**VILNIAUS UNIVERSITETAS**
**ŠIAULIŲ AKADEMIJA**

INFORMACINIŲ TECHNOLOGIJŲ VALDYMO MAGISTRO STUDIJŲ PROGRAMA

**IGOR VERBICKIJ**

**Magistro studijų baigiamasis darbas**

# MAŽŲ IR VIDUTINIŲ ORGANIZACIJŲ TIS2 KIBERNETINIO SAUGUMO VERTINIMO INFORMACINĖS SISTEMOS PROJEKTAS

Darbo vadovas (-ė) asist. dr. Irma Šileikienė

Šiauliai, 2025

**Studijuojančiojo, teikiančio baigiamąjį darbą, GARANTIJA**

***WARRANTY of Final Thesis***

| | |
|---|---|
| Vardas, pavardė<br>*Name, Surname* | **Igor Verbickij** |
| Padalinys<br>*Faculty* | **Šiaulių akademija**<br>***Šiauliai Academy*** |
| Studijų programa<br>*Study Programme* | ***INFORMACINIŲ TECHNOLOGIJŲ VALDYMO STUDIJŲ PROGRAMA***<br>***Information Technology Management Study Programme*** |
| Darbo pavadinimas<br>*Thesis topic* | ***MAŽŲ IR VIDUTINIŲ ORGANIZACIJŲ TIS2 KIBERNETINIO SAUGUMO VERTINIMO INFORMACINĖS SISTEMOS PROJEKTAS***<br>***Project of an Information System for Assessing NIS2 Cybersecurity in Small and Medium-Sized Organizations*** |
| Darbo tipas<br>*Thesis type* | **Baigiamasis darbas**<br>***Final Thesis*** |

Garantuoju, kad mano baigiamasis darbas yra parengtas sąžiningai ir savarankiškai, kitų asmenų indėlio į parengtą darbą nėra. Jokių neteisėtų mokėjimų už šį darbą niekam nesu mokėjęs.
Šiame darbe tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos yra pažymėtos literatūros nuorodose.

*I guarantee that my thesis is prepared in good faith and independently, there is no contribution to this work from other individuals. I have not made any illegal payments related to this work.*
*Quotes from other sources directly or indirectly used in this thesis, are indicated in literature references.*

**Aš, Igor Verbickij, pateikdamas (-a) šį darbą, patvirtinu** (*pažymėti*) ☒

**Embargo laikotarpis**
***Embargo Period***

Prašau nustatyti šiam baigiamajam darbui toliau nurodytos trukmės embargo laikotarpį:
*I am requesting an embargo of this thesis for the period indicated below:*

☐ _____ mėnesių / *months*
(embargo laikotarpis negali viršyti 60 mėn. / *an embargo period shall not exceed 60 months*).

☒ Embargo laikotarpis nereikalingas / *no embargo requested.*

Embargo laikotarpio nustatymo priežastis / *Reason for embargo period*:

**VILNIAUS UNIVERSITETO ŠIAULIŲ AKADEMIJOS DIRBTINIO INTELEKTO ĮRANKIŲ NAUDOJIMO RAŠTO DARBUOSE DEKLARACIJA**

Vardas, pavardė: Igor Verbickij
Studijų programa, kursas: INFORMACINIŲ TECHNOLOGIJŲ VALDYMO MAGISTRO STUDIJŲ PROGRAMA
Rašto darbo pavadinimas: MAŽŲ IR VIDUTINIŲ ORGANIZACIJŲ TIS2 KIBERNETINIO SAUGUMO VERTINIMO INFORMACINĖS SISTEMOS PROJEKTAS
Rašto darbo tipas *(pvz., referatas, kursinis darbas, baigiamasis darbas):* Baigiamasis darbas
Modulio / dalyko pavadinimas *(išskyrus baigiamojo darbo atveju):*

Deklaracijos pateikimo data: 2025.12.01

Patvirtinu, kad vertinimui pateiktas savarankiškai atliktas rašto darbas yra parengtas laikantis Vilniaus universiteto Akademinės etikos kodekso[1], Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai[2], Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarkos[3] ir Dirbtinio intelekto naudojimo Vilniaus universitete gairių[4].
Pažymiu, kad rašto darbo rengimui *buvo naudojami / nebuvo naudojami (pabraukti tinkamą variantą)* generatyvinio dirbtinio intelekto (toliau - DI) įrankiai.
Tuo atveju, jei darbo rengimui buvo pasitelkti DI įrankiai, pateikiu tikslią ir išsamią informaciją apie jų naudojimo tikslus ir apimtį:

1. DI įrankiai:
   - Naudoti įrankiai (pvz.: Connected Papers, Midjourney, GitHub Copilot ar kiti, *įrašyti*): Cursor, Perplexity, ChatGPT
   - Naudojimo tikslas (duomenų rinkimas, redagavimas, vertimas, priedų generavimas ar kitas, *įrašyti*):
     vertimas, priedų rengimas, kodo tikrinimas

2. Esminiai DI panaudojimo atvejai:

| Darbo dalis/vieta (puslapis, pastraipa) | Naudojimo tikslas | Užklausų pavyzdžiai |
|---|---|---|
| 1,2 skyrius | Teksto vertimas | Išversk tekstą |
| 3, 4 skyrius | Priedų rengimas | Pagal pateiktą informaciją sugrupuok lentelę; |

[1] Vilniaus universiteto akademinės etikos kodeksas, https://www.vu.lt/site_files/Akademines_etikos_kodeksas_suvestine_redakcija.pdf
[2] Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai, 2024-05-21_Studijuojančiųjų_RD_rengimo_gynimo_ir_kaupimo_nuostatai.pdf
[3] Vilniaus universiteto Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarka, https://www.sa.vu.lt/external/sa/files/Studiju_skyrius/VUSA_Rasto_darb%C5%B3_rengimo_ir_gynimo_tvarka_2024.pdf
[4] Dirbtinio intelekto naudojimo Vilniaus universitete gairės, https://www.vu.lt/site_files/SPN-54_2024_priedas.pdf

| | | |
|---|---|---|
| 4 skyrius | Programinio kodo tikrinimas, kūrimas | Patikrink kodą, optimizuok kodą, parenk kodą |

3. Savarankiškumas ir autorystė:
    - Patvirtinu, kad esu atsakingas(-a) už rašto darbo savarankiškumą ir autorystę: visos DI sugeneruotos rašto darbo dalys mano atidžiai patikrintos, patikslintos, pataisytos ir pažymėtos literatūros nuorodose. Darbas parengtas užtikrinant jame pateikiamų DI įrankiais sugeneruotų teksto dalių ir (ar) priedų tikslumą, patikimumą ir korektiškumą;
    - Patvirtinu, kad DI įrankiai nenaudoti darbe pateikiamų duomenų, informacijos, autorių minčių klastojimui, iškraipymui ar kitokio pobūdžio klaidinančiam pateikimui.
4. Akademinė etika:
    - Patvirtinu, kad pateikta informacija apie DI įrankių naudojimą yra tiksli ir išsami;
    - Patvirtinu, kad DI įrankiai naudoti savarankiško duomenų rinkimo, tyrimo, analizės, teksto ar priedų (*pabraukti tinkamą; jei reikia, įrašyti papildomą informaciją* sisteminimui) (pa)pildymui, o ne kaip savarankiško darbo pakaitalas;
    - Suprantu, kad nenurodytas DI įrankių naudojimas gali būti laikomas draudimo plagijuoti pažeidimu, kuris numatytas Vilniaus universiteto Akademinės etikos kodekse.

# TURINYS

# PAVEIKSLŲ SĄRAŠAS

# LENTELIŲ SĄRAŠAS

# SANTRAUKA

Baigiamajame magistro darbe nagrinėjamas TIS2 direktyvos reikalavimų taikymas organizacijų kibernetinio saugumo vertinimui. Sprendžiama problema – kaip sudėtingus teisinius ir metodinius TIS2 reikalavimus paversti mažų ir vidutinių organizacijų išteklius atitinkančiu praktinio įsivertinimo įrankiu, o darbo tikslas – suprojektuoti informacinę sistemą, kuri, remdamasi TIS2 direktyva bei ją įgyvendinančiais teisės aktais, leistų atlikti organizacijos kibernetinio saugumo statuso identifikavimą, atitikties TIS2 reikalavimams vertinimą ir, remiantis vertinimo rezultatais, pateiktų detalų nustatytų trūkumų šalinimo įgyvendinimo planą. Darbe taikyti šie metodai: lyginamoji TIS2, NIST CSF 2.0, ISO/IEC 27001 ir DORA analizė, mokslinės literatūros ir teisės aktų analizė, ENISA gerųjų praktikų, įrankių techninės dokumentacijos bei kitų antrinių šaltinių analizė, programinės įrangos reikalavimų inžinerijos ir programinės įrangos projektavimo metodai. Remiantis analizės rezultatais, buvo sukurta adaptyvi TIS2 atitikties vertinimo metodika, apimanti subjekto kibernetinio statuso nustatymą, TIS2 reikalavimų dekonstrukcija grįstą klausimyną ir darbo suskaidymo struktūros principu paremtą trūkumų šalinimo įgyvendinimo planą. Praktinėje dalyje buvo sukurtas mažiausiai gyvybingo produkto (MVP) lygmens TIS2 vertinimo įrankis - kliento pusės vieno puslapio „React“ aplikacija, įgyvendinanti sukurtas teorines metodikas. Testavimo rezultatai parodė, kad sukurtas MVP atitinka suformuluotus funkcinius ir nefunkcinius reikalavimus. Darbo ribotumus lemia dinaminė teisinių aktų kaita ir empirinio išbandymo realiose organizacijose nebuvimas, tačiau buvo pasiektas tikslas – sukurta metodologiškai pagrįsta koncepcija ir techniškai įgyvendinta TIS2 atitikties vertinimo informacinės sistema, aktuali organizacijų pasirengimui kibernetinio saugumo reikalavimų įgyvendinimui, taip pat parengtas pagrindas tolimesniems kibernetinio saugumo atitikties vertinimo praktinio taikymo empiriniams tyrimams bei koncepcijos plėtojimui, įskaitant integraciją su organizacijose naudojamais trečiųjų šalių kibernetinio saugumo sprendimų duomenimis ir įrankio panaudojimą kaip auditavimo priemonę išorės auditoriams.

# SUMMARY

This master's thesis examines the application of the requirements of the TIS2 Directive to the assessment of organizations' cybersecurity. It addresses the problem of how to transform the complex legal and methodological requirements of TIS2 into a practical self-assessment tool that matches the resources of small and medium-sized organizations, and the aim of the thesis is to design an information system which, based on the TIS2 Directive and the legal acts implementing it, enables the identification of an organization's cybersecurity status, the assessment of its compliance with TIS2 requirements and, on the basis of the assessment results, provides a detailed implementation plan for remediating identified gaps. The following methods were applied in the thesis: comparative analysis of TIS2, NIST CSF 2.0, ISO/IEC 27001 and DORA, analysis of scientific literature and legal acts, analysis of ENISA best practices, technical documentation of tools and other secondary sources, as well as software requirements engineering and software design methods. Based on the results of the analysis, an adaptive TIS2 compliance assessment methodology was developed, covering the determination of the entity's cybersecurity status, a questionnaire based on a deconstruction of the TIS2 requirements, and a remediation implementation plan built on the principle of a work breakdown structure. In the practical part, a minimum viable product (MVP)-level TIS2 assessment tool was created – a client-side single-page React application implementing the developed theoretical methodologies. The testing results showed that the created MVP meets the formulated functional and non-functional requirements. The limitations of the thesis are determined by the dynamic evolution of the legal acts and the absence of empirical testing in real organizations; nevertheless, the aim has been achieved – a methodologically grounded concept and technically implemented TIS2 compliance assessment information system has been created, which is relevant for organizations' preparedness to implement cybersecurity requirements, and a basis has been laid for further empirical research on the practical application of cybersecurity compliance assessment and for the development of the concept, including integration with data from third-party cybersecurity solutions used in organizations and the use of the tool as an auditing instrument for external auditors.

# SANTRUMPŲ SĄRAŠAS

**AWS** – „Amazon Web Services“ debesų kompiuterijos paslaugų platforma.

**BIA** – verslo poveikio analizė (angl. *Business Impact Analysis*).

**CER** – Kritinių subjektų atsparumo direktyva (angl. *Critical Entities Resilience Directive*).

**CISO** – vyriausiasis informacijos saugumo pareigūnas (angl. *Chief Information Security Officer*).

**CMDB** – konfigūracijų valdymo duomenų bazė (angl. *Configuration Management Database*).

**CSF 2.0** – NIST kibernetinio saugumo pagrindų sistema 2.0 (angl. *Cybersecurity Framework 2.0*).

**CSIRT** – kibernetinių incidentų reagavimo komanda (angl. *Computer Security Incident Response Team*).

**CVD** – koordinuotas pažeidžiamumų atskleidimas (angl. *Coordinated Vulnerability Disclosure*).

**CVE** – bendras pažeidžiamumų ir eksploatavimo sąrašas (angl. *Common Vulnerabilities and Exposures*).

**DESI** – skaitmeninės ekonomikos ir visuomenės indeksas (angl. *Digital Economy and Society Index*).

**DORA** – Skaitmeninės veiklos atsparumo aktas finansų sektoriui (angl. *Digital Operational Resilience Act*).

**DSS, WBS** – darbo suskaidymo struktūra (angl. *Work Breakdown Structure*, WBS).

**ENISA** – Europos Sąjungos kibernetinio saugumo agentūra (angl. *European Union Agency for Cybersecurity*).

**FR** – funkcinis reikalavimas (angl. *Functional Requirement*).

**GDPR** – Bendrasis duomenų apsaugos reglamentas (angl. *General Data Protection Regulation*).

**GRC** – valdymo, rizikų ir atitikties valdymo modelis (angl. *Governance, Risk and Compliance*).

**IS** – informacinė sistema.

**ISO/IEC 27001** – informacijos saugumo valdymo sistemos standartas (angl. *Information Security Management System standard*).

**ISVS** – informacijos saugumo valdymo sistema.

**IT** – informacinės technologijos.

**ITSM** – IT paslaugų valdymas (angl. *IT Service Management*).

**KPI/KRI** – veiklos ir rizikos rodikliai (angl. *Key Performance Indicator, Key Risk Indicator*).

**KSĮ** – Lietuvos Respublikos kibernetinio saugumo įstatymas.

**KSIS** – Kibernetinio saugumo informacinė sistema.

**KSRA** – Kibernetinio saugumo reikalavimų aprašas.

**MDD** – modelių grindžiama plėtra (angl. *Model-Driven Development*).

**MVO** – mažos ir vidutinės organizacijos.

**MVP** – minimaliai gyvybingas produktas (angl. *Minimum Viable Product*).

**MTTD/MTTR** – vidutinis incidento aptikimo ir atstatymo laikas (angl. *Mean Time to Detect / Mean Time to Repair/Respond/Resolve*).

**NFR** – nefunkcinis reikalavimas (angl. *Non-Functional Requirement*).

**NIS2** – Direktyva (ES) 2022/2555 dėl aukšto bendro kibernetinio saugumo lygio užtikrinimo Sąjungoje (angl. *Network and Information Security Directive 2*).

**NIST** – Nacionalinis standartų ir technologijų institutas (angl. *National Institute of Standards and Technology*).

**NKSC** – Nacionalinis kibernetinio saugumo centras.

**OLIR** – NIST internetinės informacinės nuorodos (angl. *Online Informative References*).

**PDCA** – Planuoti–Įgyvendinti–Tikrinti–Tobulinti ciklas (angl. *Plan–Do–Check–Act*).

**RPO/RTO** – atkūrimo taško ir atkūrimo laiko tikslai (angl. *Recovery Point Objective, Recovery Time Objective*).

**SCRM** – tiekimo grandinės kibernetinio saugumo rizikos valdymas (angl. *Supply Chain Risk Management*).

**SIEM** – saugumo informacijos ir įvykių valdymo sistema (angl. *Security Information and Event Management*).

**SOC** – saugumo operacijų centras (angl. *Security Operations Center*).

**SoA** – taikomumo pareiškimas (angl. *Statement of Applicability*).

**SOAR** – saugumo orkestravimo, automatizavimo ir reagavimo platforma (angl. *Security Orchestration, Automation and Response*).

**SPA** – vieno puslapio aplikacija (angl. *Single Page Application*).

**TIS2** – Tinklų ir informacinių sistemų saugumo direktyva (angl. *NIS2 Directive*).

**TLPT** – grėsmių imituojamas įsiskverbimo testavimas (angl. *Threat-Led Penetration Testing*).

**UML** – vieningoji modeliavimo kalba (angl. *Unified Modeling Language*).

**XDR** – išplėstinis grėsmių aptikimas ir reagavimas (angl. *Extended Detection and Response*).

# ĮVADAS

**Kibernetinio saugumo aktualumas šiuolaikinėje visuomenėje.**

Paskutinius porą dešimtmečių kibernetinio saugumo svarba didėja, o kaip iliustruoja tyrimai, IS saugumo problema ypač aktuali mažoms ir vidutinėms organizacijoms (MVO), pavyzdžiui ENISA grėsmių apžvalgoje teigiama, jog „per pastarąjį dešimtmetį kibernetinių atakų skaičius eksponentiškai išaugo, o atakų sudėtingumas tapo vis labiau rafinuotas. Kibernetiniai nusikaltėliai vis dažniau taikosi į mažas ir vidutines įmones, kurios turi ribotus resursus ir ne visada sugeba tinkamai apsaugoti savo IT infrastruktūrą“[[1] ] . Tai nenuostabu, mažų ir vidutinių verslų veikla vis labiau priklauso nuo informacinių technologijų, organizacijos ne tik persikelia savo procesus į skaitmeninę sferą, ką paspartino ir COVID-19 pandemija, bet dažną kartą organizacijos veikla užgimsta ir vyksta tik kibernetinėje aplinkoje, elektroninės komercijos ir paslaugų tiekimo forma. Svarbu paminėti, kad pagal skaitmeninės ekonomikos tyrimus ir statistiką, Lietuva nuolatos stiprina savo pozicijas elektroninės komercijos srityje, lyginant su kitomis ES šalimis[[2] ]. Tačiau dėl ribotų finansinių ir žmogiškųjų išteklių, kompetencijų bei profesionalumo stokos, mažos ir vidutinės organizacijos (MVO) dažnai nesugeba tinkamai pasirūpinti savo IT infrastruktūros apsauga, užtikrinti sklandžių reagavimo į saugumo incidentus procesų, organizuoti žmogiškųjų išteklių kibernetinio saugumo suvokimo mokymų ir, svarbiausia, tinkamai įsivertinti, ar minėti komponentai apskritai yra įdiegti organizacijoje, o jei įdiegti – ar jie atitinka šiuolaikinius saugumo standartus ir privalomuosius reikalavimus. Rezultate kibernetinės atakos gali sukelti didelius finansinius nuostolius, asmenų privačių duomenų nutekėjimą, negrįžtamą įmonės reputacijos praradimą, ir, nors galima pastebėti bendrą saugumo incidentų mažėjimą, didėja pavojingesnių atakų skaičius. Pagal Lietuvos Nacionalinio kibernetinio saugumo centro (toliau – NKSC) 2024 metų ataskaitą, vien 2023 metais buvo užregistruota 2 378 kibernetiniai incidentai[[3] ]. Ataskaita parodo, kad didžiausi iššūkiai – tai asmeninių duomenų apsauga ir IS spragos, todėl akivaizdu, kad veiksmingos, standartizuotos, gilesnio IS saugumo priemonės ir toliau išlieka silpniausia grandimi mažesnio didžio įmonių saugumo perimetre. Apibendrinant galima teigti, kad stebima tendencija, kad MVO susiduria su patikimų ir aiškių kibernetinio saugumo standartų, kurie padėtų efektyviai valdyti kibernetinį saugumą, įgyvendinimo iššūkiais.

**Kibernetinio saugumo standartai ir TIS2 direktyva.**

Atsakant į augančius kibernetinio saugumo iššūkius, buvo sukurti įvairūs saugumo standartai ir reguliaciniai reglamentai. Tarptautiniai standartai, tokie kaip ISO/IEC 27001ir NIST, tapo svarbiais

instrumentais kibernetinio saugumo praktikoms suvienodinti. Tuo tarpu Europos Sąjungoje ir Lietuvoje įsigaliojo naujausia ir reikšmingiausia ES kibernetinio saugumo direktyva – Tinklų ir informacinių sistemų direktyva (toliau TIS2). TIS2 tai viena iš naujausių ir svarbiausių ES kibernetinio saugumo direktyvų, orientuotų į saugumo užtikrinimą tarp ES šalių narių, kuriuo siekiama spręsti dabartinę sisteminę nepakankamos kibernetinio saugumo parengties problemą, padidinti efektyvumą ir sumažinti papildomas išlaidas, atsirandančias dėl kibernetinio saugumo incidentų[[4] ]. TIS2 ypač svarbus mažoms ir vidutinėms organizacijoms, nes suteikia iš esmės naują, aiškų ir struktūrizuotą požiūrį į kibernetinio saugumo valdymą bei apibrėžia karkasą, kaip sistemingai identifikuoti, analizuoti ir valdyti saugumo grėsmes. Tai patvirtina ir ENISA TIS2 investavimo į kibernetinį saugumo ataskaitoje pateiktas MVO palygimas su stambiomis įmonėmis[[5] ], kurioje buvo atskleista, jog daugybė TIS2 direktyvoje apibrėžtų kibernetinio saugumo valdymo aspektų MVO sektoriui yra „nauji“, „anksčiau negirdėti“ ir pan.

**Darbo naujumas aktualumas.**

Neseniai įsigaliojusi TIS2 direktyva apjungia kibernetinio saugumo standartų ir gerųjų praktikų raidą su valstybiniu reguliavimu, suteikdama organizacijoms galimybę ne tik spręsti kibernetinio saugumo iššūkius, bet ir užtikrinti atitiktį valstybės įstatymams. Tuo tarpu mažoms ir vidutinėms organizacijoms pirmiausia reikalingas paprastas ir aiškus praktinis būdas, padedantis įsivertinti pagal naujausius kibernetinio saugumo reikalavimus, pritaikytus konkrečiai organizacijai atsižvelgiant į jos veiklos pobūdį ir dydį. Šiame darbe nagrinėjama TSI2 direktyva ir jos praktinis pritaikymas MVO kibernetinio saugumo srityje, siekiant ne tik identifikuoti saugumo spragas ir neatitikimus organizacijoje, bet ir susieti vertinimo rezultatus su konkrečiomis rekomendacijomis, kibernetinio saugumo valdymo priemonėmis ir programinės įrangos sprendimais.

**Darbo tikslas.**

Tikslas – suprojektuoti informacinę sistemą, kuri, remdamasi TIS2 direktyva, padėtų atlikti kibernetinio saugumo reikalavimų vertinimą, atsižvelgiant į organizacijos sektoriaus ir veiklos kritiškumą, ir pagal vertinimo rezultatus pateiktų saugumo rekomendacijas ir diegimo planą, siekiant atitikti direktyvoje apibrėžtus reikalavimus.

**Darbo uždaviniai.**

1. Išanalizuoti TIS2 direktyvos taikymo ypatumus, ją palyginant su NIST Cybersecurity Framework 2.0 (CSF 2.0), ISO/IEC 27001:2022 bei Europos Sąjungos skaitmeninio operacinio atsparumo reglamentu (DORA).
2. Išanalizuoti organizacijoms pagal TIS2 direktyvą taikomus reikalavimus ir nustatyti jų taikymo ypatumus Lietuvos Kibernetinio saugumo įstatymo (KSĮ) kontekste.
3. Ištirti TIS2 atitikties vertinimo įrankių ir gamintojų siūlomų saugumo vertinimo instrumentų pasiūlą, identifikuojant metodinę ir praktinę nišą Lietuvos mažų ir vidutinių organizacijų poreikiams.
4. Susisteminti TIS2 reikalavimais pagrįstą kibernetinio saugumo subjekto nustatymo, atitikties vertinimo ir trūkumų šalinimo planavimo metodiką, pritaikytą praktiniam organizacijų kibernetinio saugumo vertinimui.
5. Sukurti programinės įrangos prototipą, veikiantį parengtos metodikos pagrindu, ir įvertinti jo tinkamumą MVP kontekste atlikus testavimą ir demonstracinių scenarijų įgyvendinimą.

**Tyrimo metodai:** mokslinės literatūros analizė, šaltinių analizė, lyginamoji analizė, programinės įrangos projektavimo metodai.

**Darbo apribojimai.** Darbe fokusuojamasi į techninius kibernetinio saugumo vertinimo aspektus ir atsiribojimą nuo gilesnės teisinės analizės. Taip pat projektuojamas įrankis nepretenduoja pakeisti akredituoto audito arba kitų vertinančių organizacijų metodikų, bet siekia maksimaliai supaprastinti ir struktūruoti pasiruošimą tokio pobūdžio patikroms. Sukuto programinio įrankio tikslas – pademonstruoti kibernetinio saugumo vertinimo koncepcijos veikimą, o ne analizuoti pasirinktų technologijų ypatumus, jų privalumus ir trūkumus, projekte sąmoningai atsiribojama nuo technologinių priemonių veikimo ir jų praktinio įgyvendinimo analizės bei vertinimo.

**Naudota literatūra.** Šiame darbe buvo remtasi pirminiais ir antriniais šaltiniais, apimančiais mokslinę literatūrą ir publikuotus straipsnius, techninę dokumentaciją bei teisiniais dokumentais.

**Programinės įrangos projektavimo ir kūrimo priemonės.**

Programinė įranga buvo projektuojama ir rengiama kompiuteryje su *Windows 11 Pro* operacine sistema. Reikalavimų dokumentavimui buvo naudojamas *Microsoft Word*, naudojimo scenarijų,

veikimo ir komponentų UML diagramų braižymui – *Visual Paradigm*, programinio kodo rašymui – *Visual Studio Code IDE,* taip pat *PowerShell* bibliotektų diegimui. Programinė įranga buvo konteinerizuota ir įdiegta į lokalią *Docker Desktop* aplinką. Įdiegta programinė įranga buvo paleidinėjama ir testuojama *Microsoft Edge* naršyklėje.

**Darbo aprobacijos.**

Magistro darbo tema ir pagrindiniai tyrimo rezultatai buvo aprobuoti Vilniaus universiteto Šiaulių akademijos organizuotoje jaunųjų tyrėjų tarptautinėje mokslinėje konferencijoje „Jaunasis tyrėjas išmaniajai visuomenei“, kur autorius skaitė pranešimą tema „Mažų ir vidutinių organizacijų TIS 2 kibernetinio saugumo vertinimo informacinės sistemos projektas“ (2025 m. gegužės 8 d.; pažymėjimas Nr. MVG-VUŠA-2025-326).

**Darbo struktūra ir apimtis.**

Darbas suskirstytas į penkis skyrius. I skyriuje, įgyvendinant pirmąjį darbo uždavinį, buvo analizuojami kibernetinio saugumo standartai NIST CSF 2.0 ir ISO/IEC 27001 bei Europos Sąjungos DORA reguliavimas, lyginant juos su TIS2 direktyva. II skyriuje, atliepiant antrąjį ir trečiąjį darbo uždavinius, analizuojami TIS2 direktyvos reikalavimai taikymo Lietuvoje kontekste, nagrinėjamas jų transponavimas į Lietuvos Respublikos kibernetinio saugumo įstatymo paskutiniąją redakciją bei susijusios įgyvendinimo gairės, taip pat tiriama organizacijų TIS2 atitikties vertinimo įrankių pasiūla. III skyriuje, siekiant įgyvendinti ketvirtąjį darbo uždavinį, aprašomas TIS2 atitikties vertinimo įrankio projektavimo etapas, apimant kibernetinio saugumo subjekto nustatymo ir atitikties vertinimo metodiką, adaptyvaus klausimyno struktūrą ir trūkumų šalinimo įgyvendinimo plano formavimo logiką. IV skyriuje, atliepiant penktąjį darbo uždavinį, aprašomas vertinimo įrankio techninis įgyvendinimas, jo architektūra, funkcionalumas bei testavimo rezultatai. V skyriuje apibendrinami ankstesniuose darbo skyriuose įgyvendintų uždavinių rezultatai ir pateikiamos bendrosios išvados bei pasiūlymai.

# 1. Kibernetinio saugumo standartai ir TIS2 direktyvos palyginamoji analizė

Šiuolaikinėje skaitmeninėje eroje kibernetinio saugumo reglamentavimas patyrė esmines transformacijas, formuojančias naują teisinės atsakomybės, rizikos valdymo ir technologinių standartų realybę. Europos Sąjungoje ir pasaulyje formuojasi suartėjimo tendencijos tarp nacionalinių, regioninių ir tarptautinių kibernetinio saugumo metodikų, tačiau kartu išryškėja ir specifiniai skirtumai, atspindintys skirtingas reguliacines kultūras, sektorinius prioritetus bei technologinio brandos lygį[[6] ]. Šiame skyriuje besiremiant sisteminės analizės metodu aprašyti pagrindiniai šiuolaikinio kibernetinio saugumo sąvadai - CSF2.0 gairės, ISO27001 standartas, DORA reguliavimas bei TIS2 direktyva. Analizės tikslas – nustatyti konceptualias sąsajas, techninius skirtumus, taikymo panašumus ir skirtumus  bei tokiu būdu įgryninti TIS2 direktyvos vietą kibernetinio saugumo standartų ir reguliavimų landšafte bei parengti teorinį pagrindą šio darbo tikslui – kibernetinio saugumo vertinimo įrankiui.

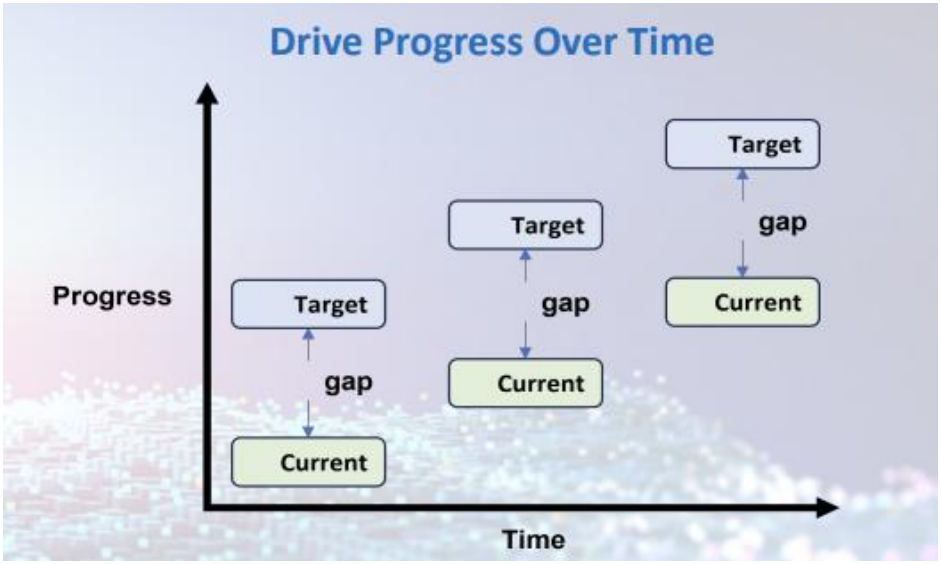
## 1.1. NIST kibernetinio saugumo gairės (CSF2.0)

NIST Cybersecurity Framework 2.0 – tai naujausia NIST parengto kibernetinio saugumo gairių dokumento redakcija, paskelbta 2024 m. vasario 26 d. Ši versija išplečia taikymo sritį už kritinės infrastruktūros ribų, akcentuoja valdymą bei tiekimo grandinės rizikas.[[7] ]. CSF2.0 architektūrą sudaro šešios pagrindinės funkcijos, pakeičiančios ankstesnį penkių funkcijų modelį: valdymas (angl. *govern*), identifikavimas (angl.  *identify*), apsauga (angl.  *protect*), aptikimą (angl. *detect*), reagavimas (angl.  *respond*) ir atstatymas ( angl. *recover*), sudarantis vadinamą gairių branduolį (angl. *CSF Core*), kaip pavaizduota žemiau 1 Pav. CSF 2.0 Funkcijos.


**1 Pav.** CSF 2.0 Funkcijos. [[7] ]

Valdymo funkcijos kaip atskiros kategorijos įtraukimas į CSF2.0 atskleidžia gilesnį suvokimą, kad kibernetinio saugumo valdymas turi būti integruojamas į organizacijos strateginio valdymo procesus, o ne traktuojamas kaip izoliuota technologinė funkcija. [[7] ] CSF2.0 pateikia aukšto lygmens kibernetinio saugumo rezultatų taksonomiją, kurią gali taikyti bet kuri organizacija, nepriklausomai nuo dydžio, sektoriaus ar brandos, siekdama geriau suprasti, įvertinti, nustatyti prioritetus ir komunikuoti savo kibernetinio saugumo [[7] ]. Naujoji valdymo funkcija apibrėžia šešias strategines kategorijas: organizacinį kontekstą, rizikos valdymo strategiją, tiekimo grandinės kibernetinio saugumo rizikų valdymą, vaidmenų, atsakomybių ir įgaliojimų apibrėžimą, politikos formavimą ir priežiūros mechanizmus.

CSF 2.0 išplėtoja organizacinių profilių taikymą ir apibrėžia „greitos pradžios“ (angl. *quick-start*) metodiką, leidžiančią įvertinti organizacijos kibernetinio saugumo būklę. Organizacinis profilis iš esmės sistemiškai parodo jos dabartinę brandą, taip pat apibrėžia kibernetinio saugumo tikslus CSF Core terminais. CSF2.0 ypatingą dėmesį skiria bendruomenių profiliams (angl. *community profiles*), kurie yra skirti sektorių ar ekosistemų poreikiams bei pritaikymui. Praktiškai taikant CSF2.0 organizacijoje, yra priskiriami profilio šablonai, skirti dabartiniam (angl. *current*) ir tiksliniam (angl. *target*) profilių sudarymui ir palyginimui. Besikeičiant organizacijai, atsirandant naujiems reikalavimams profiliai taip pat evoliucionuoja, pavaizduota 2 Pav. CSF 2.0 Profilių progresas. [[8] ]



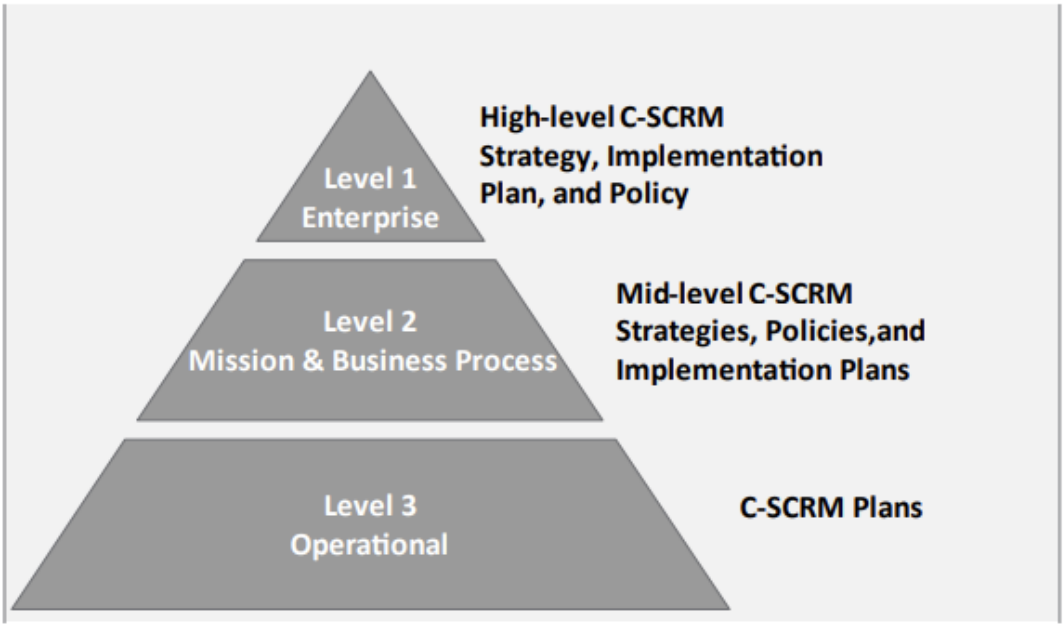

**2 Pav.** CSF 2.0 Profilių progresas. [[8] ]

CSF 2.0 įgyvendinimo lygiai (angl. *implementation tiers*) apibrėžiami keturiomis pakopomis: dalinis (angl. *partial*), rizika grindžiamas (angl. *risk-informed*), pakartojamas (angl. *repeatable*),

prisitaikantis (angl. *adaptive*), jos charakterizuoja organizacijos kibernetinio valdymo praktikos griežtumą bei padeda planuoti tobulinimą, 3 Pav. CSF 2.0 Įgyvendinimo lygiai. [[7**]** ]. Lygiai yra taikomi organizaciniams profiliams, taip apibrėžiamas kontekstas, kaip organizacija vertina kibernetines rizikas ir kokie procesai naudojami joms valdyti. [[7] ] Manoma, kad organizacijos, taikančios aukštesnius CSF lygius, demonstruoja žymiai geresnį incidentų valdymo efektyvumą bei mažesnę vidutinę atkūrimo trukmę.[[9] ]

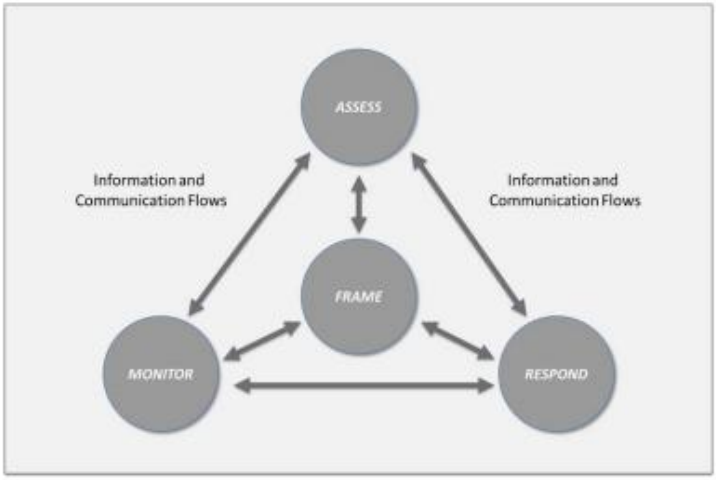

**3 Pav.** CSF 2.0 Įgyvendinimo lygiai. [[7] ]

CSF 2.0 skiria ypatingą dėmesį kibernetinio tiekimo grandinės rizikų valdymui (SCRM), apibrėždamas jį kaip atskirą valdymo funkcijos kategoriją (GV.SC). Šis struktūrinis gairių pakeitimas atspindi didėjančią trečiųjų šalių saugumo pažeidimų grėsmę, tokių kaip SolarWinds Orion tiekimo grandinės kompromitavimas 2020 m. [[10] ], Log4Shell pažeidžiamumas 2021 m. [[11] ], kt., kai tiekimo grandinės kompromitavimas paveikė tūkstančius organizacijų vienu metu. CSF2.0 dokumentuose specialioje publikacijoje apibrėžiamos praktinės SCRM įgyvendinimo gairės trijų lygių modelyje, kuris apima organizacinį, procesinį ir operacinį lygius, 4 Pav. SCF 2.0 Kibernetinio saugumo tiekimo grandinės rizikų valdymas. [[12**]** ]




**4 Pav.** SCF 2.0 Kibernetinio saugumo tiekimo grandinės rizikų valdymas. [[12] ]

SCRM kategorija apima visą tiekėjų gyvavimo ciklą, nuo rizikos identifikavimo ir vertinimo, tiekėjų pasirinkimo iki sutarčių valdymo ir incidentų reagavimo planų su partneriais [[7] ] Tiekimo valdymo metodologija apima tiekėjų klasifikavimą pagal kritiškumą, reguliarų saugumo būklės stebėjimą, sutarčių saugumo reikalavimų specifikavimą bei atsako į incidentus mechanizmus, apimančius visą tiekimo grandinę, 5 Pav. CSF 2.0 Kibernetinio saugumo tiekimo grandinės rizikų valdymo metodika. [[12**]** ]




**5 Pav.** CSF 2.0 Kibernetinio saugumo tiekimo grandinės rizikų valdymo metodika. [[12] ]

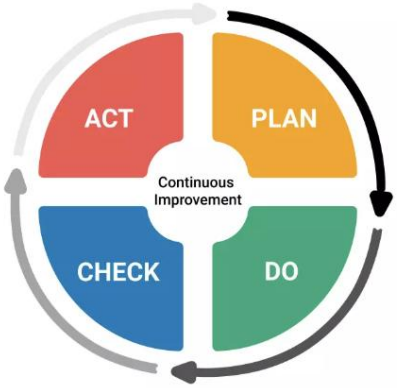
Reikšminga vietą CSF2.0 gairėse užima informatyvieji susiejimai (angl. *informative references*), kurie susieja CSF Core su kitais standartais bei gairėmis, pvz. ISO27001, CIS Controls, kitomis

metodikomis. Tai leidžia organizacijoms integruoti CSF su esamomis valdymo ir atitikties praktikomis bei palengvina taikymą skirtinguose sektoriuose. Oficialūs susiejimai skelbiami oficialiame NIST kataloge [13], žemiau pateikiamas atsako funkcijos incidentų valdymo kategorijos susiejimų pavyzdžiai, 6 Pav. Pavyzdinis  vaizdas iš CSF2.0 susiejimo su kitais standartais ir gairėmis. [[13**]** ]


**6 Pav.** Pavyzdinis  vaizdas iš CSF2.0 susiejimo su kitais standartais ir gairėmis. [[13] ]

### 1.2. Informacijos saugumo valdymo sistemos standartas ISO/IEC 27001:2022

ISO/IEC 27001:2022 – tai plačiausiai naudojamas tarptautinis informacijos saugumo valdymo standartas, priklausantis ISO 27000 šeimai. ISO/IEC 27001:2022 apibrėžia informacijos saugumo valdymo sistemą, siekiant padėti organizacijoms valdyti jų informacijos saugumą[[26] ]. Be ISO/IEC 27001:2022, svarbu paminėti šeimai priklausančius tokius standartus kaip ISO/IEC 27005:2022 (informacijos saugumo rizikos valdymas) ir ISO/IEC 27017:2022 (informacijos saugumas debesijos aplinkose), kurie papildo ISO/IEC 27001:2022 įgyvendinimą organizacijoje. 2022 m. redakcijoje ISO/IEC 27001:2022 standartas buvo iš esmės peržiūrėtas, buvo papildytas Priedas A (angl. *annex* A), kai ankstesnės 14 temų ir 114 kontrolės buvo pertvarkytos į 93 kontroles sugrupuotas į 4 temines grupes: organizacines (37 kontrolės), žmonių (8 kontrolės), fizines (14 kontrolės) ir technologines (34 kontrolės) [[23] ]. Šis struktūrinis pertvarkymas atspindi šiuolaikinio informacijos saugumo suvokimo evoliuciją, kai prioritetas teikiamas sisteminiam organizacinių procesų valdymui ir žmogiškojo veiksnio integravimui į bendrą saugumo valdymo architektūrą. Organizacinės kontrolės apima politikų formavimą, rizikų valdymą, incidentų valdymą ir tiekėjų valdymą. Žmonių kontrolės koncentruojasi į personalo patikrinimą, mokymų programas ir darbuotojų sąmoningumo ugdymą [[23] ]. Standartas fokusuojasi į nuolatinį rizikos vertinimą kaip esminį principą, siekiant užtikrinti, kad organizacijos būtų pasirengusios apsaugoti informacijos turtą. Minėto principo įgyvendinimui, standartas remiasi Planuoti-Įgyvendinti-Tikrinti-Tobulinti ciklu (angl. *Plan-Do-Check-Act*, toliau PDCA), kuris grindžiamas nuolatiniu informacijos saugumo valdymo sistemos (toliau ISVS) tobulinimu (angl. *continual improvement*).[[22] ] Žemiau ciklo vizualizacija, 7 Pav. ISO27001 Planuoti- Įgyvendinti-Tikrinti-Tobulinti principas. [[24**]** ]




**7 Pav.** ISO27001 Planuoti- Įgyvendinti-Tikrinti-Tobulinti principas. [[24] ]

Standarto įgyvendinimas organizacijoje apima kelis etapus. Pirmiausiai apibrėžiama apimtis, kuria sudaro: a) kontekstas (angl. *context*), t. y. vidiniai ir išoriniai faktoriai lemiantis informacijos saugumą; b) ribos (angl. *scope*) nustatančios kokios sistemos, procesas ir padaliniai bus įtraukti; c) identifikuojamos suinteresuotosios šalys (angl. *stakeholders*) ir d) nustatomi informacijos saugumo tikslai, atitinkantys bendros organizacijos strategijos. Proceso metu organizacija vykdo trūkumų analizę, identifikuojančią esamus ir reikalingus saugumo kontrolės mechanizmus, formuoja rizikos valdymo metodiką ir parengia Taikomumo pareiškimą (angl. *Statement of Applicability*, toliau SoA), kuriame pagrindžia kontrolės priemonių pasirinkimą. Vadovavimo (angl. *leadership*) ir politikos formavimo etape paskirstomi vadovybės įsipareigojimai, vaidmenys ir atsakomybės. ISO/IEC 27005:2022 pateikia nuoseklią metodiką (rizikos kriterijai, rizikos registras, vertinimo metodai, apdorojimo plano sudarymas ir stebėsena), suderintą su ISO/IEC 27001:2022.[[27] ] Rizikų vertinimo (angl. *assessment*) ir valdymo (angl. *treatment*) etape identifikuojami informacijos turtas (angl. *assets*), grėsmių ir pažeidžiamumų įtaka bei tikimybė, rizikos valdymo būdai - vengimas (angl. *avoidance*), mažinimas (angl. *mitigation*), perkėlimas (angl. *transfer*) ar priėmimas (angl. *acceptance*). Verta atskirai paaiškinti, jog rizikos vengimas (veiklos ar srities atsisakymas) taikomas, kai potencialūs nuostoliai viršija priimtinas ribas, tuo tarpu rizikos mažinimas apima kontrolės priemonių įgyvendinimą, siekiant sumažinti grėsmės tikimybę arba poveikį. Veiklos vertinimas užtikrina kad įdiegta ISVS būtų nuolat stebima ir vertinama, tam parengiami rodikliai (pvz., incidentų, paslaugos teikimo, našumo rodikliai), atliekamas vidaus auditas, vykdomas įgyvendinto vadovybės modelio vertinimas. ISVS tobulinimo etapas numato korekcines priemones ir nuolatinį tobulinimą, įgyvendinamą PDCA logikos pagrindu, kai vertinimo rezultatai sąlygoja nuolatinį gerinimą. Vykdant reguliarią veiklos peržiūrą, o standarto lankstumas leidžia integruoti jį su kitais valdymo sistemų standartais, pvz. tokiais kaip ISO 9001 kokybės valdymo standartu, formuojant integruotą valdymo sistemą. Svarbu išskirti standarto dėmesį dokumentavimui (angl. *documented information*) kuris apima politikas, rizikos procesus, procedūras ir veiklos įrodymus, kad būtų galima matuoti, audituoti ir peržiūrėti ISVS. Jau minėtas taikomumo pareiškimas (angl. *Statement of Applicability*, toliau SoA), privalomas dokumentas, kuris išvardija pasirinktų kontrolės priemonių taikymą, nurodo įtraukimo ar išskyrimo pagrindimą ir būklę.[[28] ] Žemiau pateiktas ISO27001 diegimo ciklas 8 Pav. ISO27001 diegimo etapai. [[29**]** ]


**8 Pav.** ISO27001 diegimo etapai. [[29] ]

Standarte pabrėžiama, jog organizacijos turi nustatyti, įgyvendinti, palaikyti ir nuolat tobulinti informacijos saugumo valdymo sistemą, ISO/IEC 27001:2022 sertifikavimas – tai būdas atitikti šio pricipo. Įprastai sertifikavimas vykdomas dviem etapais, pirmo etapo metu vertinama parengtis ir dokumentacijos pakankamumas, antrame etape tikrinamas faktinis priemonių įgyvendinimą vietoje. Po sėkmingo sertifikavimo atliekami priežiūros auditai ir pakartotinis sertifikavimas pagal ISO numatyta akreditavimo schemą, reikalavimus sertifikavimui nustato specialūs dokumentai ir tvarkos.

ISO/IEC 27001 yra suderinamas su kitais standartais ir gairėmis. Jau minėtas NIST OLIR pateikia ryšių žemėlapį tarp ISO/IEC 27001:2022 ir NIST CSF 2.0, leidžiantį sieti CSF gairių taksonomiją su ISVS reikalavimais, tai padeda praktikoje suderinti terminiją, įrodymus ir planavimo logiką.

### 1.3. Skaitmeninės veiklos atsparumo aktas (DORA)

Skaitmeninės veiklos atsparumo aktas (angl. Digital Operational Resilience Act, toliau – DORA), Reglamentas (ES) 2022/2554, paskelbtas 2022 m. gruodžio 27 d., įsigaliojo 2023 m. sausio 16 d., jo taikymas pradėtas nuo 2025 m. sausio 17 d. Šiuo aktu iš esmės suvienodintas ES finansų sektoriaus skaitmeninio atsparumo reguliavimas, nustatant vienodus reikalavimus tinklų ir informacinių sistemų saugumui visose valstybėse narėse.[[15] ] Kaip pažymi Europos vertybinių popierių ir rinkų institucija (angl. *European Securities and Markets Authority*, toliau ESMA), DORA tikslas – sustiprinti finansų subjektų informacinių ir ryšių technologijų (toliau IRT) saugumą ir užtikrinti atsparumą reikšmingiems operaciniams sutrikimams.[[14] ] DORA taikymo sritis apima platų finansų paslaugų sektorių, įskaitant kredito įstaigas, draudikus, investicines įmones, mokėjimo ir elektroninių pinigų įstaigas, centrinius vertybinių popierių depozitoriumus ir kitus finansų subjektus, taip pat kritinius trečiųjų šalių IRT paslaugų teikėjus minėtiems subjektams[[15] ] DORA yra ES reglamentas, todėl jis tiesiogiai taikomas ir skirtingai nei direktyvos (pavyzdžiui TIS2) nereikalauja perkėlimo į nacionalinę teisę, jo nuostatos pradėtos taikyti vienu metu visose ES valstybėse narėse.

DORA struktūrą formuoja penkios tarpusavyje susijusios sritys: rizikų valdymas, incidentų stebėjimas ir ataskaitos, skaitmeninių operacijų atsparumo testavimas, trečiųjų šalių rizikos valdymas ir ataskaitos ir informacijos dalijimosi mechanizmai, pav. DORA reguliavimas


**9 Pav.** DORA reguliavimo ramsčiai. [[25] ]

Kiekviena iš sričių turi atskirus įgyvendinimo ir priežiūros būdus. IRT rizikų valdymą apibrėžia integruota rizikos valdymo sistema: valdymo (angl. *governance*) ir atskaitomybės struktūros, rizikų identifikavimas, vertinimas, kontrolės priemonės ir nuolatinis tobulinimas. Rizikų valdymo taikymas

organizacijoje yra proporcingas subjekto dydžiui, t. y. mažesniems subjektams taikomas supaprastintas režimas. Įrankių, metodų, procesų ir politikų bei supaprastinto režimo nuostatas detalizuoja Deleguotasis reglamentas (ES) 2024/1774.[[16] ] IRT incidentų valdymas apibrėžia incidentų klasifikavimo kriterijus, pranešimų apie incindentus turinį bei terminus, kibernetinio saugumo pavojus ir kt. numato Deleguotasis reglamentas (ES) 2024/1772 [[17] ] Atsparumo testavimas aprašo periodinius įsiskverbimo testus, įskaitant vadinamą grėsmių pagrindu atliekamą įsiskverbimo testavimą (toliau TLPT) aukštos svarbos subjektams, kuriuos nustato Europos priežiūros institucijos, parengiančios reglamentavimo techniniai standartus (RTS), detalios specifikacijos detalizuotos Deleguotame reglamente (ES) 2025/1190 [[18] ]. Trečiųjų šalių rizikos valdymas nustato tekėjų koncentracijos rizikos vertinimą, privalomas sutartines nuostatas ir kritinių tiekėjų priežiūros sistemą. Kritiniai trečiųjų šalių paslaugų teikėjai identifikuojami atsižvelgiant į sisteminį poveikį, subjektų priklausomybę nuo jų teikiamų paslaugų  ir tiekėjo pakeičiamumą. Šiuos kriterijus detalizuoja Deleguotas reglamentas (ES) 2024/1502 [[21] ] Organizacijos turi įvertinti, kokio lygio jų priklausomybė nuo vieno ar kelių IRT tiekėjų, ypač jei tie tiekėjai aptarnauja daug finansų įstaigų, tai padeda išvengti situacijų, kai vieno tiekėjo sutrikimas paveikia visą sektorių. Sutartinėse nuostatose DORA reikalauja kad būtų aiškiai apibrėžti paslaugų tiekimo susitarimas (SLA), incidentų pranešimo tvarka, prieigos prie duomenų, paslaugų nutraukimo ir tęstinumo taisykles. Kritinių tiekėjų priežiūra ir rekomendacijų teikimą vykdo taip vadinamas pagrindinis prižiūrėtojas (angl. *lead overseer*), priskiria ES institucija. Prižiūrėtojas koordinuoja priežiūrą, įskaitant metinius planus, bendras patikras, teikia rekomendacijas ir atlieką įgyvendinimo stebėseną [[19] ] Galiausiai, informacijos dalijimosi mechanizmai leidžia subjektams keistis kibernetinių grėsmių informacija ir žvalgyba (angl. *cyber threat intelligence*, toliau CTI) siekiant stiprinti bendrą sektoriaus atsparumą. CTI užtikrina nuosekliai užtikrina informacijos mainus visoje ES, nuo prevencijos ir pasirengimo iki incidentų valdymo, testavimo, tiekimo grandinių priežiūros ir pan.[[20] ]

DORA reguliaciniai techniniai standartai (RTS) detalizuoja konkrečius techninius ir procedūrinius reikalavimus kiekvienai iš paminėtų sričių. RTS numato rizikų identifikavimo metodikas, kontrolės mechanizmus, dokumentavimo reikalavimus ir efektyvumo matavimo kriterijus, reglamentuoja incidentų klasifikavimą ir atskaitingumą, atsparumo testavimo dažnumą, metodikas, nepriklausomumo reikalavimus ir rezultatų įgyvendinimo procesus. DORA RTS reikalauja ne tik formalių procedūrų sukūrimo, bet ir jų nuolatinio tobulinimo bei efektyvumo įrodymo per reguliarius testus ir auditą. [[16] ][[17] ][[20] ]

### 1.4. TIS2 direktyvos apžvalga

TIS2 direktyva (2022/2555/ES) žymi esminį ES kibernetinio saugumo politikos plėtros etapą, kardinaliai praplėsdama nuo 2016 m. galiojusios TIS direktyvos taikymo sritį ir reguliacinį intensyvumą. Direktyva taikoma 18 kritinių sektorių, apimančių energetiką, transportą, finansus, sveikatos apsaugą, vandenį, skaitmenines paslaugas, viešąjį administravimą ir kosmoso sektorius. [[30] ] Šis išplėtimas padidino reguliuojamų organizacijų skaičių nuo kelių tūkstančių iki šimtų tūkstančių visos ES mastu. Direktyvos architektūrą formuoja dviejų lygių reguliacinis modelis, skirstant subjektus į esminius (angl. *essential entities*) ir svarbius (angl. *important entities*) pagal sektorių, organizacijos dydį ir paslaugų kritiškumą (detaliau subjektų skirstymas aprašytas šio 3 skyriaus *Kritiškumo vertinimo komponento rengimas* poskyriuje). Esminiai subjektai priklauso *Annex I* (liet. Priedas I) sektoriams ir yra laikomi kritiškai svarbiais ES valstybių funkcionavimui. Svarbūs subjektai *Annex II* (Priedui II) apima platesnį organizacijų spektrą, kurios nors nėra laikomos tokios pat kritinės bet yra pakankamai svarbios kad patekti į TIS2 reguliavimo apimtį. TIS2 apibrėžia dešimt privalomų kibernetinio saugumo priemonių, kurias turi įgyvendinti visos organizacijos patekusios į direktyvos galiojimo apimtį, jos išvardintos 21 straipsnyje:

a) rizikos analizės politikos
b) incidentų valdymas
c) veiklos tęstinumas
d) tiekimo grandinės saugumas
e) sistemų įsigijimo ir plėtros saugumas
f) veiksmingumo vertinimo politikos
g) mokymai ir kibernetinė higiena
h) kriptografijos politikos
i) žmogiškųjų išteklių saugumas ir turto valdymas
j) kelių veiksnių autentifikacija ir saugios komunikacijos

Šios priemonės formuoja išsamią kibernetinio saugumo valdymo metodiką.[[31] ] Svarbu pažymėti, jog TIS2 taiko proporcingumo principą ir vadovaujasi anksčiau minėtų identifikuotu subjektų kritiškumu, taip užtikrinant, jog kibernetinio saugumo rizikos valdymo priemonės yra atitinkamos ir veiksmingos, atsižvelgiant į esminių ir svarbių subjektų dydį bei rizikos profilį[[32] ]

TIS2 įveda asmeninės atsakomybės principą, numatoma, kad organizacijų valdymo organai yra tiesiogiai atsakingi už kibernetinio saugumo priemonių įgyvendinimą ir priežiūrą. Kaip nurodo direktyvos 20 straipsnis, valstybės turi užtikrinti, kad esminių ir svarbių subjektų valdymo organai patvirtintų kibernetinio saugumo valdymo priemones [[30] ] Kita direktyvos naujovė – tai atgrasomosios baudos, esminiams subjektams taikomos baudos iki 10 mln. EUR arba 2% metinės globalios apyvartos, o svarbiems subjektams iki 7 mln. EUR arba 1,4% apyvartos [[30] ] Taip pat gali būti taikomos kitos priemonės: veiklos sustabdymas, vadovų laikinas nušalinimas.

TIS2 direktyva buvo perkelta ir įsigaliojo Lietuvoje 2024 m. spalio 18 d., įsigaliojus Kibernetinio saugumo įstatymo pakeitimams.[[34] ] Rezultate nacionalinio kibernetinio saugumo centro vaidmuo buvo sustiprintas kaip centralizuotos kompetentingos institucijos, koordinuojančios kibernetinio saugumo priežiūrą visuose sektoriuose [[34] ] Įgyvendinimo terminai Lietuvoje buvo suskirstyti etapais: subjektų identifikavimas iki 2025 m. balandžio, atitinkamų organizacinių priemonių įgyvendinimas iki 2026 m. balandžio, techninių priemonių diegimas iki 2027 m. balandžio. Šis laipsniškas įgyvendinimas leidžia organizacijoms palaipsniui prisitaikyti prie naujųjų reikalavimų. TIS2 numato skirtingus priežiūros mechanizmus esminiams ir svarbiems subjektams. Pabrėžiama, kad esminiai subjektai patenka į proaktyvų priežiūros režimą, apimantį reguliarius auditus, saugumo skenavimus, inspekcijas ir duomenų pateikimo reikalavimus [[33] ]. Taip pat kompetentingos institucijos, Lietuvos atveju – NKSC, gali vykdyti auditus po incidentų arba gavę pranešimus apie galimus neatitikimus TIS2 reikalavimams. Svarbūs subjektai reguliuojami reaktyviu režimu, kai priežiūros veiksmai inicijuojami tik gavus pranešimus apie galimus pažeidimus arba po incidentų. Šis skirtumas atspindi proporcingumo principą, kai intensyvesnė priežiūra taikoma organizacijoms, kurių kompromitavimas gali turėti didesnį sisteminį poveikį.[[30] ]

### 1.5. NIST CSF2.0, ISO/IEC 27001, DORA ir TIS2 palyginimas ir apibendrinimas

Lyginamoji analizė atskleidžia esminius panašumus ir skirtumus tarp keturių kibernetinio saugumo užtikrinimo sistemų. Šiuolaikiniuose kibernetinio saugumo standartuose vis labiau akcentuojamas holistinis požiūris, integruojantis techninius, organizacinius ir valdymo aspektus[[6] ] Toliau darbe patogumui viename sakinyje kalbant apie lyginami standartą/gairės/direktyvą/reguliavimą bus minima „savadų lyginimas“ ir pan.  Konceptualiai visi nagrinėti sąvadai remiasi rizikos valdymo centrinio principo taikymu, tačiau skiriasi metodikų detalumu ir taikymo apimtimi. NIST CSF 2.0 siūlo lankstų, organizacijos poreikius atitinkantį rizikos valdymo modelį [[7] ] ISO 27001 numato sistemingą PDCA ciklu grindžiamą rizikos valdymo metodiką [3]. DORA reikalauja specifinės IRT rizikų valdymo sistemos finansų sektoriuje [[15] ]. NIS2 nustato minimalias privalomas rizikos valdymo priemones plačiam sektorių spektrui.[[30] ] Pažymėtina, kad visi keturi analizuojami kibernetinio saugumo sąvadai sistemingai išskiria tiekimo grandinės (trečiųjų šalių) saugumą kaip kritinę valdymo sritį: NIST CSF 2.0 įtvirtina atskirą GV.SC kategoriją valdymo funkcijoje, apibrėžiančią SCRM tikslus ir rezultatus [[7] ], ISO/IEC 27002:2022 numato nuoseklias kontrolės priemones tiekėjams, punktuose apie tiekėjų santykius, saugumą sutartyse, debesijos paslaugas [[23] ], DORA V skyrius nustato IRT trečiųjų šalių rizikos valdymo, sutarčių ir kritinių IRT teikėjų priežiūros reikalavimus[[15] ], TIS2 21 straipsnis įpareigoja užtikrinti tiekimo grandinės kibernetinį saugumą kaip vieną iš privalomų priemonių [[30] ] Organizacijų kibernetinio saugumo valdymo brandos (angl. *maturity*) vertinimo metodikos atskleidžia skirtingus požiūrius į tobulėjimo skatinimą. NIST CSF apibrėžia keturių lygių brandos vertinimo modelį, leidžiantį organizacijoms įsivertinti ir nustatyti tobulinimo kryptis.[[35] ] ISO 27001 PDCA ciklas užtikrina nuolatinį ISVS tobulinimą per reguliarų peržiūrą ir auditą.[[22] ] DORA numato periodinio atsparumo testavimo principus[[20] ] NIS2 apibrėžia reikalavimus saugumo priemonių efektyvumo vertinimo vidinių politikoms, taip pat numato organizacijų priežiūros principus.[[30] ]

Nagrinėjamuose sąvaduose vadovybės atsakomybės traktavimas atskleidžia ne tik skirtumus, bet ir esminį panašumą, t. y. strateginį kibernetinio saugumo valdymo suvokimą. NIST CSF 2.0 Valdymo funkcija pabrėžia vadovybės vaidmenį strateginiame kibernetinio saugumo [[7] ]. ISO 27001 reikalauja vadovybės įsipareigojimo ISVS įgyvendinimui ir palaikymui [[20] ]. DORA numato vadovybės tiesioginį dalyvavimą IRT strategijos formavime ir patvirtinime [[15] ]. TIS2 apibrėžia asmeninės vadovybės atsakomybės principą ir tiesiogines sankcijas [[30] ]. Tęsiant atsakomybės ir sankcijų sistemos temą, analizė atskleidė kaip skiriasi atitikties saugumo reikalavimams skatinimo modeliai. NIST CSF 2.0 – tai savanoriškas standartas, kuris neturi tiesioginių sankcijų, išskyrus

atvejus, kai jo taikymas reikalaujamas ir sankcijos yra numatytos reguliacinių ar sutartinių įsipareigojimų [[7] ]. ISO 27001 standartas analogiškai, netaiko sankcijų, tačiau standartas turi sertifikavimo sistemą, standarto nesilaikymas reikštų sertifikato netekimą kas gali lemti komercinio pobūdžio pasekmes, paslaugų tiekimo sutarčių nutraukimą ir pan. Tuo tarpu ir DORA reguliavimas ir TIS2 direktyva numato aiškias finansines sankcijas - baudas, kas atspindi ES požiūrį į privalomą kibernetinio saugumo reikalavimų vykdymą.[[15] ][[30] ]

Sisteminis keturių kibernetinio saugumo sąvadų palyginimas parodo tendencingą judėjimą link integruoto, rizikos valdymu grindžiamo, vadovybės atsakomybe išryškinto ir nuolat tobulėjančio kibernetinio saugumo valdymo modelio. Šį procesą skatina bendri kibernetinių grėsmių veiksniai, tarptautinis gerųjų praktikų dalijimasis ir reguliavimo mažinimo poreikis globalizuotoje ekonomikoje[[6] ] Taip pat analizės rezultatai parodo reikšmingas sąvadų sinergijos galimybes organizacijoms, siekiančioms efektyviai valdyti saugumą ir atitikti kompleksinius reguliacinės aplinkos reikalavimus. Pavyzdžiui NIST CSF 2.0 brandos vertinimo metodika papildo ISO 27001 nuolatinio tobulinimo procesus, tuo tarpu DORA ir NIS2 specifiniai reikalavimai gali būti integruojami su ISO 270001 standartu unifikuojant atitikties siekimo žemėlapį (angl. *roadmap*).[[37] ]

1 lentelė. **NIST CSF 2.0, ISO/IEC 27001:2022, DORA ir NIS2 palyginimas.**

| Aspektas | **NIST CSF 2.0** | **ISO/IEC 27001:2022** | **DORA – Regl. (ES) 2022/2554** | **NIS2 – Direktyva (ES) 2022/2555** |
|---|---|---|---|---|
| **Teisinė prigimtis ir privalomumas** | Savanoriškos NIST parengtos gairės; pats dokumentas nėra įstatymas, bet gali būti įtvirtintas nacionaliniuose teisės aktuose ar sutartyse. | Tarptautinis standartas, taikomas savanoriškai; organizacijos pačios sprendžia, ar siekti sertifikavimo. | Privalomas ES reglamentas, tiesiogiai taikomas ES finansų sektoriaus subjektams ir kritiniams IRT trečiųjų šalių paslaugų teikėjams. | Privaloma ES direktyva; valstybės narės privalo ją perkelti į nacionalinę teisę, nustatant privalomus kibernetinio saugumo reikalavimus. |
| **Pagrindinis tikslas** | Padėti organizacijoms suprasti, įvertinti ir valdyti kibernetines rizikas, naudojant funkcijų ir kategorijų sistemą. | Nustatyti ISVS (informacijos saugumo valdymo sistemos) reikalavimus, pagrįstus rizikos valdymo principu. | Užtikrinti skaitmeninį operacinį atsparumą – suderinti IRT rizikos valdymą, testavimą, incidentų raportavimą ir IRT tiekėjų priežiūrą finansų sektoriuje. | Siekti aukšto bendro kibernetinio saugumo lygio ES, nustatant minimalias rizikos valdymo ir incidentų pranešimo priemones svarbiausiems sektoriams. |
| **Taikymo sritis** | Globaliai taikoma savanoriška schema (kilmė – JAV federalinis institutas), skirta visų sektorių organizacijoms. | Globalus, sektoriui neutralus standartas, taikomas bet kokio tipo organizacijoms. | ES finansų sektoriaus subjektai (pvz., bankai, draudimo, investicinės įmonės) ir kritiniai IRT trečiųjų šalių paslaugų teikėjai. | ES veikiančios 18 sektorių organizacijos (Annex I ir II). |
| **Struktūra ir pagrindiniai elementai** | 6 funkcijos (Govern, Identify, Protect, Detect, Respond, Recover), detalizuojamos | Reikalavimų dalis (4–10 skyriai) ir 93 kontrolės priemonės priede A, suskirstytos teminėmis grupėmis. | 5 ramsčiai: IRT rizikos valdymas, incidentų pranešimas, skaitmeninio atsparumo testavimas, IRT | Rizikos valdymo priemonės (21 str.), incidentų pranešimas (23 str.), valdymo organų atsakomybė, |

| | | | | |
|---|---|---|---|---|
| | kategorijomis ir veiklomis. | | trečiųjų šalių rizikos valdymas, informacijos dalijimasis. | priežiūros ir sankcijų režimas. |
| **Sertifikavimas ir (arba) atitikties įrodymas** | Oficiali sertifikavimo schema nenumatyta; naudojamos savianalizės ir nepriklausomi vertinimai pagal CSF. | Akredituotų sertifikavimo įstaigų išduodamas sertifikatas 3 metų ciklui, su metinėmis priežiūros auditais. | Atitiktį vertina nacionalinės ir ES priežiūros institucijos per nuolatinę priežiūrą, patikras ir inspekcijas. | Atitiktį tikrina nacionalinės kompetentingos institucijos per priežiūrą ir auditus; gali būti remiamasi ES kibernetinio saugumo sertifikavimo schemomis. |
| **Veiksmingumo vertinimas** | Numatyti 4 brandos lygiai (Tier 1–4), skirti savianalizei, kiek sistemingai valdoma kibernetinė rizika. | Brandą lemia PDCA (plan–do–check–act) ciklas ir valdymo sistemos veiksmingumo vertinimas audito metu; formalių lygių nenumato. | Reikalaujamas nuolatinis atsparumo testavimas, įskaitant pažangias grėsmių imitacijos pratybas (TLPT) tam tikroms institucijoms. | Numatyti periodiniai rizikos valdymo priemonių vertinimai ir auditas; priežiūros institucijos gali reikalauti išorinių auditų ir veiksmų planų. |
| **Incidentų pranešimas ir valdymas** | Apibrėžia incidentų valdymo procesus ir komunikaciją, bet nenustato privalomų pranešimo terminų ar konkrečių adresatų. | Reikalauja turėti incidentų valdymo procesą ir pranešti suinteresuotosioms šalims. | Standartizuoja reikšmingų IRT incidentų pranešimą priežiūros institucijoms, nustatydamas klasifikaciją, turinį ir terminus visoje ES. | Nustato kelių pakopų pranešimo tvarką (ankstyvas įspėjimas, pirminė ir galutinė ataskaita) nacionaliniam CSIRT ir kompetentingai institucijai su aiškiais terminais. |
| **Valdymo organų vaidmuo ir atsakomybė** | Rekomenduoja, kad aukščiausioji vadovybė dalyvautų rizikos vertinime ir sprendimuose, tačiau teisinės asmeninės | Reikalauja aukščiausios vadovybės įsipareigojimo ir atsakomybės už ISVS veiksmingumą, bet sankcijos už fizinių asmenų | Valdymo organai atsakingi už IRT rizikos valdymo sistemos patvirtinimą ir stebėseną, už pažeidimus taikomos finansų teisės aktuose | Valdymo organai tiesiogiai atsakingi už kibernetinio saugumo priemonių patvirtinimą ir priežiūrą; gali būti taikoma asmeninė |

| | | | | |
|---|---|---|---|---|
| | atsakomybės nenumato. | neveiklumą nenustatytos. | numatytos sankcijos. | atsakomybė ir pareigų ribojimas. |
| **Tiekimo grandinė ir IRT trečiosios šalys** | Tiekimo grandinės kibernetinis saugumas išskiriamas kaip SCRM kategorija, numatanti rizikos identifikavimą ir kontrolės priemones. | Priedo A kontrolės A.5.19–A.5.23 reglamentuoja tiekėjų santykius ir su IRT paslaugomis susijusias rizikas. | Įtvirtina išsamią IRT trečiųjų šalių rizikos valdymo sistemą (sutartiniai reikalavimai, registrai, koncentracijos rizika) ir ES lygmens kritinių IRT paslaugų teikėjų priežiūrą. | Reikalauja vertinti tiekimo grandinės kibernetines rizikas ir mažinti kritines priklausomybes, derinamas su sektoriniais aktais, pvz., DORA. |
| **Sankcijos už neįgyvendinimą** | Sankcijų nenumato, pasekmės pirmiausiai reputacinė žala, sutarčių pažeidimas, jei CSF įtrauktas į juos. | Sankcijos – tai galiojančio sertifikato sustabdymas arba panaikinimas, sutartinės ir reputacinės pasekmės. | Numato administracines finansines sankcijas ir kitus poveikio mechanizmus, kuriuos taiko nacionalinės ir ES priežiūros institucijos. | Numato baudas, iki 10 mln. EUR arba 2 % pasaulinių metinių pajamų „essential“ subjektams ir iki 7 mln. EUR arba 1,4 % pajamų „important“ subjektams. |

Apibendrinant galima teigti, kad NIST CSF 2.0, ISO/IEC 27001, DORA ir TIS2 reikalavimai iš esmės persidengia pagrindinėse kibernetinio saugumo srityse, t.y. vadovybės įsitraukimo ir organizacinio valdymo, rizikų valdymo, incidentų valdymo, veiklos tęstinumo ir tiekimo grandinės saugumo reikalavimuose. Analizė parodė, jog plačiausią kibernetinio saugumo valdymo modelį siūlo savanoriškas NIST CSF 2.0 funkcijų modelis, tuo tarpu ISO/IEC 27001 fokusuojasi į ISVS įgyvendinimo ir palaikymo mechanizmą. DORA taikymo sritis aiškiai apibrėžta finansų sektoriaus skaitmeninio atsparumo užtikrinimu ir šioje srityje papildo tiek TIS2, tiek bendruosius kibernetinio saugumo standartus. TIS2 direktyva, priešingai, nustato privalomą minimalų kibernetinio saugumo reikalavimų lygį plataus spektro įvairių sektorių ir skirtingų didžių kibernetinio saugumo subjektams ES mastu. Dėl šių priežasčių, privalomumo ir taikymo spektro platumo, šiame darbe TIS2 direktyva pasirenkama kaip organizacijų brandos ir atitikties vertinimo pagrindas, siekiant apimti kuo platesnį praktinio panaudojimo lauką.

## 2. TIS 2 direktyvos reikalavimų analizė

TIS2 reikalavimų analizė buvo vykdoma remiantis TIS2 EU Direktyvos, Įgyvendinimo Reglamento, Lietuvos KSĮ ir kitais teisiniais dokumentais. Taip pat buvo naudojami antriniai šaltiniai – ENISA gairės, KAM KSRA, NKSC gairės ir ataskaitos. Analizuojant pirmiausiai buvo siekiama suprasti direktyvos struktūrą: direktyvos taikymo sritį, TIS2 subjektų kategorijas, reikalavimų įgyvendinimo proporcingumo principą, subjektų priežiūros ir sankcijų (baudų) diferenciaciją. Antrame etape buvo fokusuojamasi į pagrindinių TIS2 reikalavimų analizę bei susitelkta į straipsnius ir gaires kurie tiesiogiai reglamentuoja ir išaiškina subjektų pareigas, identifikuojant konkrečius žodinius nurodymus (pvz., "privalo", "užtikrina", "turi"), nurodymų objektus (kas turi būti daroma) ir sąlygas (kada, kaip dažnai, kam). Europos kibernetinio saugumo agentūros (ENISA) publikuotos gairės suteikė detalias direktyvos 21 straipsnio priemonių įgyvendinimo principus su praktiniais pavyzdžiais, kaip organizacijos turėtų interpretuoti abstrakčius reikalavimus (pvz., kas sudaro "tinkamą" atsarginių kopijų valdymą arba "veiksmingą" incidentų aptikimo sistemą). Svarbu pabrėžti, kad darbe buvo susikoncentruota į TIS2 reikalavimus, taikomus identifikuotiems kibernetinio saugumo subjektams, neaprėpiant specifinių sektorinių reikalavimų, aprašytų šiuos sektorius reguliuojančiuose reglamentuose, kaip pvz. DORA arba EIDAS. Besiremiant dokumentais, vadinamos TIS2 minimalios priemonės subjektams buvo dekonstruotos į smulkesnius reikalavimus, kurie trečiame skyriuje buvo transformuoti į kibernetinio saugumo vertinimo klausimus. Lietuvos nacionalinio Kibernetinio saugumo įstatymo analizė padėjo išskirti esminius aspektus aktualius nacionaliniam direktyvos įgyvenimui. Pavyzdžiui reikalavimų įgyvendinimo terminus – organizacinės priemonės turi būti įgyvendintos per 12 mėnesių nuo subjekto registracijos NKSC, o techninės priemonės – per 24 mėnesius. Lietuvos įstatymas detalizuoja NKSC priežiūros kompetencijas ir inspekcijų procedūras, kas o Kibernetinio Saugumo Reikalavimų Aprašas (KSRA) tapo svarbių šaltiniu atliekant detalią reikalavimų analizę.

TIS2 reikalavimų analizė buvo vykdoma remiantis TIS2 direktyva, ją įgyvendinančiu ES įgyvendinimo reglamentu, Lietuvos Respublikos Kibernetinio saugumo įstatymu (KSĮ) ir kitais susijusiais teisiniais dokumentais. Papildomai buvo naudojami antriniai šaltiniai – Europos Sąjungos kibernetinio saugumo agentūros (ENISA) gairės, Lietuvos Respublikos krašto apsaugos ministerijos patvirtintas Kibernetinio saugumo reikalavimų aprašas (KSRA), Nacionalinio kibernetinio saugumo centro (NKSC) gairės ir ataskaitos.

Analizuojant pirmiausia buvo siekiama suprasti TIS2 direktyvos struktūrą: jos taikymo sritį, TIS2 subjektų kategorijas, reikalavimų įgyvendinimo proporcingumo principą, subjektų priežiūros mechanizmus ir sankcijų (baudų) diferenciaciją. Antrame etape buvo fokusuojamasi į pagrindinių TIS2 reikalavimų analizę – identifikuojant direktyvos straipsnius ir gaires, kurie tiesiogiai reglamentuoja ir išaiškina subjektų pareigas, sistemingai fiksuojant konkrečius žodinius nurodymus (pvz., „privalo“, „užtikrina“, „turi“), nurodymų objektus (kas turi būti daroma) ir taikymo sąlygas (kada, kaip dažnai, kam).

ENISA publikuotos gairės suteikė detalius TIS2 direktyvos 21 straipsnyje numatytų priemonių įgyvendinimo principus ir praktinius pavyzdžius, kaip organizacijos galėtų interpretuoti abstrakčius reikalavimus (pvz., kas sudaro „tinkamą“ atsarginių kopijų valdymą arba „veiksmingą“ incidentų aptikimo sistemą). Svarbu pažymėti, kad darbe buvo susikoncentruota į TIS2 reikalavimus, taikomus identifikuotiems kibernetinio saugumo subjektams, neaprėpiant specifinių sektorinių reikalavimų, nustatytų atskiruose sektorius reguliuojančiuose ES reglamentuose, pavyzdžiui, DORA ar eIDAS.

Remiantis minėtais dokumentais, TIS2 numatytos minimalios priemonės subjektams buvo dekonstruototi į smulkesnius reikalavimus, kurie trečiame darbo skyriuje transformuoti į kibernetinio saugumo vertinimo klausimus. Lietuvos nacionalinio Kibernetinio saugumo įstatymo analizė padėjo išskirti esminius aspektus, aktualius direktyvos įgyvendinimui nacionaliniu lygmeniu. Pavyzdžiui, nustatyti reikalavimų įgyvendinimo terminai – organizacinės priemonės turi būti įgyvendintos per 12 mėnesių nuo subjekto registracijos NKSC, o techninės priemonės – per 24 mėnesius. Lietuvos teisės aktai taip pat detalizuoja NKSC priežiūros kompetencijas ir inspekcijų procedūras, o Kibernetinio saugumo reikalavimų aprašas (KSRA) tapo vienu pagrindinių šaltinių atliekant detalią TIS2 reikalavimų analizę.

### 2.1. Europos Sąjungos geroji patirtis – ENISA teikiamos ataskaitos ir rekomendacijos

TIS2 direktyva yra fundamentali Europos Sąjungos kibernetinio saugumo teisinė priemonė, pakeitusi ankstesnę TIS direktyvą ir reikšmingai sustiprinusi tinklų ir informacinių sistemų saugumo reikalavimus visoje Sąjungoje [[30] ] Europos Sąjungos kibernetinio saugumo agentūra (ENISA) vykdo kritinį vaidmenį įgyvendinant šią direktyvą. ENISA – tai pagrindinis ES ekspertinis centras kibernetinio saugumo srityje. Jos mandatas ir funkcijos nustatytos Reglamente (ES) 2019/881, vadinamame Kibernetinio Saugumo Akte, kuriuo ENISA suteikiamas nuolatinis mandatas ir paveda-mas Europos kibernetinio saugumo sistemos koordinavimas. ENISA, kaip žinių ir informacijos centras, teikia patarimus ir ekspertinę pagalbą Europos Komisijai ir valstybėms narėms, skatina geruųjų

praktikų mainus, veikia kaip Kompiuterinių incidentų reagavimo komanda (angl. *Computer Incident Response Team,* toliau CSIRT) bei TIS bendradarbiavimo grupės sekretoriatas.[[44] ] Nors jos veiklą reglamentuojantis ES teisės aktas yra privalomas, pati ENISA neturi įgaliojimų priimti nacionalinėms organizacijoms tiesiogiai privalomų normų ar skirti sankcijų – tai lieka valstybių narių priežiūros institucijų ir nacionalinės teisės kompetencijoje.[[44] ] TIS2 direktyvos kontekste ENISA atlieka metodologinio tilto tarp teisinių reikalavimų ir praktinio įgyvendinimo vaidmenį. Agentūra rengia technines gaires ir gerosios praktikos dokumentus, kuriais remiasi tiek ES institucijos, tiek nacionaliniai reguliuotojai bei reguliavimo subjektai – organizacijos. 2025 m. ENISA paskelbė „TIS2 Kibernetinio saugumo valdymo priemonių techninio įgyvendinimo gidą“ (angl. „*NIS2 Technical Implementation Guidance*“), šis dokumentais – tai išsami ataskaita, kurioje detalizuojamos TIS2 Direktyvos ir TIS2 įgyvendinimo Reglamento (ES) 2024/2690 nurodytos kibernetinio saugumo rizikų valdymo priemonės, pateikiami konkrečių kontrolės priemonių ir atitiktį pagrindžiančių įrodymų pavyzdžiai bei susiejimas su kibernetinio saugumo gairėmis ir standartais, pvz. jau minėtais ISO/IEC 27001 arba CSF2.0 [[45] ]

| Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 (Annex) | | European and internation | |
|---|---|---|---|
| Point No | Title | ISO standard 27001:2022 | NIST Cybersecurity Framework v2.0 |
| 1.1 | Policy on the security of network and information systems | 5.2, A.5.1, A.5.36, A.5.4, 9.3 | PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04 |
| 1.2 | Roles, responsibilities and authorities | 5.3, A.5.2, A.5.3, A.5.4 | GV.RR-02, GV.SC-02, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04 |
| 2.1 | Risk management framework | 6.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, A5.7, A.5.19, A.5.20, A.5.21 | ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, ID.RM-01, GV.RM-06, GV.RR-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04 |

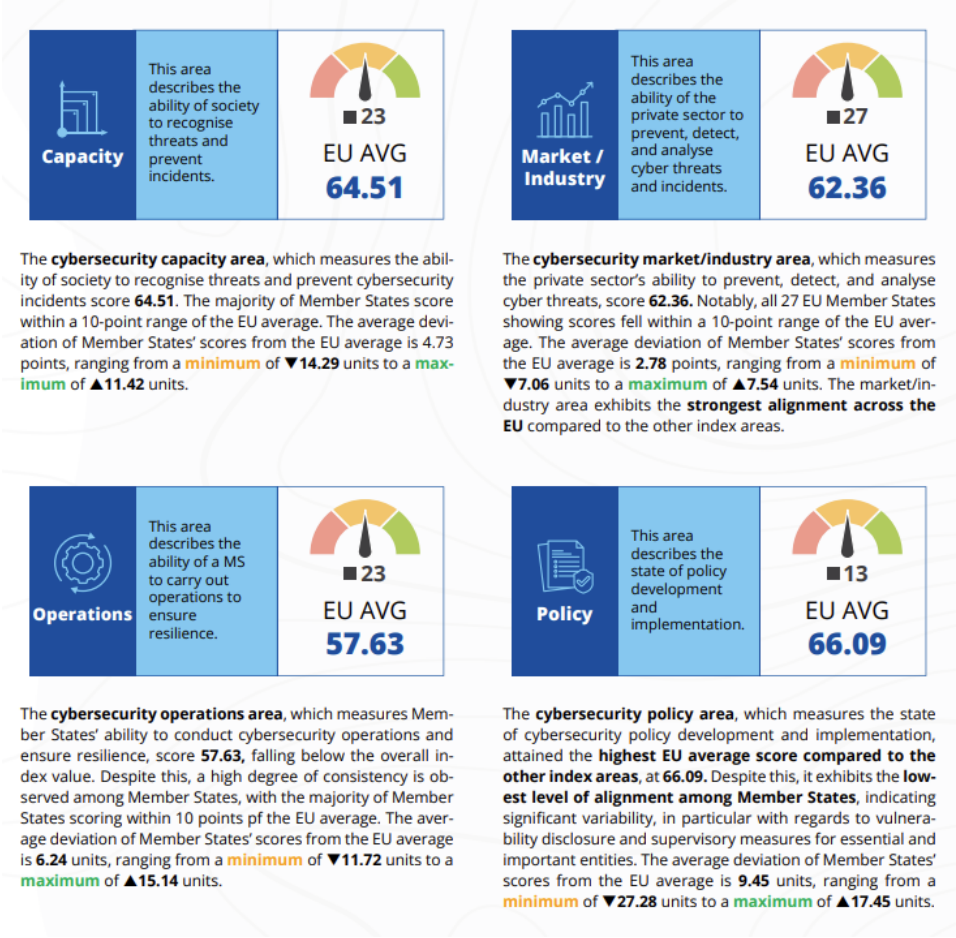
**10 Pav.** Pavyzdys iš ISO27001 ir CSF2.0 susiejimo dokumento. [[45] ]

Teisiniu požiūriu ENISA dokumentai nėra formaliai privalomi teisės aktai, tačiau praktikoje jie įgyja didelę reikšmę aiškinant TIS2 ir susijusių reglamentų turinį. Nacionalinės kibernetinio saugumo priežiūros institucijos remiasi ENISA gairėmis rengdamos metodikas, tikrinimo tvarkas, specifikacijas ir kriterijus. ENISA dokumentai suteikia struktūruotas gaires, kaip teisines TIS2

nuostatas paversti konkrečiomis techninėmis ir organizacinėmis priemonėmis. Tokiu būdu ENISA, neturėdama tiesioginių reguliavimo galių, faktiškai tampa vienu iš pagrindinių TIS2 įgyvendinimo ir harmonizavimo „varikliu“ ES mastu [[46] ]

2024 m. paskelbta „ENISA NIS360 – 2024“ ataskaita yra pirmasis globalaus masto kibernetinio saugumo brandos ir kritiškumo vertinimas pagal TIS2 direktyvą.[[39] ] Šioje studijoje vertinami NIS2 reguliuojami didelės svarbos sektoriai, pateikiama jų kibernetinio saugumo brandos ir kritiškumo analizė, identifikuojamos pažangos sritys ir esamos spragos. Ataskaitoje pabrėžiama, kad nors daugelis sektorių padarė nemažai svarbių žingsnių link TIS2 reikalavimų įgyvendinimo, vis dar egzistuoja reikšmingų spragų, ypač mažesnėse valstybėse narėse ir tarp paslaugų teikėjų, kuriems dažnai trūksta resursų sistemingam kibernetinio saugumo valdymui [[38] ][[39] ] ENISA sukaupta informacija iš skirtingų ES valstybių rodo, kad sėkmingas TIS2 direktyvos įgyvendinimas reikalauja holistinio požiūrio, apimančio ne tik technines priemones, bet ir organizacinius bei valdymo aspektus.[[38] ] Agentūra rekomenduoja taikyti rizikos valdymo principus kaip centrinę kibernetinio saugumo valdymo ašį: organizacijos turėtų pradėti nuo grėsmių modeliavimo (angl. *threat modelling*), identifikuoti kritinę infrastruktūrą ir taikyti proporcingas, rizika grįstas kontrolės priemones, atitinkančias jų rizikos profilį.[[1] ][[38] ] Rekomendacijose nuosekliai akcentuojama aukščiausios grandies vadovybės ir valdybų atsakomybė už kibernetinį saugumą. 2024 m. kibernetinio saugumo būklės ataskaitoje pabrėžiama, kad valdybos nariai ir vyresnioji vadovybė turi dalyvauti kibernetinio saugumo mokymuose ir aktyviai įsitraukti į organizacijos kibernetinio saugumo strategijos formavimą.[[38] ] Tai reiškia, kad TIS2 direktyvos įgyvendinimas negali būti traktuojamas vien kaip IT padalinio užduotis, o kibernetinis saugumas turi tapti integralia organizacinės kultūros dalimi ir būti įtrauktas į bendrą rizikos valdymo ir strateginio planavimo procesą. Savo ataskaitose ENISA nuosekliai išskiria tiekimo grandinių saugumą. Jau minėtoje „ENISA NIS360 – 2024“ ataskaitoje nurodoma, kad tiekimo grandinių saugumui būtina skirti papildomą dėmesį, įskaitant bendrą ES masto koordinuotą rizikos vertinimą ir horizontalios tiekimo grandinės saugumo politikos formavimą.[[38] ] ENISA rekomendacijose pabrėžiama, kad kritinės infrastruktūros subjektai turi nuolat vertinti savo tiekėjų ir paslaugų teikėjų kibernetinio saugumo lygį, nustatyti aiškius minimalius kibernetinio saugumo standartus ir įtraukti tiekimo grandinės reikalavimus į sutartis bei pirkimo procesus.[[38] ][[39] ] Šis požiūris ypač svarbus skaitmeninės infrastruktūros ir debesijos paslaugų sektoriuose, kur trečiųjų šalių pažeidžiamumai gali sukelti kaskadinių (angl. *cascade*) pasekmių visai ekosistemai.[[1] ]

Kitas svarbus dokumentas - naujai parengtas ES kibernetinio saugumo indeksas, kurį ENISA parengė kartu su valstybėmis narėmis, pateikia valstybių narių kibernetinio saugumo pajėgumų ir brandos vaizdą.[[40] ] Šis indeksas apibūdina valstybių narių kibernetinio saugumo būklę pagal kelias rodiklių grupes ir sudaro prielaidas tarpusavio lyginamajai analizei bei tarpusavio mokymuisi (angl. *peer-learning*) tarp valstybių. Indekso duomenys rodo, kad TIS2 direktyvos praktinis įgyvendinimas tarp valstybių narių labai skiriasi: dalis šalių jau pasiekė aukštą atitikties ir kibernetinio saugumo pajėgumų lygį, o kitos dar tik pradeda sistemingą transformaciją.[[40] ] Šis darbas fokusuojasi į organizacijų atitikties situaciją, todėl apsiribojama paminėjimu, kad ataskaita suteikia svarbų kontekstą bandant suprasti Lietuvos situaciją bendrai ir norint objektyviai ją įvertinti, lyginant ją su kitų valstybių rezultatais ir analizuojant veiksnius, lėmusius spartesnę pažangą arba atvirkščiai atsilikimą.



