėse srityse (pvz., rengiant naujus kibernetinio saugumo įstatymus ir kitus teisės aktus, apibrėžtas būtinąsias apsaugos priemones)?	1	Ar skatinate viešojo ir (arba) privačiojo sektoriaus gerąją patirtį apsaugos priemonių ir integruotosios duomenų apsaugos srityje?	1	Ar reguliariai vertinate, ar turite pakankamai išteklių (žmogiškųjų išteklių, lėšų ir priemonių) duomenų apsaugos institucijai?	1	Ar taikote kokius nors mechanizmus, skirtus naujausiems technologiniams pokyčiams stebėti, kad būtų galima pritaikyti atitinkamas gaires ir teisines nuostatas ir (arba) įsipareigojimus?	1
	2	Ar parengėte teisinį pagrindą nacionaliniu lygmeniu, kad būtų užtikrintas Bendrojo duomenų apsaugos reglamento (Reglamentas (ES) 2016/679) vykdymas, pvz., toliau taikomos arba konkretizuojamos reglamente įtvirtintų taisyklių nuostatos ar apribojimai?	0	-		Ar rengiate informuotumo didinimo ir mokymo programas šia tema?	1	Ar skatinate organizacijas ir įmones gauti sertifikatą pagal ISO/IEC 27701:2019 dėl privatumo informacijos valdymo sistemos (PIVS)?	1	Ar aktyviai dalyvaujate ir (arba) skatinate mokslinių tyrimų ir technologinės plėtros iniciatyvas, susijusias su privatumo didinimo technologijomis (PET)?	0
	3	-		-		Ar koordinuojate pranešimo apie incidentus procedūras su DAA?	1	-		-	
	4	-		-		Ar skatinate ir remiate informacijos saugumo ir privatumo techninių standartų rengimą? Ar jie specialiai pritaikyti mažosioms ir vidutinėms įmonėms (MVĮ)?	0	-		-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
	5	-		-		Ar pateikiate praktines keičiamos apimties gaires, kurios padėtų įvairių rūšių duomenų valdytojams laikytis privatumo ir duomenų apsaugos teisinių reikalavimų ir prievolių?	0	-		-	

4.1.4 4 grupė. Bendradarbiavimas

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
15. Sukurti viešojo ir privačiojo sektorių partnerystę (VPSP)	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar apskritai suprantama, kad VPSP įvairiais būdais prisideda prie kibernetinio saugumo lygio didinimo šalyje, pvz., dalydamosi interesais, susijusiais su kibernetinio saugumo pramonės augimu, bendradarbiaudamos kuriant atitinkamą kibernetinio saugumo reguliavimo sistemą, skatindamos mokslinius tyrimus ir technologinę plėtrą ir pan.?	1	Ar turite nacionalinį VPSP kūrimo veiksmų planą?	1	Ar esate sukūrę nacionalinių viešojo ir privačiojo sektorių partneryščių?	1	Ar esate sukūrę tarpsektorinių VPSP?	1	Turint omenyje naujausius technologinius ir reguliavimo pokyčius, ar galite pritaikyti arba kurti VPSP?	1
	2	-		Ar sudarote teisinį arba sutartinį pagrindą (konkretūs įstatymai, nacionalinės paskirtosios institucijos, intelektinė nuosavybė) VPSP taikymo sričiai?	1	Ar esate sukūrę konkrečių sektorių VPSP?	1	Ar sukurtose VPSP taip pat daug dėmesio skiriate viešojo ir privačiojo sektorių bendradarbiavimui?	1		
	3	-		–		Ar teikiate finansavimą VPSP kurti?	1	Ar skatinate VPSP tarp mažųjų ir vidutinių įmonių (MVĮ)?	1	-	
	4	-		–		Ar viešosios institucijos apskritai vadovauja VPSP (t. y. įsteigtas vienas viešojo sektoriaus kontaktinis centras, valdantis ir koordinuojantis VPSP, viešosios įstaigos iš anksto susitaria dėl to, ką nori pasiekti, parengtos aiškios viešojo administravimo institucijų gairės dėl jų poreikių ir apribojimų privačiajame sektoriuje ir kt.)?	1	Ar vertinate VPSP rezultatus?	1	-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
15. Sukurti viešojo ir privačiojo sektorių partnerystę (VPSP)	5	-		–		Ar priklausote Europos kibernetinio saugumo organizacijos (EKSO) sutartinei viešojo ir privačiojo sektorių partnerystei (SVPSP)?	0	-		-	
	6	-		-		Ar turite vieną arba kelias VPSP, kurios rūpinasi CSIRT?	0	-		-	
	7					Ar turite vieną arba kelias VPSP, dirbančias su ypatingos svarbos informacinės infrastruktūros apsaugos klausimais?	0				
	8	-		-		Ar turite vieną arba kelias VPSP, kurios siekia didinti informuotumą kibernetinio saugumo klausimais ir ugdyti įgūdžius?	0	-		-	
16. Įforminti viešųjų agentūrų bendradarbiavimą	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar turite neoficialių viešųjų agentūrų bendradarbiavimo kanalų?	1	Ar turite nacionalinę kibernetinio saugumo klausimams skirtą bendradarbiavimo programą (pvz., patariamosios tarybos, iniciatyvinės grupės, forumai, tarybos, kibernetiniai centrai ar ekspertų posėdžių grupės)?	1	Ar bendradarbiavimo programoje dalyvauja valdžios institucijos?	1	Ar užtikrinate, kad kibernetiniam saugumui skirti bendradarbiavimo kanalai būtų bent tarp šių viešųjų įstaigų: žvalgybos tarnybos, vidaus teisėsaugos institucijos, prokuratūros, vyriausybės subjektų, nacionalinės CSIRT ir karinių subjektų?	1	Ar viešosioms agentūroms teikiama vienoda būtiniausia informacija apie naujausius pokyčius grėsmių aplinkoje ir informuotumą apie kibernetinio saugumo padėtį?	1
	2	-		-		Ar esate sukūrę bendradarbiavimo platformų, kuriose keičiamasi informacija?	1	Ar vertinate įvairių bendradarbiavimo programų pasiekimus ir ribotumus skatinant veiksmingą bendradarbiavimą?	1	-	

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
16. Įforminti viešųjų agentūrų bendradarbiavimą	3	-		-		Ar apibrėžėte bendradarbiavimo platformų taikymo sritį (pvz., užduotys ir pareigos, klausimų sričių skaičius)?	1	-		-	
	4	-		-		Ar rengiate metinius posėdžius?	1	-		-	
	5	-		-		Ar turite įvairių geografinių regionų kompetentingų institucijų bendradarbiavimo mechanizmų, pvz., saugumo korespondentų tinklą kiekviename regione, kibernetinio saugumo pareigūną regioniniuose ekonomikos rūmuose ir pan.?	1	-		-	
17. Dalyvauti tarptautiniame bendradarbiavime (ne tik su ES valstybėmis narėmis)	a	Ar šis tikslas įtrauktas į jūsų dabartinę NKSS, ar planuojate jį įtraukti į kitą leidimą?	1	Ar turite neoficialią praktiką arba priemones, padedančias nekoordinuotai siekti tikslo?	1	Ar turite oficialiai apibrėžtą ir dokumentais pagrįstą veiksmų planą?	1	Ar peržiūrite savo veiksmų planą siekdami išbandyti jo veiksmingumą?	1	Ar turite mechanizmus, užtikrinančius, kad veiksmų planas būtų dinamiškai pritaikomas prie aplinkos pokyčių?	1
	b			Ar savo veiksmų plane apibrėžėte numatomus rezultatus, pagrindinius principus arba pagrindinę veiklą?	1	Ar turite veiksmų planą, kuriame numatytas aiškus išteklių paskirstymas ir valdymas?	1	Ar peržiūrite savo veiksmų planą, siekdami užtikrinti, kad jis būtų su tinkamais prioritetais ir optimalus?	1		
	c			Jei taikytina, ar jūsų veiksmų planas įgyvendintas ir tam tikru mastu jau yra veiksmingas?	0						
	1	Ar turite tarptautinio dalyvavimo strategiją?	1	Ar esate sudarę bendradarbiavimo susitarimų su kitomis šalimis (dvišalių, daugiašalių) arba partneriais kitose šalyse, pvz., dėl dalijimosi informacija, gebėjimų stiprinimo, paramos ir kt.?	1	Ar keičiatės informacija strateginiu lygmeniu, pvz., aukšto lygio politikos, rizikos suvokimo ir kt. srityse?	1	Ar jūsų šalies nacionalinės kibernetinio saugumo viešosios agentūros dalyvauja tarptautinio bendradarbiavimo programose?	1	Ar vadovaujate diskusijoms viena ar keliomis daugiašalių susitarimų temomis?	1
	2	Ar turite neoficialių bendradarbiavimo su kitomis šalimis kanalų?	1	Ar turite vieną bendrą kontaktinį punktą, kuris gali atlikti ryšių palaikymo funkciją, kad užtikrintų tarpvalstybinį bendradarbiavimą su valstybių narių institucijomis (bendradarbiavimo grupe, CSIRT tinklu ir pan.)?	1	Ar keičiatės informacija taktiniu lygmeniu (pvz., grėsmės subjektų biuletenis, ISAC, TTP ir kt.)?	1	Ar reguliariai vertinate tarptautinio bendradarbiavimo iniciatyvų rezultatus?	1	Ar rengiate diskusijas viena ar keliomis tarptautinių sutarčių ar konvencijų temomis?	1

NKSS tikslas	#	1 lygis	R	2 lygis	R	3 lygis	R	4 lygis	R	5 lygis	R
17. Dalyvauti tarptautiniame bendradarbiavime (ne tik su ES valstybėmis narėmis)	3	Ar viešojo sektoriaus vadovybė išreiškė ketinimą dalyvauti tarptautiniame bendradarbiavime kibernetinio saugumo srityje?	1	Ar turite atsidavusių žmonių, dalyvaujančių tarptautiniame bendradarbiavime?	1	Ar keičiatės informacija veiklos lygmeniu, pvz., veiklos koordinavimo informacija, informacija apie vykstančius incidentus, IOC ir kt.?	1	-		Ar vadovaujate diskusijoms ar deryboms viena ar daugiau temų tarptautinėse ekspertų grupėse, pvz., Pasaulinėje kibernetinės erdvės stabilumo komisijoje (GCSC), ENISA TIS bendradarbiavimo grupėje, JT vyriausybės ekspertų informacijos saugumo klausimais grupėje (GGE) ir pan.?	1
	4	-		-		Ar dalyvaujate tarptautinėse kibernetinio saugumo pratybose?	1	-		-	
	5	-		-		Ar dalyvaujate tarptautinėse gebėjimų stiprinimo iniciatyvose, pvz., mokymo, įgūdžių ugdymo, standartinių procedūrų rengimo ir pan.?	0	-		-	
	6	-		-		Ar esate sudarę savitarpio pagalbos susitarimų su kitomis šalimis, pvz., dėl teisėsaugos institucijų veiklos, teismo procesų, reagavimo į incidentus pajėgumų pasidalijimo, dalijimosi kibernetinio saugumo ištekliais ir kt.?	0	-		-	
	7	-		-		Ar pasirašėte arba ratifikavote tarptautines sutartis ar konvencijas kibernetinio saugumo srityje, pvz., Tarptautinį informacijos saugumo elgesio kodeksą, Konvenciją dėl elektroninių nusikaltimų?	0	-		-	

4.2 NAUDOJIMOSI SISTEMA GAIRĖS

Šiame skirsnyje siekiama pateikti valstybėms narėms tam tikras gaires ir rekomendacijas dėl sistemos diegimo ir klausimyno pildymo. Toliau išvardytos rekomendacijos daugiausia grindžiamos grįžtamąja informacija, gauta per pokalbius su valstybių narių atstovais:

- **Numatykite koordinavimo veiklą, kad galėtumėte rinkti ir konsoliduoti duomenis.** Dauguma valstybių narių pripažįsta, kad toks įsivertinimas turėtų užtrukti apie 15 vieno žmogaus darbo dienų. Atliekant įsivertinimą, reikės kreiptis į daug įvairių suinteresuotųjų subjektų. Todėl rekomenduojama skirti laiko pasirengimo etapui, kad būtų nustatyti visi atitinkami vyriausybinių institucijų, viešųjų agentūrų ir privačiojo sektoriaus suinteresuotieji subjektai.
- **Nustatykite centrinę įstaigą, atsakingą už įsivertinimą nacionaliniu lygmeniu.** Kadangi renkant informaciją apie visus NPVS rodiklius turi dalyvauti daug suinteresuotųjų subjektų, rekomenduojama įsteigti centrinę įstaigą ar agentūrą, kuriai būtų pavesta atlikti įsivertinimą palaikant ryšius ir koordinuojant veiksmus su visais atitinkamais suinteresuotaisiais subjektais.
- **Naudokite vertinimo procedūrą kaip būdą dalytis informacija ir bendrauti kibernetinio saugumo temomis.** Valstybių narių įgyta patirtis atskleidė, kad diskusijos (nesvarbu, ar būtų rengiami atskiri pokalbiai, ar kolektyviniai seminarai) yra gera galimybė skatinti dialogą kibernetinio saugumo klausimais ir dalytis nuomonėmis ir informacija apie tobulintinas sritis. Dalijimasis rezultatais ne tik atskleidžia pagrindinius pasiekimus, bet ir gali padėti skatinti nagrinėti kibernetinio saugumo temas.
- **Naudokitės NKSS kaip galimybe pasirinkti vertintinus tikslus.** NPVS sudarantys 17 tikslų grindžiami tikslais, kurių valstybės narės paprastai siekia savo NKSS. Į NKSS įtraukti tikslai turėtų būti naudojami kaip vertinimo priemonė. Tačiau NKSS neturėtų riboti vertinimo. Kadangi NKSS daugiausia dėmesio skiriama prioritetams, tam tikros sritys į NKSS sąmoningai neįtrauktos. Tačiau tai nereiškia, kad konkrečių pajėgumų nėra. Pavyzdžiui, tuo atveju, kai konkretus tikslas nėra įtrauktas į NKSS, tačiau šalis turi su tuo tikslu susijusių kibernetinio saugumo pajėgumų, tas tikslas gali būti vertinamas.
- **Kintant NKSS aprėpčiai, užtikrinkite, kad balų aiškinimas ir toliau atitiktų NKSS raidą.** NKSS gyvavimo ciklas yra daugiametis procesas. Kai kurių valstybių narių NKSS įgyvendinimas paprastai užtikrinamas 3–5 metų trukmės veiksmų gairėmis, kurių taikymo sritis keičiama tarp dviejų nuoseklių NKSS leidimų. Šiuo požiūriu, pateikiant įsivertinimo rezultatus tarp dviejų NKSS leidimų, reikia būti ypač apdairiems: aprėpties pokyčiai iš tiesų gali turėti įtakos galutiniam brandos balui. Rekomenduojama palyginti visos strateginių tikslų aprėpties balus skirtingais metais (t. y. bendrą balą).

Priminimas apie vertinimo balais mechanizmą – aprėpties koeficiento pavyzdys

Vertinimo balais mechanizmą sudaro du balų lygmenys:
(i) **bendras aprėpties koeficientas**, grindžiamas išsamiu strateginių tikslų sąrašu, pateiktu įsivertinimo sistemoje;
(ii) **bendras konkretus aprėpties koeficientas**, grindžiamas valstybės narės pasirinktais strateginiais tikslais (paprastai atitinkančiais konkrečios šalies NKSS nustatytus tikslus).

Pagal struktūrą (žr. 3.1 skirsnį apie vertinimo balais mechanizmą) bendras konkretus aprėpties koeficientas bus lygus bendram aprėpties koeficientui arba už jį didesnis, nes vėliau gali būti įtraukti tikslai, kurių valstybė narė neįtraukė ir dėl to bendras aprėpties koeficientas sumažėjo. Valstybei narei įtraukus naują tikslą, bendras aprėpties koeficientas padidės (t. y. bus daugiau apimamų brandos rodiklių), o bendras konkretus brandos lygis gali sumažėti (jei naujai įtrauktas tikslas yra pradiniame etape ir todėl jo brandos lygis žemas).

- **Pildydami įsivertinimo klausimyną, nepamirškite, kad pagrindinis tikslas yra padėti valstybėms narėms stiprinti kibernetinio saugumo gebėjimus.** Todėl net jei kai kuriais atvejais, atliekant įsivertinimą, gali būti sunku tiksliai atsakyti į klausimą, rekomenduojama pasirinkti bendrai priimtiniausią atsakymą. Jei, pvz., vienoje taikymo srityje atsakymas į klausimą yra TAIP, o kitoje – NE, valstybės narės turėtų nepamiršti, kad atsakius NE reikia imtis veiksmų: arba taisomojo plano, arba plano imtis veiksmų tobulintinoje srityje, ir į tai būtina atsižvelgti ateityje.

5. KITI ETAPAI

5.1 BŪSIMI PATOBULINIMAI

Per pokalbius su valstybių narių atstovais ir dokumentų tyrimo etape kaip galimi būsimi pokyčiai taip pat buvo parengtos šios rekomendacijos, kaip patobulinti dabartinę nacionalinių pajėgumų vertinimo sistemą:

- **Sukurti vertinimo balais sistemą, kad būtų galima užtikrinti didesnį tikslumą.** Pavyzdžiui, būtų galima nustatyti aprėpties procentinę dalį, o ne dvinarį atsakymą TAIP / NE, kad būtų geriau atsižvelgiama į pajėgumų konsolidavimo nacionaliniu lygmeniu sudėtingumą. Pirmiausia pasirinktas paprastas metodas su atsakymais TAIP ir NE.
- **Nustatyti kiekybinius valstybių narių NKSS veiksmingumo vertinimo parametrus.** Iš tiesų nacionalinių pajėgumų vertinimo sistemoje daugiausia dėmesio skiriama valstybių narių kibernetinio saugumo pajėgumų brandos lygio vertinimui. Tai galėtų būti papildyta parametrais, pagal kuriuos būtų vertinamas valstybių narių įgyvendinamų veiksmų ir veiksmų planų, skirtų šiems pajėgumams stiprinti, veiksmingumas. Neatrodo, kad būtų realu sukurti tokius veiksmingumo parametrus dabartiniame etape, atsižvelgiant į tai, kad yra mažai grįžtamosios informacijos šioje srityje, sunku rasti reikšmingų rodiklių, kurie susietų rezultatus su NKSS įgyvendinimu, ir nustatyti realius rodiklius, kuriuos vėliau būtų galima surinkti. Tačiau tai tebėra būsimo darbo tema.
- **Pereiti nuo įsivertinimo prie vertinimo metodo.** Ateityje sistema galėtų kisti pereinant prie vertinimo metodo, kad būtų galima nuosekliau įvertinti valstybių narių kibernetinio saugumo pajėgumų brandą. Jei vertinimą atliktų trečioji šalis, būtų galima sumažinti galimą šališkumą.