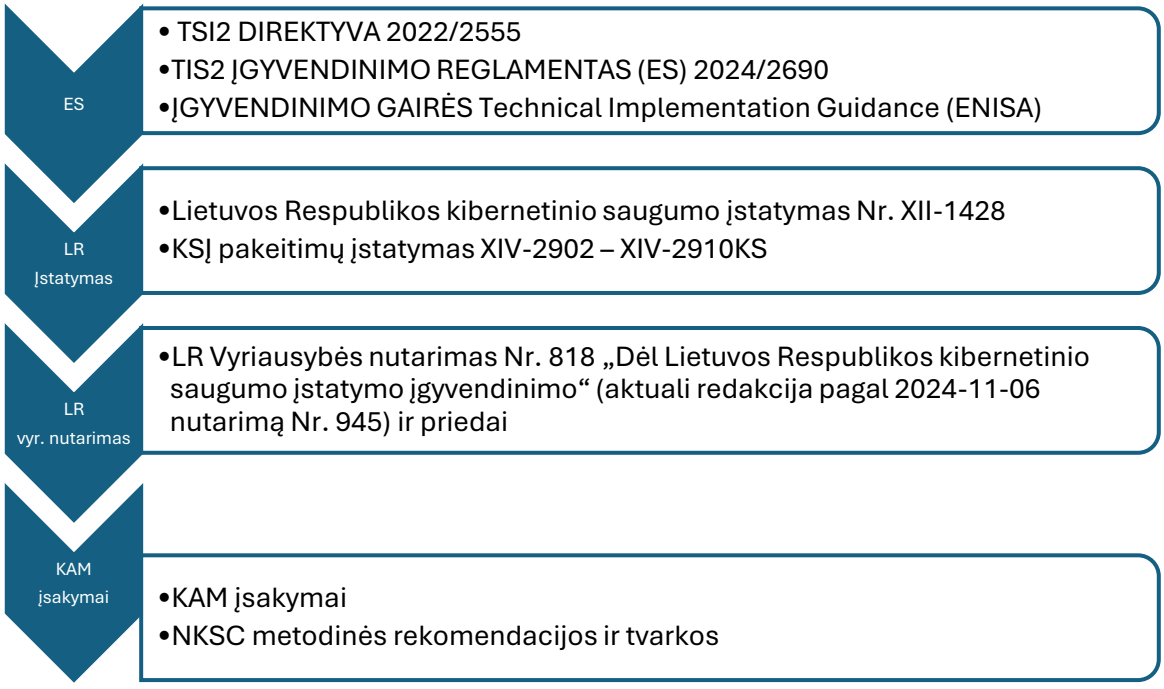

**11 Pav.** ES kibernetinio saugumo indeksas. [[40] ]

ENISA 2024 m. ataskaitoje apie kibernetinių grėsmių kraštovaizdį pažymima, kad kritinės infrastruktūros sektoriuose, tokiuose kaip energetika, transportas ir elektroninių ryšių paslaugos, 2023–2024 m. laikotarpiu fiksuotas reikšmingas incidentų skaičiaus ir sudėtingumo augimas.[[1]

][[38] ] Ataskaita išskiria pagrindines grėsmių kategorijas ir jų tendencijas, tarp jų atskirai verta paminėti išorinių valstybių remiamų veikėjų ir vadinamųjų „haktivistų“ (terminas, sudedama iš hakerių aktyvistų angl. *hacktivists*) veiklą, kuri pasireiškia kaip kibernetinio karo forma.[[1] ] Šių grėsmių visumą tiesiogiai paaiškina, kodėl Europos Sąjunga pasirinko peržiūrėti ir sustiprinti ankstesnę TIS direktyvą, apibrėždama griežtesnius TIS2 direktyvos reikalavimus tiek techniniam, tiek organizaciniam kibernetinio saugumo valdymui.

### 2.2. TIS2 reikalavimų perkėlimas į nacionalinę teisės sistemą

Lietuvoje TIS2 direktyvos nuostatos į nacionalinę teisę perkeltos (transponuotos) į Lietuvos Respublikos kibernetinio saugumo įstatymo (KSĮ) paskutinę redakciją, kurio pakeitimo įstatymas priimtas 2024 m. liepos 11 d. (Nr. XIV-2902), o suvestinė redakcija įsigaliojo 2024 m. spalio 18 d. [[34] ] Analizuojant TIS2 direktyvos perkėlimo į Lietuvos teisinę sistemą analizę, buvo atskirti skirtingi norminiai lygmenis ir jų tarpusavio ryšiai. Žemiau pavaizduota kaip TIS2 reikalavimai nuosekliai lokalizuojami iš ES teisės aktų į nacionalinį įstatymą, nutarimus ir galiausiai į praktinį įgyvendinimą, kurį koordinuoja Krašto Apsaugos Ministerija (KAM) ir Nacionalinis Kibernetinio Saugumo Centras (NKSC) pasitelkus Kibernetinio saugumo informacinę sistemą (KSIS) ir susijusius procesus.




**12 Pav.** Supaprastintas TIS2 teisinis perkėlimas į LR teisinę sistemą.

LR KSĮ ne tik „įsirašo“ TIS2 direktyvos tekstą, bet ir adaptuoja ją Lietuvos nacionaliniam teisiniam, institucinės sąrangos ir viešojo valdymo kontekstui [[34] ] Atnaujintame įstatyme esminė naujovė – tai yra aiškiai apibrėžtos esminių ir svarbių kibernetinio saugumo subjektų kategorijos, tiesiogiai atitinkančios TIS2 direktyvos logiką.[[34] ] Įtraukimas į atitinkamą kibernetinio saugumo subjektų kategoriją priklauso nuo kelių faktorių, vienas iš faktorių – tai priklausimas ypatingos svarbos ir kitų itin svarbių organizacijų sektoriui (detaliai subjektų kategorijos priskyrimo logika aprašyta šio darbo 3 skyriaus kritiškumo vertinimo komponento rengimo aprašyme). Skirtumas tarp esminių ir svarbių subjektų reguliavime yra pagrindas priežiūros režimo bei vykdymo užtikrinimo priemonių diferenciacijai. Esminiams subjektams taikoma išsami išankstinė ir vėlesnė (lot. *ex ante* ir *ex post*) priežiūra, o svarbiems subjektams taikoma tik vėlesnė (lot. *ex post*) priežiūra. Esminių subjektų atžvilgiu įstatymas leidžia taikyti griežčiausias vykdymo užtikrinimo priemones, pavyzdžiui, laikinai sustabdyti veiklą ar laikinai nušalinti vadovą nuo pareigų, taip pat skiriasi skiriamų baudų didžiai [[34] ]


**13 Pav.** Sankcijos kibernetinio saugumo subjektams. [[41] ]

Ši diferenciacija atspindi TIS2 direktyvos proporcingumo principą, kai priežiūros intensyvumas turi atitikti reguliuojamo subjekto kritiškumą ir galimo incidento poveikį.[[30] ]

Instituciniu požiūriu atnaujintas Kibernetinio saugumo įstatymas aiškiai apibrėžia kibernetinio saugumo politikos formavimo ir įgyvendinimo architektūrą. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Krašto apsaugos ministerija (KAM), o pagrindinė vykdomoji institucija, atsakinga už kibernetinio saugumo reikalavimų priežiūrą, incidentų

valdymo koordinavimą ir kibernetinio saugumo subjektų registrą, yra Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos. Svarbų vaidmenį sektorių priežiūroje taip pat atlieka Ryšių reguliavimo tarnyba (RRT) ir kitos sektorių institucijos, bendradarbiaujančios su NKSC pagal KSĮ 20 straipsnyje įtvirtintą tarpinstitucinio bendradarbiavimo modelį [[34] ]

Atnaujintas įstatymas nustato, kad esminiai ir svarbūs kibernetinio saugumo subjektai įgyja jiems taikomas pareigas tik nuo įregistravimo Kibernetinio saugumo informacinėje sistemoje (KSIS) ir įtraukimo į Kibernetinio saugumo subjektų registrą momento.[[34] ] Detaliai aprašytas KSĮ 13 straipsnio procesas, išskyrus atvejus kai subjektai identifikuojami kai pagal Vyriausybės nustatytą identifikavimo pagal specialiuosius kriterijus metodiką, organizacijos praktikoje susideda iš kelių etapų:

a) Organizacija privalo įsivertinti;
b) Atitinkanti identifikavimo kriterijus organizacija KSIS duomenų tvarkytojui pateikia KSIS nuostatuose numatytus duomenis;
c) Kibernetinio saugumo subjektą registruoja ir išregistruoja Kibernetinio saugumo informacinės sistemos duomenų tvarkytojas;
d) Institucijos, atsakingos už kibernetinio saugumo subjektų identifikavimą, numatytos KSĮ sektorių prieduose 1 ir 2, patvirtina duomenis apie kibernetinio saugumo subjektą;
e) Pasikeitus situacijai, gavus atitinkamą informaciją, KSIS duomenų tvarkytojas išregistruoja subjektą [[34] ]

Kibernetinio saugumo įstatymas ir jį įgyvendinantys teisės aktai nustato minimalų organizacinių kibernetinio saugumo priemonių lygį. Kibernetinio saugumo subjektai privalo:

a) patvirtinti kibernetinio saugumo politiką, kurioje nustatomi strateginiai saugumo tikslai, rizikos tolerancijos ribos ir priemonių įgyvendinimo programa;
b) paskirti organizacijos kibernetinio saugumo vadovą arba lygiavertę funkciją atliekantį atsakingą asmenį, vadinamą vyriausiąjį informacijos saugumo pareigūną, (angl. *Chief Information Security Officer, CISO*), kuris būtų tiesiogiai atskaitingas aukščiausiajai vadovybei;
c) užtikrinti vadovybės įsitraukimą, reguliariai aptariant kibernetinio saugumo klausimus valdymo organuose[[34] ]

Techninės priemonės apima informacijos saugumo kontrolių įgyvendinimą, tinklų ir informacinių sistemų stebėseną, prieigos valdymą, šifravimą, atsarginių kopijų darymą, pažeidžiamumų vertinimą

ir kitas priemones, išdėstytas Kibernetinio saugumo reikalavimų apraše.[[41] ] Subjektai privalo ne rečiau kaip kartą per trejus metus atlikti kibernetinio saugumo auditą, vadovaudamiesi NKSC tvirtinama metodika.[[34] ]

Incidentų valdymo srityje KSĮ perima TIS2 direktyvos 23 straipsnyje nustatytą trijų pakopų pranešimų modelį:

a) ankstyvasis įspėjimas, ne vėliau kaip per 24 valandas nuo to momento, kai subjektas sužino apie didelį kibernetinį incidentą;
b) išsamus incidento pranešimas, ne vėliau kaip per 72 valandas nuo pirmojo pranešimo;
c) galutinė ataskaita, ne vėliau kaip per vieną mėnesį nuo išsamaus pranešimo pateikimo [[42] ]

Nacionaliniu lygmeniu KSĮ 18 straipsnyje įtvirtinta, kad apie didelius kibernetinius incidentus esminiai ir svarbūs subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui, kuris koordinuoja tolimesnius veiksmus ir, esant tarpvalstybinėms pasekmėms, organizuoja sąveiką su kitomis valstybėmis narėmis ir ENISA[[34] ]

Analizuojant TIS2 direktyvos perkėlimo į Lietuvos KSĮ ypatumus, buvo pastebėta didelė struktūrinė atitiktis, tačiau taip pat pastebėta, jog Lietuvos teisė kai kurias sritis detalizavo ir papildė. Pirmiausia tai tiekimo grandinės saugumas, KSĮ ir Kibernetinio saugumo reikalavimų aiškiai įtvirtina pareigą esminiams ir svarbiems subjektams vertinti tiekėjų ir paslaugų teikėjų kibernetinio saugumo lygį bei nustatyti sutartinius reikalavimus dėl incidentų valdymo, saugumo sertifikavimo ir bendradarbiavimo aprašas [[34] ][[42] ] Antra, ypač akcentuojamas viešojo administravimo ir nacionaliniam saugumui svarbių subjektų vaidmuo, integruojant KSĮ su nacionalinio saugumo teisiniu reguliavimu ir sudarant galimybę taikyti griežtesnes vykdymo užtikrinimo priemones strateginės svarbos institucijoms [[43] ] Tai parodo, kad Lietuva į kibernetinio saugumo sistemą žvelgia ne tik kaip į technologinio, ekonominio ir visuomeninio, bet ir kaip į nacionalinio saugumo klausimą.

### 2.3. TIS2 pagrindiniai kibernetinio saugumo reikalavimų analizė.

TIS2 direktyvos 21 straipsnis nustato vienodą kibernetinio saugumo valdymo priemonių branduolį, kuris taikomas ir esminiams, ir svarbiems subjektams. Valstybės narės privalo užtikrinti, kad kibernetinio saugumo subjektai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, valdytų rizikas ir sumažintų incidentų poveikį paslaugų gavėjams bei kitoms priklausomoms paslaugoms.[[30] ] Toliau skyriuje aptariami išsamūs subjekto kibernetinio saugumo statuso nustatymo kriterijai.

TIS2 direktyvos taikymo srities nustatymas yra kompleksiškas procesas, kuris reikalauja ne tik vertinamo subjekto sektorinės priklausomybės identifikavimo, bet ir jo kritinės svarbos visuomenei bei ekonomikai vertinimo. Kritiškumo vertinimo procesas kyla iš direktyvos proporcingumo principo, kuris nustato, kad subjektai, kurių paslaugų nutraukimas turėtų rimčiausių pasekmių visuomenei, turi būti priskiriami prie esminių subjektų kategorijos ir todėl privaloma jiems taikyti maksimalias priežiūros bei reikalavimų vykdymo užtikrinimo priemonės. Kritiškumo vertinimas integruoja penkis pagrindinius vertinimo aspektus, kiekvienas iš kurių atspindi skirtingus direktyvos apsektus ir susijusius teisės aktus.

Pirmasis kritiškumo vertinimo aspektas yra ypatingos svarbos subjektų identifikavimas pagal Ypatingos svarbos subjektų atsparumo direktyvą (toliau YSS). Ši direktyva, įsigaliojo lygiagrečiai su TIS2 direktyva 2023 m. sausio mėn., jos abi skirtos Europos Sąjungos kritinės infrastruktūros atsparumui stiprinti, tačiau skirtingais aspektais: TIS2 orientuota į kibernetinius saugumą ir skaitmenines grėsmes, o YSS orientuota į fizinį atsparumą ir taip vadinamą „visų pavojų požiūrį“ (angl. *all-hazards approach*), apimantį gamtines stichijas, teroro atakas, sabotažą, vidaus grėsmes.[[55] ] ES valstybės narės privalo identifikuoti kritinius subjektus pagal YSS direktyvą iki 2026 m. liepos 17 d., Lietuvoje YSS direktyva jau yra įgyvendinama per Krizių valdymo ir civilinės saugos įstatymą, giliau YSS direktyva ir KVCS įstatymas šiame darbe nėra nagrinėjamas, apsiribojama principu: pagal YSS direktyvą identifikuoti kritiniai subjektai automatiškai laikomi esminiais subjektais (angl. *essential entities*) pagal TIS2 direktyvą.

Antrasis kritiškumo vertinimo aspektas – tai priklausomybė TIS2 direktyvos 1 Priedui (lot. *Annex I*) arba 2 Priedui (lot. *Annex II*) priedų sektorių sąrašams, Lietuvos įstatyme sektoriai įtraukti į 1 ir 2 priedus atitinkamai. 1 Priedas apima 11 ypatingai svarbių sektorių (angl. *sectors of high criticality*), 2 Priedas – 7 kitus itin svarbius sektorius (angl. *other critical sectors*). Žemiau Lentele SSEKTORIAI

pateiktas sektorių sąrašas, su sektorių detalizacija pateiktas KSĮ prieduose galima susipažinti prieduose.

2 lentelė. **TIS2 sektoriai.**

| TIS2 1 Priedas<br>(KSĮ – Ypatingos svarbos sektoriai) | TIS2 2 Priedas<br>(KSĮ - Kiti itin svarbūs sektoriai) |
|---|---|
| Energetika,<br>Transportas,<br>Bankininkystė,<br>Finansų rinkų infrastruktūros objektai,<br>Sveikatos priežiūra,<br>Geriamasis vanduo,<br>Nuotekos,<br>Skaitmeninė infrastruktūra,<br>IRT paslaugų valdymas (B2B),<br>Viešasis administravimas,<br>Kosmosas | Pašto paslaugos,<br>Atliekų tvarkymas,<br>Cheminių medžiagų gamyba ir platinimas,<br>Maisto gamyba, perdirbimas ir platinimas,<br>Gamyba,<br>Informacinės visuomenės paslaugos,<br>Moksliniai tyrimai |

Trečiasis kritiškumo vertinimo aspektas yra specialių subjektų kategorija, kuri pagal TIS2 direktyvos 2 straipsnio 2 dalį apima tris specialių tipų organizacijas, kurios automatiškai priskiriamos esminių subjektų kategorijai nepriklausomai nuo jų dydžio ar TIS2 sektorių kategorijos. Pirmoji specialių subjektų kategorija – tai kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai (angl. *Qualified Trust Service Providers*) nustatyti pagal eIDAS reglamentą. Šie subjektai teikia kvalifikuotas elektroninio parašo, antspaudų, laiko žymų ir kitas patikimumo paslaugas, kurios yra fundamentalios visos ES skaitmeninės ekonomikos funkcionalumui, todėl jų kompromitavimas turėtų tarptautinio masto pasekmes. Pagal paskutinę reglamento redakciją (įsigaliojo 2024 m. gegužę) patikimumo paslaugų teikėjai privalo atitikti ne tik eIDAS reglamento reikalavimus, bet ir TIS2 direktyvos 21 straipsnį [[56] ]. Antroji specialių subjektų kategorija – aukščiausiojo lygio domenų (angl. *Top-Level Domain*, TLD) vardų registrai ir domenų vardų sistemų (angl. *Domain Name System*, DNS) paslaugų teikėjai. TLD registrai (pvz., .lt Lietuvai) yra kritinė interneto infrastruktūros dalis, nes valdo vardų erdvės šakninį (angl. *root)* lygmenį, o DNS paslaugų teikėjai užtikrina paslaugas, be kurių „paprastų vartotojų“ internetas praktiškai neveiktų. Trečioji specialių subjektų kategorija – telekomunikacijų operatoriai, kurie teikia viešąsias elektroninių ryšių tinklus ir paslaugas pagal Europos elektroninių ryšių kodeksą[[57] ]. Ketvirtoji kategorija – viešojo administravimo subjektai nacionaliniu ar regioniniu lygmeniu, kurie, nors ir neteikia komercinės paslaugas, yra kritiniai subjektai visuomenės funkcionalumui (pvz., mokesčių administravimo, socialinio draudimo ir pan. IT infrastruktūros valdymas).

Ketvirtasis kritiškumo vertinimo aspektas yra organizacijos dydžio vertinimas pagal du kriterijus: darbuotojų skaičių ir finansinius rodiklius (metinė apyvarta arba balansas). Direktyva nustato trijų kategorijų dydžio slenkstį:

a) didelės įmonės: >250 darbuotojai IR >50 mln. eurų apyvarta;
b) vidutinio dydžio įmonės: 50–249 darbuotojai IR >10 mln. eurų apyvarta arba balansas;
c) mažos įmonės: <50 darbuotojai IR ≤10 mln. eurų apyvarta arba balansas;

Organizacijos dydžio vertinimas veikia tokiu principu – 1 Priedo sektoriaus didelės įmonės automatiškai priskiriamos prie esminių, vidutinio dydžio įmonės priskiriamos prie svarbių, o mažos įmonės nepriskiriamos TIS2 taikymo apimčiai, išskyrus atvejus, kai įmonė priklauso jau minėtai specialių subjektų kategoriją arba kai išimties tvarka priimamas specialus valstybės įstatymas dėl įmonės kritiškumo nepriklausomai nuo kitų kriterijų. Visos didelės ir vidutinės organizacijos priklausančios 2 Priedo sektoriams priskiriamos prie svarbių kibernetinio saugumo subjektų, išskyrus atvejus, kai jos atitinka specifinės reikšmės kriterijų, aprašytam žemiau kaip penktasis kritiškumo vertinimo aspektas.

Penktasis kritiškumo vertinimo aspektas – tai organizacijos specifinės reikšmės sektoriuje vertinimas, kuris taikomas 2 Priedo sektoriaus identifikuotoms didelėms ir vidutinio dydžio įmonėms, siekiant nustatyti, ar joms turėtų būti priskirtas esminių kibernetinio saugumo statusas. Apibrėžti kriterijai specifinei reikšmei identifikuoti:

a) organizacija yra vienintelis paslaugos tiekėjas valstybėje (angl. *sole provider*);
b) paslaugos nutraukimas galėtų turėti reikšmingą neigiamą poveikį visuomenės saugumui, apsaugai arba sveikatai;
c) paslaugos nutraukimas galėtų sukelti reikšmingą sisteminę riziką (angl. *significant systemic risk*);
d) organizacija turi specifinę reikšmę nacionaliniu ar regioniniu lygmeniu konkrečiam sektoriui arba paslaugų tipui;

TIS2 subjekto statuso kategorijos pavaizduotos lentele SUBJEKLTAI. Ir logika Trečiame skyriuje ši logika panaudojama vertinimo įrankio subjekto kritiškumo nustatymui.

3 lentelė. **Subjektų kategorijos.**

| Esminiai | Svarbūs |
|---|---|
| Ypatingos svarbos subjektai (CER Direktyva)<br>Specialūs subjektai<br>Priedas I didelės organizacijos<br>Priedas II specifinės reikšmės subjektai | Priedas I vidutinės organizacijos<br>Priedas II didelės ir vidutinės organizacijos |

Kaip jau buvo minėta, priklausomai nuo nustatyto subjekto kritiškumo statuso, skiriasi subjekto priežiūros intensyvumas bei skiriamos baudos ir sankcijos bet nesikeičia bazinis TIS2 reikalavimų rinkinys, tačiau reikalavimai gali turėti specifinius akcentus, numatytus įgyvendinimo gairėse, įprastai raginant didesnį dėmesį skirti atitinkamo reikalavimo įgyvendinimui, įprastai tai aktualu esminiams ir 1 Priedo sektoriams priklausantiems kibernetinio saugumo subjektams.

Tęsiant TIS2 reikalavimų analizę svarbu tiesiogiai palyginti reikalavimų formulavimą TIS2 direktyvoje ir LR KSĮ. Jau buvo minėta, jog LR KSĮ iš esmės perima TIS2 direktyvos reikalavimų struktūrą, tačiau ją semantiškai išplečia ir sukonkretina nacionalinės teisės kontekste. TIS2 formuluotės yra gana trumpos ir funkcinės, tuo tarpu LR KSĮ tie patys elementai pateikti detaliau, įtraukiant papildomas sąvokas ir patikslinimus. Taip pat KSĮ atskirai suformuluotas už kibernetinį saugumą atsakingų asmenų reikalavimas, išskiriama prieigų ir teisių valdymo politikų reikalavimas naudotojams, administratoriams ir tiekėjams bei pažymima galimybė nustatyti kitus, papildomus, reikalavimus. Galima pastebėti ir smulkesnius akcentus, pvz. LR KSĮ aiškiai pabrėžia mokymų reguliarumą, kibernetinio saugumo reikalavimų veiksmingumo įvertinimą ir kt., taip padarant reikalavimus labiau pritaikytus vėlesnei instituciniai priežiūrai. Nežiūrint į tai, šiame darbe, vertinant įmonių kibernetinį saugumą, sąvoka „TIS2 reikalavimai“ vartojama kaip apibendrinantis terminas, apimantis ir LR KSĮ įgyvendintas TIS2 direktyvos nuostatas, todėl atskirai jų neskyrimas neturėtų būti suprantamas kaip nacionalinių KSĮ reikalavimų nepaisymas ar neįvardijimas.

4 lentelė. **TIS2 ir KSĮ reikalavimų formuluočių palyginimas. [[30] ][[41] ]**

| **Reikalavimų formulavimas TIS2 direktyvoje, subjektas privalo turėti:** | **Reikalavimų formulavimas LR KSĮ** |
|---|---|
| a) rizikos analizės ir informacinių sistemų saugumo politika; | 1) kibernetinio saugumo rizikos analizės, tinklų ir informacinių sistemų kibernetinio saugumo politika; |
| | 2) už kibernetinį saugumą atsakingų asmenų, nurodytų šio įstatymo 15 straipsnyje, ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas; |
| b) incidentu valdymas; | 3) kibernetinių incidentų valdymas; |
| c) veiklos tęstinumą, pvz., atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą; | 4) veiklos tęstinumą; |
| d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais; | 5) tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais; |
| e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą; | 6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą; |
| f) politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti; | 7) politiką ir procedūras, skirtas kibernetinio saugumo reikalavimų veiksmingumui įvertinti; |
| g) pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus; | 8) kibernetinės higienos praktiką ir reguliarius kibernetinio saugumo mokymus; |
| h) kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras; | 9) kriptografijos ir šifravimo naudojimo politiką ir procedūras; |
| i) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą; | 10) žmogiškųjų išteklių saugumą, prieigos prie tinklų ir informacinių sistemų kontrolės politiką ir turto valdymą; |
| j) kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą. | 11) kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą; |
| | 12) kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų naudotojų, administratorių, kibernetinio saugumo subjektų tiekėjų, jų subtiekėjų ir kitų ūkio subjektų teisių ir prieigos prie kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų ir (ar) skaitmeninių duomenų suteikimo ir valdymo politiką; |

| | |
|---|---|
| | 13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus kibernetinio saugumo reikalavimus, nustatytus atsižvelgiant į identifikuotas atskirų sektorių kibernetinio saugumo rizikas. |

Žemiau pateiktoje struktūruotoje 5 lentelė. TIS2 reikalavimų detalizacija. vaizduojama reikalavimų detalizacija, remiantis TIS2 direktyva, TIS2 įgyvendinimo reglamentu, ENISA gairėmis ir ataskaitomis bei Lietuvos tesiės aktais – KSĮ, Vyriausybės nutarimais, KAM Kibernetinio saugumo rekomendacijų aprašu (toliau KSRA), bei NKSC rekomendacijomis.

5 lentelė. **TIS2 reikalavimų detalizacija.**

| Reikalavimas | Reikalavimo išaiškinimas |
|---|---|
| Kibernetinio saugumo rizikos analizės, tinklų ir informacinių sistemų kibernetinio saugumo politika | Reikalavimas formuluoja nuostatą, kad kibernetinio saugumo subjektai privalo turėti politiką rizikų analizei bei informacinių sistemų saugumui, kuri būtų paremta visų pavojų (angl. *all-hazards*) ir proporcingumo principu.[[30] ] NKSC parengtas „Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumento galimo turinio“ šablonas detalizuoja, kad politika turi apimti saugumo tikslus, taikomus teisės aktus, įsipareigojimus darbuotojams ir trečiosioms šalims, rizikos vertinimo tvarką, rizikos vertinimo ataskaitas ir rizikos valdymo priemonių planus bei reguliarią politikos peržiūrą.[[53] ] ENISA techninės įgyvendinimo gairės dėl kibernetinio rizikos valdymo priemonių rekomenduoja, kad rizikos analizė ir politika būtų nuolat atnaujinamos, remtųsi pripažintais Europos ir tarptautiniais standartais ir būtų integruotos į visus verslo procesus. [[32] ] |
| Už kibernetinį saugumą atsakingų asmenų ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigos | Reikalavimas įpareigoja valdymo organus patvirtinti kibernetinio saugumo rizikų valdymo priemones, prižiūrėti jų įgyvendinimą ir numato atsakomybę už TIS2 pažeidimus, taip pat nustato valdymo organų narių pareigą nuolat kelti kibernetinio saugumo kompetencijas.[[30] ] Kibernetinio saugumo subjektas turi paskirti už kibernetinį saugumą atsakingus asmenis ir apibrėžti jų funkcijas bei atsakomybes, NKSC šablonas detalizuoja, jog turi būti parengtas atsakingų asmenų ir jų funkcijų sąrašas, dokumentuotas paskyrimas ir aiškiai aprašytos pareigos [[53] ] Pavyzdžiui incidentų valdymo, rizikų valdymo vadovų, TIS turto savininkų vaidmenys. ENISA gairės rekomenduoja pareigas susieti su Europos kibernetinio saugumo kompetencijų sistemos (ECSF) rolėmis, kad būtų užtikrintas aiškus atsakomybės pasiskirstymas ir išvengta atsakomybių vakuumo.[[69] ] Praktikoje tai reiškia, kad turi būti atskirti ir formalizuoti iš vienos pusės organizacijos vadovybės atsakomybė už politikos patvirtinimą, skirtus resursus, užtikrintą įgyvendinimą, o iš kitos pusės – kibernetinį saugumą užtikrinantys operaciniai vaidmenys - *CISO*, IT vadovai, incidentų reagavimo komanda, ir pan. |

| | |
|---|---|
| Kibernetinių incidentų valdymas | Reikalavimas nustato, kad kiekvienas kibernetinio saugumo subjektas privalo turėti incidentų valdymo priemones, TIS2 direktyvoje detalizuojami incidentų pranešimo priežiūros institucijoms taisyklės ir terminai.[[30] ] NKSC incidentų valdymą įvardija kaip viena iš centrinių KSĮ rizikos valdymo priemonių, subjektai privalo valdyti incidentus ir pranešti apie didelius bei kitus reikšmingus incidentus NKSC, vadovaudamiesi Nacionaliniu kibernetinių incidentų valdymo[[42] ] planu ir KSĮ 18 straipsniu[[34] ] NKSC šablone incidentų valdymo dalyje nurodoma, kad turi būti parengtas incidentų valdymo planas, žurnalinių įrašų valdymo tvarka ir planinio testavimo ataskaitos, turi būti aprašyta incidentų aptikimo, eskalavimo, reagavimo, komunikacijos ir rezultatų vertinimo tvarka.[[53] ] ENISA incidentų valdymo gairės pabrėžia, kad incidentų valdymas turi būti struktūruotas ir apimti visą ciklą: parengtis-aptikimas-reagavimas-atstatymas-pamokų įsisavinimas, su aiškiais laiko identifikavimui ir atstatymui (angl. *Mean Time to Detect, Mean Time to Repair/Respond/Resolve,* MTTD, MTTR) našumo rodikliais (angl. *Key Performance Indicators,* KPI*)* ir suderintas su pranešimo institucijoms prievolėmis [[70] ] |
| Veiklos tęstinumas | Reikalavimas įpareigoja užtikrinti veiklos tęstinumą, įskaitant atsarginių kopijų valdymą, atkūrimą po sutrikimų ir krizių valdymą.[[30] ] Veiklos tęstinumas turi būti paremtas visų pavojų požiūriu, apimti fizinių ir kibernetinių grėsmių scenarijus, o priemonės turi būti proporcingos sektoriaus kritiškumui.[[31] ] NKSC šablonas numato, kad veiklos tęstinumo valdymo plane turi būti aprašytos taikymo sąlygos, atkūrimo kriterijai, atsakingi asmenys, valdymo ir atkūrimo grupės, atkūrimo planas, periodinis testavimas ir atsarginių kopijų atstatymo laiko ir versijų (angl. *Recovery Time Objective, Recovery Point Objective* RTO/RPO) rodikliai, taip pat atsarginių kopijų kūrimo, saugojimo ir atkūrimo tvarka bei testavimo ataskaitos. ENISA rizikos valdymo gairės rekomenduoja glaudžiai susieti verslo poveikio analizę (angl. *Business Impact Assessment,* BIA) su veiklos tęstinumo planavimu ir incidentų valdymu, kad būtų užtikrintas minimalus priimtinas paslaugų prieinamumo lygis kritinių incidentų metu.[[32] ] |
| Tiekimo grandinės saugumas, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginų tiekėjų ar paslaugų teikėjų santykiais | Reikalavimas numato, kad subjektai privalo sistemingai vertinti tiekėjų ir paslaugų teikėjų kibernetinę riziką, įskaitant produktų kokybę, saugaus kūrimo praktikas ir kritinių tiekimo grandžių pažeidžiamumus taip pat nurodoma, kad turi būti atsižvelgiama į koordinuotų ES lygmens tiekimo grandinės rizikos vertinimų rezultatus.[[30] ] ENISA „Good Practices for Supply Chain Cybersecurity“ gairės pateikia praktines rekomendacijas TIS2 subjektams, kaip įdiegti tiekėjo atrankos kriterijus, į sutartis įtraukti kibernetinio saugumo reikalavimus, atlikti periodinius tiekėjų vertinimus ir užtikrinti nuolatinį tiekimo grandinės monitoringą.[[71] ] NKSC politikos šablone tiekimo grandinės skirsnis nurodo parengti tiekimo grandinės saugumo valdymo ir tiekėjų atrankos tvarką, sudaryti tiekėjų sąrašą ir sutartis su aiškiais saugumo reikalavimais, apimančiais TIS projektavimą, kūrimą, diegimą, naudojimą, priežiūrą, modernizavimą ir kibernetinio saugumo užtikrinimą, taip pat nustatyti tiekėjų kontrolės ir priežiūros mechanizmus.[[53] ] |

| | |
|---|---|
| Tinklų ir informacinių sistemų įsigijimas, plėtojimas ir priežiūros saugumas, įskaitant spragų valdymą ir atskleidimą | Pagal reikalavimą subjektai turi užtikrinti saugumą per visą informacinės sistemos (IS) gyvavimo ciklą: įsigijimą, projektavimą, kūrimą, diegimą, eksploatavimą ir išėmimą iš eksploatacijos, įskaitant pažeidžiamumų valdymą ir atskleidimą.[[30] ] ENISA techninės įgyvendinimo gairės pabrėžia saugaus plėtojimo, pokyčių ir pataisų valdymo, nuolatinio pažeidžiamumų skenavimo ir koordinuoto pažeidžiamumų atskleidimo (angl. *Coordinated Vulnerabiltiy Disclosure,* CVD) procesų būtinybę, įskaitant suderinimą su ENISA ir ES pažeidžiamumų atskleidimo (angl. *disclosure*) iniciatyvomis.[[32] ] Kibernetinio saugumo reikalavimų apraše (KSRA), paaiškinama, reguliariai vertinti spragas, o visą tinklų informacinės sistemos spragų vertinimą atlikti ne rečiau kaip kas 6 mėnesius.[[54] ] NKSC šablone apibrėžiamas reikalavimo įgyvendinimas formalizuojamas nurodant dokumentavimo būtinumą – TIS saugos valdymo užtikrinimo tvarką, leistinos programinės įrangos sąrašą, pokyčių ir pataisų valdymo tvarką bei spragų valdymo nuostatas ir skenavimo procesus[[53] ] |
| Politikos ir procedūros, skirtos kibernetinio saugumo reikalavimų veiksmingumui įvertinti | Reikalavimas apibrežia politiką ir procedūras, skirtas įvertinti kibernetinio saugumo rizikos valdymo priemonių veiksmingumą, atitinkant nuolatinio tobulinimo principą (*plan–do–check–act*), kuriuo užtikrinama, kad įdiegtos priemonės realiai sumažina riziką.[[30] ] ENISA įgyvendinimo gairėse akcentuojama, kad ši politika turi nustatyti našumo ir rizikos rodiklius (angl. *Key Performance Indicator, Key Risk Indicator*, KPI/KRI), periodiškumą, atsakomybes ir naudoti auditų, testų, pratybų, incidentų analizės rezultatus kaip įrodymus.[[32] ] NKSC šablone numatyta, kad subjekto dokumentacijoje turi būti kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka, atitikties vertinimo ataskaita, neatitikčių šalinimo planas ir kibernetinio saugumo audito ataskaitos, o tai reiškia, kad subjektas privalo ne tik atlikti savęs įvertinimus, bet ir pasitelkti nepriklausomus auditus. [[53] ] Apskritai, ši vertinimo politika užtikrina įrodymų kaupimą ir tampa svarbiu argumentu priežiūros institucijai, jog subjektas laikosi numatytų reikalavimų. |
| Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | Šis reikalavimas apibrežia pagrindines kibernetinės higienos praktikas ir nuolatinio mokymosi principus, ir atskirai įpareigoja valdymo organų narius atlikti kibernetinio saugumo mokymus[[30] ] taip užtikrinant adekvatų rizikų suvokimą. ENISA *„Awareness and Cyber Hygiene“* iniciatyvoje nurodoma. jog efektyvi kibernetinė higiena apima saugų slaptažodžių naudojimą, programinės įrangos atnaujinimą, saugų el. pašto ir naršymo naudojimą, mobiliųjų įrenginių apsaugą, socialinės inžinerijos prevenciją ir pan., o mokymai turi būti reguliarūs, pritaikyti vaidmenims ir matuojami[[72] ] NKSC šablone įvardijama, jog subjektas turi turėti kibernetinės higienos ir mokymų organizavimo tvarką bei mokymų ataskaitas, kuriose fiksuojamos temos ir dalyvių skaičius.[[53] ] NKSC rekomendacijose subjektams papildomai siūloma orientuotis į CIS trijų spalvų kontrolės priemonių metodiką sudarant ir taikant mokymų planą.[[73] ] |
| Kriptografijos ir šifravimo naudojimo politika ir procedūros | Reikalavimas nustato, jog subjektai turi turėti politiką ir procedūras dėl kriptografijos šifravimo naudojimo – tai apima tiek algoritmų, tiek raktų valdymą ir jų atitiktį ES gailojantiems reguliavimams (asmens duomenų apsaugos, el. parašų, elektroninės atpažinties).[[30] ] ENISA nurodo, kad organizacijos turi turėti dokumentuotą kriptografijos politiką, skirti dėmesį |

| | |
|---|---|
| | algoritmų pasirinkimui, raktų generavimui, saugojimui, rotacijai, panaikinimui ir planuoti perėjimą prie kvantui atsparių algoritmų.[[74] ] Taip pat nurodoma, jog dokumentuota kriptografijos politika ir procedūros turi būti suderintos su taikomais teisės aktais ir sertifikavimo schemomis pagal ES kibernetinio saugumo aktą, kuris apibrėžia kibernetinio saugumo sertifikavimo sistemą ICT produktams ir paslaugoms.[[32] ] NKSC politikos šablone tai įvardijama kaip kriptografijos ir šifravimo naudojimo tvarka bei raktų valdymo nuostatos, kuriomis detalizuojama, kur, kokiu stiprumu ir kokiu būdu turi būti šifruojami duomenys bei komunikacijos.[[53] ] |
| Žmogiškųjų išteklių saugumas, prieigos prie tinklų ir informacinių sistemų kontrolės politika ir turto valdymas | Reikalavimas numato, jog subjektai turi užtikrinti darbuotojų prieigos kontrolės principus, t.y. mažiausias būtinas teisių lygis, pareigų atskyrimas, periodinė peržiūra bei valdyti TIS turtą, t.y. inventorizuoti, klasifikuoti, priskirti savininkus.[[30] ] ENISA gairės rekomenduoja taikyti pilną turto ciklo valdymą (nuo įsigijimo iki nurašymo) ir susieti jį su prieigos teisėmis bei žmogiškųjų išteklių procesais (įdarbinimas, pareigų keitimas, išėjimas iš darbo), kad nebūtų „pamestų“ paskyrų ir įrenginių.[[32] ] NKSC politikos šablone kaip priemonės nurodomi fizinės prieigos kontrolę, turto valdymo tvarką, įskaitant TIS turto sąrašą ir techninės įrangos gedimų registraciją.[[53] ] |
| Kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimas, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimas | Reikalavimas nurodo, kad subjektai, kai tikslinga, turi naudoti kelių veiksnių arba nuolatinio tapatumo nustatymo sprendimus, [[30] ] Tai papildoma priemonė prieigos kontrolės užtikrinimui, nes reikalaujama ne tik nustatyti, kas prie ko turi prieigą, bet ir užtikrinti, kad tapatybė būtų patvirtinama patikimais metodais. NKSC politikos šablone reikalaujama reglamentuoti kelių veiksnių tapatumo nustatymo naudojimą, išskiriant privilegijuotas paskyras ir nuotolinę prieigą bei susieti jį su naudotojų, administratorių ir tiekėjų prieigos teisių valdymu. |
| Kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų naudotojų, administratorių, kibernetinio saugumo subjektų tiekėjų, jų subtiekėjų ir kitų ūkio subjektų teisių ir prieigos prie TĮS suteikimo ir valdymo politika | Reikalavimas nacionaliniu lygiu išskiriamas TIS2 direktyvos reikalavimų sąraše ir pabrėžia, jog prieigos valdymas turi apimti ne tik vidinius naudotojus ir administratorius, bet ir tiekėjus, jų subtiekėjus bei kitus ūkio subjektus, turinčius prieigą prie TIS ar duomenų.[[34] ] NKSC politikos šablonas nurodo turėti prieigos valdymo tvarką ir atskirus sąrašus asmenų, turinčių administratoriaus teises, bei reglamentuoti naudotojų, administratorių ir paslaugų tiekėjų prieigos teisių suteikimą, keitimą, atšaukimą, slaptažodžių saugumo reikalavimus ir Kelių veiksnių tapatumo nustatymo (MFA) naudojimą. Tai praktiškai reiškia, kad organizacija privalo aiškiai identifikuoti visus subjektus, turinčius prieigą prie TIS, taikyti mažiausios reikalingos prieigos teisės principus, periodiškai peržiūrėti suteiktas prieigos teises, sutartyse su tiekėjais ir subtiekėjais apibrėžti prieigos sąlygas, prieigos auditavimo ir žurnalų įrašų kaupimo reikalavimus. |
| Kiti atskiriems sektoriams arba atskiroms | Šis reikalavimas numato, kad ES Komisijos arba valstybės lygiu gali būti priimti kiti įstatymai ir aktai, nustatantys techninius ir metodinius reikalavimus konkrečioms subjektų kategorijoms. Pavyzdžiui galiojančiame |

| | |
|---|---|
| kibernetinio saugumo subjektų grupėms taikomi kibernetinio saugumo reikalavimai, nustatytus atsižvelgiant į identifikuotas atskirų sektorių kibernetinio saugumo rizikas | ES Įgyvendinimo reglamente detalizuojamos TIS2 rizikos valdymo priemonės specialiesiems subjektams (pvz. DNS, TLD, debesijos, duomenų centrų, valdomų paslaugų ir kt.)[[31] ] Šiai grupei taikomas tiesioginis reglamento taikymas be pereinamojo laikotarpio. Analogiškai gali būti taikomas DORA finansų sektoriui[[15] ] Praktikoje tai reiškia, kad subjektas, be bendrojo TSI2/KSĮ minimalių priemonių rinkinio, turi tikrinti, ar jo sektoriui netaikomi papildomi techniniai, operaciniai ar sertifikavimo reikalavimai kituose teisės aktuose ir juos integruoti į savo kibernetinio saugumo valdymo sistemą. |

Tęsiant gilesnę reikalavimų analizę buvo parengta reikalavimų ir priemonių lentelė, kuri atlieka ryšio funkciją tarp reikalavimų formuluočių bei įgyvendinimo gairių ir praktinių priemonių organizacijose vertinimo įrankio. Reikalavimai buvo sistemiškai dekonstruoti į konkretų priemonių rinkinį, apibrėžiant, kokios organizacinės ir techninės praktikos turi būti įdiegtos, kad reikalavimas būtų laikomas įgyvendintu, trečiame skyriuje dekonstrukcijos rezultatas panaudojamas kaip vertinimo įrankio klausimų ir įgyvendinimo plano duomenų bazių pagrindas.

Apibendrinant analizę, galima teigti, jog TIS2 pagrindinių kibernetinio saugumo reikalavimai nėra vien tik izoliuotos techninės priemonės, bet tarpusavyje susijęs, visą organizacijos kibernetinio saugumo valdymo ciklą apimantis reguliacinis karkasas. Reikalavimai visapusiškai aprėpia valdymo ir atsakomybių struktūrą, rizikos vertinimą, incidentų valdymą ir veiklos tęstinumą, plėtojimo ir tiekimo grandinės saugumą, žmogiškuosius išteklius, tapatumo nustatymą ir prieigos kontrolę, kriptografiją, taip užtikrinant, kad kibernetinis saugumas būtų integruotas į kasdienius procesus, o ne traktuojamas kaip atskira IT funkcija. Toks sisteminis požiūris leidžia ne tik formaliai vertinti atitiktį reikalavimams, bet ir užtikrinti atsparumą kibernetinėms grėsmėms realiame organizacijos gyvavimo cikle.

### 2.4. TIS2 reikalavimų atitikties vertinimo įrankių analizė

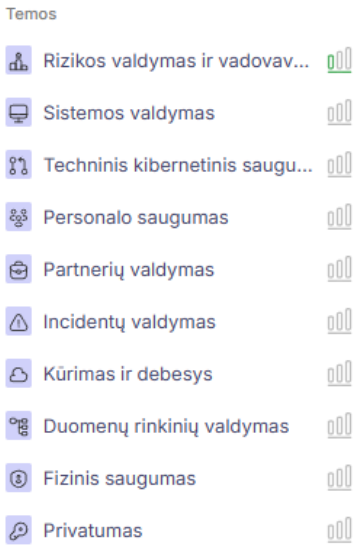
TIS2 direktyvos reikalavimų įgyvendinimas yra sudėtingas, reikalaujantis daug resursų procesas, ir kaip jau buvo minėta įvadinėje darbo dalyje, tai tampa ypatingu iššūkiu organizacijoms, neveikiančioms informacinių technologijų srityje, kurios įprastai neturi vidinių kibernetinio saugumo ekspertų ir/arba sklandžiai organizuoto IT valdymo. Šiame kontekste rinkoje atsiranda įvairių kibernetinio saugumo vertinimui skirtų produktų: trūkumų nustatymo šablonų, IT brandos vertinimo modelių ir integruotų Valdymo, Rizikų ir Atitiktis platformų(angl. *Governance, Risk and Compliance*,

toliau GRC) platformų, kurių tikslas – supaprastinti kibernetinio saugumo reikalavimų interpretavimą ir suteikti struktūruotą būdą užfiksuoti „dabartinę būklę“, nustatyti trūkumus, bei valdyti kelionę link reikalavimų įvykdymo ir atitikties. Šiame poskyryje aptariami tokio pobūdžio įrankiai, analizuojama jų vertė organizacijoms bei jų ribotumai, analizuojant buvo atsižvelgiama pirmiausiai į įrankių gebėjimą palengvinti organizacijų TIS2 atitikties kelionę. Įrankiai buvo sugrupuoti į kelias kategorijas - savianalizės klausimynai, GRC įrankiai ir kibernetinio saugumo gairių leidėjų vertinimo įrankiai.

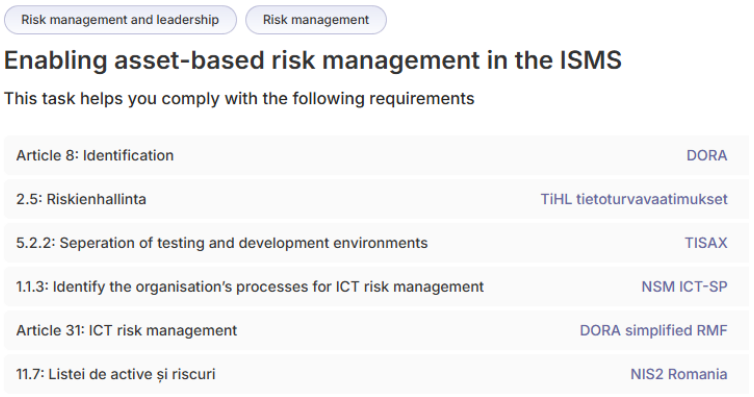
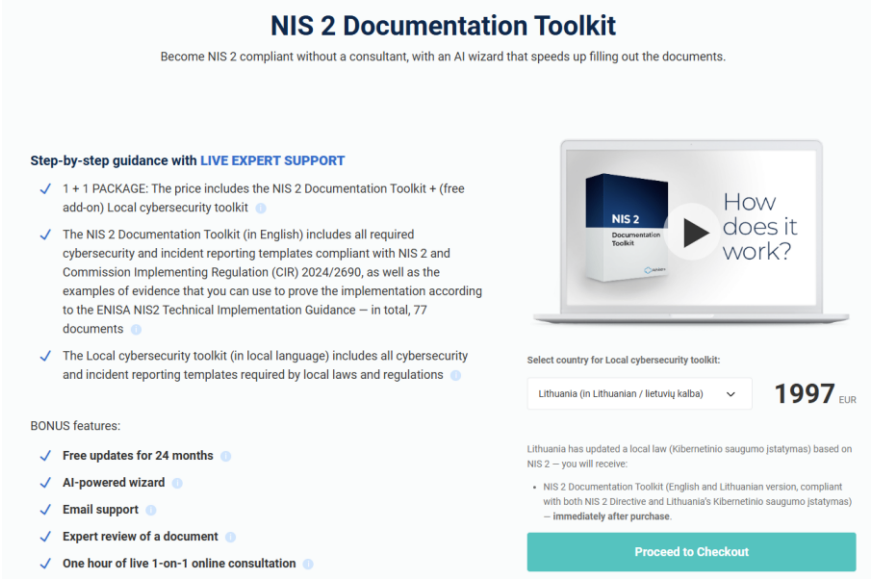
Pirmąją įrankių grupę sudaro internetu pasiekiami savęs įvertinimo klausimynai, orientuoti į greitą TIS2 atitikties spragų identifikavimą. Jie yra nemokami arba siūlo išplėstas funkcijas už papildomą mokestį, klausimynai paremti uždaro tipo klausimais ir apskaičiuoja bendrą atitikties procentą ar brandos lygį pagal TIS2 direktyvos turinį. Savo „savianalizės“ principu šitie įrankiai iš dalies primena šiame darbe rengiamo įrankio prototipą. Žemiau lentelėje analizės metu bandyti ir testuoti įrankiai

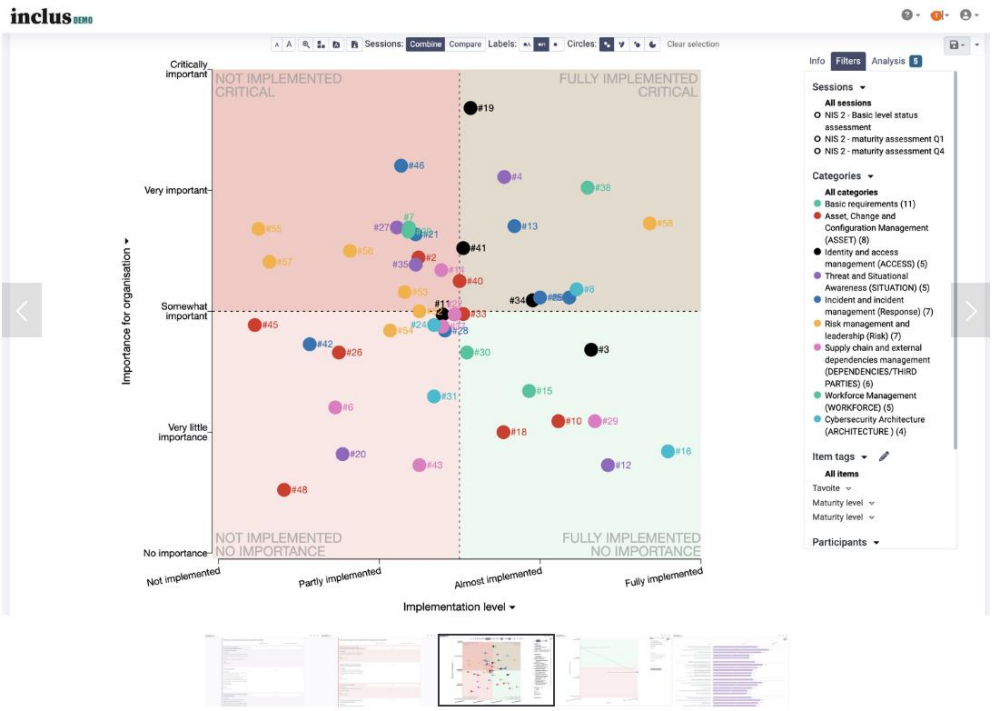
6 lentelė. **TIS2 vertinimo klausimynų palyginimas**

| | |
|---|---|
| „Cyberday“ TIS2 atitikties vertinimas | „Cyberday“ siūlo TIS2 direktyvos atitikties vertinimą, kurio metu atsakoma į 10 temų klausimus. Klausimai formuluojami kaip užduotys, vartotojas turi atsakyti ar užduotis įtraukta į įgyvendinimą ir pasirinkti dabartinė užduoties atlikimo statusą. Suriktus rezultatus „Cyberday“ pateikia kaip ataskaitą ir siūlo įsigyti mokamą produktą, kuris integruojasi į Teams ir tampa savotišku TIS2 atitikties užduočių įgyvendinimo projekto koordinavimo įrankiu.[[58] ] |



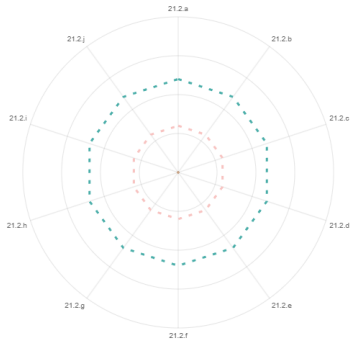

**14 Pav.** „Cyberday“ TIS2 direktyvos atitikties vertinimas.[[58] ]

| | |
|---|---|
| | Tai pat siūlomas svetainėje yra pateiktos TIS2 įgyvendinimo gairės [[59] ], kurios pagrįstos direktyvos straipsniais ir išdėstytais reikalavimais. Gairėse yra veiksmų detalizacija, o veiksmais siejami su su ne tik TIS2 reikalavimais bet ir su kitais svetainėje pristatomais reguliavimais ir standartais – CER, DORA, kt.<br><br>  <br>Risk management and leadership<br>Risk management<br>Enabling asset-based risk management in the ISMS<br>This task helps you comply with the following requirements<br>Article 8: Identification — DORA<br>2.5: Riskienhallinta — TiHL tietoturvavaatimukset<br>5.2.2: Seperation of testing and development environments — TISAX<br>1.1.3: Identify the organisation's processes for ICT risk management — NSM ICT-SP<br>Article 31: ICT risk management — DORA simplified RMF<br>11.7: Listei de active și riscuri — NIS2 Romania<br><br>**15 Pav.** „Cyberday“ rizikų valdymas.[[58] ] |
| „Advisera“ TIS2 atitikties vertinimas | „Advisera“ atitikties vertinimo klausimynas leidžia atsakyti į direktyvos reikalavimų pagrindu suformuluotus 34 klausimus, atsakant į klausimus yra skaičiuojama TIS2 atitikties procentinė išraiška, norint gauti ataskaitą reikia pateikti savo el. paštą.<br><br>„Advisera“ pateikia su TIS2 įgyvendinimu susijusių dokumentų rinkinį, taip pat svetainėje siūloma įsigyti mokamų šablonų ir paslaugų paketą.[[60] ]<br>  <br>NIS 2 Documentation Toolkit<br>Become NIS 2 compliant without a consultant, with an AI wizard that speeds up filling out the documents.<br>Step-by-step guidance with LIVE EXPERT SUPPORT<br>1 + 1 PACKAGE: The price includes the NIS 2 Documentation Toolkit + (free add-on) Local cybersecurity toolkit<br>The NIS 2 Documentation Toolkit (in English) includes all required cybersecurity and incident reporting templates compliant with NIS 2 and Commission Implementing Regulation (CIR) 2024/2690, as well as the examples of evidence that you can use to prove the implementation according to the ENISA NIS2 Technical Implementation Guidance – in total, 77 documents<br>The Local cybersecurity toolkit (in local language) includes all cybersecurity and incident reporting templates required by local laws and regulations<br>BONUS features:<br>Free updates for 24 months<br>AI-powered wizard<br>Email support<br>Expert review of a document<br>One hour of live 1-on-1 online consultation<br>NIS 2<br>Documentation Toolkit<br>How does it work?<br>Select country for Local cybersecurity toolkit:<br>Lithuania (in Lithuanian / lietuvių kalba)<br>1997 EUR<br>Lithuania has updated a local law (Kibernetinio saugumo įstatymas) based on NIS 2 – you will receive:<br>NIS 2 Documentation Toolkit (English and Lithuanian version, compliant with both NIS 2 Directive and Lithuania's Kibernetinio saugumo įstatymas) – immediately after purchase.<br>Proceed to Checkout<br>**16 Pav.** „Advisera“ TIS2 dokumentacija įgyvendinimui [[60] ] |

| | |
|---|---|
| „Inclus“ TIS2 brandos ir trūkumų analizė | „Inclus“ siūlo TSI2 brandos ir spragų analizės šabloną, skirta saugumo specialistams. [[61] ] Iš pateiktos svetainėje demonstracijos matyti jog įrankis siūlo išsamų vizualinį vertinimo reprezentavimą. Šablonas yra mokamas.<br>  <br><br>**17 Pav.** „Inclus“ vertinimo šablonas. [[61] ] |
| „Thales“ TIS2 vertinimo įrankis | „Thales“ savianalizės įrankis, susietas su TIS2 21 straipsnio 2 dalies reikalavimais, leidžia įvertinti organizacijos kibernetinio saugumo priemones ir identifikuoti silpnas vietas bei parengti apžvalginę rezultatų suvestinę. Viso yra 4 temos ir 43 klausimai. [[62] ] Suvestinė vizualizuojama direktyvos 21 str. reikalavimų žemėlapyje |

| NIS2 ARTICLE | 62443-2-1 |
|---|---|
| 21A | ORG1.1; ORG1.2; ORG1.3; ORG1.4; ORG1.5; ORG1.6; ORG2.1; ORG2.2; ORG2.3; ORG2.4 |
| 21B | EVENT1.1; EVENT1.2; EVENT1.3; EVENT1.4; EVENT1.5; EVENT1.6; EVENT1.7; EVENT1.8; EVENT1.9 |
| 21C | EVENT1.1; EVENT1.3; EVENT1.4; EVENT1.5; EVENT1.6; EVENT1.7; EVENT1.8; EVENT1.9; AVAIL1.1; AVAIL1.2; AVAIL1.3; AVAIL2.1; AVAIL2.2; AVAIL2.3; AVAIL2.4; AVAIL2.5 |
| 21D | ORG1.6 |
| 21E | ORG1.1; ORG1.2; ORG1.3; ORG1.4; ORG1.5; ORG1.6; COMP2.1; COMP2.2; COMP2.3; COMP3.1; COMP3.2; COMP3.3; COMP3.4; COMP3.5 |
| 21F | ORG1.1; ORG2.1; ORG2.2; ORG2.3; ORG2.4 |
| 21G | ORG1.1; ORG1.2; ORG1.3; ORG1.4; ORG1.5; ORG1.6; EVENT1.1; EVENT1.3; EVENT1.4; EVENT1.5; EVENT1.6; EVENT1.7; EVENT1.8; EVENT1.9 |
| 21H | DATA1.1; DATA1.2; DATA1.3; DATA1.4; DATA1.5; DATA1.6; DATA1.7; DATA1.8; DATA1.9 |
| 21I | ORG1.1; ORG1.2; ORG1.3; ORG1.4; ORG1.5; ORG1.6; ORG3.1 |
| 21J | DATA1.1; DATA1.2; DATA1.3; DATA1.4; DATA1.5; DATA1.6; DATA1.7; DATA1.8; DATA1.9; USER2.1; USER2.2; USER2.3; USER2.4 |

**18 Pav.** „Thales“ TIS2 vertinimas. [[62] ]

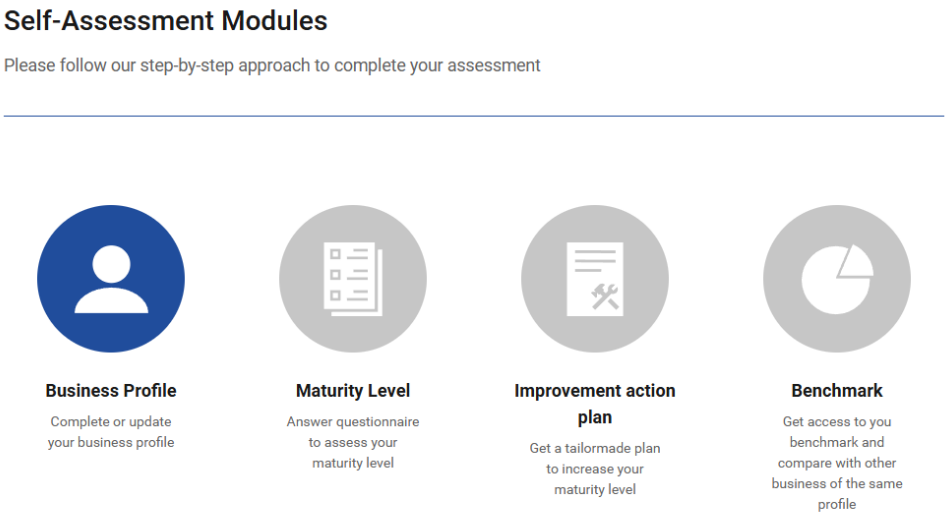

**19 Pav.** „Thales“ TIS2 vizualizacija. [[62] ]

Šie įrankiai pasižymi keliais bendrais bruožais. Pirma, jie naudoja standartizuotas atsakymų/statusų skales, tokiu būdu supaprastindami TIS2 reikalavimų interpretavimą organizacijoms be gilaus teisinio ir techninio pasirengimo. Antra, dauguma jų grindžiami bazine TIS2 21 straipsnio struktūra. Klausimynai veikia kaip pirminis vertinimas, jie leidžia specialistui greitai nustatyti, ar organizacija iš esmės atitinka direktyvos reikalavimų, tačiau nepasiekia tokio detalumo lygmens, kokio reikalautų pilnas auditas ar priežiūros institucijos patikrinimas, taip pat nepateikia praktinių trūkumų šalinimo metodikų. Iš mokamų paketų aprašymų galima daryti jog išplėstos versijos giliau fokusuojasi į teisinius/organizacinius aspektus, bet ne techninius.

Antroji įrankių grupė – komercinės integruotos GRC platformos, kuriuose TIS2 direktyva naudojama kaip vienas iš kelių galimų reguliacinių ir/arba gairių rėmų (kartu su ISO/IEC 27001, DORA, GDPR, kt.). Šios platformos leidžia ne tik atlikti vienkartinę trūkumų analizę, bet ir ištisai valdyti reikalavimų įgyvendinimo būklę, kaupti ir analizuoti rizikų registrą, taikyti kontrolės priemones, atlikti įrodymų (angl. *evidence*) rinkimą ir vykdyti vidaus auditus. Organizacijose GRC funkcionalumai integruojami su IT valdymo įrankiais (toliau ITSM) ir/arba Konfigūracijų valdymo duomenų bazėmis (toliau CMDB) ir rizikų bei atitiktis valdymas siejamas (angl. *relations*) su konkrečiais resursais ir jų konfigūracijomis. Todėl GRC modulis įprastai būna platesnio komercinio produkto dalis, iš žinomų tiekėjų verta paminėti „Service Now“ GRC[[63] ] ir „BMC Remedy“ Control-M [[64] ]. Platformose reguliavimų žemėlapiai susiejamas su kibernetinio saugumo priemonių kategorijomis bei kontrolių rinkiniais, yra pateikiami kontrolių aprašai, nurodomi atsakingi asmenys už kontrolių vykdymą, pateikiami vertinimo rodikliai bei kaupiami įrodymų šaltiniai. Šiuo aspektu GRC įrankiai primena šiame darbe rengiamo prototipo užmanymą ne tik atlikti kibernetinio saugumo vertinimą bet ir kaupti atitikties įrodymus. Apskritai GRC platformų privalumas – tai galimybė centralizuotai valdyti įvairius reguliacinius reikalavimus patogioje vartotojo sąsajoje, susieti IT resursus su kontrolėmis bei priskristi konkrečius atsakingus už kontrolės vykdymą asmenis, kurie dirbs su GRC, gaus įvairius platformos pranešimus apie reikalingus veiksmus ir kt. Tačiau šie GRC funkcionalumai ir patogumai atitinkamai reikalauja didesnių įmonės kaštų, pradedant nuo paties įrankio diegimo ir priežiūros kaštų, baigiant kompleksiniu licencijavimo modeliu, todėl GRC įrankiai iš esmės yra prieinami didelėms organizacijoms, tokiame kontekste mažesnėms įmonėms labiau patrauklūs sprendimai – baziniai savianalizės įrankiai.

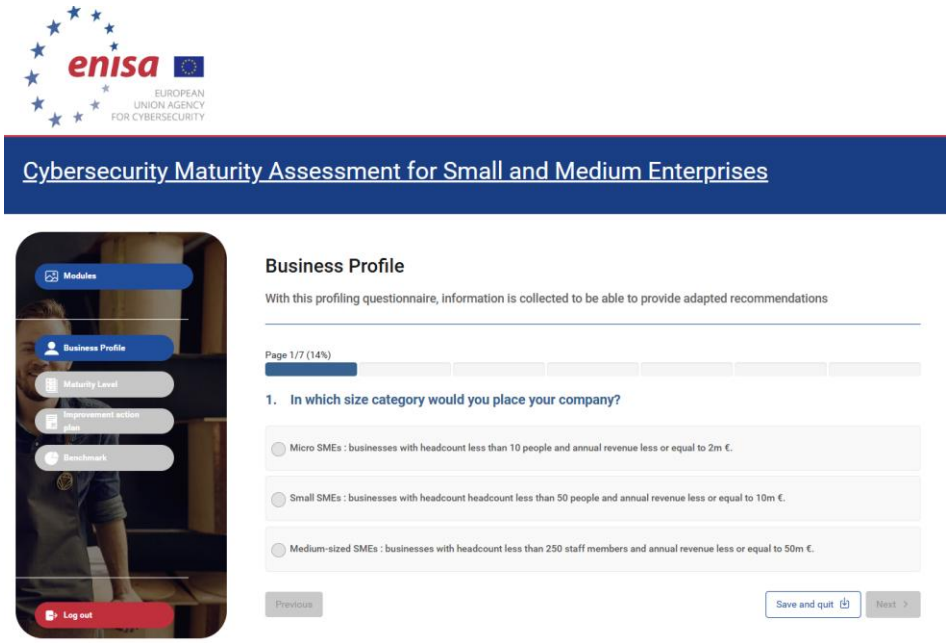
Atskirai verta paminėti projektus, parengtus institucijų. Nors jie nėra pozicionuojami kaip specialiai TIS2 atitiktį vertinimui sukurti įrankiai, savo plačia kibernetinio saugumo temos apimtimi jie gali būti pagrįstai naudojami kaip pagrindas direktyvos reikalavimų įgyvendinimui.

ENISA parengtas Kibernetinio saugumo brandos vertinimas mažoms ir vidutinėms organizacijoms (angl. *Cybersecurity Maturity Assessment for Small and Medium Enterprises*) įrankis leidžia apibrėžti organizacijos profilį, įsivertinti brandą, suformuoti priemonių planą bei palyginti organizacijos brandą su atitikties grindimis atitinkamoje industrijoje[[65] ]

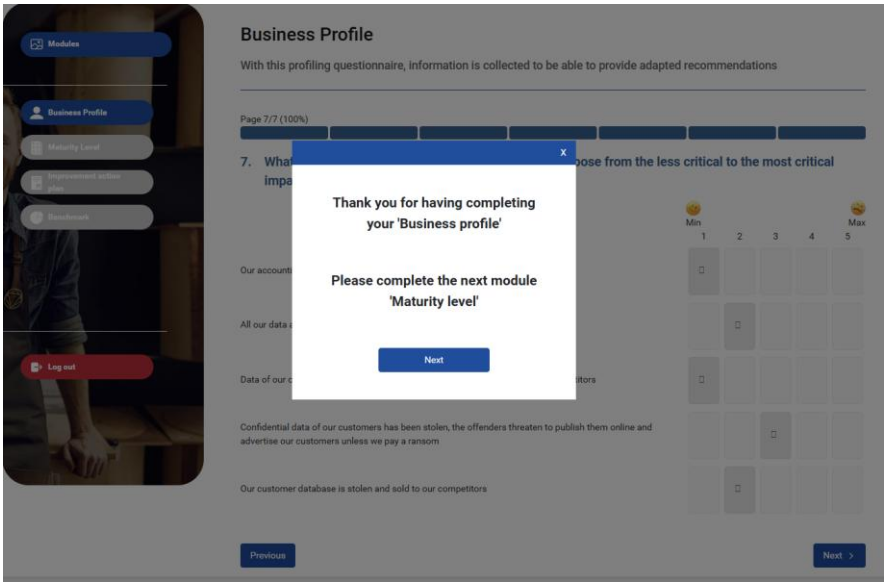



**20 Pav.** ENISA KS brandos vertinimo įrankis. (I) [[65] ]

Testavimo metu įrankis leido išbandyti profilio dalį, kurioje gana lakoniškai atsakomą į 7 klausimus. Kiti įrankio komponentai testavimo metu neveikė, todėl detaliau jų patikrinti nepavyko.




**21 Pav.** ENISA KS brandos vertinimo įrankis. (II) [[65] ]




**22 Pav.** ENISA KS brandos vertinimo įrankis. (III) [[65] ]

Bet kuriuo atveju svarbu pabrėžti kad rinkoje egzistuoja ne tik komerciniai produktai bet ir vystomi institucijų.

Specifinė įrankių grupė – standartų siejimo (angl. *mapping*) su TIS2 reikalavimais įrankiai. ISO/IEC 27001:2022 yra plačiausiai taikomas informacijos saugumo valdymo sistemos standartas, todėl ne nuostabu, jog yra didelis poreikis TIS2 atitiktį susieti su organizacijose jau egzistuojančiomis ISO 27001 praktikomis, suprantama, jeigu ISVS buvo yra įdiegta. Rinkoje esantys produktai sprendžia šį poreikį siūlant žemėlapius, siejančius TIS2 straipsniuose nurodytus saugumo valdymo priemones su ISO 27001 A priedo kontrolėmis.

NIS2 requirements mapped to ISO 27001 controls (click to expand)

| NIS2 requirement | | ISO standard 27001:2022 |
|---|---|---|
| Point No | Title | Corresponding clause and/or Annex A control |
| 1.1 | Policy on the security of network and information systems | Clause 5.2 > Information Security Policy<br>Annex A 5.1 > Policies for Information Security<br>Annex A 5.36 > Compliance with Policies, Rules, and Standards for Information Security<br>Annex 5.4 > Management Responsibilities<br>Annex 9.3 > Management Review |
| 1.2 | Roles, responsibilities, and authorities | Clause 5.3 > Roles and Responsibilities<br>Annex A 5.2 > Information Security Roles & Responsibilities<br>Annex A 5.4 > Management Responsibilities |
| 2.1 | Risk management framework | Clause 6.1 > Actions to Address Risks & Opportunities<br>Clause 6.1.2 > Information Security Risk Assessment<br>Clause 6.1.3 > Information Security Risk Treatment |

**23 Pav.** Dataguard TIS2 ir ISO 27001 siejimas. [[66] ]

| NIS2 Measures | ISO/IEC 27001 | |
|---|---|---|
| **Article 20: Governance** | | |
| | **Annex A** | |
| | A.5.1 | Policies for information security |
| | A.5.31 | Legal, statutory, regulatory and contractual requirements |
| | A.5.34 | Privacy and protection of personal Identifiable information (PII) |
| | A.5.35 | Independent review of information security |
| | A.5.36 | Compliance with policies, rules and standards for information security |
| | A.6.3 | Information security awareness, education and training |
| **Article 21: Cyber security risk management measures** | | |
| **(A)** Policies on risk analysis and information system security | 5.2 | Information security policy |
| | 6.1.2 | Information security risk assessment process |
| | 6.1.3 | Information security risk treatment process |
| | 8.2 | Information security risk assessment |
| | 8.3 | Information security risk treatment |
| | **Annex A** | |
| | A.5.1 | Policies for information security |
| **(B)** Incident handling | **Annex A** | |
| | A.5.24 | Information security incident management planning and preparation |
| | A.5.25 | Assessment and decision on information security events |
| | A.5.26 | Response to information security incidents |
| | A.5.27 | Learning from information security incidents |
| | A.5.28 | Collection of evidence |
| | A.6.8 | Information security event reporting |
| | A.8.16 | Monitoring activities |

**24 Pav.** BSI TIS2 ir ISO27001 siejimo įrankis. [[67] ]

Tokios susiejimo priemonės padeda ISO sertifikuotoms organizacijoms aiškiai matyti, kurios jau veikiančios kontrolės gali būti panaudotos TIS2 atitikties įrodymui, taip taupant kaštus. Priežiūros institucijoms tai gali būti taip pat naudinga vertinant TIS2 atitiktį, tai gali  kiek ISO 27001 sertifikatas „padengia“ minimalių atitikties reikalavimų, nors tai ir nepakeistų numatytų priežiūros procedūrų. Analogiškai, egzistuoja ir NIST CSF 2.0 susiejimo su TIS2 žemėlapiai, pavyzdžiui kibernetinio saugumo programinės įrangos gamintojas „Trescudo“ pateikia savo susiejimo žemėlapį

**NIS2 - NIST CSF 2.0 Mapping Sheet**

Quick reference for aligning EU NIS2 Directive requirements with the NIST Cybersecurity Framework 2.0 functions and categories.

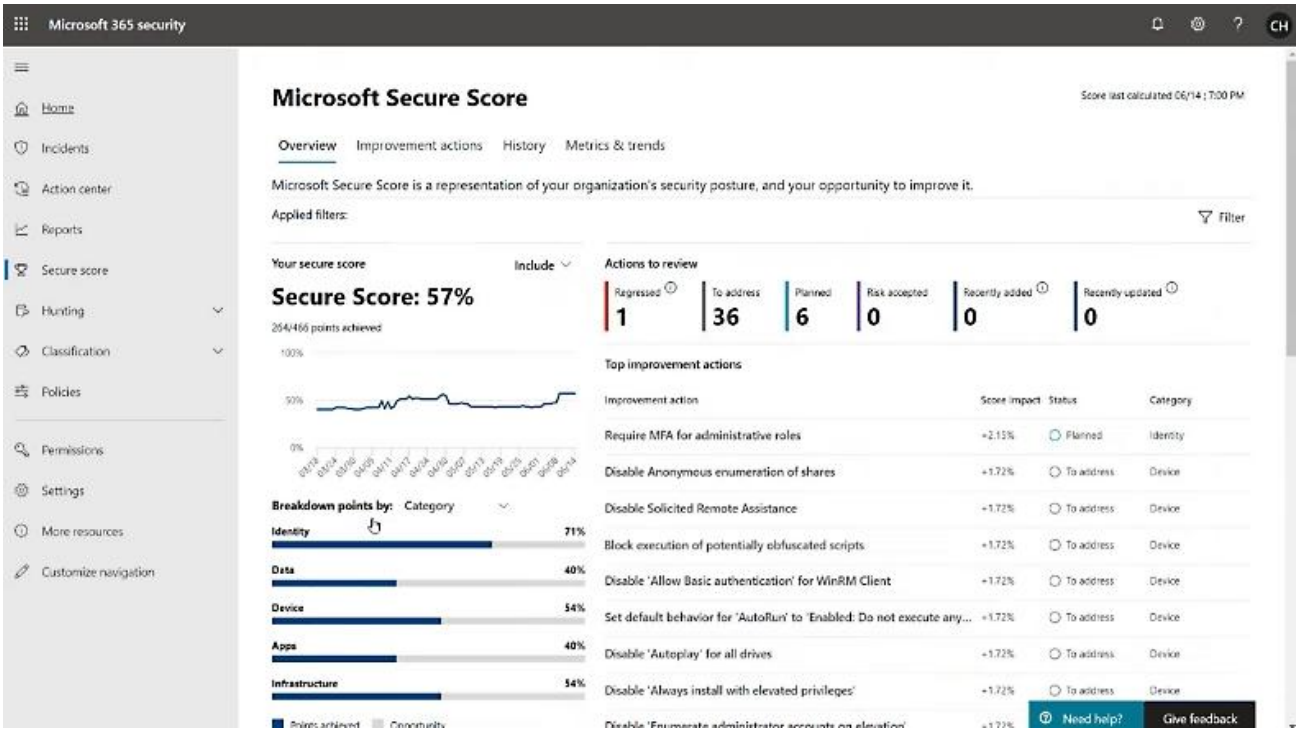
| NIS2 Requirement | NIST CSF 2.0 Function / Category |
|---|---|
| NIS2 Article 21 §1 a-b - Governance & Cyber-risk policy | GOV-PR (Govern) |
| NIS2 Article 21 §1 c - Incident handling | RS-IM (Respond: Incident Management) |
| NIS2 Article 21 §1 d - Business continuity & crisis mgmt | RC-CO (Recover: Continuity) |
| NIS2 Article 21 §1 e - Supply-chain security | ID-SC (Identify: Supply-Chain) |
| NIS2 Article 21 §1 f - Testing & auditing | GV-RV (Govern: Review) / DE-AE (Detect: Anomalies & Events) |
| NIS2 Article 23-24 - Incident notification (24 h / 72 h) | RS-CO (Respond: Communications) |
| NIS2 Article 22 - Basic cyber-hygiene & training | PR-AT (Protect: Awareness & Training) |
| NIS2 Article 25 - Vulnerability disclosure | ID-AM (Identify: Asset Management) / DE-AE |

*(c) 2025 Trescudo Cybersecurity - For guidance only.*

**25 Pav.** „Trescudo“ TIS2 ir CSF2.0 siejimas. [[68] ]

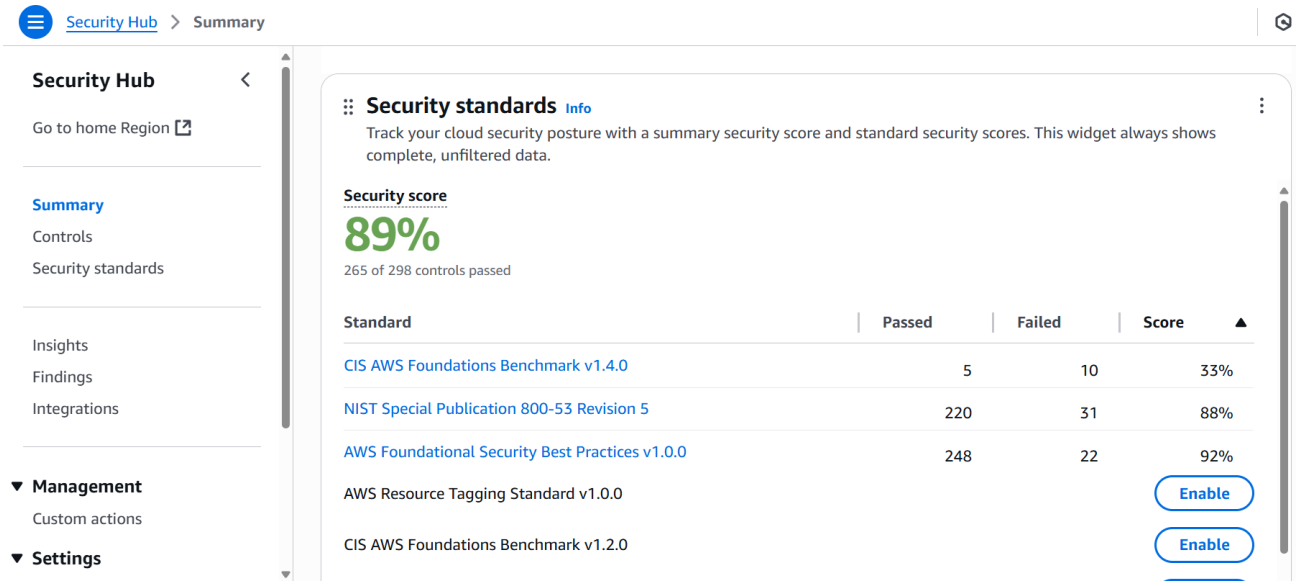
Verta paminėti „netiesioginio“ TIS2 atitikties vertinimo priemonių grupė – stambių programinės įrangos ir debesijos paslaugų gamintojų siūlomos „saugumo skalės“ ir atitikties valdymo „centrai“, analyzės metu buvo susipažinta su dvejais produktais – Microsoft *„Secure Score“* ir Amazon *„AWS Security Hub“*.

*„Secure Score“* pateikia skaitlinį organizacijos „Microsoft 365“ ir „Azure“ aplinkos saugumo būklės įvertį, apskaičiuotą pagal konfigūracijų, naudotojų elgsenos ir kitų saugumo parametrų visumą, aukštesnis balas reiškia didesnį rekomenduojamų saugumo priemonių įgyvendinimo lygį [[75] ] tačiau pats balas nėra tiesioginis pažeidimo tikimybės matavimas, apžvalgose pabrėžiama, kad „Secure Score“ vis dažniau siejamas su atitikties pasirengimu ir naudojamas kaip praktinis rodiklis organizacijoms, siekiančioms atitikti tokius standartus saugumo standartus (pvz. ISO/IEC 27001, NIST CSF), tačiau kartu įspėjama, kad per didelis pasitikėjimas šiuo rodikliu gali klaidinti, jei jis interpretuojamas kaip absoliutus kibernetinės rizikos lygio.




**26 Pav.** Microsoft „Secure Score“. Microsoft aplinkos ekranvaizdis.

AWS *„Security Hub“* aprepia saugumo įžvalgas AWS aplinkoje ir automatiškai tikrina išteklius pagal pasirinktus standartus (pvz., CIS AWS Foundations Benchmark, NIST SP 800-53, NIST SP 800-171, PCI DSS) rengdamas ataskaitas apie neatitikimus ir rekomendacijas.[[76] ] https://docs.aws.amazon.com/securityhub/latest/userguide/standards-reference.html?utm_source=chatgpt.com




**27 pav.** AWS "Security Hub ". AWS aplinkos ekranvaizdis.

Teisinių reguliavimų kontekste, šių gamintojų įrankių privalumu laikytina yra tai, jog jie užtikrina nuolatinę, automatizuotą techninių kontrolės priemonių stebėseną ir žurnalų kaupimą, taip mažinant atitikties patikros naštą ir sudarydami sąlygas nuolatinei priežiūrai [[77] ] Suprantamas ribotumas – tokie įrankiai iš esmės apima tik konkretaus tiekėjo ekosistemą (kaip šiuose pavyzdžiuose - Microsoft ar AWS), ir to nepakanka mišrioms organizacijų aplinkoms, taip pat jie orientuoti į techninių konfigūracijų ir kontrolės priemonių vertinimą, ir suprantamai nepaliečia organizacinių aspektų. Todėl tokius įrankius verta integruoti su specializuota auditavimo platforma, siekiant automatizuotai rinkti techninės atitikties įrodymus auditavimo platformoje.

Papildomai verta paminėti saugumo procesų automatizavimo ir koordinavimo (angl. Security *Orchestration, Automation and Response,* SOAR), bei išplėstinio grėsmių aptikimo ir reagavimo (angl. *Extended Detection and Response*, XDR) produktus. Šių įrankių-platformų funkcionalumas plečiasi ir tam tikra prasme organizacijose virsta vidinių rizikos ir atitikties vertinimo įrankiu. Šiuolaikinės SOAR platformos (pvz., *Splunk SOAR*, *Cortex XSOAR*) leidžia ne tik automatizuoti incidentų reagavimo ir valdymo procesus, bet ir kaupti bei agreguoti rizikos signalus į centralizuotas duomenų bazes, kuriuose kiekvienam įvykiui ar subjektui gali būti priskiriami dinamiškai skaičiuojami rizikos balai siejami su atitinkamais saugumo kontrolės reikalavimais [[78] ] XDR gamintojai papildomai integruoja atitikties šablonus ir automatizuotas ataskaitas pvz. *WatchGuard ThreatSync* su automatizuotomis ISO 27001 ir NIST ataskaitomis [[79] ] taip leisdami saugumo operacijų centro (angl. *Security Operations Center*, SOC) komandai generuoti atitikties ataskaitas tiesiai iš saugumo įvykių duomenų bazės, „realiuoju laiku“. Analogiškai kaip ir *Microsoft* ir *AWS* balų sistemos, šie produktai atspindi techninių priemonių veikimą ir atitikties reguliavimui vertinimo kontekste susiduria su tais pačiais ribotumais bei panaudojimo scenarijais – teikti įrodymus pagal specifines reikalavimų įgyvendinimo technines priemones.

Atitikties vertinimo įrankių ir metodikų pasiūla yra nevienalytė ir sparčiai auganti, iš vienos pusės atsiranda paprasti TIS2 atitikties savianalizės įrankiai, iš kitos pusės – direktyvos reikalavimai integruojami į kompleksinius GRC integruotų platformų sprendimus. Greta jų – žemėlapio tipo įrankiai-dokumentai, skirti organizacijoms, jau praktikuojančioms kibernetinio saugumo standartus. Svarbu pažymėti, kad kibernetinio saugumo brandos vertinimo metodiką ES lygmeniu siūlo ir ENISA, taip sukurdama „oficialų“ pavyzdį gamintojams. Programinės įrangos gamintojų kuriami kibernetinio saugumo vertinimo įrankiai papildo šią ekosistemą efektyvesnio saugumo valdymo ir techninių priemonių atitikties įrodymų kaupimo sprendimais.

Vis dėlto atlikta analizė atskleidė ir esminius nagrinėtų priemonių ribotumus, kurie pagrindžia poreikį kitokio įrankio kūrimui. Paprasti savianalizės klausimynai apsiriboja bendra atitikties procentine išraiška ar „brandos lygiu“, nepateikdami pakankamai detalios trūkumų analizės, prioritetizavimo ir realistiško įgyvendinimo plano, be to, neretai veikia kaip kvietimas į mokamus konsultacinius ar šablonų paketus. Kompleksinės GRC platformos, priešingai, yra funkcionaliai kompleksinės ir leidžia detaliai ir efektyviai vertinti bei valdyti organizacijos atitikties situaciją, tačiau reikalauja didelių investicijų: licencijavimo, diegimo ir palaikymo kaštų, ilgalaikių vidinių resursų ir pakankamos organizacijos esamos brandos, todėl mažesnėms ir vidutinėms organizacijoms jos dažnai nėra prieinamos praktiškai, „čia ir dabar“. Standartų siejimo su TIS2 priemonės yra orientuotos į organizacijas, kurios jau yra įsidiegusios ISO/IEC 27001 ir (arba) NIST CSF, ir pan. todėl analogiškai kaip ir GRC įrankiai, neapimtų organizacijų, kurių kibernetinio saugumo valdymo sistema dar tik formuojama. Gamintojų vertinimo priemonės tokios kaip nagrinėtos „Secure Score“, „AWS Security Hub“ daugiausia atspindi techninių konfigūracijų būklę konkrečioje tiekėjo ekosistemoje ir iš esmės neapima organizacinių procesų ir reguliacinės atitikties bei valdymo aspektų. Tuo tarpu SOAR ar XDR klasės produktai iš esmės gali tapti tam tikrų (incidentų valdymas, pažeidžiamumų valdymas) TIS2 reikalavimų priemonių įgyvendinimo būdais, bet ne holistiniu atitikties vertinimo sprendimu.. Tokiame kontekste šiame darbe projektuojamas įrankis gali tapti instrumentu, padedančiu užpildyti tarpą tarp paprastų klausimynų ir sudėtingų, didelėms organizacijoms skirtų GRC platformų, kartu numatant ir integraciją su trečiųjų šalių techninės atitikties įrodymų tiekėjais, pvz. minėtais infrastruktūros saugumo kontrolės valdymo platformomis, SOAR, XDR sistemomis ir pan.

### 2.5. Apibendrinimas

TIS 2 direktyvos reikalavimų analizė parodė, kad direktyvos įgyvendinimas yra kompleksinis ir nuolatinis procesas, reikalaujantis integruotų ir aiškiai apibrėžtų valdymo, organizacinių ir techninių kibernetinį saugumą užtikrinančių priemonių. Reikalavimų įgyvendinimas veikia proporcingumo principu pagrįstu rizikų ir saugumo valdymo modeliu, kuris apima strateginį valdymo organų įsitraukimą, nuolatinį rizikų vertinimą, incidentų valdymo ciklą, tiekimo grandinės saugumą ir veiklos tęstinumo planavimą. ENISA rengiamose ataskaitose ir gairėse sistemingai išskiriamos pagrindinės grėsmių tendencijos, sektorių pažeidžiamumai ir praktinės rekomendacijos, todėl jos tampa svarbia orientacine priemone valstybėms narėms ir kibernetinio saugumo subjektams praktiškai interpretuoti ir taikyti TIS 2 reikalavimus nacionaliniu bei organizaciniu lygmeniu. Lietuvos Respublikos kibernetinio saugumo įstatymo paskutinė redakcija, priimta 2024 m. spalio 18 d., perkelia TIS 2 direktyvos struktūrą ir logiką į nacionalinę teisinę sistemą, įstatymas ne tik suderina pagrindines

sąvokas, subjektų kategorijas ir pareigų apimtį su ES direktyvos nuostatomis, bet ir apibrėžia nacionalinę kibernetinio saugumo valdymo ir priežiūros principus, t.y. nustato kompetentingas priežiūros institucijas, jų įgaliojimus, koordinavimo mechanizmus, priežiūros priemones ir sankcijų taikymo tvarką. Kitas žodžiais TIS 2 direktyvos reikalavimai yra ne tik perkeliami, bet ir adaptuojami prie nacionalinio konteksto, sukonkretinant atskaitomybės mechanizmus.

Svarbu pabrėžti, jog kibernetinio saugumo subjekto identifikavimo metodikos, taip pat rekomendacijų bei gairių analizė suteikė teorinį pagrindą projektuojamo atitikties vertinimo įrankio turiniui ir veikimo logikai. Taip pat projektui buvo svarbi rinkoje esančių įrankių analizė, kuri parodė, kad egzistuoja tiek komercinių, tiek viešų (pvz., ENISA) sprendimų, kurie padeda organizacijoms įsivertinti savo kibernetinio saugumo brandą bei TIS 2 atitiktį. Atitikties vertinimo skirtingų įrankių metodikos pasirodė esančios nevienalytės: nuo paprastų savianalizės klausimynų, dažniausiai pateikiančių tik bendriausias rekomendacijas, iki funkcionaliai sudėtingų GRC platformų, reikalaujančių didelių investicijų ir brandžios organizacijos valdymo praktikos, taip pat didžiųjų tiekėjų techninių konfigūracijų vertinimo įrankių, orientuotų į jau veikiančias saugumo valdymo sistemas, ir įrankių, skirtų organizacijose jau įdiegtų kibernetinio saugumo standartų siejimui su TIS2. Šių įrankių analizė atskleidė, kad mažesnėms ir vidutinėms organizacijoms, tik pradedančioms TIS2 atitikties kelią ir neturinčioms išvystytos kibernetinio saugumo valdymo sistemos, trūksta praktiško, rizika ir proporcingumu grįsto, bet kartu ne ekspertams suprantamo vertinimo instrumento. Būtent šią atitikties vertinimo metodologinę „spragą“ siekiama užpildyti šiame darbe projektuojamu adaptyviu TIS 2 atitikties vertinimo įrankiu, o šitame skyriuje atlikta teorinė ir praktinė analizė ne tik suformavo TIS 2 reikalavimų interpretavimo ir taikymo kontekstą, bet ir pagrindė patį poreikį alternatyviam vertinimo požiūriui, kuris organizacijoms turėtų padėti ne tik įsivertinti jų kibernetinio saugumo būklę pagal TIS2 reikalavimus, bet ir gauti struktūruotas, identifikuotų trūkumų šalinimo veiksmų rekomendacijas.

# 3. TIS2 direktyvos atitikties vertinimo įrankio projektavimas

Skyriaus tikslas yra apjungti teorinį pagrindą ir technologines priemones, kurie kartu užtikrintų, kad projektuojamas produktas būtų metodologiškai pagrįstu, funkcionalus ir atitiktų pradinį projekto užmanymą bei formuluojamų reikalavimų. Produkto projektavimas buvo grindžiamas antrame skyriuje identifikuotais TIS2 direktyvos principais, leidžiančiais sukurti holistinį kibernetinio saugumo vertinimo modelį, kuris apimtų visus aspektus – nuo įmonės personalo iki techninių reikalavimų ir jų įgyvendinimo. Projekto tikslas – parengti mažiausią gyvybingą produktą, kuris, remdamasis Lietuvos Respublikos kibernetinio saugumo įstatymo paskutiniąja redakcija su įtrauktomis TIS2 direktyvos nuostatomis, atliktų organizacijos kibernetinio saugumo reikalavimų atitikimo vertinimą, bei, priklausomai nuo pateiktos informacijos, suformuotų vertinimo rezultatus – nustatytus trūkumus, bendrąsias rekomendacijas bei diegimo planus bei būdus trūkumams šalinti.

## 3.1. TIS2 atitikties vertinimo įrankio funkcinių ir nefunkcinių reikalavimų formulavimas

Reikalavimų formulavimas paremtas reikalavimų inžinerijos metodologija, kuri užtikrina sistemingą ir išsamų požiūrį į programinės įrangos projektavimą. Šis procesas apima ne tik funkcinių galimybių apibrėžimą, bet ir nefunkcinių charakteristikų nustatymą[[81] ], kokybės atributų formalizavimą bei priėmimo kriterijų apibrėžimą. Taikyta reikalavimų formulavimo metodologija integruoja IEEE 830 standarto reikalavimų rengimo principus[[82] ] su „SMART“ – „Konkretus, Išmatuojamas, Pasiekiamas, Reikšmingas, Apribotas laike“ (angl. *Specific, Measurable, Achievable, Relevant, Time-bound*, SMART) [[83] ] kriterijais, kartu užtikrinant aiškų įgyvendinimo ir testavimo procesą.