A PRIEDAS. DOKUMENTŲ TYRIMO REZULTATŲ APŽVALGA

A priede pateikiama ENISA ankstesnio darbo NKSS srityje santrauka ir atitinkamų viešai prieinamų kibernetinio saugumo pajėgumų brandos modelių peržiūra. Atrenkant ir peržiūrint modelius atsižvelgiama į šias prielaidas:

- ne visi modeliai grindžiami griežta mokslinių tyrimų metodika;
- modelių struktūra ir rezultatai ne visada išsamiai paaiškinami pateikiant aiškias sąsajas tarp skirtingų kiekvieną modelį apibūdinančių elementų;
- kai kuriuose modeliuose nepateikiama išsamios informacijos apie kūrimo procesą, struktūrą ir vertinimo metodiką;
- kituose mūsų rastuose modeliuose ir priemonėse nepateikiama jokios informacijos apie struktūrą ir turinį, todėl jie nėra išvardyti;
- peržiūros modeliai atrenkami atsižvelgiant į geografinę aprėptį. Pagrindinis dėmesys bus skiriamas kibernetinio saugumo pajėgumų, sukurtų siekiant įvertinti Europos šalių veiklos rezultatus, brandos modeliams. Vis dėlto svarbu išplėsti geografinę aprėptį, kad būtų galima nagrinėti gerąją patirtį kuriant brandos modelius visame pasaulyje.

Ši atitinkamų viešai prieinamų kibernetinio saugumo pajėgumų brandos modelių sisteminė apžvalga parengta naudojant individualizuotą analizės sistemą, pagrįstą J. Beckerio nustatyta brandos modelių kūrimo metodika[22]. Buvo nagrinėjami šie kiekvieno esamo brandos modelio elementai:

- **brandos modelio pavadinimas –** brandos modelio pavadinimas ir pagrindinės nuorodos;
- **institucijos šaltinis –** viešoji arba privati institucija, atsakinga už modelio kūrimą;
- **bendroji paskirtis ir tikslas –** bendra modelio taikymo sritis ir numatomas (-i) tikslas (-ai);
- **lygių skaičius ir apibrėžtis –** modelio brandos lygių skaičius ir jų bendrasis aprašymas;
- **požymių skaičius ir pavadinimai –** požymių, kurie naudojami taikant brandos modelį, skaičius ir pavadinimai. Požymių analizės tikslas yra trejopas:
  - suskirstyti brandos modelį į lengvai suprantamas dalis,
  - sujungti kelis požymius į tą patį tikslą atitinkančių požymių grupes,
  - pateikti skirtingą požiūrį į brandos lygį;
- **vertinimo metodas –** brandos modelio vertinimo metodas;
- **rezultatų pateikimas –** brandos modelio rezultatų pateikimo metodas. Šio etapo logika yra tokia: brandos modeliai būna nesėkmingi, jei yra pernelyg sudėtingi, todėl pateikimo būdas turi atitikti praktinius poreikius.

[22] Becker, J., Knackstedt, R., Pöppelbuß, J. Developing Maturity Models for IT Management: A Procedure Model and its Application. Business & Information Systems Engineering, vol. 1, no. 3, p. 213–222, Jun. 2009.
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

Ankstesnis darbas, susijęs su NKSS

2012 m. ENISA, dėdama pirmąsias pastangas, paskelbė du dokumentus NKSS tema. Pirma, NKSS kūrimo ir vykdymo etapo praktiniame vadove[23] pasiūlyti konkretūs veiksmai, kad NKSS būtų įgyvendinama sėkmingai, ir pristatomi keturi NKSS gyvavimo ciklo etapai: strategijos kūrimas, strategijos įgyvendinimas, strategijos vertinimas ir strategijos palaikymas. Antra, dokumente „Nacionalinių pastangų stiprinti kibernetinės erdvės saugumą krypties nustatymas“[24] nustatytas 2012 m. kibernetinio saugumo strategijų statusas ES ir už jos ribų ir pasiūlyta, kad valstybės narės savo NKSS nustatytų bendras temas ir skirtumus.

2014 m. paskelbta pirmoji ENISA sistema, skirta valstybės narės NKSS vertinti[25]. Šioje sistemoje pateikiamos rekomendacijos ir gerosios patirties pavyzdžiai, taip pat NKSS vertinimo gebėjimų stiprinimo priemonės (pvz., nustatyti tikslai, indėliai, išdirbiai, pagrindiniai veiklos rodikliai ir kt.). Tos priemonės strateginio planavimo etape pritaikytos įvairiems šalių poreikiams skirtinguose brandos lygiuose. Tais pačiais metais ENISA paskelbė internetinį NKSS interaktyvųjį žemėlapį[26], kuriame naudotojai gali greitai susipažinti su visų valstybių narių ir ELPA šalių NKSS, įskaitant jų strateginius tikslus ir tinkamus įgyvendinimo pavyzdžius. Ši NKSS saugykla (2014 m.) atnaujinta – 2018 m. joje pateikta įgyvendinimo pavyzdžių, o nuo 2019 m. žemėlapis veikia kaip *centrinė informacijos saugykla*, skirta valstybių narių teikiamiems duomenims apie jų pastangas didinti nacionalinį kibernetinį saugumą centralizuoti.

2016 m. paskelbtame „NKSS gerosios patirties vadove“ nustatyta penkiolika strateginių tikslų[27]. Šiame vadove taip pat analizuojama kiekvienos valstybės narės NKSS įgyvendinimo padėtis ir nustatomi įvairūs šio įgyvendinimo trūkumai ir uždaviniai.

2018 m. ENISA paskelbė „Nacionalinių kibernetinio saugumo strategijų vertinimo priemonę“[28] – interaktyvią įsivertinimo priemonę, skirtą padėti valstybėms narėms įvertinti savo strateginius prioritetus ir tikslus, susijusius su NKSS. Šia priemone, pasitelkiant paprastų klausimų rinkinį, valstybėms narėms teikiamos konkrečios kiekvieno tikslo įgyvendinimo rekomendacijos. Galiausiai 2019 m. paskelbtame leidinyje „Kibernetinio saugumo inovacijų taikymo geroji patirtis pagal NKSS“[29] pristatomos NKSS teikiamos inovacijos kibernetinio saugumo srityje. Siekiant padėti parengti būsimus novatoriškus strateginius tikslus, dokumente išdėstyti su įvairiais inovacijų aspektais susiję uždaviniai ir geroji patirtis, kaip juos supranta dalyko ekspertai.

A.1 Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis (CMM)

Valstybėms skirtą kibernetinio saugumo gebėjimų brandos modelį (CMM) parengė Visuotinis kibernetinio saugumo gebėjimų centras (Gebėjimų centras), priklausantis Oksfordo universiteto Oksfordo Martino mokyklai. Gebėjimų centro tikslas – Jungtinėje Karalystėje ir tarptautiniu mastu plėsti kibernetinio saugumo gebėjimų stiprinimo mastą ir veiksmingumą diegiant kibernetinio saugumo gebėjimų brandos modelį (CMM). CMM tiesiogiai skirtas šalims, norinčioms stiprinti savo nacionalinius kibernetinio saugumo gebėjimus. 2014 m. įdiegtas CMM

[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), atnaujinta 2019 m.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Šiuo dokumentu atnaujinamas 2012 m. vadovas: 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

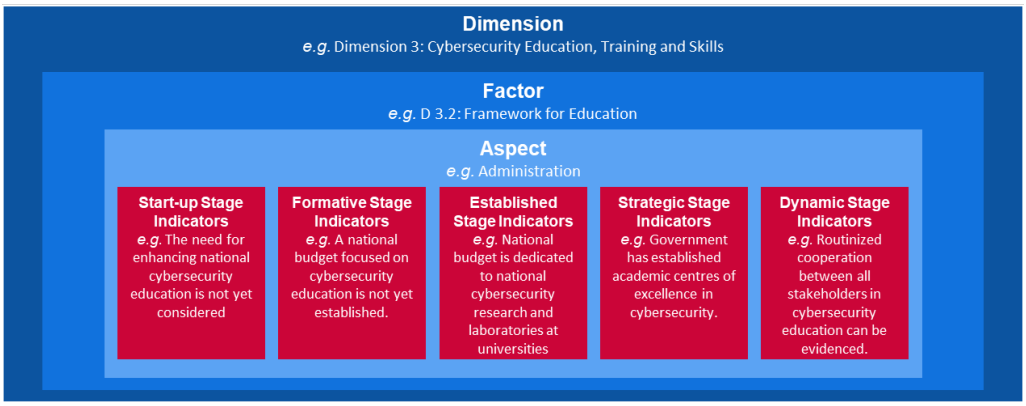
peržiūrėtas 2016 m. – po to, kai buvo panaudotas 11 nacionalinių kibernetinio saugumo gebėjimų peržiūrai.

Požymiai / matmenys

CMM laikoma, kad kibernetinio saugumo gebėjimai aprėpia **penkis matmenis**, atspindinčius kibernetinio saugumo gebėjimų grupes. Kiekviena grupė atspindi skirtingas analizės kryptis, padedančias nagrinėti ir suprasti kibernetinio saugumo gebėjimus. Atsižvelgiant į penkis matmenis, kibernetinio saugumo gebėjimų turėjimas apibūdinamas **veiksniais**. Šie elementai padeda didinti kiekvieno matmens kibernetinio saugumo gebėjimų brandą. Skirtingus kiekvieno veiksnio komponentus atspindi keli **aspektai**. Aspektai sudaro organizacinį metodą, pagal kurį rodikliai skirstomi į mažesnes grupes, kurias lengviau suprasti. Tada kiekvienas aspektas įvertinamas pasitelkiant **rodiklius**, kuriais apibūdinami etapai, veiksmai arba sudedamosios dalys, būdingi konkrečiam brandos etapui (apibrėžtam kitame skirsnyje), atsižvelgiant į konkretų aspektą, veiksnį ir matmenį.

Minėtieji terminai gali būti išdėstyti sluoksniais, kaip parodyta toliau paveiksle.

4 pav. CMM rodiklių pavyzdys



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Matmuo, pvz., 3 matmuo. Švietimas, mokymas ir įgūdžiai kibernetinio saugumo srityje
Factor e.g. D 3.2: Framework for Education	Veiksnys, pvz., 3.2. Švietimo sistema
Aspect e.g. Administration	Aspektas, pvz., administravimas
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Pradžios etapo rodikliai, pvz., nacionalinio švietimo kibernetinio saugumo klausimais stiprinimas dar nesvarstomas
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Formavimo etapo rodikliai, pvz., nacionalinis biudžetas švietimui kibernetinio saugumo klausimais dar neskirtas
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Įtvirtinimo etapo rodikliai, pvz., nacionaliniams kibernetinio saugumo tyrimams ir laboratorijoms universitetuose paskirtas nacionalinis biudžetas
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Strateginio etapo rodikliai, pvz., vyriausybė įsteigė kibernetinio saugumo švietimo akademinį kompetencijos centrą
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Dinaminio etapo rodikliai, pvz., nusistovėjęs visų suinteresuotųjų subjektų bendradarbiavimas

Toliau išsamiau apibūdinami penki matmenys:

i Kibernetinio saugumo politikos ir strategijos rengimas (6 veiksniai)
ii Atsakingos kibernetinio saugumo kultūros skatinimas visuomenėje (5 veiksniai)
iii Žinių apie kibernetinį saugumą plėtojimas (3 veiksniai)
iv Veiksmingų teisinių ir reguliavimo sistemų kūrimas (3 veiksniai)
v Rizikos kontrolė pasitelkiant standartus, organizacijas ir technologijas (7 veiksniai)

Brandos lygiai

Siekiant nustatyti, kokią pažangą šalis padarė pagal tam tikrą kibernetinio saugumo gebėjimų veiksnį ir (arba) aspektą CMM naudojami **5 brandos lygiai**. Šie lygiai atspindi esamus kibernetinio saugumo gebėjimus:

- **Pradinis.** Kibernetinio saugumo brandos nėra arba yra tik jos užuomazgos. Galbūt vyksta pradinės diskusijos dėl kibernetinio saugumo gebėjimų kūrimo, tačiau konkrečių veiksmų nesiimta. Šiame etape nėra jokių pastebimų įrodymų.
- **Formavimas.** Kai kurie aspektų požymiai ryškėja ir yra formuojami, tačiau jie gali būti *ad hoc*, netvarkingi, netiksliai apibrėžti arba tiesiog nauji. Vis dėlto yra aiškių šios veiklos įrodymų.
- **Įtvirtinimas.** Aspekto elementai yra nustatyti ir veikia. Tačiau santykinis išteklių paskirstymas nėra iki galo apgalvotas. Priimta mažai kompromisinių sprendimų dėl „santykinių“ investicijų į įvairius šio aspekto elementus. Vis dėlto aspektas yra funkcionalus ir apibrėžtas.
- **Strateginis.** Nuspręsta, kurios aspekto dalys yra svarbios ir kurios mažiau svarbios konkrečiai organizacijai ar šaliai. Strateginis etapas atspindi tai, kad šie sprendimai priimti atsižvelgiant į konkrečias šalies ar organizacijos aplinkybes.
- **Dinaminis.** Šiame etape jau įdiegti aiškūs mechanizmai strategijai keisti atsižvelgiant į vyraujančias aplinkybes, pvz., grėsmių aplinkos technologijas, pasaulinį konfliktą arba svarbius pokyčius vienoje iš susirūpinimą keliančių sričių (pvz., kibernetinių nusikaltimų ar privatumo). Dinamiškos organizacijos yra parengusios strategijų keitimo metodus. Šio etapo požymiai – greitas sprendimų priėmimas, išteklių perskirstymas ir nuolatinis dėmesys kintančiai aplinkai.

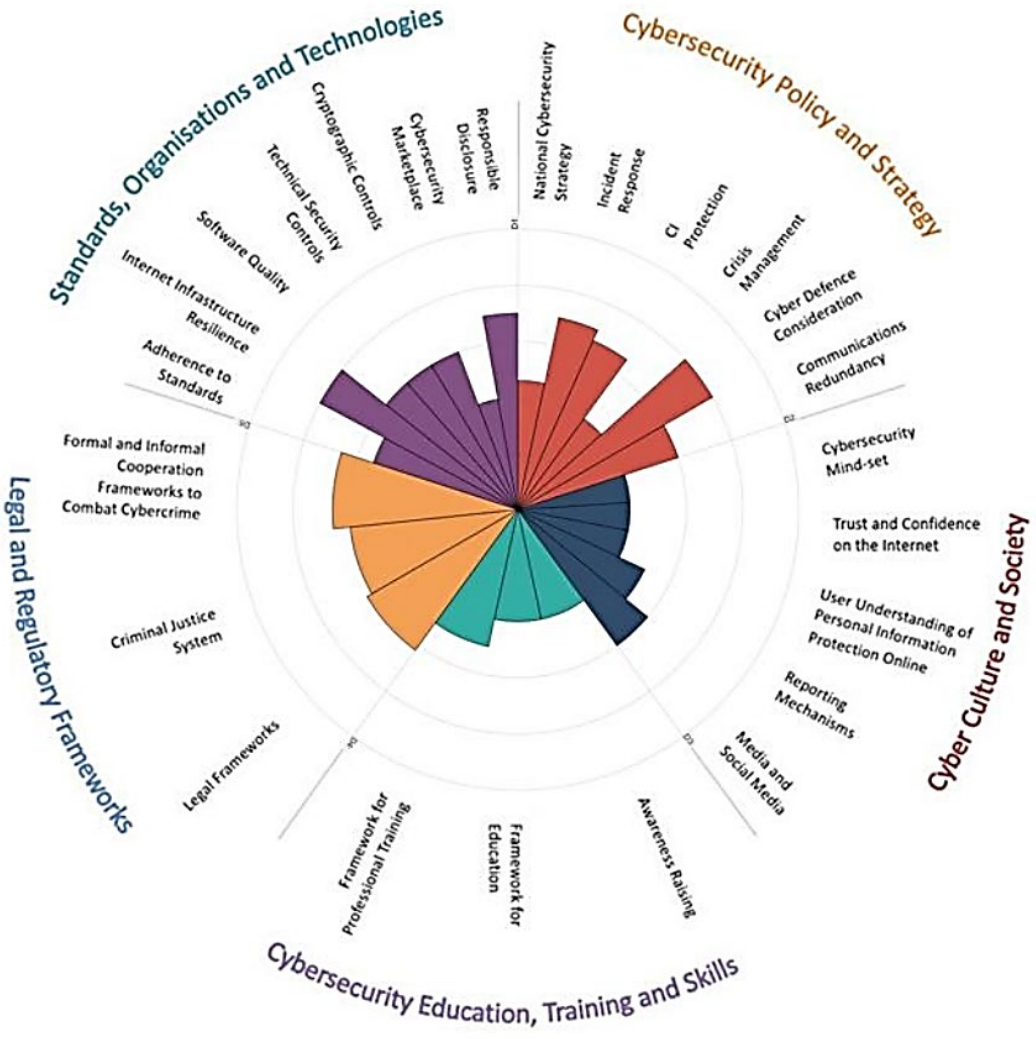
Vertinimo metodas

Kadangi Gebėjimų centras nėra išsamiai susipažinęs su kiekvienos šalies aplinkybėmis, kuriomis modelis diegiamas, jis bendradarbiauja su tarptautinėmis organizacijomis, priimančiosiomis ministerijomis ar organizacijomis atitinkamoje šalyje, siekdamas peržiūrėti kibernetinio saugumo gebėjimų brandą. Siekdamas įvertinti penkių į CMM įtrauktų matmenų brandos lygį, Gebėjimų centras ir priimančioji organizacija 2–3 dienas susitikinėja su atitinkamais nacionaliniais viešojo ir privačiojo sektorių suinteresuotaisiais subjektais, kad suburtų tikslines grupes CMM matmenų klausimams spręsti. Kiekvieną matmenį bent du kartus aptaria skirtingos suinteresuotųjų subjektų grupės. Taip sudaromas preliminarus vėlesniam vertinimui reikalingų duomenų rinkinys.