Remiantis minėta metodologija buvo paruošta 20 funkcinių reikalavimų (FR-01 iki FR-20) kuriuos galima suskirstyti į 5 kategorijas, apimančias visapusišką TIS2 atitikties vertinimo programinio produkto funkcionalumą:

1) Autentifikacijos ir autorizacijos modulio reikalavimai (FR-01, FR-02) palaikyti multiorganizacinę prieigą ir keturis vartotojų tipus – Produkto tiekėjo organizacija - Administratorius, Auditoriaus organizacija - Auditorius, Kliento organizacija - Redaguotojas ir Skaitytojas.
2) Vertinimo proceso reikalavimai (FR-03 iki FR-08) – suformuluoja esminį sistemos funkcionalumą - kritiškumo nustatymo metodika ir adaptyvų klausimyną. Reikalavimai užtikrina kad skirtingo dydžio organizacijos yra vertinamos pagal atitinkama įstatyme numatytų TIS2 reikalavimų apimtį.
3) Rezultatų apdorojimo reikalavimai (FR-09 iki FR-11) apima pateiktos informacijos vertinimo matematinį algoritmą ir trūkumų šalinimo planą su detaliais veiksmais bei žingsniai ir susijusiais aprašymais.

4) Duomenų valdymo reikalavimai (FR-12 iki FR-15) skirti užtikrinti duomenų saugojimą, atliktų vertinimų versijų valdymą ir informacijos eksporto funkcionalumą.
5) Įrodymų valdymo reikalavimai (FR-18 iki FR-20) aprašo sistemos dalį, kuri realizuoja rankinį atitikties įrodymų pateikimą ir taip pat automatizuotą duomenų surinkimą iš SIEM, GRC sprendimų ir/arba debesų paslaugų teikėjų, kitų saugumo informaciją disponuojančių programinių įrankių.

7 lentelė. **Funkcinių reikalavimų sąrašas.**

| ID | Funkcinis reikalavimas | Priklauso mybė nuo kitų reikalavimų | Detalus aprašymas | Priėmimo kriterijai |
|---|---|---|---|---|
| FR-01 | Naudotojų prisijungimas | FR-16 | Sistema turi leisti naudotojams prisijungti su naudotojo vardu ir slaptažodžiu | 1. Sistema priima 4 testinius vartotojus (superadmin, auditorius, editor, readonly)<br>2. Neteisingi duomenys rodo klaidos pranešimą<br>3. Sėkmingas prisijungimas nukreipia į pagrindinį puslapį \| |
| FR-02 | Naudotojų atsijungimas | FR-01 | Prisijungęs naudotojas gali atsijungti iš sistemos | 1. Atsijungimas grąžina į prisijungimo puslapį<br>2. Sesijos duomenys ištrinami |
| FR-03 | Įmonės kritiškumo nustatymo formos pildymas | FR-01 | Sistema turi leisti įvertinti įmonės veiklos kritiškumą | 1. Forma turi 3 laukus: sektorius, darbuotojų skaičius, kritinė inrastruktūra<br>2. Pasirinkimas sektorius iš IT/Komunikacijos, Energetika, Sveikata, Kita; Darbuotojų skaičius: skaitinis laukas (min. 1); Kritinė infrastruktūra: Taip/Ne pasirinkimas<br>3. Visi laukai privalomi |
| FR-05 | Klausimų blokų navigacija | FR-03 | Sistema turi leisti naršyti tarp teminių blokų | 1. Naršymas tarp teminių klausimų blokų<br>2. Teminių blokų klausimų kiekis priklauso nuo įmonės kritiškumo atsakymų supildymo<br>3. Galimybė bet kada pereiti prie bet kurio bloko |
| FR-06 | Atsakymų į klausimus sistema | FR-05 | Sistema turi leisti atsakyti į klausimus | 1. 5 atsakymo variantai: TAIP, NE, IŠ DALIES, NEŽINAU, PRALEISTI |

| | | | | |
|---|---|---|---|---|
| | | | | 2. Klausimų paaiškinimų rodymas<br>3. Automatinis perėjimas prie kito klausimo atsakant<br>4. Automatinis atsakymo užsikaitymas kaip “praleista” jeigu į klausimą nebuvo atsakyta ir užbaigtas formos pildymas<br>5. Bet kuriuo metu turi būti galima pateikti atsakymus rezultatų skaičiavimui, net neatsakius į visus klausimus |
| FR-07 | Klausimų priklausomybių valdymas | FR-06 | Sistema turi automatiškai valdyti klausimų priklausomybes | 1. Jei atsakoma "NE", priklausantys klausimai automatiškai pažymimi "NE" ir jie praleidžiami<br>2. Turi būti galima sugrįžti į automatiškai praleistus klausimus |
| FR-08 | Pildymo progreso atvaizdavimas | FR-06 | Sistema turi rodyti bendrą pildymo progresą | 1. Turi būti vizualus atsakytų klausimų bloke progreso skaičiavimas (atsakyta/viso)<br>2. Bendras progresas: visi atsakymai/visi klausimai |
| FR-09 | Rezultatų apdorojimas – skaičiavimas | FR-06 | Sistema turi apdoroti ir rodyti vertinimo rezultatus | 1. Bendras atitikties matematinis rezultatas (visi TAIP + visi IŠ DALIESx0.5) / viso klausimų × 100%<br>2. Sričių (blokų) rezultatai<br>3. Atsakymų statistika (TAIP, IŠ DALIES, NE, NEŽINAU/PRALEISTI)<br>4. Rezultatų grafinė vizualizacija |
| FR-11 | Diegimo plano ruošimas ir atvaizdavimas | FR-09 | Sistema turi paruošti ir atvaizduoti detalų diegimo planą | 1. Diegimo veiksmai ruošiami pagal atsakymus nevykdytoms priemonėms<br>2. Diegimo žingsniai turi 3 prioriteto lygius: KRITINIS, AUKŠTAS, VIDUTINIS<br>3. Diegimo veiksmai detalizuojami žingsniais |
| FR-12 | Duomenų Eksportavimas | FR-09, FR-10, FR-11 | Sistema turi leisti eksportuoti rezultatus į PDF | 1. PDF turi atvaizduoti pilnus vertinimo rezultatus: Atsakymai, Rekomendacijų sąrašą, Diegimo planą |

| | | | | |
|---|---|---|---|---|
| FR-13 | Paskutinio vertinimo tęsimas | FR-06 | Sistema turi leisti tęsti paskutinį vertinimą | 1. Prisijungus galima pasirinkti paskutinį vertinimą tęsti darbą su paskutinio vertinimo rezultatais<br>2. Vertinimo rezultatuose galima pasirinkti „Papildyti vertinimą“ ir pakeisti jau atsakytų klausimų atsakymus<br>3. Pateikus papildytą vertinimą yra sukuriama naują vertinimo versiją |
| FR-14 | Klausimyno pildymas iš naujo | FR-09 | Sistema turi leisti pradėti vertinimą iš naujo | 1. Pateikus atsakymus galima pasirinnkti „Pradėti iš naujo“ ir sugrįžti į kritiškumo vertinimo formą |
| FR-15 | Vertinimų istorijos valdymas | FR-09, FR-10, FR-11 | Sistema turi leisti peržiūrėti visus atliktus vertinimus | 1. Vertinimų istorijos atvaizdavimas pateikia chronologinį vertinimų sąrašą<br>2. Pasirinkus vertinimą turi atvaizduoti pilnus vertinimo rezultatus: Atsakymai, Rekomendacijų sąrašą, Diegimo planą<br>3. Galimas PDF eksportas iš istorijos |
| FR-16 | Prieiga pagal roles | Nėra | Sistema turi valdyti prieigą pagal skirtingas vartotojų roles | 1. Sistema palaiko 4 vartotojų roles: SuperAdmin, Auditorius, CustomerEditor, CustomerReadonly<br>2. Skirtingi meniu ir teisės pagal role:<br>Organizacijų valdymas (Sistemos administratorius)<br>Organizacijos vartotojų valdymas ir vertinimo pildymas (Organizacijos Redaguotojas) \|<br>Savo organizacijos rezultatų peržiūra (Organizacijos Skaitytojas)<br>Visų organizacijų rezultatų peržiūra (Auditorius) |

| | | | | |
|---|---|---|---|---|
| FR-17 | Organizacijų atskyrimas | Nėra | Sistema turi atskirti vartotojų organizacijas ir jų naudotojus | 1. Trijų tipų organizacijos:<br>1) Klausimyno tiekėjo administratorių organizacija<br>2) Organizacija atliekanti vertinimą<br>3) Auditorių organizacija |
| FR-18 | Duomenų saugojimas | Nėra | Sistema turi išsaugoti vertinimo duomenis | 1. Vertinimų istorijos išsaugojimas<br>2. Vartotojo būsenos išsaugojimas<br>3. Organizacijos duomenų išsaugojimas |
| FR-19 | Rankinis įrodymų įkėlimas (MVP nerealizuota) | Nėra | Sistema turi leisti įkelti atitikties įrodymus (dokumentus, vaizdus) | 1. Įrodymų įkėlimo vartotojo sąsaja<br>2. Skirtingų bylų tipų palaikymas (PDF, DOC, JPG, PNG<br>3. Dydžio apribojimas iki 10MB<br>4. Įrodymų tekstinio aprašymo pridėjimas<br>5. Bendras įkeltų įrodymų sąrašo atvaizdavimas<br>6. Sistema turi kategorizuoti įrodymus pagal blokus ir atskirus klausimus |
| FR-20 | Trečiųjų šalių integracija (MVP nerealizuota) | Nėra | Sistema turi leisti integruoti įrodymus iš trečiųjų šalių sistemų | 1. SIEM sistemų integracija<br>2 GRC platformų integracija<br>3. Derbesijos tiekėjų integracija<br>4. API raktų integracijai valdymas |

Programinės įrangos mažiausią gyvybingą produktas paleidžiamas lokaliai, izoliuotoje aplinkoje, todėl buvo keliami minimalūs **NFR** reikalavimai, pateikit NFR lentelėje

8 lentelė. **Nefunkcinių reikalavimų sąrašas.**

| ID | Nefunkcinis reikalavimas | Aprašymas | Kriterijai |
|---|---|---|---|
| NFR-01 | Atsako laikas | Sistema turi greitai atsakyti į vartotojo veiksmus | - Puslapio įkėlimas: < 2 sekundės<br>- Klausimų perjungimas: < 500ms<br>- Rekomendacijų generavimas: < 2 sekundės<br>- PDF generavimas: < 10 sekundžių |

| | | | |
|---|---|---|---|
| NFR-02 | Duomenų valdymas | Sistema turi efektyviai valdyti duomenis be našumo praradimo | Palaikyti iki 200 klausimų<br>Rekomendacijų duomenys<br>Diegimo plano duomenys |
| NFR-03 | Klaidų pranešimai | Sistema turi pranešti apie veikimo klaidas | Sistema nepakimba dėl klaidų ir pateikia klaidų pranešimus |
| NFR-04 | Vartotojo sąsajos aiškumas | Sistema turi būti suprantama ir tinkama naudojamui | Chrome, Firefox, Edge, Safari naršyklių palaikymas<br>Skirtingų ekranų rezoliucijų palaikymas |
| NFR-05 | Sistema turi užtikrinti duomenų saugumą | Prieiga pagal naudotojų roles | *SuperAdmin* - visų organizacijų valdymas<br>*Auditor* - visų organizacijų vertinimų peržiūra<br>*CustomerEditor* - vertinimų atlikimas<br>*CustomerReadonly* - tik peržiūra |
| NFR-06 | Sistema turi saugoti duomenis ilgalaikiam naudojimui | Duomenų išlaikymas tarp sesijų | *LocalStorage* duomenų saugojimas |

Suformuluoti techniniai reikalavimai pateikti **TR** lentelėje apima programinės įrangos vartotojo sąsajos ir serverio pusės architektūros technologijas, duomenų valdymą, diegimo ir testavimo aplinkas.

9 lentelė. **Techninių reikalavimų sąrašas.**

| ID | Techninis reikalavimas | Aprašymas | Technologijos |
|---|---|---|---|
| TR-001 | Vartotojo sąsajos architektūra | React vieno puslapio aplikacija | - React 19.1.0<br>- TypeScript 4.9.5<br>- React Hooks (useState, useEffect)<br>- CSS3 stiliai |
| TR-001 | Serverio pusės architektūra | Express.js serveris | - Node.js 18+<br>- Express.js 4.16.1<br>- Morgan logging<br>- Cookie parser |
| TR-003 | Duomenų valdymas | Kliento būsena be duomenų bazės valdymas | - React state management<br>- Local storage (sesijos duomenys)<br>- TypeScript tipai |

| | | | |
|---|---|---|---|
| TR-004 | Diegimo reikalavimas | Docker konteineris | - Docker 20+ |
| TR-005 | PDF generavimas | PDF eksportavimo funkcionalumas | - jsPDF 3.0.1<br>- html2canvas 1.4.1<br>- Canvas rendering<br>- Image processing |
| TR-006 | Testavimo reikalavimas | Testavimo infrastruktūra | - Jest 27.5.2<br>- React Testing Library 16.3.0 |

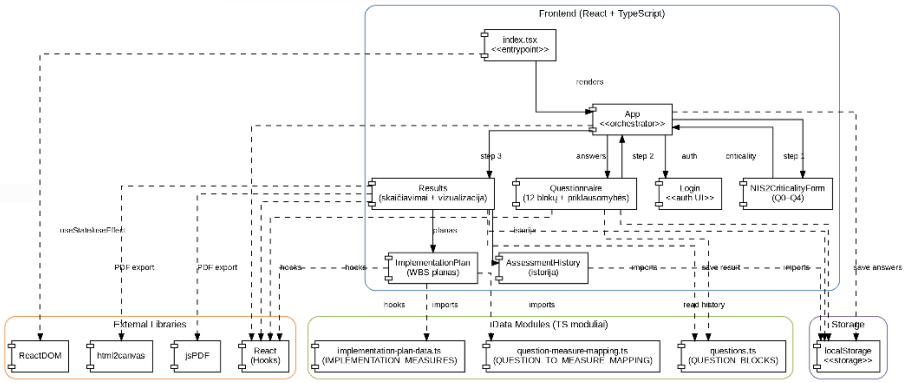
### 3.2. TIS2 atitikties vertinimo įrankio komponentų architektūros ir funkcionalumo vizualizavimas

Programinės įrangos sistemų projektavimas reikalauja nuoseklaus ir standartizuoto požiūrio į architektūros bei funkcionalumo dokumentavimą ir vizualizavimą. Vieninga modeliavimo kalba (angl. *Unified Modeling Language,* UML) yra tarptautinis standartas, skirtas programinės įrangos sistemų modeliavimui ir dokumentavimui, kuris užtikrina aiškų komunikacijos kanalą tarp projekto suinteresuotųjų šalių[[84] ]. UML 2.5.1 specifikacija, patvirtinta „Object Management Group“ organizacijos, apibrėžia 14 skirtingų diagramų tipų, kurie leidžia išsamiai dokumentuoti sistemos aspektus[[85] ]. TIS2 atitikties vertinimo įrankio projektavimo procese buvo taikytas modelių grindžiamas (angl. *model-driven development*, MDD) metodologinis požiūris, kuris pabrėžia modelių svarbą programinės įrangos kūrimo cikle[[86] ]. Šis metodas užtikrina, kad sistemos architektūra būtų aiškiai apibrėžta prieš pradedant įgyvendinimą, sumažinant projekto rizikas ir pagerinant galutinio produkto kokybę[[87] ]. Sistemos modeliavimui buvo pasirinkti trys pagrindiniai UML diagramų tipai, kurie geriausiai atskleidžia TIS2 vertinimo įrankio funkcinius ir architektūrinius aspektus:

1) Naudojimo atvejų diagramos – šios diagramos atskleidžia sistemos funkcionalumą iš vartotojo perspektyvos, apibrėždamos pagrindinius sistemos naudojimo scenarijus ir vartotojų vaidmenis.[[88] ] Naudojimo atvejų diagramos yra ypač svarbios reikalavimų inžinerijos procese, nes jos užtikrina aiškų supratimą apie sistemos tikslus ir funkcijas.[[89] ] TIS2 vertinimo įrankio kontekste naudojimo diagrama atskleidžia keturių skirtingų naudotojų rolių sąveiką su sistema.
2) Veiklos diagramos – šios schemos vaizduoja verslo procesų ir sistemos veiklos srautus, atskleidžiant sprendimų priėmimo logikos ir darbo eigų sudėtingumą.[[90] ] Veiklos diagramos yra ypač naudingos modeliuojant kompleksinius verslo procesus, kuriuose dalyvauja keli aktoriai ir egzistuoja sudėtinga sprendimų priėmimo logika.[[91] ] Parengta įrankio veiklos diagrama

atskleidžia adaptyvaus klausimyno logikos veikimą, rekomendacijų generavimo procesus ir vertinimo rezultatų apdorojimą.

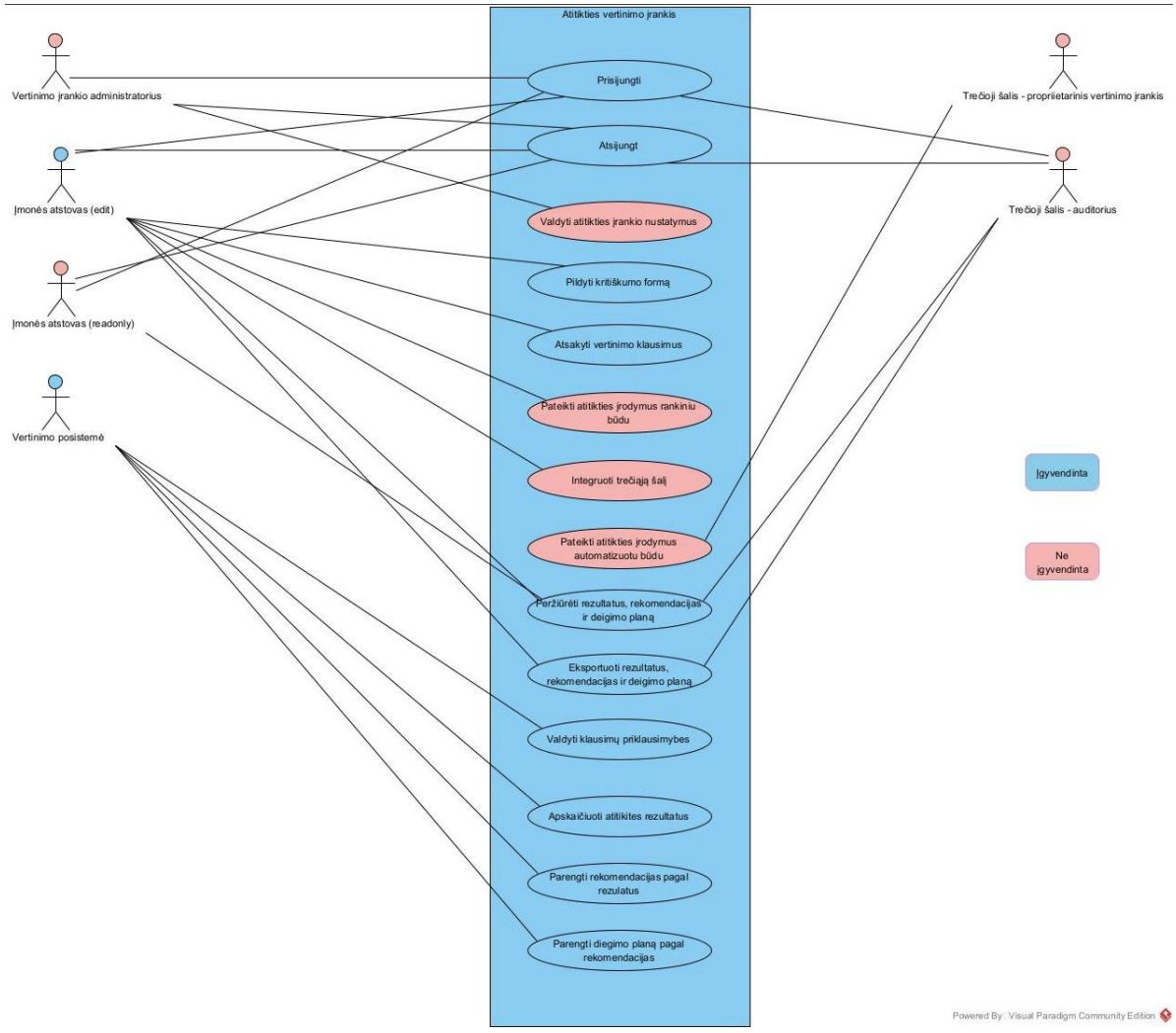
3) Komponentų diagramos atskleidžia sistemos architektūrinę struktūrą, parodydamos komponentų tarpusavio priklausomybes ir sąsajas.[[92] ] Jos yra kritiškai svarbios šiuolaikinių programinės įrangos sistemų architektūros dokumentavimui, ypač taikant mikroservisų ir modulinės architektūros principus.[[93] ] TIS2 įrankio komponentų diagrama (žr.



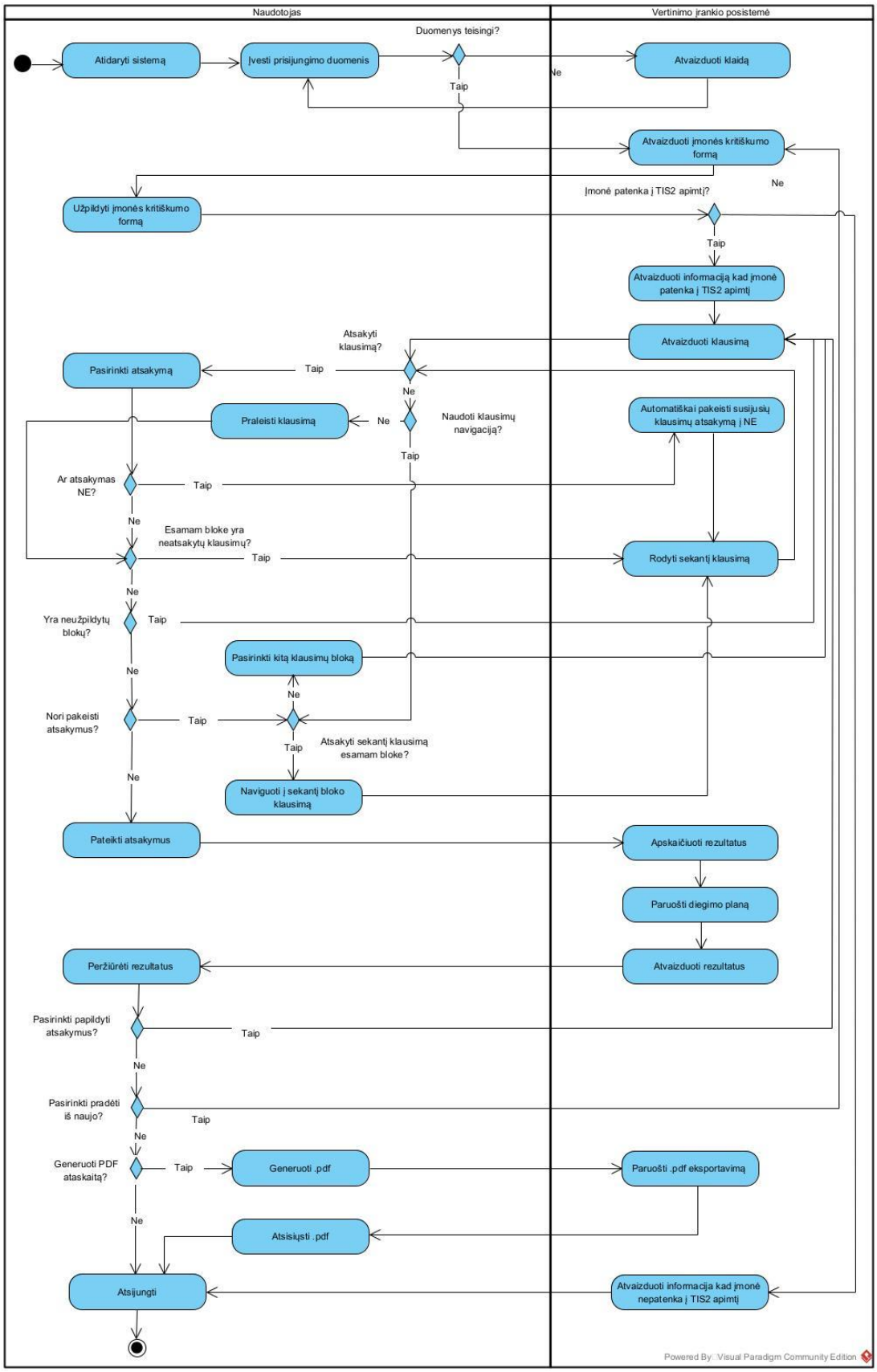

4) 30 Pav. Įrankio **„**React“ **komponentų diagrama**) atskleidžia „React“ aplikacijos komponentų hierarchiją, duomenų srautus tarp komponentų ir sistemos modulinę struktūrą.

Diagramų kūrimo procese buvo taikyti geriausi UML modeliavimo praktikos principai. Pirmiausia, buvo laikomasi abstrakcijos principo, kuris reikalauja, kad diagramos atskleistų tik esminius sistemos aspektus, vengiant perteklinio detalumo.[[94] ] Antra, buvo taikomas nuoskelumo principas, užtikrinantis, kad visi diagramų elementai būtų tarpusavyje suderinti ir atitiktų bendrą sistemos architektūros viziją.[[95] ] Trečia, buvo laikomasi užbaigtumo principo, kuris reikalauja, kad diagramų rinkinys išsamiai atskleistų visus svarbius sistemos aspektus.[[96] ] Kiekviena diagrama buvo kuriama laikantis specifinių metodologinių principų. Naudojimo atvejų diagrama buvo kuriama taikant tikslo siekimo požiūrio (angl. *goal-oriented approach),* kuris pabrėžia naudotojų tikslų identifikavimą ir sistemos funkcijų susiejimą su šiais tikslais.[[97] ] Veiklos diagramos buvo modeliuojamos naudojant proceso modeliavimo metodologiją, kuri užtikrina tikslų verslo procesų vaizdavimą ir sprendimų priėmimo logikos atskleidimą.[[98] ] Komponentų diagramos buvo kuriamos remiantis architektūros modeliavimo principais, kurie pabrėžia sistemos struktūrinių aspektų ir komponentų sąveikos dokumentavimą.[[99] ]

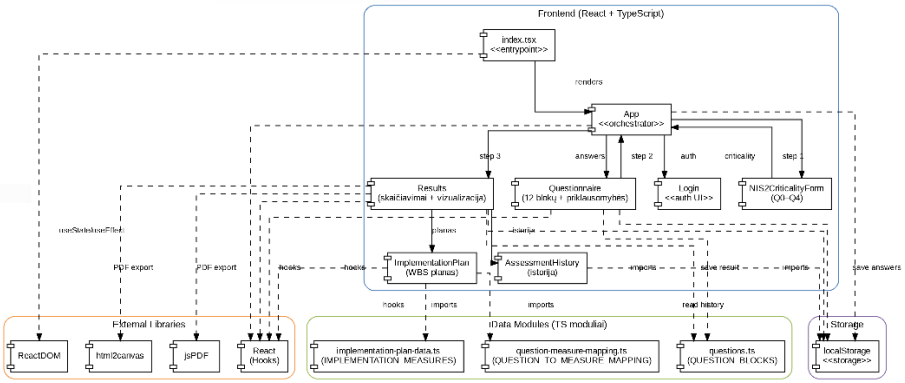
Šių UML diagramų rinkinys sudaro išsamų TIS2 atitikties vertinimo įrankio dokumentacijos pagrindą, kuris užtikrina sistemos supratimą ir sudaro prielaidas kokybiškam sistemos praktiniam įgyvendinimui. UML diagramų kūrimui buvo naudojama VizualParadigm programinė įranga, kuri palaiko visus pagrindinius UML diagramų tipus ir atitinka OMG standartus.



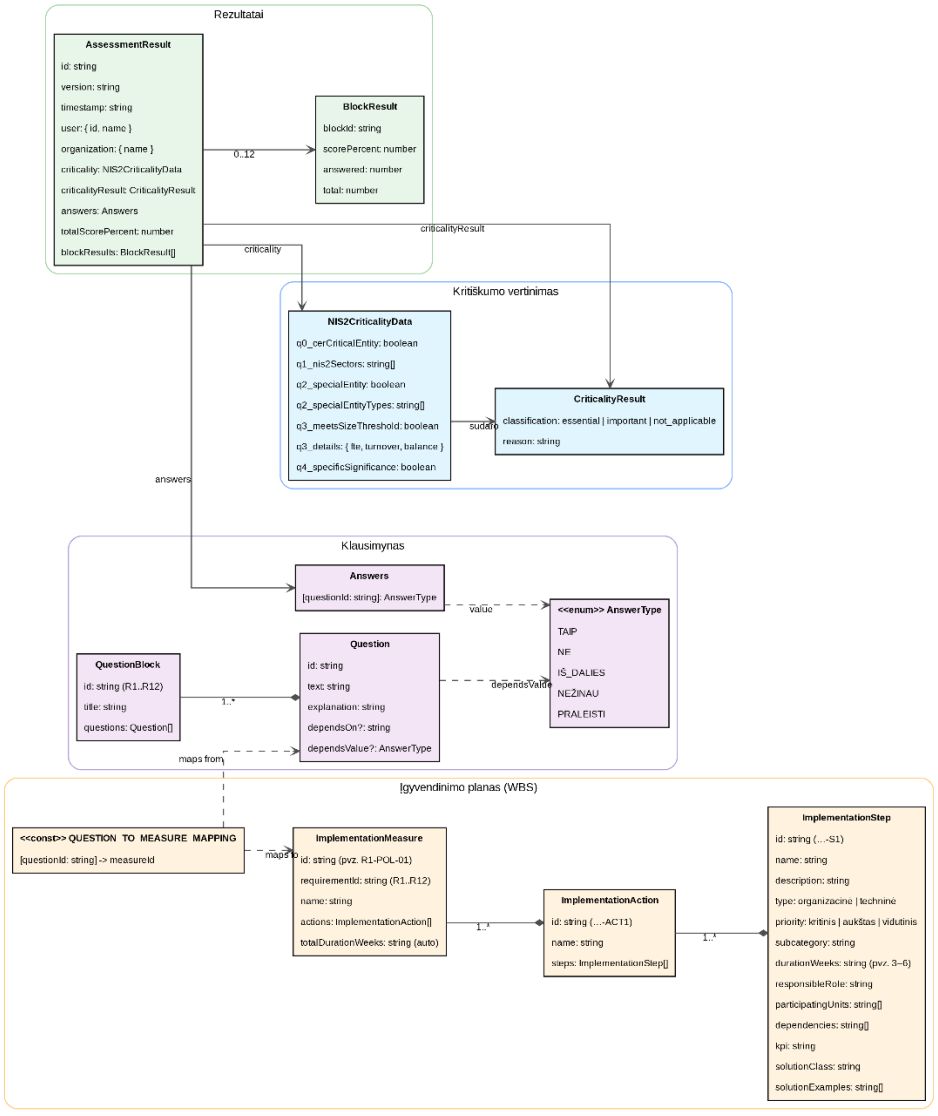

**28 Pav.** Įrankio naudojimo diagrama.




**29 Pav.** Įrankio veiklos diagrama.




**30 Pav.** Įrankio „React“ komponentų diagrama.




**31 Pav.** Įrankio klasių diagrama

### 3.3. Adaptyvaus TIS2 atitikties vertinimo įrankio metodika

Šiame skyriuje pristatoma adaptyvaus TIS2 atitikties vertinimo įrankio rengimo metodika. Ji grindžiama sistemine TIS2 direktyvos, ją įgyvendinančių ES teisės aktų, Lietuvos Respublikos kibernetinio saugumo įstatymo ir susijusių gairių (ENISA, NKSC, KAM ir kt.) analize atlikta 2 darbo skyriuje bei šių norminių reikalavimų ir rekomendacijų transformavimu į praktinį, TIS2 priemones orientuotą vertinimo modelį. Antroje darbo dalyje atliktos reikalavimų dekonstrukcijos į priemones rezultatas šiame skyriuje panaudojamas kuriant trys tarpusavyje susijusius įrankio komponentus:

1. Kritiškumo vertinimo komponentą, kuris realizuoja dinaminį organizacijos, kaip kibernetinio saugumo subjekto, vertinimą ir automatiškai klasifikuoja ją į esminį, svarbų arba nepriskirtą subjektą pagal TIS2 ir KSĮ nustatytus kriterijus.

2. Atitikties klausimyno komponentą, sugrupuotą į klausimų blokus pagal reikalavimų ir priemonių struktūrą ir naudojantį sąlyginių priklausomybių logiką pagrindinis-priklausomas (angl. *parent-child*). Tai leidžia vertinimo metu rodyti tik tuos klausimus, kurie yra aktualūs atsižvelgiant į atsakymus į ankstesnius klausimus, ir taip sumažina apklausos apimtį bei didina jos tikslumą.

3. Priemonių įgyvendinimo plano komponentą, kuris pagal vertinimą neįgyvendintas priemones išskaido į detalų įgyvendinimo veiksmų ir žingsnių planą, struktūruotą pagal darbo suskaidymo struktūros (angl. *Work Breakdown Structure,* WBS) logiką, nuo aukščiausio, priemonės lygmens, iki konkrečių veiksmų ir išmatuojamų žingsnių, kuriuos organizacija gali naudoti kaip praktinį kibernetinio saugumo priemonių diegimo ir tobulinimo planą.

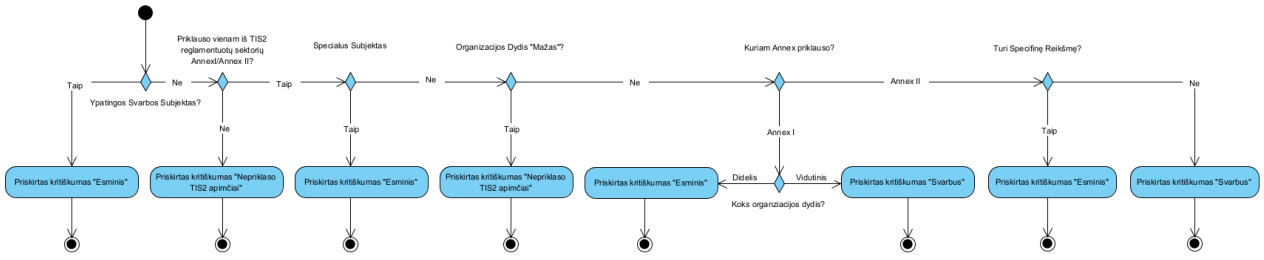
#### Kibernetinio saugumo subjekto statuso vertinimo komponentas

Ankstesniame skyriuje išanalizuoti kibernetinio saugumo subjektų statuso priskyrimo principai, kurie išskyrė pagrindinius subjektų savybių kriterijus: ypatingos svarbos subjektai (YSS, pagal CER direktyvą), specialūs subjektai, organizacijos, priklausančios TIS2 I ir II prieduose (*Annex I, Annex II*) nurodytiems sektoriams, atsižvelgiant į jų dydį ir specifinę reikšmę. Žemiau ši logika detalizuota lentelėje, kurioje skirtingų parametrų kombinacijos susiejamos su galutiniu kibernetinio saugumo subjekto status priskyrimu – *esminis*, *svarbus* arba *nepriskirta*.

10 lentelė. **Kibernetinio saugumo subjekto identifikacija.**

| YSS | SEKTORIUS | SPECIALUS SUBJEKTAS | DYDIS | SPECIFINĖ REIKŠMĖ | SUBJEKTO STATUSAS |
|---|---|---|---|---|---|
| TAIP | - | - | - | - | ESMINIS |
| NE | Nepriklauso | - | - | - | NEPRISKIRTAS |
| NE | Priedas I/ Priedas II | TAIP | - | - | ESMINIS |
| NE | Priedas I/ Priedas II | NE | MAŽAS | - | NEPRISKIRTAS |
| NE | Priedas I | NE | DIDELIS | - | ESMINIS |
| NE | Priedas I | NE | VIDUTINIS | - | SVARBUS |
| NE | Priedas II | NE | DIDELIS/ VIDUTINIS | TAIP | ESMINIS |
| NE | Priedas II | NE | DIDELIS/ VIDUTINIS | NE | SVARBUS |

Ši logika perkelta į vertinimo subjekto statuso vertinimo vertinimo komponentą. Įrankyje tai įgyvendinama kaip atskiras, nuo pagrindinio klausimyno atskirtas klausimų blokas, kurio tikslas – dinamiškai nustatyti, ar vertinama organizacija laikoma esminiu, svarbiu ar nepriskirtu kibernetinio saugumo subjektu pagal TIS2/KSĮ kriterijus. Vartotojui pateikiama trumpa uždarų klausimų seka („vartotojo kelionė per klausimus“), atspindinti subjekto identifikacijos schemą: pirmiausia klausiama, ar organizacija yra ypatingos svarbos subjektas (YSS); jei ne – ar ji priskiriama specialių subjektų kategorijai; ar organizacija veikia TIS2 reglamentuojamame sektoriuje (Annex I arba Annex II); koks yra organizacijos dydis (maža, vidutinė, didelė) ir ar ji turi specifinę reikšmę nacionaliniam saugumui ar esminėms visuomenės funkcijoms. Visi klausimai suformuluoti kaip uždari (TAIP/NE, išskyrus sektoriaus pasirinkimą iš kelių variantų), kad būtų galima juos panaudoti algoritminiam sprendimui. Klausimų blokas statusui nustatyti veikia kaip dinaminis filtro sluoksnis, tikslinantis ar naudotojui aktualu atlikti pagrindinį vertinimą pagal TIS2 reikalavimus. Žemiau pavaizduota naudotojo klausimų – atsakymų kelionė




**32 Pav.** Kibernetinio saugumo statuso nustatymo klausimų naudotojui kelionė.

**Reikalavimų ir priemonių transformavimas į vertinimo klausimus**

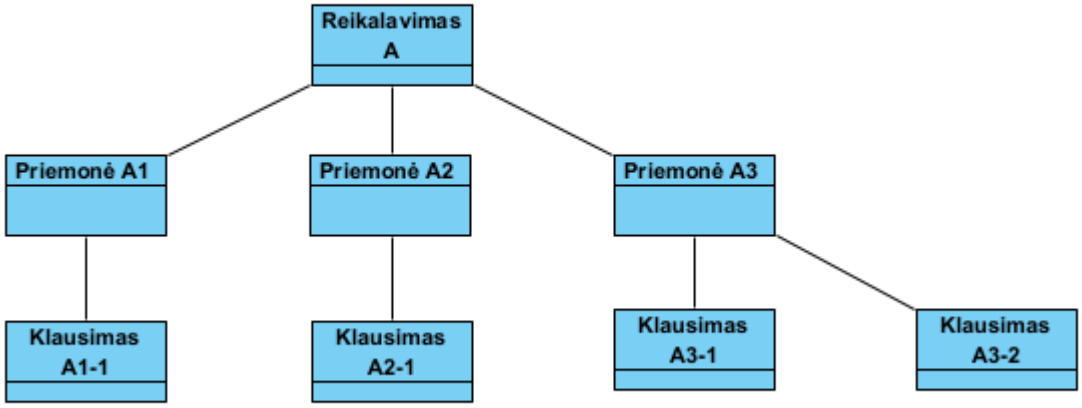
Antrame darbo skyriuje TIS2 direktyvos ir Lietuvos Respublikos kibernetinio saugumo įstatymo (KSĮ) reikalavimai buvo sistemiškai dekonstruoti į priemones, suskirstytas į organizacinių ir techninių priemonių kategorijas, šis priemonių sąrašas tapo jungiamąja grandimi tarp norminių reikalavimų ir praktinio vertinimo įrankio realizavimo. Priemonės suformuluoja kokius valdymo ir kontrolės elementus subjektas privalo turėti, taigi priemonių „turėjimo fakto“ tikrinimui, priemonių teiginiai buvo transformuoti į vertinimo klausimus.

Transformacijos logika buvo grindžiama principu, kad kiekviena priemonė turi aiškų atitikmenį klausimyne, tačiau šis ryšys nebūtinai griežtai vienas prie vieno. Daugeliu atvejų priemonė, suformuluota kaip teiginys, pvz., „Organizacijoje yra patvirtinta kibernetinio saugumo politika“, tiesiogiai apverčiama į uždarą klausimą: „Ar organizacijoje yra patvirtinta kibernetinio saugumo politika?“. Tokiu atveju išlaikomas vienas-vienas klausimo ryšys, viena priemonė lygu vienas klausimas. Vis dėlto dalis priemonių yra kompleksiškesnės ir apima kelis aiškiai atskiriamus aspektus, tokiais atvejais viena priemonė sąmoningai išskaidoma į du ar daugiau klausimų, kad kiekvienas klausimas tikrintų vieną aiškią temą ir sukuriamas vienas-daugelis ryšis. Ryšis yra vienpusis - priemonė gali virsti keliais klausimais, bet kiekvienas klausimas visada siejamas tik su viena konkrečia priemone, ne keliomis. Taip buvo siekiama išvengti dviprasmiškų atsakymų ir užtikrinti, jog klausimai paprasčiau interpretuojami, mažinama tikimybė kad bus pateiktas bendras atsakymas „taip“.  Svarbu pabrėžti, jog papildomais klausimais nebuvo modifikuojam norminė esmė, t.y. kas siekiama reikalavimu, tik detalizuojamas patikrinimo procesas.

Buvo siekiama, jog klausimų formuluotėse atsispindėtų ne abstrakčius gerosios praktikos, o konkretūs, reikalavimuose ir priemonėse užfiksuoti įpareigojimai. Klausimai nedviprasmiškai tikrina privalomų elementų buvimą ir veikimą, pasikartojančios tikrinimo formuluotės: „Ar yra patvirtinta..?“, „Ar atliekami..?“, „Ar įdiegti..?“, „Ar taikomas?“. Nors buvo atsižvelgiama į paprastumo idėją, siekiant  kad formuluotes suprastų ne tik kibernetinio saugumo specialistai, bet ir verslo atstovai, vadovai, kartu buvo vengiama abstrakcijų, ir techniniai klausimai buvo siejami su konkrečiais „sudėtingais“ objektais technologija, konfigūracija ir pan. Sudarytas klausimynas sudarė nuoseklia visuma su aiškia struktūra, klausimai sugrupuoti pagal reikalavimus, taip sudarant klausimų

blokus, taip vertinimo metu išlaikoma TIS2 apibrėžta kibernetinio saugumo valdymo logika ir seka. Pilna klausimyno versija pateikta klausimyno priede.

Kaip jau buvo minėta, kiekvienas klausimas yra unikalus ir susietas su priemone ir reikalavimu, ryšiai pavaizduoti 33 Pav. Reikalavimų - Priemonių - Klausimų pavyzdinė struktūra




**33 Pav.** Reikalavimų - Priemonių - Klausimų pavyzdinė struktūra.

Tai užtikrina, kad vėliau, rezultatų interpretavimo metu identifikuojama, kokios priemonės nėra pilnai įvykdytos ir nuo to priklauso kokį priemonių įgyvendinimo planą gaus naudotojas.

**Reikalavimų įgyvendinimo plano sudarymas.**

Reikalavimų įgyvendinimo plano sudarymui taikoma darbo suskaidymo struktūros, DSS (angl. *Work Breakdown Structure,* WBS) metodika. DSS klasikinėje projektų vadyboje suprantama kaip hierarchinis viso darbo apimties suskaidymas į vis smulkesnius komponentus, kol gaunami aiškiai apibrėžti darbų paketai ir užduotys, kuriems galima priskirti atsakomybę ir baigties kriterijus.[[80] ] Ši logika pritaikoma ne atskiro projekto planavimui, o TIS2 kibernetinio saugumo reikalavimų įgyvendinimo struktūros sukūrimui. Remiantis DSS principu, suformuota keturių lygių hierarchija:

a) Reikalavimas – aukščiausias lygis, atspindintis TIS2/KSĮ norminę nuostatą ir nusako ką privaloma pasiekti;
b) Priemonė – valdymo ir kontrolės lygis: konkreti organizacinė arba techninė priemonė (politika, procesas, technologinė kontrolė), leidžianti įgyvendinti reikalavimą.

c) Veiksmas – įgyvendinimo lygmuo, atitinkantis apčiuopiamą darbo kryptį, kurią reali organizacija gali planuoti ir priskirti atsakingam vaidmeniui.
d) Žingsnis – konkretus, įgyvendinamas ir išmatuojamas (angl. *actionable, measurable*) veiksmas, kurio rezultatas yra patikrinamas (parengtas dokumentas, atlikta konfigūracija, įvykdyti mokymai, paruošta procedūra ir pan.)

Siekiant išryškinti hierarchijos detalumą ir padaryti ją intuityviai suprantamą IT ir kibernetinio saugumo praktikams, panaudotas industrijos standartu laikomas užduočių sąrašo (angl. *backlog*) principas.

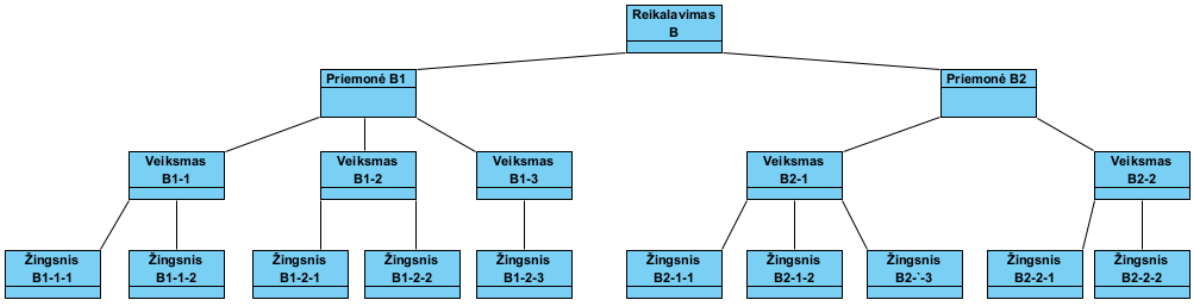
a) Reikalavimas - programinės iniciatyvos (angl. *theme*) kryptis – aukšto lygio strateginis tikslas arba reguliacinė sritis, apimanti kelias priemonių grupes, pvz. „Incidentų valdymas“,

b) Priemonė - reikšminga, bet dar suskaidoma iniciatyva (angl. *epic*) pvz., „įdiegti incidentų valdymo procesą“,

c) Veiksmas - konkreti funkcionalumo ar valdymo dalis (angl. *feature*), kurią galima planuoti kaip atskirą darbo srautą, pvz., „parengti incidentų klasifikavimo metodiką“,

d) Žingsnis - atskiros, aiškiai apibrėžtos užduotys, turinčios konkretų rezultatą (angl. *user story*), pvz., „parengti incidentų pranešimo NKSC šabloną“

Svarbu pabrėžti, kad užduočių sąrašo (*backlog*) analogija nėra pagrindinis teorinis pagrindas, o veikiau – aiškinamasios gairės, padedančios iliustruoti praktinėje darbų plotmėje ir darbų valdymo įrankiuose pvz., „Jira“ aplinkoje. Tai taip pat padėjo nustatyti praktines detalizacijos ribas. Viena priemonė paprastai skaidoma į kelius veiksmus, o vienas veiksmas į kelius žingsnius. Šios ribos nėra griežti ribojamos, kompleksiniams reikalavimams taikomas didesnis veiksmų ir (ar) žingsnių skaičius. Tačiau bendra įgyvendinimo darbų formulavimo logika išlieka visuose DSS lygiuose - vengiama pernelyg abstraktaus aiškinimo ir kitą vertus – smulkių užduočių, kurie jau taptų žingsnių detalizaciją (angl. *tasks, subtasks*). Pilnai įgyvendinimo planas pateiktas kaip atskiras priedas.




**34 Pav.** Įgyvendinimo plano pavyzdinė struktūra.

### 3.4. Apibendrinimas

Trečiajame skyriuje buvo apibrėžtas mažiausio gyvybingo produkto (angl. *minimum viable product*, MVP) tikslas bei suformuluoti reikalavimai programinei įrangai. Taip pat buvo atliktas TIS2/KSĮ teisinio reguliavimo teksto dekomponavimas į praktinį turinį, paruoštą realizacijai programinės įrangos produkte. Funkcinių, nefunkcinių ir techninių reikalavimų formulavimas užtikrino, kad įrankio projektavimas būtų grindžiamas sistemingu ir aiškiai patikrinamu reikalavimų apibrėžimu. Funkciniai reikalavimai sudarė pilną TIS2 atitikties vertinimo komponentų pagrindą. Nefunkciniai bei techniniai reikalavimai užtikrino, kad konceptualus prototipas taptų techniškai įgyvendintu, testuotinu ir toliau plečiamu produktu. Buvo pasitelkta UML modeliavimu siekiant apibrėžti skirtingų vaidmenų naudojimo scenarijus bei jų sąveiką su sistema, veiklos diagrama išskaidė statuso nustatymo ir vertinimo klausimynų ir rezultatų apdorojimo logiką, o komponentų diagrama pademonstravo „React“ aplikacijos struktūrą. TIS2 komponentų rengimo dalis parodė, kaip teisiniai reikalavimai transformuojami į praktinę, programavimo galimybę suteikiančią struktūrą. Kritiškumo vertinimo komponento logika automatiškai priskiria organizacijai kibernetinio saugumo statusą, metodinė reikalavimų ir priemonių dekonstrukcija į klausimus paruošė vertinimo klausimų komponentą, ir, galiausiai, DSS pagrindu buvo paruoštas priemonių įgyvendinimo komponentas, kuris sukuria esminę kuriamo produkto vertę – praktinę informacija diegimui, paruoštą naudoti organizacijos projektų ir užduočių valdymo aplinkoje. Paruošta medžiaga ir produkto reikalavimai sukūrė pagrindą ketvirtajame skyriuje aprašytam praktiniam prototipo įgyvendinimui.

# 4. TIS2 direktyvos atitikties vertinimo įrankio kūrimas

## 4.1. Atitikties vertinimo įrankio kūrimo aplinkos parinkimas

MVP produkto kontekste buvo pasirinkta kliento pusės (angl. *client-side*) vieno puslapio aplikacijos (angl. *Single Page Application*, SPA) architektūra, kuri užtikrina sklandžią naudotojo patirtį be puslapio perkrovimų, efektyvią navigaciją ir realaus laiko duomenų valdymą. SPA architektūra leistų visą klausimyno logiką apdoroti kliento pusėje, sumažinant serverio apkrovą ir užtikrinant greitą atsaką į naudotojo veiksmus. Priimant sprendimą buvo atsižvelgta, jog SPA atitiktų reikalavimą dėl greito atsako laiko ir leistų efektyviai valdyti sąlygines priklausomybes (angl. *parent-child*) tarp klausimų.

MVP produkto kontekste buvo pasirinkta kliento pusės (angl. client-side) vieno puslapio aplikacijos (angl. Single Page Application, SPA) architektūra, kuri užtikrina sklandžią naudotojo patirtį be puslapio perkrovimų, efektyvią navigaciją ir realaus laiko duomenų valdymą. [[101] ] SPA architektūra leistų visą klausimyno logiką apdoroti kliento pusėje, sumažinant serverio apkrovą ir užtikrinant greitą atsaką į naudotojo veiksmus. Priimant sprendimą buvo atsižvelgta, jog SPA atitiktų reikalavimą dėl greito atsako laiko ir leistų efektyviai valdyti sąlygines priklausomybes (angl. parent-child) tarp klausimų.

Tarp šiuolaikinių SPA karkasų buvo vertinami trys pagrindiniai variantai: „React“, „Vue.js“ ir „Angular“. „Angular“, kaip su savo moduline architektūra puikiai tinkamas didelėms, sudėtingoms sistemoms, tačiau pernelyg kompleksinis MVP kontekstui.[[104] ] Iš kitos pusės buvo vertinamas „Vue.js“, kuris pasižymi paprastumu, tačiau jo ekosistema yra mažesnė nei „React“, kuris ir buvo pasirinktas dėl kelių esminių privalumų – plati bibliotekų ir įrankių ekosistema, modulinė komponentų architektūra ir patogūs būsenos valdymo (angl. *state management*) mechanizmai, kurie gerai atitinka planuojamą įrankio funkcionalumą.[[102] ][[103] ] „React“, kurį 2013 m. sukūrė „Meta“ (tuomet „Facebook“), šiuo metu yra vienas populiariausių naudotojo sąsajos (angl. *frontend*) karkasų pasaulyje. Jis leidžia kurti deklaratyvų kodą, pakartotinai naudoti komponentus ir efektyviai atnaujinti dokumentų objektų modelį (angl. *Document Object Model*, DOM).[[102] ] „React“ komponentų architektūra leidžia klausimyną sudėlioti kaip hierarchinę struktūrą: kiekvienas klausimas, klausimų blokas ar naršymo elementas - tai atskiras, pakartotinai panaudojamas komponentas. Tai užtikrino kodo aiškumą, palengvino testavimą ir supaprastino kodo priežiūrą. Projekte „React“ naudojamas kartu su „TypeScript“, klausimyno duomenys yra sudėtingi ir turi daug atributų (klausimo identifikatorius, tekstas, paaiškinimai, priklausomybės, kategorijos ir kt.), todėl aiškiai apibrėžti tipai

padėjo išvengti klaidų kūrimo metu ir pagerino kodo skaitomumą.[[105] ] „TypeScript“ užtikrino, kad atributai būtų nuosekliai ir teisingai naudojami visoje sistemoje, taip sumažinant klaidų, pasirodančių tik vykdymo metu (angl. *runtime*), tikimybę.[[109] ] „React Hooks“ buvo pasirinktas kaip pagrindinis būsenos valdymo metodas. „React Hooks“ „useState“ ir „useEffect“, leidžia valdyti komponentų būseną ir šalutinius efektus be klasinių komponentų naudojimo.[[106] ] Klausimyno kontekste „useState“ buvo naudojamas saugoti atsakymus, klausimų bloką, progreso informaciją ir kitus dinamiškus duomenis. „useEffect“ užtikrino, kad veiktų klausimų priklausomybės, kai keičiasi atsakymai, ir kad duomenys būtų išsaugomi „localStorage“, kai naudotojas pateikia atsakymus. Duomenų saugojimui buvo pasirinkta naršyklės „localStorage“ technologija, kuri leidžia saugoti vertinimo duomenis kliento pusėje be serverio komunikacijos. Šis sprendimas užtikrino kliento būsenos valdymą be duomenų bazės ir taip pat kad naudotojo atsakymai būtų išsaugoti net jei naršyklė būtų uždaryta arba puslapis būtų perkrautas. localStorage yra palaikomas visose šiuolaikinėse naršyklėse ir užtikrina greitą duomenų prieigą kas atitiko projektuojamo MVP užmanymui. Testavimo tikslams buvo pasirinkti „Jest“ ir „React Testing Library“, kurie yra standartiniai „React“ įrankiai. „Jest“, kaip „JavaScript“ testavimo karkasas, užtikrina vienetinių testų (angl. unit tests) ir integracinių testų rašymą, o „React Testing Library“ leidžia testuoti komponentus iš naudotojo perspektyvos, tikrinant, ar komponentai teisingai veikia ir ar naudotojo sąsaja yra intuityvi.[[107] ][[108] ]

Apibendrinant galima teigti, jog „React“ su „TypeScript“ ir „React Hooks“ architektūra užtikrino, kad klausimyno komponentas būtų modulinis, lengvai prižiūrimas, efektyvus ir atitiktų MVP funkcinių, nefunkcinių ir techninių reikalavimų kriterijus. Šis aplinka leido greitai kurti ir testuoti funkcionalumus, užtikrino gerą naudotojo patirtį ir sudarė pagrindą tolesniam produkto plėtojimui.

### 4.2. TIS2 atitikties vertinimo įrankio kūrimas

Praktinė TIS2 atitikties vertinimo įrankio kūrimo dalis apima vertinimo proceso įgyvendinimą nuo subjekto kibernetinio saugumo statuso nustatymo iki identifikuotų atitikties trūkumų šalinimo įgyvendinimo plano parengimo. Visi projekto komponentai buvo realizuoti kaip atskiri „React“ komponentai, naudojant „TypeScript“ tipus ir „React Hooks“ būsenai valdyti. Buvo apibrėžtos TypeScript sąsajos (angl. *interfaces*) ir tipai, kurie užtikrina tipų saugumą visoje sistemoje. Žemiau pateiktos pagrindinės duomenų struktūros.

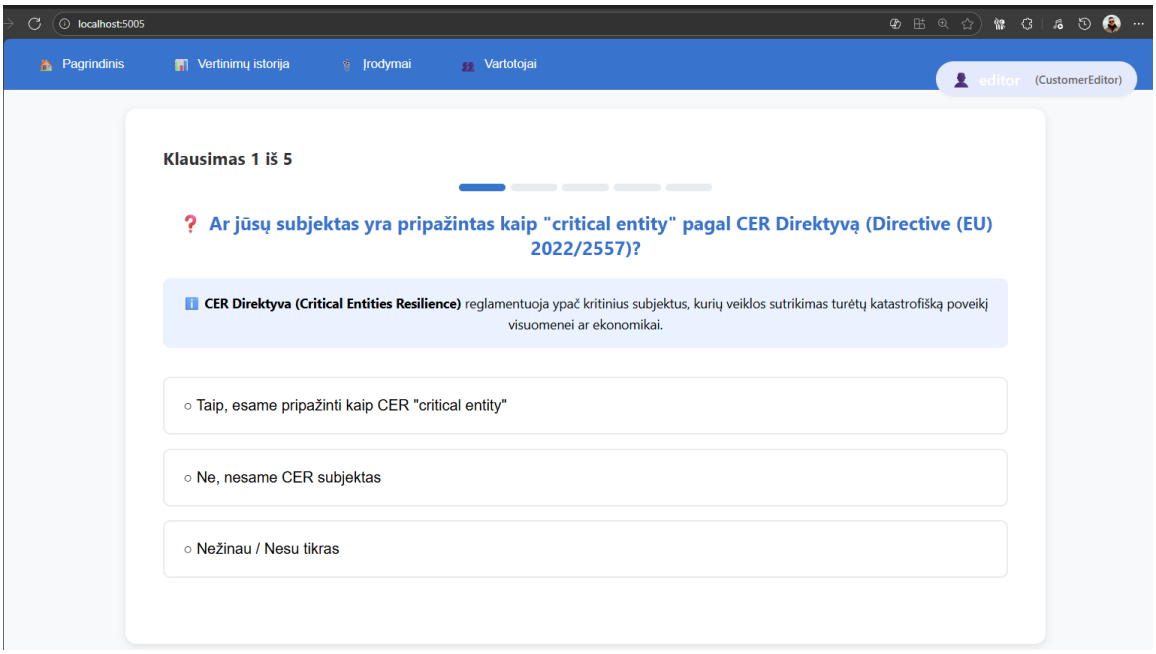
#### Subjekto kritiškumo vertinimas

Subjekto kritiškumo vertinimo duomenų struktūra „NIS2CriticalityData“ apibrėžia laukus reikalingus subjekto klasifikavimo procesui: CER kritinio subjekto statusą „q0_cerCriticalEntity“, TIS2 sektorių

sąrašą „q1_nis2Sectors“, specialių subjektų informaciją „q2_specialEntity“, „q2_specialEntityTypes“, organizacijos dydžio slenkstį „q3_meetsSizeThreshold“, „q3_details“, organizacijos specifinę reikšmę „q4_specificSignificance“.

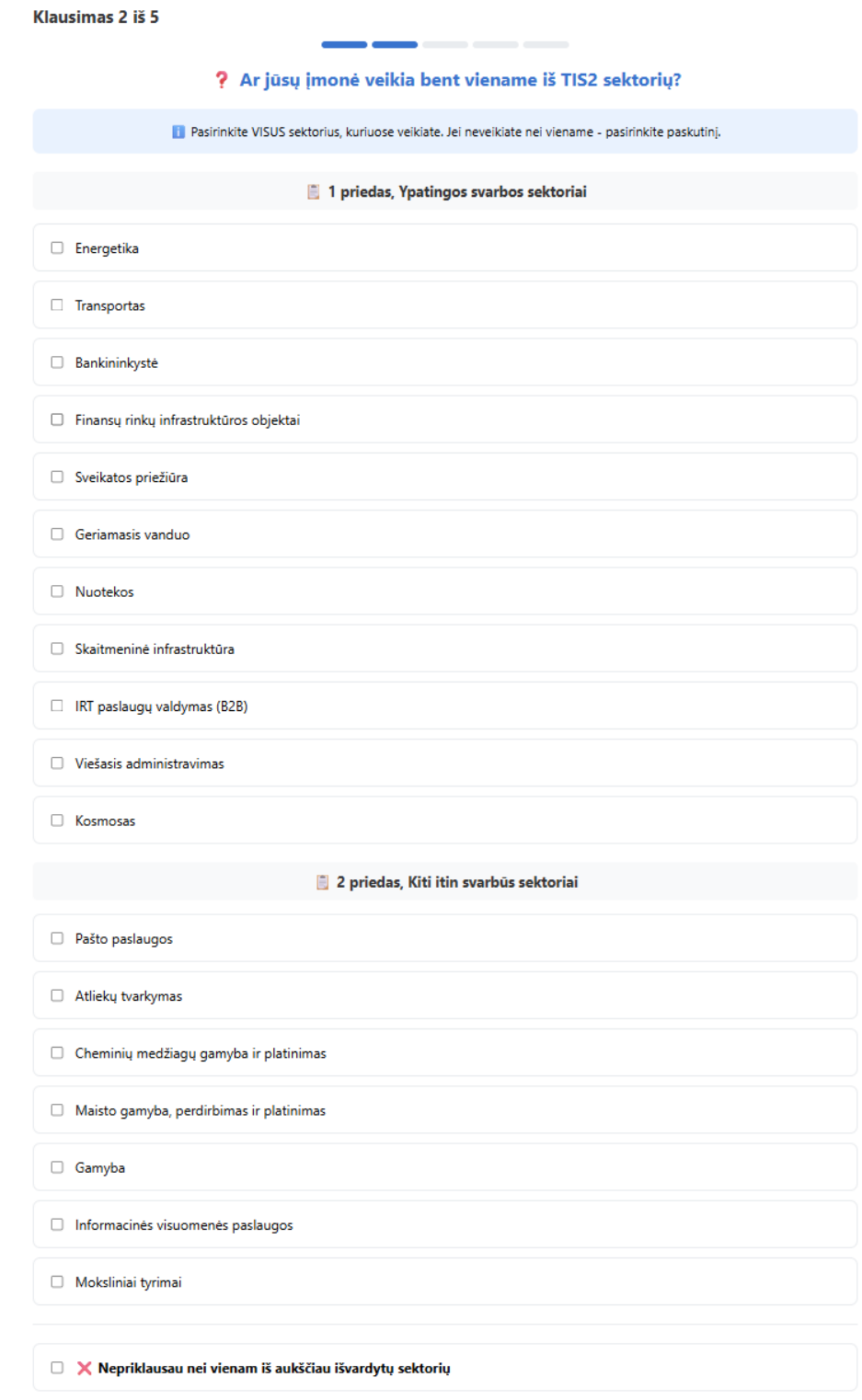
Kritiškumo vertinimo komponentas “NIS2CriticalityForm” realizuoja dinamišką organizacijos klasifikaciją kaip penkių etapų (Q0-Q4) sekos valdiklis, kur kiekvienas etapas surenka specifinę informaciją ir, priklausomai nuo atsakymų, arba pereina į kitą etapą, arba iškart nustato galutinę klasifikaciją.

Pirmasis etapas (Q0) klausia, ar organizacija yra CER direktyvos kritinis subjektas. Jei atsakymas yra teigiamas, klasifikacija nustatoma kaip „essential“ ir procesas baigiamas, kaip buvo nustatyta 2 skyriuje – CER subjektai automatiškai priskiriami prie TS2 svarbių subjektų.




**35 Pav.** Ekranvaizdis. CER kritiškumo identifikavimas.

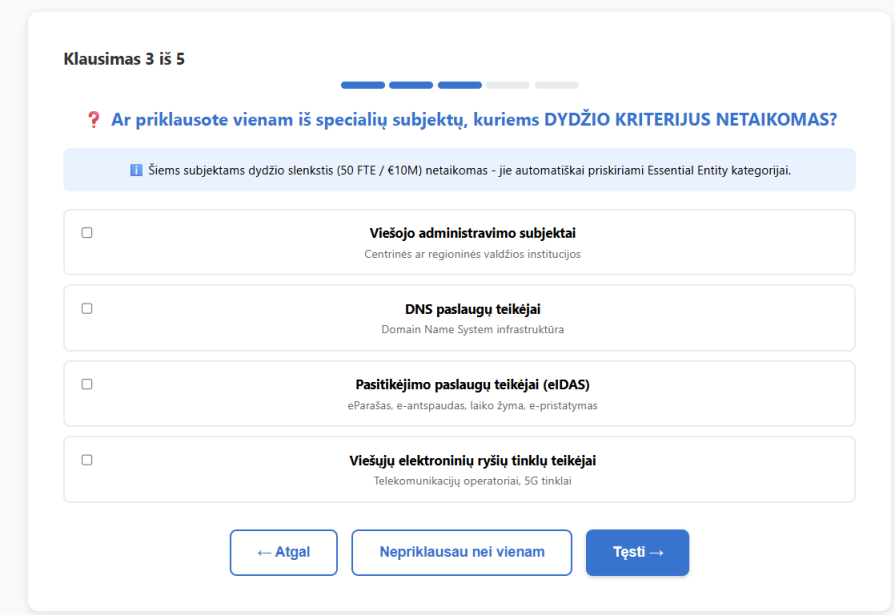
Antrasis etapas (Q1) leidžia vartotojui pasirinkti visus TIS2 sektorius, kuriuose organizacija veikia. Sektoriai yra sugrupuoti pagal TIS2 prieduose numatytas kategorijas, o vartotojas gali pasirinkti kelis sektorius arba nurodyti, kad organizacija neveikia nei viename sektoriuje. Jei organizacija neveikia TIS2 sektoriuose, subjektas klasifikuojamas kaip TSI2 „not_applicable“ ir procesas baigiamas.




**36 Pav.** Ekranvaizdis. TIS2 sektoriaus parinkimas.

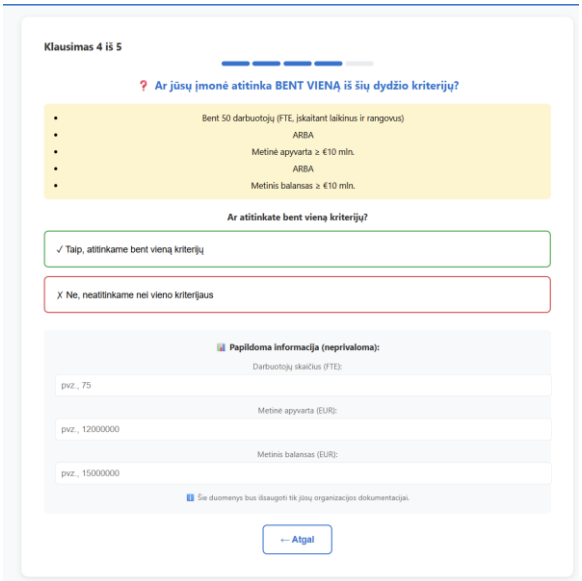
Trečiasis etapas (Q2) tikrina, ar organizacija yra specialus subjektas (DNS teikėjas, eIDAS teikėjas, telekomunikacijų tiekėjas arba viešojo administravimo subjektas). Jei atsakymas yra teigiamas,

klasifikacija nustatoma kaip „essential“, nes specialiems subjektams dydžio kriterijus netaikomas, tolimesnis tikrinimas nereikalingas.



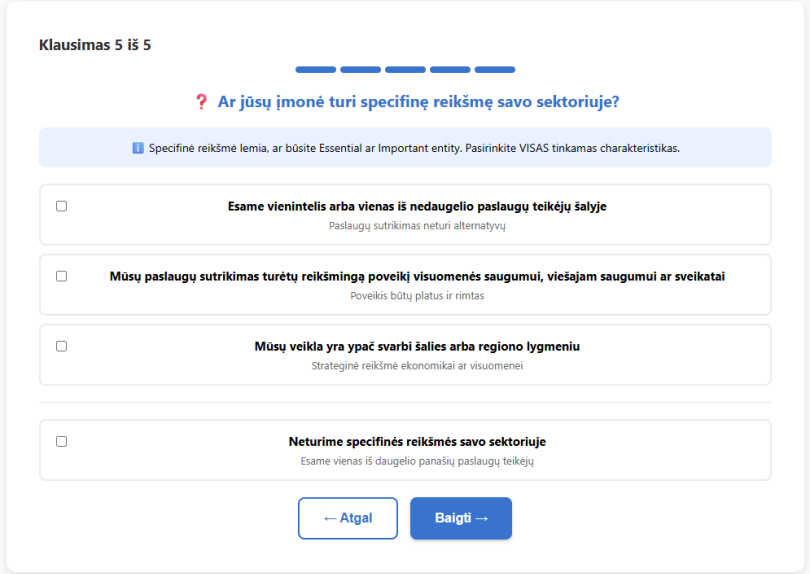

**37 Pav.** Ekranvaizdis. Specialaus subjekto identifikavimas.

Ketvirtasis etapas (Q3) tikrina, ar organizacija atitinka TIS2 numatytus dydžio slenksčius, ar turi ne mažiau kaip 50 darbuotojų ir (arba) organizacijos metinė apyvarta arba balansas yra ne mažesnis kaip 10 milijonų eurų. Jei organizacija netenkina šio kriterijaus, subjektas klasifikuojamas kaip TIS2 „not_applicable“.



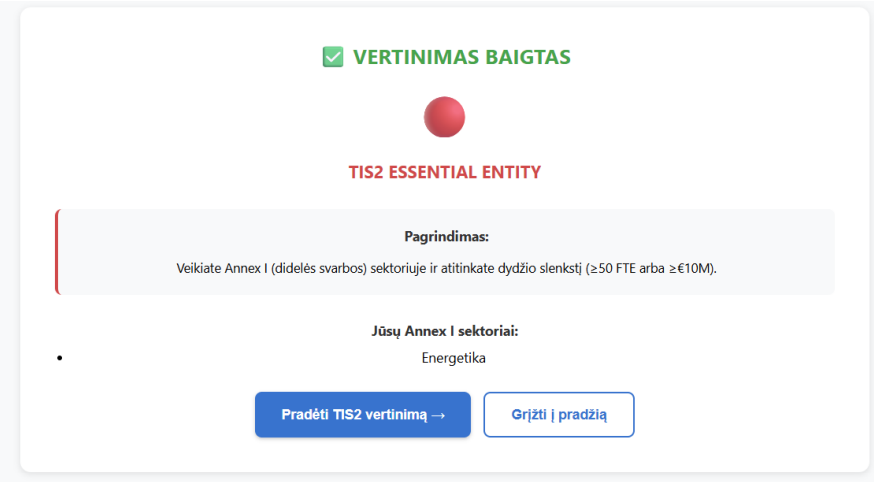

**38 Pav.** Ekranvaizdis. Subjekto dydžio nustatymas.

Penktasis etapas (Q4) taikomas tik organizacijoms, pasirinkusioms II priedo sektorių ir atitinkančioms dydžio slenkstį. Šiame etape tikrinama, ar organizacija turi specifinę reikšmę savo sektoriuje, jei specifinės reikšmės neturi, subjektas klasifikuojamas kaip „important“, jei turi – kaip „essential“.




**39 Pav.** Ekranvaizdis. Subjekto specifinės reikšmės nustatymas.

Subjekto klasifikacijos rezultato „reason“ laukas saugo klasifikacijos pagrindimą. Ši struktūra atitinka FR-03 reikalavimą dėl kritiškumo nustatymo formos pildymo. Komponento būsena yra valdoma naudojant „React“ „useState“, kur kiekvienas etapas turi savo būsenos kintamuosius, „step“ nustato dabartinį etapą, „data“ saugo surinktus duomenis, o „result“ saugo galutinį klasifikacijos rezultatą. Tokia struktūra užtikrina, kad komponentas leistų naudotojui naviguoti tarp etapų bei redaguoti ankstesnius atsakymus.




**40 Pav.** Ekranvaizdis. Nustatytas subjekto kibernetinio saugumo statusas ir pagrindimas.

**Vertinimo klausimynas**

Klausimų blokų struktūra „QuestionBlock“ grupuoja klausimus pagal temines sritis, atitinkančias TIS2 direktyvos reikalavimų struktūrą. Sistema apima 12 klausimų blokų, kurių identifikatoriai tiesiogiai siejami su TIS2 reikalavimais. Kiekvienas blokas turi unikalų identifikatorių (pvz., „R1_POLICY_RISK“), pavadinimą (pvz., „Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika“) ir susietą klausimų masyvą.

11 lentelė. **Klausimų blokai**

| **Klausimų blokas** | **Identifikatorius** |
|---|---|
| Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | R1_POLICY_RISK |
| Už kibernetinį saugumą atsakingų asmenų ir vadovo pareigos | R2_GOVERNANCE |
| Kibernetinių incidentų valdymas | R3_INCIDENT_MANAGEMENT |
| Veiklos tęstinumo užtikrinimas | R4_BUSINESS_CONTINUITY |
| Tiekimo grandinės saugumas | R5_SUPPLY_CHAIN |
| Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas | R6_SYSTEM_SECURITY |
| Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | R7_COMPLIANCE |
| Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | R8_AWARENESS |
| Kriptografijos ir šifravimo naudojimo politika ir procedūros | R9_CRYPTOGRAPHY |
| Žmogiškųjų išteklių saugumas | R10_RESOURCES |
| Tinklo saugumas | R11_NETWORK |
| Prieigos valdymas | R12_ACCESS |

Toks grupavimas užtikrina, kad vertinimo metu būtų išlaikyta nuosekli klausimų seka, kuri yra intuityviai suprantama naudotojui ir kartu atitinka TIS2 direktyvoje apibrėžtą reikalavimų struktūrą.


**41 Pav.** Ekranvaizdis. Klausimų blokai.

Klausimų blokų navigacija realizuota naudojant būsenos kintamąjį „blockIdx“, kuris nustato, kuris klausimų blokas šiuo metu rodomas naudotojui.

Vertinimo metu naudotojas gali laisvai pereiti tarp blokų, o komponentas automatiškai išsaugo atsakymus kiekviename bloke. Ši logika atitinka FR-05 reikalavimą dėl klausimų blokų navigacijos ir leidžia tiek linijinį, tiek selektyvų vertinimo scenarijų (pvz., pirmiausia vertinti svarbiausius blokų rinkinius).

Klausimų identifikatoriai struktūrizuojami pagal formatą: R[Reikalavimo_NR]-[Priemonės_ID]-[Klausimo_NR], pvz. „R1-POL-01-Q1“ reiškia pirmojo reikalavimo (R1) pirmosios priemonės (POL-01) pirmąjį klausimą (Q1). Toks žymėjimas leidžia vienareikšmiškai susieti kiekvieną klausimą su konkrečia priemone ir reikalavimu, o vėliau – su įgyvendinimo planu. Klausimų duomenų struktūra „Question“ sudaro:

a) klausimo identifikatorių „id“ (pvz., „R1-POL-01-Q1“, „R2-VAL-01-Q1“, „R3-INC-01-Q1“),
b) klausimo tekstą „text“,
c) paaiškinimą „explanation“ (perkeliamą iš „Kaip patikrinti“ stulpelio Excel faile),

d) priklausomybes „dependsOn“ (nurodo, nuo kurio kito klausimo priklauso) ir
e) lauką „dependsValue“ (nurodo, kokį atsakymą turi turėti priklausomas klausimas, kad konkretus klausimas būtų rodomas).


**42 Pav.** Ekranvaizdis. Atvaizduojamas klausimas.

Komponentas „Questionnaire“ realizuoja adaptyvų klausimyną, naudodamas sąlygines priklausomybes tarp klausimų. Priklausomybių mechanizmas leidžia užtikrinti, kad klausimas būtų rodomas tik tada, kai ankstesnis susijęs klausimas turi konkretų atsakymą. Tai atitinka FR-07 reikalavimą dėl klausimų priklausomybių valdymo. Praktinis veikimo principas yra toks: kai naudotojas atsako į klausimą, komponentas automatiškai patikrina, ar egzistuoja kitų klausimų, priklausančių nuo šio atsakymo. Jei priklausomas klausimas turi būti rodomas, jis įtraukiamas į matomų klausimų sąrašą. Jei, priešingai, priklausomas klausimas neturėtų būti rodomas (pavyzdžiui, kai į pagrindinį klausimą atsakoma „NE“), toks klausimas automatiškai pažymimas atsakymu „NE“ ir praleidžiamas. Tokia logika sumažina naudotojo apkrovą ir padeda išvengti nereikalingų klausimų situacijose, kai priemonė akivaizdžiai nėra įgyvendinama.

**Atsakymų tipai, saugojimas ir pildymo progresas.**

Atsakymų saugojimas realizuotas naudojant React „useState“ mechanizmą – objektas „answers“ saugo visus atsakymus, kur raktas yra klausimo identifikatorius, o reikšmė – atsakymo tipas. Papildomai atsakymai automatiškai išsaugomi „localStorage“ kiekvieną kartą, kai naudotojas pateikia atsakymą. Tokia realizacija užtikrina, kad duomenys būtų išsaugoti net ir naršyklei užsidarius ar puslapiui persikrovus ir atliepia praktinį poreikį atlikti vertinimą keliais etapais, be duomenų praradimo rizikos. Atsakymų tipas „AnswerType“ apibrėžia penkis galimus atsakymo į klausimus variantus: „TAIP“, „NE“, „IŠ DALIES“, „NEŽINAU“, „PRALEISTI“. Variantai atitinka FR-06

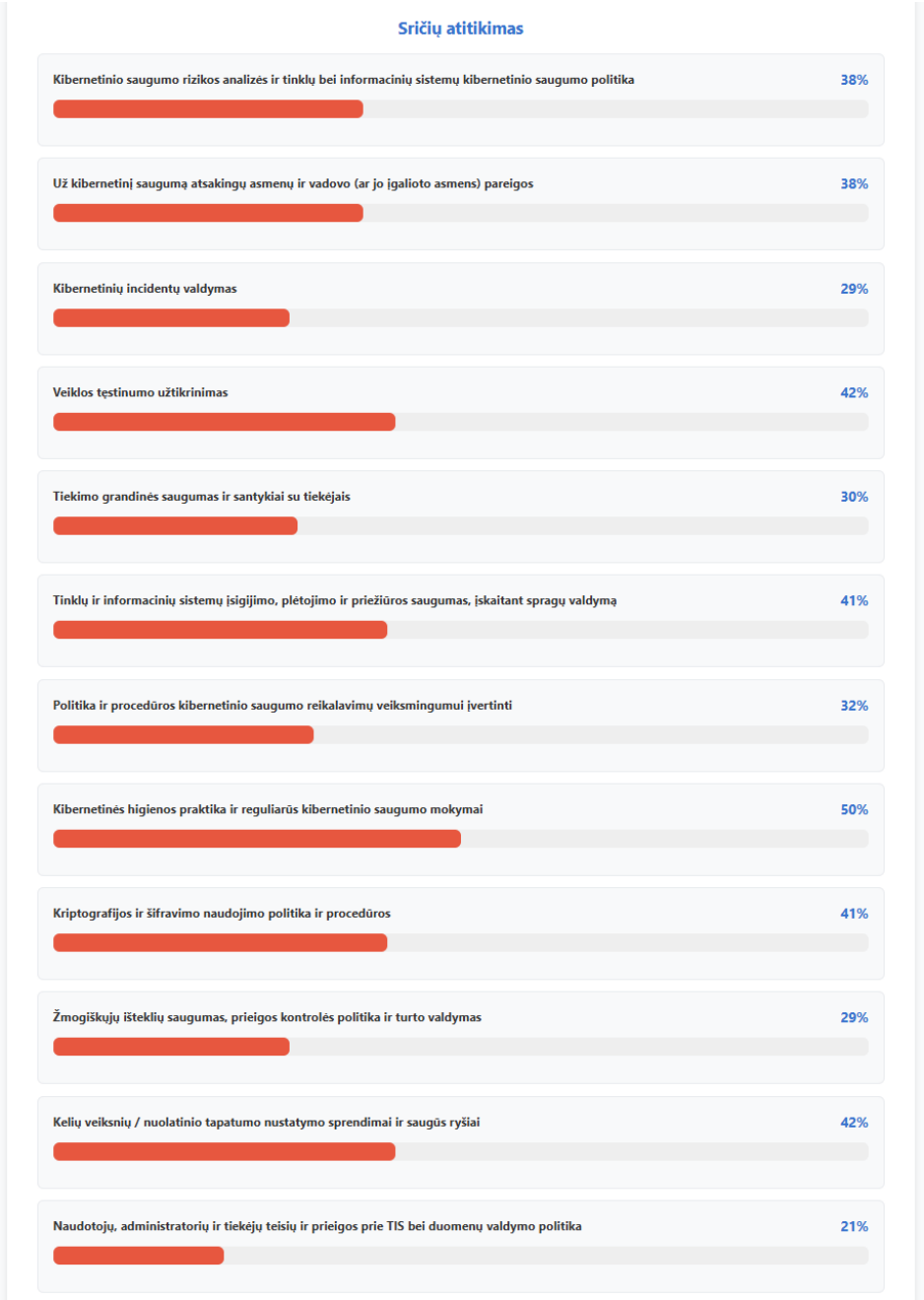
reikalavimą dėl atsakymų į klausimus sistemos ir atspindi praktinę organizacijų situaciją, kai realiose vertinimo sesijose dalis reikalavimų būna įgyvendinti tik iš dalies, o tam tikrose srityse organizacijos gali net neturėti pakankamos informacijos („NEŽINAU“), ką svarbu atskirti nuo sąmoningo „PRALEISTI“. Progreso sekimas realizuotas skaičiuojant atsakytų klausimų skaičių kiekviename bloke ir bendrą progresą visame klausimyne. Komponentas vizualiai parodo, kiek klausimų jau atsakyta ir kiek liko neatsakytų. Šis funkcionalumas atitinka FR-08 reikalavimą dėl pildymo progreso atvaizdavimo ir padeda naudotojams planuoti vertinimo trukmę, ypač kai vertinimas vykdomas etapais.

**Atsakymų rezultatų vertinimas ir vizualizacija**

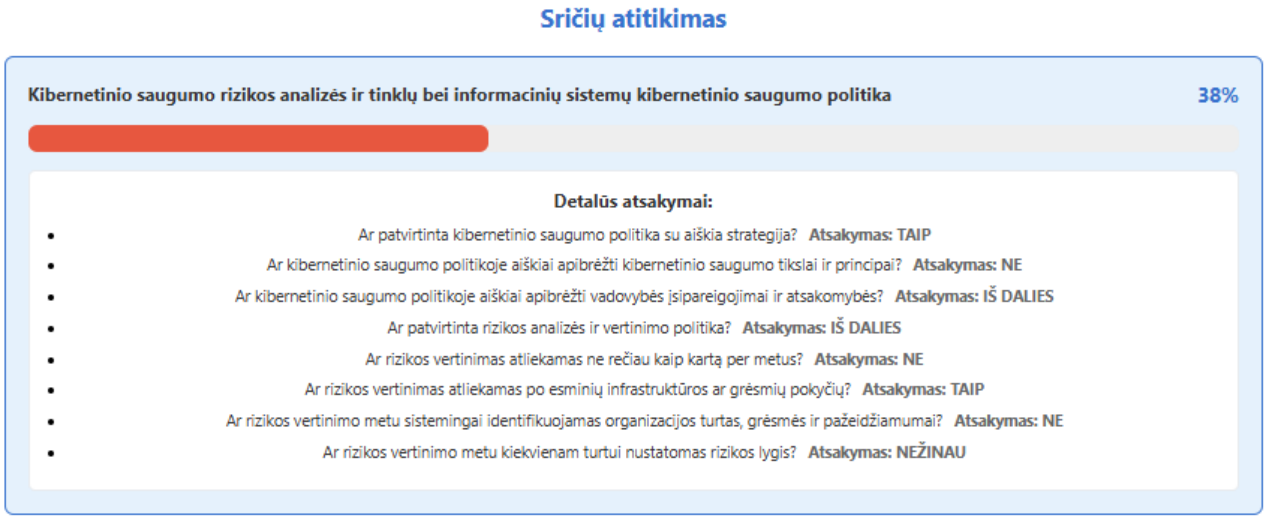
Rezultatų apdorojimo komponentas „Results“ realizuoja vertinimo rezultatų skaičiavimą, analizę ir vizualizaciją, kas atitinka FR-09 reikalavimą. Bendras atitikties procentas skaičiuojamas taikant tokį subjektyvų matematinį algoritmą: vertinimo balas = suma(visi atsakymai TAIP (vienas balas),visi atsakymai IŠ DALIES(pusė balo)) / viso klausimų × 100 %. Blokų rezultatų skaičiavimas atliekamas atskirai kiekvienam klausimų blokui taikant tą pačią formulę. Kiekvienam blokui apskaičiuojamas procentinis rodiklis, parodantis, kokia dalis klausimų buvo atsakyta „TAIP“ arba „IŠ DALIES“. Tai leidžia organizacijai identifikuoti stipriąsias ir silpnąsias sritis pagal konkrečius TIS2 reikalavimų blokus (pvz., matyti, kad incidentų valdymas („R3_INCIDENT_MANAGEMENT“) įvertintas geriau nei tiekimo grandinės saugumas („R5_SUPPLY_CHAIN“)). Rezultatų grafinė vizualizacija realizuota naudojant CSS stilius ir HTML elementus, kurie atvaizduoja progreso juostas, skaitines reikšmes ir spalvines indikacijas. Spalvinė logika atvaizduoja žalią spalvą kai rezultatas daugiau arba lygu 80 %, geltoną spalvą kai rezultatas yra tarpe nuo 50% iki 79 % ir raudoną spalvą kai rezultatas mažiau 50 %.


**43 Pav.** Ekranvaizdis. Bendrų rezultatų atvaizdavimas.

Tokiu būdu naudotojas gali greitai vizualiai identifikuoti reikalavimų blokus, kuriems būtina skirti didžiausią dėmesį. Spalvų ribos parinktos kaip kompromisas tarp akademiškai dažnai naudojamų pažymių skalės ir praktinių atitikties ribų (kritinės „raudonos“ zonos žemiau 50 %).




**44 Pav.** Ekranvaizdis. Atskirų sričių rezultatų atvaizdavimas.




**45 Pav.** Ekranvaizdis. Rezultatai per sritį ir atsakymų suvestinė.

Vertinimo rezultatų saugojimas realizuotas funkcijoje „generateAssessmentResult“, kuri sukuria „AssessmentResult“ objektą su visais reikalingais duomenimis: identifikatoriumi, naudotojo ir organizacijos informacija, laiko žyma, vertinimo versijos numeriu, subjekto kritiškumo duomenimis, atsakymais, bendru rezultatu ir blokų rezultatais. Šie rezultatai išsaugomi „localStorage“ ir gali būti naudojami vėlesnei analizei bei vertinimų istorijos peržiūrai, taip įgyvendinant FR-15 reikalavimą.

### Įgyvendinimo planas TIS2 atitikties trūkumams šalinti

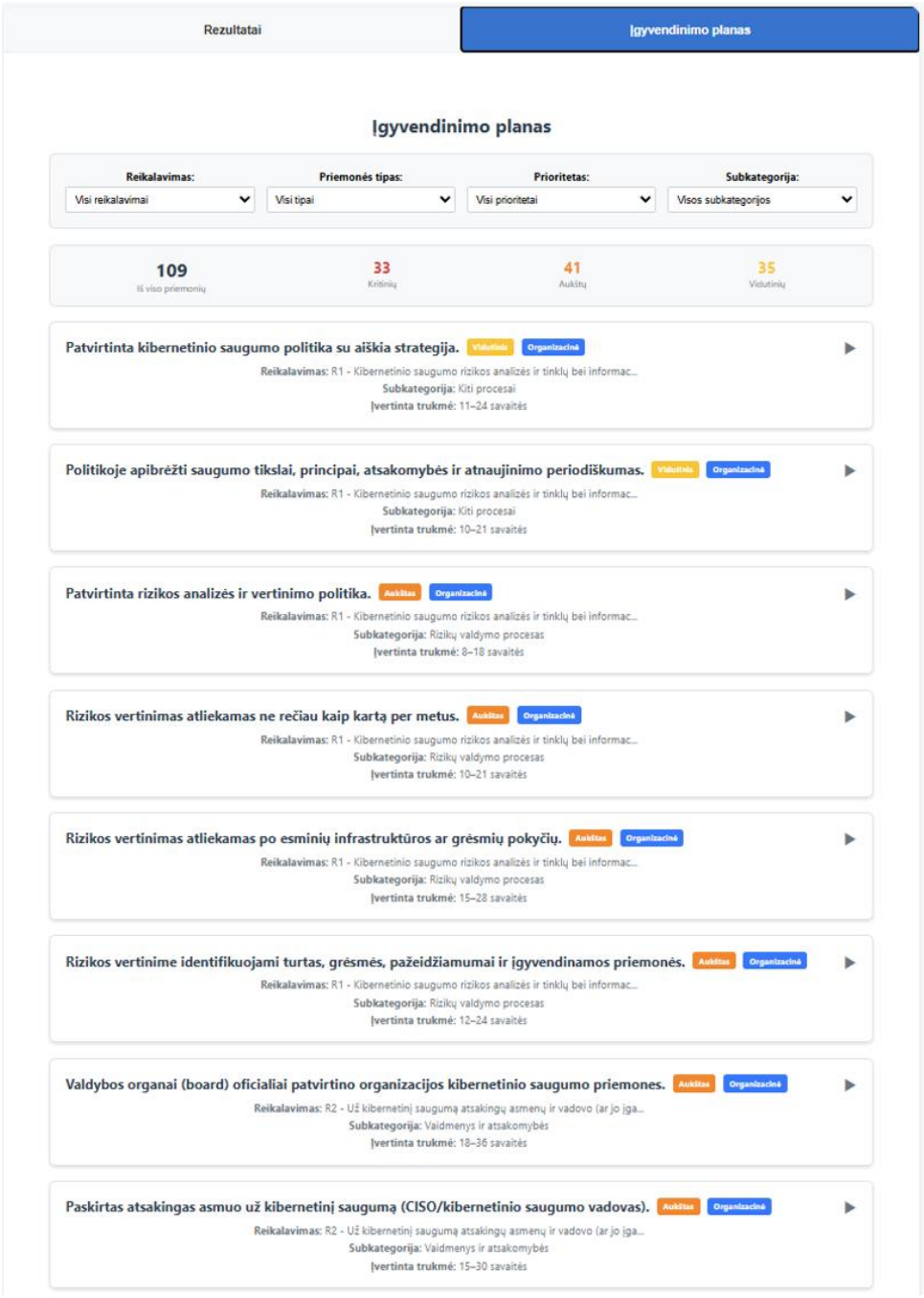
Rezultatų interpretavimo ir įgyvendinimo plano generavimo komponentas „ImplementationPlan“ transformuoja vertinimo atsakymus į praktinę, veiksmų lygmens informaciją organizacijai. Analizuojant vertinimo atsakymus, identifikuojami klausimai, kurių atsakymai yra neigiami arba daliniai (visi atsakymai, išskyrus „TAIP“), taip pat klausimai, kurie liko neatsakyti (kai klausimo identifikatoriaus nėra „answers“ objekte). Kiekvienas klausimas yra susietas su konkrečia direktyvos reikalavimo įgyvendinimo priemone per žemėlapio struktūrą „QUESTION_TO_MEASURE_MAPPING“, todėl neigiamas, dalinis ar neatsakytas klausimas traktuojamas kaip indikacija, kad atitinkama priemonė nėra pilnai įgyvendinta arba apskritai neįgyvendinta. Sistema pirmiausia peržiūri visus „QUESTION_TO_MEASURE_MAPPING“ struktūroje nurodytus klausimus ir nustato tuos, kurių atsakymai yra neigiami, daliniai arba kuriems atsakymai nepateikti. Tuomet kiekvienas toks klausimas susiejamas su konkrečia priemone, naudojant klausimo identifikatorių (pvz., „R1-POL-01-Q1“) ir ryšius priemonių duomenų bazėje. Priemonės,

susietos su tokiais klausimais, automatiškai pažymimos kaip reikalaujančios įgyvendinimo ir atvaizduojamos naudotojo sąsajoje.

Algoritmas remiasi trečiame skyriuje aprašyta darbų struktūros (WBS) metodika. Įgyvendinimo plano duomenų bazėje „IMPLEMENTATION_MEASURES“ kiekviena priemonė susieta su atitinkamais veiksmais („ImplementationAction“) ir žingsniais („ImplementationStep“). Taip užtikrinamas nuoseklus hierarchinis suskaidymas – Reikalavimas (pvz., „R1“) → Priemonė (pvz., „R1-POL-01“) → Veiksmas (pvz., „R1-POL-01-ACT1“) → Žingsnis (pvz., „R1-POL-01-ACT1-S1“).

Galutinėje detalizacijoje kiekvienas žingsnis turi šiuos atributus:

a) identifikatorių, susietą su priemone ir veiksmu (pvz., „R1-POL-01-ACT1-S1“),
b) pavadinimą ir aprašymą (perkeliamą iš stulpelio „Žingsnio aprašymas“),
c) tipą („Organizacinė“ arba „Techninė“ priemonė, iš stulpelio „Priemonės_tipas“),
d) prioritetą („kritinis“, „aukštas“ arba „vidutinis“ – tik trys lygiai, iš stulpelio „Priemonės_prioritetas“, rašomi mažosiomis raidėmis),
e) subkategoriją (pvz., „Kiti procesai“, „Rizikų valdymo procesas“, iš stulpelio „Priemonės_subkategorija“),
f) trukmę – įvertintą laiką žingsniui įgyvendinti (iš stulpelio „Žingsnio_trukmė_savaitėmis“, formatas „3–6“ savaitės),
g) atsakingą asmenį arba vaidmenį (iš „Atsakingas_vaidmuo“ stulpelio),
h) dalyvaujančius padalinius (iš „Dalyvaujantys_padaliniai“ stulpelio),
i) priklausomybes nuo kitų žingsnių (iš „Priklausomybės“ stulpelio),
j) rezultato rodiklį (iš „Rezultato rodiklis“ stulpelio),
k) sprendimo klasę (iš „Sprendimo klasė“ stulpelio),
l) sprendimo pavyzdžius (iš „Sprendimo pavyzdžiai“ stulpelio),
m) priemonės įvertintą trukmę (automatiškai apskaičiuojama sumuojant visų jos žingsnių minimalią ir maksimalią trukmę).



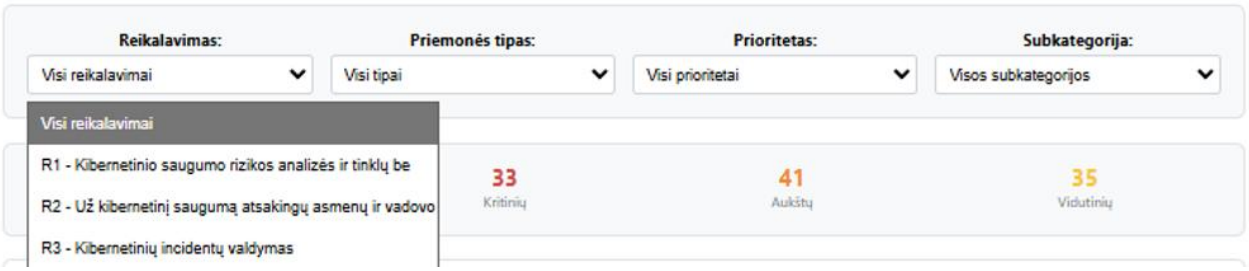

**46 Pav.** Ekranvaizdis. Įgyvendinimo plano atvaizdavimo pavyzdys.

Priemonės yra susietos su klausimais iš konkretaus klausimų bloko per „QUESTION_TO_MEASURE_MAPPING“ struktūrą ir automatiškai paveldi atitinkamą reikalavimo kategoriją (pvz., „R1“, „R2“ ir pan.). Techninių ir organizacinių priemonių atributas nustatomas kiekvienam žingsniui remiantis „Priemonės_tipas“ nurodyta informacija. Techninės priemonės apima technologinius sprendimus, konfigūracijas, įrangą ir pan., o organizacinės – procesus, politikas,

procedūras, mokymus ir kitus valdymo elementus. Trukmės pateikiamos subjektyviai autoriaus vertinamų intervalų forma (pvz. „3–6“ savaitės), siekiant atspindėti organizacijų projektų neapibrėžtumą. Subkategorijos („Rizikų valdymo procesas“, „Incidentų valdymo procesas“, „Kiti procesai“ ir kt.) buvo suformuotos taip, kad atspindėtų pagrindines organizacines ir technines veiklos sritis ir leistų filtruoti priemones pagal temines grupes, artimas praktinei GRC (Valdymas, Rizikos, Atitiktis angl. *governance, risk, compliance,* GRC) metodikai.

Naudotojo sąsajos įgyvendinimo plano filtravimas leidžia naudotojui peržiūrėti planą skirtingais pjūviais:

a) pagal reikalavimą (R1, R2, …, R12 arba „Visi reikalavimai“),
b) pagal priemonės tipą („Organizacinė“, „Techninė“ arba „Visi tipai“),
c) pagal prioritetą („kritinis“, „aukštas“, „vidutinis“ arba „Visi prioritetai“; sąmoningai atsisakyta „žemo“ prioriteto, kad planas būtų orientuotas į reikšmingiausias priemones),
d) pagal subkategoriją (21 subkategorija iš Excel failo, pvz., „Kiti procesai“, „Rizikų valdymo procesas“, „Incidentų valdymo procesas“, arba „Visos subkategorijos“).




**47 Pav.** Ekranvazdis**.** Įgyvendinimo plano filtravimas.

Po vertinimo atvaizduojamos identifikuotos neįgyvendintos ar iš dalies įgyvendintos priemonės pagal atsakymus, tuomet joms taikomi naudotojo pasirinkti filtrai (reikalavimas, tipas, prioritetas, subkategorija). Taip užtikrinama, kad naudotojas pirmiausia mato tik realiai trūkstamas priemones, o ne pilną teorinį priemonių sąrašą. Įgyvendinimo plano vizualizacija realizuota naudojant React komponentus, atvaizduojančius priemones kaip hierarchinę struktūrą su išplėtimo/suskleidimo funkcija kiekvienam lygiui (Priemonė → Veiksmas → Žingsnis). Kiekvieną žingsnį galima išplėsti ir matyti visą susijusią informaciją: trukmę, atsakingą vaidmenį, dalyvaujančius padalinius, priklausomybes, rezultato rodiklį, sprendimo klasę ir pavyzdžius.


**48 Pav.** Ekranvaizdis. Priemonė → Veiksmas → Žingsnis.

Statistikos sekcija pateikia: bendrą priemonių skaičių, vidutinę trukmę (apskaičiuojamą iš visų priemonių trukmių), bei priemonių skaičių pagal prioritetą (kritinių, aukštų, vidutinių). Tai suteikia greitą „santraukos“ vaizdą apie organizacijos laukiančio darbo apimtis.

**Komponentų integracija ir duomenų srautas**

Pagrindinis aplikacijos React komponentas „App“ valdo visą aplikacijos būseną ir koordinuoja atskirų komponentų tarpusavio sąveiką. Komponentas naudoja React „useState“ mechanizmą būsenų valdymui:

a) prisijungimo būsenos („loggedIn“, „user“),
b) navigacijos („step“),
c) subjekto kritiškumo duomenų („criticality“),
d) klausimyno rezultatų („questionnaireResult“),
e) vertinimo rezultatų („assessmentResults“),
f) dinamiškai generuojamo įgyvendinimo plano (atskiro „implementationPlan“ būsenos kintamojo nenaudojama, planas generuojamas pagal atsakymus).

Bendro duomenų srauto organizavimas:

a) naudotojas prisijungia prie sistemos;
b) naudotojas pradeda vertinimą, užpildydamas kritiškumo vertinimo formą;
c) kritiškumo duomenys perduodami klausimyno komponentui, kuris inicijuoja klausimyną;
d) naudotojas atsako į klausimus, o atsakymai saugomi komponento būsenoje ir „localStorage“;
e) užbaigus klausimyną, atsakymai perduodami rezultatų komponentui;
f) rezultatų komponentas apskaičiuoja ir atvaizduoja bendrus ir blokų rezultatus;
g) įgyvendinimo plano komponentas analizuoja atsakymus, identifikuoja neįgyvendintas priemones (įskaitant neatsakytus klausimus) ir dinamiškai generuoja įgyvendinimo planą iš „IMPLEMENTATION_MEASURES“ duomenų bazės;
h) rezultatai ir įgyvendinimo planas išsaugomi „localStorage“ ir pridedami prie vertinimų istorijos.

Tokia architektūra užtikrina, kad kiekvienas komponentas būtų pakankamai autonomiškas ir pakartotinai panaudojamas, o duomenų srautas – aiškiai apibrėžtas ir lengvai sekamas. Tai atitinka modulinės architektūros principus ir palengvina sistemos priežiūrą bei plėtrą, ypač numatant papildomų reikalavimų, naujų klausimų blokų ar alternatyvių vizualizacijų įdiegimą ateityje.

### 4.3. TIS2 atitikties vertinimo įrankio testavimas planas

TIS2 atitikties vertinimo įrankio testavimo planas buvo parengtas remiantis trečiajame skyriuje suformuluotais funkciniais (FR), nefunkciniais (NFR) ir techniniais (TR) reikalavimais, siekiant užtikrinti, kad visi šie reikalavimai būtų sistemiškai patikrinti ir patvirtinti prieš produkto pristatymą. Tokia prieiga atitinka programinės įrangos inžinerijos gerojoje praktikoje įtvirtintą reikalavimų sekamumo (angl. traceability) principą, kai kiekvienam reikalavimui yra priskiriami konkretūs testavimo atvejai ir validavimo veiklos.[[100] ] Funkcinių reikalavimų testavimas buvo orientuotas į tai, ar įrankis teisingai įgyvendina TIS2 atitikties vertinimo logiką – klausimynų šakotumą, adaptacines taisykles, rezultatų skaičiavimą ir rekomendacijų suformavimą. Nefunkcinių reikalavimų testavimu buvo vertinamas našumas, naudotojo sąsajos patogumas ir patikimumas. Techninių reikalavimų testavimas buvo vykdomas tikrinant suderinamumą su pasirinkta įrankio kūrimo aplinka.

a) **Vienetiniai testai** (angl. *unit tests*) yra skirti patikrinti atskirų komponentų ir funkcijų veikimą izoliuotai nuo kitų sistemos dalių. Testavimui buvo pasirinkti „Jest karkasas“ (TR-006) ir „React Testing Library“, kurie užtikrina, kad komponentai būtų testuojami iš vartotojo perspektyvos.
b) **Integracinių testų** (angl. *integration tests*) tikslas patikrinti, kaip skirtingi sistemos komponentai veikia kartu. Testai apima komponentų tarpusavio sąveiką, duomenų srautą tarp komponentų ir integraciją su localStorage.
c) **Sistemos testų** (angl. *system tests*) tikrina visą sistemą kaip vientisą visumą, tikrinant funkcinių reikalavimų įgyvendinimą ir vartotojo patirtį.
d) **Priėmimo testai** (angl. *acceptance tests*) remiasi priėmimo kriterijais, kurie apibrėžia, kada testas laikomas sėkmingu. Funkcinių reikalavimų priėmimo kriterijai pateikti trečiajame skyriuje, ir testai turi patvirtinti, kad visi šie kriterijai yra patenkinti.

Kiekvienas testavimo lygis turi savo tikslus ir apimtį, o jų derinys užtikrina visapusišką sistemos patikrą. Bendras testavimo tikslas – užtikrinti, kad visi funkcinių reikalavimų (FR-01 iki FR-20) priėmimo kriterijai būtų patenkinti, patikrinti, ar sistema atitinka nefunkcinių reikalavimų (NFR-01 iki NFR-06) kriterijus bei patvirtinti, kad techniniai reikalavimai (TR-001 iki TR-006) yra įgyvendinti teisingai.

### 4.4. Testavimo ataskaita

Testavimas buvo atliktas etape, kai sistema buvo pilnai funkcionali ir paruošta naudojimui. Testavimo procesas organizuotas pagal 4.3 poskyryje aprašytą testavimo planą, kuriame apibrėžti testavimo tipai,

priėmimo kriterijai ir jų ryšys su funkciniais (FR), nefunkciniais (NFR) ir techniniais (TR) reikalavimais. Testavimas vykdytas naudojant rankinius testus ir dalinį automatizuotų testų palaikymą, atsižvelgiant į MVP etapo apribojimus. Testavimo aplinka apėmė lokalią plėtros aplinką su „React 19.1.0“ ir „TypeScript 4.9.5“, „Docker“ konteinerizuotą produkcinę aplinką ir dvi naršykles („Chrome“, „Edge“).

Vienetiniai testai buvo taikomi pagrindinėms verslo logikos funkcijoms ir komponentams (kritiškumo klasifikavimo algoritmui, klausimyno „React“ komponentams, rezultatų skaičiavimo funkcijai), užtikrinant, kad atskiros dalys veikia korektiškai. Integraciniai testai buvo skirti komponentų tarpusavio sąveikai ir duomenų srautui (kritiškumo vertinimo ir klausimyno integracija, rezultatų komponentas, „localStorage“ integracija, vertinimų istorijos išsaugojimas ir atkūrimas). Sistemos ir priėmimo testai tikrino visą sistemą kaip vientisą visumą – autentifikaciją ir autorizaciją, kritiškumo nustatymo formą, klausimų blokų navigaciją, atsakymų variantų ir priklausomybių logiką, progreso atvaizdavimą, rezultatų apdorojimą, diegimo plano generavimą, vertinimų istorijos atvaizdavimą ir PDF eksporto funkciją. Nefunkcinių reikalavimų testai vertino našumą, duomenų valdymą, naudotojo sąsajos aiškumą ir duomenų išlaikymą tarp sesijų.

Konkretūs testavimo atvejai ir jų rezultatai apibendrinti 12 lentelėje, kurioje nurodyti testų identifikatoriai (T-01–T-19), susieti reikalavimai (FR, NFR, TR), scenarijų santraukos, tikėtini ir faktiniai rezultatai, testų statusas bei pagrindinės pastabos. Testų rezultatai parodė, kad funkciniai reikalavimai FR-01–FR-15 ir nefunkciniai reikalavimai NFR-01, NFR-02, NFR-04, NFR-06 yra įgyvendinti, o techniniai reikalavimai (pvz., „localStorage“ panaudojimas duomenų išlaikymui) veikia pagal numatytą logiką. Vienintelis iš dalies sėkmingas rezultatas susijęs su PDF eksporto funkcija (FR-12) – nors PDF generavimas techniškai veikė, pasirinktas formato šablonas netinkamai atvaizdavo ilgesnį turinį, todėl šios funkcijos tobulinimas MVP apimtyje nebuvo vystomas.

12 lentelė. **Testavimo ataskaita.**

| **Testo ID** | **FR/ NFR** | **Testavimo tipas / lygis** | **Scenarijaus santrauka** | **Tikėtinas rezultatas** | **Faktinis rezultatas** | **Statusas** | **Pastabos / nustatytos problemos** |
|---|---|---|---|---|---|---|---|
| T-01 | FR-03 | Vienetinis (unit) | Klasifikavimo algoritmo testavimas su visais scenarijais: CER kritinis subjektas, specialūs subjektai, I ir II priedų sektoriai, | Organizacija klasifikuojama pagal TIS2 kriterijus, rezultatas ir pagrindimas atitinka apibrėžtas taisykles. | Algoritmas teisingai klasifikavo visus scenarijus, rezultatai ir pagrindimai sutapo su tikėtais. | Sėkmingas | Pradiniame variante nebuvo pateikiamas pakankamas pagrindimo tekstas – logika papildyta, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | dydžio slenkstis, specifinės vertės. | | | | problema išspręsta. |
| T-02 | FR-05, FR-06, FR-07 | Vienetinis / komponentų | Klausimyno „React“ komponentų testavimas su skirtingomis būsenomis ir duomenimis. | Komponentai teisingai atvaizduoja turinį, reaguoja į vartotojo veiksmus ir valdo būseną. | Komponentai veikė teisingai, būsenos valdymas per „React Hooks“ buvo stabilus. | Sėkmingas | |
| T-03 | FR-09 | Vienetinis (unit) | Vertinimo rezultatų skaičiavimo funkcijos testavimas su skirtingais atsakymų deriniais. | Teisingai apskaičiuojamas bendras atitikties procentas ir kiekvieno klausimų bloko rezultatai. | Visi skaičiavimai buvo tikslūs, blokų ir bendras rezultatas sutapo su rankiniu skaičiavimu. | Sėkmingas | |
| T-04 | FR-03, FR-05 | Integracinis | Kritiškumo klasifikavimo ir klausimyno integracijos testas. | Klausimynas startuoja pagal klasifikavimo rezultatą, perduodami teisingi parametrai. | Klasifikavimo rezultatai teisingai perduodami klausimyno komponentui, startas vyksta pagal numatytą logiką. | Sėkmingas | |
| T-05 | FR-05, FR-06, FR-09 | Integracinis | Klausimyno ir rezultatų komponentų integracijos testavimas. | Atsakymai perduodami rezultatų komponentui, rezultatai skaičiuojami ir atvaizduojami teisingai. | Atsakymai buvo perduodami korektiškai, rezultatai apskaičiuoti ir atvaizduoti be neatitikimų. | Sėkmingas | |
| T-06 | FR-15, NFR-06 | Integracinis | „LocalStorage“ integracijos testas: vertinimų duomenų saugojimas, istorijos valdymas ir atkūrimas po naršyklės perkrovimo. | Duomenys išsaugomi tarp sesijų, istorija valdoma teisingai, duomenys atkuriami po perkrovimo. | Duomenys buvo patikimai saugomi ir atkuriami, istorija atvaizduojama chronologiškai, praradimų nefiksuota. | Sėkmingas | |
| T-07 | FR-01, FR-02 | Sistemos / priėmimo | Autentifikacijos ir autorizacijos testas su keturiais testiniais vartotojais („superadmin“, „auditor“, „editor“, | Teisingi duomenys leidžia prisijungti, neteisingi duomenys rodo klaidą, rolės mato skirtingus funkcionalumus. | Sistema priėmė visus keturis vartotojus pagal numatytas roles, neteisingi | Sėkmingas | Atsijungimas grąžino į prisijungimo puslapį, sesijos duomenys buvo ištrinami. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | „readonly“) ir neteisingais duomenimis. | | duomenys grąžino klaidos pranešimą. | | |
| T-08 | FR-03 | Sistemos / priėmimo | Subjekto kritiškumo nustatymo formos testavimas, tikrinant laukus, privalomumą, validaciją ir algoritmo veikimą. | Forma turi visus laukus, privalomi laukai tikrinami, klasifikavimo algoritmas veikia su visais deriniais. | Visi laukų ir validacijos kriterijai buvo patenkinti, algoritmas veikė korektiškai skirtingais scenarijais. | Sėkmingas | Pradiniame variante trūko aiškaus statuso pagrindimo – tai patobulinta. |
| T-09 | FR-05 | Sistemos / priėmimo | Klausimų blokų navigacijos testas, įskaitant laisvą perėjimą tarp blokų. | Vartotojas gali pereiti tarp blokų, duomenys išsaugomi, navigacija sklandi. | Navigacija veikė sklandžiai, atsakymai neišnyko keičiant blokus. | Sėkmingas | |
| T-10 | FR-06, FR-07 | Sistemos / priėmimo | Atsakymų sistemos ir klausimų priklausomybių testas (5 atsakymo variantai, automatinis perėjimas, „praleista“ logika). | Visi atsakymo variantai veikia, automatinis perėjimas ir „praleista“ logika veikia pagal specifikaciją. | Atsakymų pasirinkimai ir automatinis perėjimas veikė teisingai, priklausantys klausimai buvo tvarkomi pagal logiką. | Sėkmingas | Ankstesnė problema, kai priklausomi klausimai nebuvo praleidžiami, išspręsta patobulinus priklausomybių logiką. |
| T-11 | FR-08 | Sistemos / priėmimo | Pildymo progreso atvaizdavimo testas klausimų blokuose ir bendro progreso juostoje. | Progresas skaičiuojamas ir atvaizduojamas tiksliai, atnaujinamas realiu laiku. | Progreso indikatoriai buvo tikslūs ir atsinaujino kiekvieno atsakymo metu. | Sėkmingas | |
| T-12 | FR-09 | Sistemos / priėmimo | Rezultatų apdorojimo testas: bendras atitikties procentas, blokų rezultatai, atsakymų statistika ir grafinė vizualizacija. | Visi rezultatai ir grafikai atitinka apskaičiuotas reikšmes. | Bendri ir blokų rezultatai bei statistika buvo teisingi, vizualizacija atitiko skaičiavimus. | Sėkmingas | |
| T-13 | FR-11 | Sistemos / priėmimo | Diegimo plano generavimo testas pagal neįvykdytas priemones ir jų kategorijas. | Sugeneruojami veiksmai pagal neįvykdytas priemones, su kategorijomis (TECHNINĖ, ORGANIZACINĖ) ir aprašais. | Diegimo planas buvo sugeneruotas korektiškai, priemonės kategorizuotos ir aprašytos. | Sėkmingas | |
| T-14 | FR-15 | Sistemos / priėmimo | Vertinimų istorijos valdymo testas: | Istorija rodoma chronologiškai, | Istorijos atvaizdavima | Sėkmingas | PDF formato |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | chronologija, rezultatų atvaizdavimas, PDF eksportas iš istorijos įrašų. | pasirinkus įrašą rodomi pilni rezultatai, veikia PDF eksportas iš istorijos. | s ir rezultatų atkūrimas veikė teisingai, PDF eksportas iš istorijos veikė techninė prasme. | | tinkamumas vertintas atskirai per FR-12 testą. |
| T-15 | FR-12 | Sistemos / priėmimo | Rezultatų ir diegimo plano PDF eksporto funkcijos testavimas. | Sugeneruotas PDF turi pilnus rezultatus ir diegimo planą tvarkingu formatu. | PDF generavimas veikė, tačiau dokumento formatas netinkamai atvaizdavo turinį, ypač ilgesnius sąrašus. | Iš dalies sėkmingas | Lietuviški simboliai sukonfigūruoti per jsPDF, tačiau formato problemos neišspręstos – PDF eksporto atsisakyta MVP. |
| T-16 | NFR-01 | Nefunkcinis – našumas | Atsako laiko testas: puslapio įkėlimas, klausimų perjungimas, rekomendacijų generavimas, PDF generavimo trukmė. | Visi laikai neviršija nustatytų ribų (2 s, 500 ms, 2 s, 10 s). | Visi laiko kriterijai buvo patenkinti, matuota naršyklės „developer tools“ ir „performance API“. | Sėkmingas | |
| T-17 | NFR-02 | Nefunkcinis – duomenų valdymas | Sistemos elgsena su maksimaliai numatytu duomenų kiekiu (~200 eilučių priemonių, klausimų, diegimo plano įrašų). | Sistema veikia be pastebimo našumo praradimo ar sutrikimų. | Sistema veikė sklandžiai, užstrigimų ar reikšmingo lėtėjimo nefiksuota. | Sėkmingas | |
| T-18 | NFR-04 | Nefunkcinis – naudotojo sąsaja | Naudotojo sąsajos aiškumo ir suderinamumo testas „Chrome“ ir „Edge“ naršyklėse bei skirtingose rezoliucijose. | Sąsaja aiški, veikia abiejose naršyklėse ir skirtingais ekrano dydžiais. | Sąsaja buvo intuityvi, funkcijos pasiekiamos, rodymo klaidų tarp naršyklių nefiksuota. | Sėkmingas | |
| T-19 | NFR-06 | Nefunkcinis – duomenų saugojimas | Duomenų išlaikymo tarp sesijų testavimas naudojant „localStorage“. | Duomenys po naršyklės perkrovimo ar uždarymo išlieka ir atkuriami. | Duomenų išlaikymas veikė patikimai, suderinta su T-06 integraciniu testu. | Sėkmingas | |

Testavimo metu identifikuotos problemos: kritiškumo statuso pagrindimo trūkumas, neteisingas dalies priklausomų klausimų apdorojimas ir lietuviškų simbolių bei formato problemos PDF faile – buvo arba išspręstos (patobulinta klasifikavimo ir priklausomybių logika, sukonfigūruotas lietuviškų simbolių palaikymas), arba sąmoningai pažymėtos kaip MVP apribojimai, numatant jų sprendimą vėlesniuose įrankio plėtojimo iteracijų etapuose.

13 lentelė. **Identifikuotos problemos ir sprendimai.**

| **Problemos ID** | **Aprašymas** | **Sprendimas / sprendimo statusas** |
|---|---|---|
| P-01 | Kritiškumo vertinimo formoje nebuvo pateikiamas aiškus statuso priskyrimo pagrindimas. | Patobulinta klasifikacijos logika ir išplėstas pagrindimo tekstas, dabar pateikiamas aiškus statuso paaiškinimas. |
| P-02 | Klausimų priklausomybių valdyme priklausomi klausimai ne visada buvo teisingai praleidžiami atsakius „NE“ į pagrindinį klausimą. | Patobulintas priklausomybių algoritmas, užtikrinantis teisingą priklausomų klausimų apdorojimą skirtingais scenarijais. |
| P-03 | PDF generavimo funkcijoje lietuviški simboliai ir dokumento formatas nebuvo teisingai atvaizduojami. | Sukonfigūruotas jsPDF lietuviškiems simboliams, tačiau formato problemos liko – nuspręsta atsisakyti PDF eksporto MVP etape. |

### 4.5. Apibendrinimas

TIS2 atitikties vertinimo įrankio kūrimas nuosekliai įgyvendino trečiajame skyriuje suformuluotus funkcinius, nefunkcinius ir techninius reikalavimus bei praktiškai realizavo pasiūlytą įrankio koncepciją. Pasirinkta kliento pusės vieno puslapio aplikacijos (SPA) architektūra su „React“ ir „TypeScript“ pasiteisino MVP kontekste, ji užtikrino greitą reakcijos laiką, sklandžią naudotojo patirtį, adaptyvaus klausimyno logikos vykdymą kliento pusėje ir leido išvengti sudėtingos serverinės infrastruktūros. Tipais grįsta „TypeScript“ aplinka ir „React Hooks“ būsenos valdymas leido sukurti aiškią, modulinę ir lengvai prižiūrimą aplikacijos architektūrą, sumažinant programavimo klaidų tikimybę.

Įrankio funkcionalumas buvo realizuotas keturiais pagrindiniais komponentais: subjekto kritiškumo vertinimo forma, adaptyviu vertinimo klausimynu, rezultatų skaičiavimo ir vizualizavimo moduliu bei trūkumų šalinimo (įgyvendinimo) plano generatoriumi. Kiekvienas iš šių komponentų turi aiškiai apibrėžtas duomenų struktūras, atitinkančias funkcinius reikalavimus (FR-03, FR-05–FR-09, FR-11, FR-15), ir veikia kaip atskiras „React“ komponentas, integruojamas per pagrindinį „App“ modulį.

Klasifikacijos algoritmas realizuoja TIS2 direktyvos logiką (CER subjektai, specialūs subjektai, I ir II priedų sektoriai, dydžio slenksčiai, specifinė reikšmė), o klausimyno priklausomybės ir atsakymų tipų sistema leidžia įgyvendinti adaptyvų vertinimą. Rezultatų skaičiavimo funkcionalumas ir WBS principu grįstas įgyvendinimo planas transformuoja atsakymus į konkrečius techninius ir organizacinius veiksmus, taip užtikrinant perėjimą nuo atitikties vertinimo prie praktinio kibernetinio saugumo priemonių diegimo.

Testavimo planas ir jo įgyvendinimas patvirtino, kad įrankis atitinka trečiajame skyriuje nustatytų priėmimo kriterijų. Vienetiniai ir integraciniai testai parodė, kad kritiškumo klasifikavimo logika, klausimyno priklausomybės, atsakymų saugojimas ir rezultatų skaičiavimas veikia stabiliai ir be loginių klaidų. Sisteminiai ir priėmimo testai patvirtino autentifikacijos, klausimų blokų navigacijos, progreso atvaizdavimo, rezultatų statistikos ir įgyvendinimo plano generavimo funkcionalumą. Nefunkcinių reikalavimų testavimas (našumo, duomenų tvarkymo, naudotojo sąsajos aiškumo ir duomenų išsaugojimo) parodė, kad įrankis užtikrina pakankamą reakcijos laiką, išlieka stabilus dirbant su didesniais duomenų kiekiais ir patikimai saugo vertinimo informaciją „localStorage“. Testavimo metu identifikuotos problemos buvo iš esmės išspręstos, išskyrus PDF eksporto formato kokybę, nuo kurios MVP etape atsisakyta.

Parengtas TIS2 atitikties vertinimo MVP įrankis techniškai įgyvendino teorinėje dalyje suformuotą metodiką ir praktiškai patvirtino jog į reikalavimus ir priemones orientuotas klausimynas su vertinimo pagrindu parengtu įgyvendinimo planu gali tapti naudinga praktine priemone organizacijoms, siekiančioms atitikti TIS2 reikalavimų.

# 5. Bendrosios išvados ir pasiūlymai

Baigiamajame darbe buvo siekiama sujungti teorinį TIS2 direktyvos, įtrauktos į Lietuvos Respublikos kibernetinio saugumo įstatymą, pagrindą su praktiniu, įrankiu grįstu požiūriu į kibernetinio saugumo atitikties vertinimą. Šiame skyriuje apibendrinamos pagrindinės darbo išvados, aptariami ribotumai ir pateikiami pasiūlymai praktikai bei tolesniems tyrimams.

## 5.1. Bendrosios išvados

1. Atlikta kibernetinio saugumo standartų ir ES reguliavimo palyginamoji analizė parodė, kad TIS2 nėra vakuume egzistuojantis kibernetinio saugumo reguliacinis karkasas, o nuoseklus pratęsimas anksčiau sukurtų kibernetinio saugumo vertinimo ir valdymo modelių (ISO/IEC 27001, NIST CSF, DORA ir kt.). Nors skirtingi standartai pasižymi nevienodu detalumo lygiu, sektorių fokusu ir kontrolės priemonių formulavimu, juos sieja bendri principai: rizikos pagrindu grindžiamas valdymas, valdymo ir organizacinių priemonių integracija su techniniais sprendiniais bei tiekimo grandinės saugumo akcentavimas, nuolatinio tobulinimo ciklas.

2. Išanalizavus TIS2 reikalavimus Lietuvos KSĮ taikymo rėmuose, galima teigti, kad TIS2, įgyvendinimo reglamentas ir KSĮ suformuoja visuminį kibernetinio saugumo valdymo modelį, apimantį ne tik technines, bet ir vadovybės atsakomybės, rizikų, incidentų, tiekimo grandinės bei veiklos tęstinumo dimensijas. Analizės metui paaiškėjo, jog praktiškai nėra būdo be antrinių šaltinų teisės aktų formuluotes paversti konkrečiomis organizacinėmis ir techninėmis priemonėmis, tam tikslui pasitarnavo ENISA gairės ir analitinės ataskaitos, Krašto apsaugos ministerijos Kibernetinio saugumo reikalavimų aprašas, Nacionalinio kibernetinio saugumo centro gairės, kurie tapo teoriniu karkasu, leidusiu interpretuoti TIS2 reikalavimus. Atlikta analizė pagrindė poreikį metodiniams ir technologiniams sprendimams, padedantiems sujungti teisės aktų tekstą ir praktinį įgyvendinimą.

3. Ištyrus TIS2 atitikties vertinimo įrankių pasiūlą, išryškėjo projektuojamo adaptyvaus TIS2 vertinimo įrankio aktualumas, nes rinkoje vyrauja nevienalytės metodikos: minimalūs savianalizės klausimynai, resursams imlios GRC platformos, skirtos brandžioms didelėms organizacijoms, gamintojų instrumentai, susieti su konkrečiomis ekosistemomis ir menkai pritaikomi priežiūros/teisinio reguliavimo logikai ir kibernetinio saugumo standartų siejimo su TIS2 šablonai, orientuoti į stambias organizacijas, kurios jau yra įsidiegusios bent vieną atitinkamą standartą. Rezultatai parodė, jog mažoms ir vidutinėms organizacijoms, pradedančioms TIS2

kelią, trūksta praktiško, rizika ir proporcingumu grįsto, ne ekspertams suprantamo instrumento, kuris kartu pateiktų struktūruotas trūkumų šalinimo rekomendacijas.

4. Susisteminus antrame skyriuje atliktą teorinę TIS2 reikalavimų analizę nustatyta, kad trijų komponentų struktūra sudaro nuoseklų metodinį pagrindą TIS2 nuostatoms transformuoti į praktiškai vykdomą organizacijos kibernetinio saugumo vertinimo procesą, užtikrinant aiškią seką nuo taikymo srities nustatymo iki korekcinių veiksmų planavimo. Subjekto kibernetinio statuso identifikavimo komponentas, remdamasis TIS2 direktyvoje apibrėžtais kriterijais ir subjektų klasifikavimo logika, leidžia nustatyti organizacijos patekimą į TIS2 taikymo sritį. Vertinimo klausimyno komponentas apima esminius TIS2 įgyvendinimo priemonių imperatyvus ir juos operacionalizuoja vertinamais klausimais, susiedamas teisinius reikalavimus su organizacinėmis ir techninėmis saugumo priemonėmis bei sudarydamas prielaidas sisteminiam spragų identifikavimui. Trūkumų šalinimo įgyvendinimo plano komponentas, remdamasis vertinimo rezultatais, suformuoja nustatytų neatitikčių šalinimo veiksmų ir įgyvendinimo žingsnių seką, orientuotą į praktiškai įgyvendinamą TIS2 reikalavimų įgyvendinimą organizacijoje.
5. Technologiniu lygmeniu vieno puslapio aplikacijos architektūra, realizuota naudojant „React“ karkasą, sudarė sąlygas įgyvendinti dinamišką vertinimo logiką, adaptyvų klausimyno veikimą ir nuoseklų vertinimo rezultatų apdorojimą, o komponentinė „React“ struktūra palengvino iteratyvų funkcionalumo tobulinimą ir greitą sprendinių koregavimą prototipo kūrimo metu. Atlikus prototipo testavimą buvo įsitikinta, kad aplikacija atitiko suformuluotus funkcinius ir nefunkcinius reikalavimus, o jos veikimas empiriškai patvirtino parengtos metodikos praktinį pritaikomumą. Pasiektas darbo tikslas – sukurtas metodologiškai pagrįstas TIS2 atitikties vertinimo prototipas, skirtas Lietuvos organizacijų kibernetinio saugumo vertinimui ir tinkamas naudoti kaip minimalus veikiantis produktas (MVP).

### 5.2. Tyrimo ir projekto ribotumai

1. TIS2 direktyvos įgyvendinimas ES valstybėse narėse ir KSĮ poįstatyminių aktų raida yra dinamiškas procesas. Tai reiškia, kad darbo metu suformuotas klausimyno ir priemonių įgyvendinimo modelis remiasi konkrečia teisine situacija tam tikru momentu. Vėlesni pakeitimai, pvz., naujos gairės, detalizuojantys nutarimai, privalomosios techninės priemonės, kt. nėra įtraukti ir tai reiškia kad įrankio turinys privalo būti nuolatos prižiūrimas ir atnaujinamas.

2. Praktiniame MVP įgyvendinime buvo realizuotas bazinis TIS2 vertinimas, orientuotas į bendruosius TIS2 reikalavimus. Į prototipą nebuvo integruotos specializuotos reikalavimų sritys,

kurios priklauso nuo sektoriaus ir (arba) subjekto specifikos, reglamentuotos atskirais, su TIS2 įgyvendinimu nesusijusiais reguliavimais ir (arba) įstatymais.

3. TIS2 reikalavimų įgyvendinimo priemonių rinkinio, parengtų klausimų, taip pat trūkumų šalinimo veiksmų turinys neišvengiamai priklauso nuo autoriaus interpretavimo. Nors šie elementai yra grindžiami TIS2, KSĮ ir susijusiais antriniais šaltiniais, galutinis struktūravimas vis dėlto atspindi autoriaus teisinės medžiagos interpretaciją. Skirtingi ekspertai, remdamiesi tais pačiais teisės aktais ir gairėmis, galėtų pateikti alternatyvų priemonių grupavimą, klausimų formuluotes, siūlomus įgyvendinimo etapus ir pan.

4. MVP koncepcijos ribotumas – pasikliovimas žmogiškuoju faktoriumi. Įrankis remiasi savianalize, t. y. organizacijos atstovas atsako į klausimus ir vertina priemonių įgyvendinimo būklę. Tai natūraliai sukuria subjektyvumo ir šališkumo riziką, kai organizacijos gali būti linkusios savo brandą vertinti palankiau, nei ji yra realybėje. Siekiant sumažinti šią riziką, ateityje būtina integruoti įrodymų pateikimo komponentą, leidžiantį atsakymus grįsti objektyviais dokumentais ir duomenimis. MVP stadijoje šis komponentas buvo tik iš dalies konceptualizuotas ir nebuvo įdiegtas įrankio logikoje.

5. Darbas neapima empirinio tyrimo, t.y. realių organizacijų naudojimo patirtis ir rezultatų analizės. Įrankio testavimas buvo orientuotas į MVP funkcionalumo patikrinimą, nėra daromos apibendrinančios išvados apie įrankio pritaikomumą skirtingų tipų organizacijose ir naudotojų patirties (pvz., suprantamumo, patogumo, pasitenkinimo) rodiklius.

6. MVP techninis prototipas buvo orientuotas į funkcionalumo demonstravimą ir įdiegtas vietinėje „Docker“ aplinkoje, todėl jis nėra parengtas diegimui į gamybinę aplinką. Siekiant publikuoti įrankį platesniam testavimui, būtina įgyvendinti vartotojų valdymo ir prieigos kontrolės, duomenų apsaugos, atsarginių kopijų bei kitus saugaus diegimo reikalavimus, atlikti atitinkamus saugumo testus ir kt.

### 5.3. Pasiūlymai praktikai

1. Praktiniam įrankio funkcionalumui svarbu įgyvendinti automatizuotą techninės atitikties įrodymų kaupimą. Viena iš perspektyviausių praktinės plėtros krypčių – įrankio integracija su techninių kibernetinio saugumo informacijos šaltiniais, pavyzdžiui Saugumo informacijos ir įvykių valdymo platformomis (angl. - *Security Information and Event Management,* SIEM) ir pan. Tai leistų sumažinti savianalizės subjektyvumą, automatizuotai atsakyti į dalį vertinimo klausimų,

transformuoti atitikties vertinimą iš epizodinio į nuolatinės stebėsenos metodą. Tokią integracija sudarytų prielaidą įrankio naudojimui stambiuose organizacijose.

2. Tolesniems tyrimams ir įrankio plėtrai siūloma atlikti empirinį įrankio testavimą organizacijose. Tai taptų pagrindu įvertinti klausimų formuluočių suprantamumą, išanalizuoti, kaip šio ar panašių įrankių naudotojo sąsajos sprendimai veikia vadovų ir specialistų suvokimą apie riziką ir prioritetus, bei patikrinti, ar priemonių įgyvendinimo planas ir jo detalizaciją atitinka realias įmonių organizacines ir technines praktikas.
3. Galiausiai, šio darbo rezultatai atveria keletą diskusinių klausimų, kuriuos verta toliau nagrinėti akademinėse ir ekspertų bendruomenėse. Pirmiausiai, ar TIS2 atitikties vertinimas turėtų būti labiau centralizuotas valstybės lygiu, turint omenyje plėtojama ENISA vertinimo įrankį, ar paliktas komercinės rinkos dalyviams. Kaip suderinti periodinę atitikties kontrolę ir priežiūrą su realia kibernetinio saugumo kokybe, kartu kritiškai vertinant atitikties siekimą kaip reiškinį, galintį uždengti tikrąsias problemas. Kokia apimtimi TIS2 reikalavimai apskritai apima kibernetinio saugumo sritį ir yra tinkami rizikos suvaldymui, ar organizacijos gali kliautis vien tik apibrėžtų reikalavimų priemonių įgyvendinimu kaip pilna apsauga.

# INFORMACIJOS ŠALTINIŲ SĄRAŠAS


[1] European Union Agency for Cybersecurity. (2024). *Threat landscape 2024*. Prieiga internete: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA Threat Landscape 2024_0.pdf

[2] European Commission. (2022). *Digital economy and society index (DESI) 2022*. Prieiga internete: https://digital-strategy.ec.europa.eu/en/policies/desi

[3] Nacionalinis kibernetinio saugumo centras. (2023). *Nacionalinė kibernetinio saugumo ataskaita 2023*. Prieiga internete: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf

[4] European Commission. *Pasiūlymas dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 (NIS2 Direktyva)*. Prieiga internete: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0019.02/DOC_1&format=PDF

[5] European Union Agency for Cybersecurity. (2022). *NIS investments 2022*. Prieiga internete: https://www.enisa.europa.eu/sites/default/files/publications/NIS Investments 2022.pdf

[6] Djebbar, F., & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. *IEEE Access*, 11, 85315–85332. https://doi.org/10.1109/ACCESS.2023.3303205

[7] National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

[8] National Institute of Standards and Technology. (2024). *Quick-start guide for creating and using organizational profiles* (NIST SP 1301). https://doi.org/10.6028/NIST.SP.1301

[9] Schellman. (2023). *NIST CSF vs. other cybersecurity frameworks: A comparative analysis*. Prieiga internete: https://www.schellman.com

[10] Cybersecurity and Infrastructure Security Agency. (2020, December 13). *Emergency directive 21-01: Mitigate SolarWinds Orion code compromise*. Prieiga internete: https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

[11] National Institute of Standards and Technology. (2021). *CVE-2021-44228 (Log4Shell)*. National Vulnerability Database. Prieiga internete: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[12] National Institute of Standards and Technology. (2023). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST SP 800-161r1-upd1). https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[13] National Institute of Standards and Technology. (n.d.). *NIST cybersecurity framework – Informative references*. Prieiga internete: https://www.nist.gov/cyberframework/informative-references

[14] European Securities and Markets Authority. (n.d.). *Digital operational resilience Act (DORA)*. Prieiga internete: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[15] European Parliament and Council. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. *Official Journal of the European Union*, L 333, 1–79. Prieiga internete: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[16] European Commission. (2024). *Commission delegated regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 with RTS on ICT risk management tools, methods, processes, policies and the simplified framework*. Prieiga internete: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/eng

[17] European Commission. (2024). *Commission delegated regulation (EU) 2024/1772 supplementing Regulation (EU) 2022/2554 with RTS on incident classification, materiality thresholds and reporting*. Prieiga internete: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401772

[18] European Commission. (2025). *Commission delegated regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554*. Prieiga internete: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R1190

[19] Digital Operational Resilience Act. (n.d.). *Harmonisation of conditions enabling the conduct of the oversight activities*. Prieiga internete: https://www.digital-operational-resilience-act.com/Article_41.html

[20] European Supervisory Authorities. (2024, July 17). *Final report on draft RTS specifying elements related to threat-led penetration tests (TLPT) under Article 26(11) of Regulation (EU) 2022/2554 (DORA)* (JC 2024-29). Prieiga internete: https://www.esma.europa.eu/document/final-report-draft-rts-specifying-elements-related-threat-led-penetration-tests

[21] European Commission. (2024). *Commission delegated regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities*. Prieiga internete: https://eur-lex.europa.eu/eli/reg_del/2024/1502/oj

[22] International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (ISO/IEC 27001:2022).

[23] International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection – Information security controls* (ISO/IEC 27002:2022). Geneva: ISO.

[24] Businessmap. (n.d.). *What is PDCA cycle*. Prieiga internete: https://businessmap.io/lean-management/improvement/what-is-pdca-cycle

[25] Phoenix Security. (n.d.). *DORA implementation guide*. Prieiga internete: https://phoenix.security/dora-implementation/

[26] International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information security management*. Geneva: ISO.

[27] International Organization for Standardization. (2022). ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection: Guidance on managing information security risks. ISO.

[28] ISMS.online. (n.d.). ISO 27001:2022 – The Statement of Applicability (SoA). ISMS.online. Prieiga internete: https://www.isms.online/iso-27001/statement-of-applicability/

[29] ResearchGate. (n.d.). *The ISO/IEC 27-001 implementation clauses*. Prieiga internete: https://www.researchgate.net/figure/The-ISO-IEC-27-001-implementation-clauses_fig4_368402249

[30] European Parliament, & Council of the European Union. (2022). *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. *Official Journal of the European Union*. Prieiga internete: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[31] European Commission. (2024). *Commission implementing regulation (EU) 2024/2690 of 17 October 2024 laying down technical and methodological requirements concerning cybersecurity risk-management measures*. *Official Journal of the European Union*, L 2024/2690. Prieiga internete: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

[32] European Union Agency for Cybersecurity. (2025). *NIS2 technical implementation guidance*. Prieiga internete: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[33] European Union Agency for Cybersecurity. (2025). *Cybersecurity roles and skills for NIS2 essential and important entities*. Prieiga internete: https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-nis2

[34] Lietuvos Respublika. (2024). *Kibernetinio saugumo įstatymas Nr. XIII-1742*. Teisės aktų registras. Prieiga internete: https://www.tar.lt

[35] National Institute of Standards and Technology. (2024). *Quick-start guide for using the CSF tiers* (NIST SP 1302). https://doi.org/10.6028/NIST.SP.1302

[36] Cyberday. (2025). *Comparing EU cybersecurity frameworks: NIS2, GDPR, DORA and ISO 27001*. Prieiga internete: https://www.cyberday.ai/blog/comparing-eu-cybersecurity-frameworks

[37] Spector Consulting Group. (2025). *ISO 27001 vs NIS2 and DORA: Aligning compliance strategies*. Prieiga internete: https://www.spector.ie/blog/iso27001-nis2-dora/

[38] European Union Agency for Cybersecurity. (2024). *2024 report on the state of cybersecurity in the Union (condensed version)*. Prieiga internete: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[39] European Union Agency for Cybersecurity. (2025). *ENISA NIS360 – 2024: ENISA cybersecurity maturity & criticality assessment of NIS2 sectors*. Prieiga internete: https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA - NIS360 - 2024_0.pdf

[40] European Union Agency for Cybersecurity. (2025). *The EU cybersecurity index 2024 (EU-CSI)*. Prieiga internete: https://www.enisa.europa.eu/sites/default/files/2025-06/The EU Cybersecurity Index 2024_en_0.pdf

[41] Lietuvos Respublikos Vyriausybė & Krašto apsaugos ministerija. (2018/2024). *Kibernetinio saugumo politika ir gairės*. Prieiga internete: https://kam.lt/wp-content/uploads/2024/12/TIS2-brosiura_Pilnas_2024-11-29.pdf

[42] Lietuvos Respublika. (n.d.). *Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo*. Prieiga internete: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[43] Lietuvos Respublika. (n.d.). *Nacionaliniams saugumui svarbių objektų apsaugos įstatymas*. Teisės aktų registras. Prieiga internete: https://www.e-tar.lt/portal/lt/legalAct/TAR.57E0E8B29108/asr

[44] European Union. (2019). *Cybersecurity regulation (EU) 2019/881*. Prieiga internete: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[45] European Union Agency for Cybersecurity. (2025). *ENISA Technical Implementation Guidance Mapping table version 1.2* Prieiga internete: https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA_Technical_Implementation_Guidance_Mapping_table_version_1.2.xlsx

[46] ResearchGate. (n.d.). *Cybersecurity in the EU: The role of ENISA and the NIS2 Directive*. Prieiga internete: https://www.researchgate.net/publication/395950686_Cybersecurity_in_the_EU_The_Role_of_ENISA_and_the_NIS2_Directive

[47] European Union Agency for Cybersecurity. (2025). *Cyber hygiene in the health sector*. Prieiga internete: https://www.enisa.europa.eu/topics/cyber-hygiene-health-sector

[48] European Union Agency for Cybersecurity. (2025). *Cybersecurity of critical sectors*. Prieiga internete: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors

[49] European Union Agency for Cybersecurity. (n.d.). *Handbook for cyber stress tests*. Prieiga internete: https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

[50] Krašto apsaugos ministerija. (n.d.). *Kibernetinio saugumo įstatymas*. Prieiga internete: https://kam.lt/kibernetinio-saugumo-istatymas

[51] Nacionalinis kibernetinio saugumo centras. (n.d.). *Rekomendacijos kasmentiniam rizikų vertinimui*. Prieiga internete: https://www.nksc.lt/doc/biuleteniai/Rekomendacija 4 - leidinys.pdf

[52] Lietuvos Respublikos Vyriausybė. (2023). *Nacionalinis kibernetinių incidentų valdymo planas*. Prieiga internete: https://lrv.lt/media/viesa/saugykla/2023/7/rdx1ABttksU.pdf

[53] Nacionalinis kibernetinio saugumo centras. (n.d.). *Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumento (-ų) galimas turinys*. Prieiga internete: https://www.nksc.lt/doc/Tinklu_ir_informaciniu_sistemu_kibernetinio_saugumo_politikos_dokumento_galimas_turinys.pdf

[54] InvoSec. (n.d.). *Kibernetinio saugumo reikalavimų aprašas (KSRA)*. Prieiga internete: https://invosec.lt/lt/ksra/tis-saugumo-politika/

[55] European Union. (2022). *Directive (EU) 2022/2557 – Critical entities resilience directive (CER)*. Prieiga internete: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[56] European Union. (2014/2024). *Regulation (EU) No. 910/2014 ir jo atnaujintas variantas Regulation (EU) 2024/1183*. Prieiga internete: https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[57] European Union. (2018). *Directive (EU) 2018/1972 of the European Parliament and of the Council, establishing the European Electronic Communications Code*. Prieiga internete: https://eur-lex.europa.eu/eli/dir/2018/1972/oj

[58] Cyberday. (n.d.). *Free NIS2 Directive compliance assessment*. Prieiga internete: https://www.cyberday.ai/assessment/nis2-directive

[59] Cyberday. (n.d.). *NIS2 framework*. Prieiga internete: https://www.cyberday.ai/frameworks/nis2-directive

[60] Advisera. (n.d.). *NIS2 gap analysis tool*. Prieiga internete: https://advisera.com/tools/nis-2-gap-analysis-tool/

[61] Inclus. (n.d.). *NIS2 maturity gap analysis template*. Prieiga internete: https://inclus.com/templates/nis2-gap

[62] Thales. (n.d.). *Achieve NIS2 compliance with Thales' self-assessment tool*. Prieiga internete: https://cds.thalesgroup.com/en/hot-topics/achieve-nis2-compliance-thales-self-assessment-tool

[63] ServiceNow. (n.d.). *Governance, risk and compliance (GRC)*. Prieiga internete: https://www.servicenow.com/products/governance-risk-and-compliance.html

[64] BMC. (n.d.). *BMC Remedy Control-M: Risk management and financial automation*. Prieiga internete: https://www.bmc.com/it-solutions/finance-automation/risk-management.html

[65] European Union Agency for Cybersecurity. (n.d.). *Cybersecurity maturity assessment for small and medium enterprises*. Prieiga internete: https://tools.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises

[66] Dataguard. (n.d.). *ISO 27001 mapping*. Prieiga internete: https://www.dataguard.com/nis2/iso-27001-mapping

[67] BSI Group. (n.d.). *BSI mapping tool – ISO/IEC 27001 and NIS2*. Prieiga internete: https://www.bsigroup.com/globalassets/localfiles/de-de/isoiec-27001/ressourcen/bsi-ce-nis2-mapping-tool-25-en-de.pdf

[68] Trescudo Cybersecurity. (n.d.). *NIS2, NIST CSF mapping*. Prieiga internete: https://trescudo.com/assets/notices/nis2_nist_csf_mapping.pdf

[69] European Union Agency for Cybersecurity. (n.d.). *European cybersecurity skills framework (ECSF)*. Prieiga internete: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

[70] European Union Agency for Cybersecurity. (n.d.). *Good practice guide for incident management*. Prieiga internete: https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

[71] European Union Agency for Cybersecurity. (n.d.). *Good practices for supply chain cybersecurity*. Prieiga internete: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[72] European Union Agency for Cybersecurity. (n.d.). *Awareness and cyber hygiene*. Prieiga internete: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene

[73] Nacionalinis kibernetinio saugumo centras. (n.d.). *Kibernetinio saugumo centro rekomendacijos kibernetinio saugumo subjektams*. Prieiga internete: https://www.nksc.lt/doc/NKSC_rekomendacijos_kibernetinio_saugumo_subjektams.pdf

[74] European Union Agency for Cybersecurity. (n.d.). *Cryptography*. Prieiga internete: https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography

[75] Microsoft. (2025). *Microsoft secure score*. Prieiga internete: https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score

[76] Amazon Web Services. (n.d.). *Standards reference for Security Hub CSPM*. Prieiga internete: https://docs.aws.amazon.com/securityhub/latest/userguide/standards-reference.html

[77] Microsoft. (n.d.). *Microsoft 365 secure score enterprise playbook*. Prieiga internete: https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score

[78] Splunk. (n.d.). *Risk notable playbook pack descriptions*. Prieiga internete: https://help.splunk.com/en/splunk-enterprise-security-8/security-content-update/how-to-use-splunk-security-content/5.13/use-splunk-soar-playbooks-and-workbooks-from-the-risk-notable-playbook-pack/see-descriptions-of-playbooks-in-the-risk-notable-playbook-pack

[79] WatchGuard. (n.d.). *Automated continuous compliance*. Prieiga internete: https://www.watchguard.com/wgrd-products/compliance-reports

[80] Project Management Institute. (n.d.). *Work breakdown structure (WBS): Basic principles*. Prieiga internete: https://www.pmi.org/learning/library/work-breakdown-structure-basic-principles-4883

[81] Pakki, N. R. (2016). *Managing quality requirements in requirements engineering process* [Master's thesis]. University of Skövde.

[82] IEEE. (1998). *IEEE Std 830-1998: IEEE recommended practice for software requirements specifications*. IEEE Computer Society.

[83] ACM SIGSOFT. (1995). SMART requirements. *Software Engineering Notes*, 20(2).

[84] Object Management Group. (2017). *OMG unified modeling language (OMG UML), Version 2.5.1* (OMG Document Number: formal/2017-12-05). Prieiga internete: https://www.omg.org/spec/UML/2.5.1/

[85] Rumbaugh, J., Jacobson, I., & Booch, G. (2004). *The unified modeling language reference manual* (2nd ed.). Addison-Wesley Professional.

[86] Schmidt, D. C. (2006). Model-driven engineering. *Computer*, 39(2), 25–31. https://doi.org/10.1109/MC.2006.58

[87] Mellor, S. J., Scott, K., Uhl, A., & Weise, D. (2004). *MDA distilled: Principles of model-driven architecture*. Addison-Wesley Professional.

[88] Jacobson, I., Christerson, M., Jonsson, P., & Övergaard, G. (1992). *Object-oriented software engineering: A use case driven approach*. Addison-Wesley.

[89] Cockburn, A. (2001). *Writing effective use cases*. Addison-Wesley Professional.

[90] Eriksson, H. E., & Penker, M. (2000). *Business modeling with UML: Business patterns at work*. John Wiley & Sons.

[91] Fowler, M. (2003). *UML distilled: A brief guide to the standard object modeling language* (3rd ed.). Addison-Wesley Professional.

[92] Cheesman, J., & Daniels, J. (2000). *UML components: A simple process for specifying component-based software*. Addison-Wesley Professional.

[93] Bass, L., Clements, P., & Kazman, R. (2012). *Software architecture in practice* (3rd ed.). Addison-Wesley Professional.

[94] Larman, C. (2004). *Applying UML and patterns: An introduction to object-oriented analysis and design and iterative development* (3rd ed.). Prentice Hall.

[95] Booch, G., Rumbaugh, J., & Jacobson, I. (2005). *The unified modeling language user guide* (2nd ed.). Addison-Wesley Professional.

[96] Stevens, P., & Pooley, R. (2006). *Using UML: Software engineering with objects and components* (2nd ed.). Addison-Wesley.

[97] Yu, E. S. (1997). Towards modelling and reasoning support for early-phase requirements engineering. In *Proceedings of the third IEEE international symposium on requirements engineering* (pp. 226–235).

[98] Van Der Aalst, W. M. (2016). *Process mining: Data science in action* (2nd ed.). Springer.

[99] Taylor, R. N., Medvidovic, N., & Dashofy, E. M. (2009). *Software architecture: Foundations, theory, and practice*. John Wiley & Sons.

[100] Sommerville, I. (2015). *Software engineering* (10th ed.). Pearson.

[101] Adobe. (2023, July 19). *Single-page applications (SPAs) – what they are and how they work*. Adobe Business. Prieiga internete: https://business.adobe.com/blog/basics/learn-the-benefits-of-single-page-apps-spa

[102] React. (n.d.). *Quick start – React documentation*. Prieiga internete: https://react.dev/learn

[103] Vue.js. (n.d.). *Introduction – Vue.js 3 documentation*. Prieiga internete: https://vuejs.org/guide/introduction

[104] Angular. (n.d.). *What is Angular?* Prieiga internete: https://angular.dev/overview

[105] TypeScript. (n.d.). *TypeScript: JavaScript with syntax for types*. Microsoft. Prieiga internete: https://www.typescriptlang.org/

[106] React. (n.d.). *React reference – Hooks API*. Prieiga internete: https://react.dev/reference/react

[107] Jest. (2025, June 10). *Getting started – Jest documentation*. Prieiga internete: https://jestjs.io/docs/getting-started

[108] Testing Library. (2024, June 3). *Introduction – React Testing Library*. Prieiga internete: https://testing-library.com/docs/react-testing-library/intro/

[109] TypeScript. (n.d.). *The starting point for learning TypeScript – Documentation*. Microsoft. Prieiga internete: https://www.typescriptlang.org/docs/

# PRIEDAI

## 1. Teisės aktai susiję su TIS2 perkėlimu į Lietuvos teisinę sistemą

| Lygmuo | Teisės aktas (Nr., data, URL) |
|---|---|
| ES | Direktyva (ES) 2022/2555 (TIS2), 2022-12-14<br>URL: https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32022L2555 |
| ES | Komisijos įgyvendinimo reglamentas (ES) 2024/2690, 2024-10-17<br>URL: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32024R2690 |
| Seimo įstatymas | Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428 (2014-12-11; nauja redakcija nuo 2024-10-18)<br>URL: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/NBYwOzbGen |
| | |
| Seimo įstatymas | KS įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIV-2902, 2024-07-11<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/1a8657f2427a11efb121d2fe3a0eff27 |
| Seimo įstatymas | Aviacijos įstatymo Nr. VIII-2066 41 str. pakeitimo įstatymas Nr. XIV-2903, 2024-07-11<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a02a44b2427b11efb121d2fe3a0eff27 |
| Seimo įstatymas | Administracinių nusižengimų kodekso 479, 480 ir 589 str. ir priedo pakeitimo įstatymas Nr. XIV-2904, 2024-07-11<br>URL: https://www.teisesakturegistras.lt/portal/lt/legalAct/c6afa0a049bd11efbdaea558de59136c |
| Seimo įstatymas | Elektroninių ryšių įstatymo Nr. IX-2135 3, 8, 23, 36, 44, 45, 51, 74, 82, 98 straipsnių ir priedo pakeitimo įstatymas Nr. XIV-2905, 2024-07-11<br>URL: https://www.e-tar.lt/portal/lt/legalAct/28bb929049be11efbdaea558de59136c |
| Seimo įstatymas | Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo Nr. IX-1132 1, 2, 13 ir 18 straipsnių pakeitimo įstatymas Nr. XIV-2906, 2024-07-11<br>URL: https://e-tar.lt/mobile/legalAct.html?documentId=7329ae2049be11efbdaea558de59136c&lang=lt |
| Seimo įstatymas | Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo Nr. XIII-1120 4 straipsnio pakeitimo įstatymas Nr. XIV-2907, 2024-07-11<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/50bccb30427d11efb121d2fe3a0eff27 |
| Seimo įstatymas | Valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 3, 4, 5, 7, 14, 15, 26, 27, 39, 41, 42, 43 ir 46 straipsnių pakeitimo įstatymas Nr. XIV-2908, 2024-07-11<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/8d0eb032427d11efb121d2fe3a0eff27 |
| Seimo įstatymas | Viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 37, 47 ir 87 straipsnių pakeitimo įstatymas Nr. XIV-2909, 2024-07-11<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/cd56d5a3427d11efb121d2fe3a0eff27 |
| Vyriausybės nutarimas | LR Vyriausybės 2018-08-13 nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (aktuali suvestinė redakcija, pakeista nutarimu Nr. 945, 2024-11-06)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f |
| Vyriausybės nutarimas - Nutarimo Nr. 818 priedas | Nacionalinis kibernetinių incidentų valdymo planas (Nutarimo Nr. 818 priedas)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f |
| Vyriausybės patvirtinta Nutarimo Nr. 818 priedas | Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodika (Nutarimo Nr. 818 priedas)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f |
| Vyriausybės patvirtintas Nutarimo Nr. 818 priedas | Kibernetinio saugumo reikalavimų aprašas (Nutarimo Nr. 818 priedas)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f |
| Vyriausybės patvirtintas Nutarimo Nr. 818 priedas | Vykdymo užtikrinimo priemonių taikymo kibernetinio saugumo subjektams tvarkos aprašas (Nutarimo Nr. 818 priedas)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f |
| Seimo nutarimas | Nacionalinio saugumo strategija (Seimo nutarimas Nr. IX-907)<br>URL: https://www.e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2 |
| Seimo nutarimas | Krašto apsaugos sistemos stiprinimo ir plėtros programa (Seimo nutarimas Nr. XIV-2505, 2024-03-21)<br>URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e3acb430e78f11ee9fdedfc979ae62a9 |
| | |

## 2. LR Kibernetinio Saugumo Įstatymo sektorių priedai.

2.1.YPATINGOS SVARBOS SEKTORIAI.

| Sektorius | Subsektorius | Subjekto rūšis | Institucija, atsakinga už identifikavimą |
|---|---|---|---|
| 1. Energetika | 1.1. Elektra | 1.1.1. Elektros energetikos įmonės, atliekančios elektros energijos tiekimo funkciją. | Lietuvos Respublikos energetikos ministerija |
| | | 1.1.2. Elektros energijos skirstomųjų tinklų operatorius. | Energetikos ministerija |
| | | 1.1.3. Elektros energijos perdavimo sistemos operatorius. | Energetikos ministerija |
| | | 1.1.4. Elektros energijos gamintojas. | Energetikos ministerija |
| | | 1.1.5. Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/943 dėl elektros energijos vidaus rinkos 2 straipsnio 8 punkte. | Energetikos ministerija |
| | | 1.1.6. Elektros energijos rinkos dalyviai, kaip apibrėžta Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys elektros energijos paklausos telkimo, energijos kaupimo paslaugas ir elektros energijos reguliavimo apkrovos paslaugas. | Energetikos ministerija |
| | | 1.1.7. Elektromobilių įkrovimo prieigos operatoriai. | Energetikos ministerija |
| | 1.2. Centralizuotas šilumos ir vėsumos tiekimas | 1.2.1. Centralizuoto šilumos ar vėsumos energijos tiekimo operatoriai. | Energetikos ministerija |
| | 1.3. Nafta | 1.3.1. Naftotiekį valdanti įmonė. | Energetikos ministerija |

| | | | |
|---|---|---|---|
| | | 1.3.2. Naftos gamybos įmonė.<br><br>Naftos perdirbimo įmonė.<br><br>Naftą importuojanti įmonė, naftą įvežanti įmonė, naftos atsargas kaupianti įmonė, naftos atsargas tvarkanti įmonė. | Energetikos ministerija |
| | | 1.3.3. Centrinė naftos produktus ir naftos atsargas kaupianti ir tvarkanti organizacija. | Energetikos ministerija |
| | 1.4. Dujos | 1.4.1. Gamtinių dujų tiekimo įmonė. | Energetikos ministerija |

| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už identifikavimą** |
|---|---|---|---|
| | | 1.4.2. Gamtinių dujų skirstymo sistemos operatorius. | Energetikos ministerija |
| | | 1.4.3. Gamtinių dujų perdavimo sistemos operatorius. | Energetikos ministerija |
| | | 1.4.4. Gamtinių dujų laikymo sistemos operatorius. | Energetikos ministerija |
| | | 1.4.5. Suskystintų gamtinių dujų sistemos operatorius. | Energetikos ministerija |
| | | 1.4.6. Gamtinių dujų įmonė. | Energetikos ministerija |
| | | 1.4.7. Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai. | Energetikos ministerija |
| | 1.5. Vandenilis | 1.5.1. Vandenilio gamybos, laikymo ir perdavimo operatoriai. | Energetikos ministerija |
| 2. Transportas | 2.1. Oro transportas | 2.1.1. Oro vežėjai, kaip apibrėžta 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinančio Reglamentą (EB) Nr. 2320/2002 3 straipsnio 4 punkte, naudojami komerciniais tikslais. | Lietuvos Respublikos susisiekimo ministerija |

| | | | |
|---|---|---|---|
| | | 2.1.2. Oro uostas, įskaitant 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES, II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir oro uostą valdančios įmonės vadovas.<br><br>Subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius. | Susisiekimo ministerija |
| | | 2.1.3. Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo paslaugas, kaip apibrėžta 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004, nustatančio bendro Europos dangaus sukūrimo pagrindą, 2 straipsnio 1 punkte. | Susisiekimo ministerija |
| | 2.2. Geležinkelių transportas | 2.2.1. Geležinkelių infrastruktūros valdytojas. | Susisiekimo ministerija |
| | | 2.2.2. Geležinkelių įmonė (vežėjas). | Susisiekimo ministerija |

| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už identifikavimą** |
|---|---|---|---|
| | | 2.2.3. Geležinkelių paslaugų įrenginių operatorius. | Susisiekimo ministerija |
| | 2.3. Vandens transportas | 2.3.1. Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų. | Susisiekimo ministerija |

| | | | |
|---|---|---|---|
| | | 2.3.2. Uostus, įskaitant jų uosto įrenginius, kaip apibrėžta Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, valdančios įmonės ir subjektai, vykdantys uostuose esančių įrenginių eksploatavimą, valdymą ir techninę priežiūrą. | Susisiekimo ministerija |
| | | 2.3.3. Laivų eismo tarnybų operatoriai. | Susisiekimo ministerija |
| | 2.4. Kelių transportas | 2.4.1. Kelių direkcijos, kaip apibrėžta 2014 m. gruodžio 18 d. Komisijos deleguotojo reglamento (ES) Nr. 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis, 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis. | Susisiekimo ministerija |
| | | 2.4.2. Intelektinių transporto sistemų operatoriai. | Susisiekimo ministerija |
| 3. Bankininkystė | | 3.1.1. Kredito įstaigos, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 4 straipsnio 1 punkte. | Lietuvos Respublikos finansų ministerija |

| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už identifikavimą** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 4. Finansų rinkų infrastruktūros objektai | | 4.1.1. Prekybos vietų operatoriai. | Finansų ministerija |
| | | 4.1.2. Pagrindinės sandorio šalys, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų 2 straipsnio 1 punkte. | Finansų ministerija |
| 5. Sveikatos priežiūra | | 5.1.1. Asmens sveikatos priežiūros įstaiga. | Lietuvos Respublikos sveikatos apsaugos ministerija |
| | | 5.1.2. Europos Sąjungos etaloninės laboratorijos, nurodytos 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES, 15 straipsnyje. | Sveikatos apsaugos ministerija |
| | | 5.1.3. Subjektai, vykdantys vaistų (vaistinių preparatų), mokslinių tyrimų ir kūrimo veiklą. | Sveikatos apsaugos ministerija |
| | | 5.1.4. Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 21 skyriuje. | Sveikatos apsaugos ministerija |

| | | | |
|---|---|---|---|
| | | 5.1.5. Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama pagal 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje 22 straipsnį. | Sveikatos apsaugos ministerija |

| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už identifikavimą** |
|---|---|---|---|
| 6. Geriamasis vanduo | | 6.1.1. Žmonėms vartoti skirto vandens tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis. | Lietuvos Respublikos aplinkos ministerija |
| 7. Nuotekos | | 7.1.1. Nuotekas renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis. | Aplinkos ministerija |
| 8. Skaitmeninė infrastruktūra | | 8.1.1. Interneto duomenų srautų mainų taško teikėjai. | Susisiekimo ministerija |
| | | 8.1.2. Domenų vardų sistemos paslaugų teikėjai. | Lietuvos Respublikos ekonomikos ir inovacijų ministerija |

| | | | |
|---|---|---|---|
| | | 8.1.3. Aukščiausio lygio domenų vardų registravimo paslaugas teikiantys subjektai. | Ekonomikos ir inovacijų ministerija |
| | | 8.1.4. Debesijos paslaugų teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 8.1.5. Duomenų centrų paslaugų teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 8.1.6. Paskirstytojo turinio teikimo tinklo teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 8.1.7. Patikimumo užtikrinimo paslaugų teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 8.1.8. Viešųjų elektroninių ryšių tinklų teikėjai. | Susisiekimo ministerija |
| | | 8.1.9. Viešųjų elektroninių ryšių paslaugų teikėjai. | Susisiekimo ministerija |
| 9. Informacinių ir ryšių technologijų paslaugų valdymas (paslaugos „verslas verslui“) | | 9.1.1. Valdomų paslaugų teikėjai. | Ministerijos |
| | | 9.1.2. Valdomų kibernetinio saugumo paslaugų teikėjai. | Ministerijos |
| 10. Viešasis administravimas | | 10.1.1. Valstybinio administravimo subjektai. | Lietuvos Respublikos |
| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už identifikavimą** |
| | | | vidaus reikalų ministerija |
| | | 10.1.2. Regioninio administravimo subjektai ir savivaldybių administravimo subjektai. | Vidaus reikalų ministerija |

| | | | |
|---|---|---|---|
| 11. Kosmosas | | 11.1.1. Lietuvos Respublikos įsteigtos arba privatiems subjektams priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus. | Ekonomikos ir inovacijų ministerija |

2.2. KITI ITIN SVARBŪS SEKTORIAI.

| Sektorius | Subsektorius | Subjekto rūšis | Institucija, atsakinga už subjektų identifikavimą |
|---|---|---|---|
| 1. Pašto paslaugos | | 1.1.1. Pašto paslaugos teikėjai. | Lietuvos Respublikos susisiekimo ministerija |
| 2. Atliekų tvarkymas | | 2.1.1. Atliekų tvarkymo paslaugų teikėjai, išskyrus paslaugų teikėjus, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas. | Lietuvos Respublikos aplinkos ministerija |
| 3. Cheminių medžiagų gamyba ir platinimas | | 3.1.1. Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiančio Europos cheminių medžiagų agentūrą, iš dalies keičiančio Direktyvą 1999/45/EB bei panaikinančio Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB, 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip | Aplinkos ministerija |

| | | | |
|---|---|---|---|
| | | apibrėžta to paties reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės. | |
| 4. Maisto gamyba, perdirbimas ir platinimas | | 4.1.1. Maisto verslo įmonės, kaip apibrėžta 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002, nustatančio maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiančio Europos maisto saugos tarnybą ir nustatančio su maisto saugos klausimais susijusias procedūras, 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą. | Lietuvos Respublikos žemės ūkio ministerija |

| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už subjektų identifikavimą** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 5. Gamyba | 5.1. Medicinos priemonių ir *in vitro* diagnostikos medicinos priemonių gamyba | 5.1.1. Medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB, 2 straipsnio 1 punkte, gaminantys subjektai ir *in vitro* diagnostikos medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES, 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šio įstatymo I priedo 5.1.5 papunktyje nurodytas medicinos priemones gaminančius subjektus. | Lietuvos Respublikos sveikatos apsaugos ministerija |
| | 5.2. Kompiuterinių, elektroninių ir optinių gaminių gamyba | 5.2.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 26 skyriuje. | Lietuvos Respublikos ekonomikos ir inovacijų ministerija |
| | 5.3. Elektros įrangos gamyba | 5.3.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 27 skyriuje. | Lietuvos Respublikos energetikos ministerija |
| | 5.4. Niekur kitur nepriskirtų mašinų ir įrangos gamyba | 5.4.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 28 skyriuje. | Ministerijos |

| | | | |
|---|---|---|---|
| | 5.5. Motorinių transporto priemonių, priekabų ir puspriekabių gamyba | 5.5.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 29 skyriuje. | Susisiekimo ministerija |
| | 5.6. Kitos transporto įrangos gamyba | 5.6.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio | Susisiekimo ministerija |
| **Sektorius** | **Subsektorius** | **Subjekto rūšis** | **Institucija, atsakinga už subjektų identifikavimą** |
| | | 29 skyriuje. | |
| 6. Informacinės visuomenės paslaugos | | 6.1.1. Elektroninių prekyviečių paslaugų teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 6.1.2. Paieškos sistemų teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 6.1.3. Socialinių tinklų paslaugų platformos teikėjai. | Ekonomikos ir inovacijų ministerija |
| | | 6.1.4. Elektroninės informacijos prieglobos paslaugų teikėjai. | Ekonomikos ir inovacijų ministerija |
| 7. Moksliniai tyrimai | | 7.1.1. Mokslinius tyrimus vykdantys subjektai. | Lietuvos Respublikos švietimo, mokslo ir sporto ministerija |

## 3. TIS2 reikalavimų įgyvendinimo dekonstrukcija į priemones

| Reikalavimas | Įgyvendinimo priemonės |
|---|---|
| Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | Patvirtinta kibernetinio saugumo politika su aiškia strategija.<br>Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas.<br>Patvirtinta rizikos analizės ir vertinimo politika.<br>Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus.<br>Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių.<br>Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. |
| Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones.<br>Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas).<br>CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų.<br>Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai.<br>Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose.<br>Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus.<br>Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. |
| Kibernetinių incidentų valdymas | Patvirtintas kibernetinių incidentų valdymo planas.<br>Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka.<br>Organizacija gali aptikti kibernetinius incidentus realiuoju laiku.<br>Audito įrašai (logs) renkami iš visų kritinių sistemų.<br>Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį.<br>Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection).<br>Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų.<br>Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju.<br>Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo.<br>Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val.<br>Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo.<br>Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas.<br>Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. |
| Veiklos tęstinumo užtikrinimas | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas.<br>Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective).<br>Patvirtintas krizių valdymo planas (crisis management).<br>Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka.<br>Atsarginės kopijos kuriamos reguliariai ir automatizuotai.<br>Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija.<br>Atsarginės kopijos yra ŠIFRUOTOS. |

| | |
|---|---|
| | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų.<br>Kritinės IT sistemos yra dubliuotos (HA - high availability).<br>Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy).<br>Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). |
| Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | Patvirtinta tiekimo grandinės saugumo politika.<br>Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai.<br>Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai.<br>Sutartyse numatyta incidentų pranešimo pareiga tiekėjams.<br>Sutartyse numatyta teisė audituoti tiekėjus.<br>Tvarkomas kritinių tiekėjų ir paslaugų registras.<br>Vertinama tiekėjų keliama kibernetinio saugumo rizika.<br>Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22).<br>Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. |
| Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika.<br>Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle).<br>Nustatyta pokyčių valdymo (change management) tvarka.<br>Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje.<br>Tvarkomas turto ir programinės įrangos inventorius (asset inventory).<br>Taikoma pataisų valdymo (patch management) tvarka.<br>Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d).<br>Atliekamas pažeidžiamumų skanavimas (vulnerability scanning).<br>Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra.<br>Naudojama tik legali, licencijuota programinė įranga. |
| Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | Metinis vidaus auditas atliekamas.<br>Po auditų parengiami neatitikčių šalinimo planai.<br>Atliekami išorės penetracijos testavimai.<br>Matuojami kibernetinio saugumo KPI (metrics).<br>Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h.<br>Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site).<br>Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.).<br>Yra patvirtinta priemonių veiksmingumo vertinimo politika.<br>Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės). |
| Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika.<br>Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus.<br>Mokymai kartojami reguliariai (ne rečiau 1x per metus).<br>Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). |

| | |
|---|---|
| | Atliekamos phishing simuliacijos darbuotojams.<br>Darbuotojai informuojami apie aktualias kibernetines grėsmes. |
| Kriptografijos ir šifravimo naudojimo politika ir procedūros | Patvirtinta kriptografijos ir šifravimo politika.<br>Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika.<br>Nustatyta kriptografinių raktų valdymo tvarka.<br>Duomenys šifruojami perdavimo metu (data in transit).<br>Duomenys šifruojami saugojimo metu (data at rest).<br>VPN ryšiai naudoja tvirtą šifravimą.<br>Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą.<br>Naudojami patikimų CA (Certificate Authority) sertifikatai.<br>Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME).<br>Naudojami HSM (Hardware Security Modules) kritiniams raktams. |
| Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | Patvirtinta žmogiškųjų išteklių saugumo politika.<br>Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms.<br>Darbuotojai pasirašo konfidencialumo susitarimus (NDA).<br>Patvirtinta turto valdymo politika.<br>Turtas klasifikuojamas pagal svarbą ir jautrumą.<br>Fizinė prieiga prie serverių patalpų yra kontroliuojama.<br>Mobilieji įrenginiai valdomi centralizuotai (MDM).<br>Mobiliųjų įrenginių diskai yra šifruoti. |
| Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS.<br>Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals).<br>Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms.<br>Naudojamos saugios komunikacijos priemonės (secured voice, video, text).<br>Yra saugios avarinio ryšio sistemos.<br>Tinklas segmentuotas į saugumo zonas.<br>Naudojamos ugniasienės (firewalls) tarp segmentų.<br>Įdiegta endpoint apsauga (EDR/Antivirus).<br>Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing).<br>Naudojamas web filtering / proxy sprendimas.<br>Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia.<br>Tinklo srautai stebimi (network monitoring).<br>Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP).<br>Debesijos (cloud) prieiga yra kontroliuojama ir stebima. |
| Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei | Patvirtinta prieigos kontrolės politika.<br>Taikomas mažiausių teisių principas (least privilege). |

| | |
|---|---|
| duomenų valdymo politika | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos.<br>Reguliariai peržiūrimos vartotojų prieigos teisės.<br>Privilegijuotų paskyrų prisijungimai registruojami ir stebimi.<br>Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju.<br>Patvirtinta prieigos kontrolės politika.<br>Taikomas mažiausių teisių principas (least privilege).<br>Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. |

# 4. TIS2 vertinimo įrankio klausimynas

| Reikalavimo_ID | Reikalavimas_pavadinimas_Klausimų_blokas | Priemones_ID | Priemonė | Priemones_tipas | Klausimo_ID | Klausimas | Klausimo_eil_nr | Klausimo_tipas | Parent_Klausimo_ID | Rodomas_jei_atsakymas |
|---|---|---|---|---|---|---|---|---|---|---|
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | R1-POL-01-Q1 | Ar patvirtinta kibernetinio saugumo politika su aiškia strategija? | 1 | root | | |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | R1-POL-02-Q1 | Ar kibernetinio saugumo politikoje aiškiai apibrėžti kibernetinio saugumo tikslai ir principai? | 1 | child | R1-POL-01-Q1 | TAIP |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | R1-POL-02-Q2 | Ar kibernetinio saugumo politikoje aiškiai apibrėžti vadovybės įsipareigojimai ir atsakomybės? | 2 | child | R1-POL-01-Q1 | TAIP |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-01 | Patvirtinta rizikos analizės ir vertinimo politika. | Organizacinė | R1-RIZ-01-Q1 | Ar patvirtinta rizikos analizės ir vertinimo politika? | 1 | root | | |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-02 | Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. | Organizacinė | R1-RIZ-02-Q1 | Ar rizikos vertinimas atliekamas ne rečiau kaip kartą per metus? | 1 | root | | |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-03 | Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių. | Organizacinė | R1-RIZ-03-Q1 | Ar rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių? | 1 | child | R1-RIZ-02-Q1 | TAIP |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | R1-RIZ-04-Q1 | Ar rizikos vertinimo metu sistemingai identifikuojamas organizacijos turtas, grėsmės ir pažeidžiamumai? | 1 | child | R1-RIZ-02-Q1 | TAIP |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | R1-RIZ-04-Q2 | Ar rizikos vertinimo metu kiekvienam turtui nustatomas rizikos lygis? | 2 | child | R1-RIZ-02-Q1 | TAIP |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | R2-VAL-01-Q1 | Ar valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones? | 1 | root | | |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | R2-VAL-02-Q1 | Ar paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas)? | 1 | root | | |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-03 | CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų. | Organizacinė | R2-VAL-03-Q1 | Ar cISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų? | 1 | child | R2-VAL-02-Q1 | TAIP |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | R2-VAL-04-Q1 | Ar apie paskirtus atsakingus asmenis už kibernetinį saugumą informuotas NKSC? | 1 | child | R2-VAL-02-Q1 | TAIP |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | R2-VAL-04-Q2 | Ar apie paskirtus atsakingus asmenis už kibernetinį saugumą informuoti organizacijos darbuotojai? | 2 | child | R2-VAL-02-Q1 | TAIP |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | R2-VAL-05-Q1 | Ar visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose? | 1 | root | | |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-06 | Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus. | Organizacinė | R2-VAL-06-Q1 | Ar valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus? | 1 | root | | |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-07 | Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. | Organizacinė | R2-VAL-07-Q1 | Ar organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje? | 1 | root | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | R3-INC-01-Q1 | Ar patvirtintas kibernetinių incidentų valdymo planas? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | R3-INC-02-Q1 | Ar incidentų valdymo plane apibrėžtas incidentų klasifikavimas (pvz., pagal poveikį ir kritiškumą)? | 1 | child | R3-INC-01-Q1 | TAIP |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | R3-INC-02-Q2 | Ar incidentų valdymo plane aiškiai apibrėžtos incidentų valdymo atsakomybės ir vaidmenys? | 2 | child | R3-INC-01-Q1 | TAIP |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | R3-INC-02-Q3 | Ar incidentų valdymo plane nustatyta incidentų komunikacijos tvarka (vidinė ir išorinė)? | 3 | child | R3-INC-01-Q1 | TAIP |
| R3 | Kibernetinių incidentų valdymas | INC-03 | Organizacija gali aptikti kibernetinius incidentus realiuoju laiku. | Techninė | R3-INC-03-Q1 | Ar organizacija gali aptikti kibernetinius incidentus realiuoju laiku? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-04 | Audito įrašai (logs) renkami iš visų kritinių sistemų. | Techninė | R3-INC-04-Q1 | Ar audito įrašai (logs) renkami iš visų kritinių sistemų? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-05 | Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį. | Techninė | R3-INC-05-Q1 | Ar audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | R3-INC-06-Q1 | Ar žurnaliniai įrašai saugomi apsaugotai (apribota prieiga, apsauga nuo neteisėto pasiekimo)? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | R3-INC-06-Q2 | Ar žurnaliniai įrašai saugomi nekeičiama forma (užtikrinamas įrašų integralumas)? | 2 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-07 | Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų. | Organizacinė | R3-INC-07-Q1 | Ar reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-08 | Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju. | Organizacinė | R3-INC-08-Q1 | Ar organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-09 | Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo. | Organizacinė | R3-INC-09-Q1 | Ar gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-10 | Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val. | Organizacinė | R3-INC-10-Q1 | Ar gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-11 | Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo. | Organizacinė | R3-INC-11-Q1 | Ar gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-12 | Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas. | Organizacinė | R3-INC-12-Q1 | Ar informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | R3-INC-13-Q1 | Ar po reikšmingų kibernetinių incidentų atliekama giluminė analizė (lessons learned)? | 1 | root | | |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | R3-INC-13-Q2 | Ar pagal incidentų analizės rezultatus atnaujinami ir tobulinami procesai bei priemonės? | 2 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-01 | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas. | Organizacinė | R4-TĘS-01-Q1 | Ar patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-02 | Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective). | Organizacinė | R4-TĘS-02-Q1 | Ar plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective)? | 1 | child | R4-TĘS-01-Q1 | TAIP |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-03 | Patvirtintas krizių valdymo planas (crisis management). | Organizacinė | R4-TĘS-03-Q1 | Ar patvirtintas krizių valdymo planas (crisis management)? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | R4-TĘS-04-Q1 | Ar organizacijoje apibrėžta atsarginių kopijų kūrimo ir saugojimo tvarka? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | R4-TĘS-04-Q2 | Ar organizacijoje apibrėžta atsarginių kopijų testavimo ir duomenų atkūrimo tvarka? | 2 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | R4-TĘS-05-Q1 | Ar atsarginės kopijos kuriamos reguliariai pagal nustatytą grafiką? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | R4-TĘS-05-Q2 | Ar atsarginių kopijų kūrimas maksimaliai automatizuotas (backup jobs, planiniai užduočių tvarkaraščiai)? | 2 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-06 | Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija. | Techninė | R4-TĘS-06-Q1 | Ar atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija? | 1 | child | R4-TĘS-05-Q1 | TAIP |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-07 | Atsarginės kopijos yra ŠIFRUOTOS. | Techninė | R4-TĘS-07-Q1 | Ar atsarginės kopijos yra ŠIFRUOTOS? | 1 | child | R4-TĘS-05-Q1 | TAIP |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-08 | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų. | Organizacinė | R4-TĘS-08-Q1 | Ar reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų? | 1 | child | R4-TĘS-05-Q1 | TAIP |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-09 | Kritinės IT sistemos yra dubliuotos (HA - high availability). | Techninė | R4-TĘS-09-Q1 | Ar kritinės IT sistemos yra dubliuotos (HA - high availability)? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-10 | Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy). | Techninė | R4-TĘS-10-Q1 | Ar esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy)? | 1 | root | | |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-11 | Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). | Organizacinė | R4-TĘS-11-Q1 | Ar atliekamos BCP/DRP pratybos (ne rečiau 1x per metus)? | 1 | child | R4-TĘS-01-Q1 | TAIP |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-01 | Patvirtinta tiekimo grandinės saugumo politika. | Organizacinė | R5-TIEK-01-Q1 | Ar patvirtinta tiekimo grandinės saugumo politika? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-02 | Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai. | Organizacinė | R5-TIEK-02-Q1 | Ar apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-03 | Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai. | Organizacinė | R5-TIEK-03-Q1 | Ar sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-04 | Sutartyse numatyta incidentų pranešimo pareiga tiekėjams. | Organizacinė | R5-TIEK-04-Q1 | Ar sutartyse numatyta incidentų pranešimo pareiga tiekėjams? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-05 | Sutartyse numatyta teisė audituoti tiekėjus. | Organizacinė | R5-TIEK-05-Q1 | Ar sutartyse numatyta teisė audituoti tiekėjus? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | R5-TIEK-06-Q1 | Ar organizacijoje nustatyta incidentų su tiekėjais valdymo tvarka? | 1 | child | R5-TIEK-01-Q1 | TAIP |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | R5-TIEK-06-Q2 | Ar incidentų su tiekėjais valdymo tvarkoje aiškiai nustatyta tiekėjų ir kitų suinteresuotųjų šalių informavimo tvarka? | 2 | child | R5-TIEK-01-Q1 | TAIP |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-07 | Vertinama tiekėjų keliama kibernetinio saugumo rizika. | Organizacinė | R5-TIEK-07-Q1 | Ar vertinama tiekėjų keliama kibernetinio saugumo rizika? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-08 | Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22). | Organizacinė | R5-TIEK-08-Q1 | Ar organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22)? | 1 | root | | |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais | TIEK-09 | Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. | Techninė | R5-TIEK-09-Q1 | Ar naudojamos automatizuotos tiekėjų rizikos valdymo platformos? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | R6-PLĖ-01-Q1 | Ar organizacijoje patvirtinta sistemų saugaus įsigijimo politika? | 1 | root | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | R6-PLĖ-01-Q2 | Ar sistemų saugaus įsigijimo politika apima sistemų plėtros ir priežiūros (maintenance) reikalavimus? | 2 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | R6-PLĖ-02-Q1 | Ar naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle)? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-03 | Nustatyta pokyčių valdymo (change management) tvarka. | Organizacinė | R6-PLĖ-03-Q1 | Ar nustatyta pokyčių valdymo (change management) tvarka? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-04 | Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje. | Organizacinė | R6-PLĖ-04-Q1 | Ar pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje? | 1 | child | R6-PLĖ-03-Q1 | TAIP |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | R6-PLĖ-05-Q1 | Ar tvarkomas turto ir programinės įrangos inventorius (asset inventory)? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | R6-PLĖ-06-Q1 | Ar taikoma pataisų valdymo (patch management) tvarka? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-07 | Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d). | Techninė | R6-PLĖ-07-Q1 | Ar kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d)? | 1 | child | R6-PLĖ-06-Q1 | TAIP |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-08 | Atliekamas pažeidžiamumų skanavimas (vulnerability scanning). | Techninė | R6-PLĖ-08-Q1 | Ar atliekamas pažeidžiamumų skanavimas (vulnerability scanning)? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-09 | Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra. | Organizacinė | R6-PLĖ-09-Q1 | Ar yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra? | 1 | root | | |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą | PLĖ-10 | Naudojama tik legali, licencijuota programinė įranga. | Organizacinė | R6-PLĖ-10-Q1 | Ar naudojama tik legali, licencijuota programinė įranga? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-01 | Metinis vidaus auditas atliekamas. | Organizacinė | R7-ATIT-01-Q1 | Ar metinis vidaus auditas atliekamas? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-02 | Po auditų parengiami neatitikčių šalinimo planai. | Organizacinė | R7-ATIT-02-Q1 | Ar po auditų parengiami neatitikčių šalinimo planai? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | R7-ATIT-03-Q1 | Ar atliekami išorės penetracijos testavimai? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | R7-ATIT-04-Q1 | Ar matuojami kibernetinio saugumo KPI (metrics)? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-05 | Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h. | Organizacinė | R7-ATIT-05-Q1 | Ar organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-06 | Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site). | Organizacinė | R7-ATIT-06-Q1 | Ar organizacija pasiruošusi NKSC vietinei inspekcijai (on-site)? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | R7-ATIT-07-Q1 | Ar organizacija yra susipažinusi su TIS2 ir nacionalinių teisės aktų reikalavimų įgyvendinimo terminais? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | R7-ATIT-07-Q2 | Ar organizacija turi planą ir resursus, leidžiančius laiku įgyvendinti nustatytus reikalavimų terminus? | 2 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | R7-POL-03-Q1 | Ar yra patvirtinta priemonių veiksmingumo vertinimo politika? | 1 | root | | |
| R7 | Politika ir procedūros kibernetinio saugumo | POL-04 | Apibrėžta auditų ir testavimų | Organizacinė | R7-POL-04-Q1 | Ar organizacijoje apibrėžtas vidaus ir išorės auditų | 1 | child | R7-POL-03-Q1 | TAIP |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | reikalavimų veiksmingumui įvertinti | | periodiškumas (vidaus/išorės). | | | periodiškumas kibernetinio saugumo srityje? | | | | |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-04 | Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės). | Organizacinė | R7-POL-04-Q2 | Ar organizacijoje apibrėžtas techninių testų (pvz., penetracijos testų, pažeidžiamumų skanavimo) periodiškumas? | 2 | child | R7-POL-03-Q1 | TAIP |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | R8-MOK-01-Q1 | Ar patvirtinta darbuotojų kibernetinio saugumo mokymų politika? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-02 | Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus. | Organizacinė | R8-MOK-02-Q1 | Ar visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-03 | Mokymai kartojami reguliariai (ne rečiau 1x per metus). | Organizacinė | R8-MOK-03-Q1 | Ar mokymai kartojami reguliariai (ne rečiau 1x per metus)? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-04 | Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). | Organizacinė | R8-MOK-04-Q1 | Ar organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing)? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-05 | Atliekamos phishing simuliacijos darbuotojams. | Organizacinė | R8-MOK-05-Q1 | Ar atliekamos phishing simuliacijos darbuotojams? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | R8-MOK-06-Q1 | Ar darbuotojai reguliariai informuojami apie aktualias kibernetines grėsmes? | 1 | root | | |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | R8-MOK-06-Q2 | Ar darbuotojams periodiškai pateikiami realūs kibernetinių incidentų pavyzdžiai ir iš jų gautos pamokos? | 2 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | R9-KRIP-01-Q1 | Ar patvirtinta kriptografijos ir šifravimo politika? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | R9-KRIP-02-Q1 | Ar kriptografijos ir šifravimo politikoje nurodytas leistinų kriptografinių algoritmų sąrašas? | 1 | child | R9-KRIP-01-Q1 | TAIP |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | R9-KRIP-02-Q2 | Ar kriptografijos ir šifravimo politikoje nustatyti minimalių kriptografinių raktų ilgių reikalavimai? | 2 | child | R9-KRIP-01-Q1 | TAIP |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | R9-KRIP-03-Q1 | Ar nustatyta kriptografinių raktų valdymo tvarka? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-04 | Duomenys šifruojami perdavimo metu (data in transit). | Techninė | R9-KRIP-04-Q1 | Ar duomenys šifruojami perdavimo metu (data in transit)? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-05 | Duomenys šifruojami saugojimo metu (data at rest). | Techninė | R9-KRIP-05-Q1 | Ar duomenys šifruojami saugojimo metu (data at rest)? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-06 | VPN ryšiai naudoja tvirtą šifravimą. | Techninė | R9-KRIP-06-Q1 | Ar vPN ryšiai naudoja tvirtą šifravimą? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-07 | Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą. | Techninė | R9-KRIP-07-Q1 | Ar belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-08 | Naudojami patikimų CA (Certificate Authority) sertifikatai. | Techninė | R9-KRIP-08-Q1 | Ar naudojami patikimų CA (Certificate Authority) sertifikatai? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-09 | Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME). | Techninė | R9-KRIP-09-Q1 | Ar naudojamas automatizuotas sertifikatų valdymas (pvz. ACME)? | 1 | root | | |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-10 | Naudojami HSM (Hardware Security Modules) kritiniams raktams. | Techninė | R9-KRIP-10-Q1 | Ar naudojami HSM (Hardware Security Modules) kritiniams raktams? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | R10-HRT-01-Q1 | Ar darbuotojai yra pasirašę konfidencialumo įsipareigojimus? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | R10-HRT-01-Q2 | Ar darbuotojai yra susipažinę ir pasirašę elgesio bei IT naudojimo taisykles? | 2 | root | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-02 | Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms. | Organizacinė | R10-HRT-02-Q1 | Ar atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | R10-HRT-03-Q1 | Ar organizacijoje yra formalus darbuotojų priėmimo ir išėjimo procesas? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | R10-HRT-03-Q2 | Ar darbuotojų priėmimo ir išėjimo procese aiškiai apibrėžti prieigų suteikimo ir nutraukimo žingsniai? | 2 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-04 | Patvirtinta turto valdymo politika. | Organizacinė | R10-HRT-04-Q1 | Ar patvirtinta turto valdymo politika? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | R10-HRT-05-Q1 | Ar turtas (įranga, IT sistemos, duomenys) klasifikuojamas pagal svarbą organizacijos veiklai? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | R10-HRT-05-Q2 | Ar turtas klasifikuojamas pagal informacijos jautrumą (pvz., asmens duomenys, konfidenciali informacija)? | 2 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-06 | Fizinė prieiga prie serverių patalpų yra kontroliuojama. | Techninė | R10-HRT-06-Q1 | Ar fizinė prieiga prie serverių patalpų yra kontroliuojama? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-07 | Mobilieji įrenginiai valdomi centralizuotai (MDM). | Techninė | R10-HRT-07-Q1 | Ar mobilieji įrenginiai valdomi centralizuotai (MDM)? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-08 | Mobiliųjų įrenginių diskai yra šifruoti. | Techninė | R10-HRT-08-Q1 | Ar organizacijoje nustatyta lankytojų registracijos tvarka (registracijos žurnalas ar sistema)? | 1 | root | | |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-08 | Mobiliųjų įrenginių diskai yra šifruoti. | Techninė | R10-HRT-08-Q2 | Ar organizacijoje nustatyta lankytojų palydos tvarka (lankytojai nevaikšto be palydos į saugomas zonas)? | 2 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-06 | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS. | Techninė | R11-PRIEI-06-Q1 | Ar įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | R11-PRIEI-07-Q1 | Ar kelių veiksnių autentifikacija (MFA) taikoma prisijungimams prie kritinių sistemų? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | R11-PRIEI-07-Q2 | Ar kelių veiksnių autentifikacija (MFA) taikoma nuotolinei prieigai (VPN, remote desktop ir pan.)? | 2 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | R11-PRIEI-08-Q1 | Ar kelių veiksnių autentifikacija (MFA) taikoma administratorių paskyroms? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | R11-PRIEI-08-Q2 | Ar kelių veiksnių autentifikacija (MFA) taikoma prieigai prie duomenų bazių sistemų? | 2 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-09 | Naudojamos saugios komunikacijos priemonės (secured voice, video, text). | Techninė | R11-PRIEI-09-Q1 | Ar naudojamos saugios komunikacijos priemonės (secured voice, video, text)? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | PRIEI-10 | Yra saugios avarinio ryšio sistemos. | Techninė | R11-PRIEI-10-Q1 | Ar yra saugios avarinio ryšio sistemos? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-01 | Tinklas segmentuotas į saugumo zonas. | Techninė | R11-TINK-01-Q1 | Ar tinklas segmentuotas į saugumo zonas? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-02 | Naudojamos ugniasienės (firewalls) tarp segmentų. | Techninė | R11-TINK-02-Q1 | Ar naudojamos ugniasienės (firewalls) tarp segmentų? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-03 | Įdiegta endpoint apsauga (EDR/Antivirus). | Techninė | R11-TINK-03-Q1 | Ar įdiegta endpoint apsauga (EDR/Antivirus)? | 1 | root | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-04 | Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing). | Techninė | R11-TINK-04-Q1 | Ar naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing)? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-05 | Naudojamas web filtering / proxy sprendimas. | Techninė | R11-TINK-05-Q1 | Ar naudojamas web filtering / proxy sprendimas? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-06 | Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia. | Techninė | R11-TINK-06-Q1 | Ar tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-07 | Tinklo srautai stebimi (network monitoring). | Techninė | R11-TINK-07-Q1 | Ar tinklo srautai stebimi (network monitoring)? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | R11-TINK-08-Q1 | Ar administratorių prieiga prie sistemų vyksta per saugius protokolus (pvz., SSH, HTTPS, VPN)? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | R11-TINK-08-Q2 | Ar administratorių prisijungimams naudojami dedikuoti jump serveriai / bastion host'ai? | 2 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | R11-TINK-09-Q1 | Ar debesijos (cloud) paslaugų prieiga yra centralizuotai kontroliuojama (valdomos paskyros, teisių suteikimas)? | 1 | root | | |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | R11-TINK-09-Q2 | Ar debesijos (cloud) prieiga atitinka organizacijos nustatytas saugumo ir naudojimo taisykles? | 2 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | R12-PRIEI-01-Q1 | Ar patvirtinta prieigos kontrolės politika? | 1 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-02 | Taikomas mažiausių teisių principas (least privilege). | Techninė | R12-PRIEI-02-Q1 | Ar taikomas mažiausių teisių principas (least privilege)? | 1 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-03 | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. | Techninė | R12-PRIEI-03-Q1 | Ar naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos? | 1 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-04 | Reguliariai peržiūrimos vartotojų prieigos teisės. | Organizacinė | R12-PRIEI-04-Q1 | Ar reguliariai peržiūrimos vartotojų prieigos teisės? | 1 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | R12-PRIEI-05-Q1 | Ar privilegijuotų paskyrų prisijungimai registruojami (kaupiami žurnalų įrašuose)? | 1 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | R12-PRIEI-05-Q2 | Ar privilegijuotų paskyrų prisijungimai ir veikla yra aktyviai stebimi ir peržiūrimi (monitoring / review)? | 2 | root | | |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | R12-PRIEI-11-Q1 | Ar darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju? | 1 | root | | |