Rezultatų pateikimo būdas

Taikant CMM apžvelgiamas kiekvienos šalies brandos lygis naudojant radarą, sudarytą iš penkių dalių – po vieną kiekvienam matmeniui. Kiekvienas matmuo sudaro penktadalį grafiko, o penki kiekvieno veiksnio brandos etapai tęsiasi nuo grafiko vidurio; kaip parodyta toliau, pradžios etapas yra arčiausiai grafiko vidurio, o dinaminis – prie jo išorinės ribos.

5 pav. CMM. Rezultatų apžvalga



Standards, Organisations and Technologies	Standartai, organizacijos ir technologijos
Legal Regulatory Frameworks	Teisinės reguliavimo sistemos
Cybersecurity Education, Training and Skills	Švietimas, mokymas ir įgūdžiai kibernetinio saugumo srityje
Cybersecurity Policy and Strategy	Kibernetinio saugumo politika ir strategija
Cyber Culture and Society	Kibernetinė kultūra ir visuomenė
Responsible Disclosure	Atsakingas informacijos atskleidimas
Cybersecurity market place	Kibernetinio saugumo rinka
Cryptographic Controls	Kriptografiniai valdikliai
Software Quality	Programinės įrangos kokybė
Internet Infrastructure Resilience	Interneto infrastruktūros atsparumas
Adherence to Standards	Standartų laikymasis
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Oficialios ir neoficialios bendradarbiavimo sistemos kovojant su kibernetiniais nusikaltimais
Criminal Justice System	Baudžiamosios teisenos sistema
Legal Frameworks	Teisinės sistemos
Framework for Professional Training	Profesinio mokymo sistema
Framework for Education	Švietimo sistema
Awareness Raising	Informuotumo didinimas
Media and Social Medai	Žiniasklaida ir socialinė žiniasklaida
Reporting Mechanisms	Ataskaitų teikimo mechanizmai
User Understanding of Personal Information Protection Online	Naudotojo supratimas apie asmens duomenų apsaugą internete
Trust and Confidence on the Internet	Pasitikėjimas internetu
Cybersecurity Mind-set	Kibernetinio saugumo samprata
Communications Redundancy	Ryšių perteklius
Cyber Defence Consideration	Kibernetinės gynybos klausimas
Crisis Management	Krizių valdymas
CI Protection	Ypatingos svarbos infrastruktūros apsauga
Incident Response	Reagavimas į incidentus
National Cybersecurity Strategy	Nacionalinė kibernetinio saugumo strategija

Visuotinis kibernetinio saugumo gebėjimų centras, Oksfordo Martino mokykla, Oksfordo universitetas, 2017 m.

A.2 Kibernetinio saugumo pajėgumų brandos modelis (C2M2)

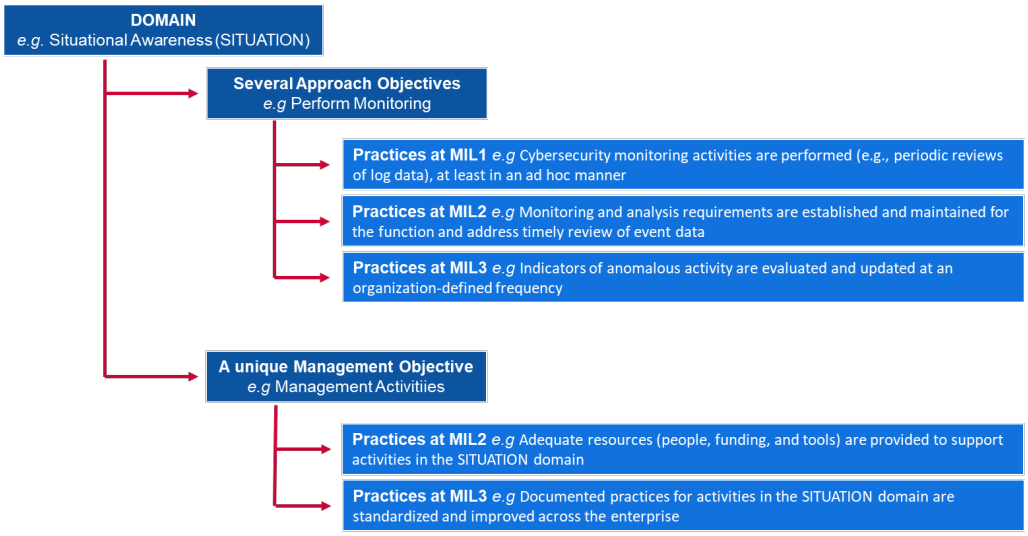
JAV energetikos departamentas, bendradarbiaudamas su privačiojo ir viešojo sektorių ekspertais, parengė kibernetinio saugumo pajėgumų brandos modelį (C2M2). Gebėjimų centro tikslas – padėti visų sektorių, rūšių ir dydžių organizacijoms įvertinti ir tobulinti savo kibernetinio saugumo programas ir didinti veiklos atsparumą. C2M2 daugiausia dėmesio skiriama kibernetinio saugumo praktikos, susijusios su informacijos, informacinių technologijų (IT) ir operacijų technologijų (OT) ištekliais ir aplinka, kurioje jos veikia, įgyvendinimui ir valdymui. C2M2 brandos modeliai apibrėžiami taip: „savybių, požymių, rodiklių ar modelių rinkinys, atspindintis pajėgumą ir pažangą tam tikroje srityje“. C2M2, iš pradžių įdiegtas 2014 m., buvo peržiūrėtas 2019 m.

Požymiai / matmenys

C2M2 atsižvelgiama į **dešimt sričių**, atspindinčių logišką kibernetinio saugumo praktikos rūšių grupavimą. Kiekviena praktika – tai veikla, kurią organizacija gali vykdyti, kad sukurtų ir parengtų pajėgumus šioje srityje. Tada kiekviena sritis susiejama su **išskirtiniu valdymo tikslu** ir **keliais metodo tikslais**. Atsižvelgiant tiek į metodą, tiek į valdymo tikslus, pasitelkiant **kelių rūšių praktiką** išsamiai aprašoma įforminta veikla.

Šių sąvokų ryšys apibendrinamas toliau:

6 pav. C2M2 rodiklio pavyzdys



Domain eg Situational Awareness (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency
A unique Management Objectve e.g. Management Activities
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise

Sritis, pvz., informuotumas apie padėtį (PADĖTIS)
Keletas metodo tikslų, pvz., stebėsenos vykdymas
1 BRL praktika, pvz., kibernetinio saugumo stebėsenos veikla (pvz., periodinė surašytų duomenų peržiūra), vykdoma bent *ad hoc*
2 BRL praktika, pvz., nustatomi ir palaikomi stebėsenos ir analizės reikalavimai, kad būtų galima laiku peržiūrėti įvykių duomenis
3 BRL praktika, pvz., nejprastos veiklos rodikliai vertinami ir atnaujinami organizacijos nustatytu dažnumu
Išskirtinis valdymo tikslas, pvz., valdymo veikla
2 BRL praktika, pvz., siekiant remti veiklą srityje PADĖTIS, skiriami tinkami ištekliai (žmonės, finansavimas ir priemonės)
3 BRL praktika, pvz., dokumentais grindžiama praktika, susijusi su veikla srityje PADĖTIS, yra standartizuota ir tobulinama visoje įstaigoje

Toliau išsamiau apibūdinamos dešimt sričių:

i Rizikos valdymas (RIZIKA)
ii Išteklių, pokyčių ir konfigūracijos valdymas (IŠTEKLIAI)

iii Tapatybės ir prieigos valdymas (PRIEIGA)
iv Grėsmių ir pažeidžiamumo valdymas (GRĖSMĖ)
v Informuotumas apie padėtį (PADĖTIS)
vi Reagavimas į įvykius ir incidentus (REAGAVIMAS)
vii Tiekimo grandinės ir išorės priklausomybės valdymas (PRIKLAUSOMYBĖ)
viii Darbo jėgos valdymas (DARBO JĖGA)
ix Kibernetinio saugumo struktūra (STRUKTŪRA)
x Kibernetinio saugumo programos valdymas (PROGRAMA)

Brandos lygiai

Siekiant nustatyti dvejopą brandos pažangą – metodo pažangą ir valdymo pažangą – C2M2 naudojami **4 brandos lygiai** (vadinamieji brandos rodiklių lygiai – BRL). BRL kinta nuo 0 BRL iki 3 BRL ir turi būti taikomi kiekvienai sričiai atskirai.

- **0 BRL**. Praktika nevykdoma.
- **1 BRL**. Pradinė praktika vykdoma, tačiau gali būti *ad hoc* .
- **2 BRL**. Valdymo ypatybės:
  - praktika dokumentuota;
  - paskirti tinkami ištekliai procesui remti;
  - praktiką vykdantys darbuotojai turi reikiamus įgūdžius ir žinias;
  - praktikos vykdymo atsakomybės sritys ir įgaliojimai paskirstyti.

  Metodo ypatybė:
  - praktika yra išsamesnė arba pažangesnė nei 1 BRL.
- **3 BRL**. Valdymo ypatybės:
  - veikla vykdoma vadovaujantis politika (arba kitomis organizacinėmis gairėmis);
  - konkrečios srities veiklos tikslai nustatyti ir stebimi, kad būtų galima stebėti pažangą;
  - konkrečios srities veiklos dokumentuota praktika yra standartizuota ir tobulinama visoje įstaigoje.

  Metodo ypatybė:
  - praktika yra išsamesnė arba pažangesnė nei 2 BRL.

Vertinimo metodas

C2M2 skirtas naudoti taikant **įsivertinimo metodiką** ir priemonių rinkinį (pateikiamas paprašius), kad organizacija galėtų įvertinti ir patobulinti savo kibernetinio saugumo programą. Įsivertinimas naudojant priemonių rinkinį gali būti atliktas per vieną dieną, bet norint atlikti griežtesnį vertinimą priemonių rinkinį galima pritaikyti. Be to, C2M2 galima taikyti rengiant naują kibernetinio saugumo programą.

Modelio turinys pateikiamas labai abstrakčiai, kad jį galėtų aiškinti įvairių rūšių, struktūrų, dydžių ir pramonės sektorių organizacijos. Platus modelio taikymas sektoriuje gali padėti atlikti sektoriaus kibernetinio saugumo pajėgumų lyginamąją analizę.

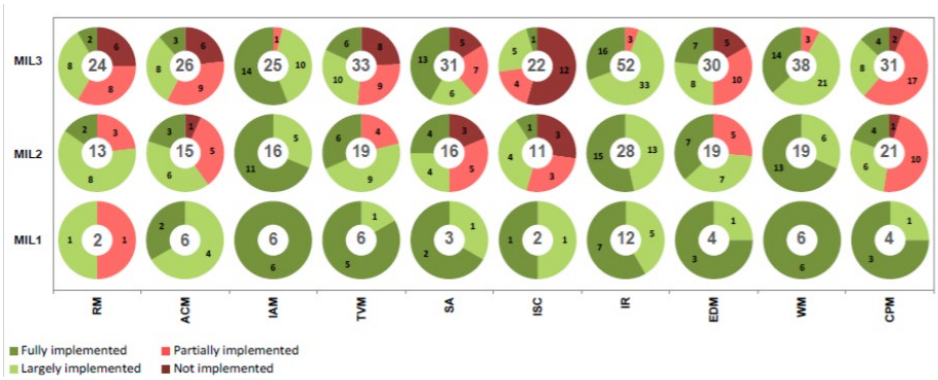
Rezultatų pateikimo būdas

C2M2 pateikiama vertinimo balais ataskaita, parengta remiantis apklausos rezultatais. Ataskaitos rezultatai pateikiami dviem būdais: tikslo rodinys, kuriame atsakymai į klausimus apie praktiką pateikiami pagal kiekvieną sritį ir jos tikslus, ir srities rodinys, kuriame pateikiami visų sričių ir BRL atsakymai. Abu rodiniai pateikiami tokioje vaizdavimo sistemoje, kuriai būdingos skritulinės diagramos – po vieną kiekvienam atsakymui, ir šviesoforo principu grindžiamas vertinimo mechanizmas. Kaip matyti 7 pav., skritulio raudonose dalyse nurodyta, į kiek klausimų atsakyta „Neįgyvendinta“ (tamsiai raudona spalva) arba „Iš dalies įgyvendinta“ (šviesiai raudona spalva). Žaliose dalyse nurodyta, į kiek klausimų atsakyta „Iš esmės įgyvendinta“ (šviesiai žalia spalva) arba „Visiškai įgyvendinta“ (tamsiai žalia spalva).

7 pav. pateikiamas vertinimo balais brandos vertinimo pabaigoje kortelės pavyzdys. X ašyje nurodyta 10 C2M2 sričių, o Y ašyje – brandos rodiklių lygiai (BRL). Pažvelgus į diagramą ir atsižvelgiant į rizikos valdymo (RV) sritį, galima pastebėti tris skritulines diagramas, kurių

kiekviena atitinka kiekvieną brandos lygį: 1 BL, 2 BL ir 3 BL. Kalbant apie RV sritį, diagramoje išryškėja, kad, norint pasiekti pirmąjį brandos lygį (1 BL), reikia įvertinti du elementus. Šiuo atveju vienas žymimas „Iš esmės įgyvendinta“, kitas – „Iš dalies įgyvendinta“. Kalbant apie antrąjį brandos lygį (2 BL), modelyje numatyta, kad reikia įvertinti 13 elementų. Du iš šių 13 elementų priklauso pirmajam lygiui (1 BL), 11 – antrajam lygiui (2 BL). Tas pats taikoma ir trečiajam lygiui (3 BL).

7 pav. C2M2. Srities rodinio pavyzdys



Fully implemented	Visiškai įgyvendinta
Largely implemented	Iš esmės įgyvendinta
Partially implemented	Iš dalies įgyvendinta
Not implemented	Neįgyvendinta
MIL1	1 BRL
MIL2	2 BRL
MIL3	3 BRL
RM	RV
ACM	IPV
IAM	TPV
TVM	GPV
SA	SV
ISC	ISK
IR	RP
EDM	EDV
WM	DJV
CPM	KSPV

Šaltinis – JAV energetikos departamentas, Elektros tiekimo ir energijos patikimumo tarnyba, 2015 m.

A.3 Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistema

Nacionalinis standartų ir technologijų institutas (NIST) parengė ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistemą. Joje siekiama pateikti kibernetinio saugumo veiksmų gaires ir valdyti rizikas organizacijoje. Ji skirta visų rūšių organizacijoms, neatsižvelgiant į jų dydį, kibernetiniam saugumui kylančios rizikos laipsnį ar kibernetinio saugumo sudėtingumą. Tai sistema, o ne modelis, todėl ji sudaryta kitaip nei pirmiau nagrinėti modeliai.

Sistemą sudaro trys dalys: sistemos pagrindas, įgyvendinimo pakopos ir sistemos profiliai:

- **Sistemos pagrindas** – tai kibernetinio saugumo veikla, siekiami rezultatai ir taikytinos nuorodos, kurios yra bendros visuose ypatingos svarbos infrastruktūros sektoriuose. Jos panašios į kibernetinio saugumo gebėjimų brandos modelių požymius ar matmenis.
- **Sistemos įgyvendinimo pakopos** (toliau – pakopos) nurodo, kaip organizacija vertina kibernetiniam saugumui kylančią riziką ir taikomus tos rizikos valdymo procesus. Pakopomis, kurios kinta nuo dalinės (1 pakopa) iki pritaikomos (4 pakopa), apibūdinamas vis didėjantis kibernetiniam saugumui kylančios rizikos valdymo praktikos griežtumo laipsnis ir sudėtingumas. Pakopos nėra brandos lygiai, jomis

veikiau siekiama padėti priimti organizacinius sprendimus, kaip valdyti kibernetiniam saugumui kylančią riziką, taip pat kuriems organizacijos aspektams teikiama pirmenybė ir kuriems galėtų būti skiriama daugiau išteklių.

- **Sistemos profilis** (toliau – profilis) – tai rezultatai, pagrįsti veiklos poreikiais, kuriuos organizacija pasirinko iš sistemos kategorijų ir pakategorių. Profilį galima apibūdinti atsižvelgiant į standartų, gairių ir praktikos suderinimą su sistemos pagrindu, taikant konkretų įgyvendinimo scenarijų. Profiliai gali būti naudojami kibernetinio saugumo padėties gerinimo galimybėms nustatyti, lyginant dabartinį profilį („yra“) su tiksliniu profiliu („turi būti“).

Sistemos pagrindas

Sistemos pagrindą sudaro penkios **funkcijos**. Vertinant kartu, šios funkcijos suteikia aukšto lygio strateginį vaizdą apie organizacijos kibernetiniam saugumui kylančios rizikos valdymo gyvavimo ciklą. Tada, remiantis sistemos pagrindu, nustatomos kiekvienos funkcijos pagrindinės **kategorijos** ir **pakategorės** ir jos suderinamos su pavyzdinėmis informacinėmis nuorodomis, pvz., galiojančiais kiekvienos pakategorės standartais, gairėmis ir praktika.