# 5. TIS2 vertinimo įrankio trūkumų šalinimo įgyvendinimo planas

## 5.1. Įgyvendinimo priemonės.

| Reikalavimo_ID | Reikalavimas_pavadinimas | Priemones_ID | Priemonė | Priemonės_tipas | Priemonės_prioritetas | Priemonės_subkategorija |
|---|---|---|---|---|---|---|
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-01 | Patvirtinta kibernetinio saugumo politika su aiškia strategija. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | POL-02 | Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas. | Organizacinė | vidutinis | Kiti procesai |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-01 | Patvirtinta rizikos analizės ir vertinimo politika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-01 | Patvirtinta rizikos analizės ir vertinimo politika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-01 | Patvirtinta rizikos analizės ir vertinimo politika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-01 | Patvirtinta rizikos analizės ir vertinimo politika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-02 | Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-02 | Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-02 | Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. | Organizacinė | aukštas | Rizikų valdymo procesas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-02 | Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-03 | Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-03 | Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-03 | Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-03 | Rizikos vertinimas atliekamas po esminių infrastruktūros ar grėsmių pokyčių. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R1 | Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika | RIZ-04 | Rizikos vertinime identifikuojami turtas, grėsmės, pažeidžiamumai ir įgyvendinamos priemonės. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-01 | Valdybos organai (board) oficialiai patvirtino organizacijos kibernetinio saugumo priemones. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | aukštas | Vaidmenys ir atsakomybės |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-02 | Paskirtas atsakingas asmuo už kibernetinį saugumą (CISO/kibernetinio saugumo vadovas). | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-03 | CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-03 | CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-03 | CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-03 | CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-04 | Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai. | Organizacinė | aukštas | Vaidmenys ir atsakomybės |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |

| | | | | | | |
|---|---|---|---|---|---|---|
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-05 | Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-06 | Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-06 | Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-06 | Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-06 | Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus. | Organizacinė | vidutinis | Personalo mokymai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-07 | Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. | Organizacinė | vidutinis | Kiti procesai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-07 | Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. | Organizacinė | vidutinis | Kiti procesai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-07 | Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. | Organizacinė | vidutinis | Kiti procesai |
| R2 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos | VAL-07 | Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje. | Organizacinė | vidutinis | Kiti procesai |
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-01 | Patvirtintas kibernetinių incidentų valdymo planas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | kritinis | Incidentų valdymo procesas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-02 | Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-03 | Organizacija gali aptikti kibernetinius incidentus realiuoju laiku. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-03 | Organizacija gali aptikti kibernetinius incidentus realiuoju laiku. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-03 | Organizacija gali aptikti kibernetinius incidentus realiuoju laiku. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-03 | Organizacija gali aptikti kibernetinius incidentus realiuoju laiku. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-04 | Audito įrašai (logs) renkami iš visų kritinių sistemų. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-04 | Audito įrašai (logs) renkami iš visų kritinių sistemų. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-04 | Audito įrašai (logs) renkami iš visų kritinių sistemų. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-04 | Audito įrašai (logs) renkami iš visų kritinių sistemų. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-05 | Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-05 | Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-05 | Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-05 | Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | kritinis | Incidentų aptikimas ir valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-06 | Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R3 | Kibernetinių incidentų valdymas | INC-07 | Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-07 | Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-07 | Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-07 | Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-08 | Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-08 | Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-08 | Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-08 | Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-09 | Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-09 | Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-09 | Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-09 | Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-10 | Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val. | Organizacinė | kritinis | Incidentų valdymo procesas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R3 | Kibernetinių incidentų valdymas | INC-10 | Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-10 | Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-10 | Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-11 | Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-11 | Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-11 | Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-11 | Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-12 | Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-12 | Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-12 | Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-12 | Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R3 | Kibernetinių incidentų valdymas | INC-13 | Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai. | Organizacinė | kritinis | Incidentų valdymo procesas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-01 | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas. | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-01 | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas. | Organizacinė | kritinis | Verslo tęstinumo valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-01 | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas. | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-01 | Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas. | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-02 | Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-02 | Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-02 | Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-02 | Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-03 | Patvirtintas krizių valdymo planas (crisis management). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-03 | Patvirtintas krizių valdymo planas (crisis management). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-03 | Patvirtintas krizių valdymo planas (crisis management). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-03 | Patvirtintas krizių valdymo planas (crisis management). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-04 | Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-05 | Atsarginės kopijos kuriamos reguliariai ir automatizuotai. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-06 | Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-06 | Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-06 | Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-06 | Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-07 | Atsarginės kopijos yra ŠIFRUOTOS. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-07 | Atsarginės kopijos yra ŠIFRUOTOS. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-07 | Atsarginės kopijos yra ŠIFRUOTOS. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-07 | Atsarginės kopijos yra ŠIFRUOTOS. | Techninė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-08 | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-08 | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-08 | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-08 | Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų. | Organizacinė | kritinis | Atsarginės kopijos ir atkūrimas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-09 | Kritinės IT sistemos yra dubliuotos (HA - high availability). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-09 | Kritinės IT sistemos yra dubliuotos (HA - high availability). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-09 | Kritinės IT sistemos yra dubliuotos (HA - high availability). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-09 | Kritinės IT sistemos yra dubliuotos (HA - high availability). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-10 | Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-10 | Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-10 | Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-10 | Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy). | Techninė | aukštas | Tinklo infrastruktūra |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-11 | Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-11 | Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-11 | Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R4 | Veiklos tęstinumo užtikrinimas | TĘS-11 | Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus). | Organizacinė | kritinis | Verslo tęstinumo valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-01 | Patvirtinta tiekimo grandinės saugumo politika. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-01 | Patvirtinta tiekimo grandinės saugumo politika. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-01 | Patvirtinta tiekimo grandinės saugumo politika. | Organizacinė | aukštas | Tiekimo grandinės valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-01 | Patvirtinta tiekimo grandinės saugumo politika. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-02 | Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-02 | Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-02 | Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-02 | Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-03 | Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-03 | Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-03 | Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-03 | Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-04 | Sutartyse numatyta incidentų pranešimo pareiga tiekėjams. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-04 | Sutartyse numatyta incidentų pranešimo pareiga tiekėjams. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-04 | Sutartyse numatyta incidentų pranešimo pareiga tiekėjams. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-04 | Sutartyse numatyta incidentų pranešimo pareiga tiekėjams. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-05 | Sutartyse numatyta teisė audituoti tiekėjus. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-05 | Sutartyse numatyta teisė audituoti tiekėjus. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-05 | Sutartyse numatyta teisė audituoti tiekėjus. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-05 | Sutartyse numatyta teisė audituoti tiekėjus. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-06 | Tvarkomas kritinių tiekėjų ir paslaugų registras. | Organizacinė | aukštas | Tiekimo grandinės valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-07 | Vertinama tiekėjų keliama kibernetinio saugumo rizika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-07 | Vertinama tiekėjų keliama kibernetinio saugumo rizika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-07 | Vertinama tiekėjų keliama kibernetinio saugumo rizika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-07 | Vertinama tiekėjų keliama kibernetinio saugumo rizika. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-08 | Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22). | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-08 | Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22). | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-08 | Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22). | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-08 | Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22). | Organizacinė | aukštas | Rizikų valdymo procesas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-09 | Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. | Techninė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-09 | Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. | Techninė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-09 | Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. | Techninė | aukštas | Tiekimo grandinės valdymas |
| R5 | Tiekimo grandinės saugumas ir santykiai su tiekėjais / paslaugų teikėjais | TIEK-09 | Naudojamos automatizuotos tiekėjų rizikos valdymo platformos. | Techninė | aukštas | Tiekimo grandinės valdymas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | vidutinis | Programinės įrangos saugumas |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-01 | Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-02 | Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle). | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-03 | Nustatyta pokyčių valdymo (change management) tvarka. | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-03 | Nustatyta pokyčių valdymo (change management) tvarka. | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-03 | Nustatyta pokyčių valdymo (change management) tvarka. | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-04 | Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje. | Organizacinė | vidutinis | Programinės įrangos saugumas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-04 | Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-04 | Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-04 | Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-05 | Tvarkomas turto ir programinės įrangos inventorius (asset inventory). | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-06 | Taikoma pataisų valdymo (patch management) tvarka. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-07 | Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-07 | Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-07 | Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-08 | Atliekamas pažeidžiamumų skanavimas (vulnerability scanning). | Techninė | vidutinis | Programinės įrangos saugumas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-08 | Atliekamas pažeidžiamumų skanavimas (vulnerability scanning). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-08 | Atliekamas pažeidžiamumų skanavimas (vulnerability scanning). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-08 | Atliekamas pažeidžiamumų skanavimas (vulnerability scanning). | Techninė | vidutinis | Programinės įrangos saugumas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-09 | Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-09 | Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-09 | Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-09 | Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra. | Organizacinė | aukštas | Rizikų valdymo procesas |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-10 | Naudojama tik legali, licencijuota programinė įranga. | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-10 | Naudojama tik legali, licencijuota programinė įranga. | Organizacinė | vidutinis | Kiti procesai |
| R6 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (įskaitant spragų valdymą) | PLĖ-10 | Naudojama tik legali, licencijuota programinė įranga. | Organizacinė | vidutinis | Kiti procesai |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-01 | Metinis vidaus auditas atliekamas. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-01 | Metinis vidaus auditas atliekamas. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-01 | Metinis vidaus auditas atliekamas. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-01 | Metinis vidaus auditas atliekamas. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-02 | Po auditų parengiami neatitikčių šalinimo planai. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-02 | Po auditų parengiami neatitikčių šalinimo planai. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-02 | Po auditų parengiami neatitikčių šalinimo planai. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-02 | Po auditų parengiami neatitikčių šalinimo planai. | Organizacinė | vidutinis | Atitikties vertinimas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-03 | Atliekami išorės penetracijos testavimai. | Organizacinė | vidutinis | Programinės įrangos saugumas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-04 | Matuojami kibernetinio saugumo KPI (metrics). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-05 | Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h. | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-05 | Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h. | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-05 | Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h. | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-05 | Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h. | Organizacinė | vidutinis | Procesų / žinių valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-06 | Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-06 | Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-06 | Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-06 | Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | ATIT-07 | Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.). | Organizacinė | vidutinis | Procesų / žinių valdymas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | vidutinis | Atitikties vertinimas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-03 | Yra patvirtinta priemonių veiksmingumo vertinimo politika. | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-04 | Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-04 | Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės). | Organizacinė | vidutinis | Atitikties vertinimas |
| R7 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti | POL-04 | Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės). | Organizacinė | vidutinis | Atitikties vertinimas |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-01 | Patvirtinta darbuotojų kibernetinio saugumo mokymų politika. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-02 | Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-02 | Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-02 | Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-02 | Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-03 | Mokymai kartojami reguliariai (ne rečiau 1x per metus). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-03 | Mokymai kartojami reguliariai (ne rečiau 1x per metus). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-03 | Mokymai kartojami reguliariai (ne rečiau 1x per metus). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-03 | Mokymai kartojami reguliariai (ne rečiau 1x per metus). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-04 | Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-04 | Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). | Organizacinė | vidutinis | Personalo mokymai |

| | | | | | | |
|---|---|---|---|---|---|---|
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-04 | Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-04 | Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing). | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-05 | Atliekamos phishing simuliacijos darbuotojams. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-05 | Atliekamos phishing simuliacijos darbuotojams. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-05 | Atliekamos phishing simuliacijos darbuotojams. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-05 | Atliekamos phishing simuliacijos darbuotojams. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | vidutinis | Personalo mokymai |
| R8 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai | MOK-06 | Darbuotojai informuojami apie aktualias kibernetines grėsmes. | Organizacinė | vidutinis | Personalo mokymai |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-01 | Patvirtinta kriptografijos ir šifravimo politika. | Organizacinė | aukštas | Kriptografija |

| | | | | | | |
|---|---|---|---|---|---|---|
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-02 | Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-03 | Nustatyta kriptografinių raktų valdymo tvarka. | Organizacinė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-04 | Duomenys šifruojami perdavimo metu (data in transit). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-04 | Duomenys šifruojami perdavimo metu (data in transit). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-04 | Duomenys šifruojami perdavimo metu (data in transit). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-04 | Duomenys šifruojami perdavimo metu (data in transit). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-05 | Duomenys šifruojami saugojimo metu (data at rest). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-05 | Duomenys šifruojami saugojimo metu (data at rest). | Techninė | aukštas | Kriptografija |

| | | | | | | |
|---|---|---|---|---|---|---|
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-05 | Duomenys šifruojami saugojimo metu (data at rest). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-05 | Duomenys šifruojami saugojimo metu (data at rest). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-06 | VPN ryšiai naudoja tvirtą šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-06 | VPN ryšiai naudoja tvirtą šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-06 | VPN ryšiai naudoja tvirtą šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-06 | VPN ryšiai naudoja tvirtą šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-07 | Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-07 | Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-07 | Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-07 | Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą. | Techninė | aukštas | Tinklo saugumas |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-08 | Naudojami patikimų CA (Certificate Authority) sertifikatai. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-08 | Naudojami patikimų CA (Certificate Authority) sertifikatai. | Techninė | aukštas | Kriptografija |

| | | | | | | |
|---|---|---|---|---|---|---|
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-08 | Naudojami patikimų CA (Certificate Authority) sertifikatai. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-08 | Naudojami patikimų CA (Certificate Authority) sertifikatai. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-09 | Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-09 | Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-09 | Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-09 | Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME). | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-10 | Naudojami HSM (Hardware Security Modules) kritiniams raktams. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-10 | Naudojami HSM (Hardware Security Modules) kritiniams raktams. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-10 | Naudojami HSM (Hardware Security Modules) kritiniams raktams. | Techninė | aukštas | Kriptografija |
| R9 | Kriptografijos ir šifravimo naudojimo politika ir procedūros | KRIP-10 | Naudojami HSM (Hardware Security Modules) kritiniams raktams. | Techninė | aukštas | Kriptografija |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-01 | Patvirtinta žmogiškųjų išteklių saugumo politika. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-02 | Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-02 | Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-02 | Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-02 | Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms. | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-03 | Darbuotojai pasirašo konfidencialumo susitarimus (NDA). | Organizacinė | vidutinis | Žmogiškųjų išteklių saugumas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-04 | Patvirtinta turto valdymo politika. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-04 | Patvirtinta turto valdymo politika. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-04 | Patvirtinta turto valdymo politika. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-04 | Patvirtinta turto valdymo politika. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | aukštas | Turto valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-05 | Turtas klasifikuojamas pagal svarbą ir jautrumą. | Organizacinė | aukštas | Turto valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-06 | Fizinė prieiga prie serverių patalpų yra kontroliuojama. | Techninė | aukštas | Fizinė apsauga |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-06 | Fizinė prieiga prie serverių patalpų yra kontroliuojama. | Techninė | aukštas | Fizinė apsauga |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-06 | Fizinė prieiga prie serverių patalpų yra kontroliuojama. | Techninė | aukštas | Fizinė apsauga |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-06 | Fizinė prieiga prie serverių patalpų yra kontroliuojama. | Techninė | aukštas | Fizinė apsauga |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-07 | Mobilieji įrenginiai valdomi centralizuotai (MDM). | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-07 | Mobilieji įrenginiai valdomi centralizuotai (MDM). | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-07 | Mobilieji įrenginiai valdomi centralizuotai (MDM). | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-07 | Mobilieji įrenginiai valdomi centralizuotai (MDM). | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-08 | Mobiliųjų įrenginių diskai yra šifruoti. | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-08 | Mobiliųjų įrenginių diskai yra šifruoti. | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R10 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas | HRT-08 | Mobiliųjų įrenginių diskai yra šifruoti. | Techninė | vidutinis | Mobilių įrenginių valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-06 | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-06 | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-06 | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-06 | Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | kritinis | Prieigos valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-07 | Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals). | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-08 | Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms. | Techninė | kritinis | Prieigos valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-09 | Naudojamos saugios komunikacijos priemonės (secured voice, video, text). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-09 | Naudojamos saugios komunikacijos priemonės (secured voice, video, text). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-09 | Naudojamos saugios komunikacijos priemonės (secured voice, video, text). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-09 | Naudojamos saugios komunikacijos priemonės (secured voice, video, text). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-10 | Yra saugios avarinio ryšio sistemos. | Techninė | kritinis | Verslo tęstinumo valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-10 | Yra saugios avarinio ryšio sistemos. | Techninė | kritinis | Verslo tęstinumo valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-10 | Yra saugios avarinio ryšio sistemos. | Techninė | kritinis | Verslo tęstinumo valdymas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | PRIEI-10 | Yra saugios avarinio ryšio sistemos. | Techninė | kritinis | Verslo tęstinumo valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-01 | Tinklas segmentuotas į saugumo zonas. | Techninė | aukštas | Tinklo infrastruktūra |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-01 | Tinklas segmentuotas į saugumo zonas. | Techninė | aukštas | Tinklo infrastruktūra |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-01 | Tinklas segmentuotas į saugumo zonas. | Techninė | aukštas | Tinklo infrastruktūra |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-01 | Tinklas segmentuotas į saugumo zonas. | Techninė | aukštas | Tinklo infrastruktūra |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-02 | Naudojamos ugniasienės (firewalls) tarp segmentų. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-02 | Naudojamos ugniasienės (firewalls) tarp segmentų. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-02 | Naudojamos ugniasienės (firewalls) tarp segmentų. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-02 | Naudojamos ugniasienės (firewalls) tarp segmentų. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-03 | Įdiegta endpoint apsauga (EDR/Antivirus). | Techninė | vidutinis | Programinės įrangos saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-03 | Įdiegta endpoint apsauga (EDR/Antivirus). | Techninė | vidutinis | Programinės įrangos saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-03 | Įdiegta endpoint apsauga (EDR/Antivirus). | Techninė | vidutinis | Programinės įrangos saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-03 | Įdiegta endpoint apsauga (EDR/Antivirus). | Techninė | vidutinis | Programinės įrangos saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-04 | Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-04 | Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-04 | Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing). | Techninė | aukštas | Tinklo saugumas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-04 | Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-05 | Naudojamas web filtering / proxy sprendimas. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-05 | Naudojamas web filtering / proxy sprendimas. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-05 | Naudojamas web filtering / proxy sprendimas. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-05 | Naudojamas web filtering / proxy sprendimas. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-06 | Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-06 | Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-06 | Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-07 | Tinklo srautai stebimi (network monitoring). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-07 | Tinklo srautai stebimi (network monitoring). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-07 | Tinklo srautai stebimi (network monitoring). | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-08 | Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP). | Techninė | aukštas | Tinklo saugumas |

| | | | | | | |
|---|---|---|---|---|---|---|
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | aukštas | Tinklo saugumas |
| R11 | Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs (įskaitant avarinius) ryšiai | TINK-09 | Debesijos (cloud) prieiga yra kontroliuojama ir stebima. | Techninė | aukštas | Tinklo saugumas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-01 | Patvirtinta prieigos kontrolės politika. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-02 | Taikomas mažiausių teisių principas (least privilege). | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-02 | Taikomas mažiausių teisių principas (least privilege). | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-02 | Taikomas mažiausių teisių principas (least privilege). | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-02 | Taikomas mažiausių teisių principas (least privilege). | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-03 | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-03 | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-03 | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. | Techninė | kritinis | Prieigos valdymas |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-03 | Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. | Techninė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-04 | Reguliariai peržiūrimos vartotojų prieigos teisės. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-04 | Reguliariai peržiūrimos vartotojų prieigos teisės. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-04 | Reguliariai peržiūrimos vartotojų prieigos teisės. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-04 | Reguliariai peržiūrimos vartotojų prieigos teisės. | Organizacinė | kritinis | Prieigos valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-05 | Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. | Techninė | kritinis | Incidentų aptikimas ir valdymas |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | vidutinis | Kiti procesai |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | vidutinis | Kiti procesai |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | vidutinis | Kiti procesai |
| R12 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | vidutinis | Kiti procesai |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 6 | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika | PRIEI-11 | Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. | Techninė | vidutinis | Kiti procesai |

## 5.2. Įgyvendinimo veiksmai.

| Veiksmo_ID | Veiksmo_NR_priemonėje | Veiksmo pavadinimas | Veiksmo aprašymas |
|---|---|---|---|
| R1-POL-01-ACT1 | 1 | Parengti ir patvirtinti kibernetinio saugumo politikos dokumentą | Sukurti kibernetinio saugumo politikos dokumentą, kuris apibrėžia organizacijos požiūrį į kibernetinį saugumą ir pagrindinius įsipareigojimus. |
| R1-POL-01-ACT1 | 1 | Parengti ir patvirtinti kibernetinio saugumo politikos dokumentą | Sukurti kibernetinio saugumo politikos dokumentą, kuris apibrėžia organizacijos požiūrį į kibernetinį saugumą ir pagrindinius įsipareigojimus. |
| R1-POL-01-ACT1 | 1 | Parengti ir patvirtinti kibernetinio saugumo politikos dokumentą | Sukurti kibernetinio saugumo politikos dokumentą, kuris apibrėžia organizacijos požiūrį į kibernetinį saugumą ir pagrindinius įsipareigojimus. |
| R1-POL-01-ACT2 | 2 | Įdiegti politikos komunikavimo ir prieinamumo mechanizmą | Užtikrinti, kad kibernetinio saugumo politika būtų lengvai pasiekiama ir žinoma visiems darbuotojams. |
| R1-POL-01-ACT2 | 2 | Įdiegti politikos komunikavimo ir prieinamumo mechanizmą | Užtikrinti, kad kibernetinio saugumo politika būtų lengvai pasiekiama ir žinoma visiems darbuotojams. |
| R1-POL-02-ACT1 | 1 | Suformuluoti kibernetinio saugumo tikslus ir principus | Aiškiai aprašyti, kokius kibernetinio saugumo tikslus siekia organizacija ir kokiais principais jie grindžiami. |
| R1-POL-02-ACT1 | 1 | Suformuluoti kibernetinio saugumo tikslus ir principus | Aiškiai aprašyti, kokius kibernetinio saugumo tikslus siekia organizacija ir kokiais principais jie grindžiami. |
| R1-POL-02-ACT2 | 2 | Apibrėžti atsakomybes ir politikos peržiūros periodiškumą | Politikoje aprašyti, kas atsakingas už jos įgyvendinimą ir peržiūrą bei kaip dažnai ji turi būti peržiūrima. |
| R1-POL-02-ACT2 | 2 | Apibrėžti atsakomybes ir politikos peržiūros periodiškumą | Politikoje aprašyti, kas atsakingas už jos įgyvendinimą ir peržiūrą bei kaip dažnai ji turi būti peržiūrima. |
| R1-RIZ-01-ACT1 | 1 | Sukurti rizikos analizės ir vertinimo politiką | Aprašyti, kaip organizacija identifikuoja, vertina ir valdo kibernetines rizikas. |
| R1-RIZ-01-ACT1 | 1 | Sukurti rizikos analizės ir vertinimo politiką | Aprašyti, kaip organizacija identifikuoja, vertina ir valdo kibernetines rizkas. |
| R1-RIZ-01-ACT2 | 2 | Patvirtinti rizikos analizės ir vertinimo politiką vadovo / valdybos lygiu | Formalizuoti rizikos vertinimo politiką organizacijos valdymo lygiu. |
| R1-RIZ-01-ACT2 | 2 | Patvirtinti rizikos analizės ir vertinimo politiką vadovo / valdybos lygiu | Formalizuoti rizikos vertinimo politiką organizacijos valdymo lygiu. |
| R1-RIZ-02-ACT1 | 1 | Suplanuoti metinį kibernetinių rizikų vertinimo ciklą | Nustatyti, kad rizikos vertinimas būtų atliekamas reguliariai, ne rečiau kaip kartą per metus. |

| | | | |
|---|---|---|---|
| R1-RIZ-02-ACT1 | 1 | Suplanuoti metinį kibernetinių rizikų vertinimo ciklą | Nustatyti, kad rizikos vertinimas būtų atliekamas reguliariai, ne rečiau kaip kartą per metus. |
| R1-RIZ-02-ACT2 | 2 | Organizuoti metinį rizikos vertinimo atlikimą | Užtikrinti, kad suplanuotas metinis rizikos vertinimas faktiškai būtų atliktas ir dokumentuotas. |
| R1-RIZ-02-ACT2 | 2 | Organizuoti metinį rizikos vertinimo atlikimą | Užtikrinti, kad suplanuotas metinis rizikos vertinimas faktiškai būtų atliktas ir dokumentuotas. |
| R1-RIZ-03-ACT1 | 1 | Apibrėžti esminių pokyčių, reikalaujančių papildomo rizikos vertinimo, kriterijus | Nustatyti, kokie infrastruktūros, paslaugų ar grėsmių pokyčiai laikomi pakankamai reikšmingais, kad būtų atliktas neplaninis rizikos vertinimas. |
| R1-RIZ-03-ACT1 | 1 | Apibrėžti esminių pokyčių, reikalaujančių papildomo rizikos vertinimo, kriterijus | Nustatyti, kokie infrastruktūros, paslaugų ar grėsmių pokyčiai laikomi pakankamai reikšmingais, kad būtų atliktas neplaninis rizikos vertinimas. |
| R1-RIZ-03-ACT2 | 2 | Įdiegti neplaninių rizikos vertinimų inicijavimo ir vykdymo procesą | Užtikrinti, kad po esminių pokyčių būtų laiku inicijuotas ir atliktas papildomas rizikos vertinimas. |
| R1-RIZ-03-ACT2 | 2 | Įdiegti neplaninių rizikos vertinimų inicijavimo ir vykdymo procesą | Užtikrinti, kad po esminių pokyčių būtų laiku inicijuotas ir atliktas papildomas rizikos vertinimas. |
| R1-RIZ-04-ACT1 | 1 | Sukurti ir palaikyti kibernetinio saugumo turto registrą | Identifikuoti ir registruoti turtą, kuris patenka į kibernetinio rizikos vertinimo apimtį. |
| R1-RIZ-04-ACT1 | 1 | Sukurti ir palaikyti kibernetinio saugumo turto registrą | Identifikuoti ir registruoti turtą, kuris patenka į kibernetinio rizikos vertinimo apimtį. |
| R1-RIZ-04-ACT2 | 2 | Integruoti turto, grėsmių, pažeidžiamumų ir priemonių analizę į rizikos vertinimo šabloną | Rizikos vertinimo metu sistemingai vertinti turtą, grėsmes, pažeidžiamumus ir jau įdiegtas bei planuojamas priemones. |
| R1-RIZ-04-ACT2 | 2 | Integruoti turto, grėsmių, pažeidžiamumų ir priemonių analizę į rizikos vertinimo šabloną | Rizikos vertinimo metu sistemingai vertinti turtą, grėsmes, pažeidžiamumus ir jau įdiegtas bei planuojamas priemones. |
| R2-VAL-01-ACT1 | 1 | Parengti kibernetinio saugumo priemonių paketą valdybos tvirtinimui | Identifikuoti ir sugrupuoti pagrindines kibernetinio saugumo priemones (politikas, procesus, technines kontrolės priemones), kurios turi būti patvirtintos valdybos, ir parengti sprendimo projektą. |
| R2-VAL-01-ACT1 | 1 | Parengti kibernetinio saugumo priemonių paketą valdybos tvirtinimui | Identifikuoti ir sugrupuoti pagrindines kibernetinio saugumo priemones (politikas, procesus, technines kontrolės priemones), kurios turi būti patvirtintos valdybos, ir parengti sprendimo projektą. |
| R2-VAL-01-ACT1 | 1 | Parengti kibernetinio saugumo priemonių paketą valdybos tvirtinimui | Identifikuoti ir sugrupuoti pagrindines kibernetinio saugumo priemones (politikas, procesus, technines kontrolės priemones), kurios turi būti patvirtintos valdybos, ir parengti sprendimo projektą. |
| R2-VAL-01-ACT2 | 2 | Dokumentuoti valdybos sprendimą ir integruoti jį į vidaus valdymo dokumentus | Užtikrinti, kad valdybos sprendimas dėl kibernetinio saugumo priemonių būtų tinkamai protokoluotas, saugomas ir atspindėtas organizacijos vidaus dokumentuose bei komunikacijoje. |
| R2-VAL-01-ACT2 | 2 | Dokumentuoti valdybos sprendimą ir integruoti jį į vidaus valdymo dokumentus | Užtikrinti, kad valdybos sprendimas dėl kibernetinio saugumo priemonių būtų tinkamai protokoluotas, saugomas ir atspindėtas organizacijos vidaus dokumentuose bei komunikacijoje. |
| R2-VAL-01-ACT2 | 2 | Dokumentuoti valdybos sprendimą ir integruoti jį į vidaus valdymo dokumentus | Užtikrinti, kad valdybos sprendimas dėl kibernetinio saugumo priemonių būtų tinkamai protokoluotas, saugomas ir atspindėtas organizacijos vidaus dokumentuose bei komunikacijoje. |
| R2-VAL-02-ACT1 | 1 | Apibrėžti CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo vaidmenį ir atsakomybę | Sukurti formalų CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo rolės aprašą, apimantį atsakomybes, įgaliojimus ir atskaitomybės linijas. |

| | | | |
|---|---|---|---|
| R2-VAL-02-ACT1 | 1 | Apibrėžti CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo vaidmenį ir atsakomybę | Sukurti formalų CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo rolės aprašą, apimantį atsakomybes, įgaliojimus ir atskaitomybės linijas. |
| R2-VAL-02-ACT2 | 2 | Formaliai paskirti CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovą | Priimti oficialų sprendimą dėl atsakingo asmens paskyrimo ir dokumentuoti tai vidaus aktuose bei komunikacijoje. |
| R2-VAL-02-ACT2 | 2 | Formaliai paskirti CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovą | Priimti oficialų sprendimą dėl atsakingo asmens paskyrimo ir dokumentuoti tai vidaus aktuose bei komunikacijoje. |
| R2-VAL-02-ACT2 | 2 | Formaliai paskirti CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovą | Priimti oficialų sprendimą dėl atsakingo asmens paskyrimo ir dokumentuoti tai vidaus aktuose bei komunikacijoje. |
| R2-VAL-03-ACT1 | 1 | Įvertinti esamą CISO (Chief Information Security Officer, informacijos saugos vadovas) ir IT (Information Technology, informacinės technologijos) administravimo funkcijų atskyrimo būklę | Analitiškai įvertinti, ar dabartinėje organizacinėje struktūroje CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcija yra pakankamai atskirta nuo IT (Information Technology, informacinės technologijos) administravimo ir operacijų. |
| R2-VAL-03-ACT1 | 1 | Įvertinti esamą CISO (Chief Information Security Officer, informacijos saugos vadovas) ir IT (Information Technology, informacinės technologijos) administravimo funkcijų atskyrimo būklę | Analitiškai įvertinti, ar dabartinėje organizacinėje struktūroje CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcija yra pakankamai atskirta nuo IT (Information Technology, informacinės technologijos) administravimo ir operacijų. |
| R2-VAL-03-ACT2 | 2 | Pertvarkyti organizacinę struktūrą, užtikrinant CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcijos nepriklausomumą | Įgyvendinti organizacinius pokyčius, kurie atskiria CISO (Chief Information Security Officer, informacijos saugos vadovas) funkciją nuo IT (Information Technology, informacinės technologijos) administravimo ir suteikia jai pakankamą nepriklausomumą. |
| R2-VAL-03-ACT2 | 2 | Pertvarkyti organizacinę struktūrą, užtikrinant CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcijos nepriklausomumą | Įgyvendinti organizacinius pokyčius, kurie atskiria CISO (Chief Information Security Officer, informacijos saugos vadovas) funkciją nuo IT (Information Technology, informacinės technologijos) administravimo ir suteikia jai pakankamą nepriklausomumą. |
| R2-VAL-04-ACT1 | 1 | Informuoti NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) apie paskirtus kibernetinio saugumo atsakingus asmenis | Organizuoti formalų atsakingų asmenų (CISO (Chief Information Security Officer, informacijos saugos vadovas) ir kitų kontaktinių asmenų) pateikimą NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) nustatyta tvarka. |
| R2-VAL-04-ACT1 | 1 | Informuoti NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) apie paskirtus kibernetinio saugumo atsakingus asmenis | Organizuoti formalų atsakingų asmenų (CISO (Chief Information Security Officer, informacijos saugos vadovas) ir kitų kontaktinių asmenų) pateikimą NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) nustatyta tvarka. |
| R2-VAL-04-ACT2 | 2 | Komunikuoti paskirtus kibernetinio saugumo atsakingus asmenis organizacijos viduje | Užtikrinti, kad darbuotojai žinotų, kas organizacijoje atsakingas už kibernetinio saugumo klausimus ir kaip su juo susisiekti. |
| R2-VAL-04-ACT2 | 2 | Komunikuoti paskirtus kibernetinio saugumo atsakingus asmenis organizacijos viduje | Užtikrinti, kad darbuotojai žinotų, kas organizacijoje atsakingas už kibernetinio saugumo klausimus ir kaip su juo susisiekti. |
| R2-VAL-05-ACT1 | 1 | Sukurti kibernetinio saugumo mokymų programą valdybos nariams | Parengti specialiai valdybos nariams skirtą mokymų programą, apimančią strateginius kibernetinio saugumo aspektus, rizikas ir valdymo atsakomybes. |
| R2-VAL-05-ACT1 | 1 | Sukurti kibernetinio saugumo mokymų programą valdybos nariams | Parengti specialiai valdybos nariams skirtą mokymų programą, apimančią strateginius kibernetinio saugumo aspektus, rizikas ir valdymo atsakomybes. |
| R2-VAL-05-ACT1 | 1 | Sukurti kibernetinio saugumo mokymų programą valdybos nariams | Parengti specialiai valdybos nariams skirtą mokymų programą, apimančią strateginius kibernetinio saugumo aspektus, rizikas ir valdymo atsakomybes. |

| | | | |
|---|---|---|---|
| R2-VAL-05-ACT2 | 2 | Organizuoti ir fiksuoti valdybos narių dalyvavimą kibernetinio saugumo mokymuose | Suplanuoti konkrečias mokymų sesijas, užtikrinti valdybos narių dalyvavimą ir tinkamai dokumentuoti mokymus. |
| R2-VAL-05-ACT2 | 2 | Organizuoti ir fiksuoti valdybos narių dalyvavimą kibernetinio saugumo mokymuose | Suplanuoti konkrečias mokymų sesijas, užtikrinti valdybos narių dalyvavimą ir tinkamai dokumentuoti mokymus. |
| R2-VAL-05-ACT2 | 2 | Organizuoti ir fiksuoti valdybos narių dalyvavimą kibernetinio saugumo mokymuose | Suplanuoti konkrečias mokymų sesijas, užtikrinti valdybos narių dalyvavimą ir tinkamai dokumentuoti mokymus. |
| R2-VAL-06-ACT1 | 1 | Integruoti valdybos atsakomybės ir sankcijų turinį į mokymų programą | Papildyti valdybos mokymų turinį konkrečiomis temomis apie asmeninę atsakomybę, sankcijas ir teisinius padarinius už kibernetinio saugumo reikalavimų nevykdymą. |
| R2-VAL-06-ACT1 | 1 | Integruoti valdybos atsakomybės ir sankcijų turinį į mokymų programą | Papildyti valdybos mokymų turinį konkrečiomis temomis apie asmeninę atsakomybę, sankcijas ir teisinius padarinius už kibernetinio saugumo reikalavimų nevykdymą. |
| R2-VAL-06-ACT2 | 2 | Užtikrinti, kad valdybos nariai reflektuotų ir patvirtintų savo atsakomybę | Sukurti mechanizmus, kuriais valdybos nariai patvirtina, jog supranta savo atsakomybę, ir periodiškai tai peržiūri. |
| R2-VAL-06-ACT2 | 2 | Užtikrinti, kad valdybos nariai reflektuotų ir patvirtintų savo atsakomybę | Sukurti mechanizmus, kuriais valdybos nariai patvirtina, jog supranta savo atsakomybę, ir periodiškai tai peržiūri. |
| R2-VAL-07-ACT1 | 1 | Nustatyti registracijos NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) Kibernetinio saugumo informacinėje sistemoje poreikį ir reikalavimus | Patikrinti, ar organizacija patenka į subjektų, privalančių registruotis NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) KSIS (kibernetinio saugumo informacinė sistema (KSIS)), sąrašą ir kokie duomenys turi būti pateikti. |
| R2-VAL-07-ACT1 | 1 | Nustatyti registracijos NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) Kibernetinio saugumo informacinėje sistemoje poreikį ir reikalavimus | Patikrinti, ar organizacija patenka į subjektų, privalančių registruotis NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) KSIS (kibernetinio saugumo informacinė sistema (KSIS)), sąrašą ir kokie duomenys turi būti pateikti. |
| R2-VAL-07-ACT2 | 2 | Užregistruoti organizaciją NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) Kibernetinio saugumo informacinėje sistemoje ir palaikyti duomenų aktualumą | Atlikti registraciją NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) KSIS (kibernetinio saugumo informacinė sistema (KSIS)) ir nustatyti procesą, kaip bus atnaujinami organizacijos duomenys, pasikeitus aplinkybėms. |
| R2-VAL-07-ACT2 | 2 | Užregistruoti organizaciją NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) Kibernetinio saugumo informacinėje sistemoje ir palaikyti duomenų aktualumą | Atlikti registraciją NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) KSIS (kibernetinio saugumo informacinė sistema (KSIS)) ir nustatyti procesą, kaip bus atnaujinami organizacijos duomenys, pasikeitus aplinkybėms. |
| R3-INC-01-ACT1 | 1 | Parengti kibernetinių incidentų valdymo planą | Sukurti išsamų incidentų valdymo planą, apimantį incidentų gyvavimo ciklą, etapus ir pagrindinius atsakomybių bei sprendimų priėmimo principus. |
| R3-INC-01-ACT1 | 1 | Parengti kibernetinių incidentų valdymo planą | Sukurti išsamų incidentų valdymo planą, apimantį incidentų gyvavimo ciklą, etapus ir pagrindinius atsakomybių bei sprendimų priėmimo principus. |
| R3-INC-01-ACT2 | 2 | Patvirtinti incidentų valdymo planą ir nustatyti jo peržiūros tvarką | Užtikrinti, kad incidentų valdymo planas būtų formaliai patvirtintas ir periodiškai peržiūrimas atsižvelgiant į naujas grėsmes ir incidentų patirtį. |
| R3-INC-01-ACT2 | 2 | Patvirtinti incidentų valdymo planą ir nustatyti jo peržiūros tvarką | Užtikrinti, kad incidentų valdymo planas būtų formaliai patvirtintas ir periodiškai peržiūrimas atsižvelgiant į naujas grėsmes ir incidentų patirtį. |
| R3-INC-01-ACT2 | 2 | Patvirtinti incidentų valdymo planą ir nustatyti jo peržiūros tvarką | Užtikrinti, kad incidentų valdymo planas būtų formaliai patvirtintas ir periodiškai peržiūrimas atsižvelgiant į naujas grėsmes ir incidentų patirtį. |

| | | | |
|---|---|---|---|
| R3-INC-02-ACT1 | 1 | Sukurti incidentų klasifikavimo ir prioritetų nustatymo sistemą | Apibrėžti incidentų kategorijas, kritiškumo lygius ir susieti juos su reagavimo terminais bei eskalavimo taisyklėmis. |
| R3-INC-02-ACT1 | 1 | Sukurti incidentų klasifikavimo ir prioritetų nustatymo sistemą | Apibrėžti incidentų kategorijas, kritiškumo lygius ir susieti juos su reagavimo terminais bei eskalavimo taisyklėmis. |
| R3-INC-02-ACT2 | 2 | Apibrėžti incidentų valdymo atsakomybes ir komunikacijos grandinę | Nustatyti, kas organizacijoje atsakingas už incidentų registravimą, analizę, sprendimų priėmimą ir komunikaciją su išorės institucijomis bei klientais. |
| R3-INC-02-ACT2 | 2 | Apibrėžti incidentų valdymo atsakomybes ir komunikacijos grandinę | Nustatyti, kas organizacijoje atsakingas už incidentų registravimą, analizę, sprendimų priėmimą ir komunikaciją su išorės institucijomis bei klientais. |
| R3-INC-03-ACT1 | 1 | Įvertinti esamas incidentų aptikimo priemones ir aprėptį | Analizuoti, kokios techninės priemonės šiuo metu naudojamos incidentams aptikti ir kokią infrastruktūros dalį jos realiai dengia. |
| R3-INC-03-ACT1 | 1 | Įvertinti esamas incidentų aptikimo priemones ir aprėptį | Analizuoti, kokios techninės priemonės šiuo metu naudojamos incidentams aptikti ir kokią infrastruktūros dalį jos realiai dengia. |
| R3-INC-03-ACT2 | 2 | Sustiprinti incidentų aptikimą realiuoju laiku | Įdiegti arba sustiprinti SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema)/EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas) ir kitus monitoring'o sprendimus, užtikrinančius artimą realiam laikui incidentų identifikavimą ir eskalavimą. |
| R3-INC-03-ACT2 | 2 | Sustiprinti incidentų aptikimą realiuoju laiku | Įdiegti arba sustiprinti SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema)/EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas) ir kitus monitoring'o sprendimus, užtikrinančius artimą realiam laikui incidentų identifikavimą ir eskalavimą. |
| R3-INC-04-ACT1 | 1 | Nustatyti kritines sistemas ir jų žurnalų rinkimo apimtį | Identifikuoti kritines sistemas ir apibrėžti, kokie įvykiai iš jų turi būti renkami incidentų aptikimo ir tyrimo tikslais. |
| R3-INC-04-ACT1 | 1 | Nustatyti kritines sistemas ir jų žurnalų rinkimo apimtį | Identifikuoti kritines sistemas ir apibrėžti, kokie įvykiai iš jų turi būti renkami incidentų aptikimo ir tyrimo tikslais. |
| R3-INC-04-ACT2 | 2 | Centralizuoti kritinių sistemų žurnalų rinkimą | Įgyvendinti techninį sprendimą, leidžiantį centralizuotai rinkti ir saugoti žurnalus iš visų kritinių sistemų. |
| R3-INC-04-ACT2 | 2 | Centralizuoti kritinių sistemų žurnalų rinkimą | Įgyvendinti techninį sprendimą, leidžiantį centralizuotai rinkti ir saugoti žurnalus iš visų kritinių sistemų. |
| R3-INC-05-ACT1 | 1 | Parengti žurnalų saugojimo politiką ir reikalavimus | Apibrėžti minimalų žurnalų saugojimo laiką pagal teisės aktus, reguliuotojų rekomendacijas ir organizacijos poreikius. |
| R3-INC-05-ACT1 | 1 | Parengti žurnalų saugojimo politiką ir reikalavimus | Apibrėžti minimalų žurnalų saugojimo laiką pagal teisės aktus, reguliuotojų rekomendacijas ir organizacijos poreikius. |

| | | | |
|---|---|---|---|
| R3-INC-05-ACT2 | 2 | Sukonfigūruoti žurnalų saugojimo terminus techninėse sistemose | Techninėse žurnalų rinkimo ir saugojimo sistemose nustatyti saugojimo trukmę, atsižvelgiant į politikos reikalavimus ir saugojimo apimtis. |
| R3-INC-05-ACT2 | 2 | Sukonfigūruoti žurnalų saugojimo terminus techninėse sistemose | Techninėse žurnalų rinkimo ir saugojimo sistemose nustatyti saugojimo trukmę, atsižvelgiant į politikos reikalavimus ir saugojimo apimtis. |
| R3-INC-06-ACT1 | 1 | Nustatyti žurnalų vientisumo kontrolės reikalavimus | Apibrėžti, kokiu lygiu turi būti užtikrintas žurnalų integritetas ir kokios techninės priemonės tam bus naudojamos. |
| R3-INC-06-ACT1 | 1 | Nustatyti žurnalų vientisumo kontrolės reikalavimus | Apibrėžti, kokiu lygiu turi būti užtikrintas žurnalų integritetas ir kokios techninės priemonės tam bus naudojamos. |
| R3-INC-06-ACT2 | 2 | Įgyvendinti žurnalų vientisumo kontrolės mechanizmus | Sukonfigūruoti žurnalų saugyklas ir prieigos mechanizmus taip, kad neautorizuotas žurnalų keitimas ar ištrynimas būtų aptinkamas ar techniškai neįmanomas. |
| R3-INC-06-ACT2 | 2 | Įgyvendinti žurnalų vientisumo kontrolės mechanizmus | Sukonfigūruoti žurnalų saugyklas ir prieigos mechanizmus taip, kad neautorizuotas žurnalų keitimas ar ištrynimas būtų aptinkamas ar techniškai neįmanomas. |
| R3-INC-07-ACT1 | 1 | Apibrėžti žurnalų peržiūros ir eskalavimo procesą | Nustatyti, kokie žurnalai, kokiu periodiškumu ir kokiu detalumu turi būti peržiūrimi bei kaip identifikuotos anomalijos eskaluojamos incidentų valdymo komandai. |
| R3-INC-07-ACT1 | 1 | Apibrėžti žurnalų peržiūros ir eskalavimo procesą | Nustatyti, kokie žurnalai, kokiu periodiškumu ir kokiu detalumu turi būti peržiūrimi bei kaip identifikuotos anomalijos eskaluojamos incidentų valdymo komandai. |
| R3-INC-07-ACT2 | 2 | Įdiegti žurnalų analizės vykdymą ir stebėti efektyvumą | Organizuoti žurnalų analizės vykdymą pagal nustatytą grafiką ir sekti pagrindinius veiklos rodiklius. |
| R3-INC-07-ACT2 | 2 | Įdiegti žurnalų analizės vykdymą ir stebėti efektyvumą | Organizuoti žurnalų analizės vykdymą pagal nustatytą grafiką ir sekti pagrindinius veiklos rodiklius. |
| R3-INC-08-ACT1 | 1 | Įvertinti organizacijos incidentų tyrimo / forensikos galimybes | Nustatyti, kokius incidentų tyrimo ir skaitmeninės forensikos veiksmus organizacija gali atlikti savarankiškai, o kuriems reikalingi išoriniai partneriai. |
| R3-INC-08-ACT1 | 1 | Įvertinti organizacijos incidentų tyrimo / forensikos galimybes | Nustatyti, kokius incidentų tyrimo ir skaitmeninės forensikos veiksmus organizacija gali atlikti savarankiškai, o kuriems reikalingi išoriniai partneriai. |
| R3-INC-08-ACT2 | 2 | Sukurti ar sustiprinti incidentų tyrimo ir forensikos pajėgumus | Viduje suformuoti minimalų incidentų tyrimo pajėgumą ir / arba sudaryti sutartis su išoriniais forensikos paslaugų teikėjais. |
| R3-INC-08-ACT2 | 2 | Sukurti ar sustiprinti incidentų tyrimo ir forensikos pajėgumus | Viduje suformuoti minimalų incidentų tyrimo pajėgumą ir / arba sudaryti sutartis su išoriniais forensikos paslaugų teikėjais. |
| R3-INC-09-ACT1 | 1 | Sukurti ankstyvo įspėjimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procesą | Nustatyti, kokie incidentai ir kokiomis sąlygomis turi būti traktuojami kaip reikšmingi, bei apibrėžti procesą, kaip per 24 val. parengiamas ir pateikiamas įspėjimas NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)). |
| R3-INC-09-ACT1 | 1 | Sukurti ankstyvo įspėjimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procesą | Nustatyti, kokie incidentai ir kokiomis sąlygomis turi būti traktuojami kaip reikšmingi, bei apibrėžti procesą, kaip per 24 val. parengiamas ir pateikiamas įspėjimas NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)). |
| R3-INC-09-ACT2 | 2 | Įtvirtinti ankstyvo įspėjimo procesą praktikoje | Užtikrinti, kad ankstyvo įspėjimo procesas būtų žinomas incidentų reagavimo komandoms ir būtų periodiškai testuojamas. |

| | | | |
|---|---|---|---|
| R3-INC-09-ACT2 | 2 | Įtvirtinti ankstyvo įspėjimo procesą praktikoje | Užtikrinti, kad ankstyvo įspėjimo procesas būtų žinomas incidentų reagavimo komandoms ir būtų periodiškai testuojamas. |
| R3-INC-10-ACT1 | 1 | Sukurti incidento pranešimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procedūrą ir dokumentų šablonus | Aprašyti žingsnius ir atsakomybės, kaip surenkama informacija incidento pranešimui ir parengiami dokumentai pagal NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) reikalavimus. |
| R3-INC-10-ACT1 | 1 | Sukurti incidento pranešimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procedūrą ir dokumentų šablonus | Aprašyti žingsnius ir atsakomybės, kaip surenkama informacija incidento pranešimui ir parengiami dokumentai pagal NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) reikalavimus. |
| R3-INC-10-ACT2 | 2 | Įtvirtinti incidentų pranešimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procesą praktikoje | Užtikrinti, kad atsakingi asmenys žinotų pranešimo tvarką ir būtų įmanoma surinkti reikiamą informaciją per 72 valandas. |
| R3-INC-10-ACT2 | 2 | Įtvirtinti incidentų pranešimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procesą praktikoje | Užtikrinti, kad atsakingi asmenys žinotų pranešimo tvarką ir būtų įmanoma surinkti reikiamą informaciją per 72 valandas. |
| R3-INC-11-ACT1 | 1 | Sukurti incidentų galutinės ataskaitos struktūrą ir parengimo procesą | Nustatyti, kokia informacija turi būti pateikiama galutinėje ataskaitoje ir kokie padaliniai prisideda prie jos parengimo. |
| R3-INC-11-ACT1 | 1 | Sukurti incidentų galutinės ataskaitos struktūrą ir parengimo procesą | Nustatyti, kokia informacija turi būti pateikiama galutinėje ataskaitoje ir kokie padaliniai prisideda prie jos parengimo. |
| R3-INC-11-ACT2 | 2 | Įgyvendinti galutinių ataskaitų rengimo procesą | Suorganizuoti incidentų tyrimo ir dokumentavimo veiksmus taip, kad galutinė ataskaita būtų parengta per vieną mėnesį. |
| R3-INC-11-ACT2 | 2 | Įgyvendinti galutinių ataskaitų rengimo procesą | Suorganizuoti incidentų tyrimo ir dokumentavimo veiksmus taip, kad galutinė ataskaita būtų parengta per vieną mėnesį. |
| R3-INC-12-ACT1 | 1 | Apibrėžti incidentų, apie kuriuos informuojami klientai, kriterijus | Nustatyti, kokiais atvejais klientai privalo būti informuoti apie incidentus ir kokia informacija jiems teikiama. |
| R3-INC-12-ACT1 | 1 | Apibrėžti incidentų, apie kuriuos informuojami klientai, kriterijus | Nustatyti, kokiais atvejais klientai privalo būti informuoti apie incidentus ir kokia informacija jiems teikiama. |
| R3-INC-12-ACT2 | 2 | Įgyvendinti klientų informavimo procesą incidentų atvejais | Užtikrinti, kad klientų informavimas būtų koordinuotas, nuoseklus ir dokumentuotas. |
| R3-INC-12-ACT2 | 2 | Įgyvendinti klientų informavimo procesą incidentų atvejais | Užtikrinti, kad klientų informavimas būtų koordinuotas, nuoseklus ir dokumentuotas. |
| R3-INC-13-ACT1 | 1 | Sukurti po incidentų atliekamos pamokų analizės procesą | Nustatyti, kaip ir kada atliekama incidento peržiūra po įvykio, kokie dalyviai įtraukiami ir kokie rezultatai tikimasi. |
| R3-INC-13-ACT1 | 1 | Sukurti po incidentų atliekamos pamokų analizės procesą | Nustatyti, kaip ir kada atliekama incidento peržiūra po įvykio, kokie dalyviai įtraukiami ir kokie rezultatai tikimasi. |
| R3-INC-13-ACT2 | 2 | Integruoti pamokas į procesų, kontrolės ir mokymų tobulinimą | Užtikrinti, kad pamokų analizės išvados virstų konkrečiomis tobulinimo priemonėmis ir būtų stebimas jų įgyvendinimas. |
| R3-INC-13-ACT2 | 2 | Integruoti pamokas į procesų, kontrolės ir mokymų tobulinimą | Užtikrinti, kad pamokų analizės išvados virstų konkrečiomis tobulinimo priemonėmis ir būtų stebimas jų įgyvendinimas. |

| | | | |
|---|---|---|---|
| R4-TĘS-01-ACT1 | 1 | Parengti veiklos tęstinumo ir IT (Information Technology, informacinės technologijos) atkūrimo (BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas)) planą | Sukurti išsamų BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą, grįstą rizikos vertinimu, kritinių procesų ir priklausomybių analize. |
| R4-TĘS-01-ACT1 | 1 | Parengti veiklos tęstinumo ir IT (Information Technology, informacinės technologijos) atkūrimo (BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas)) planą | Sukurti išsamų BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą, grįstą rizikos vertinimu, kritinių procesų ir priklausomybių analize. |
| R4-TĘS-01-ACT2 | 2 | Patvirtinti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą ir nustatyti jo peržiūros tvarką | Formalizuoti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą, užtikrinant vadovybės pritarimą ir periodinę peržiūrą. |
| R4-TĘS-01-ACT2 | 2 | Patvirtinti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą ir nustatyti jo peržiūros tvarką | Formalizuoti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą, užtikrinant vadovybės pritarimą ir periodinę peržiūrą. |
| R4-TĘS-02-ACT1 | 1 | Nustatyti RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO)) ir RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) kritinėms paslaugoms | Suderinti su verslo padaliniais ir IT (Information Technology, informacinės technologijos), kokio atkūrimo laiko (RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))) ir duomenų praradimo apimties (RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO))) reikia kiekvienai kritinei paslaugai. |
| R4-TĘS-02-ACT1 | 1 | Nustatyti RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO)) ir RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) kritinėms paslaugoms | Suderinti su verslo padaliniais ir IT (Information Technology, informacinės technologijos), kokio atkūrimo laiko (RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))) ir duomenų praradimo apimties (RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO))) reikia kiekvienai kritinei paslaugai. |
| R4-TĘS-02-ACT2 | 2 | Integruoti RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslus į BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) ir technologinius sprendimus | Užtikrinti, kad RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslai būtų aiškiai dokumentuoti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) plane ir atitinkamai įgyvendinti atsarginių kopijų, HA (High Availability, didelio pasiekiamumo architektūra) ir georedundancy sprendimuose. |
| R4-TĘS-02-ACT2 | 2 | Integruoti RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslus į BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) ir technologinius sprendimus | Užtikrinti, kad RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslai būtų aiškiai dokumentuoti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) plane ir atitinkamai įgyvendinti atsarginių kopijų, HA (High Availability, didelio pasiekiamumo architektūra) ir georedundancy sprendimuose. |
| R4-TĘS-03-ACT1 | 1 | Parengti krizių valdymo (crisis management) planą | Apibrėžti krizinės situacijos sąvoką, krizių valdymo komandą, sprendimų priėmimo tvarką ir komunikacijos principus. |
| R4-TĘS-03-ACT1 | 1 | Parengti krizių valdymo (crisis management) planą | Apibrėžti krizinės situacijos sąvoką, krizių valdymo komandą, sprendimų priėmimo tvarką ir komunikacijos principus. |
| R4-TĘS-03-ACT2 | 2 | Patvirtinti krizių valdymo planą ir suderinti su kitais planais | Integruoti krizių valdymo planą su BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas), incidentų ir komunikacijos planais. |
| R4-TĘS-03-ACT2 | 2 | Patvirtinti krizių valdymo planą ir suderinti su kitais planais | Integruoti krizių valdymo planą su BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster |

| | | | |
|---|---|---|---|
| | | | Recovery Plan, veiklos atkūrimo planas), incidentų ir komunikacijos planais. |
| R4-TĘS-04-ACT1 | 1 | Parengti atsarginių kopijų (backup) politiką ir standartus | Dokumentuoti reikalavimus dėl atsarginių kopijų dažnio, apimties, saugojimo vietos, testavimo ir atsakomybių. |
| R4-TĘS-04-ACT1 | 1 | Parengti atsarginių kopijų (backup) politiką ir standartus | Dokumentuoti reikalavimus dėl atsarginių kopijų dažnio, apimties, saugojimo vietos, testavimo ir atsakomybių. |
| R4-TĘS-04-ACT2 | 2 | Patvirtinti atsarginių kopijų tvarką ir integruoti į operacijas | Formalizuoti atsarginių kopijų tvarką ir užtikrinti, kad IT (Information Technology, informacinės technologijos) operacijos jos laikytųsi. |
| R4-TĘS-04-ACT2 | 2 | Patvirtinti atsarginių kopijų tvarką ir integruoti į operacijas | Formalizuoti atsarginių kopijų tvarką ir užtikrinti, kad IT (Information Technology, informacinės technologijos) operacijos jos laikytųsi. |
| R4-TĘS-05-ACT1 | 1 | Sukonfigūruoti automatizuotus backup procesus | Parinkti ir sukonfigūruoti techninius sprendimus, kurie automatiškai kuria atsargines kopijas pagal politiką. |
| R4-TĘS-05-ACT1 | 1 | Sukonfigūruoti automatizuotus backup procesus | Parinkti ir sukonfigūruoti techninius sprendimus, kurie automatiškai kuria atsargines kopijas pagal politiką. |
| R4-TĘS-05-ACT2 | 2 | Įdiegti atsarginių kopijų stebėsenos ir incidentų valdymo tvarką | Sukonfigūruoti monitoringą ir reagavimą į nepavykusias atsarginių kopijų užduotis. |
| R4-TĘS-05-ACT2 | 2 | Įdiegti atsarginių kopijų stebėsenos ir incidentų valdymo tvarką | Sukonfigūruoti monitoringą ir reagavimą į nepavykusias atsarginių kopijų užduotis. |
| R4-TĘS-06-ACT1 | 1 | Pasirinkti ir suprojektuoti offsite atsarginių kopijų saugojimo sprendimą | Nustatyti, kokio tipo offsite saugykla bus naudojama (antrinis DC (Domain Controller, domeno valdiklis), debesija, juostų saugykla) ir kokie izoliacijos reikalavimai taikomi. |
| R4-TĘS-06-ACT1 | 1 | Pasirinkti ir suprojektuoti offsite atsarginių kopijų saugojimo sprendimą | Nustatyti, kokio tipo offsite saugykla bus naudojama (antrinis DC (Domain Controller, domeno valdiklis), debesija, juostų saugykla) ir kokie izoliacijos reikalavimai taikomi. |
| R4-TĘS-06-ACT2 | 2 | Įdiegti offsite atsarginių kopijų replikavimą ir izoliaciją | Techniniu lygmeniu užtikrinti, kad atsarginės kopijos būtų replikuojamos ir saugomos izoliuotoje aplinkoje. |
| R4-TĘS-06-ACT2 | 2 | Įdiegti offsite atsarginių kopijų replikavimą ir izoliaciją | Techniniu lygmeniu užtikrinti, kad atsarginės kopijos būtų replikuojamos ir saugomos izoliuotoje aplinkoje. |
| R4-TĘS-07-ACT1 | 1 | Apibrėžti šifravimo politiką atsarginėms kopijoms | Dokumentuoti, kokiu lygiu ir kokiomis priemonėmis turi būti šifruojamos atsarginės kopijos bei kaip valdomi raktai. |
| R4-TĘS-07-ACT1 | 1 | Apibrėžti šifravimo politiką atsarginėms kopijoms | Dokumentuoti, kokiu lygiu ir kokiomis priemonėmis turi būti šifruojamos atsarginės kopijos bei kaip valdomi raktai. |
| R4-TĘS-07-ACT2 | 2 | Sukonfigūruoti šifravimą atsarginių kopijų kūrimo ir saugojimo infrastruktūroje | Techniniu lygmeniu įjungti ir patikrinti šifravimą backup sprendimuose bei užtikrinti saugų raktų valdymą. |

| | | | |
|---|---|---|---|
| R4-TĘS-07-ACT2 | 2 | Sukonfigūruoti šifravimą atsarginių kopijų kūrimo ir saugojimo infrastruktūroje | Techniniu lygmeniu įjungti ir patikrinti šifravimą backup sprendimuose bei užtikrinti saugų raktų valdymą. |
| R4-TĘS-08-ACT1 | 1 | Sukurti atsarginių kopijų atkūrimo testavimo planą | Apibrėžti, kokios sistemos, kokiu dažniu ir kokiu mastu turi būti testuojamos atkuriant duomenis iš atsarginių kopijų. |
| R4-TĘS-08-ACT1 | 1 | Sukurti atsarginių kopijų atkūrimo testavimo planą | Apibrėžti, kokios sistemos, kokiu dažniu ir kokiu mastu turi būti testuojamos atkuriant duomenis iš atsarginių kopijų. |
| R4-TĘS-08-ACT2 | 2 | Įgyvendinti duomenų atkūrimo testus ir vertinti rezultatus | Reguliariai vykdyti atkūrimo testus, fiksuoti rezultatus ir imtis tobulinimo priemonių. |
| R4-TĘS-08-ACT2 | 2 | Įgyvendinti duomenų atkūrimo testus ir vertinti rezultatus | Reguliariai vykdyti atkūrimo testus, fiksuoti rezultatus ir imtis tobulinimo priemonių. |
| R4-TĘS-09-ACT1 | 1 | Suplanuoti kritinių sistemų aukšto pasiekiamumo (HA (High Availability, didelio pasiekiamumo architektūra)) architektūrą | Identifikuoti kritines sistemas ir suplanuoti joms HA (High Availability, didelio pasiekiamumo architektūra) architektūrą (clustering, load balancing, redundanti komponentai). |
| R4-TĘS-09-ACT1 | 1 | Suplanuoti kritinių sistemų aukšto pasiekiamumo (HA (High Availability, didelio pasiekiamumo architektūra)) architektūrą | Identifikuoti kritines sistemas ir suplanuoti joms HA (High Availability, didelio pasiekiamumo architektūra) architektūrą (clustering, load balancing, redundanti komponentai). |
| R4-TĘS-09-ACT2 | 2 | Įdiegti HA (High Availability, didelio pasiekiamumo architektūra) sprendimus ir atlikti failover testus | Techniniu lygmeniu įdiegti HA (High Availability, didelio pasiekiamumo architektūra) sprendimus ir periodiškai testuoti jų veikimą. |
| R4-TĘS-09-ACT2 | 2 | Įdiegti HA (High Availability, didelio pasiekiamumo architektūra) sprendimus ir atlikti failover testus | Techniniu lygmeniu įdiegti HA (High Availability, didelio pasiekiamumo architektūra) sprendimus ir periodiškai testuoti jų veikimą. |
| R4-TĘS-10-ACT1 | 1 | Apibrėžti esminių sistemų georedundancy strategiją | Nustatyti, kurios sistemos turi būti geografiškai dubliuotos ir kokiu būdu (antrinis DC (Domain Controller, domeno valdiklis), multi-region cloud). |
| R4-TĘS-10-ACT1 | 1 | Apibrėžti esminių sistemų georedundancy strategiją | Nustatyti, kurios sistemos turi būti geografiškai dubliuotos ir kokiu būdu (antrinis DC (Domain Controller, domeno valdiklis), multi-region cloud). |
| R4-TĘS-10-ACT2 | 2 | Įdiegti geografinę dubliaciją ir testuoti perjungimą | Realizuoti georedundancy architektūrą ir periodiškai testuoti, ar sistema gali perjungti paslaugas į kitą lokaciją. |
| R4-TĘS-10-ACT2 | 2 | Įdiegti geografinę dubliaciją ir testuoti perjungimą | Realizuoti georedundancy architektūrą ir periodiškai testuoti, ar sistema gali perjungti paslaugas į kitą lokaciją. |
| R4-TĘS-11-ACT1 | 1 | Parengti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybų planą ir scenarijus | Apibrėžti pratybų tikslus, scenarijus, dalyvius ir periodiškumą (bent kartą per metus). |
| R4-TĘS-11-ACT1 | 1 | Parengti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybų planą ir scenarijus | Apibrėžti pratybų tikslus, scenarijus, dalyvius ir periodiškumą (bent kartą per metus). |

| | | | |
|---|---|---|---|
| R4-TĘS-11-ACT2 | 2 | Įgyvendinti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybas ir panaudoti rezultatus tobulinimui | Reguliariai vykdyti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybas ir remiantis jų rezultatais tobulinti planus ir procesus. |
| R4-TĘS-11-ACT2 | 2 | Įgyvendinti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybas ir panaudoti rezultatus tobulinimui | Reguliariai vykdyti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybas ir remiantis jų rezultatais tobulinti planus ir procesus. |
| R5-TIEK-01-ACT1 | 1 | Parengti tiekimo grandinės saugumo politikos projektą | Sukurti politikos dokumentą, apimantį tiekėjų atranką, vertinimą, stebėseną, incidentų valdymą ir nutraukimo sąlygas. |
| R5-TIEK-01-ACT1 | 1 | Parengti tiekimo grandinės saugumo politikos projektą | Sukurti politikos dokumentą, apimantį tiekėjų atranką, vertinimą, stebėseną, incidentų valdymą ir nutraukimo sąlygas. |
| R5-TIEK-01-ACT2 | 2 | Patvirtinti ir iškomunikuoti tiekimo grandinės saugumo politiką | Užtikrinti, kad politika būtų patvirtinta vadovybės ir žinoma pirkimų, IT (Information Technology, informacinės technologijos) ir verslo komandoms. |
| R5-TIEK-01-ACT2 | 2 | Patvirtinti ir iškomunikuoti tiekimo grandinės saugumo politiką | Užtikrinti, kad politika būtų patvirtinta vadovybės ir žinoma pirkimų, IT (Information Technology, informacinės technologijos) ir verslo komandoms. |
| R5-TIEK-02-ACT1 | 1 | Sukurti tiekėjų kibernetinio saugumo atrankos kriterijus | Nustatyti, kokie saugumo aspektai turi būti vertinami prieš pasirenkant tiekėją (pvz., sertifikatai, procesai, technologijos). |
| R5-TIEK-02-ACT1 | 1 | Sukurti tiekėjų kibernetinio saugumo atrankos kriterijus | Nustatyti, kokie saugumo aspektai turi būti vertinami prieš pasirenkant tiekėją (pvz., sertifikatai, procesai, technologijos). |
| R5-TIEK-02-ACT2 | 2 | Integruoti saugumo atrankos kriterijus į pirkimų procesą | Užtikrinti, kad atrankos kriterijai būtų realiai taikomi pirkimų metu. |
| R5-TIEK-02-ACT2 | 2 | Integruoti saugumo atrankos kriterijus į pirkimų procesą | Užtikrinti, kad atrankos kriterijai būtų realiai taikomi pirkimų metu. |
| R5-TIEK-03-ACT1 | 1 | Sukurti standartinių kibernetinio saugumo sąlygų rinkinį sutartims | Parengti tipinių sutartinių punktų rinkinį, apimantį saugumo reikalavimus, auditą, incidentų pranešimą, subtiekėjus ir paslaugų nutraukimą. |
| R5-TIEK-03-ACT1 | 1 | Sukurti standartinių kibernetinio saugumo sąlygų rinkinį sutartims | Parengti tipinių sutartinių punktų rinkinį, apimantį saugumo reikalavimus, auditą, incidentų pranešimą, subtiekėjus ir paslaugų nutraukimą. |
| R5-TIEK-03-ACT2 | 2 | Taikyti standartines saugumo sąlygas sudarant ir atnaujinant sutartis | Užtikrinti, kad naujos ir atnaujinamos sutartys su tiekėjais sistemingai įtrauktų standartinius saugumo reikalavimus. |
| R5-TIEK-03-ACT2 | 2 | Taikyti standartines saugumo sąlygas sudarant ir atnaujinant sutartis | Užtikrinti, kad naujos ir atnaujinamos sutartys su tiekėjais sistemingai įtrauktų standartinius saugumo reikalavimus. |
| R5-TIEK-04-ACT1 | 1 | Sukurti tiekėjų incidentų pranešimo reikalavimų rinkinį | Apibrėžti, kokie incidentai turi būti pranešami, kokiu terminu ir kokią informaciją tiekėjas turi pateikti. |
| R5-TIEK-04-ACT1 | 1 | Sukurti tiekėjų incidentų pranešimo reikalavimų rinkinį | Apibrėžti, kokie incidentai turi būti pranešami, kokiu terminu ir kokią informaciją tiekėjas turi pateikti. |
| R5-TIEK-04-ACT2 | 2 | Įtraukti incidentų pranešimo reikalavimus į sutartis ir incidentų valdymo procesą | Užtikrinti, kad tiekėjų incidentų pranešimo pareiga būtų įtvirtinta sutartyse ir integruota į incidentų valdymo procedūras. |
| R5-TIEK-04-ACT2 | 2 | Įtraukti incidentų pranešimo reikalavimus į sutartis ir incidentų valdymo procesą | Užtikrinti, kad tiekėjų incidentų pranešimo pareiga būtų įtvirtinta sutartyse ir integruota į incidentų valdymo procedūras. |
| R5-TIEK-05-ACT1 | 1 | Sukurti tiekėjų auditavimo politiką ir kriterijus | Nustatyti, kada ir kokiu mastu gali būti audituojami tiekėjai ir kokios alternatyvos (pvz., trečiųjų šalių ataskaitos) priimtinos. |

| | | | |
|---|---|---|---|
| R5-TIEK-05-ACT1 | 1 | Sukurti tiekėjų auditavimo politiką ir kriterijus | Nustatyti, kada ir kokiu mastu gali būti audituojami tiekėjai ir kokios alternatyvos (pvz., trečiųjų šalių ataskaitos) priimtinos. |
| R5-TIEK-05-ACT2 | 2 | Įdiegti tiekėjų kibernetinio saugumo audito procesą | Sukurti praktinį tiekėjų auditų planą ir periodiškai jį vykdyti. |
| R5-TIEK-05-ACT2 | 2 | Įdiegti tiekėjų kibernetinio saugumo audito procesą | Sukurti praktinį tiekėjų auditų planą ir periodiškai jį vykdyti. |
| R5-TIEK-06-ACT1 | 1 | Apibrėžti kritinių tiekėjų kriterijus ir sukurti registrą | Nustatyti, kurie tiekėjai laikomi kritiniais ir kokia informacija turi būti kaupiama apie juos registre. |
| R5-TIEK-06-ACT1 | 1 | Apibrėžti kritinių tiekėjų kriterijus ir sukurti registrą | Nustatyti, kurie tiekėjai laikomi kritiniais ir kokia informacija turi būti kaupiama apie juos registre. |
| R5-TIEK-06-ACT2 | 2 | Užpildyti kritinių tiekėjų registrą ir nustatyti palaikymo atsakomybes | Sistemingai užpildyti registrą ir paskirti atsakingus už jo palaikymą. |
| R5-TIEK-06-ACT2 | 2 | Užpildyti kritinių tiekėjų registrą ir nustatyti palaikymo atsakomybes | Sistemingai užpildyti registrą ir paskirti atsakingus už jo palaikymą. |
| R5-TIEK-07-ACT1 | 1 | Sukurti tiekėjų kibernetinio saugumo rizikos vertinimo metodiką | Apibrėžti, kokie rizikos veiksniai ir šaltiniai vertinami, kokia scoring logika taikoma ir kaip rizika susiejama su kritiškumu. |
| R5-TIEK-07-ACT1 | 1 | Sukurti tiekėjų kibernetinio saugumo rizikos vertinimo metodiką | Apibrėžti, kokie rizikos veiksniai ir šaltiniai vertinami, kokia scoring logika taikoma ir kaip rizika susiejama su kritiškumu. |
| R5-TIEK-07-ACT2 | 2 | Pritaikyti rizikos vertinimo metodiką kritiniams tiekėjams | Įvertinti kritinius tiekėjus pagal parengtą metodiką ir susieti rezultatus su rizikos registru ir veiksmų planais. |
| R5-TIEK-07-ACT2 | 2 | Pritaikyti rizikos vertinimo metodiką kritiniams tiekėjams | Įvertinti kritinius tiekėjus pagal parengtą metodiką ir susieti rezultatus su rizikos registru ir veiksmų planais. |
| R5-TIEK-08-ACT1 | 1 | Nustatyti atsakomybę už ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) tiekimo grandinės rizikos vertinimų stebėseną | Paskirti atsakingą funkciją, kuri reguliariai seka ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) ir nacionalinių institucijų skelbiamus tiekimo grandinės rizikos vertinimus ir gaires. |
| R5-TIEK-08-ACT1 | 1 | Nustatyti atsakomybę už ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) tiekimo grandinės rizikos vertinimų stebėseną | Paskirti atsakingą funkciją, kuri reguliariai seka ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) ir nacionalinių institucijų skelbiamus tiekimo grandinės rizikos vertinimus ir gaires. |
| R5-TIEK-08-ACT2 | 2 | Pritaikyti ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) tiekimo grandinės rizikos vertinimų išvadas organizacijos tiekėjų valdyme | Organizacijos tiekėjų rizikos vertinimo ir atrankos kriterijus koreguoti atsižvelgiant į ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) ir nacionalinius rizikos vertinimus. |
| R5-TIEK-08-ACT2 | 2 | Pritaikyti ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) tiekimo grandinės rizikos vertinimų išvadas organizacijos tiekėjų valdyme | Organizacijos tiekėjų rizikos vertinimo ir atrankos kriterijus koreguoti atsižvelgiant į ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) ir nacionalinius rizikos vertinimus. |
| R5-TIEK-09-ACT1 | 1 | Parinkti ir įdiegti tiekėjų rizikos valdymo (TPRM (Third-Party Risk Management, trečiųjų šalių rizikos valdymas)) sprendimą | Įvertinti rinkos sprendimus ir pasirinkti platformą, kuri palaiko klausimynus, sertifikatų rinkimą, scoring'ą ir ataskaitas. |
| R5-TIEK-09-ACT1 | 1 | Parinkti ir įdiegti tiekėjų rizikos valdymo (TPRM (Third-Party Risk Management, trečiųjų šalių rizikos valdymas)) sprendimą | Įvertinti rinkos sprendimus ir pasirinkti platformą, kuri palaiko klausimynus, sertifikatų rinkimą, scoring'ą ir ataskaitas. |

| | | | |
|---|---|---|---|
| R5-TIEK-09-ACT2 | 2 | Sukonfigūruoti klausimynus, scoring'ą ir integracijas TPRM (Third-Party Risk Management, trečiųjų šalių rizikos valdymas) platformoje | Perkelti metodiką ir procesus į platformą, užtikrinant automatizuotą klausimynų siuntimą, scoring'ą ir ataskaitas. |
| R5-TIEK-09-ACT2 | 2 | Sukonfigūruoti klausimynus, scoring'ą ir integracijas TPRM (Third-Party Risk Management, trečiųjų šalių rizikos valdymas) platformoje | Perkelti metodiką ir procesus į platformą, užtikrinant automatizuotą klausimynų siuntimą, scoring'ą ir ataskaitas. |
| R6-PLĖ-01-ACT1 | 1 | Apibrėžti saugaus įsigijimo ir plėtros politikos taikymo sritį bei principus | Nustatyti, kokiems projektams, sistemoms ir paslaugoms taikoma saugaus įsigijimo ir plėtros politika ir kokie esminiai saugumo principai privalomi. |
| R6-PLĖ-01-ACT1 | 1 | Apibrėžti saugaus įsigijimo ir plėtros politikos taikymo sritį bei principus | Nustatyti, kokiems projektams, sistemoms ir paslaugoms taikoma saugaus įsigijimo ir plėtros politika ir kokie esminiai saugumo principai privalomi. |
| R6-PLĖ-01-ACT2 | 2 | Parengti ir suderinti saugaus įsigijimo ir plėtros politikos dokumentą | Sukurti detalų politikos dokumentą ir suderinti jį su pagrindiniais suinteresuotais padaliniais. |
| R6-PLĖ-01-ACT2 | 2 | Parengti ir suderinti saugaus įsigijimo ir plėtros politikos dokumentą | Sukurti detalų politikos dokumentą ir suderinti jį su pagrindiniais suinteresuotais padaliniais. |
| R6-PLĖ-01-ACT3 | 3 | Patvirtinti politiką ir integruoti ją į projektų bei pirkimų valdymo procesus | Užtikrinti, kad politika būtų oficialiai patvirtinta ir privaloma projektų ir pirkimų valdyme. |
| R6-PLĖ-02-ACT1 | 1 | Pasirinkti ir adaptuoti saugaus SDLC (Software Development Lifecycle, programinės įrangos kūrimo gyvavimo ciklas) modelį | Išsirinkti ir pritaikyti organizacijai tinkamą saugaus SDLC (Software Development Lifecycle, programinės įrangos kūrimo gyvavimo ciklas) modelį, apibrėžiant saugumo veiklas kiekviename etape. |
| R6-PLĖ-02-ACT2 | 2 | Integruoti saugumo kontrolės priemones į kūrimo ir CI (Continuous Integration, nuolatinio integravimo praktika)/CD (Compact Disc, kompaktinis diskas) procesus | Techniniu lygmeniu įdiegti statinę ir dinaminę analizę, priklausomybių skenavimą ir kitus saugumo kontrolės taškus kūrimo grandinėje. |
| R6-PLĖ-02-ACT2 | 2 | Integruoti saugumo kontrolės priemones į kūrimo ir CI (Continuous Integration, nuolatinio integravimo praktika)/CD (Compact Disc, kompaktinis diskas) procesus | Techniniu lygmeniu įdiegti statinę ir dinaminę analizę, priklausomybių skenavimą ir kitus saugumo kontrolės taškus kūrimo grandinėje. |
| R6-PLĖ-02-ACT2 | 2 | Integruoti saugumo kontrolės priemones į kūrimo ir CI (Continuous Integration, nuolatinio integravimo praktika)/CD (Compact Disc, kompaktinis diskas) procesus | Techniniu lygmeniu įdiegti statinę ir dinaminę analizę, priklausomybių skenavimą ir kitus saugumo kontrolės taškus kūrimo grandinėje. |
| R6-PLĖ-02-ACT3 | 3 | Nustatyti saugumo vartus ir apmokyti kūrimo komandas | Apibrėžti, kokie saugumo kriterijai turi būti įvykdyti prieš leidžiant pakeitimus į produkciją, ir apmokyti komandas jais naudotis. |

| | | | |
|---|---|---|---|
| R6-PLĖ-02-ACT3 | 3 | Nustatyti saugumo vartus ir apmokyti kūrimo komandas | Apibrėžti, kokie saugumo kriterijai turi būti įvykdyti prieš leidžiant pakeitimus į produkciją, ir apmokyti komandas jais naudotis. |
| R6-PLĖ-03-ACT1 | 1 | Sukurti pokyčių valdymo proceso aprašą | Apibrėžti, kaip registruojami, vertinami, tvirtinami, testuojami ir diegiami pokyčiai IT (Information Technology, informacinės technologijos) sistemose. |
| R6-PLĖ-03-ACT1 | 1 | Sukurti pokyčių valdymo proceso aprašą | Apibrėžti, kaip registruojami, vertinami, tvirtinami, testuojami ir diegiami pokyčiai IT (Information Technology, informacinės technologijos) sistemose. |
| R6-PLĖ-03-ACT2 | 2 | Integruoti pokyčių valdymo procesą į ITSM (IT Service Management, IT paslaugų valdymas) įrankį ir kasdienį darbą | Užtikrinti, kad pokyčių valdymo procesas būtų taikomas praktikoje per ITSM (IT Service Management, IT paslaugų valdymas) sistemą. |
| R6-PLĖ-04-ACT1 | 1 | Sukurti ir tvarkyti atskiras aplinkas pokyčių testavimui | Sukurti aiškią aplinkų strategiją ir užtikrinti, kad pokyčiai pirmiausia būtų diegiami neprodukcinėse aplinkose. |
| R6-PLĖ-04-ACT1 | 1 | Sukurti ir tvarkyti atskiras aplinkas pokyčių testavimui | Sukurti aiškią aplinkų strategiją ir užtikrinti, kad pokyčiai pirmiausia būtų diegiami neprodukcinėse aplinkose. |
| R6-PLĖ-04-ACT2 | 2 | Formalizuoti privalomą pokyčių testavimą prieš diegimą | Pokyčių valdymo procese įtvirtinti reikalavimą testuoti pokyčius ir dokumentuoti testavimo rezultatus. |
| R6-PLĖ-04-ACT2 | 2 | Formalizuoti privalomą pokyčių testavimą prieš diegimą | Pokyčių valdymo procese įtvirtinti reikalavimą testuoti pokyčius ir dokumentuoti testavimo rezultatus. |
| R6-PLĖ-05-ACT1 | 1 | Sukurti IT (Information Technology, informacinės technologijos) turto ir programinės įrangos inventoriaus modelį | Apibrėžti, kokie duomenys renkami apie turtą ir programinę įrangą, ir kas atsakingas už jų atnaujinimą. |
| R6-PLĖ-05-ACT1 | 1 | Sukurti IT (Information Technology, informacinės technologijos) turto ir programinės įrangos inventoriaus modelį | Apibrėžti, kokie duomenys renkami apie turtą ir programinę įrangą, ir kas atsakingas už jų atnaujinimą. |
| R6-PLĖ-05-ACT1 | 1 | Sukurti IT (Information Technology, informacinės technologijos) turto ir programinės įrangos inventoriaus modelį | Apibrėžti, kokie duomenys renkami apie turtą ir programinę įrangą, ir kas atsakingas už jų atnaujinimą. |
| R6-PLĖ-05-ACT2 | 2 | Įdiegti įrankį ir procesus inventoriaus palaikymui | Parinkti technologiją ir sukurti procesą, kaip inventorius bus pildomas ir palaikomas aktualus. |
| R6-PLĖ-05-ACT2 | 2 | Įdiegti įrankį ir procesus inventoriaus palaikymui | Parinkti technologiją ir sukurti procesą, kaip inventorius bus pildomas ir palaikomas aktualus. |
| R6-PLĖ-06-ACT1 | 1 | Parengti pataisų valdymo politiką ir terminus | Nustatyti, kaip dažnai tikrinami atnaujinimai, kokie prioritetai taikomi ir per kiek laiko turi būti diegiamos skirtingo kritiškumo pataisos. |
| R6-PLĖ-06-ACT1 | 1 | Parengti pataisų valdymo politiką ir terminus | Nustatyti, kaip dažnai tikrinami atnaujinimai, kokie prioritetai taikomi ir per kiek laiko turi būti diegiamos skirtingo kritiškumo pataisos. |

| | | | |
|---|---|---|---|
| R6-PLĖ-06-ACT2 | 2 | Sukurti operacinį pataisų valdymo procesą | Aprašyti praktinį procesą, kaip identifikuojamos, testuojamos ir diegiamos pataisos įvairiems IT (Information Technology, informacinės technologijos) komponentams. |
| R6-PLĖ-06-ACT2 | 2 | Sukurti operacinį pataisų valdymo procesą | Aprašyti praktinį procesą, kaip identifikuojamos, testuojamos ir diegiamos pataisos įvairiems IT (Information Technology, informacinės technologijos) komponentams. |
| R6-PLĖ-06-ACT3 | 3 | Automatizuoti pataisų diegimą ir stebėseną | Naudoti specializuotus įrankius pataisų diegimui ir atitikties stebėsenai. |
| R6-PLĖ-07-ACT1 | 1 | Nustatyti kritinių pataisų taikymo apimtį kritinėms sistemoms | Susieti kritinių pataisų politiką su kritinių sistemų ir paslaugų sąrašu. |
| R6-PLĖ-07-ACT2 | 2 | Įdiegti kritinių pataisų atitikties monitoringą | Stebėti, ar kritinės pataisos įdiegiamos per nustatytą laiką, ir generuoti ataskaitas. |
| R6-PLĖ-07-ACT2 | 2 | Įdiegti kritinių pataisų atitikties monitoringą | Stebėti, ar kritinės pataisos įdiegiamos per nustatytą laiką, ir generuoti ataskaitas. |
| R6-PLĖ-08-ACT1 | 1 | Parinkti pažeidžiamumų skanavimo įrankius ir nustatyti skanavimo aprėptį | Pasirinkti tinkamus skanavimo įrankius ir apibrėžti, kurios sistemos, tinklo segmentai ir aplikacijos skenuojamos ir kokiu dažniu. |
| R6-PLĖ-08-ACT1 | 1 | Parinkti pažeidžiamumų skanavimo įrankius ir nustatyti skanavimo aprėptį | Pasirinkti tinkamus skanavimo įrankius ir apibrėžti, kurios sistemos, tinklo segmentai ir aplikacijos skenuojamos ir kokiu dažniu. |
| R6-PLĖ-08-ACT2 | 2 | Panaudoti skanavimo rezultatus pataisų ir rizikos valdyme | Užtikrinti, kad pažeidžiamumų skanavimo rezultatai būtų sistemingai naudojami pataisų planavimui ir rizikos mažinimui. |
| R6-PLĖ-08-ACT2 | 2 | Panaudoti skanavimo rezultatus pataisų ir rizikos valdyme | Užtikrinti, kad pažeidžiamumų skanavimo rezultatai būtų sistemingai naudojami pataisų planavimui ir rizikos mažinimui. |
| R6-PLĖ-09-ACT1 | 1 | Sukurti pažeidžiamumų atskleidimo politikos dokumentą | Apibrėžti, kokia informacija ir kokiais kanalais gali būti pranešta apie spragas bei kokių veiksmų imsis organizacija. |
| R6-PLĖ-09-ACT1 | 1 | Sukurti pažeidžiamumų atskleidimo politikos dokumentą | Apibrėžti, kokia informacija ir kokiais kanalais gali būti pranešta apie spragas bei kokių veiksmų imsis organizacija. |
| R6-PLĖ-09-ACT2 | 2 | Paskelbti pažeidžiamumų atskleidimo politiką ir apdorojimo procesą | Padaryti politiką viešai prieinamą ir užtikrinti, kad pranešimai būtų integruoti į vidinį incidentų ir spragų valdymą. |
| R6-PLĖ-09-ACT2 | 2 | Paskelbti pažeidžiamumų atskleidimo politiką ir apdorojimo procesą | Padaryti politiką viešai prieinamą ir užtikrinti, kad pranešimai būtų integruoti į vidinį incidentų ir spragų valdymą. |
| R6-PLĖ-10-ACT1 | 1 | Sukurti ir įgyvendinti programinės įrangos valdymo politiką | Apibrėžti, kaip programinė įranga įsigyjama, diegiama, inventorizuojama ir tikrinama licencijų atitiktis. |
| R6-PLĖ-10-ACT1 | 1 | Sukurti ir įgyvendinti programinės įrangos valdymo politiką | Apibrėžti, kaip programinė įranga įsigyjama, diegiama, inventorizuojama ir tikrinama licencijų atitiktis. |
| R6-PLĖ-10-ACT1 | 1 | Sukurti ir įgyvendinti programinės įrangos valdymo politiką | Apibrėžti, kaip programinė įranga įsigyjama, diegiama, inventorizuojama ir tikrinama licencijų atitiktis. |