Funkcijos ir kategorijos toliau aprašomos išsamiau:

i **Nustatyti** – plėtoti organizacinį supratimą apie tai, kaip valdyti kibernetinio saugumo rizikas, gresiančias sistemoms, žmonėms, ištekliams, duomenims ir pajėgumams.
- Pakategorės: turto valdymas; verslo aplinka; valdymas; rizikos vertinimas; rizikos valdymo strategija.

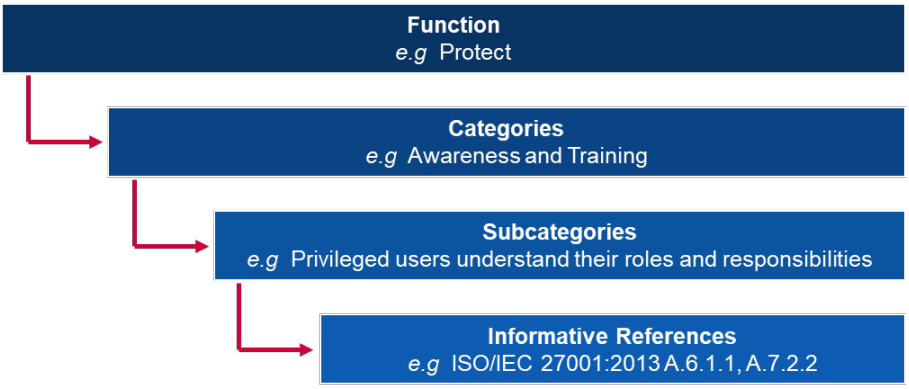
ii **Apsaugoti** – parengti ir įgyvendinti tinkamas apsaugos priemones, kad būtų užtikrinamas ypatingos svarbos paslaugų teikimas.
- Pakategorės: tapatybės duomenų tvarkymas ir prieigos kontrolė; informuotumas ir mokymas; duomenų saugumas; informacijos apsaugos procesai ir procedūros; priežiūra; apsauginės technologijos.

iii **Aptikti** – plėsti ir įgyvendinti atitinkamą veiklą, kuria siekiama nustatyti kibernetinio saugumo įvykio faktą.
- Pakategorės: anomalijos ir įvykiai; nuolatinė saugumo stebėsena; aptikimo procesai.

iv **Reaguoti** – plėsti ir įgyvendinti atitinkamą veiklą, kad būtų imamasi veiksmų dėl nustatyto kibernetinio saugumo incidento.
- Pakategorės: reagavimo planavimas; ryšiai; analizė; švelninimas; patobulinimai.

v **Atkurti** – plėsti ir įgyvendinti tinkamą veiklą siekiant išlaikyti atsparumo planus ir atkurti visus dėl kibernetinio saugumo incidento sutrikusius pajėgumus ar paslaugas.
- Pakategorės: atkūrimo planavimas; patobulinimai; ryšiai.

8 pav. Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistemos pavyzdys



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Funkcija, pvz., projektas
Kategorijos, pvz., informuotumas ir mokymas
Pakategorės, pvz., privilegijuotieji naudotojai supranta savo funkcijas ir atsakomybę
Informacinės nuorodos, pvz., ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Pakopos

Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistema grindžiama **4 pakopomis**, kurių kiekviena nustatoma pagal tris kryptis: rizikos valdymo procesą, integruotą rizikos valdymo programą ir išorės subjektų dalyvavimą. Pakopas reikia vertinti ne kaip brandos lygius, o kaip sistemą, kuria organizacijoms suteikiama galimybė aplinkybėmis pagrįsti savo požiūrį į kibernetiniam saugumui kylančią riziką ir į tai rizikai valdyti taikomus procesus.

- **1 pakopa. Dalinė**
  - **Rizikos valdymo procesas**: organizacinė kibernetiniam saugumui kylančios rizikos valdymo praktika nėra oficialiai patvirtinta, o rizika valdoma *ad hoc* ir kartais atsakomuoju būdu.
  - **Integruota rizikos valdymo programa**: organizacinio lygmens informuotumas apie kibernetiniam saugumui kylančią riziką yra ribotas. Kibernetiniam saugumui kylančios rizikos valdymą organizacija vykdo nereguliariai, atsižvelgdama į kiekvieną konkretų atvejį, ir gali neturėti procedūrų, pagal kurias organizacijoje būtų galima dalytis informacija apie kibernetinį saugumą.
  - **Išorės subjektų dalyvavimas**: organizacija nesupranta savo vaidmens didesnėje ekosistemoje, kiek tai susiję su jos priklausomybe ar priklausomais asmenimis. Organizacija paprastai nežino apie jos tiekiamų ir naudojamų produktų, taip pat teikiamų ir naudojamų paslaugų kibernetinės tiekimo grandinės riziką.
- **2 pakopa. Rizika žinoma**
  - **Rizikos valdymo procesas**: rizikos valdymo praktika yra patvirtina vadovybės, tačiau ji negali būti nustatyta kaip organizacinė politika.
  - **Integruota rizikos valdymo programa**: organizaciniu lygmeniu žinoma apie kibernetiniam saugumui kylančią riziką, tačiau nėra nustatytas visos organizacijos kibernetiniam saugumui kylančios rizikos valdymo metodas. Atliekamas organizacinio ir išorinio turto kibernetinės rizikos vertinimas, tačiau jis paprastai negali būti arba nėra kartojamas.
  - **Išorės subjektų dalyvavimas**: apskritai organizacija supranta savo vaidmenį didesnėje ekosistemoje, atsižvelgdama į savo priklausomybę arba priklausomus asmenis, bet ne į abu aspektus. Be to, organizacija žino apie kibernetinės tiekimo grandinės riziką, susijusią su jos tiekiamais ir naudojamais produktais ir teikiamomis ir naudojamomis paslaugomis, tačiau nesiima nuoseklių ar oficialių veiksmų dėl tos rizikos.
- **3 pakopa. Galimybė kartoti**
  - **Rizikos valdymo procesas**: organizacijos rizikos valdymo praktika yra oficialiai patvirtinta ir apibrėžta. Organizacinė kibernetinio saugumo praktika reguliariai atnaujinama remiantis rizikos valdymo procesų taikymu keičiant veiklos ir (arba) misijos reikalavimus ir kintančia grėsmių ir technologijų aplinka.
  - **Integruota rizikos valdymo programa**: kibernetiniam saugumui kylančiai rizikai valdyti taikomas visos organizacijos metodas. Rizika pagrįsta politika, procesai ir procedūros apibrėžiamos, įgyvendinamos taip, kaip numatyta, ir peržiūrimos. Vyresnieji vadovai užtikrina, kad būtų atsižvelgiama į kibernetinį saugumą visose organizacijos veiklos kryptyse.
  - **Išorės subjektų dalyvavimas**: organizacija supranta savo vaidmenį, priklausomybę ir priklausomus asmenis didesnėje ekosistemoje ir gali padėti bendruomenei geriau suprasti riziką. Organizacija žino apie jos tiekiamų ir naudojamų produktų bei teikiamų ir naudojamų paslaugų kibernetinės tiekimo grandinės riziką.
- **4 pakopa. Galimybė pritaikyti**
  - **Rizikos valdymo procesas**: organizacija pritaiko savo kibernetinio saugumo praktiką, remdamasi ankstesne ir dabartine veikla kibernetinio saugumo srityje, įskaitant įgytą patirtį ir numatomus rodiklius.
  - **Integruota rizikos valdymo programa**: kibernetiniam saugumui kylančiai rizikai valdyti taikomas visos organizacijos metodas, pagal kurį, siekiant reaguoti į galimus kibernetinio saugumo įvykius, taikoma rizika pagrįsta politika, procesai ir procedūros.

- **Išorės subjektų dalyvavimas**: organizacija supranta savo vaidmenį, priklausomybę ir priklausomus asmenis didesnėje ekosistemoje ir padeda bendruomenei geriau suprasti riziką.

Vertinimo metodas

Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistemos paskirtis – leisti organizacijoms pačioms įvertinti savo riziką, kad jų požiūris į kibernetinį saugumą ir investicijos būtų racionalesni, veiksmingesni ir vertingesni. Kad galėtų patikrinti investicijų veiksmingumą, organizacija pirmiausia turi aiškiai suprasti savo organizacinius tikslus, tų tikslų ryšį ir remiamus kibernetinio saugumo rezultatus. Sistemos pagrindo kibernetinio saugumo rezultatai padeda atlikti investicijų veiksmingumo ir kibernetinio saugumo veiklos įsivertinimą.

A.4 Kataro kibernetinio saugumo pajėgumų brandos modelis (Q-C2M2)

2018 m. Kataro universiteto teisės kolegija parengė Kataro kibernetinio saugumo pajėgumų brandumo modelį (Q-C2M2). Q-C2M2 grindžiamas įvairiais esamais modeliais, siekiant parengti išsamią vertinimo metodiką Kataro kibernetinio saugumo sistemai sustiprinti.

Požymiai / matmenys

Q-C2M2 grindžiamas Nacionalinio standartų ir technologijų instituto (NIST) sistemos metodu, pagal kurį pagrindinės modelio sritys yra penkios pagrindinės funkcijos. Šios penkios pagrindinės funkcijos taikomos Kataro aplinkybėmis, nes jos būdingos visiems ypatingos svarbos infrastruktūros sektoriams, o tai yra svarbus Kataro kibernetinio saugumo sistemos elementas. Q-C2M2 grindžiamas **penkiomis sritimis**, kurių kiekviena padalyta į keletą **posričių**, kad apimtų visą kibernetinio saugumo pajėgumų brandos spektrą.

Toliau šios penkios sritys apibūdinamos išsamiau:

i **Supratimo sritis** apima keturis posričius: kibernetinės erdvės valdymą, išteklius, riziką ir mokymą.
ii **Apsaugos srities** posričiai apima duomenų saugumą, technologijų saugumą, prieigos kontrolės užtikrinimą, ryšių saugumą ir personalo patikimumą.
iii **Poveikio sritis** apima stebėsenos, incidentų valdymo, aptikimo, analizės ir poveikio posričius.
iv **Reagavimo sritis** apima reagavimo planavimą, švelninimą ir pranešimą apie reagavimą.
v **Išlaikymo sritis** apima atkūrimo planavimą, tęstinumo valdymą, tobulinimą ir išorės subjektų priklausomybę.

Brandos lygiai

Q-C2M2 naudojami **5 brandos lygiai**, kuriais matuojama valstybinio subjekto arba nevalstybinės organizacijos pajėgumų branda pagrindinių funkcijų lygmeniu. Šiais lygiais siekiama įvertinti penkių sričių, apibūdintų ankstesniame skirsnyje, brandą.

- **Inicijavimas**: kai kuriose srityse taikoma *ad hoc* kibernetinio saugumo praktika ir procesai.
- **Įgyvendinimas**: priimta politika, kuria siekiama įgyvendinti visą su kibernetiniu saugumu susijusią veiklą tose srityse, kad įgyvendinimas būtų užbaigtas tam tikru metu.
- **Plėtojimas**: įgyvendinama politika ir praktika, kuriomis siekiama plėtoti ir tobulinti su kibernetiniu saugumu susijusią veiklą tose srityse, siekiant pasiūlyti įgyvendinti naują veiklą.
- **Pritaikymas**: iš naujo apsvarstoma ir peržiūrima veikla kibernetinio saugumo srityje ir patvirtinama praktika, pagrįsta prognozavimo rodikliais, nustatytais remiantis ankstesne patirtimi ir priemonėmis.
- **Tęstinumas**: tęsiamas pritaikymo etapas, daugiau dėmesio skiriant guvumui ir spartai įgyvendinant veiklą tose srityse.

Vertinimo metodas

Q-C2M2 yra ankstyvo mokslinių tyrimų etapo ir dar neparuoštas įgyvendinti. Tai sistema, kurią būtų galima naudoti siekiant ateityje įdiegti išsamų Kataro organizacijų vertinimo modelį.

A.5 Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)

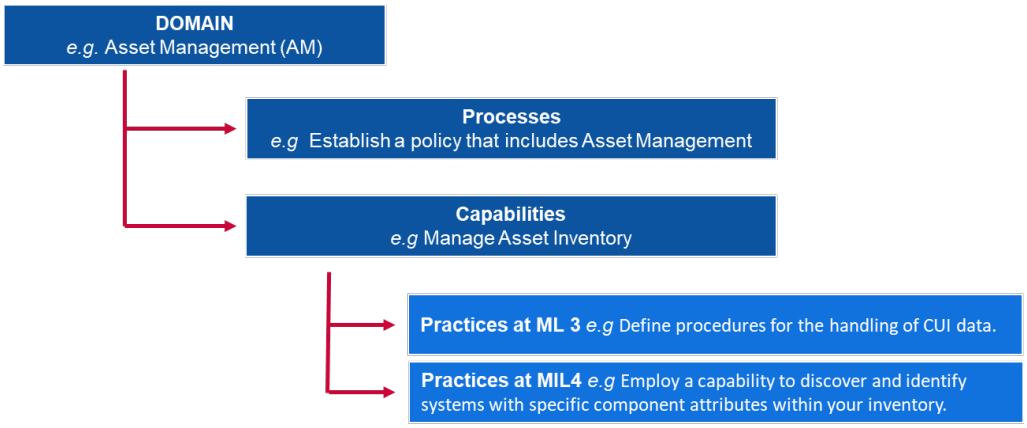
JAV gynybos departamentas (angl. *Department of Defense – DoD*), bendradarbiaudamas su Carnegie ir Mellono universitetu ir Johno Hopkinso universiteto taikomosios fizikos laboratorija, parengė kibernetinio saugumo brandos modelių sertifikavimo (CMMC) sistemą. Pagrindinis *DoD* tikslas kuriant šį modelį – apsaugoti informaciją nuo gynybos pramoninės bazės (GPB) sektoriaus. Informacija, kuriai skirta CMMC, klasifikuojama kaip „federalinių sutarčių informacija“, vyriausybės pateikta arba pagal sutartį parengta informacija, kuri nėra skirta viešai skelbti, arba „kontroliuojama neįslaptinta informacija“, kuri turi būti saugoma arba platinama laikantis įstatymų, kitų teisės aktų ir visos vyriausybės politikos. Taikant CMMC vertinama kibernetinio saugumo branda, be to, ji apima gerąją patirtį ir sertifikavimo elementą, kad būtų užtikrinamas su kiekvienu brandos lygiu susijusios praktikos įgyvendinimas. Naujausia CMMC versija paskelbta 2020 m.

Požymiai / matmenys

CMMC apima **septyniolika sričių**, atspindinčių kibernetinio saugumo procesų ir pajėgumų grupes. Kiekviena sritis skirstoma į kelis **procesus**, kurie yra panašūs visose srityse, ir vieną iš daugelio **pajėgumų**, apimančių daugiau kaip penkis brandos lygius. Pajėgumai (arba pajėgumas) išsamiai aprašomi kiekvieno atitinkamo brandos lygio **praktikoje**.

Toliau apibūdinamas šių sąvokų ryšys:

9 pav. CMMC rodiklių pavyzdys



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

SRITIS, pvz., išteklių valdymas (IV)
Procesai
pvz., politikos, kuri apimtų išteklių valdymą, nustatymas
Pajėgumai
pvz., išteklių aprašo valdymas
3 BL praktika, pvz., nustatyti KNI tvarkymo procedūras
4 BL praktika, pvz., gebėti atrasti ir nustatyti sistemas, turinčias konkrečių sudedamųjų savybių

Toliau išvardijama septyniolika sričių:

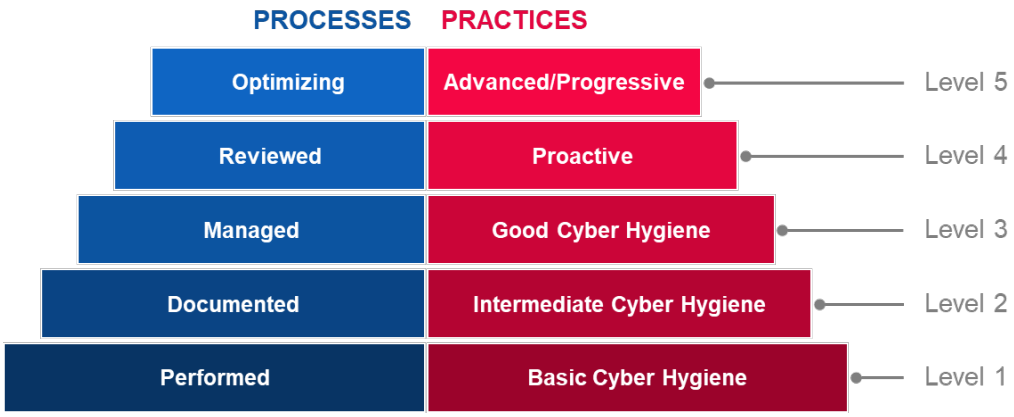
i Prieigos kontrolė (PK)
ii Išteklių valdymas (IV)
iii Auditas ir atskaitomybė (AA)
iv Informuotumas ir mokymas (AM)
v Konfigūracijos valdymas (KV)
vi Tapatybės ir tapatumo nustatymas (TTN)
vii Reagavimas į incidentus (RI)
viii Priežiūra (PR)

ix Žiniasklaidos apsauga (ŽA)
x Personalo patikimumas (PP)
xi Fizinė apsauga (FA)
xii Atkūrimas (AT)
xiii Rizikos valdymas (RV)
xiv Saugumo vertinimas (SV)
xv Informuotumas apie padėtį (IP)
xvi Sistemų ir ryšių apsauga (SRA)
xvii Sistemos ir informacijos vientisumas (SIV)

Brandos lygiai

CMMC naudojami **5 brandos lygiai**, nustatyti remiantis procesais ir praktika. Tam, kad būtų pasiektas tam tikras CMMC brandos lygis, organizacija turi pati įvykdyti procesų ir praktikos sąlygas. Tai taip pat reiškia, kad turi būti įvykdytos visos žemesnio lygio sąlygos.

10 pav. CMMC brandos lygiai



PROCESSES	PROCESAI
Optimizing	Optimizuojama
Reviewed	Peržiūrėta
Managed	Valdoma
Documented	Dokumentuota
Performed	Vykdoma
PRACTICES	PRAKTIKA
Advanced/Progressive	Pažangi
Proactive	Iniciatyvi
Good Cyber Hygiene	Gera kibernetinė higiena
Intermediate Cyber Hygiene	Vidutinė kibernetinė higiena
Basic Cyber Hygiene	Bazinė kibernetinė higiena
Level 5	5 lygis
Level 4	4 lygis
Level 3	3 lygis
Level 2	2 lygis
Level 1	1 lygis

- **1 lygis**
  - **Procesai – vykdoma**: nes organizacija gali vykdyti šią praktiką tik *ad hoc* būdu ir gali kliautis dokumentais arba ne. 1 lygio proceso branda nevertinama.
  - **Praktika – bazinė kibernetinė higiena**: 1 lygyje daugiausia dėmesio skiriama FSI (federalinių sutarčių informacijos) apsaugai ir jį sudaro tik ta praktika, kuri atitinka pagrindinius apsaugos reikalavimus.
- **2 lygis**
  - **Procesai – dokumentuota**: 2 lygyje reikalaujama, kad organizacija nustatytų ir dokumentuotų savo pastangų, susijusių su CMMC įgyvendinimu, praktiką ir politiką. Praktikos dokumentavimas leidžia asmenims ją taikyti pakartotinai. Organizacijos plėtoja brandžius pajėgumus dokumentuodamos savo procesus ir tuo pat metu juos naudodamos.

- **Praktika – vidutinė kibernetinė higiena**: 2 lygis naudojamas persikeliant iš 1 lygio į 3. Jį sudaro NIST SP 800-171 nurodytų saugumo reikalavimų poaibis, taip pat kituose standartuose ir informacijos šaltiniuose numatyta praktika.

- **3 lygis**
  - **Procesai – valdoma**: 3 lygyje reikalaujama, kad organizacija parengtų, tvarkytų ir suteiktų išteklių planui, kuriame atskleistas praktinis veiklos valdymas. Į planą gali būti įtraukta informacija apie misijas, tikslus, projektų planus, išteklių paskirstymą, reikiamą mokymą ir atitinkamų suinteresuotųjų subjektų dalyvavimą.
  - **Praktika – gera kibernetinė higiena**: 3 lygyje daugiausia dėmesio skiriama KNI apsaugai ir jis apima visus saugumo reikalavimus, nurodytus NIST SP 800-171, taip pat papildomą kituose standartuose numatytą praktiką ir nuorodas į grėsmių mažinimą.
- **4 lygis**
  - **Procesai – peržiūrėta**: 4 lygyje reikalaujama, kad organizacija peržiūrėtų ir įvertintų veiksmingumo užtikrinimo praktiką. Organizacijos gali ne tik vertinti veiksmingumą, bet ir prireikus imtis taisomųjų veiksmų ir nuolat informuoti apie būseną ar problemas aukštesnio lygio vadovybę.
  - **Praktika – iniciatyvi**: 4 lygis orientuotas į KNI (kontroliuojamos neįslaptintos informacijos) apsaugą ir apima sugriežtintų saugumo reikalavimų pogrupį. Šia praktika stiprinami organizacijos pajėgumai nustatyti besikeičiančią taktiką, metodus ir procedūras, į juos reaguoti ir prie jų prisitaikyti.
- **5 lygis**
  - **Procesai – optimizuojama**: 5 lygyje reikalaujama, kad organizacija standartizuotų ir optimizuotų procesų įgyvendinimą visoje organizacijoje.
  - **Praktika – pažangi / iniciatyvi**: 5 lygyje daugiausia dėmesio skiriama KNI apsaugai. Papildoma praktika didinamas kibernetinio saugumo pajėgumų išsamumas ir sudėtingumas.

Vertinimo metodas

CMMC yra palyginti naujas modelis, užbaigtas 2020 m. pirmąjį ketvirtį. Kol kas jis neįdiegtas jokioje organizacijoje. Vis dėlto *DoD* rangovai tikisi susisiekti su sertifikuotais trečiųjų šalių egzaminuotojais, kad jie galėtų atlikti auditą. *DoD* tikisi, kad jo rangovai įgyvendins gerąją patirtį, kad padidintų kibernetinį saugumą ir neskelbtinos informacijos apsaugą.

A.6 Bendruomenės kibernetinio saugumo brandos modelis (CCSMM)

Bendruomenės kibernetinio saugumo brandos modelį (CCSMM) parengė Teksaso universiteto Infrastruktūros užtikrinimo ir apsaugos centras. CCSMM tikslas – geriau apibrėžti metodus, kuriais remiantis būtų galima nustatyti dabartinį bendruomenės statusą jos kibernetinio pasirengimo srityje ir pateikti gaires, kaip bendruomenės galėtų stebėti savo pasirengimo pastangas. CCSMM tikslinės bendruomenės daugiausia yra vietos arba valstijų vyriausybės. CCSMM sukurtas 2007 m.

Požymiai / matmenys

Brandos lygiai apibrėžiami pagal **6 pagrindinius matmenis**, apimančius įvairius bendruomenių ir organizacijų kibernetinio saugumo aspektus. Šie kiekvieno brandos lygio matmenys yra aiškiai apibrėžti (išsamiai aprašyti 31 pav. **CCSMM** matmenų apibendrinimas). 6 matmenys:

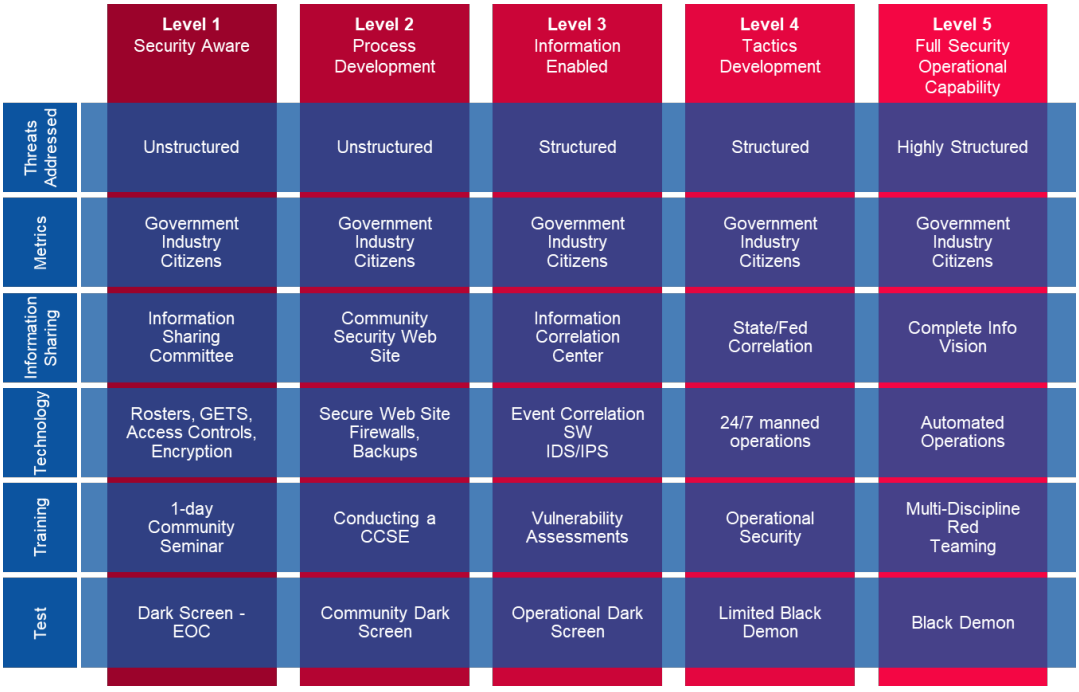
i Pašalintos grėsmės
ii Metrika
iii Dalijimasis informacija
iv Technologija
v Mokymas
vi Bandymas

Brandos lygiai

CCSMM grindžiamas **5 brandos lygiais**, remiantis pagrindinėmis grėsmių ir veiksmų, kurių imamasi nurodytu lygiu, rūšimis.

- **1 lygis. Informacija apie saugumą**
  Šio lygio veiklos tikslas – informuoti asmenis ir organizacijas apie grėsmes, problemas ir su kibernetiniu saugumu susijusius klausimus.
- **2 lygis. Procesų plėtojimas**
  Lygis, skirtas padėti bendruomenėms nustatyti ir tobulinti saugumo procesus, reikalingus siekiant veiksmingai spręsti kibernetinio saugumo problemas.
- **3 lygis. Galimybė susipažinti su informacija**
  Sukurta siekiant pagerinti dalijimosi informacija mechanizmus bendruomenėje, kad bendruomenė galėtų veiksmingai susieti informaciją, kuri, atrodo, skiriasi.
- **4 lygis. Taktikos plėtojimas**
  Šio lygio elementais siekiama kurti geresnius ir iniciatyvesnius išpuolių nustatymo ir reagavimo į juos metodus. Šiame lygyje turėtų būti įdiegta dauguma prevencijos metodų.
- **5 lygis. Visapusiškas saugumo veiklos pajėgumas**
  Šis lygis atspindi tuos elementus, kurie turėtų būti įdiegti, kad bet kuri organizacija galėtų manyti esanti visiškai pasirengusi reaguoti į bet kokios rūšies kibernetinę grėsmę.

31 pav. CCSMM matmenų apibendrinimas pagal lygį



Level 1	1 lygis
Security Aware	Informacija apie saugumą
Level 2	2 lygis
Process Development	Procesų plėtojimas
Level 3	3 lygis
Information Enabled	Galimybė susipažinti su informacija
Level 4	4 lygis
Tactics Development	Taktikos plėtojimas
Level 5	5 lygis
Full Security Operational Capability	Visapusiškas saugumo veiklos pajėgumas
Threats Addressed	Pašalintos grėsmės
Metrics	Metrika
Information sharing	Dalijimasis informacija
Technology	Technologija
Training	Mokymas
Test	Bandymas

Unstructured	Struktūra nenustatyta
Governement	Vyriausybė
Industry	Pramonė
Citizens	Piliečiai
Information Sharing Committee	Dalijimosi informacija komitetas
Rosters, GETS, Assess Controls, Encryption	Sąrašai, GETS, vertinimo kontrolė, šifravimas
1-dat Community Seminar	1 dienos bendruomenei skirtas seminaras
Dark Screen – EOC	Juodas ekranas – EOC
Unstructured	Struktūra nenustatyta
Governement	Vyriausybė
Industry	Pramonė
Citizens	Piliečiai
Community Security Web site	Bendruomenės saugumui skirta interneto svetainė
Secure Web Site Firewalls, Backups	Saugios interneto svetainių užkardos, atsarginės kopijos
Conudcting a CCSE	CCSE vykdymas
Community Dark Screen	Bendruomenei skirtas juodas ekranas
Structured	Struktūra nustatyta
Governement	Vyriausybė
Industry	Pramonė
Citizens	Piliečiai
Information Correlation Center	Informacijos koreliavimo centras
Event Correlation SW IDS/IPS	Programinės įrangos IDS / IPS įvykių koreliacija
Vulnerability Assessment	Pažeidžiamumo vertinimas
Operational Dark Screen	Veiklos juodas ekranas
Structured	Struktūra nustatyta
Governement	Vyriausybė
Industry	Pramonė
Citizens	Piliečiai
State/Fed Correlation	Valstybinė / federalinė koreliacija
24/7 manned operations	Visą parą 7 dienas per savaitę valdomos operacijos
Operational Security	Veiklos saugumas
Limited Black Demon	Ribotas „juodasis demonas“

Vertinimo metodas

CCSMM, kaip vertinimo metodiką, turėtų įdiegti bendruomenės, padedant valstybės ir federalinėms teisėsaugos institucijoms. Juo siekiama padėti bendruomenei apibrėžti svarbiausius, labiausiai tikėtinus ir saugotinus tikslus (ir jų apsaugos mastą). Atsižvelgiant į šiuos tikslus, galima parengti planus, kad kiekvienas bendruomenės aspektas atitiktų reikiamą kibernetinio saugumo brandos lygį. CCSMM sukaupta speciali žvalgybinė informacija padeda nustatyti įvairių bandymų ir pratybų, kurie gali būti naudojami nustatytų programų veiksmingumui vertinti, tikslus.

A.7 NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis (ISMM)

Informacijos saugumo brandos modelis (ISMM) sukurtas Saudo Arabijos Karaliaus Fahdo naftos ir mineralų universiteto Kompiuterių mokslo ir inžinerijos kolegijoje. Tai naujas pajėgumų brandos modelis, taikomas kibernetinio saugumo priemonių įgyvendinimui vertinti. ISMM tikslas – sudaryti sąlygas organizacijoms nuolat vertinti savo įgyvendinimo pažangą, reguliariai naudojant tą pačią matavimo priemonę, siekiant užtikrinti, kad būtų išlaikoma norima saugumo padėtis. ISMM sukurtas 2017 m.

Požymiai / matmenys

ISMM grindžiamas esamomis įvertintomis NIST sistemos sritimis ir papildo atitikties vertinimo aspektą. Tai reiškia, kad modelis apima **23 vertinamas sritis**, kuriose organizacija turi užtikrinti tinkamą saugumo būseną. 23 vertinamos sritys:

i Išteklių valdymas
ii Verslo aplinka
iii Valdymas
iv Rizikos vertinimas
v Rizikos valdymo strategija
vi Atitikties vertinimas
vii Prieigos kontrolė
viii Informuotumas ir mokymas

ix Duomenų saugumas
x Informacijos apsaugos procesai ir procedūros
xi Priežiūra
xii Apsauginė technologija
xiii Anomalijos ir įvykiai
xiv Nuolatinė saugumo stebėsena
xv Aptikimo procesai
xvi Reagavimo planavimas
xvii Atsakomieji ryšiai
xviii Reagavimo analizė
xix Reagavimo švelninimas
xx Reagavimo patobulinimai
xxi Atkūrimo planavimas
xxii Atkūrimo patobulinimai
xxiii Pranešimas apie atkūrimą

Brandos lygiai

ISMM grindžiamas **5 brandos lygiais**, kurie, deja, nėra išsamiai aprašyti turimuose dokumentuose.

- **1 lygis.** Procesas vykdomas
- **2 lygis.** Procesas valdomas
- **3 lygis.** Procesas nusistovėjęs
- **4 lygis.** Procesas nuspėjamas
- **5 lygis.** Procesas optimizuojamas

Vertinimo metodas

ISMM nesiūloma jokios konkrečios metodikos, pagal kurią organizacijos galėtų atlikti vertinimą.

A.8 Viešojo sektoriaus vidaus audito pajėgumų modelis (IA-CM)

Vidaus audito pajėgumų modelį (IA-CM) parengė Vidaus auditorių mokslinių tyrimų fondo institutas, siekdamas stiprinti gebėjimus ir tarpininkauti, pasitelkiant įsivertinimą viešajame sektoriuje. Audito specialistams skirtame IA-CM pateikiama paties modelio apžvalga ir taikymo vadovas, siekiant padėti taikyti modelį kaip įsivertinimo priemonę.

Nepaisant to, kad IA-CM yra orientuotas į vidaus audito pajėgumus, o ne į kibernetinio saugumo gebėjimų stiprinimą, modelis sukurtas kaip viešojo sektoriaus subjektų brandos įsivertinimo priemonė, kurią galima taikyti visame pasaulyje siekiant pagerinti procesus ir veiksmingumą. Kadangi taikymo sritis nėra orientuota į kibernetinį saugumą, požymiai nebus nagrinėjami. IA-CM užbaigtas 2009 m.

Brandos lygiai

Vidaus audito pajėgumų modelis (IA-CM) apima **5 brandos lygius**, kurių kiekvienu apibūdinamos to lygio vidaus audito veiklos ypatybės ir pajėgumai. Atsižvelgiant į modelyje nurodytus pajėgumų lygius, pateikiamos nuolatinio tobulinimo veiksmų gairės.

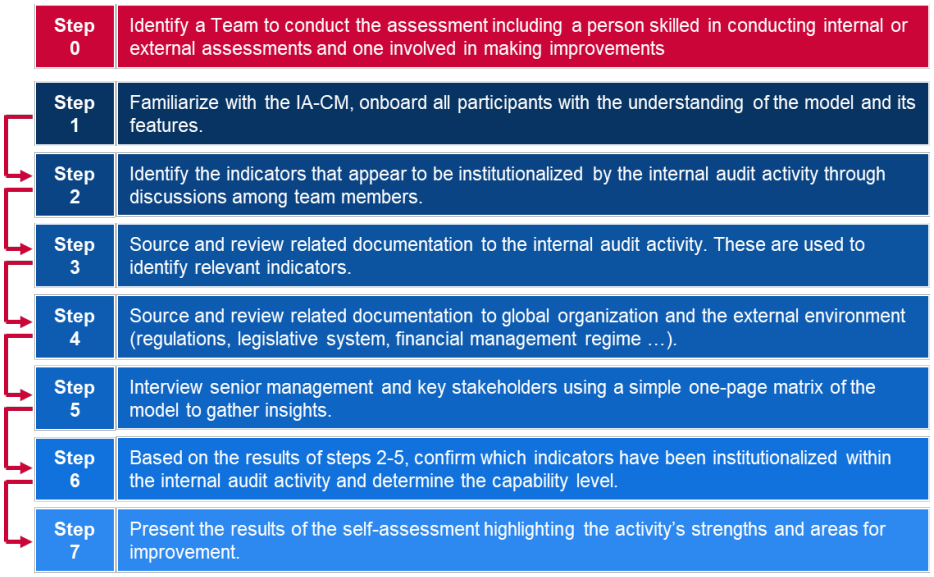
- **1 lygis. Pradinis**
  Nėra tvarių, pakartojamų pajėgumų – priklauso nuo atskirų pastangų
  - *Ad hoc* arba be struktūros.
  - Atskiri vieni bendri auditai arba dokumentų ir sandorių peržiūros siekiant tikslumo ir atitikties.
  - Rezultatai priklauso nuo konkretaus pareigas einančio asmens įgūdžių.
  - Tik profesinių asociacijų nustatyta profesinė praktika.
  - Prireikus finansavimą tvirtina vadovybė.
  - Nėra infrastruktūros.
  - Auditoriai gali priklausyti didesniam organizaciniam padaliniui.
  - Instituciniai pajėgumai nėra plėtojami.