| | | | |
|---|---|---|---|
| R7-ATIT-01-ACT1 | 1 | Apibrėžti kibernetinio saugumo vidaus audito apimtį ir metodiką | Nustatyti, kokios sritys, procesai ir sistemos bus vertinamos ir kokiais kriterijais remiantis. |
| R7-ATIT-01-ACT1 | 1 | Apibrėžti kibernetinio saugumo vidaus audito apimtį ir metodiką | Nustatyti, kokios sritys, procesai ir sistemos bus vertinamos ir kokiais kriterijais remiantis. |
| R7-ATIT-01-ACT2 | 2 | Suplanuoti ir atlikti metinį kibernetinio saugumo vidaus auditą | Parengti metinį planą ir praktiškai atlikti audito veiklas. |
| R7-ATIT-01-ACT2 | 2 | Suplanuoti ir atlikti metinį kibernetinio saugumo vidaus auditą | Parengti metinį planą ir praktiškai atlikti audito veiklas. |
| R7-ATIT-02-ACT1 | 1 | Sukurti neatitikčių registravimo ir korekcinių veiksmų planavimo tvarką | Apibrėžti, kaip registruojamos audito išvados ir kaip planuojami jas šalinantys veiksmai. |
| R7-ATIT-02-ACT1 | 1 | Sukurti neatitikčių registravimo ir korekcinių veiksmų planavimo tvarką | Apibrėžti, kaip registruojamos audito išvados ir kaip planuojami jas šalinantys veiksmai. |
| R7-ATIT-02-ACT2 | 2 | Įgyvendinti korekcinių veiksmų stebėseną ir atsiskaitymą | Sukurti mechanizmą, kaip stebimas korekcinių veiksmų įgyvendinimas ir apie tai atsiskaitoma vadovybei. |
| R7-ATIT-02-ACT2 | 2 | Įgyvendinti korekcinių veiksmų stebėseną ir atsiskaitymą | Sukurti mechanizmą, kaip stebimas korekcinių veiksmų įgyvendinimas ir apie tai atsiskaitoma vadovybei. |
| R7-ATIT-03-ACT1 | 1 | Apibrėžti penetracijos testavimo strategiją | Nustatyti, kurios sistemos testuojamos, kokiu dažniu ir kokio tipo testavimas taikomas (black/grey/white box). |
| R7-ATIT-03-ACT1 | 1 | Apibrėžti penetracijos testavimo strategiją | Nustatyti, kurios sistemos testuojamos, kokiu dažniu ir kokio tipo testavimas taikomas (black/grey/white box). |
| R7-ATIT-03-ACT2 | 2 | Organizuoti ir vykdyti išorinius penetracijos testavimus | Pasirinkti kvalifikuotus tiekėjus ir užtikrinti, kad testai būtų tinkamai suplanuoti ir įgyvendinti. |
| R7-ATIT-03-ACT2 | 2 | Organizuoti ir vykdyti išorinius penetracijos testavimus | Pasirinkti kvalifikuotus tiekėjus ir užtikrinti, kad testai būtų tinkamai suplanuoti ir įgyvendinti. |
| R7-ATIT-03-ACT3 | 3 | Integruoti penetracijos testų rezultatus į pataisų ir rizikos valdymą | Užtikrinti, kad testų metu rastos spragos būtų sistemingai pašalinamos ir stebimos. |
| R7-ATIT-04-ACT1 | 1 | Apibrėžti kibernetinio saugumo KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) ir KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) rodiklius | Pasirinkti ir aprašyti pagrindinius rodiklius, kurie leis vertinti reikalavimų įgyvendinimą ir riziką. |
| R7-ATIT-04-ACT1 | 1 | Apibrėžti kibernetinio saugumo KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) ir KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) rodiklius | Pasirinkti ir aprašyti pagrindinius rodiklius, kurie leis vertinti reikalavimų įgyvendinimą ir riziką. |
| R7-ATIT-04-ACT1 | 1 | Apibrėžti kibernetinio saugumo KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) ir KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) rodiklius | Pasirinkti ir aprašyti pagrindinius rodiklius, kurie leis vertinti reikalavimų įgyvendinimą ir riziką. |
| R7-ATIT-04-ACT2 | 2 | Automatizuoti KPI (Key Performance Indicator, pagrindinis veiklos rodiklis)/KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) rinkimą ir ataskaitų teikimą | Sukurti praktinį būdą rinkti ir atvaizduoti rodiklius vadovybei ir atsakingoms komandoms. |

| | | | |
|---|---|---|---|
| R7-ATIT-04-ACT2 | 2 | Automatizuoti KPI (Key Performance Indicator, pagrindinis veiklos rodiklis)/KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) rinkimą ir ataskaitų teikimą | Sukurti praktinį būdą rinkti ir atvaizduoti rodiklius vadovybei ir atsakingoms komandoms. |
| R7-ATIT-05-ACT1 | 1 | Sudaryti kibernetinio saugumo dokumentacijos katalogą ir struktūrą | Identifikuoti ir sugrupuoti visus svarbiausius kibernetinio saugumo dokumentus ir įrašus. |
| R7-ATIT-05-ACT1 | 1 | Sudaryti kibernetinio saugumo dokumentacijos katalogą ir struktūrą | Identifikuoti ir sugrupuoti visus svarbiausius kibernetinio saugumo dokumentus ir įrašus. |
| R7-ATIT-05-ACT2 | 2 | Užtikrinti dokumentų prieinamumą ir aktualumą auditoriams | Nustatyti atsakomybes už dokumentų atnaujinimą ir sukurti efektyvų pateikimo auditoriams mechanizmą. |
| R7-ATIT-05-ACT2 | 2 | Užtikrinti dokumentų prieinamumą ir aktualumą auditoriams | Nustatyti atsakomybes už dokumentų atnaujinimą ir sukurti efektyvų pateikimo auditoriams mechanizmą. |
| R7-ATIT-06-ACT1 | 1 | Išanalizuoti NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijų tvarką ir reikalavimus | Susipažinti su NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) patikrinimų gairėmis, tiksliniais klausimynais ir pagrindiniais vertinimo aspektais. |
| R7-ATIT-06-ACT2 | 2 | Sukurti pasirengimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijai planą ir atlikti bandomąją peržiūrą | Sukurti praktinį planą ir periodiškai jį išbandyti, imituojant realią inspekciją. |
| R7-ATIT-06-ACT2 | 2 | Sukurti pasirengimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijai planą ir atlikti bandomąją peržiūrą | Sukurti praktinį planą ir periodiškai jį išbandyti, imituojant realią inspekciją. |
| R7-ATIT-06-ACT2 | 2 | Sukurti pasirengimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijai planą ir atlikti bandomąją peržiūrą | Sukurti praktinį planą ir periodiškai jį išbandyti, imituojant realią inspekciją. |
| R7-ATIT-07-ACT1 | 1 | Nustatyti atsakomybę už TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) ir susijusių gairių stebėseną | Paskirti funkciją, kuri seka teisės aktų, NKSC (Nacionalinis kibernetinio saugumo centras (NKSC))/ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA) gairių ir įgyvendinimo terminų pokyčius. |
| R7-ATIT-07-ACT1 | 1 | Nustatyti atsakomybę už TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) ir susijusių gairių stebėseną | Paskirti funkciją, kuri seka teisės aktų, NKSC (Nacionalinis kibernetinio saugumo centras (NKSC))/ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA) gairių ir įgyvendinimo terminų pokyčius. |
| R7-ATIT-07-ACT2 | 2 | Struktūruotai informuoti vadovybę apie terminus ir inspekcijų tvarką | Užtikrinti, kad vadovybė žinotų, iki kada turi būti įgyvendintos priemonės ir kaip vyks patikrinimai. |
| R7-ATIT-07-ACT2 | 2 | Struktūruotai informuoti vadovybę apie terminus ir inspekcijų tvarką | Užtikrinti, kad vadovybė žinotų, iki kada turi būti įgyvendintos priemonės ir kaip vyks patikrinimai. |

| | | | |
|---|---|---|---|
| R7-POL-03-ACT1 | 1 | Sukurti priemonių veiksmingumo vertinimo politikos konceptą | Nustatyti, ką reiškia „veiksminga priemonė“, kokiais būdais ir kokiu dažniu tai vertinama. |
| R7-POL-03-ACT1 | 1 | Sukurti priemonių veiksmingumo vertinimo politikos konceptą | Nustatyti, ką reiškia „veiksminga priemonė“, kokiais būdais ir kokiu dažniu tai vertinama. |
| R7-POL-03-ACT1 | 1 | Sukurti priemonių veiksmingumo vertinimo politikos konceptą | Nustatyti, ką reiškia „veiksminga priemonė“, kokiais būdais ir kokiu dažniu tai vertinama. |
| R7-POL-03-ACT2 | 2 | Sukurti ir patvirtinti priemonių veiksmingumo vertinimo politiką | Politikos lygmeniu aprašyti, kaip ir kada vertinama kibernetinio saugumo priemonių veiksmingumas. |
| R7-POL-03-ACT2 | 2 | Sukurti ir patvirtinti priemonių veiksmingumo vertinimo politiką | Politikos lygmeniu aprašyti, kaip ir kada vertinama kibernetinio saugumo priemonių veiksmingumas. |
| R7-POL-04-ACT1 | 1 | Sukurti kibernetinio saugumo vertinimo veiklų metinį/ilgalaikį kalendorių | Apjungti vidinius auditų, pen-testų, pratybų, KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) peržiūrų ir kitų vertinimo veiklų periodiškumą į bendrą planą. |
| R7-POL-04-ACT1 | 1 | Sukurti kibernetinio saugumo vertinimo veiklų metinį/ilgalaikį kalendorių | Apjungti vidinius auditų, pen-testų, pratybų, KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) peržiūrų ir kitų vertinimo veiklų periodiškumą į bendrą planą. |
| R7-POL-04-ACT2 | 2 | Įtvirtinti periodiškumą politikoje ir procesuose | Aprašyti, kokiu dažniu turi būti atliekamos vertinimo veiklos, ir susieti tai su rizikos lygiu. |
| R8-MOK-01-ACT1 | 1 | Apibrėžti kibernetinio saugumo mokymų programos konceptą | Sukonstruoti, kokias temas, darbuotojų grupes ir tikslus turi apimti kibernetinio saugumo mokymų programa. |
| R8-MOK-01-ACT1 | 1 | Apibrėžti kibernetinio saugumo mokymų programos konceptą | Sukonstruoti, kokias temas, darbuotojų grupes ir tikslus turi apimti kibernetinio saugumo mokymų programa. |
| R8-MOK-01-ACT1 | 1 | Apibrėžti kibernetinio saugumo mokymų programos konceptą | Sukonstruoti, kokias temas, darbuotojų grupes ir tikslus turi apimti kibernetinio saugumo mokymų programa. |
| R8-MOK-01-ACT2 | 2 | Dokumentuoti ir patvirtinti mokymų politiką | Sukurti formalų politikos dokumentą ir jį patvirtinti vadovybės lygiu. |
| R8-MOK-01-ACT2 | 2 | Dokumentuoti ir patvirtinti mokymų politiką | Sukurti formalų politikos dokumentą ir jį patvirtinti vadovybės lygiu. |
| R8-MOK-02-ACT1 | 1 | Įtraukti įvadinius mokymus į onboarding'o procesą | Padaryti kibernetinio saugumo mokymus privaloma naujo darbuotojo įvedimo dalimi. |
| R8-MOK-02-ACT1 | 1 | Įtraukti įvadinius mokymus į onboarding'o procesą | Padaryti kibernetinio saugumo mokymus privaloma naujo darbuotojo įvedimo dalimi. |
| R8-MOK-02-ACT2 | 2 | Organizuoti įvadinių mokymų vykdymą ir stebėti dalyvavimą | Parinkti mokymų formatą, įrankius ir užtikrinti, kad visi nauji darbuotojai realiai praeitų mokymus. |
| R8-MOK-02-ACT2 | 2 | Organizuoti įvadinių mokymų vykdymą ir stebėti dalyvavimą | Parinkti mokymų formatą, įrankius ir užtikrinti, kad visi nauji darbuotojai realiai praeitų mokymus. |

| | | | |
|---|---|---|---|
| R8-MOK-03-ACT1 | 1 | Aprašyti periodinių mokymų tvarką | Politikos ir procedūrų lygiu įtvirtinti, kad mokymai kartojami reguliariai, ir aprašyti, kaip tai daroma. |
| R8-MOK-03-ACT1 | 1 | Aprašyti periodinių mokymų tvarką | Politikos ir procedūrų lygiu įtvirtinti, kad mokymai kartojami reguliariai, ir aprašyti, kaip tai daroma. |
| R8-MOK-03-ACT2 | 2 | Suplanuoti ir vykdyti periodinius mokymų ciklus | Parengti metinį periodinių mokymų planą ir įdiegti stebėsenos mechanizmą. |
| R8-MOK-03-ACT2 | 2 | Suplanuoti ir vykdyti periodinius mokymų ciklus | Parengti metinį periodinių mokymų planą ir įdiegti stebėsenos mechanizmą. |
| R8-MOK-04-ACT1 | 1 | Sukurti kibernetinės higienos kampanijų planą | Nustatyti, kokios informacinės kampanijos bus rengiamos, kokiomis priemonėmis ir kokiu dažniu. |
| R8-MOK-04-ACT1 | 1 | Sukurti kibernetinės higienos kampanijų planą | Nustatyti, kokios informacinės kampanijos bus rengiamos, kokiomis priemonėmis ir kokiu dažniu. |
| R8-MOK-04-ACT2 | 2 | Vykdyti kampanijas ir stebėti darbuotojų įsitraukimą | Organizuoti konkrečias kampanijas ir matuoti jų pasiekiamumą bei poveikį. |
| R8-MOK-04-ACT2 | 2 | Vykdyti kampanijas ir stebėti darbuotojų įsitraukimą | Organizuoti konkrečias kampanijas ir matuoti jų pasiekiamumą bei poveikį. |
| R8-MOK-05-ACT1 | 1 | Apibrėžti phishing simuliacijų tikslus ir apimtį | Nustatyti, kokios darbuotojų grupės ir kokiu dažniu bus testuojamos, kokie scenarijai naudojami. |
| R8-MOK-05-ACT1 | 1 | Apibrėžti phishing simuliacijų tikslus ir apimtį | Nustatyti, kokios darbuotojų grupės ir kokiu dažniu bus testuojamos, kokie scenarijai naudojami. |
| R8-MOK-05-ACT2 | 2 | Naudoti specializuotus phishing simuliacijų įrankius ir analizuoti rezultatus | Pasirinkti techninius įrankius ir organizuoti simuliacijas su atitinkama analitika. |
| R8-MOK-05-ACT2 | 2 | Naudoti specializuotus phishing simuliacijų įrankius ir analizuoti rezultatus | Pasirinkti techninius įrankius ir organizuoti simuliacijas su atitinkama analitika. |
| R8-MOK-06-ACT1 | 1 | Sukurti grėsmių informacijos gavimo ir filtravimo mechanizmą | Apibrėžti, iš kur gaunama informacija apie grėsmes ir kas atsakingas už jos įvertinimą prieš siunčiant darbuotojams. |
| R8-MOK-06-ACT1 | 1 | Sukurti grėsmių informacijos gavimo ir filtravimo mechanizmą | Apibrėžti, iš kur gaunama informacija apie grėsmes ir kas atsakingas už jos įvertinimą prieš siunčiant darbuotojams. |
| R8-MOK-06-ACT2 | 2 | Informuoti darbuotojus apie aktualias grėsmes per nustatytus kanalus | Parinkti, kokiais kanalais ir kokiu dažniu siunčiami įspėjimai ir edukacinė informacija. |
| R8-MOK-06-ACT2 | 2 | Informuoti darbuotojus apie aktualias grėsmes per nustatytus kanalus | Parinkti, kokiais kanalais ir kokiu dažniu siunčiami įspėjimai ir edukacinė informacija. |
| R9-KRIP-01-ACT1 | 1 | Sukurti kriptografijos valdymo koncepciją | Apibrėžti, kokiu tikslu ir kuriose srityse organizacija taiko kriptografiją, kokius standartus ir teisės aktus remiasi. |
| R9-KRIP-01-ACT1 | 1 | Sukurti kriptografijos valdymo koncepciją | Apibrėžti, kokiu tikslu ir kuriose srityse organizacija taiko kriptografiją, kokius standartus ir teisės aktus remiasi. |
| R9-KRIP-01-ACT1 | 1 | Sukurti kriptografijos valdymo koncepciją | Apibrėžti, kokiu tikslu ir kuriose srityse organizacija taiko kriptografiją, kokius standartus ir teisės aktus remiasi. |

| | | | |
|---|---|---|---|
| R9-KRIP-01-ACT2 | 2 | Dokumentuoti ir patvirtinti kriptografijos ir šifravimo politiką | Parengti formalų politikos dokumentą ir jį patvirtinti valdymo lygmeniu. |
| R9-KRIP-01-ACT2 | 2 | Dokumentuoti ir patvirtinti kriptografijos ir šifravimo politiką | Parengti formalų politikos dokumentą ir jį patvirtinti valdymo lygmeniu. |
| R9-KRIP-02-ACT1 | 1 | Sukurti kriptografinių algoritmų ir protokolų standartą | Remiantis gerosiomis praktikomis ir reguliaciniais reikalavimais, aprašyti leistinas ir draudžiamas kriptografijos konfigūracijas. |
| R9-KRIP-02-ACT1 | 1 | Sukurti kriptografinių algoritmų ir protokolų standartą | Remiantis gerosiomis praktikomis ir reguliaciniais reikalavimais, aprašyti leistinas ir draudžiamas kriptografijos konfigūracijas. |
| R9-KRIP-02-ACT2 | 2 | Įtvirtinti kriptografijos standartą techninėse specifikacijose ir priežiūroje | Padaryti taip, kad algoritmų/protokolų standartas būtų taikomas naujoms ir esamoms sistemoms per techninius reikalavimus ir kontrolės priemones. |
| R9-KRIP-02-ACT2 | 2 | Įtvirtinti kriptografijos standartą techninėse specifikacijose ir priežiūroje | Padaryti taip, kad algoritmų/protokolų standartas būtų taikomas naujoms ir esamoms sistemoms per techninius reikalavimus ir kontrolės priemones. |
| R9-KRIP-03-ACT1 | 1 | Sukurti raktų valdymo politiką ir rolę | Nustatyti, kas atsakingas už raktų valdymą ir kokie bendrieji principai taikomi visiems raktams. |
| R9-KRIP-03-ACT1 | 1 | Sukurti raktų valdymo politiką ir rolę | Nustatyti, kas atsakingas už raktų valdymą ir kokie bendrieji principai taikomi visiems raktams. |
| R9-KRIP-03-ACT2 | 2 | Aprašyti raktų gyvavimo ciklą ir technines kontrolės priemones | Sukonstruoti praktinį raktų gyvavimo ciklą ir įdiegti technines priemones saugiam raktų valdymui. |
| R9-KRIP-03-ACT2 | 2 | Aprašyti raktų gyvavimo ciklą ir technines kontrolės priemones | Sukonstruoti praktinį raktų gyvavimo ciklą ir įdiegti technines priemones saugiam raktų valdymui. |
| R9-KRIP-04-ACT1 | 1 | Sukartografuoti duomenų srautus ir nustatyti šifravimo poreikį | Išanalizuoti, kokie vidiniai ir išoriniai ryšiai turi būti šifruojami. |
| R9-KRIP-04-ACT1 | 1 | Sukartografuoti duomenų srautus ir nustatyti šifravimo poreikį | Išanalizuoti, kokie vidiniai ir išoriniai ryšiai turi būti šifruojami. |
| R9-KRIP-04-ACT2 | 2 | Konfigūruoti saugius tinklo protokolus duomenų perdavimui | Techniniu lygmeniu užtikrinti, kad prioritetiniai srautai būtų šifruojami saugiais protokolais. |
| R9-KRIP-04-ACT2 | 2 | Konfigūruoti saugius tinklo protokolus duomenų perdavimui | Techniniu lygmeniu užtikrinti, kad prioritetiniai srautai būtų šifruojami saugiais protokolais. |

| | | | |
|---|---|---|---|
| R9-KRIP-05-ACT1 | 1 | Sukartografuoti duomenų saugyklas ir šifravimo poreikį | Identifikuoti, kur saugomi jautrūs duomenys ir kur šifravimas yra privalomas ar rekomenduojamas. |
| R9-KRIP-05-ACT1 | 1 | Sukartografuoti duomenų saugyklas ir šifravimo poreikį | Identifikuoti, kur saugomi jautrūs duomenys ir kur šifravimas yra privalomas ar rekomenduojamas. |
| R9-KRIP-05-ACT2 | 2 | Techniniu lygmeniu įgyvendinti duomenų šifravimą saugojimo metu | Sukonfigūruoti šifravimą duomenų bazėse, failų sistemose, diskuose ir atsarginėse kopijose. |
| R9-KRIP-05-ACT2 | 2 | Techniniu lygmeniu įgyvendinti duomenų šifravimą saugojimo metu | Sukonfigūruoti šifravimą duomenų bazėse, failų sistemose, diskuose ir atsarginėse kopijose. |
| R9-KRIP-06-ACT1 | 1 | Aprašyti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) naudojimo ir šifravimo standartus | Nustatyti, kokie VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) tipai ir šifravimo metodai leidžiami bei kokioms naudotojų/sistemų grupėms jie taikomi. |
| R9-KRIP-06-ACT1 | 1 | Aprašyti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) naudojimo ir šifravimo standartus | Nustatyti, kokie VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) tipai ir šifravimo metodai leidžiami bei kokioms naudotojų/sistemų grupėms jie taikomi. |
| R9-KRIP-06-ACT2 | 2 | Sukonfigūruoti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus pagal standartus | Techniniu lygmeniu suderinti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus su nustatytais šifravimo standartais ir prieigos politikomis. |
| R9-KRIP-06-ACT2 | 2 | Sukonfigūruoti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus pagal standartus | Techniniu lygmeniu suderinti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus su nustatytais šifravimo standartais ir prieigos politikomis. |
| R9-KRIP-07-ACT1 | 1 | Suplanuoti WiFi tinklų architektūrą ir segmentavimą | Atskiriant vidinius, svečių ir kitus tinklus, nustatyti skirtingus saugumo lygius ir reikalavimus. |
| R9-KRIP-07-ACT1 | 1 | Suplanuoti WiFi tinklų architektūrą ir segmentavimą | Atskiriant vidinius, svečių ir kitus tinklus, nustatyti skirtingus saugumo lygius ir reikalavimus. |
| R9-KRIP-07-ACT2 | 2 | Sukonfigūruoti saugius WiFi protokolus ir autentifikaciją | Techniniu lygmeniu užtikrinti, kad vidiniai WiFi tinklai naudotų stiprią šifravimą ir centralizuotą autentifikaciją. |
| R9-KRIP-07-ACT2 | 2 | Sukonfigūruoti saugius WiFi protokolus ir autentifikaciją | Techniniu lygmeniu užtikrinti, kad vidiniai WiFi tinklai naudotų stiprią šifravimą ir centralizuotą autentifikaciją. |
| R9-KRIP-08-ACT1 | 1 | Sukartografuoti sertifikatų naudojimą organizacijoje | Identifikuoti, kuriose sistemose ir paslaugose naudojami TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) ir kiti sertifikatai, ir kokie CA (Certification Authority, sertifikavimo institucija) šiuo metu naudojami. |

| | | | |
|---|---|---|---|
| R9-KRIP-08-ACT1 | 1 | Sukartografuoti sertifikatų naudojimą organizacijoje | Identifikuoti, kuriose sistemose ir paslaugose naudojami TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) ir kiti sertifikatai, ir kokie CA (Certification Authority, sertifikavimo institucija) šiuo metu naudojami. |
| R9-KRIP-08-ACT2 | 2 | Sukurti CA (Certification Authority, sertifikavimo institucija) naudojimo ir sertifikatų išdavimo taisykles | Aprašyti, kokie CA (Certification Authority, sertifikavimo institucija) yra leidžiami, kaip išduodami ir diegiami sertifikatai, kaip prižiūrima patikimumo grandinė. |
| R9-KRIP-08-ACT2 | 2 | Sukurti CA (Certification Authority, sertifikavimo institucija) naudojimo ir sertifikatų išdavimo taisykles | Aprašyti, kokie CA (Certification Authority, sertifikavimo institucija) yra leidžiami, kaip išduodami ir diegiami sertifikatai, kaip prižiūrima patikimumo grandinė. |
| R9-KRIP-09-ACT1 | 1 | Įvertinti ir pasirinkti sertifikatų valdymo technologiją | Įvertinti turimus įrankius ir rinkos sprendimus sertifikatų valdymui automatizuoti. |
| R9-KRIP-09-ACT1 | 1 | Įvertinti ir pasirinkti sertifikatų valdymo technologiją | Įvertinti turimus įrankius ir rinkos sprendimus sertifikatų valdymui automatizuoti. |
| R9-KRIP-09-ACT2 | 2 | Įdiegti sertifikatų gyvavimo ciklo automatizavimą | Sukonfigūruoti automatizuotą sertifikatų išdavimą, diegimą ir atnaujinimą kritinėse sistemose. |
| R9-KRIP-09-ACT2 | 2 | Įdiegti sertifikatų gyvavimo ciklo automatizavimą | Sukonfigūruoti automatizuotą sertifikatų išdavimą, diegimą ir atnaujinimą kritinėse sistemose. |
| R9-KRIP-10-ACT1 | 1 | Nustatyti, kurie raktai laikomi kritiniais ir turi būti saugomi HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM)) | Apibrėžti, kurie raktai turi būti saugomi aukštesnio lygio apsaugos priemonėmis (HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga)). |
| R9-KRIP-10-ACT1 | 1 | Nustatyti, kurie raktai laikomi kritiniais ir turi būti saugomi HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM)) | Apibrėžti, kurie raktai turi būti saugomi aukštesnio lygio apsaugos priemonėmis (HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga)). |
| R9-KRIP-10-ACT2 | 2 | Techniniu lygmeniu įgyvendinti HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) naudojimą kritiniams raktams | Pasirinkti ir įdiegti HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) sprendimą ir perkelti kritinius raktus pagal nustatytas procedūras. |
| R9-KRIP-10-ACT2 | 2 | Techniniu lygmeniu įgyvendinti HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) naudojimą kritiniams raktams | Pasirinkti ir įdiegti HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) sprendimą ir perkelti kritinius raktus pagal nustatytas procedūras. |
| R10-HRT-01-ACT1 | 1 | Sukurti žmogiškųjų išteklių saugumo politikos konceptą | Nustatyti, kokias darbuotojų gyvavimo ciklo stadijas ir rizikas turi apimti HR (Human Resources, žmogiškieji ištekliai) saugumo politika. |

| | | | |
|---|---|---|---|
| R10-HRT-01-ACT1 | 1 | Sukurti žmogiškųjų išteklių saugumo politikos konceptą | Nustatyti, kokias darbuotojų gyvavimo ciklo stadijas ir rizikas turi apimti HR (Human Resources, žmogiškieji ištekliai) saugumo politika. |
| R10-HRT-01-ACT2 | 2 | Dokumentuoti ir patvirtinti HR (Human Resources, žmogiškieji ištekliai) saugumo politiką | Sukurti formalų HR (Human Resources, žmogiškieji ištekliai) saugumo politikos dokumentą ir gauti vadovybės patvirtinimą. |
| R10-HRT-01-ACT2 | 2 | Dokumentuoti ir patvirtinti HR (Human Resources, žmogiškieji ištekliai) saugumo politiką | Sukurti formalų HR (Human Resources, žmogiškieji ištekliai) saugumo politikos dokumentą ir gauti vadovybės patvirtinimą. |
| R10-HRT-01-ACT3 | 3 | Įdiegti HR (Human Resources, žmogiškieji ištekliai) saugumo politiką į kasdienius procesus | Užtikrinti, kad HR (Human Resources, žmogiškieji ištekliai) saugumo politika nebūtų vien dokumentas, o realiai taikoma praktikoje. |
| R10-HRT-01-ACT3 | 3 | Įdiegti HR (Human Resources, žmogiškieji ištekliai) saugumo politiką į kasdienius procesus | Užtikrinti, kad HR (Human Resources, žmogiškieji ištekliai) saugumo politika nebūtų vien dokumentas, o realiai taikoma praktikoje. |
| R10-HRT-02-ACT1 | 1 | Identifikuoti kritines pareigas ir patikrinimų apimtį | Nustatyti pareigas, kurioms būtini papildomi patikrinimai, ir kokie patikrinimo elementai taikomi. |
| R10-HRT-02-ACT1 | 1 | Identifikuoti kritines pareigas ir patikrinimų apimtį | Nustatyti pareigas, kurioms būtini papildomi patikrinimai, ir kokie patikrinimo elementai taikomi. |
| R10-HRT-02-ACT2 | 2 | Integruoti fono patikrinimus į įdarbinimo ir pareigų keitimo procesą | Padaryti, kad fono patikrinimai būtų nuosekli ir kontroliuojama įdarbinimo proceso dalis. |
| R10-HRT-02-ACT2 | 2 | Integruoti fono patikrinimus į įdarbinimo ir pareigų keitimo procesą | Padaryti, kad fono patikrinimai būtų nuosekli ir kontroliuojama įdarbinimo proceso dalis. |
| R10-HRT-03-ACT1 | 1 | Standartizuoti konfidencialumo ir elgesio susitarimus | Sukurti vieningus dokumentų šablonus, taikomus darbuotojams ir rangovams. |
| R10-HRT-03-ACT1 | 1 | Standartizuoti konfidencialumo ir elgesio susitarimus | Sukurti vieningus dokumentų šablonus, taikomus darbuotojams ir rangovams. |
| R10-HRT-03-ACT2 | 2 | Užtikrinti konfidencialumo ir elgesio taisyklių pasirašymą ir atnaujinimą | Padaryti, kad susitarimų pasirašymas būtų privaloma įdarbinimo ir prieigos suteikimo sąlyga. |
| R10-HRT-03-ACT2 | 2 | Užtikrinti konfidencialumo ir elgesio taisyklių pasirašymą ir atnaujinimą | Padaryti, kad susitarimų pasirašymas būtų privaloma įdarbinimo ir prieigos suteikimo sąlyga. |
| R10-HRT-04-ACT1 | 1 | Apibrėžti, koks turtas patenka į turto valdymo politiką | Suskirstyti turtą į kategorijas ir nustatyti, kurie objektai turi būti valdomi centralizuotai. |
| R10-HRT-04-ACT1 | 1 | Apibrėžti, koks turtas patenka į turto valdymo politiką | Suskirstyti turtą į kategorijas ir nustatyti, kurie objektai turi būti valdomi centralizuotai. |
| R10-HRT-04-ACT2 | 2 | Dokumentuoti turto valdymo principus ir atsakomybes | Sukurti formalų turto valdymo politikos dokumentą ir gauti vadovybės patvirtinimą. |
| R10-HRT-04-ACT2 | 2 | Dokumentuoti turto valdymo principus ir atsakomybes | Sukurti formalų turto valdymo politikos dokumentą ir gauti vadovybės patvirtinimą. |
| R10-HRT-05-ACT1 | 1 | Apibrėžti turto klasifikavimo lygius ir kriterijus | Sukurti paprastą, bet pakankamai detalų klasifikavimo modelį, tinkamą visai organizacijai. |
| R10-HRT-05-ACT1 | 1 | Apibrėžti turto klasifikavimo lygius ir kriterijus | Sukurti paprastą, bet pakankamai detalų klasifikavimo modelį, tinkamą visai organizacijai. |
| R10-HRT-05-ACT2 | 2 | Praktiškai pritaikyti klasifikavimą turto registre | Užtikrinti, kad turtas būtų klasifikuotas ir klasifikacija būtų palaikoma aktuali. |

| | | | |
|---|---|---|---|
| R10-HRT-05-ACT2 | 2 | Praktiškai pritaikyti klasifikavimą turto registre | Užtikrinti, kad turtas būtų klasifikuotas ir klasifikacija būtų palaikoma aktuali. |
| R10-HRT-06-ACT1 | 1 | Sukurti fizinės saugos ir prieigos taisykles kritinėms patalpoms | Nustatyti, kas ir kokiomis sąlygomis gali patekti į serverines ir kitas kritines patalpas. |
| R10-HRT-06-ACT1 | 1 | Sukurti fizinės saugos ir prieigos taisykles kritinėms patalpoms | Nustatyti, kas ir kokiomis sąlygomis gali patekti į serverines ir kitas kritines patalpas. |
| R10-HRT-06-ACT2 | 2 | Techniniu lygmeniu kontroliuoti ir registruoti prieigą | Naudoti prieigos kontrolės sistemas, žurnalus ir, jei reikia, vaizdo stebėseną. |
| R10-HRT-06-ACT2 | 2 | Techniniu lygmeniu kontroliuoti ir registruoti prieigą | Naudoti prieigos kontrolės sistemas, žurnalus ir, jei reikia, vaizdo stebėseną. |
| R10-HRT-07-ACT1 | 1 | Pasirinkti ir įsidiegti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) platformą | Įvertinti ir pasirinkti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) sprendimą, tinkantį organizacijos naudojamoms platformoms. |
| R10-HRT-07-ACT1 | 1 | Pasirinkti ir įsidiegti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) platformą | Įvertinti ir pasirinkti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) sprendimą, tinkantį organizacijos naudojamoms platformoms. |
| R10-HRT-07-ACT2 | 2 | Enrolinti įrenginius ir pritaikyti saugumo politiką | Prijungti įrenginius prie MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) ir taikyti saugumo konfigūracijas. |
| R10-HRT-07-ACT2 | 2 | Enrolinti įrenginius ir pritaikyti saugumo politiką | Prijungti įrenginius prie MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) ir taikyti saugumo konfigūracijas. |
| R10-HRT-08-ACT1 | 1 | Aprašyti privalomą diskų šifravimą mobiliuosiuose įrenginiuose | Nustatyti, kuriems įrenginiams privalomas šifravimas ir kokios technologijos leidžiamos. |
| R10-HRT-08-ACT2 | 2 | Sukonfigūruoti šifravimą ir monitoringą per MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) | Naudoti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) ar kitus įrankius, kad būtų techniškai užtikrinamas ir stebimas šifravimas. |
| R10-HRT-08-ACT2 | 2 | Sukonfigūruoti šifravimą ir monitoringą per MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) | Naudoti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) ar kitus įrankius, kad būtų techniškai užtikrinamas ir stebimas šifravimas. |
| R11-PRIEI-06-ACT1 | 1 | Suskaičiuoti ir klasifikuoti privilegijuotas paskyras | Išsigryninti, kurioms paskyroms ir sistemoms MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) yra kritiškai svarbi kontrolė. |
| R11-PRIEI-06-ACT1 | 1 | Suskaičiuoti ir klasifikuoti privilegijuotas paskyras | Išsigryninti, kurioms paskyroms ir sistemoms MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) yra kritiškai svarbi kontrolė. |
| R11-PRIEI-06-ACT2 | 2 | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) sprendimą privilegijuotoms paskyroms | Techniniu lygmeniu užtikrinti, kad prisijungiant privilegijuotomis paskyromis visada būtų naudojama MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija). |
| R11-PRIEI-06-ACT2 | 2 | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) sprendimą privilegijuotoms paskyroms | Techniniu lygmeniu užtikrinti, kad prisijungiant privilegijuotomis paskyromis visada būtų naudojama MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija). |

| | | | |
|---|---|---|---|
| R11-PRIEI-07-ACT1 | 1 | Sukartografuoti nuotolinės prieigos vektorius | Nustatyti, per kokius kanalus naudotojai gali pasiekti vidines sistemas iš išorės. |
| R11-PRIEI-07-ACT1 | 1 | Sukartografuoti nuotolinės prieigos vektorius | Nustatyti, per kokius kanalus naudotojai gali pasiekti vidines sistemas iš išorės. |
| R11-PRIEI-07-ACT2 | 2 | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) ir web portalams | Techniniu lygmeniu sujungti nuotolinės prieigos sprendimus su MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) paslauga. |
| R11-PRIEI-07-ACT2 | 2 | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) ir web portalams | Techniniu lygmeniu sujungti nuotolinės prieigos sprendimus su MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) paslauga. |
| R11-PRIEI-08-ACT1 | 1 | Klasifikuoti sistemas pagal kritiškumą MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) požiūriu | Išsigryninti, kurios sistemos laikomos kritinėmis ir turi naudoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija). |
| R11-PRIEI-08-ACT1 | 1 | Klasifikuoti sistemas pagal kritiškumą MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) požiūriu | Išsigryninti, kurios sistemos laikomos kritinėmis ir turi naudoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija). |
| R11-PRIEI-08-ACT2 | 2 | Techniniu lygmeniu įgyvendinti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) kritinėms sistemoms/DB (Database, duomenų bazė) | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) arba alternatyvias prieigos kontrolės priemones ten, kur tiesioginė MFA integracija neįmanoma. |
| R11-PRIEI-08-ACT2 | 2 | Techniniu lygmeniu įgyvendinti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) kritinėms sistemoms/DB (Database, duomenų bazė) | Sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) arba alternatyvias prieigos kontrolės priemones ten, kur tiesioginė MFA integracija neįmanoma. |
| R11-PRIEI-09-ACT1 | 1 | Aprašyti saugios komunikacijos naudojimo atvejus | Nustatyti, kokie pokalbiai ir kanalai privalo naudoti šifravimą. |
| R11-PRIEI-09-ACT1 | 1 | Aprašyti saugios komunikacijos naudojimo atvejus | Nustatyti, kokie pokalbiai ir kanalai privalo naudoti šifravimą. |
| R11-PRIEI-09-ACT2 | 2 | Technologiškai užtikrinti šifruotą komunikaciją | Pasirinkti ir įdiegti sprendimus, užtikrinančius šifruotą balsą, vaizdą ir tekstą. |
| R11-PRIEI-09-ACT2 | 2 | Technologiškai užtikrinti šifruotą komunikaciją | Pasirinkti ir įdiegti sprendimus, užtikrinančius šifruotą balsą, vaizdą ir tekstą. |
| R11-PRIEI-10-ACT1 | 1 | Aprašyti avarinio ryšio modelį incidentų ir krizių metu | Nustatyti, kaip organizacija komunikuos kibernetinio incidento, IT (Information Technology, informacinės technologijos) sutrikimo ar fizinės krizės atveju. |
| R11-PRIEI-10-ACT1 | 1 | Aprašyti avarinio ryšio modelį incidentų ir krizių metu | Nustatyti, kaip organizacija komunikuos kibernetinio incidento, IT (Information Technology, informacinės technologijos) sutrikimo ar fizinės krizės atveju. |

| | | | |
|---|---|---|---|
| R11-PRIEI-10-ACT2 | 2 | Techniniu lygmeniu užtikrinti avarinio ryšio kanalų veikimą | Suteikti priemones kritiniams vaidmenims ir periodiškai tikrinti jų veikimą. |
| R11-PRIEI-10-ACT2 | 2 | Techniniu lygmeniu užtikrinti avarinio ryšio kanalų veikimą | Suteikti priemones kritiniams vaidmenims ir periodiškai tikrinti jų veikimą. |
| R11-TINK-01-ACT1 | 1 | Sukurti tinklo zonų ir segmentų modelį | Aprašyti, kaip logiškai ir fiziškai atskiriamos tinklo zonos pagal riziką ir funkciją. |
| R11-TINK-01-ACT1 | 1 | Sukurti tinklo zonų ir segmentų modelį | Aprašyti, kaip logiškai ir fiziškai atskiriamos tinklo zonos pagal riziką ir funkciją. |
| R11-TINK-01-ACT2 | 2 | Realizuoti tinklo segmentavimą naudojant VLAN (Virtual Local Area Network, virtualus vietinis tinklas (VLAN)), router'ius ir ugniasienes | Sukonfigūruoti tinklo įrangą taip, kad zonos būtų atskirtos ir kontroliuojamos. |
| R11-TINK-01-ACT2 | 2 | Realizuoti tinklo segmentavimą naudojant VLAN (Virtual Local Area Network, virtualus vietinis tinklas (VLAN)), router'ius ir ugniasienes | Sukonfigūruoti tinklo įrangą taip, kad zonos būtų atskirtos ir kontroliuojamos. |
| R11-TINK-02-ACT1 | 1 | Sukurti tarpzoninių srautų valdymo politiką | Aprašyti, kokie srautai tarp zonų leidžiami ir kokiais principais kuriamos taisyklės. |
| R11-TINK-02-ACT1 | 1 | Sukurti tarpzoninių srautų valdymo politiką | Aprašyti, kokie srautai tarp zonų leidžiami ir kokiais principais kuriamos taisyklės. |
| R11-TINK-02-ACT2 | 2 | Sukonfigūruoti ir prižiūrėti ugniasienes | Techniniu lygmeniu sukurti, optimizuoti ir stebėti ugniasienių taisykles. |
| R11-TINK-02-ACT2 | 2 | Sukonfigūruoti ir prižiūrėti ugniasienes | Techniniu lygmeniu sukurti, optimizuoti ir stebėti ugniasienių taisykles. |
| R11-TINK-03-ACT1 | 1 | Nustatyti, kurie įrenginiai turi būti dengiami EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas)/AV (Antivirus, antivirusinė programinė įranga) | Sukurti aiškią endpoint apsaugos aprėpties politiką. |
| R11-TINK-03-ACT1 | 1 | Nustatyti, kurie įrenginiai turi būti dengiami EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas)/AV (Antivirus, antivirusinė programinė įranga) | Sukurti aiškią endpoint apsaugos aprėpties politiką. |
| R11-TINK-03-ACT2 | 2 | Implementuoti centriniu būdu valdomą endpoint apsaugą | Diegti ir konfigūruoti apsaugos agentus įrenginiuose, įskaitant nuotolinius. |
| R11-TINK-03-ACT2 | 2 | Implementuoti centriniu būdu valdomą endpoint apsaugą | Diegti ir konfigūruoti apsaugos agentus įrenginiuose, įskaitant nuotolinius. |
| R11-TINK-04-ACT1 | 1 | Diegti el. pašto filtravimo ir anti-phishing priemones | Užtikrinti, kad prieš pasiekiant naudotojus el. laiškai būtų filtruojami ir analizuojami. |
| R11-TINK-04-ACT1 | 1 | Diegti el. pašto filtravimo ir anti-phishing priemones | Užtikrinti, kad prieš pasiekiant naudotojus el. laiškai būtų filtruojami ir analizuojami. |

| | | | |
|---|---|---|---|
| R11-TINK-04-ACT2 | 2 | Stebėti el. pašto grėsmes ir įtraukti naudotojus | Naudotojai tampa papildomu apsaugos sluoksniu, o saugumo komanda stebi grėsmių tendencijas. |
| R11-TINK-04-ACT2 | 2 | Stebėti el. pašto grėsmes ir įtraukti naudotojus | Naudotojai tampa papildomu apsaugos sluoksniu, o saugumo komanda stebi grėsmių tendencijas. |
| R11-TINK-05-ACT1 | 1 | Aprašyti interneto naudojimo ir filtravimo taisykles | Sukurti aiškią politiką, ką leidžiama/nedraudziama pasiekti iš organizacijos tinklo. |
| R11-TINK-05-ACT1 | 1 | Aprašyti interneto naudojimo ir filtravimo taisykles | Sukurti aiškią politiką, ką leidžiama/nedraudziama pasiekti iš organizacijos tinklo. |
| R11-TINK-05-ACT2 | 2 | Implementuoti web filtering / proxy sprendimą | Techniniu lygmeniu užtikrinti interneto srauto filtravimą pagal nustatytą politiką. |
| R11-TINK-05-ACT2 | 2 | Implementuoti web filtering / proxy sprendimą | Techniniu lygmeniu užtikrinti interneto srauto filtravimą pagal nustatytą politiką. |
| R11-TINK-06-ACT1 | 1 | Pasirinkti, kur ir kaip diegti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) | Apsispręsti, ar naudoti tinklinį IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema), host-based IDS, ar hibridinį modelį. |
| R11-TINK-06-ACT2 | 2 | Suinstaliuoti ir sureguliuoti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) taisykles | Praktiškai įdiegti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) ir suderinti signatūras bei taisykles, kad būtų naudingi alertai. |
| R11-TINK-06-ACT2 | 2 | Suinstaliuoti ir sureguliuoti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) taisykles | Praktiškai įdiegti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) ir suderinti signatūras bei taisykles, kad būtų naudingi alertai. |
| R11-TINK-07-ACT1 | 1 | Nusistatyti tinklo srautų stebėsenos tikslus | Suprasti, kokius srautus ir kokiais tikslais reikia stebėti (saugumas, našumas, incidentų tyrimas). |
| R11-TINK-07-ACT2 | 2 | Implementuoti tinklo stebėsenos ir analizės įrankius | Rinkti ir naudoti tinklo duomenis incidentų aptikimui ir veiklos stabilumui užtikrinti. |
| R11-TINK-07-ACT2 | 2 | Implementuoti tinklo stebėsenos ir analizės įrankius | Rinkti ir naudoti tinklo duomenis incidentų aptikimui ir veiklos stabilumui užtikrinti. |
| R11-TINK-08-ACT1 | 1 | Patikrinti administravimo prieigos būdus | Nustatyti, kur naudojami nesaugūs protokolai (pvz., telnet, HTTP (Hypertext Transfer Protocol, hiperteksto perdavimo protokolas HTTP), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) be šifravimo). |
| R11-TINK-08-ACT1 | 1 | Patikrinti administravimo prieigos būdus | Nustatyti, kur naudojami nesaugūs protokolai (pvz., telnet, HTTP (Hypertext Transfer Protocol, hiperteksto perdavimo protokolas HTTP), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) be šifravimo). |

| | | | |
|---|---|---|---|
| R11-TINK-08-ACT2 | 2 | Sukonfigūruoti administravimo prieigą per saugius kanalus | Naudoti tik saugius protokolus ir pageidautina centralizuotus valdymo kanalus. |
| R11-TINK-08-ACT2 | 2 | Sukonfigūruoti administravimo prieigą per saugius kanalus | Naudoti tik saugius protokolus ir pageidautina centralizuotus valdymo kanalus. |
| R11-TINK-09-ACT1 | 1 | Suprasti esamą cloud prieigos kraštovaizdį | Nustatyti, kokios cloud platformos naudojamos ir kaip tvarkoma prieiga. |
| R11-TINK-09-ACT1 | 1 | Suprasti esamą cloud prieigos kraštovaizdį | Nustatyti, kokios cloud platformos naudojamos ir kaip tvarkoma prieiga. |
| R11-TINK-09-ACT2 | 2 | Sujungti cloud aplinkas su IDP (Identity Provider, tapatybės teikėjas (IdP)) ir MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) | Naudoti vieningą identiteto ir prieigos valdymą debesijos aplinkoms. |
| R11-TINK-09-ACT2 | 2 | Sujungti cloud aplinkas su IDP (Identity Provider, tapatybės teikėjas (IdP)) ir MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) | Naudoti vieningą identiteto ir prieigos valdymą debesijos aplinkoms. |
| R12-PRIEI-01-ACT1 | 1 | Apibrėžti prieigos kontrolės politikos taikymo sritį ir pagrindinius principus | Nusistatyti, kokius naudotojus, sistemas ir prieigos tipus apims politika, ir kokie pagrindiniai saugumo principai bus taikomi. |
| R12-PRIEI-01-ACT1 | 1 | Apibrėžti prieigos kontrolės politikos taikymo sritį ir pagrindinius principus | Nusistatyti, kokius naudotojus, sistemas ir prieigos tipus apims politika, ir kokie pagrindiniai saugumo principai bus taikomi. |
| R12-PRIEI-01-ACT2 | 2 | Sukurti ir patvirtinti prieigos kontrolės politiką | Dokumentuoti prieigos kontrolės politiką ir gauti vadovybės patvirtinimą. |
| R12-PRIEI-01-ACT2 | 2 | Sukurti ir patvirtinti prieigos kontrolės politiką | Dokumentuoti prieigos kontrolės politiką ir gauti vadovybės patvirtinimą. |
| R12-PRIEI-01-ACT3 | 3 | Įdiegti politiką į praktinius procesus ir užtikrinti jos atnaujinimą | Susieti politiką su praktiniais procesais (onboarding, offboarding, tiekėjų valdymas) ir nustatyti peržiūros periodiškumą. |
| R12-PRIEI-01-ACT3 | 3 | Įdiegti politiką į praktinius procesus ir užtikrinti jos atnaujinimą | Susieti politiką su praktiniais procesais (onboarding, offboarding, tiekėjų valdymas) ir nustatyti peržiūros periodiškumą. |
| R12-PRIEI-02-ACT1 | 1 | Sukurti teisių ir rolių modelį pagal funkcijas | Aprašyti, kokias funkcijas atlieka skirtingi vaidmenys ir kokių teisių jiems reikia. |
| R12-PRIEI-02-ACT1 | 1 | Sukurti teisių ir rolių modelį pagal funkcijas | Aprašyti, kokias funkcijas atlieka skirtingi vaidmenys ir kokių teisių jiems reikia. |
| R12-PRIEI-02-ACT2 | 2 | Sukonfigūruoti sistemas pagal mažiausių teisių principą | Pridėti ir / arba perkonfigūruoti roles bei teises, kad naudotojai turėtų tik būtiniausias prieigas. |
| R12-PRIEI-02-ACT2 | 2 | Sukonfigūruoti sistemas pagal mažiausių teisių principą | Pridėti ir / arba perkonfigūruoti roles bei teises, kad naudotojai turėtų tik būtiniausias prieigas. |
| R12-PRIEI-03-ACT1 | 1 | Nustatyti atskirų administracinių paskyrų naudojimo taisykles | Apibrėžti, kada ir kokiais tikslais naudojamos administratoriaus paskyros, draudžiant jų naudojimą kasdieniam darbui. |

| | | | |
|---|---|---|---|
| R12-PRIEI-03-ACT1 | 1 | Nustatyti atskirų administracinių paskyrų naudojimo taisykles | Apibrėžti, kada ir kokiais tikslais naudojamos administratoriaus paskyros, draudžiant jų naudojimą kasdieniam darbui. |
| R12-PRIEI-03-ACT2 | 2 | Sukonfigūruoti ir valdyti atskiras administravimo paskyras | Sukurti ir / arba atskirti administravimo paskyras, nustatyti jų naudojimo ir monitoring'o taisykles. |
| R12-PRIEI-03-ACT2 | 2 | Sukonfigūruoti ir valdyti atskiras administravimo paskyras | Sukurti ir / arba atskirti administravimo paskyras, nustatyti jų naudojimo ir monitoring'o taisykles. |
| R12-PRIEI-04-ACT1 | 1 | Nustatyti prieigos peržiūrų periodiškumą ir atsakomybes | Apibrėžti, kas, kaip dažnai ir kokiu būdu peržiūri naudotojų teises. |
| R12-PRIEI-04-ACT1 | 1 | Nustatyti prieigos peržiūrų periodiškumą ir atsakomybes | Apibrėžti, kas, kaip dažnai ir kokiu būdu peržiūri naudotojų teises. |
| R12-PRIEI-04-ACT2 | 2 | Vykdyti ir, kiek įmanoma, automatizuoti prieigos peržiūras | Naudoti ataskaitas ir įrankius, kad peržiūros vyktų sklandžiai ir būtų užfiksuotos. |
| R12-PRIEI-04-ACT2 | 2 | Vykdyti ir, kiek įmanoma, automatizuoti prieigos peržiūras | Naudoti ataskaitas ir įrankius, kad peržiūros vyktų sklandžiai ir būtų užfiksuotos. |
| R12-PRIEI-05-ACT1 | 1 | Aprašyti, kokie įvykiai turi būti registruojami privilegijuotoms paskyroms | Sukurti reikalavimus, kokius veiksmus ir kiek laiko reikia saugoti auditui ir incidentų tyrimams. |
| R12-PRIEI-05-ACT1 | 1 | Aprašyti, kokie įvykiai turi būti registruojami privilegijuotoms paskyroms | Sukurti reikalavimus, kokius veiksmus ir kiek laiko reikia saugoti auditui ir incidentų tyrimams. |
| R12-PRIEI-05-ACT2 | 2 | Techniniu lygmeniu užtikrinti privilegijuotų paskyrų veiklos stebėseną | Įgalinti privilegijuotų paskyrų veiklos logų siuntimą į SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) ar analogišką sprendimą ir nustatyti alertus. |
| R12-PRIEI-05-ACT2 | 2 | Techniniu lygmeniu užtikrinti privilegijuotų paskyrų veiklos stebėseną | Įgalinti privilegijuotų paskyrų veiklos logų siuntimą į SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) ar analogišką sprendimą ir nustatyti alertus. |
| R12-PRIEI-11-ACT1 | 1 | Sukurti joiner/mover/leaver proceso aprašą | Aprašyti, kaip registruojami nauji darbuotojai, keičiasi jų rolės ir nutraukiami darbo santykiai prieigos kontrolės požiūriu. |
| R12-PRIEI-11-ACT1 | 1 | Sukurti joiner/mover/leaver proceso aprašą | Aprašyti, kaip registruojami nauji darbuotojai, keičiasi jų rolės ir nutraukiami darbo santykiai prieigos kontrolės požiūriu. |
| R12-PRIEI-11-ACT2 | 2 | Automatizuoti paskyrų kūrimą ir uždarymą | Sujungti HR (Human Resources, žmogiškieji ištekliai) sistemą su IAM (Identity and Access Management, tapatybių ir prieigos valdymas)/IDP (Identity Provider, tapatybės teikėjas (IdP)) ir įgyvendinti automatines taisykles darbuotojų paskyrų valdymui. |

| | | | |
|---|---|---|---|
| R12-PRIEI-11-ACT2 | 2 | Automatizuoti paskyrų kūrimą ir uždarymą | Sujungti HR (Human Resources, žmogiškieji ištekliai) sistemą su IAM (Identity and Access Management, tapatybių ir prieigos valdymas)/IDP (Identity Provider, tapatybės teikėjas (IdP)) ir įgyvendinti automatines taisykles darbuotojų paskyrų valdymui. |
| R12-PRIEI-11-ACT2 | 2 | Automatizuoti paskyrų kūrimą ir uždarymą | Sujungti HR (Human Resources, žmogiškieji ištekliai) sistemą su IAM (Identity and Access Management, tapatybių ir prieigos valdymas)/IDP (Identity Provider, tapatybės teikėjas (IdP)) ir įgyvendinti automatines taisykles darbuotojų paskyrų valdymui. |

## 5.3. Įgyvendinimo žingsniai.

| Žingsnio_ID | Žingsnio_NR_veiksme | Žingsnio aprašymas |
|---|---|---|
| R1-POL-01-ACT1-S1 | 1 | Surinkti taikomų teisės aktų ir standartų reikalavimus. |
| R1-POL-01-ACT1-S2 | 2 | Parengti politikos struktūrą (taikymo sritis, tikslai, principai, vaidmenys, ryšys su kitomis politikomis). |
| R1-POL-01-ACT1-S3 | 3 | Suderinti politikos projektą su suinteresuotomis šalimis ir pateikti tvirtinti vadovybei / valdybai. |
| R1-POL-01-ACT2-S1 | 1 | Publikuoti patvirtintą politiką vidinėje žinių bazėje ar intranete. |
| R1-POL-01-ACT2-S2 | 2 | Informuoti darbuotojus apie naują / atnaujintą politiką el. paštu ar per vidines komunikacijos priemones. |
| R1-POL-02-ACT1-S1 | 1 | Identifikuoti pagrindines kibernetinio saugumo sritis (konfidencialumas, vientisumas, prieinamumas, atsparumas). |
| R1-POL-02-ACT1-S2 | 2 | Suformuluoti 3–7 aiškius kibernetinio saugumo tikslus (pvz., sumažinti incidentų skaičių, didinti vartotojų sąmoningumą). |
| R1-POL-02-ACT2-S1 | 1 | Priskirti politikos savininką (owner) ir apibrėžti jo atsakomybes. |
| R1-POL-02-ACT2-S2 | 2 | Nustatyti privalomą politikos peržiūros periodiškumą (pvz., kas 12 ar 24 mėn.) ir įtraukti tai į dokumentą. |
| R1-RIZ-01-ACT1-S1 | 1 | Nuspręsti, kokia rizikos vertinimo metodika bus naudojama (kokie rizikos lygiai, matricos, kriterijai). |
| R1-RIZ-01-ACT1-S2 | 2 | Aprašyti rizikos vertinimo žingsnius (turto identifikavimas, grėsmių ir pažeidžiamumų analizė, rizikos įvertinimas, priemonių parinkimas). |

| | | |
|---|---|---|
| R1-RIZ-01-ACT2-S1 | 1 | Suderinti rizikos vertinimo politiką su pagrindiniais suinteresuotais padaliniais. |
| R1-RIZ-01-ACT2-S2 | 2 | Publikuoti patvirtintą rizikos vertinimo politiką ir informuoti atsakingus asmenis apie jos taikymą. |
| R1-RIZ-02-ACT1-S1 | 1 | Sukurti metinį rizikos vertinimo planą su numatytomis datomis ir atsakingais asmenimis. |
| R1-RIZ-02-ACT1-S2 | 2 | Įtraukti rizikos vertinimo aktyvumą į organizacijos metinį veiklos planą ir valdymo darbotvarkę. |
| R1-RIZ-02-ACT2-S1 | 1 | Sukviesti dalyvaujančias šalis (IT (Information Technology, informacinės technologijos), verslo padalinius, saugumo funkciją) rizikos vertinimo sesijoms. |
| R1-RIZ-02-ACT2-S2 | 2 | Parengti rizikos vertinimo ataskaitą su identifikuotomis rizikomis, priemonių prioritetais ir atsakingais asmenimis. |
| R1-RIZ-03-ACT1-S1 | 1 | Sukurti ir dokumentuoti sąrašą įvykių, kurie laikomi esminiais pokyčiais (pvz., naujos kritinės sistemos diegimas, migracija į debesiją, esminis architektūros pakeitimas). |
| R1-RIZ-03-ACT1-S2 | 2 | Įtraukti kriterijus į pokyčių valdymo (change management) ir architektūros peržiūros procesus. |
| R1-RIZ-03-ACT2-S1 | 1 | Sukonfigūruoti darbo srautą, kuris automatiškai priskiria užduotį rizikos komandai, kai registruojamas esminis pokytis. |
| R1-RIZ-03-ACT2-S2 | 2 | Dokumentuoti atliktų neplaninių rizikos vertinimų rezultatus ir atnaujinti rizikų registrą. |
| R1-RIZ-04-ACT1-S1 | 1 | Nustatyti turto kategorijas (sistemos, aplikacijos, duomenų rinkiniai, įranga) ir klasifikavimo kriterijus (kritiškumas, jautrumas). |
| R1-RIZ-04-ACT1-S2 | 2 | Sudaryti ir periodiškai atnaujinti IT (Information Technology, informacinės technologijos) ir informacinio turto sąrašą su savininkais (owners). |
| R1-RIZ-04-ACT2-S1 | 1 | Parengti rizikos vertinimo šabloną, kuriame būtų atskiri laukai turtui, grėsmėms, pažeidžiamumams, esamoms ir planuojamoms priemonėms. |
| R1-RIZ-04-ACT2-S2 | 2 | Užtikrinti, kad atliekant rizikos vertinimą šablonas būtų pilnai pildomas ir rezultatai perkeliami į rizikų registrą. |
| R2-VAL-01-ACT1-S1 | 1 | Sudaromas visų galiojančių ir planuojamų kibernetinio saugumo priemonių (politikos, procedūros, techninės kontrolės priemonės) sąrašas, identifikuojant jų savininkus ir taikymo sritį. |
| R2-VAL-01-ACT1-S2 | 2 | Parengiamas valdybos sprendimo (nutarimo arba protokolinio sprendimo) projektas, kuriuo patvirtinamas kibernetinio saugumo priemonių paketas ir jo taikymo principai. |
| R2-VAL-01-ACT1-S3 | 3 | Į valdybos posėdžio darbotvarkę įtraukiamas punktas dėl kibernetinio saugumo priemonių paketo patvirtinimo ir užtikrinamas medžiagos pateikimas valdybos nariams iš anksto. |
| R2-VAL-01-ACT2-S1 | 1 | Valdybos posėdžio protokole užfiksuojamas sprendimas dėl kibernetinio saugumo priemonių paketo patvirtinimo ir nurodomi pagrindiniai įsipareigojimai. |
| R2-VAL-01-ACT2-S2 | 2 | Atnaujinamos organizacijos vidaus tvarkos, nuostatai ir dokumentų registrai, aiškiai nurodant, kad kibernetinio saugumo priemonės yra patvirtintos valdybos sprendimu. |

| | | |
|---|---|---|
| R2-VAL-01-ACT2-S3 | 3 | Apie valdybos sprendimą dėl kibernetinio saugumo priemonių informuojama vadovų komanda ir kiti atsakingi asmenys (pvz., per vadovų susirinkimą ar vidinę komunikaciją). |
| R2-VAL-02-ACT1-S1 | 1 | Parengiamas CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo pareigybės aprašymas, apibrėžiant pagrindines funkcijas (politikų kūrimas, rizikos vertinimo koordinavimas, incidentų valdymo priežiūra ir t. t.). |
| R2-VAL-02-ACT1-S2 | 2 | Nustatoma CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo atskaitomybė (pvz., tiesiogiai generaliniam direktoriui, valdybai ar jos komitetui) ir tai įtvirtinama organizacinėje struktūroje. |
| R2-VAL-02-ACT2-S1 | 1 | Pasirenkamas kandidatas į CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo pareigas, įvertinant jo kompetenciją, nepriklausomumą ir interesų konfliktus. |
| R2-VAL-02-ACT2-S2 | 2 | Priimamas formalus sprendimas (įsakymas, potvarkis arba valdybos nutarimas) dėl CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovo paskyrimo. |
| R2-VAL-02-ACT2-S3 | 3 | Apie paskirtą CISO (Chief Information Security Officer, informacijos saugos vadovas) / kibernetinio saugumo vadovą informuojami darbuotojai (pvz., per intranetą, el. laišką, vadovų susirinkimą) ir atnaujinamos kontaktų bei atsakomybės skiltys. |
| R2-VAL-03-ACT1-S1 | 1 | Peržiūrima organizacinė struktūra, pareigybių aprašymai ir ataskaitų teikimo linijos, identifikuojant, ar CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcijos nėra pavestos tam pačiam asmeniui, kuris atsakingas už IT (Information Technology, informacinės technologijos) infrastruktūros administravimą. |
| R2-VAL-03-ACT1-S2 | 2 | Identifikuojamos interesų konfliktų rizikos (pvz., kai tas pats asmuo atsakingas ir už kontrolės priemonių diegimą, ir už jų priežiūrą) ir dokumentuojamos rekomendacijos dėl atskyrimo. |
| R2-VAL-03-ACT2-S1 | 1 | Patvirtinamas sprendimas dėl CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcijos atskyrimo nuo IT (Information Technology, informacinės technologijos) administravimo (pvz., CISO perkeliamas į rizikų / atitikties funkciją arba tampa tiesiogiai pavaldus generaliniam direktoriui / valdybai). |
| R2-VAL-03-ACT2-S2 | 2 | Atnaujinami pareigybių aprašymai, organizacinė struktūra ir atskaitomybės schema, atspindint naują CISO (Chief Information Security Officer, informacijos saugos vadovas) funkcijos vietą ir jos santykį su IT (Information Technology, informacinės technologijos) administravimu. |
| R2-VAL-04-ACT1-S1 | 1 | Patikrinami KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) ir NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) gairėse numatyti reikalavimai dėl atsakingų asmenų (kontaktinių punktų) pateikimo ir atnaujinimo periodiškumo. |
| R2-VAL-04-ACT1-S2 | 2 | Per NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) nustatytas priemones (pvz., Kibernetinio saugumo informacinę sistemą) pateikiama informacija apie paskirtus atsakingus asmenis ir jų kontaktus. |
| R2-VAL-04-ACT2-S1 | 1 | Atnaujinamas intranetas, organizacinės struktūros diagramos ir kontaktų puslapiai, aiškiai nurodant CISO (Chief Information Security Officer, informacijos saugos vadovas) ir kitų kibernetinio saugumo kontaktų vardus, pareigas ir kontaktus. |
| R2-VAL-04-ACT2-S2 | 2 | Darbuotojams išsiunčiamas vidinis pranešimas (el. paštu ar per kitą komunikacijos kanalą) apie paskirtus atsakingus asmenis ir nurodoma, kokiais klausimais į juos kreiptis. |
| R2-VAL-05-ACT1-S1 | 1 | Identifikuojamos pagrindinės temos valdybos mokymams (NIS2 (Network and Information Security Directive 2, antroji ES tinklų ir informacinių sistemų saugumo direktyva (NIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) reikalavimai valdybai, kritinių paslaugų rizikos, incidentų valdymo atsakomybės, sankcijos ir reputacinės rizikos). |

| | | |
|---|---|---|
| R2-VAL-05-ACT1-S2 | 2 | Pasirenkamas mokymų formatas (kontaktiniai seminarai, nuotoliniai mokymai, e-mokymai) ir vidinis ar išorinis lektorius. |
| R2-VAL-05-ACT1-S3 | 3 | Mokymų programa suderinama su valdyba (pvz., patvirtinama valdybos ar audito komiteto posėdyje) kaip privaloma visiems valdybos nariams. |
| R2-VAL-05-ACT2-S1 | 1 | Suplanuojamos mokymų datos ir integruojamos į valdybos posėdžių ar atskirų sesijų kalendorių. |
| R2-VAL-05-ACT2-S2 | 2 | Įvykdomi mokymai ir fiksuojamas kiekvieno valdybos nario dalyvavimas (dalyvių sąrašai, pasirašymai, LMS (Learning Management System, mokymų valdymo sistema) ataskaitos). |
| R2-VAL-05-ACT2-S3 | 3 | Parengiama trumpoji ataskaita valdybai apie įvykusius mokymus, dalyvavimo statistiką ir numatomą periodiškumą (pvz., kartą per metus). |
| R2-VAL-06-ACT1-S1 | 1 | Identifikuojamos konkrečios NIS2 (Network and Information Security Directive 2, antroji ES tinklų ir informacinių sistemų saugumo direktyva (NIS2)) ir KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) nuostatos, susijusios su valdybos narių atsakomybe, priežiūra ir galimomis sankcijomis. |
| R2-VAL-06-ACT1-S2 | 2 | Mokymų medžiagoje paruošiami praktiniai pavyzdžiai (case studies) apie incidentų ir pažeidimų atvejus, kuriuose išryškėja valdybos atsakomybė. |
| R2-VAL-06-ACT2-S1 | 1 | Į mokymų sesiją įtraukiama diskusijos dalis, kurioje valdybos nariai aptaria savo atsakomybę, užduoda klausimus ir gauna atsakymus iš teisės / atitikties ekspertų. |
| R2-VAL-06-ACT2-S2 | 2 | Parengiamas ir pasirašomas valdybos narių patvirtinimas (pvz., deklaracija ar protokolo ištrauka), kad jie susipažino su atsakomybe ir supranta galimas sankcijas. |
| R2-VAL-07-ACT1-S1 | 1 | Peržiūrimi KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas), poįstatyminiai aktai ir NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) gairės, nustatant subjektų, privalančių registruotis Kibernetinio saugumo informacinėje sistemoje, kriterijus. |
| R2-VAL-07-ACT1-S2 | 2 | Surenkami reikalingi registracijos duomenys (organizacijos pavadinimas, kodas, kontaktiniai asmenys, paslaugų rūšys ir kt.). |
| R2-VAL-07-ACT2-S1 | 1 | Per NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) Kibernetinio saugumo informacinę sistemą užpildomos registracijos formos ir pateikiami organizacijos duomenys. |
| R2-VAL-07-ACT2-S2 | 2 | Sukuriama procedūra / vidaus taisyklė, nustatanti, kaip ir kada atnaujinami KSIS (kibernetinio saugumo informacinė sistema (KSIS)) duomenys (pvz., pasikeitus CISO (Chief Information Security Officer, informacijos saugos vadovas), kontaktiniams asmenims ar paslaugų apimčiai). |
| R3-INC-01-ACT1-S1 | 1 | Surenkama informacija apie esamus incidentų reagavimo, krizių valdymo ir verslo tęstinumo procesus, siekiant išvengti dubliavimo ir užtikrinti suderinamumą. |
| R3-INC-01-ACT1-S2 | 2 | Parengiamas incidentų valdymo plano projektas, apimantis identifikavimą, eskalavimą, analizę, komunikaciją, atstatymą ir veiklos atnaujinimą. |
| R3-INC-01-ACT2-S1 | 1 | Incidentų valdymo plano projektas suderinamas su vadovybe ir pagrindiniais suinteresuotaisiais asmenimis (IT (Information Technology, informacinės technologijos), verslo, teisininkų, komunikacijos atstovais). |

| | | |
|---|---|---|
| R3-INC-01-ACT2-S2 | 2 | Planą patvirtina valdyba ar generalinis direktorius, o planas įtraukiamas į oficialų vidaus dokumentų registrą. |
| R3-INC-01-ACT2-S3 | 3 | Nustatoma plano peržiūros ir atnaujinimo periodiškumo tvarka (pvz., kartą per metus arba po kiekvieno reikšmingo incidento) ir ji dokumentuojama. |
| R3-INC-02-ACT1-S1 | 1 | Parengiami incidentų tipų pavyzdžiai (pvz., DDoS, įsibrovimai, duomenų nutekėjimas, paslaugų sutrikimai) ir priskiriami jiems kritiškumo lygiai. |
| R3-INC-02-ACT1-S2 | 2 | Incidentų klasifikavimui nustatomi objektyvūs kriterijai (pvz., paveiktų naudotojų skaičius, paslaugų sutrikimo trukmė, teisinės ir reputacinės pasekmės). |
| R3-INC-02-ACT2-S1 | 1 | Sudaroma incidentų valdymo RACI (Responsible, Accountable, Consulted, Informed, atsakingų, atskaitingų, konsultuojamų ir informuojamų asmenų RACI matrica) matrica, apibrėžianti atsakomybes (Responsible, Accountable, Consulted, Informed) kiekviename incidento valdymo etape. |
| R3-INC-02-ACT2-S2 | 2 | Incidentų valdymo plane aprašomi vidinės ir išorinės komunikacijos kanalai (NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)), kitos institucijos, klientai, tiekėjai, žiniasklaida) ir pranešimų turinio principai. |
| R3-INC-03-ACT1-S1 | 1 | Sudaromas naudojamų incidentų aptikimo priemonių (IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema), EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas), SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema), WAF (Web Application Firewall, žiniatinklio programų ugniasienė), antivirusai ir t. t.) sąrašas ir nustatoma, kokias sistemas / segmentus jos dengia. |
| R3-INC-03-ACT1-S2 | 2 | Identifikuojamos spragos, kuriose nėra pakankamų incidentų aptikimo priemonių (pvz., debesijos aplinkos, nuotoliniai vartotojai, OT (Operational Technology, operacinės technologijos) segmentai). |
| R3-INC-03-ACT2-S1 | 1 | Pasirenkami ir suplanuojami incidentų aptikimo sprendimų plėtros / diegimo veiksmai (pvz., SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) plėtra, EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas) išplėtimas į visas darbo vietas, IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) įdiegimas kritiniuose segmentuose). |
| R3-INC-03-ACT2-S2 | 2 | Konfigūruojamos įspėjimų taisyklės ir koreliacijos scenarijai, užtikrinant, kad kritinio lygio incidentai būtų aptikti ir eskaluoti artimu realiam laikui režimu. |
| R3-INC-04-ACT1-S1 | 1 | Parengiamas kritinių sistemų sąrašas (serveriai, duomenų bazės, aplikacijos, tinklo įranga, debesijos paslaugos) ir susiejamas su verslo paslaugomis. |
| R3-INC-04-ACT1-S2 | 2 | Nustatomi žurnalų tipai ir įvykių kategorijos, kurios turi būti renkami iš kiekvienos kritinės sistemos (prisijungimai, konfigūracijos pokyčiai, privilegijuota veikla, klaidos ir t. t.). |
| R3-INC-04-ACT2-S1 | 1 | Pasirenkamas ar sustiprinamas centralizuoto žurnalų rinkimo sprendimas (pvz., SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema), logų valdymo platforma) ir parengiamas diegimo planas. |
| R3-INC-04-ACT2-S2 | 2 | Sukonfigūruojami žurnalų agentai ar integracijos, užtikrinant, kad visos kritinės sistemos siunčia reikiamus įvykius į centralizuotą sprendimą. |
| R3-INC-05-ACT1-S1 | 1 | Teisės ir atitikties specialistai įvertina galiojančius teisės aktus ir sektoriaus rekomendacijas dėl žurnalų saugojimo terminų. |
| R3-INC-05-ACT1-S2 | 2 | Remiantis teisine analize, parengiama žurnalų saugojimo politika, apibrėžianti skirtingų logų tipų saugojimo terminus ir prieigos taisykles. |

| | | |
|---|---|---|
| R3-INC-05-ACT2-S1 | 1 | Centralizuotame logų rinkimo sprendime (SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) ar log management) nustatomi žurnalų saugojimo terminai pagal kiekvienos logų kategorijos politiką. |
| R3-INC-05-ACT2-S2 | 2 | Periodiškai peržiūrimi žurnalų saugojimo nustatymai ir faktinės saugojimo trukmės, užtikrinant atitiktį politikai ir optimalią saugojimo apimtį. |
| R3-INC-06-ACT1-S1 | 1 | Įvertinama, kokie žurnalai gali būti naudojami kaip įrodymai incidentų tyrimuose ar teisinėse procedūrose ir jiems nustatomi aukštesni integriteto reikalavimai. |
| R3-INC-06-ACT1-S2 | 2 | Parenkamos techninės priemonės žurnalų vientisumui užtikrinti (pvz., saugyklos, kriptografiniai parašai, hash'ai, prieigos kontrolė). |
| R3-INC-06-ACT2-S1 | 1 | Žurnalų saugykloms pritaikomos WORM (Write Once Read Many, kartą įrašyk – daug kartų skaityk (WORM) saugojimo principas) arba panašios funkcijos, ribojančios žurnalų modifikavimą ir ištrynimą iki nustatyto termino pabaigos. |
| R3-INC-06-ACT2-S2 | 2 | Įdiegiami žurnalų vientisumo tikrinimo mechanizmai (pvz., periodinis hash'ų tikrinimas, integriteto ataskaitos) ir apibrėžiama, kaip reaguojama į pažeidimus. |
| R3-INC-07-ACT1-S1 | 1 | Sudaromas peržiūrėtinų žurnalų sąrašas ir nustatomas peržiūros periodiškumas (pvz., realaus laiko monitoringas kritinėms sistemoms, dienos / savaitės ataskaitos mažiau kritinėms). |
| R3-INC-07-ACT1-S2 | 2 | Apibrėžiami eskalavimo kriterijai ir ataskaitų formatas, kai žurnalų analizės metu randamos anomalijos ar galimi incidentai. |
| R3-INC-07-ACT2-S1 | 1 | Paskiriami atsakingi asmenys / komandos už žurnalų analizę ir nustatoma, kaip fiksuojami peržiūrų rezultatai (pvz., ticket sistemoje ar ataskaitose). |
| R3-INC-07-ACT2-S2 | 2 | Nustatomi ir stebimi KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) (pvz., peržiūrėtų ataskaitų skaičius, aptiktų anomalijų skaičius, reakcijos laikas į nustatytas anomalijas). |
| R3-INC-08-ACT1-S1 | 1 | Atliekama kompetencijų ir priemonių analizė (turimos forensikos priemonės, specialistų patirtis, procesai) ir identifikuojami trūkumai. |
| R3-INC-08-ACT1-S2 | 2 | Nustatoma, kokiems incidentų tipams būtini specializuoti forensikos veiksmai ir kokio lygio reagavimas (vidinis ar išorinis) reikalingas. |
| R3-INC-08-ACT2-S1 | 1 | Parengiama incidentų tyrimo ir forensikos veiklų procedūra, apibrėžianti veiksmus, atsakomybes ir įrodymų grandinės (chain of custody) užtikrinimą. |
| R3-INC-08-ACT2-S2 | 2 | Jei trūksta vidinių kompetencijų, sudaromos sutartys ar preliminarios sutartys su išoriniais incidentų tyrimo / forensikos paslaugų teikėjais. |
| R3-INC-09-ACT1-S1 | 1 | Remiantis NIS2 (Network and Information Security Directive 2, antroji ES tinklų ir informacinių sistemų saugumo direktyva (NIS2)), KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) ir NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) gairėmis, nustatomi kriterijai, kada incidentas laikomas reikšmingu ir reikalauja ankstyvo įspėjimo (pvz., didelė apimtis, poveikis kritinėms paslaugoms). |
| R3-INC-09-ACT1-S2 | 2 | Sukuriamas ankstyvo įspėjimo procesas, apibrėžiantis atsakingus asmenis, informacijos rinkimo veiksmus ir sprendimo priėmimo seką per pirmąsias incidento valandas. |
| R3-INC-09-ACT2-S1 | 1 | Incidentų reagavimo ir SOC (Security Operations Center, saugumo operacijų centras) komandoms pristatomas ankstyvo įspėjimo procesas, paaiškinant, kada ir kaip inicijuojamas pranešimas NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)). |

| | | |
|---|---|---|
| R3-INC-09-ACT2-S2 | 2 | Organizuojami incidentų valdymo pratybų scenarijai, kuriuose imituojamas reikšmingas incidentas ir testuojamas ankstyvo įspėjimo procesas. |
| R3-INC-10-ACT1-S1 | 1 | Analizuojami NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) reikalavimai dėl incidentų pranešimų turinio ir struktūros (pvz., KSIS (kibernetinio saugumo informacinė sistema (KSIS)) formos, reikalaujami laukai). |
| R3-INC-10-ACT1-S2 | 2 | Parengiamas incidento pranešimo šablonas, atitinkantis NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) reikalavimus ir pritaikytas vidiniam informacijos surinkimui per pirmąsias incidento valandas. |
| R3-INC-10-ACT2-S1 | 1 | Incidentų valdymo ir verslo padaliniams pristatoma incidentų pranešimo NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) procedūra ir paaiškinama, kokius duomenis reikia pateikti ir kokiais terminais. |
| R3-INC-10-ACT2-S2 | 2 | Incidentų valdymo pratybų metu testuojamas incidento pranešimo per 72 valandas procesas, vertinant, ar įmanoma surinkti reikiamą informaciją laiku. |
| R3-INC-11-ACT1-S1 | 1 | Analizuojami NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) ir kitų reguliuotojų reikalavimai galutinėms incidentų ataskaitoms (priežastys, poveikis, priemonės, pamokos ir t. t.). |
| R3-INC-11-ACT1-S2 | 2 | Sukuriamas galutinės ataskaitos šablonas, apimantis incidento chronologiją, priežastis, poveikį, taikytas ir planuojamas priemones bei pamokas organizacijai. |
| R3-INC-11-ACT2-S1 | 1 | Incidentų valdymo procese apibrėžiami terminai ir atsakomybės už duomenų, reikalingų galutinei ataskaitai, pateikimą iš IT (Information Technology, informacinės technologijos), verslo, teisinės ir komunikacijos funkcijų. |
| R3-INC-11-ACT2-S2 | 2 | Po incidentų reguliariai vertinama, ar galutinės ataskaitos parengiamos per nustatytą terminą, ir, jei reikia, koreguojamas procesas. |
| R3-INC-12-ACT1-S1 | 1 | Remiantis sutartiniais įsipareigojimais, teisiniais reikalavimais ir gerąja praktika, nustatomi kriterijai, kada incidentas reikalauja klientų informavimo. |
| R3-INC-12-ACT1-S2 | 2 | Parengiami klientų informavimo pranešimų šablonai skirtingiems incidentų tipams ir kritiškumo lygiams. |
| R3-INC-12-ACT2-S1 | 1 | Incidentų valdymo plane apibrėžiama, kas inicijuoja klientų informavimą, kokius kanalus naudoja (el. paštas, portalas, SMS (Short Message Service, trumposios SMS žinutės) ir pan.) ir kaip fiksuojamas išsiųstų pranešimų faktas. |
| R3-INC-12-ACT2-S2 | 2 | Atliekamos pratybos arba testiniai scenarijai, kurių metu tikrinama, ar klientų informavimo procesas veikia ir nekelia papildomų rizikų (pvz., duomenų apsaugos). |
| R3-INC-13-ACT1-S1 | 1 | Incidentų valdymo plane apibrėžiama, kad po reikšmingų incidentų organizuojamas „post-incident review“ arba „lessons learned“ susitikimas per nustatytą laiką (pvz., per 2–4 savaites po incidento uždarymo). |
| R3-INC-13-ACT1-S2 | 2 | Parengiamas pamokų analizės susitikimo šablonas (darbotvarkė, klausimynas), apimantis priežastis, veiksmų efektyvumą, komunikaciją ir prevencines priemones. |
| R3-INC-13-ACT2-S1 | 1 | Po kiekvieno pamokų analizės susitikimo parengiamas tobulinimo priemonių sąrašas (procesų pakeitimai, papildomos kontrolės, mokymai) su atsakomybėmis ir terminais. |
| R3-INC-13-ACT2-S2 | 2 | Periodiškai peržiūrimas tobulinimo priemonių įgyvendinimo statusas ir atnaujinamos susijusios politikos, procedūros bei mokymų medžiaga. |

| | | |
|---|---|---|
| R4-TĘS-01-ACT1-S1 | 1 | Surinkti informaciją apie kritinius verslo procesus, IT (Information Technology, informacinės technologijos) sistemas, tiekėjus ir priklausomybes, pasinaudojant rizikos ir verslo poveikio analizės (BIA (Business Impact Analysis, verslo poveikio analizė)) rezultatais. |
| R4-TĘS-01-ACT1-S2 | 2 | Parengti BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) plano struktūrą ir turinį (scenarijai, atsakomybės, atkūrimo procedūros, komunikacija, sąveika su incidentų valdymo ir krizių valdymo planais). |
| R4-TĘS-01-ACT2-S1 | 1 | BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) plano projektas suderinamas su vadovybe ir pagrindiniais suinteresuotais padaliniais, integruojant pastabas ir užtikrinant, kad planas būtų realistiškas. |
| R4-TĘS-01-ACT2-S2 | 2 | BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) planą patvirtina vadovybė (pvz., generalinis direktorius ar valdyba), jis įtraukiamas į oficialų dokumentų registrą ir nustatomas peržiūros periodiškumas (pvz., kasmet). |
| R4-TĘS-02-ACT1-S1 | 1 | Organizuojami verslo ir IT (Information Technology, informacinės technologijos) workshop'ai, kuriuose aptariami kiekvienos kritinės paslaugos toleruojami prastovos ir duomenų praradimo laikai. |
| R4-TĘS-02-ACT1-S2 | 2 | RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslai suderinami su esamomis ar planuojamomis techninėmis galimybėmis (backup, HA (High Availability, didelio pasiekiamumo architektūra), georedundancy) ir patvirtinami vadovybės lygmeniu. |
| R4-TĘS-02-ACT2-S1 | 1 | BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) plane prie kiekvienos kritinės paslaugos ir sistemos įtraukiami patvirtinti RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslai ir atsakomybės už jų pasiekimą. |
| R4-TĘS-02-ACT2-S2 | 2 | RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslai perduodami infrastruktūros ir sistemų architektams, kad būtų įvertintas jų įgyvendinimas atsarginių kopijų, HA (High Availability, didelio pasiekiamumo architektūra) ir georedundancy sprendimuose. |
| R4-TĘS-03-ACT1-S1 | 1 | Nustatomi kriterijai, kada incidentas ar sutrikimas eskaluojamas į krizės lygį (pvz., reikšminga reputacinė žala, masiniai klientų sutrikimai, reguliuotojų įsitraukimas). |
| R4-TĘS-03-ACT1-S2 | 2 | Sukuriama krizių valdymo komanda (CMT (Change Management Tool, pakeitimų valdymo įrankis)), apibrėžiamos jos rolės ir atsakomybės bei sprendimų priėmimo tvarka. |
| R4-TĘS-03-ACT2-S1 | 1 | Parengiamas krizių valdymo plano dokumentas, apimantis veiksmų seką, komunikaciją, eskalavimą ir sąveiką su BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) ir incidentų valdymo planais. |
| R4-TĘS-03-ACT2-S2 | 2 | Krizių valdymo planas patvirtinamas vadovybės ir įtraukiamas į organizacijos valdymo dokumentų sistemą. |

| | | |
|---|---|---|
| R4-TĘS-04-ACT1-S1 | 1 | Inventorizuoti sistemas ir duomenų rinkinius, kuriems privaloma taikyti atsarginį kopijavimą, susiejant juos su RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslais. |
| R4-TĘS-04-ACT1-S2 | 2 | Parengiama atsarginių kopijų politika, apibrėžianti kopijavimo dažnį, saugojimo terminus, šifravimo ir offsite reikalavimus bei testavimo periodiškumą. |
| R4-TĘS-04-ACT2-S1 | 1 | Atsarginių kopijų politika ir tvarka patvirtinama vadovybės lygmeniu ir įtraukiama į IT (Information Technology, informacinės technologijos) bei saugumo valdymo dokumentus. |
| R4-TĘS-04-ACT2-S2 | 2 | IT (Information Technology, informacinės technologijos) operacijų procedūrose ir darbo instrukcijose integruojami atsarginių kopijų tvarkos reikalavimai ir atsakomybės. |
| R4-TĘS-05-ACT1-S1 | 1 | Pasirenkami ir sukonfigūruojami atsarginių kopijų sprendimai (pvz., Veeam, Commvault, Rubrik, debesijos backup paslaugos) kritinėms sistemoms. |
| R4-TĘS-05-ACT1-S2 | 2 | Sukuriami automatizuotų backup užduočių grafikai ir konfigūracijos pagal RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) reikalavimus (pilnos, inkrementinės, diferencialinės kopijos). |
| R4-TĘS-05-ACT2-S1 | 1 | Backup sistemose ir monitoring'o įrankiuose sukonfigūruojami įspėjimai apie nepavykusias backup užduotis ir kritinius nukrypimus. |
| R4-TĘS-05-ACT2-S2 | 2 | Sukuriama procedūra, apibrėžianti, kaip reaguojama į nepavykusias backup užduotis ir kaip greitai jos turi būti pašalintos. |
| R4-TĘS-06-ACT1-S1 | 1 | Įvertinami galimi offsite saugojimo variantai (second data center, cloud backup, juostų saugyklos) ir jų atitikimas saugumo bei reguliaciniams reikalavimams. |
| R4-TĘS-06-ACT1-S2 | 2 | Sudaromi techniniai ir sutartiniai reikalavimai offsite saugyklai, akcentuojant fizinę ir loginę izoliaciją nuo pagrindinės infrastruktūros. |
| R4-TĘS-06-ACT2-S1 | 1 | Sukonfigūruojamas atsarginių kopijų replikavimas į offsite saugyklą, naudojant tinklo segmentavimo ir prieigos kontrolės mechanizmus. |
| R4-TĘS-06-ACT2-S2 | 2 | Patikrinama, ar offsite aplinka nėra pasiekiama per tuos pačius administravimo kanalus kaip gamybinė aplinka (pvz., atskiri administravimo account'ai, segmentuotas tinklas). |
| R4-TĘS-07-ACT1-S1 | 1 | Įvertinami teisiniai, reguliaciniai ir vidiniai reikalavimai dėl duomenų šifravimo ir saugojimo, įskaitant jautrių ir asmens duomenų apsaugą. |
| R4-TĘS-07-ACT1-S2 | 2 | Parengiamas atsarginių kopijų šifravimo ir raktų valdymo politikos priedas, apibrėžiantis algoritmus, raktų saugojimą, rotaciją ir prieigos ribojimą. |
| R4-TĘS-07-ACT2-S1 | 1 | Backup sistemose įjungiamos šifravimo funkcijos (on-prem ir cloud) pagal politikos reikalavimus, užtikrinant šifravimą tiek perdavimo, tiek saugojimo metu. |

| | | |
|---|---|---|
| R4-TĘS-07-ACT2-S2 | 2 | Konfigūruojamas centralizuotas raktų valdymas (KMS (Key Management Service, kriptografinių raktų valdymo paslauga)/HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))), ribojant prieigą prie raktų ir fiksuojant audito žurnalus apie raktų naudojimą. |
| R4-TĘS-08-ACT1-S1 | 1 | Parengiamas atkūrimo testavimo grafikas (bent 2 kartus per metus), nustatant, kurios sistemos ir kokio tipo duomenys bus atkuriami kiekvieno testo metu. |
| R4-TĘS-08-ACT1-S2 | 2 | Parengiami atkūrimo testavimo scenarijai, kurie imituoja realias situacijas (duomenų praradimas, sistemos sugadinimas, ransomware). |
| R4-TĘS-08-ACT2-S1 | 1 | Pagal grafiką vykdomi duomenų atkūrimo testai, matuojant atkūrimo trukmę ir lyginant ją su RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) tikslais. |
| R4-TĘS-08-ACT2-S2 | 2 | Remiantis testų rezultatais parengiamas tobulinimo priemonių sąrašas (konfigūracijų keitimai, infrastruktūros stiprinimas, procesų korekcijos) ir sekamas jų įgyvendinimas. |
| R4-TĘS-09-ACT1-S1 | 1 | Identifikuojamos sistemos, kurioms būtinas HA (High Availability, didelio pasiekiamumo architektūra) pagal RTO (Recovery Time Objective, atkūrimo laiko tikslas (RTO))/RPO (Recovery Point Objective, atkūrimo taško tikslas (RPO)) ir veiklos tęstinumo reikalavimus. |
| R4-TĘS-09-ACT1-S2 | 2 | Parengiami HA (High Availability, didelio pasiekiamumo architektūra) architektūros principai (active-active, active-passive, failover mechanizmai) ir techniniai dizaino dokumentai. |
| R4-TĘS-09-ACT2-S1 | 1 | Įdiegiamos HA (High Availability, didelio pasiekiamumo architektūra) funkcijos (pvz., serverių klasteriai, load balancer'iai, redundanti maitinimo ir tinklo maršrutai) pagal parengtą architektūrą. |
| R4-TĘS-09-ACT2-S2 | 2 | Organizuojami periodiniai failover testai, tikrinant, ar gedimo atveju paslaugos persijungia į atsarginius komponentus be reikšmingos prastovos. |
| R4-TĘS-10-ACT1-S1 | 1 | Remiantis veiklos tęstinumo ir rizikos analize identifikuojamos esminės sistemos, kurioms reikia geografinės dubliacijos. |
| R4-TĘS-10-ACT1-S2 | 2 | Parengiama georedundancy strategija (on-prem antrinis DC (Domain Controller, domeno valdiklis), keli debesijos regionai, hibridiniai sprendimai) ir techninis dizainas. |
| R4-TĘS-10-ACT2-S1 | 1 | Įdiegiami georedundancy sprendimai (pvz., du duomenų centrai, multi-region cloud, duomenų replikacija) pagal parengtą strategiją. |
| R4-TĘS-10-ACT2-S2 | 2 | Organizuojami periodiniai georedundancy perjungimo (switchover / failover) testai, vertinant paslaugų prieinamumą ir poveikį naudotojams. |
| R4-TĘS-11-ACT1-S1 | 1 | Sudaryti metinį BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybų grafiką, nustatant, kurie scenarijai (IT (Information Technology, informacinės technologijos) gedimas, tiekėjo sutrikimas, regioninis incidentas) bus testuojami ir kada. |
| R4-TĘS-11-ACT1-S2 | 2 | Parengiami detalūs pratybų scenarijai, įskaitant tikslus, įsikišimo taškus, vertinimo kriterijus ir komunikacijos reikalavimus. |
| R4-TĘS-11-ACT2-S1 | 1 | Organizuojamos ir vykdomos BCP (Business Continuity Plan, verslo tęstinumo planas)/DRP (Disaster Recovery Plan, veiklos atkūrimo planas) pratybos pagal scenarijus, įtraukiant verslo, IT (Information Technology, informacinės technologijos), komunikacijos ir krizių valdymo komandas. |