- **2 lygis. Infrastruktūros**
  Tvari ir kartotinė praktika ir procedūros
  - Svarbus 2 lygio klausimas arba uždavinys – kaip nustatyti ir išsaugoti procesų pakartojamumą, taigi ir pakartojamą pajėgumą.
  - Nustatomi vidaus audito ataskaitų teikimo santykiai, valdymo ir administracinė infrastruktūra, profesinė praktika ir procesai (vidaus audito gairės, procesai ir procedūros).
  - Audito planavimas iš esmės grindžiamas valdymo prioritetais.
  - Nuolat kliaujamasi konkrečių asmenų įgūdžiais ir gebėjimais.
  - Standartų laikomasi iš dalies.
- **3 lygis. Integruotas**
  Vienodai taikomas integruotas valdymas ir profesinė praktika
  - Vidaus audito politika, procesai ir procedūros yra apibrėžiami, dokumentuojami ir integruojami tarpusavyje ir į organizacijos infrastruktūrą.
  - Vidaus audito valdymas ir profesinė praktika yra tinkamai nustatyti ir vienodai taikomi visoje vidaus audito veikloje.
  - Vidaus auditas pradeda derėti su organizacijos veikla ir jai kylančia rizika.
  - Vidaus auditas kinta nuo tradicinio vidaus audito atlikimo iki įtraukimo į grupę ir konsultacijų dėl veiklos ir rizikos valdymo teikimo.
  - Daugiausia dėmesio skiriama komandų kūrimui ir vidaus audito veiklos gebėjimams, taip pat nepriklausomumui ir objektyvumui.
  - Paprastai laikomasi standartų.
- **4 lygis. Valdomas**
  Integruojama visos organizacijos informacija, kad būtų pagerintas valdymas ir rizikos valdymas
  - Vidaus auditas ir pagrindinių suinteresuotųjų subjektų lūkesčiai yra suderinti.
  - Nustatyti veiksmingumo parametrai, skirti vidaus audito procesams ir rezultatams vertinti ir stebėti.
  - Pripažįstama, kad vidaus auditu labai prisidedama prie organizacijos veiklos.
  - Vidaus audito funkcijos yra neatsiejama organizacijos valdymo ir rizikos valdymo dalis.
  - Vidaus audito skyrius tinkamai valdomas.
  - Rizika vertinama ir valdoma kiekybiškai.
  - Ugdomi reikiami įgūdžiai ir gebėjimai, kad būtų galima atsinaujinti ir dalytis žiniomis (vidaus audito metu ir organizacijoje).
- **5 lygis. Optimizuojamas**
  Mokymasis iš organizacijos vidaus ir išorės subjektų siekiant nuolat tobulėti
  - Vidaus auditas suvokiamas kaip mokymosi organizacija, kurioje nuolat tobulinami procesai ir diegiamos naujovės.
  - Vidaus audito tikslais naudojama organizacijos vidaus ir išorės informacija, kuria padedama siekti strateginių tikslų.
  - Užtikrinami pasaulinio lygio / rekomenduojami / gerosios patirties rezultatai.
  - Vidaus auditas yra svarbi organizacijos valdymo struktūros dalis.
  - Užtikrinami aukščiausio lygio profesiniai ir specialūs įgūdžiai.
  - Atskiros, skyriaus ir organizacijos veiklos rezultatų vertinimo priemonės yra visapusiškai integruotos, kad
  - būtų gerinami veiklos rezultatai.

Vertinimo metodas

Vidaus audito pajėgumų modelis yra aiškiai sukurtas įsivertinimui atlikti. Jame nurodomi nuodugnūs veiksmai, kurių reikia imtis, kad IA-CM ir jo dalys būtų naudojamos individualiems poreikiams. Prieš pradedant įsivertinimą, turi būti nustatyta konkreti grupė, įskaitant bent vieną asmenį, turintį įgūdžių atlikti vidaus audito vidaus ar išorės vertinimus, ir vieną asmenį, kuris dalyvauja atliekant patobulinimus šioje srityje.

12 pav. Įsivertinimo pagal IA-CM veiksmai



Step 0	0 veiksmas
Step 1	1 veiksmas
Step 2	2 veiksmas
Step 3	3 veiksmas
Step 4	4 veiksmas
Step 5	5 veiksmas
Step 6	6 veiksmas
Step 7	7 veiksmas
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Nustatyti grupę, kuri atliktų vertinimą, įskaitant vieną asmenį, galintį atlikti vidaus ar išorės vertinimus, ir vieną asmenį, dalyvaujantį atliekant patobulinimus.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Supažindinti visus dalyvius su IA-CM modeliu ir jo savybėmis.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Pasitelkiant grupės narių diskusijas nustatyti vidaus audito veiklos įformintus rodiklius.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Gauti su vidaus audito veikla susijusius dokumentus ir juos peržiūrėti. Jie naudojami atitinkamiems rodikliams nustatyti.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Gauti su visuotiniu organizavimu ir išorės aplinka susijusius dokumentus ir juos peržiūrėti (reglamentai, teisėkūros sistema, finansų valdymo tvarka ir kt.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Pasikalbėti su vyresniąja vadovybe ir pagrindiniais suinteresuotaisiais subjektais naudojant paprastą vieno puslapio modelio matricą įžvalgoms gauti.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Remiantis 2–5 veiksmų rezultatais, patvirtinti, kokie rodikliai įforminti vykdant vidaus audito veiklą, ir nustatyti gebėjimų lygį.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Pateikti įsivertinimo rezultatus, atkreipiant dėmesį į veiklos stiprybes ir tobulintinas sritis.

A.9 Visuotinis kibernetinio saugumo indeksas (VKSI)

Visuotinis kibernetinio saugumo indeksas (VKSI) yra Tarptautinės telekomunikacijų sąjungos (ITU) iniciatyva, kuria siekiama peržiūrėti kibernetinio saugumo pastangas ir padėtį visuose ITU regionuose – Afrikoje, Šiaurės ir Pietų Amerikoje, Arabų šalyse, Azijos ir Ramiojo vandenyno šalys, NVS ir Europoje – ir atkreipiamas dėmesys į tas šalis, kurios deda daug pastangų ir taiko rekomenduojamą praktiką. VKSI tikslas – padėti šalims nustatyti tobulintinas sritis kibernetinio saugumo srityje, taip pat paskatinti jas imtis veiksmų savo reitingui gerinti ir taip padėti gerinti bendrą kibernetinio saugumo lygį visame pasaulyje.

Kadangi VKSI yra indeksas, o ne brandumo modelis, jame naudojami ne brandumo lygiai, o veikiau vertinimo balai, leidžiantys palyginti šalių ir regionų visuotines kibernetinio saugumo pastangas.

Požymiai / matmenys

Visuotinis kibernetinio saugumo indeksas (VKSI) grindžiamas penkiais Pasaulinės kibernetinio saugumo darbotvarkės ramsčiais. Šie ramsčiai sudaro penkis VKSI antrinius indeksus ir kiekvienas iš jų apima rodiklių rinkinį. Penki ramsčiai ir rodikliai:

i **Teisinio pobūdžio**: priemonės, grindžiamos teisės institucijomis ir sistemomis, susijusiomis su kibernetiniu saugumu ir kibernetiniais nusikaltimais.
- Teisės aktai dėl kibernetinių nusikaltimų
- Kibernetinio saugumo reguliavimas
- Teisės aktai dėl brukalo sulaikymo

ii **Techninio pobūdžio**: priemonės, grindžiamos techninėmis institucijomis ir sistemomis, susijusiomis su kibernetiniu saugumu.
- CERT / CIRT / CSRIT
- Standartų įgyvendinimo sistema
- Standartizacijos įstaiga
- Techniniai mechanizmai ir pajėgumai, naudojami brukalo klausimui spręsti
- Debesijos naudojimas kibernetinio saugumo reikmėms
- Vaikų apsaugos internete mechanizmai

iii **Organizacinio pobūdžio**: priemonės, grindžiamos esamomis politikos koordinavimo institucijomis ir kibernetinio saugumo plėtros nacionaliniu lygmeniu strategijomis.
- Nacionalinė kibernetinio saugumo strategija
- Atsakinga agentūra
- Kibernetinis saugumas

iv **Gebėjimų stiprinimo**: priemonės, grindžiamos esamomis mokslinių tyrimų ir technologinės plėtros, švietimo ir mokymo programomis, sertifikuotais specialistais ir viešojo sektoriaus agentūromis, skatinančiomis gebėjimų stiprinimą.
- Viešos informuotumo didinimo kampanijos
- Kibernetinio saugumo specialistų sertifikavimo ir akreditavimo sistema
- Profesinio mokymo kursai kibernetinio saugumo srityje
- Švietimo kibernetinio saugumo klausimais programos arba akademinės mokymo programos
- Kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros programos
- Skatinamieji mechanizmai

v **Bendradarbiavimo**: priemonės, grindžiamos partnerystėmis, bendradarbiavimo sistemomis ir keitimosi informacija tinklais.
- Dvišaliai susitarimai
- Daugiašaliai susitarimai
- Dalyvavimas tarptautiniuose forumuose ir (arba) asociacijų veikloje
- Viešojo ir privačiojo sektorių partnerystės
- Agentūrų partnerystės ir (arba) agentūros vidaus partnerystės
- Geroji patirtis

Vertinimo metodas

VKSI yra įsivertinimo priemonė, paremta apklausa, sudaryta iš klausimų su dviem atsakymų variantais, klausimų su pasirinktinais atsakymų variantais ir klausimų, į kuriuos galima atsakyti laisvai[30]. Klausimai su dviem atsakymų variantais užkerta kelią subjektyvia nuomone pagrįstiems ir šališkiems atsakymams. Klausimai su pasirinktinais atsakymų variantais padeda sutaupyti laiko ir atlikti tikslesnę duomenų analizę. Be to, paprasta dichotominė skalė leidžia atlikti greitesnį ir sudėtingesnį vertinimą, nes nereikia ilgų atsakymų, o tai paspartina ir supaprastina atsakymų pateikimo ir tolesnio vertinimo procesą. Respondentui tereikia patvirtinti tam tikrų nustatytų kibernetinio saugumo sprendimų buvimą arba nebuvimą. Internetinės apklausos mechanizmas, taikomas atsakymams rinkti ir atitinkamai medžiagai nusiųsti, leidžia ekspertų grupei išgauti gerosios patirties pavyzdžius ir atlikti tam tikrus teminius kokybinius vertinimus.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

Bendras VKSI procesas įgyvendinamas taip:

- Visiems dalyviams išsiunčiamas kvietimas, kuriame jie informuojami apie iniciatyvą ir kuriame prašoma nurodyti ryšių punktą, atsakingą už visų svarbių duomenų rinkimą ir internetinio VKSI klausimyno užpildymą. Patvirtintą ryšių punktą internetinės apklausos metu ITU oficialiai pakviečia atsakyti į klausimyno klausimus.
- Pirminių duomenų rinkimas (taikoma šalims, kurios neatsako į klausimyno klausimus):
  - ITU, naudodama viešai prieinamus duomenis ir internetinius tyrimus, parengia pradinį atsakymo į klausimyno klausimus projektą.
  - Klausimyno projektas nusiunčiamas ryšių punktams peržiūrėti.
  - Ryšių punktai patikslina ir grąžina klausimyno projektą.
  - Pataisytas klausimyno projektas nusiunčiamas kiekvienam ryšių punktui galutinai patvirtinti.
  - Patikrintas klausimynas naudojamas analizei atlikti, balams nustatyti ir reitinguoti.
- Antrinių duomenų rinkimas (taikoma šalims, kurios atsako į klausimyno klausimus):
  - ITU nustato trūkstamus atsakymus, patvirtinamuosius dokumentus, nuorodas ir kt.
  - Prireikus ryšių punktas patikslina atsakymus.
  - Pataisytas klausimyno projektas nusiunčiamas kiekvienam ryšių punktui galutinai patvirtinti.
  - Patikrintas klausimynas naudojamas analizei atlikti, balams nustatyti ir reitinguoti.

A.10 Kibernetinės galios indeksas (KGI)

Kibernetinės galios indeksas (KGI) sukurtas 2011 m. pagal „Economist Intelligence Unit“ mokslinių tyrimų programą, kurią rėmė „Booz Allen Hamilton“. KGI yra „dinamiškas kiekybinis ir kokybinis modelis <...>, pagal kurį vertinami konkretūs kibernetinės aplinkos požymiai, susiję su keturiais kibernetinės galios veiksniais: teisės ir reguliavimo sistema, ekonominėmis ir socialinėmis aplinkybėmis, technologijų infrastruktūra ir taikymu pramonėje. Pagal šį modelį nagrinėjama skaitmeninė pažanga keturiose pramonės srityse“[31]. Taikant kibernetinės galios indeksą siekiama palyginti G 20 šalių pajėgumą atlaikyti kibernetinius išpuolius ir diegti klestinčiai ir saugiai ekonomikai būtiną skaitmeninę infrastruktūrą. Pagal KGI pateiktą lyginamąjį standartą daugiausia dėmesio skiriama 19-ai G 20 šalių (išskyrus ES). Tada indeksu žymimas šalių reitingas pagal kiekvieną rodiklį.

Požymiai / matmenys

Kibernetinės galios indeksas (KGI) grindžiamas keturiais kibernetinės galios veiksniais. Tada kiekviena kategorija vertinama pagal kelis rodiklius, kad kiekvienai šaliai būtų suteiktas konkretus balas. Kategorijos ir ramsčiai:

i **Teisinė ir reguliavimo sistema**
  - Vyriausybės įsipareigojimas plėtoti kibernetinę erdvę
  - Kibernetinės erdvės apsaugos politika
  - Cenzūra kibernetinėje erdvėje (arba jos nebuvimas)
  - Politinis veiksmingumas
  - Intelektinės nuosavybės apsauga

ii **Ekonominės ir socialinės aplinkybės**
  - Išsilavinimo lygiai
  - Techniniai įgūdžiai
  - Prekybos atvirumas
  - Inovacijų lygis verslo aplinkoje

iii **Technologijų infrastruktūra**
  - Galimybė naudotis informacinėmis ir ryšių technologijomis

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Informacinių ir ryšių technologijų kokybė
- Informacinių ir ryšių technologijų įperkamumas
- Išlaidos informacinėms technologijoms
- Saugių serverių skaičius

iv **Taikymas pramonėje**

- Pažangieji tinklai
- E. sveikata
- E. prekyba
- Intelektinė transporto sistema
- E. valdžia

Vertinimo metodas

KGI yra kiekybinio ir kokybinio vertinimo balais modelis. Vertinimą atliko „Economist Intelligence Unit“, naudodamas turimų statistinių šaltinių kiekybinius rodiklius ir atlikdamas skaičiavimus, kai duomenų trūko. Pagrindiniai naudojami šaltiniai: „Economist Intelligence Unit“, Jungtinių Tautų švietimo, mokslo ir kultūros organizacija (UNESCO), Tarptautinė telekomunikacijų sąjunga (ITU) ir Pasaulio bankas.

A.11 Kibernetinės galios indeksas (KGI)

Šiame skirsnyje apibendrinamos pagrindinės esamų brandos modelių analizės išvados. 5 lentelėje – Nagrinėtų brandos modelių apžvalga – pateikiama kiekvieno modelio pagrindinių charakteristikų apžvalga pagal modifikuotą J. Beckerio modelį. 6 lentelėje – Brandos lygių palyginimas – pateikiamos nagrinėtų modelių brandos lygių aukšto lygio apibrėžtys. 7 lentelėje pateikiama kiekvieno modelio matmenų arba požymių apžvalga.

5 lentelė. Nagrinėtų brandos modelių apžvalga

Modelio pavadinimas	Institucinis šaltinis	Tikslas	Tikslinė auditorija	Lygių skaičius	Požymių skaičius	Vertinimo metodas	Rezultatų pateikimas
Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis (CMM)	Visuotinis kibernetinio saugumo gebėjimų centras Oksfordo universitetas	Didinti kibernetinio saugumo gebėjimų stiprinimo mastą ir veiksmingumą tarptautiniu mastu	Šalys	5	5 pagrindiniai matmenys	Bendradarbiavimas su vietos organizacija siekiant patobulinti modelį prieš jį taikant nacionaliniu lygmeniu	5 dalių radaras
Kibernetinio saugumo pajėgumų brandos modelis (C2M2)	JAV energetikos departamentas (DOE)	Padėti organizacijoms įvertinti ir tobulinti savo kibernetinio saugumo programas ir didinti veiklos atsparumą	Visų sektorių, rūšių ir dydžių organizacijos	4	10 pagrindinių sričių	Įsivertinimo metodika ir priemonių rinkinys	Balų kortelė su skritulinėmis diagramomis
Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistema	Nacionalinis standartų ir technologijų institutas (NIST)	Sistema, kuria siekiama pateikti gaires dėl veiklos kibernetinio saugumo srityje, ir valdyti riziką organizacijose	Organizacijos	Netaikoma (4 pakopos)	5 pagrindinės funkcijos	Įsivertinimas	-
Kataro kibernetinio saugumo pajėgumų brandos modelis (Q-C2M2)	Kataro universiteto Teisės kolegija	Pateikti veiksmingą modelį, kurį būtų galima naudoti Kataro kibernetinio saugumo sistemai palyginti, įvertinti ir tobulinti	Kataro organizacijos	5	5 pagrindinės sritys	–	-
Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)	JAV gynybos departamentas (DOD)	Skatinti informacijos apsaugos gerąją patirtį kibernetinio saugumo srityje	Gynybos pramonės bazės sektoriaus (DIB) organizacijos	5	17 pagrindinių sričių	Trečiųjų šalių auditorių atliekamas vertinimas	-
Bendruomenės kibernetinio saugumo brandos modelis (CCSMM)	Teksaso universiteto Infrastruktūros užtikrinimo ir apsaugos centras	Nustatyti dabartinį bendruomenės statusą jos kibernetinio pasirengimo srityje ir pateikti gaires, kaip bendruomenės galėtų stebėti savo pasirengimo pastangas	Bendruomenės (vietos arba valstijų vyriausybės)	5	6 pagrindiniai matmenys	Vertinimas bendruomenėse, dalyvaujant valstybinėms ir federalinėms teisėsaugos institucijoms	-
NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis (ISMM)	Kompiuterių mokslo ir inžinerijos kolegija Karaliaus Fahdo naftos ir mineralų universitetas, Dahranas, Saudo Arabija	Sudaryti sąlygas organizacijoms vertinti savo įgyvendinimo pažangą laikui bėgant, siekiant užtikrinti, kad jos išsaugotų pageidaujamą saugumo padėtį	Organizacijos	5	23 vertinamos sritys	–	-
Viešojo sektoriaus vidaus audito pajėgumų modelis (IA-CM)	Vidaus auditorių mokslinių tyrimų fondo institutas	Stiprinti vidaus audito pajėgumą ir tarpininkavimą pasitelkiant įsivertinimą viešajame sektoriuje	Viešojo sektoriaus organizacijos	5	6 elementai	Įsivertinimas	-
Visuotinis kibernetinio saugumo indeksas (VKSI)	Tarptautinė telekomunikacijų sąjunga (ITU)	Peržiūrėti įsipareigojimą dėl kibernetinio saugumo, apžvelgti padėtį ir padėti šalims nustatyti tobulintinas sritis kibernetinio saugumo srityje	Šalys	Netaikoma	5 ramsčiai	Įsivertinimas	Reitingų lentelė

Kibernetinės galios indeksas (KGI)	„Economist Intelligence Unit“ ir „Booz Allen Hamilton“	Palyginti G 20 šalių pajėgumą atremti kibernetinius išpuolius ir diegti klestinčiai ir saugiai ekonomikai būtiną skaitmeninę infrastruktūrą	G 20 šalys	Netaikoma	4 kategorijos	„Economist Intelligence Unit“ atliekama lyginamoji analizė	Reitingų lentelė

6 lentelė. Brandos lygių palyginimas

Modelis	1 lygis	2 lygis	3 lygis	4 lygis	5 lygis
Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis (CMM)	**Pradinis** Kibernetinio saugumo brandos nėra arba yra tik jos užuomazgos. Galbūt vyksta pradinės diskusijos dėl kibernetinio saugumo gebėjimų kūrimo, tačiau konkrečių veiksmų nesiimta. Šiame etape nėra jokių pastebimų įrodymų.	**Formavimas** Kai kurie aspektų požymiai ryškėja ir yra formuojami, tačiau jie gali būti *ad hoc*, netvarkingi, netiksliai apibrėžti arba tiesiog nauji. Vis dėlto yra aiškių šios veiklos įrodymų.	**Įtvirtinimas** Aspekto elementai yra nustatyti ir veikia. Tačiau santykinis išteklių paskirstymas nėra iki galo apgalvotas. Priimta mažai kompromisinių sprendimų dėl „santykinių“ investicijų į įvairius šio aspekto elementus. Vis dėlto aspektas yra funkcionalus ir apibrėžtas.	**Strateginis** Nuspręsta, kurios aspekto dalys yra svarbios ir kurios mažiau svarbios konkrečiai organizacijai ar šaliai. Strateginis etapas atspindi tai, kad šie sprendimai buvo priimti atsižvelgiant į konkrečias šalies ar organizacijos aplinkybes.	**Dinaminis** Jau įdiegti aiškūs mechanizmai strategijai keisti atsižvelgiant į vyraujančias aplinkybes, pvz., grėsmių aplinkos technologijas, pasaulinį konfliktą arba svarbius pokyčius vienoje iš susirūpinimą keliančių sričių (pvz., kibernetinių nusikaltimų ar privatumo). Dinamiškos organizacijos yra parengusios strategijų keitimo metodus. Šio etapo požymiai – greitas sprendimų priėmimas, išteklių perskirstymas ir nuolatinis dėmesys kintančiai aplinkai.
Kibernetinio saugumo pajėgumų brandos modelis (C2M2)	**0 BRL** Praktika nevykdoma.	**1 BRL** Pradinė praktika vykdoma, tačiau gali būti *ad hoc*.	**2 BRL** Valdymo ypatybės: praktika dokumentuojama; paskirti tinkami ištekliai procesui remti; praktiką vykdantys darbuotojai turi reikiamus įgūdžius ir žinias; praktikos vykdymo atsakomybės sritys ir įgaliojimai paskirstyti. Metodo ypatybė: praktika yra išsamesnė arba pažangesnė nei 1 BRL.	**3 BRL** Valdymo ypatybės: veikla vykdoma vadovaujantis politika (arba kitomis organizacinėmis gairėmis); konkrečios srities veiklos efektyvumo tikslai nustatyti ir stebimi, kad būtų galima stebėti pažangą; konkrečios srities veiklos dokumentuota praktika yra standartizuota ir tobulinama visoje įstaigoje. Metodo ypatybė: praktika yra išsamesnė arba pažangesnė nei 2 BRL.	–
NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis (ISMM)	**Procesas vykdomas**	**Procesas valdomas**	**Procesas nusistovėjęs**	**Procesas nuspėjamas**	**Procesas optimizuojamas**

Kataro kibernetinio saugumo pajėgumų brandos modelis (Q-C2M2)	**Inicijavimas** Kai kuriose srityse taikoma *ad hoc* kibernetinio saugumo praktika ir procesai.	**Plėtojimas** Įgyvendinama politika ir praktika su kibernetiniu saugumu susijusiai veiklai srityse plėtoti ir tobulinti, siekiant pasiūlyti naujų įgyvendintinų veiklų.	**Įgyvendinimas** Priimta politika, kuria siekiama įgyvendinti visą su kibernetiniu saugumu susijusią veiklą srityse, kad įgyvendinimas būtų užbaigtas tam tikru metu.	**Pritaikymas** Iš naujo apsvarstoma ir peržiūrima kibernetinio saugumo srities veikla ir tvirtinama praktika, pagrįsta prognozavimo rodikliais, nustatytais remiantis ankstesne patirtimi ir priemonėmis.	**Paslankumas** Tęsiamas pritaikymo etapas, daugiau dėmesio skiriant paslankumui ir spartai įgyvendinant veiklą srityse.
Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)	**Procesai: vykdoma** Kadangi organizacija gali vykdyti šią praktiką tik *ad hoc* būdu ir gali kliautis dokumentavimo procesu arba ne, 1 lygio atveju branda nevertinama. **Praktika: bazinė kibernetinė higiena** 1 lygyje daugiausia dėmesio skiriama FSI (federalinių sutarčių informacijos) apsaugai ir jį sudaro tik ta praktika, kuri atitinka pagrindinius apsaugos reikalavimus.	**Procesai: dokumentuota** 2 lygyje reikalaujama, kad organizacija nustatytų ir dokumentuotų savo pastangų, susijusių su CMMC, įgyvendinimu, praktiką ir politiką. Praktikos dokumentavimas leidžia asmenims ją taikyti pakartotinai. Organizacijos išsiugdo brandžius pajėgumus dokumentuodamos savo procesus ir kartu juos naudodamos. **Praktika: vidutinė kibernetinė higiena** 2 lygis naudojamas persikeliant iš 1 lygio į 3 ir jį sudaro NIST SP 800-171 nurodytų saugumo reikalavimų poaibis, taip pat kituose standartuose ir informacijos šaltiniuose numatyta praktika.	**Procesai: valdoma** 3 lygyje reikalaujama, kad organizacija parengtų, palaikytų ir aprūpintų ištekliais planą, kuriame būtų atskleistas praktinis veiklos valdymas. Į planą gali būti įtraukta informacija apie misijas, tikslus, projektų planus, išteklių paskirstymą, reikiamą mokymą ir atitinkamų suinteresuotųjų subjektų dalyvavimą. **Praktika: gera kibernetinė higiena** 3 lygyje daugiausia dėmesio skiriama kontroliuojamos neįslaptintos informacijos (KNI) apsaugai ir jis apima visus saugumo reikalavimus, nurodytus NIST SP 800-171, taip pat papildomą kituose standartuose numatytą praktiką ir nuorodas į grėsmių mažinimą.	**Procesai: peržiūrėta** 4 lygyje reikalaujama, kad organizacija peržiūrėtų ir įvertintų veiksmingumo užtikrinimo praktiką. Organizacijos gali ne tik vertinti veiksmingumą, bet ir prireikus imtis taisomųjų veiksmų ir nuolat informuoti apie būseną ar problemas aukštesnio lygio vadovybę. **Praktika: iniciatyvi** 4 lygis orientuotas į KNI (kontroliuojamos neįslaptintos informacijos) apsaugą ir apima sugriežtintų saugumo reikalavimų pogrupį. Šia praktika stiprinami organizacijos pajėgumai nustatyti besikeičiančią taktiką, metodus ir procedūras, į juos reaguoti ir prie jų prisitaikyti.	**Procesai: optimizuojama** 5 lygyje reikalaujama, kad organizacija standartizuotų ir optimizuotų procesų įgyvendinimą visoje organizacijoje. **Praktika: pažangi / iniciatyvi** 5 lygyje daugiausia dėmesio skiriama kontroliuojamos neįslaptintos informacijos (KNI) apsaugai. Papildoma praktika didinamas kibernetinio saugumo pajėgumų išsamumas ir sudėtingumas.
Bendruomenės kibernetinio saugumo brandos modelis (CCSMM)	**Informacija apie saugumą** Pagrindinis šio lygio veiklos tikslas – informuoti asmenis ir organizacijas apie grėsmes, problemas ir su kibernetiniu saugumu susijusius klausimus.	**Procesų plėtojimas** Lygis, skirtas padėti bendruomenėms nustatyti saugumo procesus, reikalingus siekiant veiksmingai spręsti kibernetinio saugumo problemas, ir juos tobulinti.	**Galimybė susipažinti su informacija** Sukurta siekiant pagerinti dalijimosi informacija mechanizmus bendruomenėje, kad bendruomenė galėtų veiksmingai susieti informaciją, kuri, atrodo, skiriasi.	**Taktikos plėtojimas** Šio lygio elementais siekiama kurti geresnius ir iniciatyvesnius išpuolių nustatymo ir reagavimo į juos metodus. Šiame lygyje turėtų būti įdiegta dauguma prevencijos metodų.	**Visapusiškas saugumo veiklos pajėgumas** Šis lygis atspindi tuos elementus, kurie turėtų būti įdiegti, kad bet kuri organizacija galėtų manyti esanti visiškai pasirengusi reaguoti į bet kokios rūšies kibernetinę grėsmę.
Viešojo sektoriaus vidaus audito pajėgumų modelis (IA-CM)	**Pradinis** Nėra tvarių, pakartojamų pajėgumų – priklauso nuo atskirų pastangų	**Infrastruktūros** Tvari ir kartotinė praktika ir procedūros	**Integruotas** Vienodai taikomas integruotas valdymas ir profesinė praktika	**Valdomas** Integruojama visos organizacijos informacija, kad būtų pagerintas valdymas ir rizikos valdymas	**Optimizuojamas** Mokymasis iš organizacijos vidaus ir išorės subjektų siekiant nuolat tobulėti

7 lentelė. Požymių ir (arba) matmenų palyginimas

	Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis (CMM)	Kibernetinio saugumo pajėgumų brandos modelis (C2M2)	Kataro kibernetinio saugumo pajėgumų brandos modelis (Q-C2M2)	Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)	Kibernetinio saugumo brandos modelių sertifikavimas (CMMC)	NIST kibernetinio saugumo sistemos informacijos saugumo brandos modelis (ISMM)	Ypatingos svarbos infrastruktūros kibernetinio saugumo didinimo sistema	Visuotinis kibernetinio saugumo indeksas (VKSI)	Kibernetinės galios indeksas (KGI)
Lygiai	Penki matmenys, suskirstyti į kelis veiksnius, apimančius įvairius aspektus ir rodiklius (4 pav)	Dešimt sričių, įskaitant išskirtinį valdymo tikslą ir kelis metodo tikslus (6 pav.)	Penkios sritys, suskirstytos į posričius	Septyniolika sričių, suskirstytų į procesus ir nuo vieno iki daugiau pajėgumų, kurie vėliau išskaidomi į praktikas (9 pav.)	Šeši pagrindiniai matmenys	Dvidešimt trys vertinamos sritys	Penkios funkcijos su pagrindinėmis kategorijomis ir pakategorėmis (8 pav.)	Penki ramsčiai, įskaitant kelis rodiklius	Keturios kategorijos su keliais rodikliais
Požymiai / matmenys	i Kibernetinio saugumo politikos ir strategijos rengimas ii Atsakingos visuomenės kibernetinio saugumo kultūros skatinimas visuomenėje iii Žinių apie kibernetinį saugumą plėtojimas iv Veiksmingų teisinių ir reguliavimo sistemų kūrimas v Rizikos kontrolė pasitelkiant standartus, organizacijas ir technologijas	i Rizikos valdymas ii Išteklių, pokyčių ir konfigūracijos valdymas iii Tapatybės ir prieigos valdymas iv Grėsmių ir pažeidžiamumo valdymas v Informuotumas apie padėtį vi Reagavimas į įvykius ir incidentus vii Tiekimo grandinės ir išorės priklausomybių valdymas viii Darbo jėgos valdymas ix Kibernetinio saugumo struktūra x Kibernetinio saugumo programos valdymas	i Supratimas (kibernetinės erdvės valdymas, ištekliai, rizika ir mokymas) ii Apsauga (duomenų saugumas, technologijų saugumas, prieigos kontrolės saugumas, ryšių saugumas ir personalo patikimumas) iii Poveikis (stebėsena, incidentų valdymas, aptikimas, analizė ir poveikis) iv Reagavimas (reagavimo planavimas, švelninimas ir reagavimo komunikavimas) v Išlaikymas (atkūrimo planavimas, tęstinumo valdymas, tobulinimas ir išorės subjektų priklausomybės)	i Prieigos kontrolė ii Išteklių valdymas iii Auditas ir atskaitomybė iv Informuotumas ir mokymas v Konfigūracijos valdymas vi Tapatybės ir tapatumo nustatymas vii Reagavimas į incidentus viii Priežiūra ix Žiniasklaidos apsauga x Personalo patikimumas xi Fizinė apsauga xii Atkūrimas xiii Rizikos valdymas xiv Saugumo vertinimas xv Informuotumas apie padėtį xvi Sistemų ir ryšių apsauga xvii Sistemos ir informacijos vientisumas	i Pašalintos grėsmės ii Metrika iii Dalijimasis informacija iv Technologija v Mokymas vi Bandymas	i Išteklių valdymas ii Verslo aplinka iii Valdymas iv Rizikos vertinimas v Rizikos valdymo strategija vi Atitikties vertinimas vii Prieigos kontrolė viii Informuotumas ir mokymas ix Duomenų saugumas x Informacijos apsaugos procesai ir procedūros xi Priežiūra xii Apsauginė technologija xiii Anomalijos ir įvykiai xiv Nuolatinė saugumo stebėsena xv Aptikimo procesai xvi Reagavimo planavimas xvii Atsakomieji ryšiai xviii Reagavimo analizė xix Reagavimo švelninimas xx Reagavimo patobulinimai xxi Atkūrimo planavimas xxii Atkūrimo patobulinimai xxiii Pranešimas apie atkūrimą	i Nustatyti ii Apsaugoti iii Aptikti iv Reaguoti v Atkurti	i Teisinio pobūdžio ii Techninio pobūdžio iii Organizacinio pobūdžio iv Gebėjimų stiprinimo v Bendradarbiavimo	i Teisinė ir reguliavimo sistema ii Ekonominės ir socialinės aplinkybės iii Technologijų infrastruktūra iv Taikymas pramonėje

B PRIEDAS. DOKUMENTŲ TYRIMO BIBLIOGRAFIJA

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

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

Anna, S., *et al.* (2016). Stocktaking, analysis and recommendations on the protection of CIIs. Skelbiama adresu 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. Skelbiama adresu https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf

Belgian Government (2012). Cyber Security Strategy. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019). National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Skelbiama adresu 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

Council of Ministers (2019). Portuguese Official Journal, Series 1 — No. 108 - Resolution of the Council of Ministers No. 92/2019. Skelbiama adresu 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 (data nenurodyta). Skelbiama adresu https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011).

Specialised cybercrime units – Good practice study. Skelbiama adresu https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (data nenurodyta). Skelbiama adresu 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. (data nenurodyta). Welcome to the NCSS Training Tool.

Dekker, M. A. C. (2014). Technical Guideline on Incident Reporting. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Europos Komisija (2012). Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje. Skelbiama adresu https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

European Network and Information Security Agency (2012). NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

European Network and Information Security Agency (2012). NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

European Network and Information Security Agency (2016). Guidelines for SMEs on the security of personal data processing.

European Network and Information Security Agency (2016). NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

European Union and Agency for Network and Information Security (2017). Handbook on security of personal data processing. Skelbiama adresu http://dx.publications.europa.eu/10.2824/569768

European Union and Agency for Network and Information Security (2014). ENISA CERT inventory. Inventory of CERT teams and activities in Europe. Skelbiama adresu 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. Skelbiama adresu https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Federal Chancellery of the Republic of Austria (2013). Austrian Cyber Security Strategy. Skelbiama adresu 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

Federal Ministry of the Interior (2011). Cyber Security Strategy for Germany. Skelbiama adresu 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. Skelbiama adresu http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L. European Union and European Network and Information Security Agency (2015). The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Skelbiama adresu http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

French Prime Minister's Office (2014). French National Digital Security Strategy. Skelbiama adresu 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. Skelbiama adresu 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*. Skelbiama adresu https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Government of Bulgaria (2015). National Cyber Security Strategy – Cyber-resistant Bulgaria 2020.