| | | |
|---|---|---|
| R4-TĘS-11-ACT2-S2 | 2 | Po pratybų parengiamos pamokų analizės (lessons learned) ataskaitos, atnaujinami planai ir pratybų rezultatai integruojami į tobulinimo planus. |
| R5-TIEK-01-ACT1-S1 | 1 | Surinkti reikalavimus iš TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas), ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA) ir NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) gairių bei vidinių politikų (kibernetinio saugumo, rizikų valdymo, pirkimų) ir apibrėžti politikos taikymo sritį. |
| R5-TIEK-01-ACT1-S2 | 2 | Parengti politikos projektą, apibrėžiant tiekėjų klasifikavimą, atrankos ir vertinimo kriterijus, sutartinius reikalavimus, stebėseną ir nutraukimą. |
| R5-TIEK-01-ACT2-S1 | 1 | Politikos projektas derinamas su vadovybe ir pagrindiniais suinteresuotais padaliniais, integruojamos pastabos ir atliekami koregavimai. |
| R5-TIEK-01-ACT2-S2 | 2 | Politika oficialiai patvirtinama (pvz., vadovo įsakymu), paskelbiama vidinėje sistemoje ir pristatoma pirkimų, IT (Information Technology, informacinės technologijos) ir verslo komandoms. |
| R5-TIEK-02-ACT1-S1 | 1 | Identifikuoti tiekėjų kategorijas (IT (Information Technology, informacinės technologijos) paslaugos, SaaS, infrastruktūra, kritinės paslaugos) ir kiekvienai kategorijai nustatyti minimalų saugumo lygį. |
| R5-TIEK-02-ACT1-S2 | 2 | Parengti kibernetinio saugumo atrankos klausimyną ar kontrolinį sąrašą, kuris naudojamas vertinant potencialius tiekėjus. |
| R5-TIEK-02-ACT2-S1 | 1 | Atrankos kriterijai ir klausimynai integruojami į pirkimų procedūras, RFP (Request for Proposal, pasiūlymo pateikimo užklausa)/RFQ (Request for Quotation, komercinio pasiūlymo (kainos) užklausa) šablonus ir tiekėjų vertinimo formas. |
| R5-TIEK-02-ACT2-S2 | 2 | Pirkimų specialistams organizuojami trumpi mokymai, kaip taikyti kibernetinio saugumo kriterijus tiekėjų atrankoje. |
| R5-TIEK-03-ACT1-S1 | 1 | Analizuoti galiojančias sutartis ir identifikuoti trūkstamus ar nepakankamus kibernetinio saugumo reikalavimus. |
| R5-TIEK-03-ACT1-S2 | 2 | Parengti standartinių sutartinių sąlygų rinkinį (security appendix), įskaitant reikalavimus dėl ISMS (Information Security Management System, informacijos saugos valdymo sistema), incidentų pranešimo, auditų, subtiekėjų ir paslaugų nutraukimo. |
| R5-TIEK-03-ACT2-S1 | 1 | Atnaujinti sutartinių šablonų katalogą, įtraukiant standartinį saugumo priedą ir nuorodas į jį pirkimų procedūrose. |
| R5-TIEK-03-ACT2-S2 | 2 | Sudaryti planą, kaip palaipsniui peržiūrėti ir, esant galimybei, atnaujinti esamas sutartis, įtraukiant standartinius saugumo reikalavimus. |
| R5-TIEK-04-ACT1-S1 | 1 | Nustatyti incidentų tipus ir kritiškumo lygius, kurie privalo būti pranešti (pvz., duomenų nutekėjimas, paslaugų nepasiekiamumas, kompromitacija). |
| R5-TIEK-04-ACT1-S2 | 2 | Parengti standartinį incidento pranešimo šabloną tiekėjams (ką pateikti: laikas, apimtis, paveiktos paslaugos, taikytos priemonės). |
| R5-TIEK-04-ACT2-S1 | 1 | Atnaujinti sutartinius šablonus, įtraukiant incidentų pranešimo terminus, turinio reikalavimus ir komunikacijos kanalus. |
| R5-TIEK-04-ACT2-S2 | 2 | Incidentų valdymo plane numatyti atsakingi asmenys ir komunikacijos kanalai, per kuriuos tiekėjai teikia pranešimus, bei jų integracija į vidinį incidentų registrą. |
| R5-TIEK-05-ACT1-S1 | 1 | Nustatyti tiekėjų rizikos lygio ir kritiškumo kriterijus, nuo kurių priklauso auditavimo mastas ir dažnis. |
| R5-TIEK-05-ACT1-S2 | 2 | Parengti standartinius sutartinius punktus, suteikiančius organizacijai teisę audituoti tiekėją arba gauti nepriklausomą audito ataskaitą (pvz., ISO (International Organization for Standardization, Tarptautinė standartizacijos organizacija (ISO)) 27001, SOC (Security Operations Center, saugumo operacijų centras) 2). |

| | | |
|---|---|---|
| R5-TIEK-05-ACT2-S1 | 1 | Sudaryti metinį kritinių tiekėjų auditavimo grafiką, įskaitant vietoje atliekamus auditus, nuotolinius vertinimus ar trečiųjų šalių ataskaitų peržiūras. |
| R5-TIEK-05-ACT2-S2 | 2 | Įdiegti procesą, kaip fiksuojami audito rezultatai, nustatomos korekcinės priemonės tiekėjui ir sekamas jų įgyvendinimas. |
| R5-TIEK-06-ACT1-S1 | 1 | Nustatyti kritiškumo kriterijus (pvz., poveikis esminėms paslaugoms, duomenų jautrumas, rinkoje neturimi alternatyvūs tiekėjai). |
| R5-TIEK-06-ACT1-S2 | 2 | Parengti kritinių tiekėjų registro struktūrą (tiekėjas, paslaugos aprašymas, kritiškumo lygis, sutarties duomenys, atsakingas savininkas). |
| R5-TIEK-06-ACT2-S1 | 1 | Surinkti informaciją apie esamus tiekėjus, taikant kritiškumo kriterijus ir užpildyti registrą pradiniu duomenų rinkiniu. |
| R5-TIEK-06-ACT2-S2 | 2 | Nustatyti registro peržiūros periodiškumą (pvz., kas ketvirtį) ir atsakingus asmenis, kurie atnaujina informaciją apie tiekėjus ir paslaugas. |
| R5-TIEK-07-ACT1-S1 | 1 | Nustatyti rizikos veiksnius (pvz., paslaugos kritiškumas, duomenų tipai, tiekėjo brandos lygis, geografinė vieta) ir jų svorius. |
| R5-TIEK-07-ACT1-S2 | 2 | Parengti tiekėjų rizikos vertinimo metodikos dokumentą ir scoring lenteles (žemas / vidutinis / aukštas rizikos lygis). |
| R5-TIEK-07-ACT2-S1 | 1 | Surinkti duomenis apie kritinius tiekėjus (klausimynai, auditų rezultatai, sertifikatai, vieša informacija) ir taikyti scoring metodiką. |
| R5-TIEK-07-ACT2-S2 | 2 | Rizikos vertinimo rezultatus įrašyti į centralizuotą rizikų registrą ir parengti prioritetinių rizikos mažinimo priemonių sąrašą. |
| R5-TIEK-08-ACT1-S1 | 1 | Identifikuoti pagrindinius šaltinius (Europos Komisija, ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA), nacionalinės CSIRT (Computer Security Incident Response Team, kompiuterių saugos incidentų reagavimo komanda)/NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)), sektoriaus priežiūros institucijos), kuriuose skelbiami tiekimo grandinės rizikos vertinimai. |
| R5-TIEK-08-ACT1-S2 | 2 | Nustatyti periodiškumą (pvz., kas ketvirtį) ir formatą, kuriuo atsakinga funkcija apibendrina naujausius vertinimus ir rekomendacijas. |
| R5-TIEK-08-ACT2-S1 | 1 | Periodinių suvestinių pagrindu peržiūrėti tiekėjų atrankos kriterijus, rizikos scoring metodiką ir sutartinius reikalavimus, identifikuojant, ar reikia papildomų apribojimų ar sąlygų. |
| R5-TIEK-08-ACT2-S2 | 2 | Kritiškiems tiekėjams, kuriuos tiesiogiai paliečia ES (Elasticsearch, „Elasticsearch“ paieškos ir analizės variklis) rizikos vertinimų išvados (pvz., kritinės infrastruktūros įrangos ar debesijos tiekėjai), atlikti papildomą tikslingą rizikos vertinimą ar peržiūrą. |
| R5-TIEK-09-ACT1-S1 | 1 | Atlikti TPRM (Third-Party Risk Management, trečiųjų šalių rizikos valdymas) sprendimų rinkos analizę, įvertinant funkcionalumą (klausimynai, workflow, scoring), integracijų galimybes ir kainą. |
| R5-TIEK-09-ACT1-S2 | 2 | Įdiegti pasirinktą platformą (on-prem ar SaaS), sukonfigūruojant naudotojų prieigos lygius, tiekėjų katalogą ir bazinius workflow. |
| R5-TIEK-09-ACT2-S1 | 1 | Sukonfigūruoti tiekėjų klausimynus, scoring taisykles ir rizikos lygių ribas pagal patvirtintą metodiką. |

| | | |
|---|---|---|
| R5-TIEK-09-ACT2-S2 | 2 | Sukonfigūruoti integracijas su pirkimų sistemomis ar GRC (Governance, Risk and Compliance, valdymo, rizikos ir atitikties (GRC) modelis) įrankiais, kad tiekėjų rizikos duomenys būtų matomi perkančiosioms ir rizikų valdymo funkcijoms. |
| R6-PLĖ-01-ACT1-S1 | 1 | Identifikuoti sistemas ir paslaugas (vidines ir išorines), kurioms privalomai taikoma saugaus įsigijimo ir plėtros politika (pvz., esminės ir svarbios paslaugos pagal TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))). |
| R6-PLĖ-01-ACT1-S2 | 2 | Sukonkretinti saugumo principus (pvz., security by design, default secure configuration, least privilege, tiekimo grandinės sauga), kurie turi būti taikomi visuose įsigijimo ir plėtros etapuose. |
| R6-PLĖ-01-ACT2-S1 | 1 | Parengti politikos dokumento projektą, apimantį reikalavimus dėl saugumo įsigyjant sistemas, vykdant plėtrą, įdiegiant pokyčius ir atliekant priežiūrą. |
| R6-PLĖ-01-ACT2-S2 | 2 | Suderinti politikos projektą su vadovybe ir pagrindiniais padaliniais, integruojant pastabas ir išlaikant balansą tarp saugumo ir verslo poreikių. |
| R6-PLĖ-01-ACT3-S1 | 1 | Politiką patvirtina vadovybė, ji registruojama dokumentų valdymo sistemoje ir įtraukiama į projektų bei pirkimų metodikas kaip privaloma nuoroda. |
| R6-PLĖ-02-ACT1-S1 | 1 | Remiantis pramonės praktikomis (pvz., Microsoft SDL (Security Development Lifecycle, saugos vystymo gyvavimo ciklas), OWASP (Open Worldwide Application Security Project, OWASP atvirasis programų saugumo projektas) SAMM (Software Assurance Maturity Model, programų saugumo brandos modelis SAMM)) apibrėžti, kokios saugumo veiklos atliekamos planavimo, dizaino, kūrimo, testavimo ir eksploatacijos etapuose. |
| R6-PLĖ-02-ACT2-S1 | 1 | Sukonfigūruoti statinės kodo analizės (SAST (Static Application Security Testing, statinis programų saugumo testavimas)) įrankius, integruojant juos į kodo saugyklas ir CI (Continuous Integration, nuolatinio integravimo praktika)/CD (Compact Disc, kompaktinis diskas) pipeline'us. |
| R6-PLĖ-02-ACT2-S2 | 2 | Įdiegti atvirojo kodo ir trečiųjų šalių priklausomybių (SCA (Software Composition Analysis, programinės įrangos komponentų analizė)) skenavimą, kad būtų identifikuojamos žinomos pažeidžiamos bibliotekos. |
| R6-PLĖ-02-ACT2-S3 | 3 | Kritinėms internetu pasiekiamoms sistemoms įdiegti dinaminio testavimo (DAST (Dynamic Application Security Testing, dinaminis programų saugumo testavimas)) ar interaktyvaus testavimo (IAST (Interactive Application Security Testing, interaktyvus programų saugumo testavimas)) sprendimus, vykdomus testinėje aplinkoje. |
| R6-PLĖ-02-ACT3-S1 | 1 | Sutarti dėl minimalios priimtinos saugumo kokybės (pvz., kritinių pažeidžiamumų negali būti, aukštų – ne daugiau nei nustatytas skaičius) ir įtraukti tai į release vartų kriterijus. |
| R6-PLĖ-02-ACT3-S2 | 2 | Organizuoti tikslinius mokymus kūrėjams, testuotojams ir produktų savininkams apie saugaus SDLC (Software Development Lifecycle, programinės įrangos kūrimo gyvavimo ciklas) praktiką ir naujai įdiegtus įrankius. |

| | | |
|---|---|---|
| R6-PLĖ-03-ACT1-S1 | 1 | Apibrėžti pokyčių tipus (standartiniai, normalūs, skubūs) ir jų apdorojimo seką (registravimas, vertinimas, tvirtinimas, testavimas, diegimas, post-implementation peržiūra). |
| R6-PLĖ-03-ACT1-S2 | 2 | Į procesą įtraukti privalomą saugumo impact vertinimą kritiniams pokyčiams (pvz., konfigūracijos keitimai, naujų komponentų diegimas). |
| R6-PLĖ-03-ACT2-S1 | 1 | Sukonfigūruoti ITSM (IT Service Management, IT paslaugų valdymas) įrankį (pvz., ServiceNow, JIRA (Jira, „Jira“ projektų ir užduočių valdymo sistema) Service Management, BMC (BMC Software, BMC IT (Information Technology, informacinės technologijos) paslaugų valdymo ir stebėsenos sprendimai) Remedy), kad visi pokyčiai būtų registruojami, tvirtinami ir audituojami pagal aprašytą procesą. |
| R6-PLĖ-04-ACT1-S1 | 1 | Nustatyti ir dokumentuoti aplinkų modelį (development, test, staging, production) bei duomenų naudojimo taisykles (pvz., pseudonimizuoti produkcijos duomenys testavimui). |
| R6-PLĖ-04-ACT1-S2 | 2 | Užtikrinti, kad kritinėms sistemoms egzistuoja atskiros testavimo aplinkos ir jos techniškai atskirtos nuo produkcijos (tinklo ir prieigos kontrole). |
| R6-PLĖ-04-ACT2-S1 | 1 | Papildyti change valdymo formą privalomais laukais apie atliktą testavimą (aplinka, scenarijai, rezultatai) ir atsakingų asmenų patvirtinimus. |
| R6-PLĖ-04-ACT2-S2 | 2 | Nustatyti kriterijus, kada pokytis gali būti išimtinai diegiamas be pilno testavimo (pvz., kritinis pataisymas), ir sugriežtinti tokių išimčių tvirtinimo tvarką. |
| R6-PLĖ-05-ACT1-S1 | 1 | Nustatyti, kokius turto ir programinės įrangos tipus inventorius apims (serveriai, darbo stotys, tinklo įranga, aplikacijos, duomenų bazės, SaaS paslaugos). |
| R6-PLĖ-05-ACT1-S2 | 2 | Nuspręsti, kokie duomenų laukai privalomi kiekvienam objektui (pvz., savininkas, vieta, OS (Operating System, operacinė sistema) versija, aplikacijos versija, tiekėjas, palaikymo sutartis). |
| R6-PLĖ-05-ACT1-S3 | 3 | Paskirti atsakingus savininkus už turto ir programinės įrangos įrašų tikslumą (pvz., pagal sistemas ar paslaugas). |
| R6-PLĖ-05-ACT2-S1 | 1 | Pasirinkti inventoriaus/CMDB (Configuration Management Database, konfigūracijų valdymo duomenų bazė) sprendimą (pvz., ServiceNow CMDB, Lansweeper, GLPI (Gestionnaire Libre de Parc Informatique, GLPI atvirojo kodo IT (Information Technology, informacinės technologijos) turto ir paslaugų valdymo sistema)) ir sukonfigūruoti jį pagal nustatytą duomenų modelį. |
| R6-PLĖ-05-ACT2-S2 | 2 | Sukonfigūruoti automatizuotą turto aptikimą (discovery) ir periodinį duomenų sulyginimą su realia infrastruktūra. |
| R6-PLĖ-06-ACT1-S1 | 1 | Apibrėžti pataisų kategorijas (OS (Operating System, operacinė sistema), programinės įrangos, firmware, trečiųjų šalių produktų) ir kritiškumo lygius (kritinės, aukštos, vidutinės, žemos). |
| R6-PLĖ-06-ACT1-S2 | 2 | Nustatyti terminus, per kuriuos skirtingo kritiškumo pataisos turi būti įdiegtos (pvz., kritinės per 7 dienas, aukštos per 30 dienų ir pan.). |
| R6-PLĖ-06-ACT2-S1 | 1 | Aprašyti veiksmų seką: informacijos apie naujas pataisas gavimas, įtakos vertinimas, testavimas, diegimo planavimas ir vykdymas, post-patch stebėsena. |

| | | |
|---|---|---|
| R6-PLĖ-06-ACT2-S2 | 2 | Nustatyti išimčių tvarką, kai pataisos negali būti įdiegtos per nustatytą laiką (kompensacinės priemonės, vadovybės patvirtinimas). |
| R6-PLĖ-06-ACT3-S1 | 1 | Pasirinkti ir įdiegti pataisų valdymo įrankius (pvz., Microsoft WSUS (Windows Server Update Services, „Windows Server Update Services“ atnaujinimų platinimo sistema)/SCCM (System Center Configuration Manager, „System Center Configuration Manager“ sistema), Linux repo valdymas, trečiųjų šalių patch management sprendimai) ir sukonfigūruoti automatizuotus diegimo langus. |
| R6-PLĖ-07-ACT1-S1 | 1 | Pagal kritinių sistemų sąrašą ir IT (Information Technology, informacinės technologijos) turto inventorių nustatyti, kokiems serveriams, darbo stotims, aplikacijoms ir tinklo įrangai privaloma taikyti kritinių pataisų SLA (Service Level Agreement, paslaugų lygio sutartis). |
| R6-PLĖ-07-ACT2-S1 | 1 | Sukonfigūruoti pataisų valdymo įrankius taip, kad būtų galima matuoti laiką nuo pataisos išleidimo iki jos įdiegimo kiekviename kritiniame objekte. |
| R6-PLĖ-07-ACT2-S2 | 2 | Reguliariai (pvz., kas mėnesį) peržiūrėti ataskaitas ir eskaluoti atvejus, kai kritinės pataisos neįdiegtos per nustatytą SLA (Service Level Agreement, paslaugų lygio sutartis). |
| R6-PLĖ-08-ACT1-S1 | 1 | Įvertinti komercinius ir atviro kodo skanerius ir pasirinkti sprendimus infrastruktūrai (network/host) ir aplikacijoms. |
| R6-PLĖ-08-ACT1-S2 | 2 | Sudaryti skanavimo planą (dažnis, laiko langai, prioritetiniai segmentai) ir nustatyti, kurios sistemos skenuojamos automatizuotai. |
| R6-PLĖ-08-ACT2-S1 | 1 | Sukurti procesą, kaip skanavimo rezultatai perkeliami į pataisų valdymo ir rizikos registrus (pvz., automatinis ticket'ų generavimas kritinėms spragoms). |
| R6-PLĖ-08-ACT2-S2 | 2 | Nustatyti minimalias atitikties ribas (pvz., % pataisytų kritinių spragų per nustatytą laiką) ir reguliariai teikti suvestines vadovybei. |
| R6-PLĖ-09-ACT1-S1 | 1 | Parengti politikos projektą, apimantį kontaktinius kanalus (pvz., security@…), priimtiną testavimo elgseną ir išskirtas draudžiamas veiklas (pvz., duomenų eksfiltracija). |
| R6-PLĖ-09-ACT1-S2 | 2 | Suderinti politiką su teisės ir atitikties funkcijomis, įvertinant potencialius teisinius ir reputacinius aspektus. |
| R6-PLĖ-09-ACT2-S1 | 1 | Paskelbti politiką viešai (pvz., organizacijos tinklalapio security puslapyje, security.txt faile) ir užtikrinti, kad kanalai realiai veiktų. |
| R6-PLĖ-09-ACT2-S2 | 2 | Sukurti vidinę procedūrą, kaip gauti pranešimai registruojami, vertinami, prioritetizuojami ir susiejami su pataisų bei incidentų valdymu. |
| R6-PLĖ-10-ACT1-S1 | 1 | Parengti programinės įrangos valdymo politiką, apibrėžiančią leidžiamus programinės įrangos šaltinius, pirkimų kanalus ir diegimo tvarką. |
| R6-PLĖ-10-ACT1-S2 | 2 | Sukonfigūruoti techninius mechanizmus, ribojančius neautorizuotos programinės įrangos diegimą (pvz., administratoriaus teisės, application whitelisting). |
| R6-PLĖ-10-ACT1-S3 | 3 | Reguliariai atlikti licencijų ir naudojamos programinės įrangos auditus, lyginant inventorių su licencijų sutartimis ir taikant korekcines priemones. |

| | | |
|---|---|---|
| R7-ATIT-01-ACT1-S1 | 1 | Parengti vidaus audito programą, apimančią TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) reikalavimus, vidines politikas (saugumo, rizikų, tiekimo grandinės, incidentų valdymo, BCP (Business Continuity Plan, verslo tęstinumo planas)) ir pagrindinius procesus. |
| R7-ATIT-01-ACT1-S2 | 2 | Pasirinkti audito metodiką (pvz., ISO (International Organization for Standardization, Tarptautinė standartizacijos organizacija (ISO)) 19011 pagrindu) ir apibrėžti vertinimo kriterijus bei įrodymų rinkimo būdus (interviu, dokumentų analizė, testavimas). |
| R7-ATIT-01-ACT2-S1 | 1 | Parengti metinį vidaus audito planą, įtraukiant kibernetinio saugumo auditą ir jo apimtį, suderinti su vadovybe. |
| R7-ATIT-01-ACT2-S2 | 2 | Atlikti auditą pagal patvirtintą programą, dokumentuoti išvadas ir parengti audito ataskaitą su identifikuotomis stiprybėmis ir trūkumais. |
| R7-ATIT-02-ACT1-S1 | 1 | Sukurti centralizuotą neatitikčių registrą, kuriame fiksuojamos vidinių ir išorinių auditų išvados, kritiškumas ir atsakingi asmenys. |
| R7-ATIT-02-ACT1-S2 | 2 | Apibrėžti korekcinių veiksmų planavimo principus: terminais, prioritetais, atsakomybėmis ir būtinomis priemonėmis kiekvienai neatitikčiai. |
| R7-ATIT-02-ACT2-S1 | 1 | Nustatyti periodinius peržiūros susitikimus, kurių metu atsakingi asmenys pateikia informaciją apie korekcinių veiksmų įgyvendinimo progresą. |
| R7-ATIT-02-ACT2-S2 | 2 | Parengti periodines suvestines vadovybei apie pagrindines neatitiktis, jų kritiškumą ir įgyvendinimo progresą. |
| R7-ATIT-03-ACT1-S1 | 1 | Identifikuoti kritines internetu pasiekiamas sistemas ir paslaugas, kurioms būtinas periodinis penetracijos testavimas. |
| R7-ATIT-03-ACT1-S2 | 2 | Nustatyti pen-testų tipą, periodiškumą (pvz., kartą per metus ar po esminių pokyčių) ir minimalų apimtį (testo scenarijus, OWASP (Open Worldwide Application Security Project, OWASP atvirasis programų saugumo projektas) TOP 10 ir pan.). |
| R7-ATIT-03-ACT2-S1 | 1 | Pasirinkti sertifikuotus tiekėjus (pvz., CREST (Council of Registered Ethical Security Testers, tarptautinė sertifikuotų saugumo testuotojų organizacija), OSCP (Offensive Security Certified Professional, Offensive Security sertifikuotas profesionalas (OSCP)) sertifikuotas personalas), numatyti SOW (Statement of Work, darbo apimties aprašas (SOW)) ir ribines sąlygas (scope, laikotarpis, legalūs testai). |
| R7-ATIT-03-ACT2-S2 | 2 | Suplanuoti ir atlikti penetracijos testus, užtikrinant, kad ataskaitose būtų aiškiai nurodytos spragos, jų kritiškumas ir rekomenduojamos priemonės. |
| R7-ATIT-03-ACT3-S1 | 1 | Rastas spragas registruoti pažeidžiamumų ir pataisų valdymo sistemose, nustatyti prioritetus ir stebėti jų pašalinimo progresą. |
| R7-ATIT-04-ACT1-S1 | 1 | Identifikuoti pagrindines saugumo sritis (incidentai, pažeidžiamumai, pataisos, tiekėjų rizika, mokymai, atsarginės kopijos) ir kiekvienai priskirti matuojamus rodiklius. |
| R7-ATIT-04-ACT1-S2 | 2 | Kiekvienam rodikliui aprašyti formulę, duomenų šaltinius, matavimo dažnį ir atsakingus už duomenų pateikimą. |
| R7-ATIT-04-ACT1-S3 | 3 | Sutarti su vadovybe dėl tikslinių reikšmių ir įspėjimo ribų (thresholds), kurios signalizuoja apie padidėjusią riziką ar nepakankamą veiksmingumą. |
| R7-ATIT-04-ACT2-S1 | 1 | Pasirinkti ataskaitų ir vizualizavimo įrankius (pvz., Power BI (Business Intelligence, verslo analitika), Tableau, GRC (Governance, Risk and Compliance, valdymo, rizikos ir atitikties (GRC) modelis) platformos skydeliai) ir sukurti kibernetinio saugumo KPI (Key Performance Indicator, pagrindinis veiklos rodiklis)/KRI (Key Risk Indicator, pagrindinis rizikos rodiklis) dashboard'ą. |

| | | |
|---|---|---|
| R7-ATIT-04-ACT2-S2 | 2 | Nustatyti periodinį (pvz., mėnesinį ar ketvirtinį) rodiklių peržiūros ritmą ir atsakingus asmenis, kurie iš jų daro išvadas ir siūlo korekcinius veiksmus. |
| R7-ATIT-05-ACT1-S1 | 1 | Inventorizuoti esamus kibernetinio saugumo dokumentus (politikos, procedūros, rizikos vertinimai, incidentų ataskaitos, auditų ataskaitos, mokymų įrašai ir pan.). |
| R7-ATIT-05-ACT1-S2 | 2 | Sukonstruoti logišką dokumentų struktūrą (pvz., pagal temas ar reikalavimų blokus) ir aprašyti, kur ir kaip dokumentai saugomi (DMS (Document Management System, dokumentų valdymo sistema), SharePoint, GRC (Governance, Risk and Compliance, valdymo, rizikos ir atitikties (GRC) modelis)). |
| R7-ATIT-05-ACT2-S1 | 1 | Priskirti dokumentų savininkus, atsakingus už periodinį (pvz., kartą per metus) dokumentų peržiūrėjimą ir atnaujinimą. |
| R7-ATIT-05-ACT2-S2 | 2 | Sukurti procedūrą, kaip reikalavimų atveju (pvz., NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcija, išorinis auditas) greitai surenkami ir perduodami reikiami dokumentai. |
| R7-ATIT-06-ACT1-S1 | 1 | Peržiūrėti NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) skelbiamas patikrinimų gaires, kontrolinius sąrašus ir, jei įmanoma, ankstesnių inspekcijų patirtį sektoriuje. |
| R7-ATIT-06-ACT2-S1 | 1 | Sudaryti NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijos pasirengimo kontrolinį sąrašą (dokumentai, įrašai, atsakingi asmenys, kontaktai, infrastruktūros aprašai). |
| R7-ATIT-06-ACT2-S2 | 2 | Organizuoti vidinę „bandomąją“ inspekciją, kurioje imituojami NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) klausimai ir vertinimas, fiksuojamos spragos pasirengime. |
| R7-ATIT-06-ACT2-S3 | 3 | Parengti veiksmų planą NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) inspekcijos pasirengimo spragoms pašalinti ir priskirti terminus bei atsakomybę. |
| R7-ATIT-07-ACT1-S1 | 1 | Identifikuoti pagrindinius šaltinius (Seimas, Vyriausybė, NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)), ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA), sektoriaus priežiūros institucijos) ir užsiprenumeruoti naujienas apie TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) įgyvendinimą. |
| R7-ATIT-07-ACT1-S2 | 2 | Aprašyti, kaip reguliariai (pvz., kartą per ketvirtį) rengiamos santraukos apie pasikeitusius terminus, inspekcijų tvarkas ir naujas gaires. |
| R7-ATIT-07-ACT2-S1 | 1 | Parengti informacinius pranešimus ar pristatymus vadovybei ir pagrindiniams padaliniams apie TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) įgyvendinimo terminus ir priežiūros institucijų rolę. |
| R7-ATIT-07-ACT2-S2 | 2 | Suderinti vidinius TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2)) įgyvendinimo planus ir projektų terminus su teisės aktuose ir gairėse nurodytais galutiniais terminais. |

| | | |
|---|---|---|
| R7-POL-03-ACT1-S1 | 1 | Identifikuoti pagrindines priemonių grupes (organizacinės, techninės, tiekimo grandinės, incidentų valdymo, BCP (Business Continuity Plan, verslo tęstinumo planas), mokymai) ir numatyti joms vertinimo metodus (auditai, testai, pratybos, KPI (Key Performance Indicator, pagrindinis veiklos rodiklis)). |
| R7-POL-03-ACT1-S2 | 2 | Nustatyti veiksmingumo kriterijus (pvz., incidentų skaičiaus mažėjimas, laiko iki pataisymo sutrumpėjimas, auditų neatitikčių mažėjimas). |
| R7-POL-03-ACT1-S3 | 3 | Suderinti veiksmingumo vertinimo principus su vadovybe, kad jie atitiktų organizacijos rizikos apetitą ir strateginius tikslus. |
| R7-POL-03-ACT2-S1 | 1 | Parengti politikos dokumentą, integruojant auditus, pen-testus, KPI (Key Performance Indicator, pagrindinis veiklos rodiklis)/KRI (Key Risk Indicator, pagrindinis rizikos rodiklis), pratybas ir kitus vertinimo mechanizmus į vieną nuoseklią schemą. |
| R7-POL-03-ACT2-S2 | 2 | Suderinti ir patvirtinti politiką vadovybės lygiu ir paskelbti ją kaip privalomą kibernetinio saugumo valdymo dalį. |
| R7-POL-04-ACT1-S1 | 1 | Surinkti informaciją apie visas planuojamas vertinimo veiklas (vidiniai auditai, išoriniai auditai, pen-testai, BCP (Business Continuity Plan, verslo tęstinumo planas) pratybos, incidentų pratybos, KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) peržiūros) ir jų dabartinį dažnį. |
| R7-POL-04-ACT1-S2 | 2 | Sudaryti metinį/2–3 metų iš anksto planuojamą vertinimo veiklų kalendorių, atsižvelgiant į TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) reikalavimus ir resursų galimybes. |
| R7-POL-04-ACT2-S1 | 1 | Atnaujinti priemonių veiksmingumo vertinimo politiką ir susijusius procesų aprašus, įtraukiant aiškų minimalų auditų, testavimų ir pratybų periodiškumą pagal rizikos lygį. |
| R8-MOK-01-ACT1-S1 | 1 | Identifikuoti darbuotojų grupes (pvz., visi darbuotojai, IT (Information Technology, informacinės technologijos) personalas, vadovybė, trečiųjų šalių atstovai) ir jų specifinius mokymų poreikius. |
| R8-MOK-01-ACT1-S2 | 2 | Atsižvelgiant į TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) reikalavimus ir ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA)/NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) rekomendacijas, sudaryti bazinį temų sąrašą (phishing, slaptažodžiai, darbo nuotoliniu būdu, incidentų pranešimas ir pan.). |
| R8-MOK-01-ACT1-S3 | 3 | Nustatyti mokymų tikslus (pvz., darbuotojų žinomumo didinimas, klaidų mažinimas) ir atitinkamus rodiklius (testų rezultatai, incidentų skaičius). |
| R8-MOK-01-ACT2-S1 | 1 | Parengti mokymų politikos dokumentą, kuriame aprašomos tikslinės grupės, temos, periodiškumas, atsakomybės ir įrodymų (registrų) tvarkymas. |
| R8-MOK-01-ACT2-S2 | 2 | Suderinti ir patvirtinti politiką vadovybės lygiu, įtraukti ją į organizacijos politikų rinkinį ir paskelbti darbuotojams. |
| R8-MOK-02-ACT1-S1 | 1 | Atnaujinti įdarbinimo/onboarding'o procedūras, numatant, kad kibernetinio saugumo mokymai turi būti atlikti per pirmąsias darbo savaites. |
| R8-MOK-02-ACT1-S2 | 2 | Aprašyti aiškius terminus (pvz., mokymai atlikti per 30 dienų nuo darbo pradžios) ir pasekmes, jei mokymai neįvykdomi laiku. |
| R8-MOK-02-ACT2-S1 | 1 | Pasirinkti mokymų formatą (e-learning platforma, kontaktinės sesijos) ir įrankius (pvz., LMS (Learning Management System, mokymų valdymo sistema): Moodle, SAP (Systems, Applications and Products in Data Processing, SAP verslo valdymo (ERP) platforma) SuccessFactors, Udemy for Business). |
| R8-MOK-02-ACT2-S2 | 2 | Sukurti ataskaitas ir priminimus, rodančius, kurie nauji darbuotojai dar neatliko įvadinių mokymų per nustatytą laiką. |

| | | |
|---|---|---|
| R8-MOK-03-ACT1-S1 | 1 | Atnaujinti mokymų politiką ir procedūras, įrašant reikalavimą visiems darbuotojams kartoti kibernetinio saugumo mokymus ne rečiau kaip kartą per metus. |
| R8-MOK-03-ACT1-S2 | 2 | Nustatyti, kaip tvarkoma išimčių tvarka (pvz., ilgalaikės atostogos) ir kaip persikelia reikalavimai grįžus į darbą. |
| R8-MOK-03-ACT2-S1 | 1 | Sukurti metinį mokymų kalendorių ir priskirti mokymų bangas (batch'us) skirtingoms darbuotojų grupėms, kad būtų išlyginta darbo apkrova. |
| R8-MOK-03-ACT2-S2 | 2 | Sukurti ataskaitas ir KPI (Key Performance Indicator, pagrindinis veiklos rodiklis) (pvz., % darbuotojų, kurie per paskutinius 12 mėnesių atliko mokymus) ir reguliariai teikti suvestines vadovybei. |
| R8-MOK-04-ACT1-S1 | 1 | Nustatyti pagrindines kampanijų temas (pvz., slaptažodžių higiena, socialinė inžinerija, saugus darbas nuotoliniu būdu, mobilių įrenginių sauga). |
| R8-MOK-04-ACT1-S2 | 2 | Nuspręsti kampanijų formatus (plakatai, intraneto naujienos, trumpi video, žinių viktorinos) ir periodiškumą (pvz., 1–2 kampanijos per ketvirtį). |
| R8-MOK-04-ACT2-S1 | 1 | Parengti ir išsiųsti komunikacines medžiagas per pasirinktas priemones (el. paštas, intranetas, Teams/Slack žinutės, plakatas biure). |
| R8-MOK-04-ACT2-S2 | 2 | Matuoti kampanijų pasiekiamumą (pvz., atidarymo rodiklius, intraneto peržiūras, viktorinų rezultatus) ir prireikus koreguoti temas ar formatus. |
| R8-MOK-05-ACT1-S1 | 1 | Nustatyti simuliacijų dažnį (pvz., kas 1–3 mėn.), apimtį (visiems darbuotojams ar tik atrinktoms grupėms) ir scenarijų sudėtingumo lygius. |
| R8-MOK-05-ACT1-S2 | 2 | Apibrėžti elgesio po simuliacijos taisykles (pvz., kaip informuojami nesėkmingai sureagavę darbuotojai, kaip suteikiami papildomi mokymai). |
| R8-MOK-05-ACT2-S1 | 1 | Pasirinkti phishing simuliacijų įrankį (pvz., KnowBe4, Cofense, Microsoft Attack Simulator) ir jį suintegruoti su el. pašto sistema. |
| R8-MOK-05-ACT2-S2 | 2 | Reguliariai vykdyti simuliacijas ir rengti ataskaitas apie paspaudimo, prisijungimo duomenų suvedimo rodiklius ir tendencijas, dalintis jomis su vadovybe. |
| R8-MOK-06-ACT1-S1 | 1 | Identifikuoti patikimus grėsmių informacijos šaltinius (NKSC (Nacionalinis kibernetinio saugumo centras (NKSC)) pranešimai, ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA) įspėjimai, CSIRT (Computer Security Incident Response Team, kompiuterių saugos incidentų reagavimo komanda), tiekėjų bullet'inai) ir užtikrinti jų prenumeratą. |
| R8-MOK-06-ACT1-S2 | 2 | Aprašyti, kaip vertinama gauta informacija (aktualumas, poveikis organizacijai) ir kada nusprendžiama ją komunikuoti darbuotojams. |
| R8-MOK-06-ACT2-S1 | 1 | Pasirinkti komunikacijos kanalus (el. paštas, intraneto naujienos, Teams/Slack kanalai) ir sukurti standartizuotą „grėsmių įspėjimo“ žinutės šabloną. |
| R8-MOK-06-ACT2-S2 | 2 | Nustatyti minimalų periodiškumą (pvz., mėnesinis „threat digest“) ir ad hoc įspėjimus kritinių grėsmių atveju, matuoti atidarymus ir reakcijas. |
| R9-KRIP-01-ACT1-S1 | 1 | Identifikuoti duomenų tipus ir sritis, kuriose būtina kriptografija (pvz., klientų duomenys, autentifikavimo duomenys, atsarginės kopijos, tarpduomenų srautai). |
| R9-KRIP-01-ACT1-S2 | 2 | Peržiūrėti taikomus teisės aktus ir standartus (TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas), BDAR (Bendrasis duomenų apsaugos reglamentas), ISO (International Organization for Standardization, Tarptautinė standartizacijos organizacija (ISO)) 27001/27002, ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA) rekomendacijas) ir išskirti reikalavimus kriptografijai. |
| R9-KRIP-01-ACT1-S3 | 3 | Aprašyti aukšto lygio kriptografijos valdymo tikslus (konfidencialumas, vientisumas, prieinamumas, neatskleidimas) ir rizikos toleranciją (pvz., draudžiamus algoritmus). |

| | | |
|---|---|---|
| R9-KRIP-01-ACT2-S1 | 1 | Parengti kriptografijos politikos projektą, aprašantį taikymo sritis, atsakomybes, sprendimų priėmimo principus ir sąsają su kitomis politikomis (IT (Information Technology, informacinės technologijos), duomenų apsaugos, BCP (Business Continuity Plan, verslo tęstinumo planas)). |
| R9-KRIP-01-ACT2-S2 | 2 | Suderinti ir patvirtinti politiką vadovybės lygiu, paskelbti ją darbuotojams ir numatyti periodinio peržiūrėjimo (pvz., kas 2 metus) tvarką. |
| R9-KRIP-02-ACT1-S1 | 1 | Remiantis ENISA (European Union Agency for Cybersecurity, Europos Sąjungos kibernetinio saugumo agentūra ENISA), NIST (National Institute of Standards and Technology, JAV Nacionalinis standartų ir technologijų institutas (NIST)), vendor'ų rekomendacijomis ir TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas) reikalavimais, sudaryti leistinų algoritmų, raktų ilgių ir protokolų sąrašą (pvz., TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) 1.2/1.3, AES-256 (Advanced Encryption Standard 256-bit, 256 bitų ilgio AES simetrinio šifravimo standartas), RSA (Rivest–Shamir–Adleman, asimetriškas šifravimo algoritmas RSA) ≥ 2048 bitų, draudžiant TLS 1.0/1.1, SHA-1 (Secure Hash Algorithm 1, kriptografinė maišos funkcija SHA-1)). |
| R9-KRIP-02-ACT1-S2 | 2 | Susieti algoritmų/protokolų sąrašą su duomenų kategorijomis ir sistemomis (pvz., kokie TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS)/cipher suite reikalavimai taikomi viešoms svetainėms, VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), duomenų bazėms). |
| R9-KRIP-02-ACT2-S1 | 1 | Atnaujinti technines specifikacijas ir architektūrinius šablonus (pvz., API (Application Programming Interface, programavimo sąsaja tarp sistemų ar komponentų) gateway, web serverių, duomenų bazių konfigūraciją), įrašant privalomus kriptografijos parametrus. |
| R9-KRIP-02-ACT2-S2 | 2 | Įtraukti algoritmų/protokolų patikrą į konfigūracijų ir pažeidžiamumų skenavimą (pvz., SSL (Secure Sockets Layer, SSL ryšio šifravimo protokolas) Labs, Nessus, Qualys) ir nustatyti neatitikimų šalinimo tvarką. |
| R9-KRIP-03-ACT1-S1 | 1 | Identifikuoti raktų tipus (TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) sertifikatų raktai, duomenų bazės raktai, diskų šifravimo raktai, HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) raktai) ir sudaryti jų registrą. |
| R9-KRIP-03-ACT1-S2 | 2 | Priskirti raktų valdymo rolę (Key Management Owner) ir aprašyti atsakomybes: raktų registras, rotacijos stebėsena, incidentų valdymas dėl raktų nutekėjimo. |
| R9-KRIP-03-ACT2-S1 | 1 | Aprašyti raktų generavimo, paskirstymo, saugojimo, rotacijos ir sunaikinimo taisykles, įskaitant minimalius raktų ilgius ir galiojimo trukmę. |
| R9-KRIP-03-ACT2-S2 | 2 | Pasirinkti ir įdiegti raktų valdymo technologijas (pvz., AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) KMS (Key Management Service, kriptografinių raktų valdymo paslauga), Azure Key Vault, GCP (Google Cloud Platform, „Google Cloud“ debesų kompiuterijos platforma) KMS, HashiCorp Vault), užtikrinant centralizuotą raktų saugojimą ir prieigos kontrolę. |
| R9-KRIP-03-ACT2-S3 | 3 | Nustatyti automatizuotą raktų rotaciją ir expiracijos stebėseną, kad pasibaigęs ar kompromituotas raktas būtų laiku pakeistas. |
| R9-KRIP-04-ACT1-S1 | 1 | Parengti duomenų srautų žemėlapį (tinklų diagramas), identifikuojant srautus tarp naudotojų, programų, duomenų bazių, tiekėjų sistemų. |
| R9-KRIP-04-ACT1-S2 | 2 | Pažymėti, kuriems srautams taikomas privalomas šifravimas pagal politiką (pvz., klientų duomenys, prisijungimo duomenys, administravimo sąsajos). |
| R9-KRIP-04-ACT2-S1 | 1 | Sukonfigūruoti TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) 1.2/1.3 su stipriomis cipher suite žemiau pateiktoms paslaugoms: web serveriams (pvz., Nginx, Apache), API (Application Programming Interface, programavimo sąsaja tarp sistemų ar komponentų) gateway, el. pašto serveriams, duomenų perdavimo tuneliams. |
| R9-KRIP-04-ACT2-S2 | 2 | Naudoti automatizuotus įrankius (pvz., SSL (Secure Sockets Layer, SSL ryšio šifravimo protokolas) Labs, Nessus, Qualys), kad periodiškai tikrinti, ar nėra nesaugių protokolų ir cipher suite, ir inicijuoti pataisymus. |

| | | |
|---|---|---|
| R9-KRIP-05-ACT1-S1 | 1 | Inventorizuoti duomenų saugyklas (duomenų bazės, failų serveriai, objektų saugyklos, SaaS sistemų duomenys) ir jų saugomų duomenų tipus. |
| R9-KRIP-05-ACT1-S2 | 2 | Kiekvienai saugyklai nustatyti, ar privalomas šifravimas (pvz., pagal BDAR (Bendrasis duomenų apsaugos reglamentas), TIS2 (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Tinklų ir informacinių sistemų saugumo direktyva (TIS2))/KSĮ (Lietuvos Respublikos kibernetinio saugumo įstatymas)) ir kokio lygio (diskų, failų, kolonėlių, backupų šifravimas). |
| R9-KRIP-05-ACT2-S1 | 1 | Įdiegti diskų ir duomenų bazių šifravimą (pvz., BitLocker, LUKS (Linux Unified Key Setup, Linux disko šifravimo mechanizmas LUKS), MS (Microsoft, „Microsoft“ technologijos ar paslaugos) SQL (Structured Query Language, duomenų bazių užklausų kalba SQL) TDE (Transparent Data Encryption, skaidrus duomenų šifravimas (TDE)), Oracle TDE, AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) EBS (Elastic Block Store, „Amazon“ EBS blokinis saugyklos sprendimas) Encryption, Azure Disk Encryption), naudojant centralizuotą raktų valdymą (KMS (Key Management Service, kriptografinių raktų valdymo paslauga)). |
| R9-KRIP-05-ACT2-S2 | 2 | Užtikrinti, kad atsarginės kopijos taip pat būtų šifruojamos (pvz., backup sprendimuose įjungti šifravimą, naudoti saugius backup saugyklų sprendimus – Veeam, Commvault, cloud backup'us). |
| R9-KRIP-06-ACT1-S1 | 1 | Sukurti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) naudojimo politiką, aprašant jungimosi scenarijus (nuotoliniai darbuotojai, tiekėjai, administravimo prieiga) ir saugumo reikalavimus. |
| R9-KRIP-06-ACT1-S2 | 2 | Aprašyti leistinus VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) protokolus ir šifravimo nustatymus (pvz., IPsec IKEv2, TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS)-based VPN, AES-256 (Advanced Encryption Standard 256-bit, 256 bitų ilgio AES simetrinio šifravimo standartas), draudžiant pasenusius protokolus PPTP (Point-to-Point Tunneling Protocol, taško–taško tuneliavimo protokolas PPTP), L2TP be IPsec). |
| R9-KRIP-06-ACT2-S1 | 1 | Sukonfigūruoti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus (pvz., Cisco AnyConnect, Fortinet, Palo Alto GlobalProtect, OpenVPN, WireGuard) pagal nustatytus šifravimo standartus ir autentifikavimą (MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija)). |
| R9-KRIP-06-ACT2-S2 | 2 | Įtraukti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) konfigūracijos ir šifravimo parametrų tikrinimą į reguliarias saugumo apžvalgas ir pažeidžiamumų skenavimą. |
| R9-KRIP-07-ACT1-S1 | 1 | Inventorizuoti esamus WiFi prieigos taškus ir tinklus (vidiniai, svečių, IoT) bei jų naudojimo paskirtį. |
| R9-KRIP-07-ACT1-S2 | 2 | Sukurti WiFi segmentavimo planą, numatant atskiras SSID (Service Set Identifier, belaidžio tinklo identifikatorius (SSID)) vidiniam, svečių ir kitų tipų srautams, su skirtingais saugumo lygiais ir prieigos taisyklėmis. |
| R9-KRIP-07-ACT2-S1 | 1 | WiFi infrastruktūroje (pvz., Cisco, Aruba, Ubiquiti) įjungti WPA3 (Wi-Fi Protected Access 3, „Wi-Fi Protected Access 3“ šifravimo standartas) arba WPA2 (Wi-Fi Protected Access 2, „Wi-Fi Protected Access 2“ šifravimo standartas)-Enterprise su 802.1X, naudojant RADIUS (Remote Authentication Dial-In User Service, tinklo autentifikavimo protokolas RADIUS)/AAA (Authentication, Authorization and Accounting, tapatybės nustatymo, autorizavimo ir apskaitos modelis) sprendimą (pvz., Microsoft NPS (Net Promoter Score, klientų lojalumo rodiklis (NPS)), Cisco ISE (Identity Services Engine, tapatybės paslaugų variklis (pvz., „Cisco ISE“))). |
| R9-KRIP-07-ACT2-S2 | 2 | Įtraukti WiFi konfigūracijos ir šifravimo būklės tikrinimą į reguliarias saugumo apžvalgas ir pažeidžiamumų skenavimą (pvz., wireless security assessment). |
| R9-KRIP-08-ACT1-S1 | 1 | Inventorizuoti TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS)/SSL (Secure Sockets Layer, SSL ryšio šifravimo protokolas) sertifikatus (viešas svetaines, API (Application Programming Interface, programavimo sąsaja tarp sistemų ar komponentų), VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), el. paštą, vidinius portalus) ir nustatyti, iš kokių CA (Certification Authority, sertifikavimo institucija) jie išduoti. |

| | | |
|---|---|---|
| R9-KRIP-08-ACT1-S2 | 2 | Atskirti viešoms paslaugoms naudojamus sertifikatus (iš viešų CA (Certification Authority, sertifikavimo institucija), pvz., DigiCert, GlobalSign, Let's Encrypt) ir vidiniams tikslams naudojamus sertifikatus (vidinis CA, pvz., Microsoft AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga) CS (Cyber Security, kibernetinis saugumas), HashiCorp Vault PKI (Public Key Infrastructure, viešojo rakto infrastruktūra)). |
| R9-KRIP-08-ACT2-S1 | 1 | Parengti sertifikatų išdavimo ir naudojimo procedūrą, nurodant leidžiamus CA (Certification Authority, sertifikavimo institucija), išdavimo procesą, patvirtinimo žingsnius ir pateikimo į gamybą tvarką. |
| R9-KRIP-08-ACT2-S2 | 2 | Įtraukti sertifikatų patikimumo ir galiojimo patikrą į reguliarius saugumo patikrinimus (pvz., SSL (Secure Sockets Layer, SSL ryšio šifravimo protokolas)/TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS) auditai, endpoint'ų skenavimas). |
| R9-KRIP-09-ACT1-S1 | 1 | Įvertinti esamą sertifikatų valdymo praktiką ir identifikuoti problemas (pasibaigę sertifikatai, necentralizuotas valdymas, neaiški atsakomybė). |
| R9-KRIP-09-ACT1-S2 | 2 | Įvertinti rinkos sprendimus (pvz., cert-manager Kubernetes aplinkai, Venafi, Smallstep, AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) ACM (Association for Computing Machinery, tarptautinė kompiuterių mokslo asociacija), Azure Key Vault, Let's Encrypt su ACME (ACME Corporation, pavyzdinis (fiktyvus) įmonės pavadinimas)) ir parinkti tinkamiausius organizacijos architektūrai. |
| R9-KRIP-09-ACT2-S1 | 1 | Sukonfigūruoti automatizuotą sertifikatų išdavimą ir atnaujinimą (pvz., ACME (ACME Corporation, pavyzdinis (fiktyvus) įmonės pavadinimas) protokolas su Let's Encrypt, cert-manager Kubernetes klasteriuose, AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) ACM (Association for Computing Machinery, tarptautinė kompiuterių mokslo asociacija) integracija su load balanceriais). |
| R9-KRIP-09-ACT2-S2 | 2 | Sukurti monitoringą ir įspėjimus dėl sertifikatų galiojimo pabaigos ir automatizavimo klaidų (pvz., integracija su SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema)/monitoringo sistema – Prometheus, Grafana, Zabbix). |
| R9-KRIP-10-ACT1-S1 | 1 | Iš raktų registro (R9-03) identifikuoti raktus, kurie naudojami autentifikavimui, parašo teikimui, root/issuing CA (Certification Authority, sertifikavimo institucija), aukštos vertės duomenų šifravimui. |
| R9-KRIP-10-ACT1-S2 | 2 | Nustatyti reikalaujamą apsaugos lygį (pvz., HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM)) atitinkantys FIPS (Federal Information Processing Standards, federaciniai informacijos apdorojimo standartai (FIPS)) 140-2/3, eIDAS QSCD (Qualified Signature Creation Device, kvalifikuotas parašo kūrimo įrenginys), ar cloud HSM/KMS (Key Management Service, kriptografinių raktų valdymo paslauga) su atitinkamais sertifikatais). |
| R9-KRIP-10-ACT2-S1 | 1 | Pasirinkti HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM)) ar cloud KMS (Key Management Service, kriptografinių raktų valdymo paslauga) sprendimą (pvz., Thales Luna, Utimaco, AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) CloudHSM, Azure Managed HSM, GCP (Google Cloud Platform, „Google Cloud“ debesų kompiuterijos platforma) Cloud HSM) ir suintegruoti jį su kritinėmis sistemomis (PKI (Public Key Infrastructure, viešojo rakto infrastruktūra), autentifikavimo serveriai, transakcijų sistemos). |
| R9-KRIP-10-ACT2-S2 | 2 | Parengti ir įvykdyti kritinių raktų perkėlimo planą į HSM (Hardware Security Module, aparatūrinis saugumo modulis (HSM))/KMS (Key Management Service, kriptografinių raktų valdymo paslauga), užtikrinant minimalų paslaugų sutrikimą ir galimybę atsukti pakeitimus (rollback), jei iškyla problemų. |
| R10-HRT-01-ACT1-S1 | 1 | Identifikuoti HR (Human Resources, žmogiškieji ištekliai) procesus, turinčius įtakos kibernetiniam saugumui (įdarbinimas, pareigų keitimas, laikinos prieigos, darbo santykių pabaiga, rangovai, praktikantai). |
| R10-HRT-01-ACT1-S2 | 2 | Nustatyti pagrindinius HR (Human Resources, žmogiškieji ištekliai) saugumo principus (pvz., „need-to-know“, pareigų atskyrimas, fono patikrinimai, konfidencialumas, atsakomybė už turtą). |

| | | |
|---|---|---|
| R10-HRT-01-ACT2-S1 | 1 | Parengti HR (Human Resources, žmogiškieji ištekliai) saugumo politikos projektą, apibrėžiant atsakomybes (HR, vadovai, darbuotojai), privalomus tikrinimus, elgesio reikalavimus ir ryšį su kitomis politikomis (IT (Information Technology, informacinės technologijos), prieigos, turto valdymo). |
| R10-HRT-01-ACT2-S2 | 2 | Suderinti politiką su vadovybe ir darbuotojų atstovais (jei taikoma), patvirtinti ją vadovo įsakymu ir paskelbti vidinėse komunikacijos priemonėse. |
| R10-HRT-01-ACT3-S1 | 1 | Atnaujinti HR (Human Resources, žmogiškieji ištekliai) procedūras, šablonus ir kontrolinius sąrašus (įdarbinimo, išėjimo, pareigų keitimo), kad juose būtų aiškiai įtvirtinti saugumo reikalavimai. |
| R10-HRT-01-ACT3-S2 | 2 | Nustatyti periodinę HR (Human Resources, žmogiškieji ištekliai) saugumo politikos ir susijusių procesų peržiūrą (pvz., kas 2 metus arba pasikeitus teisės aktams). |
| R10-HRT-02-ACT1-S1 | 1 | Sudaryti pareigybių sąrašą, turinčių aukštas prieigos teises ar kritinę įtaką (pvz., sistemų administratoriai, saugumo specialistai, finansinių operacijų tvirtintojai). |
| R10-HRT-02-ACT1-S2 | 2 | Apibrėžti patikrinimo tipą ir apimtį (pvz., teistumo pažyma, finansinės istorijos patikra, ankstesnių darbdavių rekomendacijos), laikantis darbo teisės ir duomenų apsaugos reikalavimų. |
| R10-HRT-02-ACT2-S1 | 1 | Atnaujinti įdarbinimo ir pareigų keitimo procedūras, įtraukiant fono patikrinimo žingsnius, atsakomybes ir sprendimo kriterijus (priimti/nepriimti). |
| R10-HRT-02-ACT2-S2 | 2 | Nustatyti duomenų saugojimo, dokumentavimo ir peržiūros tvarką (kas ir kiek laiko saugo patikrinimų įrodymus, kaip užtikrinamas konfidencialumas). |
| R10-HRT-03-ACT1-S1 | 1 | Parengti konfidencialumo susitarimo (NDA (Non-Disclosure Agreement, konfidencialumo sutartis)) ir priimtino naudojimo taisyklių (Acceptable Use Policy) šablonus, suderintus su BDAR (Bendrasis duomenų apsaugos reglamentas), darbo ir komercine teise. |
| R10-HRT-03-ACT1-S2 | 2 | Apibrėžti, kuriems asmenų tipams taikomi kurie dokumentai (darbuotojai, laikini darbuotojai, rangovai, partnerių atstovai). |
| R10-HRT-03-ACT2-S1 | 1 | Įtraukti NDA (Non-Disclosure Agreement, konfidencialumo sutartis) ir elgesio taisyklių pasirašymą į onboarding'o kontrolinius sąrašus ir prieigos suteikimo procesą (be pasirašymo – nepradedamas darbas su sistemomis). |
| R10-HRT-03-ACT2-S2 | 2 | Sukurti procesą, kaip susitarimai peržiūrimi ir atnaujinami (pvz., pasikeitus politikoms), ir kaip centralizuotai saugomi pasirašyti dokumentai (HRIS (Human Resources Information System, žmogiškųjų išteklių informacinė sistema), dokumentų valdymo sistema). |
| R10-HRT-04-ACT1-S1 | 1 | Identifikuoti turto kategorijas (pvz., informacinės sistemos, serveriai, darbo vietos, mobilūs įrenginiai, programinė įranga, duomenų rinkiniai) ir jų savininkus (asset owners). |
| R10-HRT-04-ACT1-S2 | 2 | Nustatyti, kuris turtas yra kritinis veiklos tęstinumui ir kibernetiniam saugumui, ir pažymėti tai turto registre. |
| R10-HRT-04-ACT2-S1 | 1 | Parengti turto valdymo politiką, apibrėžiančią turto identifikavimo, registravimo, klasifikavimo, inventorizavimo ir nurašymo principus bei atsakomybes. |
| R10-HRT-04-ACT2-S2 | 2 | Suderinti turto valdymo politiką su vadovybe ir patvirtinti ją vadovo įsakymu, paskelbti ją atitinkamiems darbuotojams (IT (Information Technology, informacinės technologijos), finansams, verslo savininkams). |
| R10-HRT-05-ACT1-S1 | 1 | Nustatyti klasifikavimo lygius (pvz., Viešas, Vidaus, Konfidencialus, Labai konfidencialus) ir kiekvieno lygio aprašą bei pavyzdžius. |
| R10-HRT-05-ACT1-S2 | 2 | Sujungti klasifikavimo modelį su duomenų apsaugos ir prieigos valdymo reikalavimais (pvz., kokiam lygiui privalomas šifravimas, papildoma autentifikacija, saugojimo ribos). |
| R10-HRT-05-ACT2-S1 | 1 | Atnaujinti turto registrą, pridedant klasifikavimo lauką ir priskiriant klasifikaciją bent kritiniam turtui ir jautriems duomenims. |
| R10-HRT-05-ACT2-S2 | 2 | Įdiegti taisyklę, kad naujas turtas (sistemos, duomenų rinkiniai) būtų klasifikuotas sukūrimo ar įsigijimo metu, ne vėliau. |

| | | |
|---|---|---|
| R10-HRT-06-ACT1-S1 | 1 | Identifikuoti kritines patalpas (serverinės, tinklo mazgai, UPS (Uninterruptible Power Supply, nenutrūkstamo maitinimo šaltinis) patalpos) ir priskirti joms apsaugos lygį. |
| R10-HRT-06-ACT1-S2 | 2 | Parengti fizinės prieigos taisykles (kas turi teisę patekti, kokiu pagrindu, kokiu laiku, su kokiu leidimu) ir aprašyti išimčių tvarką (pvz., rangovams). |
| R10-HRT-06-ACT2-S1 | 1 | Įdiegti fizinės prieigos kontrolės priemones (kortelių skaitytuvai, PIN (Personal Identification Number, asmeninis identifikavimo numeris (PIN)) kodai, biometriniai sprendimai) ir, jei reikia, vaizdo stebėjimą serverinėse. |
| R10-HRT-06-ACT2-S2 | 2 | Užtikrinti, kad prieigos žurnalai (badge logs) ir vaizdo įrašai būtų saugomi nustatytą laikotarpį ir peržiūrimi incidentų ar auditų atveju. |
| R10-HRT-07-ACT1-S1 | 1 | Įvertinti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) sprendimus (pvz., Microsoft Intune, VMware Workspace ONE, MobileIron, Jamf) atsižvelgiant į naudojamas OS (Operating System, operacinė sistema) (iOS, Android) ir integraciją su esamomis sistemomis. |
| R10-HRT-07-ACT1-S2 | 2 | Įdiegti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) platformą ir sukonfigūruoti bazinę integraciją (naudotojų katalogas, el. paštas, WiFi profiliai, VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) profiliai). |
| R10-HRT-07-ACT2-S1 | 1 | Parengti enrolinimo procedūrą (kaip įrenginiai prijungiami prie MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema)) ir ją įtraukti į naujų įrenginių išdavimo procesą. |
| R10-HRT-07-ACT2-S2 | 2 | Sukurti ir pritaikyti MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) politikas (ekrano užraktas, šifravimas, OS (Operating System, operacinė sistema) atnaujinimai, draudžiamos programos) bei nustatyti neatitikties valdymo taisykles. |
| R10-HRT-08-ACT1-S1 | 1 | Aprašyti, kad visiems darbo (arba BYOD (Bring Your Own Device, naudotojo asmeninių įrenginių naudojimo darbe politika) su prieiga prie vidinių sistemų) mobiliems įrenginiams privalomas įjungtas diskų šifravimas, ir nurodyti palaikomas technologijas (pvz., BitLocker, FileVault, Android/iOS built-in encryption). |
| R10-HRT-08-ACT2-S1 | 1 | Per MDM (Mobile Device Management, mobiliųjų įrenginių valdymo sistema) ar OS (Operating System, operacinė sistema) valdymo įrankius įjungti privalomą diskų šifravimą visiems valdomiems įrenginiams ir aprašyti išimčių tvarką (jei tokios leidžiamos). |
| R10-HRT-08-ACT2-S2 | 2 | Sukurti ataskaitas ir įspėjimus apie nešifruotus ar neatitinkančius reikalavimų įrenginius ir nustatyti reakcijos tvarką (pvz., prieigos blokavimas). |
| R11-PRIEI-06-ACT1-S1 | 1 | Inventorizuoti privilegijuotas paskyras (domain admin, serverių admin, DB (Database, duomenų bazė) admin, programų admin, saugumo sistemų admin) ir jas susieti su sistemomis. |
| R11-PRIEI-06-ACT1-S2 | 2 | Nustatyti prioritetines sistemas, kuriose MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) turi būti diegiama pirmiausiai (AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga), VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), bastion host, kritinių verslo sistemų admin sąsajos). |
| R11-PRIEI-06-ACT2-S1 | 1 | Pasirinkti ir sukonfigūruoti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) sprendimą (pvz., Azure AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga) MFA, Duo Security, Okta, Google Authenticator, FIDO2 (Fast IDentity Online 2, šiuolaikinis be slaptažodžių autentifikavimo standartas FIDO2) raktai) integruojant jį su katalogo paslauga ir svarbiausiomis sistemomis. |
| R11-PRIEI-06-ACT2-S2 | 2 | Įjungti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) visoms privilegijuotoms paskyroms, taikant „MFA required“ politiką ir nustatyti išimčių valdymo tvarką (laikinės išimtys, patvirtinimai). |
| R11-PRIEI-07-ACT1-S1 | 1 | Inventorizuoti visus nuotolinės prieigos kanalus (VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) gateway, web portalai, administravimo sąsajos iš interneto). |

| | | |
|---|---|---|
| R11-PRIEI-07-ACT1-S2 | 2 | Pažymėti kanaluose naudojamus autentifikavimo mechanizmus ir identifikuoti, kur MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) dar netaikoma. |
| R11-PRIEI-07-ACT2-S1 | 1 | Integruoti VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) sprendimus, RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) gateway ir nuotolinius portalus su MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) (pvz., per SAML (Security Assertion Markup Language, SAML saugumo teiginių žymėjimo kalba)/OIDC (OpenID Connect, tapatybės federacijos standartas OpenID Connect), RADIUS (Remote Authentication Dial-In User Service, tinklo autentifikavimo protokolas RADIUS) integraciją su Azure AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga) MFA, Duo ir pan.). |
| R11-PRIEI-07-ACT2-S2 | 2 | Įjungti politiką „MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) required from external network“, apribojant prisijungimą be MFA iš interneto ir nustatant atitinkamas išimtis tik išimtiniais atvejais. |
| R11-PRIEI-08-ACT1-S1 | 1 | Remiantis rizikos vertinimu ir turto klasifikavimu, identifikuoti kritines verslo sistemas ir duomenų bazes (finansinės, klientų duomenų, operacinės sistemos). |
| R11-PRIEI-08-ACT1-S2 | 2 | Įvertinti, kokie prisijungimo mechanizmai šiuo metu taikomi (vietiniai vartotojai, AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga) integracija, SSO (Single Sign-On, vieningo prisijungimo (SSO) mechanizmas)) ir kur MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) nėra įmanoma tiesiogiai. |
| R11-PRIEI-08-ACT2-S1 | 1 | Ten, kur įmanoma, integruoti sistemas ir DB (Database, duomenų bazė) su identiteto tiekėju (IDP (Identity Provider, tapatybės teikėjas (IdP))) ir MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) (pvz., per SSO (Single Sign-On, vieningo prisijungimo (SSO) mechanizmas), bastion host, jump server, PAM (Privileged Access Management, privilegijuotos prieigos valdymas) sprendimus). |
| R11-PRIEI-08-ACT2-S2 | 2 | Kur MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) integracija tiesiogiai neįmanoma, naudoti alternatyvias priemones (pvz., VPN (Virtual Private Network, virtualus privatus tinklas (VPN)) su MFA + bastion host, privileged access management), apribojant tiesioginę prieigą. |
| R11-PRIEI-09-ACT1-S1 | 1 | Identifikuoti verslo situacijas, kuriose perduodama jautri ar konfidenciali informacija (incidents handling, vadovybės diskusijos, klientų duomenys, tiekimo grandinės rizikos). |
| R11-PRIEI-09-ACT1-S2 | 2 | Parengti gaires, kuriuose kanaluose leidžiama aptarti skirtingų lygių informaciją (pvz., vidinis Teams/Zoom su E2EE, saugi el. pašto šifravimo priemonė, draudžiami atviri kanalai). |
| R11-PRIEI-09-ACT2-S1 | 1 | Parinkti ir sukonfigūruoti saugius komunikacijos sprendimus (pvz., Microsoft Teams su E2EE, Signal, šifruota el. pašto infrastruktūra su S/MIME (Multipurpose Internet Mail Extensions, el. pašto priedų ir turinio standarto MIME specifikacija) ar PGP (Pretty Good Privacy, PGP duomenų ir el. pašto šifravimo standartas)). |
| R11-PRIEI-09-ACT2-S2 | 2 | Integruoti šiuos sprendimus su naudotojų katalogu ir nustatyti saugumo parametrus (MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija), E2EE, saugios saugyklos), taip pat parengti naudotojams instrukcijas. |
| R11-PRIEI-10-ACT1-S1 | 1 | Identifikuoti kritinius vaidmenis ir komandas, kurioms reikia specialių avarinio ryšio kanalų (incidentų valdymo komanda, vadovybė, IT (Information Technology, informacinės technologijos), komunikacijos, verslo kritinių padalinių vadovai). |
| R11-PRIEI-10-ACT1-S2 | 2 | Aprašyti avarinio ryšio kanalus (pvz., alternatyvūs mobiliojo ryšio tinklai, rezerviniai pokalbių kanalai, saugios žinučių grupės) ir jų naudojimo principus. |
| R11-PRIEI-10-ACT2-S1 | 1 | Suteikti kritiniams vaidmenims prieigą prie avarinio ryšio priemonių (pvz., atskiros SIM (Security Information Management, saugumo informacijos valdymas (SIM)) kortelės, specialios žinutės/konferencijų platformos, rezervinės darbo vietos). |

| | | |
|---|---|---|
| R11-PRIEI-10-ACT2-S2 | 2 | Įtraukti avarinio ryšio kanalų testavimą į BC (Business Continuity, verslo tęstinumas)/DR (Disaster Recovery, veiklos atkūrimas po sutrikimų) ir incidentų valdymo pratybas (pvz., kartą per metus atlikti testinį iškvietimą/komunikaciją). |
| R11-TINK-01-ACT1-S1 | 1 | Parengti esamo tinklo diagramos versiją (LAN (Local Area Network, vietinis kompiuterių tinklas (LAN)), WAN (Wide Area Network, tolimųjų ryšių tinklas (WAN)), VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), WiFi, serverių segmentai, debesijos jungtys). |
| R11-TINK-01-ACT1-S2 | 2 | Nustatyti, kokias zonas reikia atskirti (pvz., vartotojų LAN (Local Area Network, vietinis kompiuterių tinklas (LAN)), serverių segmentas, administravimo tinklas, svečių WiFi, partnerių jungtys, OT (Operational Technology, operacinės technologijos) tinklai) ir kokie tarp jų turi būti ryšiai. |
| R11-TINK-01-ACT2-S1 | 1 | Sukonfigūruoti VLAN (Virtual Local Area Network, virtualus vietinis tinklas (VLAN)), maršrutizavimą ir ugniasienes taip, kad tarp zonų būtų tik būtini srautai, laikantis mažiausios privilegijos principo. |
| R11-TINK-01-ACT2-S2 | 2 | Dokumentuoti naują tinklo architektūrą ir įtraukti ją į konfigūracijos valdymo bei pokyčių valdymo procesus. |
| R11-TINK-02-ACT1-S1 | 1 | Sudaryti tarpzoninių srautų matricą (source zone → destination zone → port/protocol → purpose) ir įvertinti ją saugumo požiūriu. |
| R11-TINK-02-ACT1-S2 | 2 | Aprašyti ugniasienių taisyklių kūrimo ir peržiūros principus (deny by default, change management, periodinės taisyklių recenzijos). |
| R11-TINK-02-ACT2-S1 | 1 | Per ugniasienes (pvz., Fortinet, Palo Alto, Check Point) sukurti taisykles pagal srautų matricą, pašalinti nereikalingas taisykles ir užtikrinti „default deny“ principą tarp zonų. |
| R11-TINK-02-ACT2-S2 | 2 | Įdiegti ugniasienių žurnalų rinkimą ir koreliuoti įvykius per SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) arba logų analizės sistemą, nustatant alertus dėl įtartinų srautų. |
| R11-TINK-03-ACT1-S1 | 1 | Inventorizuoti darbo stotis, serverius ir kitus endpoint'us (įskaitant nuotolinius ir hibridinius darbuotojus), pažymint OS (Operating System, operacinė sistema) tipą ir kritiškumą. |
| R11-TINK-03-ACT1-S2 | 2 | Aprašyti endpoint apsaugos reikalavimus (real-time protection, centralizuotas valdymas, logų rinkimas, reakcijos priemonės) ir prioritetą kritiniams serveriams. |
| R11-TINK-03-ACT2-S1 | 1 | Pasirinkti ir įdiegti EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas)/AV (Antivirus, antivirusinė programinė įranga) sprendimą (pvz., Microsoft Defender for Endpoint, CrowdStrike, SentinelOne, ESET (ESET, „ESET“ antivirusinė ir saugumo programinė įranga)), sukonfigūruojant politiką pagal kritiškumą. |
| R11-TINK-03-ACT2-S2 | 2 | Nustatyti automatinius atnaujinimus, politikų taikymą ir įspėjimus, integruoti EDR (Endpoint Detection and Response, galinių įrenginių aptikimo ir reagavimo sprendimas)/AV (Antivirus, antivirusinė programinė įranga) logus į SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) arba centralų logų sprendimą. |
| R11-TINK-04-ACT1-S1 | 1 | Pasirinkti el. pašto saugumo sprendimą (pvz., Microsoft Defender for Office 365, Proofpoint, Mimecast) ir sukonfigūruoti filtravimo taisykles (spam, malware, phishing). |
| R11-TINK-04-ACT1-S2 | 2 | Sukonfigūruoti SPF (Sender Policy Framework, siuntėjo politikos sistema (SPF)), DKIM (DomainKeys Identified Mail, el. pašto autentifikavimo mechanizmas DKIM) ir DMARC (Domain-based Message Authentication, Reporting and Conformance, el. pašto autentifikavimo ir ataskaitų teikimo standartas DMARC) įrašus, siekiant sumažinti domeno spoofing riziką ir gerinti laiškų reputaciją. |
| R11-TINK-04-ACT2-S1 | 1 | Nustatyti el. pašto grėsmių ataskaitų teikimo kanalą (pvz., „Report phishing“ mygtukas kliente) ir instrukcijas naudotojams, kaip elgtis su įtartinais laiškais. |

| | | |
|---|---|---|
| R11-TINK-04-ACT2-S2 | 2 | Periodiškai analizuoti el. pašto grėsmių ataskaitas ir incidentus, atnaujinti filtravimo taisykles ir mokymų turinį pagal pastebėtas tendencijas. |
| R11-TINK-05-ACT1-S1 | 1 | Parengti priimtino interneto naudojimo taisykles (Acceptable Use), apibrėžiant draudžiamas kategorijas (pvz., malware, gambling, adult, anonymizers). |
| R11-TINK-05-ACT1-S2 | 2 | Nustatyti specialius reikalavimus kritinėms rolėms (pvz., saugumo analitikams, kurie gali reikėti prieigos prie plačios svetainių grupės testavimo tikslais). |
| R11-TINK-05-ACT2-S1 | 1 | Pasirinkti ir įdiegti web filtravimo sprendimą (pvz., secure web gateway, Zscaler, Cisco Umbrella, proxy su URL (Uniform Resource Locator, interneto ištekliaus adresas (URL)) kategorijomis) ir pritaikyti politiką pagal priimtino naudojimo taisykles. |
| R11-TINK-05-ACT2-S2 | 2 | Įdiegti žurnalų rinkimą ir ataskaitas apie blokuotus bandymus, kategorijas ir rizikingus naudotojų elgesio modelius. |
| R11-TINK-06-ACT1-S1 | 1 | Įvertinti infrastruktūros architektūrą ir nustatyti taškus, kur IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) teiks didžiausią vertę (perimetro ugniasienės, tarp kritinių zonų, serverių segmentas, debesijos aplinkos). |
| R11-TINK-06-ACT2-S1 | 1 | Įdiegti IDS (Intrusion Detection System, įsilaužimų aptikimo sistema)/IPS (Intrusion Prevention System, įsilaužimų prevencijos sistema) sprendimą (pvz., Snort, Suricata, Zeek, komerciniai NGFW (Next-Generation Firewall, naujos kartos ugniasienė) su IDS/IPS moduliais) ir sujungti jį su tinklo segmentais pagal planą. |
| R11-TINK-06-ACT2-S2 | 2 | Sukonfigūruoti taisykles, prioritetus ir alertų srautus (į SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema), el. paštą, ticketing), nustatyti triukšmo mažinimo ir klaidingų pavojaus signalų valdymo tvarką. |
| R11-TINK-07-ACT1-S1 | 1 | Nustatyti, kurios tinklo atkarpos (core, perimetras, tarp zonų, VPN (Virtual Private Network, virtualus privatus tinklas (VPN))) turi būti stebimos ir kokius rodiklius reikia rinkti (NetFlow, latency, packet loss, anomalijos). |
| R11-TINK-07-ACT2-S1 | 1 | Įdiegti tinklo monitoring'o įrankius (pvz., Zabbix, PRTG (Paessler Router Traffic Grapher, PRTG tinklo stebėsenos sistema), SolarWinds, nTop, NetFlow kolektorius) ir sukonfigūruoti duomenų rinkimą iš maršrutizatorių, ugniasienių, switch'ų. |
| R11-TINK-07-ACT2-S2 | 2 | Sukurti pranešimų ir ataskaitų rinkinį (alertus dėl anomalių srautų, našumo kritimo, DDoS požymių) ir integruoti juos su incidentų valdymo procesu. |
| R11-TINK-08-ACT1-S1 | 1 | Atlikti auditą, identifikuojant visus administravimo kanalus (serveriai, tinklo įranga, programos) ir juose naudojamus protokolus. |
| R11-TINK-08-ACT1-S2 | 2 | Sudaryti planą, kaip išjungti nesaugius protokolus (telnet, HTTP (Hypertext Transfer Protocol, hiperteksto perdavimo protokolas HTTP), RSH, senus SSH (Secure Shell, saugus nuotolinės komandinės eilutės protokolas SSH)/SSL (Secure Sockets Layer, SSL ryšio šifravimo protokolas) variantus) ir juos pakeisti saugiais atitikmenimis. |
| R11-TINK-08-ACT2-S1 | 1 | Įdiegti ir sukonfigūruoti saugius protokolus (SSH (Secure Shell, saugus nuotolinės komandinės eilutės protokolas SSH), HTTPS (Hypertext Transfer Protocol Secure, saugus hiperteksto perdavimo protokolas HTTPS), RDP (Remote Desktop Protocol, nuotolinio darbalaukio protokolas) over TLS (Transport Layer Security, transportinio lygmens saugumo protokolas TLS)/VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), bastion host, jump server), išjungiant nesaugias alternatyvas. |
| R11-TINK-08-ACT2-S2 | 2 | Įtraukti administravimo kanalų kontrolę į reguliarius saugumo testus (vulnerability scan, configuration audit) ir incidentų tyrimų scenarijus. |

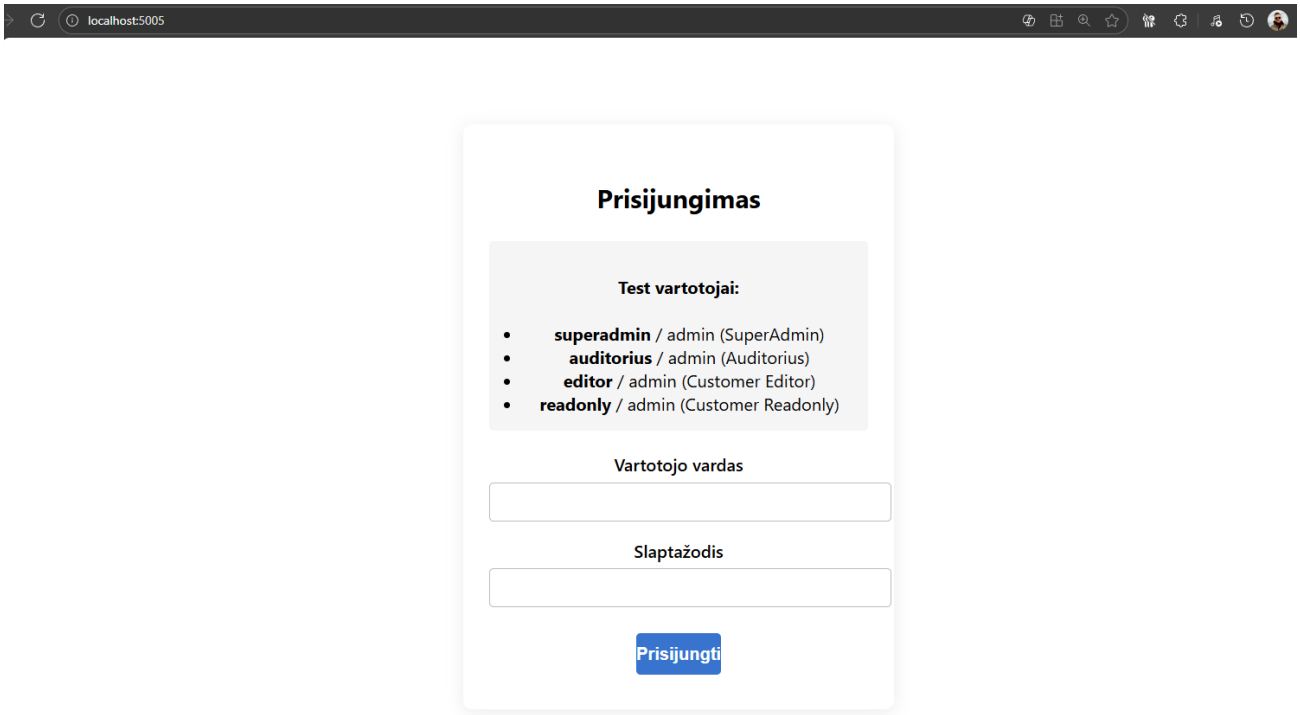
| | | |
|---|---|---|
| R11-TINK-09-ACT1-S1 | 1 | Inventorizuoti naudojamas cloud platformas (pvz., AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma), Azure, GCP (Google Cloud Platform, „Google Cloud“ debesų kompiuterijos platforma), SaaS paslaugos) ir paskyrų tipus (organizacinės, asmeninės, service accounts). |
| R11-TINK-09-ACT1-S2 | 2 | Įvertinti, ar cloud prieiga valdoma per centralizuotą IDP (Identity Provider, tapatybės teikėjas (IdP)) (SSO (Single Sign-On, vieningo prisijungimo (SSO) mechanizmas)) ir ar visoms privilegijuotoms paskyroms taikomas MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija). |
| R11-TINK-09-ACT2-S1 | 1 | Integruoti cloud platformas su organizacijos IDP (Identity Provider, tapatybės teikėjas (IdP)) (pvz., Azure AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga), Okta) ir įjungti MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) visoms admin bei, jei įmanoma, visoms naudotojų paskyroms. |
| R11-TINK-09-ACT2-S2 | 2 | Naudoti cloud security posture management (CSPM (Cloud Security Posture Management, debesų saugumo būsenos valdymo priemonės)) ar built-in įrankius (pvz., Azure Security Center, AWS (Amazon Web Services, „Amazon“ debesų kompiuterijos paslaugų platforma) Security Hub) prieigos politikų ir konfigūracijų atitikčiai stebėti. |
| R12-PRIEI-01-ACT1-S1 | 1 | Identifikuoti naudotojų grupes (darbuotojai, administratoriai, tiekėjų atstovai, partneriai) ir prieigos tipus (vidinė, nuotolinė, trečiųjų šalių) bei juos aprašyti. |
| R12-PRIEI-01-ACT1-S2 | 2 | Sutarti dėl pagrindinių prieigos kontrolės principų (least privilege, need-to-know, separation of duties, „default deny“, laikini leidimai) ir jų apibrėžimų. |
| R12-PRIEI-01-ACT2-S1 | 1 | Parengti prieigos kontrolės politikos dokumentą, apimantį rolėmis grįstą prieigą (RBAC (Role-Based Access Control, vaidmenimis grindžiama prieigos kontrolė)), tiekėjų ir partnerių prieigą, nuotolinę prieigą, slaptažodžių ir MFA (Multi-Factor Authentication, daugiaveiksnė autentifikacija) reikalavimus. |
| R12-PRIEI-01-ACT2-S2 | 2 | Suderinti politiką su vadovybe ir patvirtinti vadovo įsakymu, paskelbti prieinamoje vidinėje erdvėje ir komunikuoti darbuotojams. |
| R12-PRIEI-01-ACT3-S1 | 1 | Atnaujinti naudotojų įdarbinimo, rolės keitimo, darbo santykių nutraukimo ir tiekėjų prieigos suteikimo procedūras, kad jos atitiktų prieigos kontrolės politiką. |
| R12-PRIEI-01-ACT3-S2 | 2 | Nustatyti politikos peržiūros dažnį (pvz., kas 1–2 metus arba po esminių pokyčių) ir atsakingą vaidmenį už peržiūrą bei atnaujinimą. |
| R12-PRIEI-02-ACT1-S1 | 1 | Identifikuoti standartines verslo ir IT (Information Technology, informacinės technologijos) roles (pvz., buhalteris, klientų aptarnavimas, sistemos vartotojas, sistemos administratorius) ir joms būdingas funkcijas. |
| R12-PRIEI-02-ACT1-S2 | 2 | Sukurti teisių matricą (role → sistemos funkcijos → leidžiami veiksmai), atskiriant standartines ir privilegijuotas teises. |
| R12-PRIEI-02-ACT2-S1 | 1 | Per IDP (Identity Provider, tapatybės teikėjas (IdP))/IAM (Identity and Access Management, tapatybių ir prieigos valdymas) ir kritines sistemas sukurti roles pagal teisių matricą ir perkelti naudotojus nuo individualių teisių prie rolių pagrindu suteikiamos prieigos. |
| R12-PRIEI-02-ACT2-S2 | 2 | Pašalinti perteklines teises (pvz., „admin“ ten, kur jos nebūtinos) ir įdiegti procesą, kaip reguliariai aptikti ir koreguoti „privilege creep“ atvejus. |
| R12-PRIEI-03-ACT1-S1 | 1 | Parengti gaires, kad visi administratoriai privalo turėti dvi paskyras: standartinę vartotojo paskyrą ir atskirą administracinę paskyrą tik administravimo užduotims. |
| R12-PRIEI-03-ACT1-S2 | 2 | Draudžiama naudoti bendras (shared) administratorių paskyras, išskyrus išimtiniais atvejais, kurie turi būti dokumentuoti ir papildomai kontroliuojami. |
| R12-PRIEI-03-ACT2-S1 | 1 | Per AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga)/IDP (Identity Provider, tapatybės teikėjas (IdP)) ir sistemų valdymo įrankius sukurti atskiras administracines paskyras, priskiriant jas tik reikalingoms admin rolių grupėms. |

| | | |
|---|---|---|
| R12-PRIEI-03-ACT2-S2 | 2 | Įdiegti monitoringą ir auditą administracinių paskyrų prisijungimams (pvz., per SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema), PAM (Privileged Access Management, privilegijuotos prieigos valdymas)), kad būtų galima atsekti veiksmus ir aptikti anomalijas. |
| R12-PRIEI-04-ACT1-S1 | 1 | Nustatyti, kokios sistemos ir naudotojų grupės privalomai turi būti įtrauktos į periodines prieigos peržiūras (pvz., kritinės sistemos, privilegijuotos paskyros, tiekėjų paskyros). |
| R12-PRIEI-04-ACT1-S2 | 2 | Aprašyti peržiūrų dažnį (pvz., kartą per metus visiems, kas ketvirtį – privilegijuotoms paskyroms) ir atsakingus peržiūrėtojus (sistemos savininkai, padalinių vadovai). |
| R12-PRIEI-04-ACT2-S1 | 1 | Sukurti prieigos ataskaitas iš IAM (Identity and Access Management, tapatybių ir prieigos valdymas)/IDP (Identity Provider, tapatybės teikėjas (IdP)) ir kritinių sistemų (naudotojas → rolės → sistemos) ir pateikti jas peržiūrėtojams patvirtinimui arba korekcijai. |
| R12-PRIEI-04-ACT2-S2 | 2 | Užfiksuoti peržiūrų sprendimus (palikti, keisti, atšaukti prieigą) ir inicijuoti teisių korekcijas, įtraukiant IT (Information Technology, informacinės technologijos)/ IAM (Identity and Access Management, tapatybių ir prieigos valdymas) komandą įgyvendinimui. |
| R12-PRIEI-05-ACT1-S1 | 1 | Aprašyti, kokie priviliegijuotų paskyrų įvykiai turi būti registruojami (prisijungimai, nesėkmingi bandymai, konfigūracijų keitimai, vartotojų ir teisių keitimai). |
| R12-PRIEI-05-ACT1-S2 | 2 | Nustatyti logų saugojimo laikotarpį ir prieigos prie logų kontrolę, atsižvelgiant į teisės aktų ir vidinės politikos reikalavimus. |
| R12-PRIEI-05-ACT2-S1 | 1 | Sukonfigūruoti sistemas (AD (Active Directory, „Active Directory“ katalogų ir tapatybių valdymo paslauga), PAM (Privileged Access Management, privilegijuotos prieigos valdymas), kritines aplikacijas), kad privilegijuotų paskyrų įvykiai būtų siunčiami į SIEM (Security Information and Event Management, saugumo informacijos ir įvykių valdymo sistema) ar centralizuotą logų valdymo sprendimą. |
| R12-PRIEI-05-ACT2-S2 | 2 | Sukurti koreliacijos taisykles ir alertus (pvz., prisijungimai neįprastu laiku, iš neįprastos vietos, masiniai teisių keitimai) ir susieti juos su incidentų valdymo procesu. |
| R12-PRIEI-11-ACT1-S1 | 1 | Aprašyti, kokią informaciją HR (Human Resources, žmogiškieji ištekliai) turi pateikti IT (Information Technology, informacinės technologijos) apie naujus darbuotojus, rolių pasikeitimus ir darbo santykių nutraukimą (vardas, rolė, padalinys, pradžios/pabaigos datos). |
| R12-PRIEI-11-ACT1-S2 | 2 | Nustatyti terminus, per kuriuos IT (Information Technology, informacinės technologijos) privalo sukurti, pakeisti arba panaikinti prieigos teises (pvz., nauja paskyra – iki pirmos darbo dienos, nutraukimas – per 24 val. nuo atleidimo). |
| R12-PRIEI-11-ACT2-S1 | 1 | Integruoti HR (Human Resources, žmogiškieji ištekliai) sistemą su IAM (Identity and Access Management, tapatybių ir prieigos valdymas)/IDP (Identity Provider, tapatybės teikėjas (IdP)) (pvz., per API (Application Programming Interface, programavimo sąsaja tarp sistemų ar komponentų), failų mainus ar specializuotą integracijos sprendimą), kad darbuotojų statuso pokyčiai būtų perduodami automatiškai. |
| R12-PRIEI-11-ACT2-S2 | 2 | Sukonfigūruoti automatines taisykles, kad darbuotojui išėjus būtų nedelsiant išjungiama jo prieiga (disable account), atšaukiami token'ai, VPN (Virtual Private Network, virtualus privatus tinklas (VPN)), el. paštas ir kt. prieigos. |

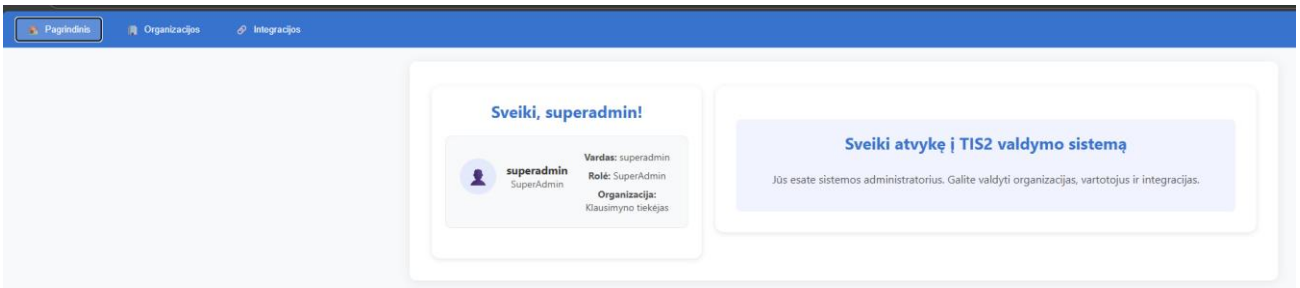
| | | |
|---|---|---|
| R12-PRIEI-11-ACT2-S3 | 3 | Įdiegti reguliarias ataskaitas apie buvusių darbuotojų aktyvias paskyras ir JML (Joiner-Mover-Leaver, darbuotojų gyvavimo ciklo (priėmimo, perkėlimo, išėjimo) procesas) SLA (Service Level Agreement, paslaugų lygio sutartis) laikymąsi, inicijuoti korekcines priemones nustačius nukrypimus. |