Government of Croatia (2015). The National Cyber Security Strategy of The Republic of Croatia. Skelbiama adresu https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Government of Greece (2017). National Cyber Security Strategy. Skelbiama adresu 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

Government of Hungary (2018). Strategy for the Security of Network and Information Systems. Skelbiama adresu 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

Government of Ireland (2019). National Cyber Security Strategy. Skelbiama adresu https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Government of Ireland (2019).. National Cyber Security Strategy. Skelbiama adresu 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 (ed.) (2009). Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

International Telecommunication Union (ITU) (2018). The Global Cybersecurity Index. Skelbiama adresu https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunication Union (ITU) (2018). Guide to developing a national cybersecurity strategy. Skelbiama adresu 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 Government (2014). Cyber Security Strategy of Latvia. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministry for Competitiveness and Digital, Maritime and Services Economy (2016). Malta Cyber Security Strategy. Skelbiama adresu 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

Ministry of Economic Affairs and Communications (2019). Cybersecurity Strategy – Republic of Estonia. Skelbiama adresu https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Lietuvos Respublikos krašto apsaugos ministerija (2018). Nacionalinė kibernetinio saugumo strategija

National Cyber Security Centre (2015). National Cyber Security Strategy of the Czech Republic. Skelbiama adresu https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cyber Security Strategies – Interactive Map (data nenurodyta). Skelbiama adresu https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

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

National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Skelbiama adresu http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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

OECD, European Union and Joint Research Centre – European Commission (2008). Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Skelbiama adresu https://www.oecd.org/sdd/42495745.pdf

Office of the commissioner of Electronic Communications and Postal Regulations (2012). Cybersecurity Strategy of the Republic of Cyprus.

Europos Sąjungos oficialusis leidinys (2008). 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. Skelbiama adresu https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Organisation for Economic Co-operation and Development (OECD) (2012). Cybersecurity policy making at a turning point. Skelbiama adresu 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.

Presidency of the Council of Ministers (2017). The Italian Cybersecurity Action Plan. Skelbiama adresu 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. Skelbiama adresu http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Romanian Government (2013). Cyber security strategy of Romania. Skelbiama adresu 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., European Union Agency for Cybersecurity (2019). Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Skelbiama adresu https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN

Secretariat of the Security Committee (2019). Finland's Cyber Security Strategy 2019. Skelbiama adresu https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovakian Government (2015). Cyber Security Concept of the Slovak Republic. Skelbiama adresu 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). 2016 m. liepos 6 d. Europos Parlamento ir Tarybos Direktyva 2016/1148/ES

Smith, R. (2016). 2016 m. liepos 6 d. Europos Parlamento ir Tarybos Direktyva 2016/1148/ES, Smith, R., *Core EU Legislation*. London: Macmillan Education. Skelbiama adresu https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=EN

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

Swedish Government (2017). Nationell strategi för samhällets informations- och cybersäkerhet. Skelbiama adresu https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

The Danish Government – Ministry of Finance (2018). Danish Cyber and Information Security Strategy. Skelbiama adresu https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

The Federal Council (2018). National strategy for the protection of Switzerland against cyber risks.

The Luxembourguish Government Council (2018). National Cybersecurity Strategy. Skelbiama adresu 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

The Netherlands Governement (2018). National Cyber Security Agenda. Skelbiama adresu 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

The White House (2018). National Cyber Strategy of the United States of America. Skelbiama adresu https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

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

Trimintzios, P., Gavrila, R., European Network and Information Security Agency (2013). National-level risk assessments: an analysis report. Skelbiama adresu 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. Skelbiama adresu 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. Skelbiama adresu http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016–2021 (2016). Skelbiama adresu 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. Skelbiama adresu https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

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

C PRIEDAS. KITI NAGRINĖTI TIKSLAI

Toliau nurodyti tikslai buvo nagrinėjami atliekant dokumentų tyrimą ir ENISA vykdytus pokalbius. Šie tikslai nėra įtraukti į nacionalinių pajėgumų vertinimo sistemą, tačiau jie atspindi temas, kurias verta aptarti. Kiekviename iš tolesnių poskyrių bus paaiškinta, kodėl tikslas buvo atmestas.

- Parengti konkretiems sektoriams skirtas kibernetinio saugumo strategijas.
- Kovoti su dezinformacijos kampanijomis.
- Saugios pažangiosios technologijos (5G, dirbtinis intelektas, kvantinė kompiuterija ir kt.).
- Užtikrinti duomenų suverenumą.
- Teikti paskatas plėtoti draudimo kibernetinėje erdvėje sektorių.

Parengti konkretiems sektoriams skirtas kibernetinio saugumo strategijas

Priėmus konkretiems sektoriams skirtas strategijas, orientuotas į sektorių intervencines priemones ir paskatas, neabejotinai sustiprėja decentralizuoti pajėgumai. Tai ypač būdinga valstybėms narėms, kurių esminių paslaugų operatoriai turi veikti pagal skirtingas sistemas ir taisykles ir kuriose yra daug dėl universalaus kibernetinio saugumo pobūdžio priklausomų subjektų. Iš tiesų keliose valstybėse narėse yra dešimtys kiekvieno sektoriaus ypatumus išmanančių nacionalinių valdžios institucijų ir reguliavimo institucijų, įgaliotų užtikrinti kiekvieno sektoriaus reguliavimo vykdymą.

Pavyzdžiui, Danija pradėjo įgyvendinti šešias tikslines strategijas, skirtas ypatingos svarbos sektorių pastangoms kibernetinio ir informacijos saugumo srityje, kad būtų stiprinami decentralizuoti kibernetinio ir informacijos saugumo pajėgumai. Kiekvienas sektoriaus skyrius, be kita ko, prisidės prie grėsmių vertinimo sektoriaus lygmeniu, stebėsenos, pasirengimo pratybų, saugumo sistemų kūrimo, dalijimosi žiniomis ir nurodymų. Konkretiems sektoriams skirtos strategijos apima šiuos sektorius:

- energetikos;
- sveikatos priežiūros;
- transporto;
- telekomunikacijų;
- finansų ir
- jūrų.

Kitos valstybės narės išreiškė norą apsvarstyti konkretiems sektoriams skirtas kibernetinio saugumo strategijas, kad jos atitiktų visus reguliavimo reikalavimus. Vis dėlto reikia pažymėti, kad toks tikslas gali tikti ne visoms valstybėms narėms, – tai priklauso nuo jų dydžio, nacionalinės politikos ir brandos. Kadangi buvo labai sunku užtikrinti, kad sistema aprėptų visus ypatumus, ENISA šio tikslo į sistemą neįtraukė.

Kovoti su dezinformacijos kampanijomis

Valstybės narės savo nacionalinėse kibernetinio saugumo strategijose užtikrina pagrindinių principų, kaip antai žmogaus teisių, skaidrumo ir visuomenės pasitikėjimo, apsaugą. Tai labai svarbu, ypač kalbant apie dezinformaciją, kuri skleidžiama per tradicines naujienų žiniasklaidos

priemones arba socialinės žiniasklaidos platformose. Be to, kibernetinis saugumas šiuo metu yra vienas didžiausių iššūkių prieš rinkimus. Iš tiesų ne vienoje šalyje, kuri ruošėsi svarbiems rinkimams, pastebėta tokių reiškinių kaip melagingos informacijos arba neigiamos propagandos skleidimas. Ši grėsmė gali pakenkti ES demokratiniam procesui. Europos lygmeniu Komisija parengė veiksmų planą[32], kuriuo siekiama sustiprinti kovą su dezinformacija Europoje. Šiame plane daugiausia dėmesio skiriama 4 pagrindinėms sritims (aptikimo, bendradarbiavimo, bendradarbiavimo su interneto platformomis ir informuotumo). Juo siekiama stiprinti ES pajėgumus ir valstybių narių bendradarbiavimą.

4 iš 19 apklaustų šalių išreiškė ketinimą savo NKSS spręsti dezinformacijos ir propagandos problemą.

Pavyzdžiui, Prancūzijos NKSS[33] pažymima: „valstybė privalo informuoti piliečius apie manipuliavimo ir propagandos metodų, kuriuos taiko internete veikiantys piktavaliai subjektai, riziką. Pavyzdžiui, po 2015 m. sausio mėn. įvykdytų teroristinių išpuolių prieš Prancūziją vyriausybė sukūrė informacinę platformą apie rizikas, susijusias su islamo radikalėjimu per elektroninių ryšių tinklus – Stop-djihadisme.gouv.fr.“ Šis metodas galėtų būti išplėtotas, kad galėtų būti taikomas reaguojant į kitus propagandos ar destabilizavimo reiškinius.

Kalbant apie kitą pavyzdį, 2019–2024 m. Lenkijos NKSS[34] teigiama: „atsižvelgiant į manipuliacinę veiklą, pavyzdžiui, dezinformacijos kampanijas, reikia imtis sistemingų veiksmų ir didinti piliečių informuotumą tikrinant informacijos autentiškumą ir reaguojant į bandymus ją iškraipyti.“

Vis dėlto per ENISA surengtus pokalbius kelios valstybės narės sutiko, kad jos šio klausimo nėra įtraukusios į savo NKSS kaip grėsmės kibernetiniam saugumui, o veikiau sprendžia jį platesniu visuomenės lygmeniu, pvz., per politines iniciatyvas.

Saugios pažangiosios technologijos (5G ryšys, dirbtinis intelektas, kvantinė kompiuterija ir kt.)

Dabartinė kibernetinių grėsmių aplinka toliau plečiasi, todėl kuriant naujas technologijas greičiausiai didės kibernetinių išpuolių intensyvumas ir skaičius, taip pat taps įvairesni grėsmės subjektų naudojami metodai, priemonės ir taikiniai. Šie nauji technologiniai sprendimai – pažangiosios technologijos – gali tapti Europos skaitmeninės rinkos sudedamosiomis dalimis. Siekiant apsaugoti didėjančią valstybių narių skaitmeninę priklausomybę ir naujų technologijų atsiradimą, turėtų būti nustatytos paskatos ir visavertė politika, kuria būtų remiamas saugus ir patikimas šių technologijų plėtojimas ir diegimas ES.

Atliekant valstybių narių NKSS dokumentų tyrimą, valstybėms narėms pateiktos šios pažangiosios technologijos: 5G, DI, kvantinė kompiuterija, kriptografija, paribio kompiuterija, susietosios ir autonominės transporto priemonės, didieji ir išmanieji duomenys, blokų grandinė, robotika ir daiktų internetas.

Konkrečiau, 2020 m. pradžioje Europos Komisija paskelbė komunikatą, kuriame valstybės narės raginamos imtis veiksmų, kad būtų įgyvendintos 5G priemonių rinkinio išvadose rekomenduojamos priemonės[35]. Šis 5G priemonių rinkinys parengtas po to, kai 2019 m. Komisija priėmė Rekomendaciją (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo, kurioje raginama laikytis bendro Europos požiūrio į 5G tinklų saugumą[36].

[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
[36] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32019H0534.

Per ENISA surengtus pokalbiuose išaiškėjo, kad ši tema yra veikiau universali tema, nagrinėjama NKSS, o ne konkretus tikslas *per se*.

Užtikrinti duomenų suverenumą

Viena vertus, kibernetinė erdvė gali būti vertinama kaip puiki visuotinė bendroji erdvė, kuri yra lengvai prieinama, užtikrinanti aukšto lygio junglumą ir galinti suteikti didelių socialinio ir ekonominio augimo galimybių. Kita vertus, kibernetinei erdvei taip pat būdinga silpna jurisdikcija, sunkumas priskirti veiksmus, sienų nebuvimas ir jungtinės sistemos, kurios gali būti akytos ir kurių duomenys gali būti pavagiami ar net prieinami užsienio šalių vyriausybėms. Be šių dviejų perspektyvų, skaitmeninei ekosistemai būdinga tai, kad internetinių paslaugų platformos ir infrastruktūra yra sutelktos vos kelių subjektų rankose. Visi minėti aspektai verčia valstybes nares skatinti skaitmeninį suverenumą. Skaitmeninio suverenumo užtikrinimas reiškia, kad piliečiai ir įmonės gali visapusiškai klestėti naudodamiesi patikimomis skaitmeninėmis paslaugomis ir IRT produktais, nebijodami dėl savo asmens duomenų, skaitmeninio turto, ekonominio savarankiškumo ar politinės įtakos.

Duomenų suverenumą, arba skaitmeninį suverenumą, remia valstybės narės nacionaliniu ir Europos lygmenimis. Nors atrodo, kad valstybės narės šio klausimo tiesiogiai nesprendžia savo NKSS kaip konkretaus tikslo, jos šį klausimą sprendžia kaip universalų principą arba išdėsto savo ketinimą užtikrinti skaitmeninį suverenumą nacionaliniu lygmeniu, kaip apibrėžta *ad hoc* leidiniuose, daugiausia dėmesio skirdamos svarbiausioms technologijoms. Pavyzdžiui, 2018 m. Prancūzijos kibernetinės gynybos strateginėje apžvalgoje teigiama, kad „siekiant užtikrinti skaitmeninį suverenumą itin svarbu kontroliuoti šias technologijas: ryšių šifravimą, kibernetinių išpuolių aptikimą, profesionalų mobiliųjį radijo ryšį, debesijos kompiuteriją ir dirbtinį intelektą“[37].

Europos lygmeniu valstybės narės aktyviai dalyvauja rengiant Europos duomenų strategiją (COM/2020/66 *final*) ir kuriant IRT skaitmeninių produktų, paslaugų ir procesų ES sertifikavimo sistemą, nustatytą ES kibernetinio saugumo aktu (2019/881), siekdamos užtikrinti strateginį skaitmeninį savarankiškumą Europos lygmeniu.

Pokalbiai su valstybėmis narėmis atskleidė, kad skaitmeninis suverenumas dažnai laikomas platesnio masto klausimu nei tik kibernetinis saugumas. Todėl valstybės narės šio klausimo nesprendžia savo NKSS, o tos, kurios sprendžia, nelaiko jo konkrečiu tikslu *per se*.

Teikti paskatas plėtoti kibernetinių rizikų draudimo sektorių

Žvelgiant į dabartinį kibernetinių rizikų draudimo sektorių matyti, kad pasaulinė rinka neabejotinai išaugo. Tačiau jo gyvavimas dar tik prasidėjo, nes būtina surinkti duomenis ir sukurti daug precedentų (pvz., tylioji aprėptis, sisteminė kibernetiniam saugumui kylanti rizika ir kt.). Be to, apskaičiuoti nuostoliai, patirti dėl kibernetinių išpuolių visame pasaulyje, yra keliais lygiais didesni nei dabartiniai kibernetinių rizikų draudimo sektoriaus pajėgumai (TVF darbinis dokumentas „Kibernetiniam saugumui kylanti rizika finansų sektoriuje. Kiekybinio vertinimo sistema“ (WP/18/143). Vis dėlto kibernetinių rizikų draudimo sektoriaus plėtra neabejotinai gali būti pelninga ir duoti pradžią veiksmingiems mechanizmams. Iš tiesų kibernetinių rizikų draudimo mechanizmai gali padėti:

- didinti informuotumą apie kibernetines rizikas įmonėse;
- atlikti kiekybinį kibernetinių rizikų poveikio vertinimą;
- gerinti kibernetinės rizikos valdymą;
- teikti paramą organizacijoms, nukentėjusioms nuo kibernetinių išpuolių;
- padengti dėl kibernetinio išpuolio patirtą (turtinę ar neturtinę) žalą.

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Kai kurios valstybės narės ėmėsi veiksmų šiuo klausimu. Pavyzdžiai:

- Estija savo NKSS pritaikė požiūrį „palaukim ir pamatysim“: „Siekiant apskritai sušvelninti kibernetines rizikas privačiajame sektoriuje, bus analizuojama kibernetinių rizikų draudimo paslaugų paklausa ir pasiūla Estijoje ir tuo remiantis susitarta dėl susijusių šalių bendradarbiavimo principų, įskaitant dalijimąsi informacija, rizikos vertinimo rengimą ir pan. Šiandien Estijos rinkoje kibernetinių rizikų draudimo paslaugų teikėjų yra nedaug, todėl pirmiausia reikia nustatyti, kas ką siūlo. Draudimo suteikiamos apsaugos sudėtingumas dažnai laikomas kliūtimi plėtoti kibernetinių rizikų draudimo rinką.“
- Liuksemburgas savo NKSS konkrečiai pritaria kibernetinių rizikų draudimo sektoriaus plėtrai: „1 tikslas. Kurti naujus produktus ir paslaugas. Siekiant sutelkti rizikas ir paskatinti skaitmeninių kibernetinių incidentų aukas kreiptis pagalbos į ekspertus, kad incidentai būtų suvaldomi ir kad būtų atkurta nuo piktavališkų veiksmų nukentėjusi sistema, draudimo bendrovės bus skatinamos kurti konkrečius produktus, skirtus draudimui nuo kibernetinių rizikų.“

Respondentų atsakymai šia tema buvo gana įvairūs: kai kurios valstybės narės pareiškė neseniai ėmusios diskutuoti kibernetinių rizikų draudimo tema, o kitos pritarė, kad, nors ši tema daug žadanti, sektorius dar nėra pakankamai subrendęs. Vis dėlto daug respondentų pareiškė, jog ši tema nėra jų NKSS dalis, nes ji buvo laikoma pernelyg specifine arba nepatenkančia į NKSS taikymo sritį.

TP-02-21-253-LT-N

Apie Europos Sąjungos kibernetinio saugumo agentūrą

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra Sąjungos agentūra, kurios tikslas – pasiekti bendrą aukštą kibernetinio saugumo lygį visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įkurta 2004 m. ir sustiprinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų, kuriuose naudojamos kibernetinio saugumo sertifikavimo schemos, patikimumą, bendradarbiauja su valstybėmis narėmis ir ES įstaigomis ir padeda Europai pasirengti būsimiems kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra kartu su savo pagrindiniais suinteresuotaisiais subjektais siekia stiprinti pasitikėjimą susietąja ekonomika, didinti Sąjungos infrastruktūros atsparumą, užtikrinti Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos rasite svetainėje 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 978-92-9204-492-3
DOI 10.2824/588763