# 6. TIS2 vertinimo įrankio naudotojo sąsajos ekranvaizdžiai

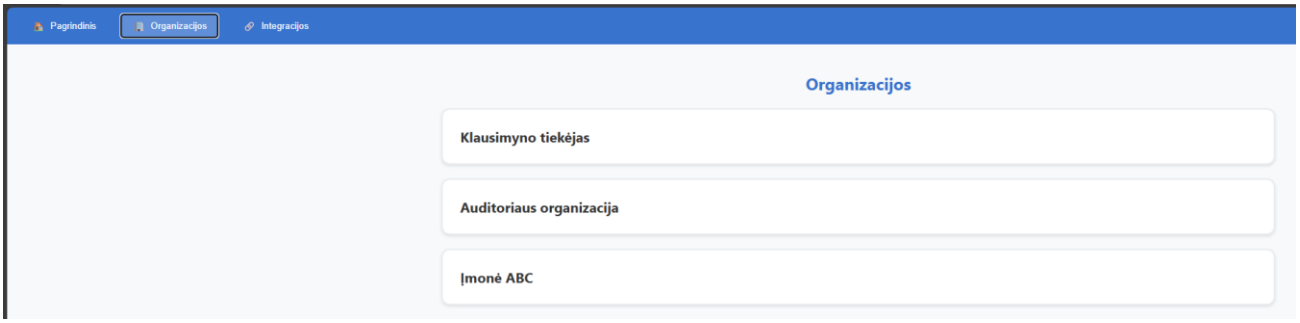
## Prisijungimo ekranas



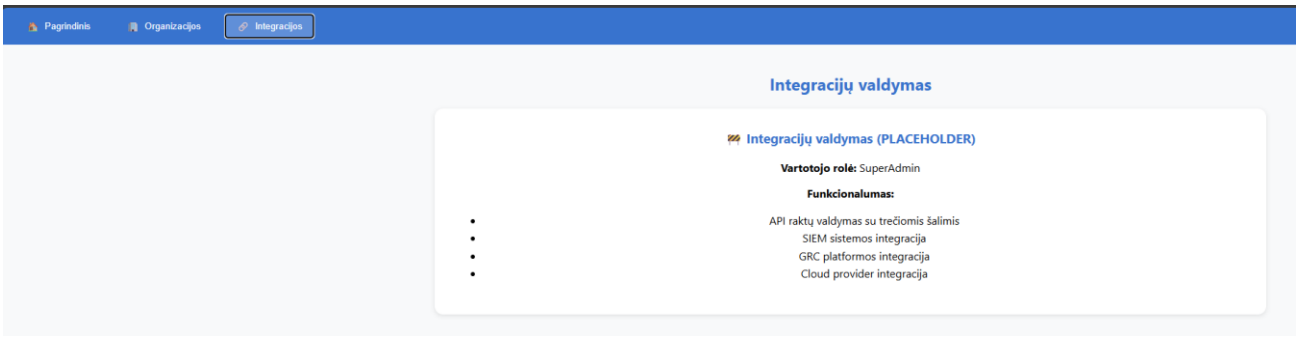

## Įrankio naudotojo SUPERADMIN naudojimo aplinka



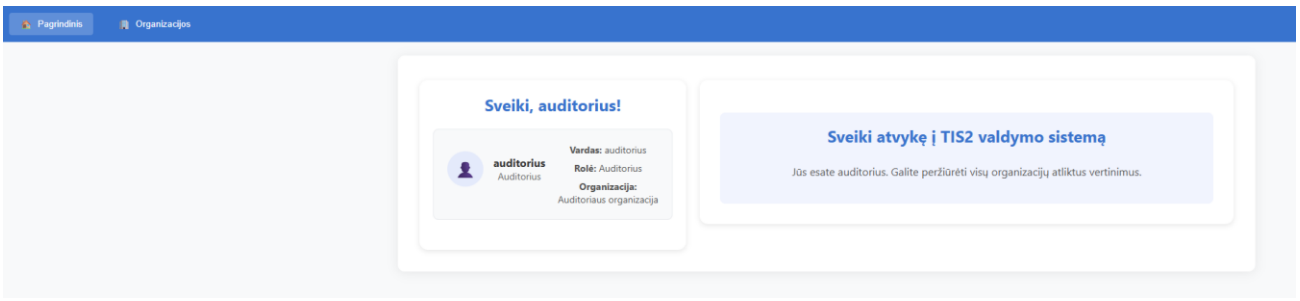

Organizacijų galinčių atlikti vertinimus arba juos tikrinti valdymas (konceptas, nerealizuota)



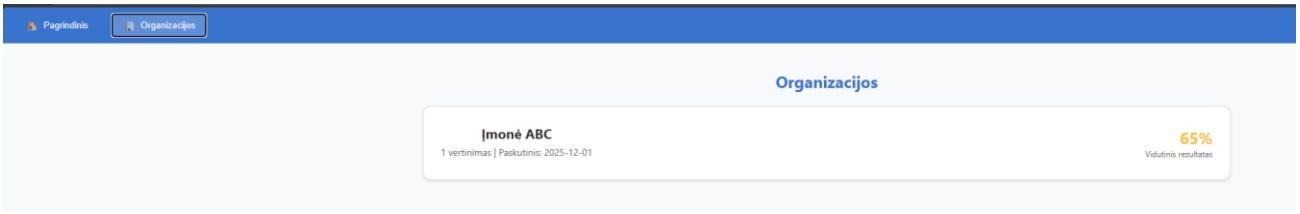

Integracijų su trečiosiomis šalimis įrodymų automatiniam pateikimui valdymas (konceptas, nerealizuota)



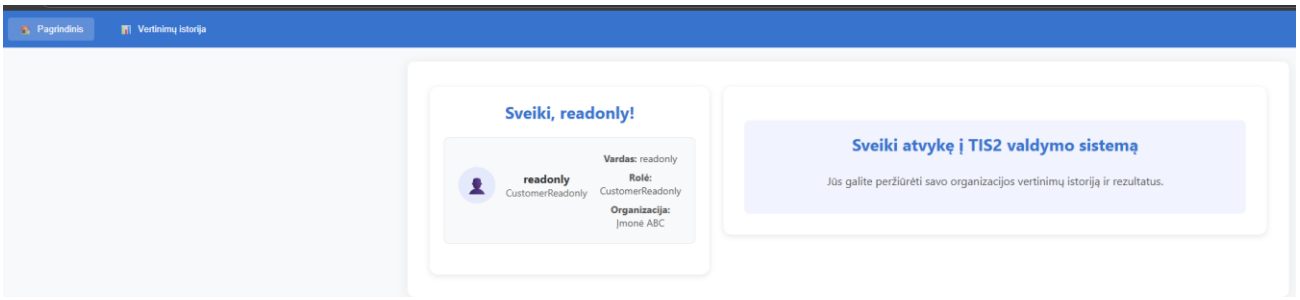

## Įrankio naudotojo AUDITOR naudojimo aplinka



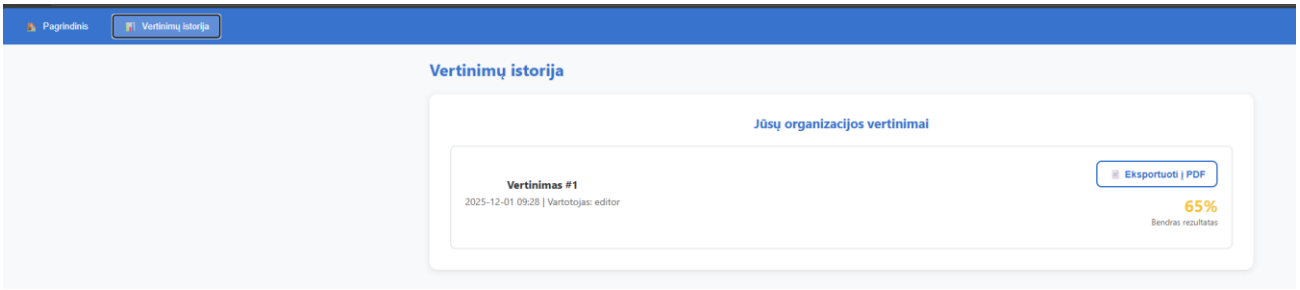

Visų organizacijų atliktų vertinimų peržiūra



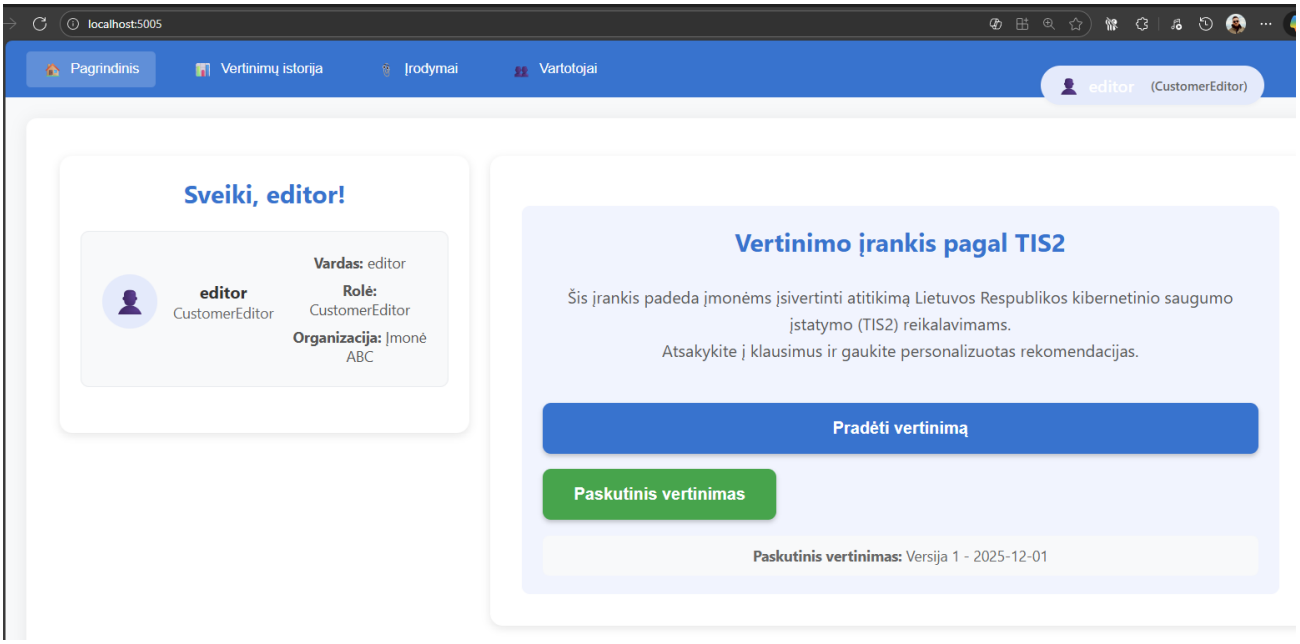
### Įrankio naudotojo READONLY naudojimo aplinka



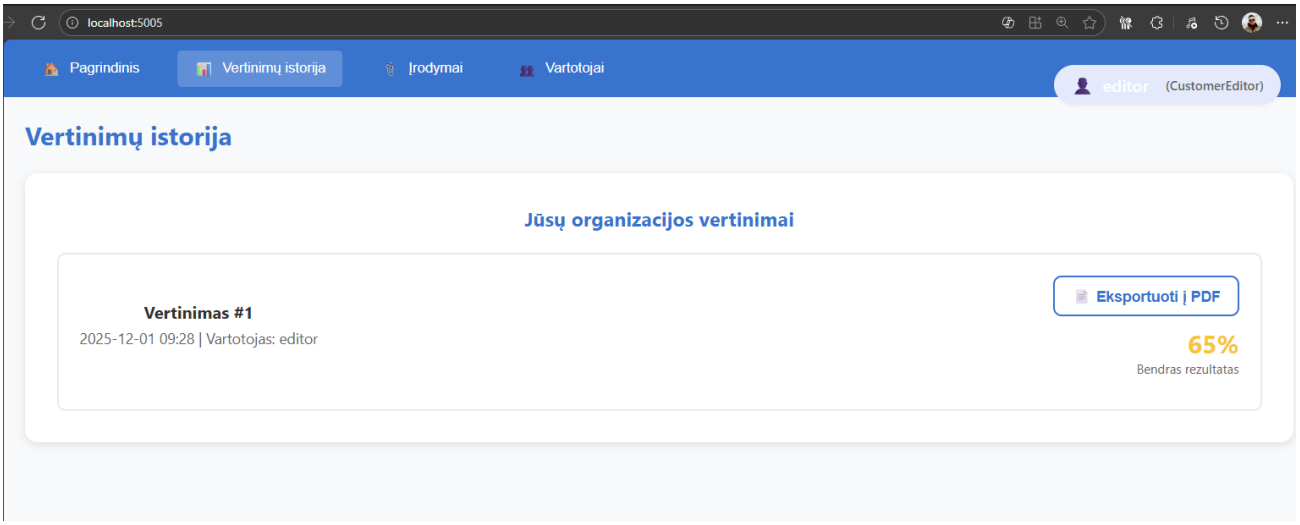

Organizacijos kuriai priklauso READONLY atlikto vertinimo peržiūra



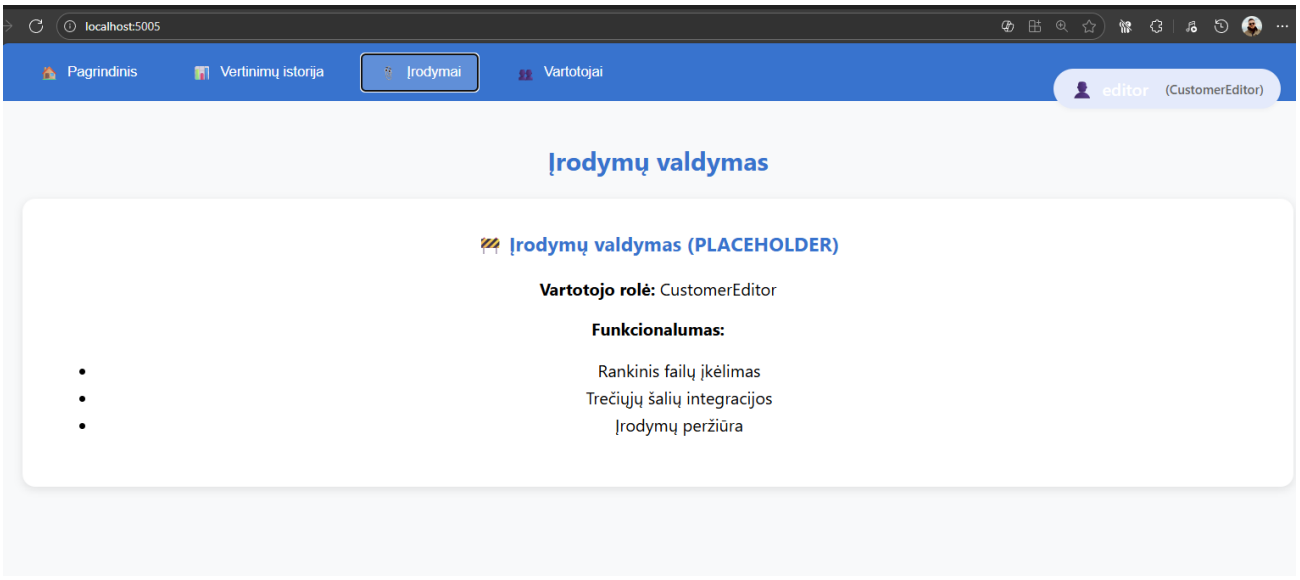

### Įrankio naudotojo EDITOR naudojimo aplinka



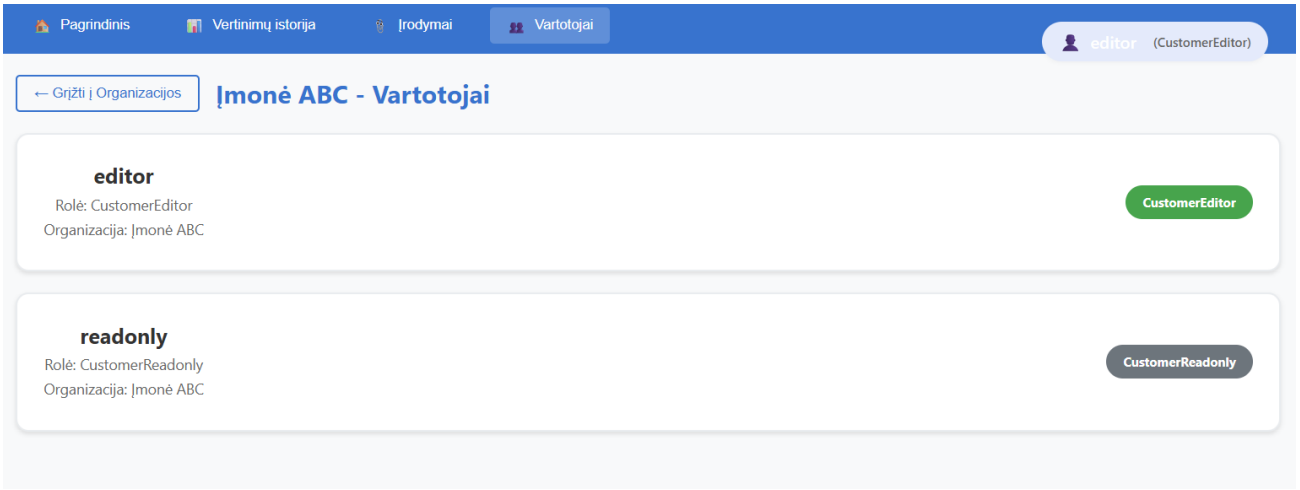

Vertinimo istorijos peržiūra



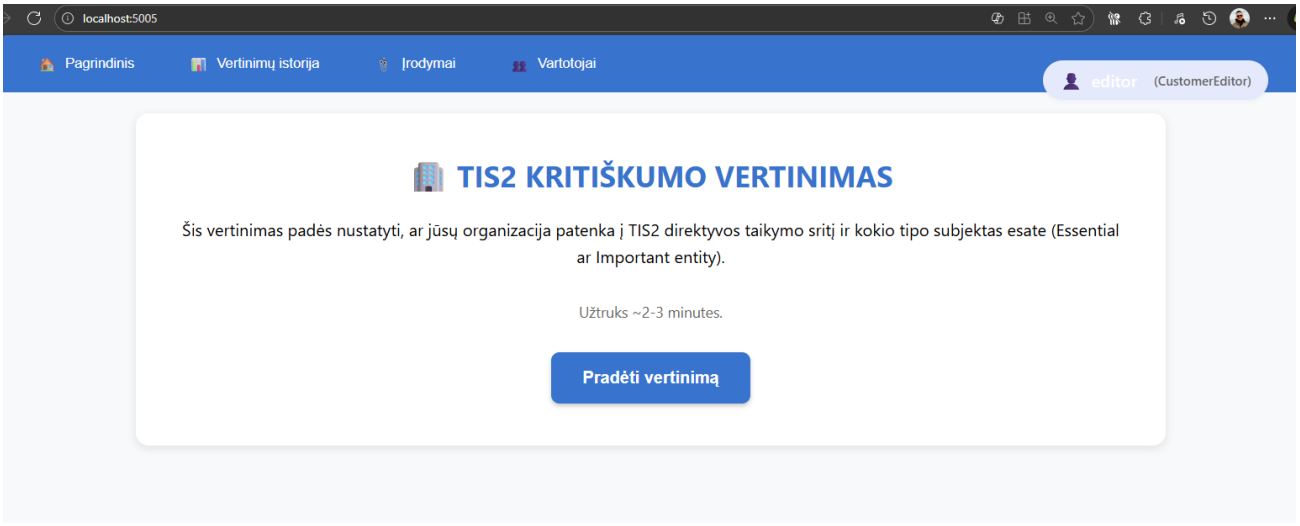

Atitikties įrodymų valdymas (konceptas, nerealizuota)

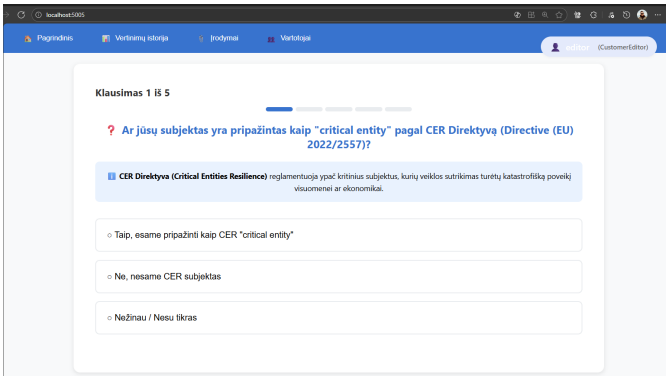


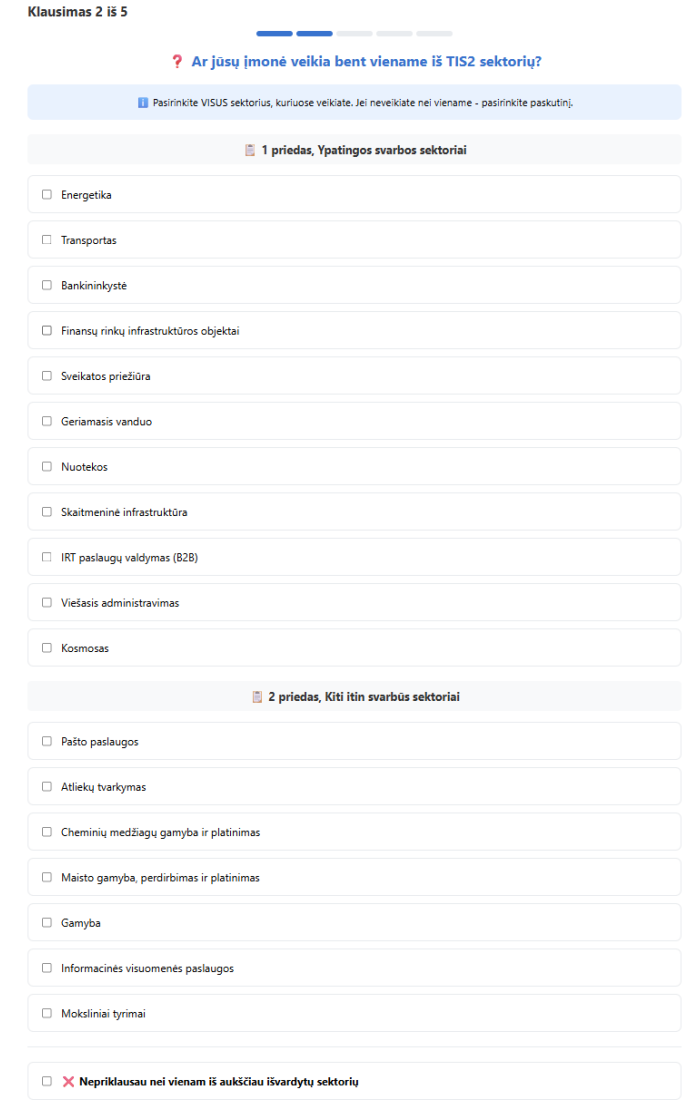

Organizacijos vartotojų valdymas (konceptas, nerealizuota)

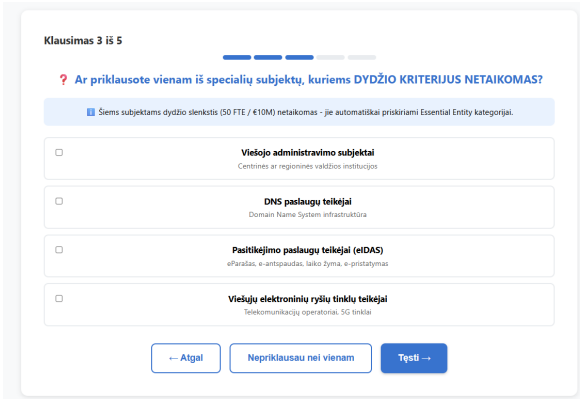


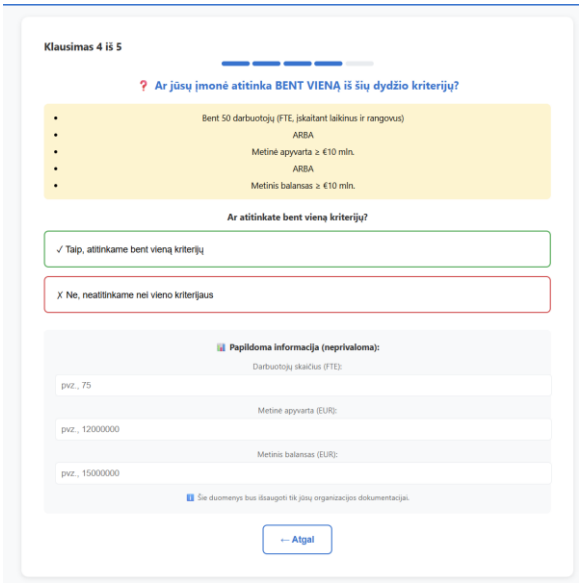
TIS2 kibernetinio saugumo statuso nustatymo klausimynas



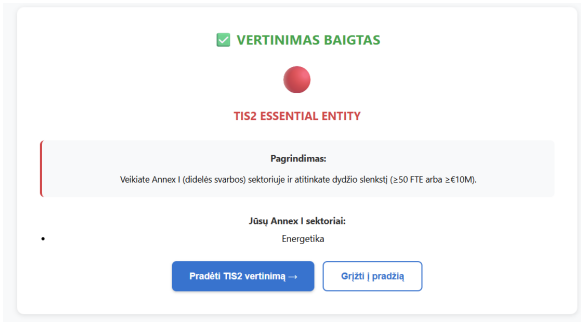




Klausimas 2 iš 5
❓ Ar jūsų įmonė veikia bent viename iš TIS2 sektorių?
ℹ️ Pasirinkite VISUS sektorius, kuriuose veikiate. Jei neveikiate nei viename - pasirinkite paskutinį.
📋 1 priedas, Ypatingos svarbos sektoriai
Energetika
Transportas
Bankininkystė
Finansų rinkų infrastruktūros objektai
Sveikatos priežiūra
Geriamasis vanduo
Nuotekos
Skaitmeninė infrastruktūra
IRT paslaugų valdymas (B2B)
Viešasis administravimas
Kosmosas
📋 2 priedas, Kiti itin svarbūs sektoriai
Pašto paslaugos
Atliekų tvarkymas
Cheminių medžiagų gamyba ir platinimas
Maisto gamyba, perdirbimas ir platinimas
Gamyba
Informacinės visuomenės paslaugos
Moksliniai tyrimai
❌ Nepriklausau nei vienam iš aukščiau išvardytų sektorių

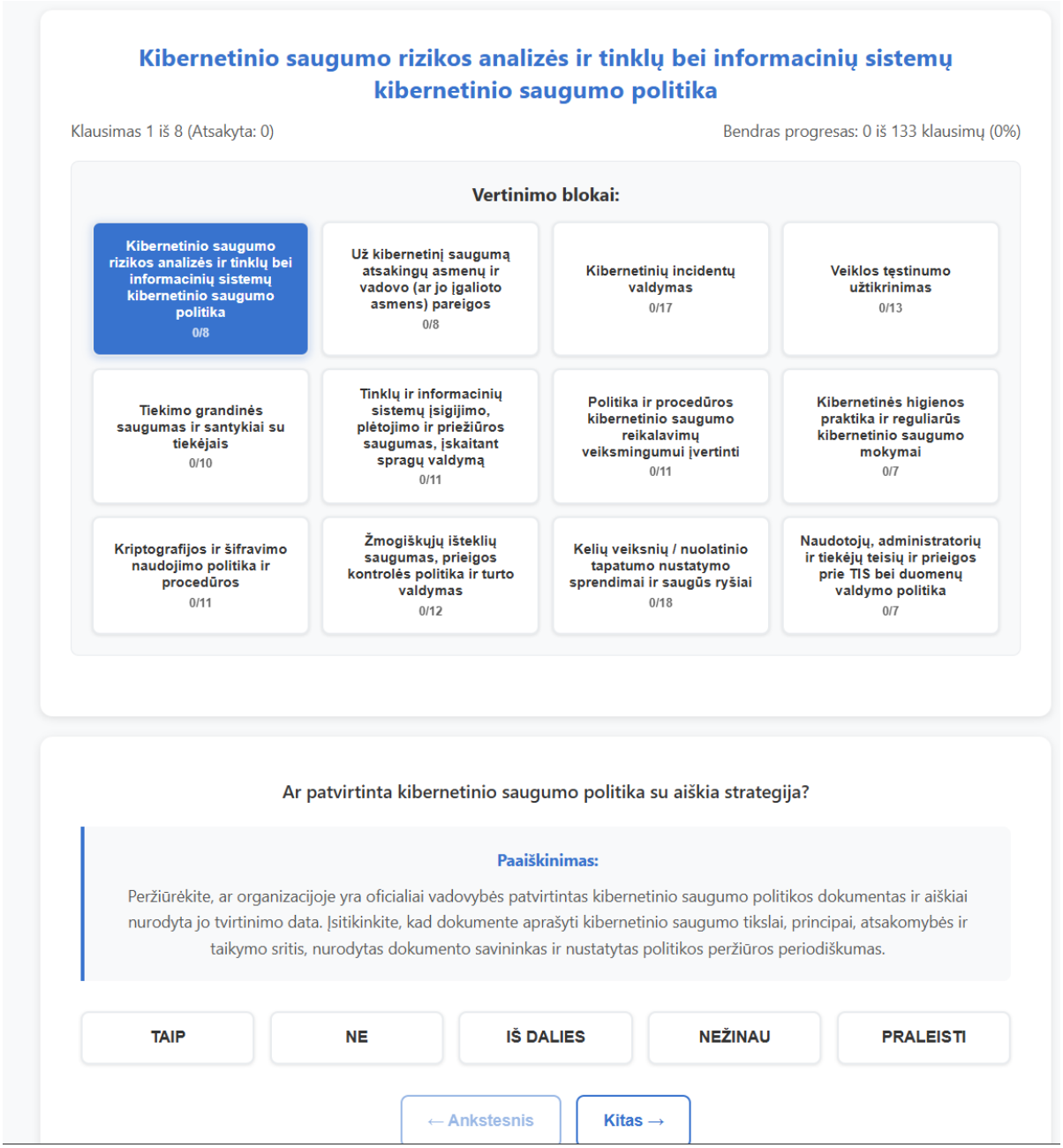

Klausimas 3 iš 5
❓ Ar priklausote vienam iš specialių subjektų, kuriems DYDŽIO KRITERIJUS NETAIKOMAS?
ℹ️ Šiems subjektams dydžio slenkstis (50 FTE / €10M) netaikomas - jie automatiškai priskiriami Essential Entity kategorijai.
Viešojo administravimo subjektai
Centrinės ar regioninės valdžios institucijos
DNS paslaugų teikėjai
Domain Name System infrastruktūra
Pasitikėjimo paslaugų teikėjai (eIDAS)
eParašas, e-antspaudas, laiko žyma, e-pristatymas
Viešųjų elektroninių ryšių tinklų teikėjai
Telekomunikacijų operatoriai, 5G tinklai
← Atgal
Nepriklausau nei vienam
Tęsti →




Kibernetinio saugumo vertinimo statuso nustatymo rezultatas



Adaptyvus atitikties vertinimo klausimynas, 12 blokų, 133 klausimai



Klausimas 1 iš 18 (Atsakyta: 0) Bendras progresas: 3 iš 133 klausimų (2%)

**Vertinimo blokai:**

| | | | |
|---|---|---|---|
| Kibernetinio saugumo rizikos analizės ir tinklų bei informacinių sistemų kibernetinio saugumo politika 3/8 | Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įgalioto asmens) pareigos 0/8 | Kibernetinių incidentų valdymas 0/17 | Veiklos tęstinumo užtikrinimas 0/13 |
| Tiekimo grandinės saugumas ir santykiai su tiekėjais 0/10 | Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas, įskaitant spragų valdymą 0/11 | Politika ir procedūros kibernetinio saugumo reikalavimų veiksmingumui įvertinti 0/11 | Kibernetinės higienos praktika ir reguliarūs kibernetinio saugumo mokymai 0/7 |
| Kriptografijos ir šifravimo naudojimo politika ir procedūros 0/11 | Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas 0/12 | **Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir saugūs ryšiai 0/18** | Naudotojų, administratorių ir tiekėjų teisių ir prieigos prie TIS bei duomenų valdymo politika 0/7 |

Ar įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS?

**Paaiškinimas:**

Peržiūrėkite atitinkamų tinklo ar sistemų konfigūracijos nustatymus ir patikrinkite, ar jie atitinka organizacijos kibernetinio saugumo reikalavimus. Įsitikinkite, kad taikomi tinkami šifravimo, autentifikavimo, filtravimo ar prieigos kontrolės nustatymai, o pakeitimai atliekami per pokyčių valdymo procesą.

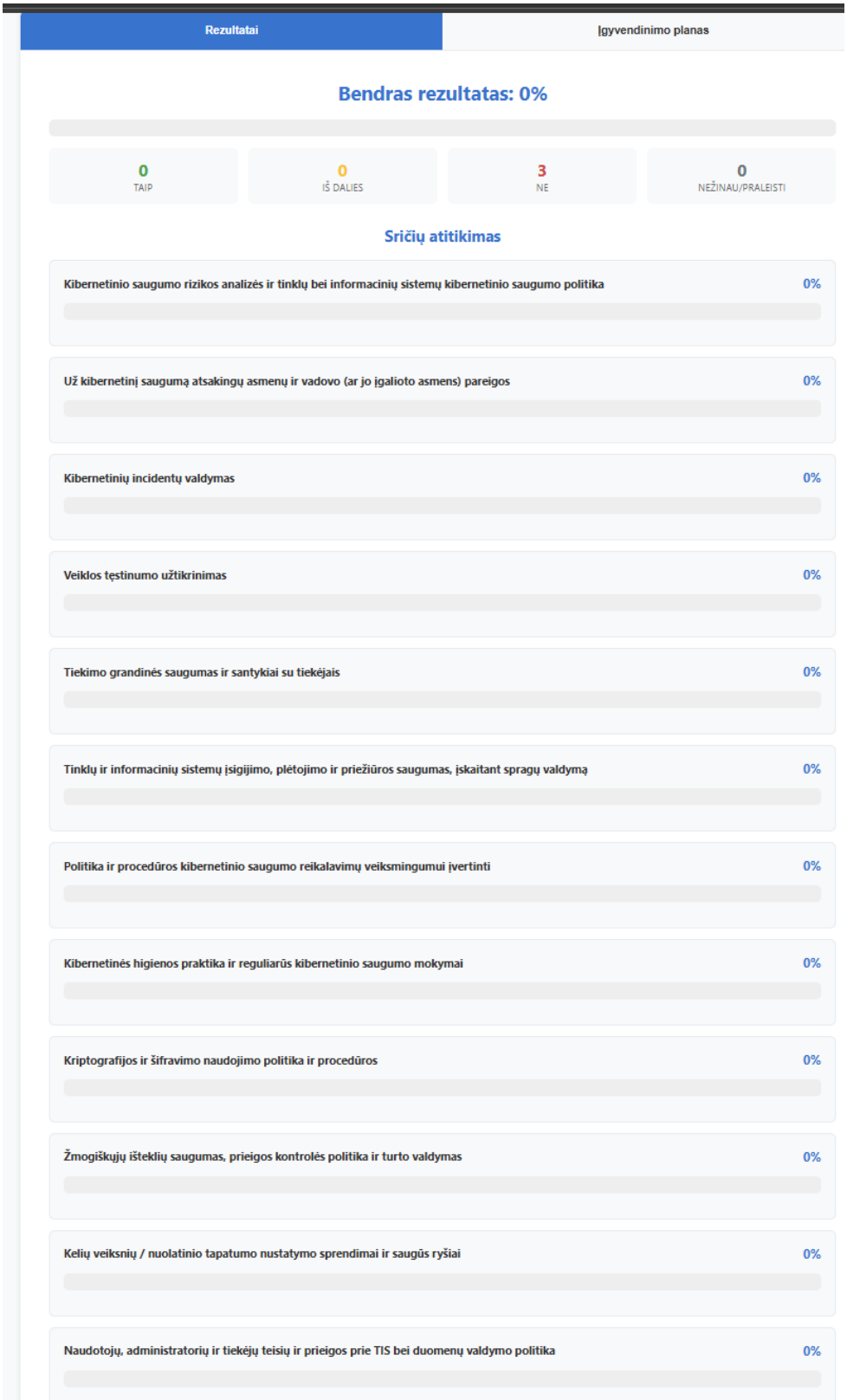
TAIP | NE | IŠ DALIES | NEŽINAU | PRALEISTI

← Ankstesnis | Kitas →

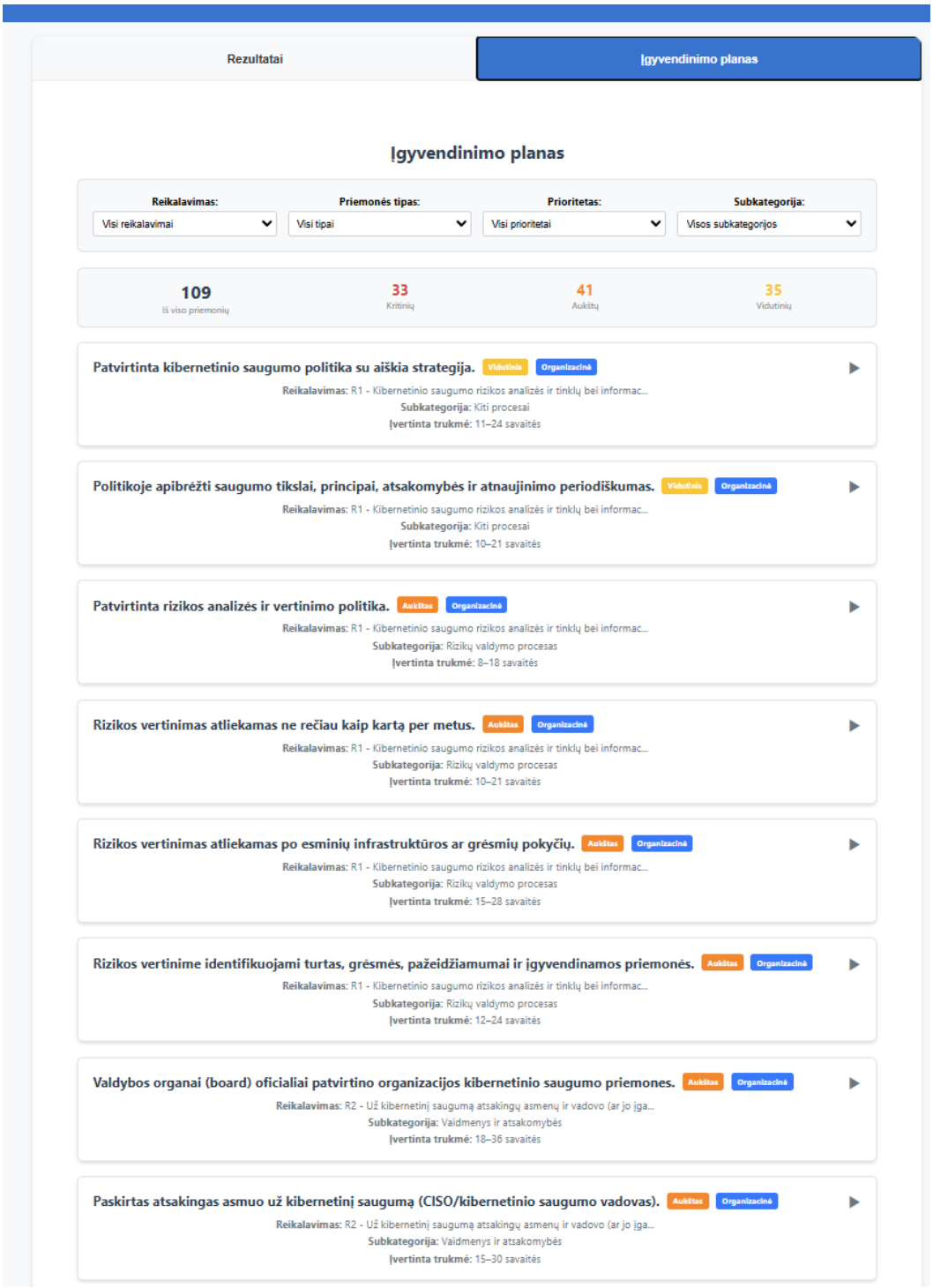
Pateikti vertinimą

Galite pateikti vertinimą bet kuriuo metu, net jei neatsakyta į visus klausimus

Atlikto vertinimo rezultatų pristatymas



Pagal atliktą vertinimą trūkumų šalinimo įgyvendinimo planas (pavyzdyje pateiktas pilnas planas)



**CISO funkcijos yra atskirtos nuo techninių IT administravimo funkcijų.** Aukštas Organizacinė

**Reikalavimas:** R2 - Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įga...
**Subkategorija:** Vaidmenys ir atsakomybės
**Įvertinta trukmė:** 10–21 savaitės

**Apie paskirtus atsakingus asmenis informuota NKSC ir organizacijos darbuotojai.** Aukštas Organizacinė

**Reikalavimas:** R2 - Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įga...
**Subkategorija:** Vaidmenys ir atsakomybės
**Įvertinta trukmė:** 12–24 savaitės

**Visi valdybos nariai PRIVALOMA TVARKA dalyvavo kibernetinio saugumo mokymuose.** Vidutinis Organizacinė

**Reikalavimas:** R2 - Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įga...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 18–36 savaitės

**Valdybos nariai suvokia savo asmeninę atsakomybę ir galimas sankcijas už NIS2 pažeidimus.** Vidutinis Organizacinė

**Reikalavimas:** R2 - Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įga...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 12–24 savaitės

**Organizacija užregistruota NKSC Kibernetinio saugumo informacinėje sistemoje.** Vidutinis Organizacinė

**Reikalavimas:** R2 - Už kibernetinį saugumą atsakingų asmenų ir vadovo (ar jo įga...
**Subkategorija:** Kiti procesai
**Įvertinta trukmė:** 10–21 savaitės

**Patvirtintas kibernetinių incidentų valdymo planas.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 15–30 savaitės

**Plane apibrėžti incidentų klasifikavimas, atsakomybės, komunikacijos tvarka.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Organizacija gali aptikti kibernetinius incidentus realiuoju laiku.** Kritinis Techninė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Audito įrašai (logs) renkami iš visų kritinių sistemų.** Kritinis Techninė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Audito įrašai saugomi ne trumpiau kaip teisės aktų reikalaujamą laikotarpį.** Kritinis Techninė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Žurnaliniai įrašai saugomi apsaugotai ir nekeičiami (integrity protection).** Kritinis Techninė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Reguliariai peržiūrimi įvykių žurnalai ir ieškoma anomalijų.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 10–21 savaitės

**Organizacija turi incidentų tyrimo (forensics) pajėgumus ar sutartį su teikėju.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Gali pateikti ANKSTYVĄ ĮSPĖJIMĄ (early warning) NKSC per 24 val. nuo reikšmingo incidento sužinojimo.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Gali pateikti INCIDENTO PRANEŠIMĄ su pirminiu vertinimu NKSC per 72 val.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Gali pateikti GALUTINĘ ATASKAITĄ per 1 mėn. nuo incidento pranešimo.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Informuojami paslaugų gavėjai apie incidentus, galinčius paveikti jų paslaugas.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Po incidentų atliekama giluminė analizė (lessons learned) ir tobulinami procesai.** Kritinis Organizacinė

**Reikalavimas:** R3 - Kibernetinių incidentų valdymas...
**Subkategorija:** Incidentų valdymo procesas
**Įvertinta trukmė:** 10–21 savaitės

**Patvirtintas veiklos tęstinumo ir atkūrimo (BCP/DRP) planas.** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Verslo tęstinumo valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Plane nustatyti RTO (Recovery Time Objective) ir RPO (Recovery Point Objective).** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Verslo tęstinumo valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Patvirtintas krizių valdymo planas (crisis management).** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Verslo tęstinumo valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Apibrėžta atsarginių kopijų kūrimo, saugojimo ir testavimo tvarka.** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Atsarginės kopijos kuriamos reguliariai ir automatizuotai.** Kritinis Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija.** Kritinis Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Atsarginės kopijos saugomos ATSKIROJE VIETOJE (offsite) su fizine/logine izoliacija.** Kritinis Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Atsarginės kopijos yra ŠIFRUOTOS.** Kritinis Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Reguliariai (bent 2x per metus) testuojamas duomenų atkūrimas iš atsarginių kopijų.** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Atsarginės kopijos ir atkūrimas
**Įvertinta trukmė:** 12–24 savaitės

**Kritinės IT sistemos yra dubliuotos (HA - high availability).** Aukštas Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Tinklo infrastruktūra
**Įvertinta trukmė:** 12–24 savaitės

**Esminės sistemos įdiegtos skirtingose geografinėse lokacijose (georedundancy).** Aukštas Techninė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Tinklo infrastruktūra
**Įvertinta trukmė:** 12–24 savaitės

**Atliekamos BCP/DRP pratybos (ne rečiau 1x per metus).** Kritinis Organizacinė

**Reikalavimas:** R4 - Veiklos tęstinumo užtikrinimas...
**Subkategorija:** Verslo tęstinumo valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Patvirtinta tiekimo grandinės saugumo politika.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Apibrėžti tiekėjų kibernetinio saugumo atrankos kriterijai.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Sutartyse su tiekėjais įtraukti kibernetinio saugumo reikalavimai.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Sutartyse numatyta incidentų pranešimo pareiga tiekėjams.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Sutartyse numatyta teisė audituoti tiekėjus.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 15–28 savaitės

**Tvarkomas kritinių tiekėjų ir paslaugų registras.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Vertinama tiekėjų keliama kibernetinio saugumo rizika.** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Rizikų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Organizacija atsižvelgia į ES koordinuotų tiekimo grandinės rizikos vertinimų rezultatus (Art. 22).** Aukštas Organizacinė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Rizikų valdymo procesas
**Įvertinta trukmė:** 8–18 savaitės

**Naudojamos automatizuotos tiekėjų rizikos valdymo platformos.** Aukštas Techninė

**Reikalavimas:** R5 - Tiekimo grandinės saugumas ir santykiai su tiekėjais / pasla...
**Subkategorija:** Tiekimo grandinės valdymas
**Įvertinta trukmė:** 21–36 savaitės

**Patvirtinta sistemų saugaus įsigijimo, plėtros ir priežiūros politika.** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 13–27 savaitės

**Naudojamas saugus programinės įrangos kūrimo ciklas (SDLC - Secure Development Lifecycle).** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 27–48 savaitės

**Nustatyta pokyčių valdymo (change management) tvarka.** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Kiti procesai
**Įvertinta trukmė:** 12–22 savaitės

**Pokyčiai testuojami prieš įdiegimą produkcinėje aplinkoje.** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 12–24 savaitės

**Tvarkomas turto ir programinės įrangos inventorius (asset inventory).** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Kiti procesai
**Įvertinta trukmė:** 19–35 savaitės

**Taikoma pataisų valdymo (patch management) tvarka.** Aukštas Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Rizikų valdymo procesas
**Įvertinta trukmė:** 18–34 savaitės

**Kritinės saugumo pataisy (security patches) diegiamos per nustatytą terminą (pvz. 30d).** Vidutinis Techninė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 10–19 savaitės

**Atliekamas pažeidžiamumų skanavimas (vulnerability scanning).** Vidutinis Techninė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 12–24 savaitės

**Yra pažeidžiamumų atskleidimo (vulnerability disclosure) procedūra.** Aukštas Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Rizikų valdymo procesas
**Įvertinta trukmė:** 12–24 savaitės

**Naudojama tik legali, licencijuota programinė įranga.** Vidutinis Organizacinė

**Reikalavimas:** R6 - Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priež...
**Subkategorija:** Kiti procesai
**Įvertinta trukmė:** 12–22 savaitės

**Metinis vidaus auditas atliekamas.** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 12–24 savaitės

**Po auditų parengiami neatitikčių šalinimo planai.** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 12–24 savaitės

**Atliekami išorės penetracijos testavimai.** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 13–27 savaitės

**Matuojami kibernetinio saugumo KPI (metrics).** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 13–27 savaitės

**Organizacija gali pateikti reikiamą dokumentaciją priežiūros institucijai per 24h.** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Procesų / žinių valdymas
**Įvertinta trukmė:** 12–24 savaitės

**Organizacija pasiruošusi NKSC vietinei inspekcijai (on-site).** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 10–21 savaitės

**Organizacija susipažinusi su įgyvendinimo terminais (12 mėn. org. / 24 mėn. tech.).** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Procesų / žinių valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Yra patvirtinta priemonių veiksmingumo vertinimo politika.** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 15–30 savaitės

**Apibrėžta auditų ir testavimų periodiškumas (vidaus/išorės).** Vidutinis Organizacinė

**Reikalavimas:** R7 - Politika ir procedūros kibernetinio saugumo reikalavimų veik...
**Subkategorija:** Atitikties vertinimas
**Įvertinta trukmė:** 9–18 savaitės

**Patvirtinta darbuotojų kibernetinio saugumo mokymų politika.** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 13–27 savaitės

**Visi darbuotojai praeina įvadinius kibernetinio saugumo mokymus.** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 12–24 savaitės

**Mokymai kartojami reguliariai (ne rečiau 1x per metus).** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 12–24 savaitės

**Organizuojamos kibernetinės higienos kampanijos (pvz. saugūs slaptažodžiai, phishing).** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 10–21 savaitės

**Atliekamos phishing simuliacijos darbuotojams.** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 15–28 savaitės

**Darbuotojai informuojami apie aktualias kibernetines grėsmes.** Vidutinis Organizacinė

**Reikalavimas:** R8 - Kibernetinės higienos praktika ir reguliarūs kibernetinio sa...
**Subkategorija:** Personalo mokymai
**Įvertinta trukmė:** 12–24 savaitės

**Patvirtinta kriptografijos ir šifravimo politika.** Aukštas Organizacinė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 11–24 savaitės

**Politikoje nurodyta leistinų kriptografinių algoritmų ir raktų ilgių politika.** Aukštas Organizacinė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 12–24 savaitės

**Nustatyta kriptografinių raktų valdymo tvarka.** Aukštas Organizacinė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 18–34 savaitės

**Duomenys šifruojami perdavimo metu (data in transit).** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 15–28 savaitės

**Duomenys šifruojami saugojimo metu (data at rest).** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 15–28 savaitės

**VPN ryšiai naudoja tvirtą šifravimą.** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 15–28 savaitės

**Belaidis tinklas (WiFi) naudoja WPA3 ar WPA2-Enterprise šifravimą.** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 12–24 savaitės

**Naudojami patikimų CA (Certificate Authority) sertifikatai.** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 12–24 savaitės

**Naudojamas automatizuotas sertifikatų valdymas (pvz. ACME).** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 13–25 savaitės

**Naudojami HSM (Hardware Security Modules) kritiniams raktams.** Aukštas Techninė

**Reikalavimas:** R9 - Kriptografijos ir šifravimo naudojimo politika ir procedūros...
**Subkategorija:** Kriptografija
**Įvertinta trukmė:** 13–25 savaitės

**Patvirtinta žmogiškųjų išteklių saugumo politika.** Vidutinis Organizacinė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Žmogiškųjų išteklių saugumas
**Įvertinta trukmė:** 16–33 savaitės

**Atliekami fono patikrinimai (background checks) jautrioms IT pareigybėms.** Vidutinis Organizacinė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Žmogiškųjų išteklių saugumas
**Įvertinta trukmė:** 12–24 savaitės

**Darbuotojai pasirašo konfidencialumo susitarimus (NDA).** Vidutinis Organizacinė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Žmogiškųjų išteklių saugumas
**Įvertinta trukmė:** 12–24 savaitės

**Patvirtinta turto valdymo politika.** Aukštas Organizacinė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Turto valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Turtas klasifikuojamas pagal svarbą ir jautrumą.** Aukštas Organizacinė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Turto valdymas
**Įvertinta trukmė:** 15–28 savaitės

**Fizinė prieiga prie serverių patalpų yra kontroliuojama.** Aukštas Techninė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Fizinė apsauga
**Įvertinta trukmė:** 13–25 savaitės

**Mobilieji įrenginiai valdomi centralizuotai (MDM).** Vidutinis Techninė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Mobilių įrenginių valdymas
**Įvertinta trukmė:** 15–28 savaitės

**Mobiliųjų įrenginių diskai yra šifruoti.** Vidutinis Techninė

**Reikalavimas:** R10 - Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir...
**Subkategorija:** Mobilių įrenginių valdymas
**Įvertinta trukmė:** 9–18 savaitės

**Įdiegta MFA (daugiakomponentė autentifikacija) PRIVILEGIJUOTOMS PASKYROMS.** Kritinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Prieigos valdymas
**Įvertinta trukmė:** 15–28 savaitės

**Įdiegta MFA NUOTOLINEI PRIEIGAI (VPN, RDP, web portals).** Kritinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Prieigos valdymas
**Įvertinta trukmė:** 13–25 savaitės

**Įdiegta MFA KRITINĖMS SISTEMOMS ir duomenų bazėms.** Kritinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Prieigos valdymas
**Įvertinta trukmė:** 13–25 savaitės

**Naudojamos saugios komunikacijos priemonės (secured voice, video, text).** Aukštas Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 16–29 savaitės

**Yra saugios avarinio ryšio sistemos.** Kritinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Verslo tęstinumo valdymas
**Įvertinta trukmė:** 10–21 savaitės

**Tinklas segmentuotas į saugumo zonas.** Aukštas Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo infrastruktūra
**Įvertinta trukmė:** 15–28 savaitės

**Naudojamos ugniasienės (firewalls) tarp segmentų.** Aukštas Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 15–28 savaitės

**Įdiegta endpoint apsauga (EDR/Antivirus).** Vidutinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Programinės įrangos saugumas
**Įvertinta trukmė:** 18–32 savaitės

**Naudojamas el. pašto saugumo sprendimas (anti-spam, anti-phishing).** Aukštas Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 18–32 savaitės

**Naudojamas web filtering / proxy sprendimas.** Aukštas Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 18–32 savaitės

**Tinklo įsibrovimų aptikimo/prevencijos sistema (IDS/IPS) veikia.** Kritinis Techninė

**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 15–26 savaitės

**Tinklo srautai stebimi (network monitoring).** Kritinis Techninė

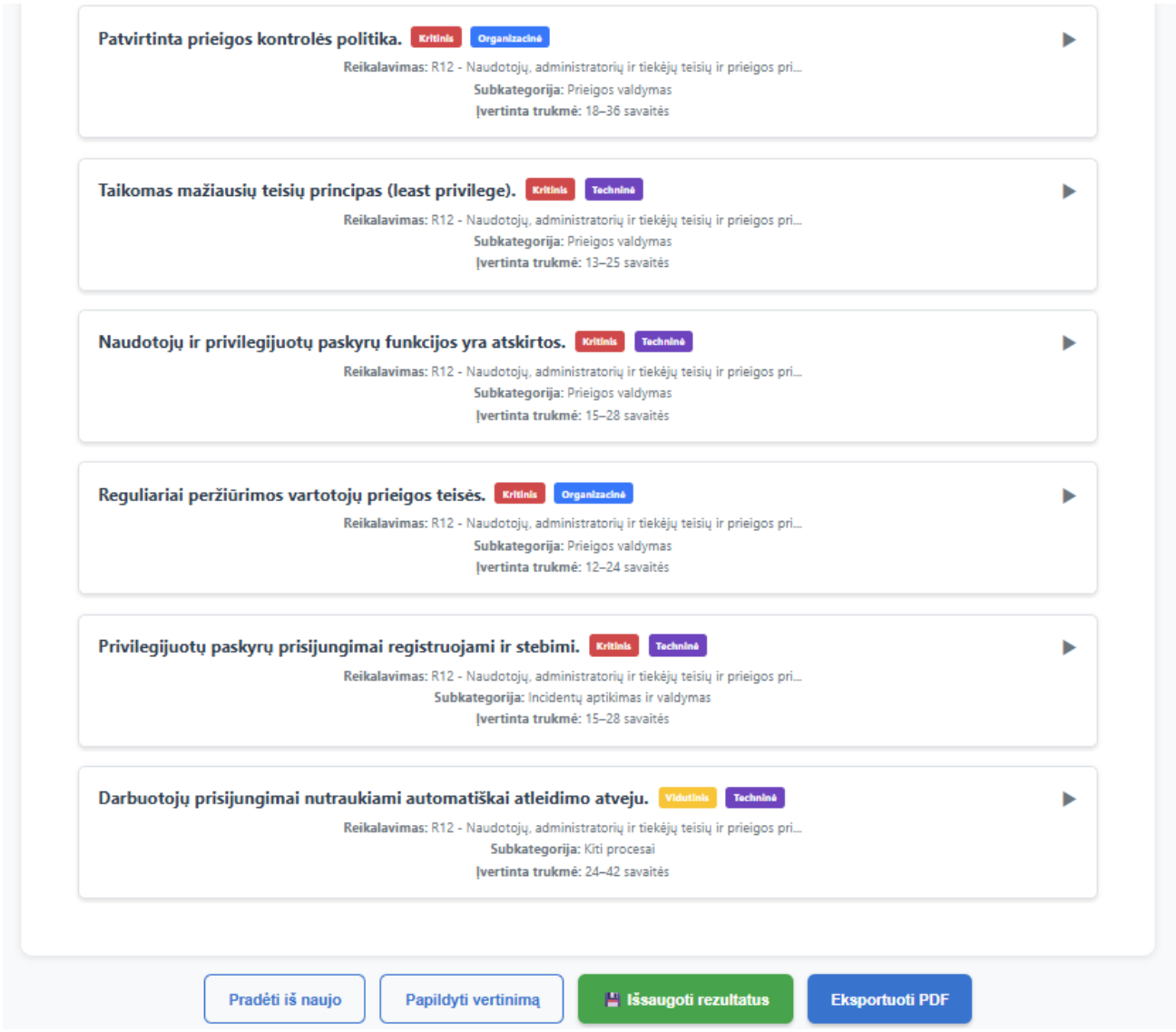
**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Incidentų aptikimas ir valdymas
**Įvertinta trukmė:** 15–26 savaitės

**Administratoriams prieiga vyksta per saugius protokolus (SSH, HTTPS, ne Telnet/HTTP).** Aukštas Techninė

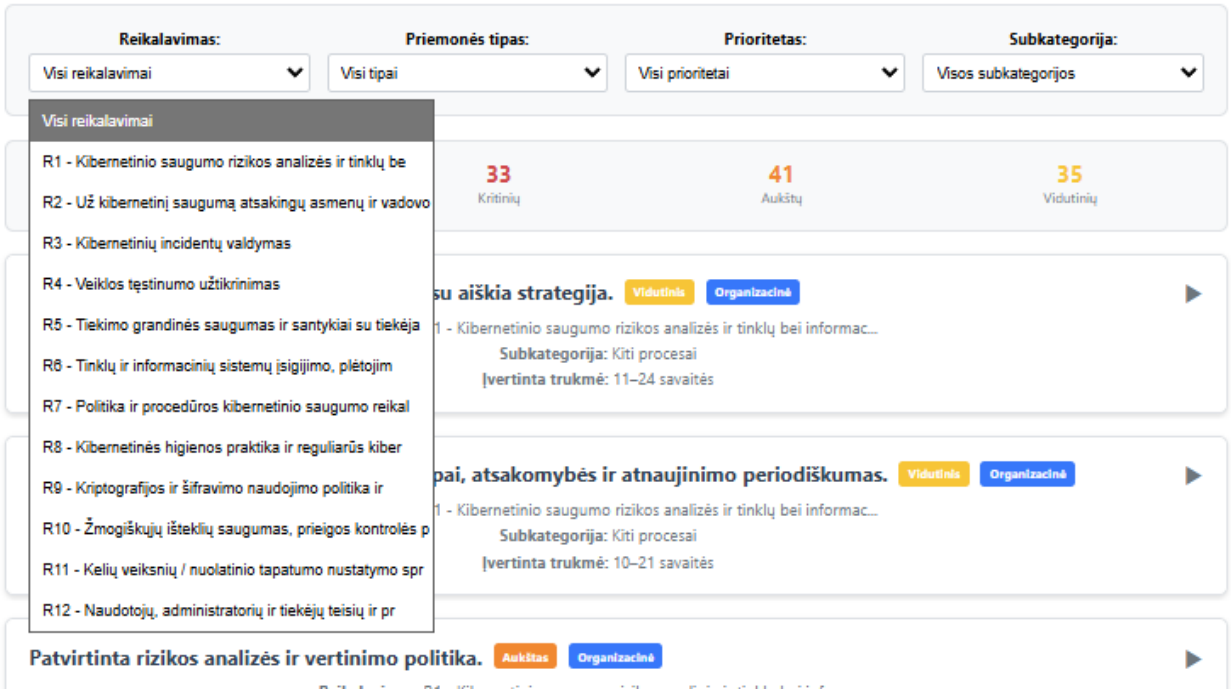
**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 15–28 savaitės

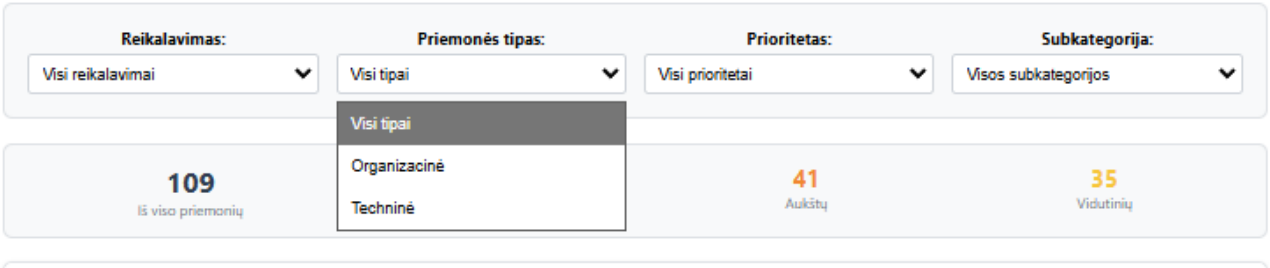
**Debesijos (cloud) prieiga yra kontroliuojama ir stebima.** Aukštas Techninė

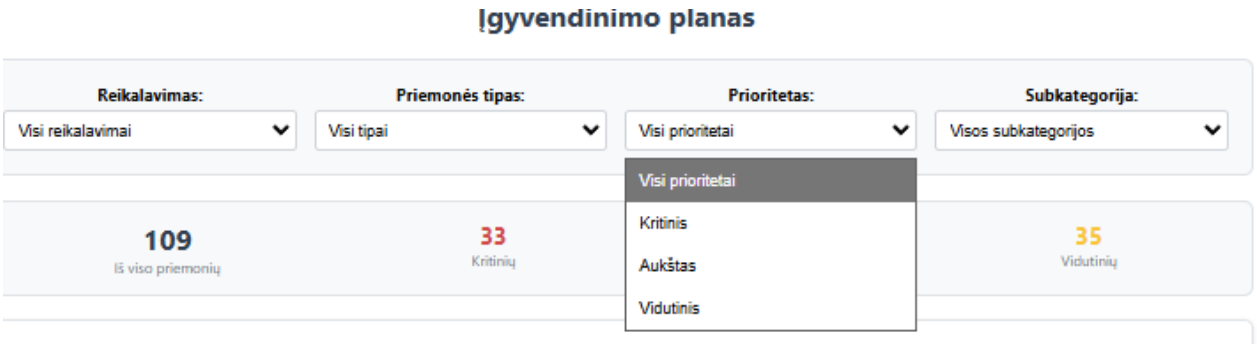
**Reikalavimas:** R11 - Kelių veiksnių / nuolatinio tapatumo nustatymo sprendimai ir...
**Subkategorija:** Tinklo saugumas
**Įvertinta trukmė:** 15–28 savaitės

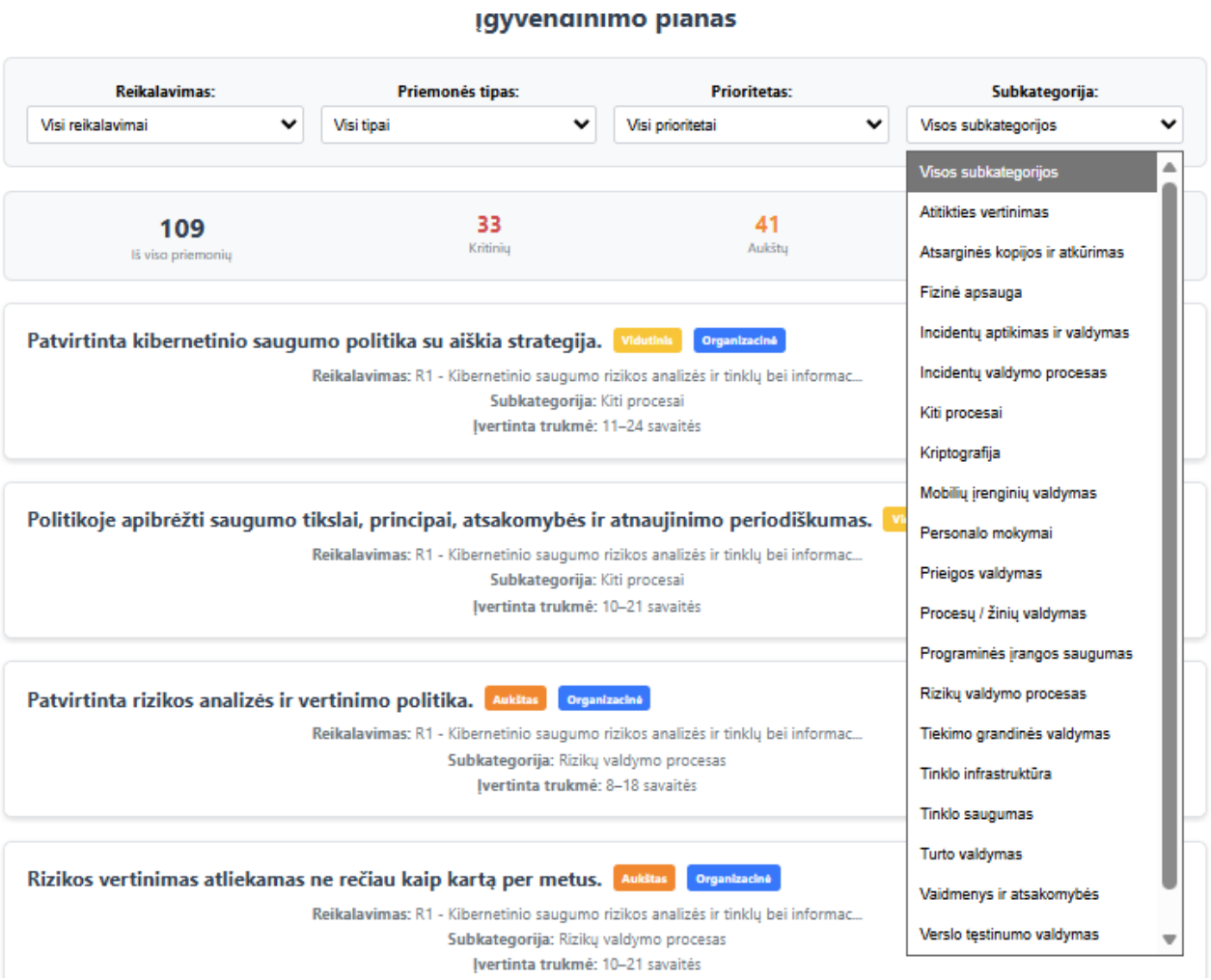

Patvirtinta prieigos kontrolės politika. Kritinis Organizacinė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Prieigos valdymas
Įvertinta trukmė: 18–36 savaitės
Taikomas mažiausių teisių principas (least privilege). Kritinis Techninė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Prieigos valdymas
Įvertinta trukmė: 13–25 savaitės
Naudotojų ir privilegijuotų paskyrų funkcijos yra atskirtos. Kritinis Techninė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Prieigos valdymas
Įvertinta trukmė: 15–28 savaitės
Reguliariai peržiūrimos vartotojų prieigos teisės. Kritinis Organizacinė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Prieigos valdymas
Įvertinta trukmė: 12–24 savaitės
Privilegijuotų paskyrų prisijungimai registruojami ir stebimi. Kritinis Techninė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Incidentų aptikimas ir valdymas
Įvertinta trukmė: 15–28 savaitės
Darbuotojų prisijungimai nutraukiami automatiškai atleidimo atveju. Vidutinis Techninė
Reikalavimas: R12 - Naudotojų, administratorių ir tiekėjų teisių ir prieigos pri...
Subkategorija: Kiti procesai
Įvertinta trukmė: 24–42 savaitės
Pradėti iš naujo
Papildyti vertinimą
Išsaugoti rezultatus
Eksportuoti PDF

Įgyvendinimo plano filtravimo funkcionalumas




Įgyvendinimo planas
Reikalavimas:
Visi reikalavimai
Priemonės tipas:
Visi tipai
Prioritetas:
Visi prioritetai
Subkategorija:
Visos subkategorijos
109
Iš viso priemonių
33
Kritinių
41
Aukštų
Patvirtinta kibernetinio saugumo politika su aiškia strategija.
Vidutinis
Organizacinė
Reikalavimas: R1 - Kibernetinio saugumo rizikos analizės ir tinklų bei informac...
Subkategorija: Kiti procesai
Įvertinta trukmė: 11–24 savaitės
Politikoje apibrėžti saugumo tikslai, principai, atsakomybės ir atnaujinimo periodiškumas.
Reikalavimas: R1 - Kibernetinio saugumo rizikos analizės ir tinklų bei informac...
Subkategorija: Kiti procesai
Įvertinta trukmė: 10–21 savaitės
Patvirtinta rizikos analizės ir vertinimo politika.
Aukštas
Organizacinė
Reikalavimas: R1 - Kibernetinio saugumo rizikos analizės ir tinklų bei informac...
Subkategorija: Rizikų valdymo procesas
Įvertinta trukmė: 8–18 savaitės
Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus.
Aukštas
Organizacinė
Reikalavimas: R1 - Kibernetinio saugumo rizikos analizės ir tinklų bei informac...
Subkategorija: Rizikų valdymo procesas
Įvertinta trukmė: 10–21 savaitės
Visos subkategorijos
Atitikties vertinimas
Atsarginės kopijos ir atkūrimas
Fizinė apsauga
Incidentų aptikimas ir valdymas
Incidentų valdymo procesas
Kiti procesai
Kriptografija
Mobilių įrenginių valdymas
Personalo mokymai
Prieigos valdymas
Procesų / žinių valdymas
Programinės įrangos saugumas
Rizikų valdymo procesas
Tiekimo grandinės valdymas
Tinklo infrastruktūra
Tinklo saugumas
Turto valdymas
Vaidmenys ir atsakomybės
Verslo tęstinumo valdymas

Vienos priemonės įgyvendinimo detalizacija veiksmais ir žingsniais

**Patvirtinta kibernetinio saugumo politika su aiškia strategija.** Vidutinis Organizacinė

**Reikalavimas:** R1 - Kibernetinio saugumo rizikos analizės ir tinklų bei informac...
**Subkategorija:** Kiti procesai
**Įvertinta trukmė:** 11–24 savaitės

**Veiksmas 1: Parengti ir patvirtinti kibernetinio saugumo politikos dokumentą**
Sukurti kibernetinio saugumo politikos dokumentą, kuris apibrėžia organizacijos požiūrį į kibernetin...

Sukurti kibernetinio saugumo politikos dokumentą, kuris apibrėžia organizacijos požiūrį į kibernetinį saugumą ir pagrindinius įsipareigojimus.

**Žingsnis 1: Surinkti taikomų teisės aktų ir standartų reikalavimus.**

| Trukmė: | Atsakingas: | Dalyvaujantys: | Priklausomybės: |
|---|---|---|---|
| 3–6 savaitės | Informacinio saugumo vadovas | IT (Information Technology, informacinės technologijos), Teisė, Verslas, Rizikų valdymas | Nėra, pradinė veikla. |

| Rezultato rodiklis: | Sprendimo klasė: | Pavyzdžiai: |
|---|---|---|
| Parengtas kibernetinio saugumo politikos projekto dokumentas. | Dokumentų / žinių valdymas | Confluence, SharePoint, dokumentų valdymo sistema |

**Žingsnis 2: Parengti politikos struktūrą (taikymo sritis, tikslai, principai, vaidmenys, ryšys su kitomis politikomis).**

| Trukmė: | Atsakingas: | Dalyvaujantys: | Priklausomybės: |
|---|---|---|---|
| 3–6 savaitės | Informacinio saugumo vadovas | IT (Information Technology, informacinės technologijos), Rizikų valdymas | Surinkti reikalavimai politikos turiniui. |

| Rezultato rodiklis: | Sprendimo klasė: | Pavyzdžiai: |
|---|---|---|
| Politikos dokumentas turi visus numatytus struktūrinius skyrius. | Dokumentų / žinių valdymas | Confluence šablonai, Word / O365 |

**Žingsnis 3: Suderinti politikos projektą su suinteresuotomis šalimis ir pateikti tvirtinti vadovybei / valdybai.**

| Trukmė: | Atsakingas: | Dalyvaujantys: | Priklausomybės: |
|---|---|---|---|
| 3–6 savaitės | Informacinio saugumo vadovas | Vadovybė, Teisė | Parengtas ir suderintas politikos projektas. |

| Rezultato rodiklis: | Sprendimo klasė: | Pavyzdžiai: |
|---|---|---|
| Patvirtinta kibernetinio saugumo politika su tvirtinimo data. | Valdymo ir sprendimų priėmimo procesas | Valdybos posėdžio medžiaga, sprendimo protokolas |

**Veiksmas 2: Įdiegti politikos komunikavimo ir prieinamumo mechanizmą**
Užtikrinti, kad kibernetinio saugumo politika būtų lengvai pasiekiama ir žinoma visiems darbuotojams...

Užtikrinti, kad kibernetinio saugumo politika būtų lengvai pasiekiama ir žinoma visiems darbuotojams.

**Žingsnis 1: Publikuoti patvirtintą politiką vidinėje žinių bazėje ar intranete.**

| Trukmė: | Atsakingas: | Dalyvaujantys: | Priklausomybės: |
|---|---|---|---|
| 1–3 savaitės | Informacinio saugumo vadovas | IT (Information Technology, informacinės technologijos), Komunikacija, HR (Human Resources, žmogiškieji ištekliai) | Politika turi būti patvirtinta. |

| Rezultato rodiklis: | Sprendimo klasė: | Pavyzdžiai: |
|---|---|---|
| Politika pasiekiama visiems darbuotojams vienoje centralizuotoje vietoje. | Intranetas / žinių bazė | SharePoint, Confluence, vidinis portalas |

**Žingsnis 2: Informuoti darbuotojus apie naują / atnaujintą politiką el. paštu ar per vidines komunikacijos priemones.**

| Trukmė: | Atsakingas: | Dalyvaujantys: | Priklausomybės: |
|---|---|---|---|
| 1–3 savaitės | Komunikacijos vadovas | CISO (Chief Information Security Officer, informacijos saugos vadovas), HR (Human Resources, žmogiškieji ištekliai) | Politika paskelbta intranete. |

| Rezultato rodiklis: | Sprendimo klasė: | Pavyzdžiai: |
|---|---|---|
| >80 % darbuotojų patvirtina susipažinimą su politika. | Vidinė komunikacija | MS (Microsoft, „Microsoft" technologijos ar paslaugos) Teams, el. paštas, naujienlaiškis |

## 7. TIS2 vertinimo įrankio programinio kodo pavyzdžiai

Priede pateikiamos TIS2 atitikties vertinimo įrankio programinio kodo ištraukos ir trumpi paaiškinimai. Priedas skirtas parodyti, kaip teoriniai reikalavimai buvo perkelti į praktinį sprendimą. Programinės įrangos tikslas – pademonstruoti vertinimo įrankio koncepcijos funkcionavima, bet ne pačių pasirinktų technologijų ypatumų, trukumų arba privalomų, šiame projekto etape yra atsiribojama nuo technologinio koncepcijos rengimo priemonių parinkimo ir įgyvendinimo metodikos analizės ir vertinimo.

Aplikacija realizuota naudojant **React** ir **TypeScript**, duomenys saugomi naršyklės **localStorage**, o rezultatai naudotojui pateikiami per interaktyvią vieno puslapio aplikaciją (SPA).

TIS2 atitikties vertinimo įrankis sukurtas laikantis šių esminių principų:

1. Komponentinė architektūra: naudotojo kelias suskaidytas į atskirus modulius (kritiškumo nustatymas, klausimynas, įgyvendinimo planas), kurie bendrauja per aiškiai apibrėžtus duomenų modelius.
2. Būsenos valdymas React Hooks pagalba: useState ir useMemo panaudoti tiek paprastam UI valdymui, tiek sudėtingesniems skaičiavimams (filtravimui, istorijos tvarkymui).
3. Tipų saugumas: TypeScript užtikrina, kad vartotojų rolės, vertinimo rezultatai, klausimų blokai ir įgyvendinimo priemonės būtų tvarkomi nuosekliai ir tipiškai teisingai.
4. Naudojimo logikos atskyrimas: TIS2 klasifikacijos algoritmas, trūkumų analizė ir įgyvendinimo plano generavimas realizuoti atskiromis funkcijomis, kurias būtų galima testuoti ir keisti nepriklausomai nuo UI.
5. Praktinis taikomumas: įgyvendinimo plano struktūra su metaduomenimis, gamintojų pavyzdžiais, procesiniais žingsniais ir kt. detalėmis leidžia įrankį naudoti ne tik vertinimui, bet ir kaip konkrečių veiksmų planą organizacijai.

Pagrindinės išorinės priklausomybės.

```
// Failas: frontend-v5/package.json (ištrauka)
{
  "dependencies": {
    "react": "^19.1.0",
    "react-dom": "^19.1.0",
    "react-scripts": "5.0.1",
    "typescript": "^4.9.5",
    "html2canvas": "^1.4.1",
    "jspdf": "^3.0.1",
    "@testing-library/react": "^16.3.0",
    "@testing-library/jest-dom": "^6.6.3",
    "web-vitals": "^2.1.4"
```

```
  }
}
```

React ir React DOM – komponentų bazė ir renderinimas;

TypeScript – tipų sistema ir kodo kokybės užtikrinimas;

React Scripts – build ir vystymo aplinka (Create React App);

jsPDF ir html2canvas – PDF generavimui iš HTML turinio;

Testing Library – komponentų testavimui.

**Aplikacijos struktūra**

Pagrindiniame komponente App.tsx apibrėžiami tipai, bendras vertinimo rezultato modelis ir jungiami moduliai (kritiškumo vertinimas, klausimynas, įgyvendinimo planas, rezultatų saugojimas).

frontend-v5/src/App.tsx

```
import React, { useState, useEffect, useCallback } from 'react';
import './App.css';
import { QUESTION_BLOCKS, QuestionBlock, Question } from './questions';
import jsPDF from 'jspdf';
import html2canvas from 'html2canvas';
import Recommendations from './components/Recommendations';
import ImplementationPlan from './components/ImplementationPlan';
import NIS2CriticalityForm from './components/NIS2CriticalityForm';
import { RecommendationPriority } from './recommendations';
import { ImplementationType } from './implementation-details';
```

Vartotojų rolėms naudojamas **TypeScript** tipų modelis (UserRole, User, AssessmentResult) užtikrina tipų saugumą, sistemoje numatytos keturios vartotojų rolės

```
type UserRole = 'SuperAdmin' | 'Auditorius' | 'CustomerEditor' | 'CustomerReadonly';
interface User {
  username: string;
  role: UserRole;
  organization?: string;
}
```

Vertinimo rezultato struktūra AssessmentResult struktūra saugo visą vieno vertinimo būseną: organizacijos kritiškumą, atsakymus į klausimus, bendrą ir blokų balus, vertinimo versiją ir laiką.

```
interface AssessmentResult {
  id: string;
  userId: string;
  organization: string;
  timestamp: string;
```

```
  version: number;
  criticality: {
    sector: string;
    employees: string;
    criticalInfra: string;
    nis2Classification?: 'essential' | 'important' | 'not_applicable';
    nis2Data?: NIS2CriticalityData;
  };
  answers: { [questionId: string]: string };
  score: number;
  blockResults: Array<{
    id: string;
    title: string;
    score: number;
    total: number;
  }>;
}
```

Aplikacija užkraunama standartiniu React paleidimo būdu index.tsx. naudojamas modernus **React 18** createRoot API, komponentas App renderinamas į DOM elementą root, kuris tampa visos SPA aplikacijos konteineriu.

```
// Failas: frontend-v5/src/index.tsx
import React from 'react';
import ReactDOM from 'react-dom/client';
import './index.css';
import App from './App';
import reportWebVitals from './reportWebVitals';

const root = ReactDOM.createRoot(
  document.getElementById('root') as HTMLElement
);

root.render(
  <React.StrictMode>
    <App />
  </React.StrictMode>
);
```

```
reportWebVitals();
```

**TIS2 kritiškumo vertinimo modulis**

Kritiškumo vertinimo modulis realizuoja žingsninį (wizard) procesą, kurio tikslas nustatyti, ar organizacija patenka į **Essential**, **Important** ar **not applicable** kategoriją pagal TIS2 direktyvą. NIS2CriticalityForm atsakingas už naudotojo „apklausą“ dėl sektoriaus, specialaus subjekto statuso, dydžio kriterijų ir specifinės reikšmės.

```
// Failas: frontend-v5/src/components/NIS2CriticalityForm.tsx

const NIS2CriticalityForm: React.FC<NIS2CriticalityFormProps> = ({

  onComplete,

  ANNEX_I_SECTORS,

  ANNEX_II_SECTORS,

  SPECIAL_ENTITIES,

  SPECIFIC_SIGNIFICANCE,

  calculateClassification

}) => {

  const [step, setStep] = useState<0 | 1 | 2 | 3 | 4>(0);

  const [data, setData] = useState<NIS2CriticalityData>({});

  const [result, setResult] = useState<NIS2CriticalityData | null>(null);

  const [showIntro, setShowIntro] = useState<boolean>(true);


  // Q1 – sektoriai

  const [selectedSectors, setSelectedSectors] = useState<string[]>([]);

  // Q2 – specialūs subjektai

  const [selectedSpecialEntities, setSelectedSpecialEntities] = useState<string[]>([]);

  // Q3 – dydžio kriterijai

  const [employees, setEmployees] = useState<string>('');

  const [revenue, setRevenue] = useState<string>('');

  const [balance, setBalance] = useState<string>('');

  // Q4 – specifinė reikšmė

  const [selectedSignificance, setSelectedSignificance] = useState<string[]>([]);


  const ALL_SECTORS = [...ANNEX_I_SECTORS, ...ANNEX_II_SECTORS];


  // Q0: CER kritinis subjektas

  const handleQ0 = (answer: 'yes' | 'no' | 'unknown') => {

    const newData = { ...data, q0_cerCriticalEntity: answer };
```

```
  if (answer === 'yes') {
    const finalResult = calculateClassification(newData);
    setResult(finalResult);
  } else {
    setData(newData);
    setStep(1);
  }
};

// Q1: Sektoriai
const handleQ1Submit = () => {
  const newData = { ...data, q1_nis2Sectors: selectedSectors };

  if (selectedSectors.includes('none') || selectedSectors.length === 0) {
    const finalResult = calculateClassification(newData);
    setResult(finalResult);
  } else {
    setData(newData);
    setStep(2);
  }
};

// Q2: Specialus subjektas
const handleQ2Submit = (answer: 'yes' | 'no') => {
  const newData = {
    ...data,
    q2_specialEntity: answer,
    q2_specialEntityTypes: answer === 'yes' ? selectedSpecialEntities : []
  };

  if (answer === 'yes') {
    const finalResult = calculateClassification(newData);
    setResult(finalResult);
  } else {
    setData(newData);
    setStep(3);
```

```
  }
};

// Q3: Dydžio slenkstis
const handleQ3Submit = (meetsThreshold: 'yes' | 'no') => {
  const details = meetsThreshold === 'yes' ? {
    employees: employees ? parseInt(employees) : undefined,
    revenue: revenue ? parseInt(revenue) : undefined,
    balance: balance ? parseInt(balance) : undefined
  } : undefined;

  const newData = { ...data, q3_meetsSizeThreshold: meetsThreshold, q3_details: details };

  if (meetsThreshold === 'no') {
    const finalResult = calculateClassification(newData);
    setResult(finalResult);
    return;
  }

  const hasAnnexI = newData.q1_nis2Sectors?.some(sectorId =>
    ANNEX_I_SECTORS.some(ai => ai.id === sectorId)
  );

  if (hasAnnexI) {
    const finalResult = calculateClassification(newData);
    setResult(finalResult);
  } else {
    setData(newData);
    setStep(4);
  }
};

// Q4: Specifinė reikšmė
const handleQ4Submit = () => {
  const newData = { ...data, q4_specificSignificance: selectedSignificance };
  const finalResult = calculateClassification(newData);
```

```
  setResult(finalResult);
 };
```

Svarbiausi bruožai:

- naudojamas **žingsnis po žingsnio** metodas (Q0–Q4);
- kiekvienam žingsniui palaikoma atskira būsena (useState), o rezultatas skaičiuojamas tik tada, kai surenkama pakankamai duomenų;
- funkcija calculateClassification atskiria verslo logiką (teisines taisykles) nuo pateikimo logikos.

**TIS2 kibernetinio saugumo subjekto statuso  klasifikacijos algoritmas**

Klasifikacijos algoritmas realizuotas kaip atskira funkcija calculateNIS2Classification, kuri nuosekliai pritaiko direktyvos kriterijus.

```
// Failas: frontend-v5/src/App.tsx
const calculateNIS2Classification = (data: NIS2CriticalityData): NIS2CriticalityData => {
 // Q0: CER kritinis subjektas
 if (data.q0_cerCriticalEntity === 'yes') {
  return {
   ...data,
   classification: 'essential',
   reason: 'CER Directive kritiniai subjektai automatiškai priskiriami prie Essential Entity kategorijos pagal TIS2 direktyvos 21 straipsnio 2 dalį, nepriklausomai nuo organizacijos dydžio ar veiklos sektoriaus.'
  };
 }

 // Q1: Sektorius
 if (!data.q1_nis2Sectors || data.q1_nis2Sectors.length === 0 || data.q1_nis2Sectors.includes('none')) {
  return {
   ...data,
   classification: 'not_applicable',
   reason: 'Jūsų organizacija neveikia nei viename iš TIS2 direktyvos I ar II priede nurodytų sektorių, todėl TIS2 reikalavimai jums netaikomi.'
  };
 }

 // Q2: Specialus subjektas
 if (data.q2_specialEntity === 'yes') {
  return {
   ...data,
```

```
    classification: 'essential',
    reason: 'Esate specialus subjektas (DNS / eIDAS / Telco / Viešas administravimas), kuriam dydžio kriterijus netaikomas pagal TIS2 direktyvos 2 straipsnio 2 dalį.'
   };
  }

  // Q3: Dydžio slenkstis (≥50 FTE ARBA ≥€10M)
  if (data.q3_meetsSizeThreshold === 'no') {
   return {
    ...data,
    classification: 'not_applicable',
    reason: 'Nors veikiate TIS2 sektoriuje, jūsų organizacija netenkinamas dydžio slenksčio reikalavimo (<50 darbuotojų IR <€10 mln. apyvarta/balansas).'
   };
  }

  // Tikrinama, ar yra Annex I ir / ar Annex II sektorių
  const hasAnnexI = data.q1_nis2Sectors.some(sectorId =>
   ANNEX_I_SECTORS.some(ai => ai.id === sectorId)
  );

  const hasAnnexII = data.q1_nis2Sectors.some(sectorId =>
   ANNEX_II_SECTORS.some(aii => aii.id === sectorId)
  );

  if (hasAnnexI) {
   return {
    ...data,
    classification: 'essential',
    reason: 'Veikiate Annex I (didelės svarbos) sektoriuje ir atitinkate dydžio slenkstį (≥50 FTE arba ≥€10M).',
    annexI: true,
    annexII: hasAnnexII
   };
  }

  // Q4: Specifinė reikšmė (tik Annex II)
  if (data.q4_specificSignificance?.includes('no_significance')) {
```

```
    return {
      ...data,
      classification: 'important',
      reason: 'Veikiate Annex II (kiti svarbūs) sektoriuje, atitinkate dydžio slenkstį, bet neturite specifinės reikšmės savo sektoriuje.',
      annexI: false,
      annexII: true
    };
  }

  return {
    ...data,
    classification: 'essential',
    reason: 'Veikiate Annex II (kiti svarbūs) sektoriuje, atitinkate dydžio slenkstį IR turite specifinę reikšmę savo sektoriuje.',
    annexI: false,
    annexII: true
  };
};
```

Algoritmas:

- pirma tikrina **CER** kritinio subjekto statusą;
- tuomet – veiklos sektorius (Annex I / Annex II arba nevykdo veiklos TIS2 sektoriuose);
- specialūs subjektai (DNS, eIDAS, telekomunikacijos, viešasis administravimas) automatiškai priskiriami **Essential** kategorijai;
- tikrinamas **dydžio slenkstis** (≥50 FTE arba ≥10 mln. EUR);
- Annex II atveju, „specifinė reikšmė“ lemia skirtumą tarp **Important** ir **Essential**.

**Klausimyno modulis**

Klausimynas paremtas bendru duomenų modeliu, kuriame klausimai grupuojami į blokų struktūrą pagal TIS2 reikalavimus.

```
// Failas: frontend-v5/src/questions.ts
export type Question = {
  id: string;
  text: string;
  dependsOn?: string;
  dependsValue?: string;
  explanation?: string;
};
```

```
export type QuestionBlock = {
  id: string;
  title: string;
  questions: Question[];
};
```

Klausimų modelyje id užtikrina nuoseklų susiejimą su reikalavimais ir priemonėmis; dependsOn ir dependsValue leidžia aprašyti priklausomybes tarp klausimų; explanation naudojamas naudotojui pateikti papildomą paaiškinimą (pvz. norminių aktų nuorodas).

**Klausimyno komponentas.**

Klausimyno komponentas valdo blokų navigaciją, klausimų būseną ir bendrą progresą. Klausimai grupuojami į 12 reikalavimų blokų, kurių progresas skaičiuojamas atskirai; jei į „tėvinį“ klausimą atsakoma **NE** arba **NEŽINAU**, visi nuo jo priklausomi klausimai automatiškai žymimi **NE** – taip išvengiama nereikalingų klausimų; bendras progreso indikatorius parodo, kiek klausimų atsakyta visame klausimyne.

```
// Failas: frontend-v5/src/App.tsx (Questionnaire komponentas)
function Questionnaire({ onFinish }: { onFinish: (answers: any) => void }) {
  const [blockIdx, setBlockIdx] = useState(0);
  const [answers, setAnswers] = useState<{ [qid: string]: AnswerType }>({});
  const block: QuestionBlock = QUESTION_BLOCKS[blockIdx];

  // Rodome visus klausimus be priklausomybių filtravimo
  const visibleQuestions = block.questions;

  const [currentIdx, setCurrentIdx] = useState(0);
  const question: Question = visibleQuestions[currentIdx];
  const total = visibleQuestions.length;
  const answered = visibleQuestions.filter(q => answers[q.id]).length;

  // Jei atsakoma NE/NEŽINAU, priklausomi klausimai automatiškai žymimi NE
  const handleAnswer = (ans: AnswerType) => {
    setAnswers(prev => {
      let newAnswers = { ...prev, [question.id]: ans };
      if ((ans === 'NE' || ans === 'NEŽINAU') && block.questions.some((q: Question) => q.dependsOn === question.id)) {
        block.questions.forEach((q: Question) => {
          if (q.dependsOn === question.id) {
            newAnswers[q.id] = 'NE';
          }
        });
      }
```

```
    return newAnswers;
  });
  if (currentIdx < total - 1) {
    setCurrentIdx(currentIdx + 1);
  }
};

const handleSubmit = () => {
  onFinish(answers);
};

const handleBlockChange = (newBlockIdx: number) => {
  setBlockIdx(newBlockIdx);
  setCurrentIdx(0);
};

const totalQuestions = QUESTION_BLOCKS.reduce((sum, b) => sum + b.questions.length, 0);
const totalAnswered = Object.keys(answers).length;
const overallProgress = Math.round((totalAnswered / totalQuestions) * 100);

return (
  <div>
    {/* Blokų antraštės, progreso rodymas ir atsakymo mygtukai (TAIP/NE/IŠ DALIES/NEŽINAU/PRALEISTI) */}
  </div>
);
}
```

**Vertinimo rezultato generavimas.**

Funkcija generateAssessmentResult konvertuoja atsakymus į kiekybinį balą (bendrą ir kiekvieno bloko).

Naudojamas vertinimo modelis:

- **TAIP** = 1 balas;
- **IŠ DALIES** = 0,5 balo;
- **NE / NEŽINAU / PRALEISTI** = 0 balų.

Tokiu būdu skaičiuojamas tiek bendras, tiek kiekvieno bloko procentinis rezultatas. Automatiškai sugeneruojamas unikalus vertinimo ID, parenkamas naujas **versijos numeris**, remiantis esama organizacijos istorija, išsaugomas vertinimo laikas (timestamp).

```
// Failas: frontend-v5/src/App.tsx

const generateAssessmentResult = (
```

```
  userId: string,
  organization: string,
  criticality: any,
  answers: any
): AssessmentResult => {
  const allQuestions = QUESTION_BLOCKS.flatMap(block => block.questions);
  const total = allQuestions.length;
  const yes = Object.values(answers).filter((a) => a === 'TAIP').length;
  const partial = Object.values(answers).filter((a) => a === 'IŠ DALIES').length;
  const score = Math.round((yes + 0.5 * partial) / total * 100);

  const blockResults = QUESTION_BLOCKS.map(block => {
    const blockQuestions = block.questions;
    const blockTotal = blockQuestions.length;
    const blockYes = blockQuestions.filter(q => answers[q.id] === 'TAIP').length;
    const blockPartial = blockQuestions.filter(q => answers[q.id] === 'IŠ DALIES').length;
    return {
      id: block.id,
      title: block.title,
      score: Math.round((blockYes + 0.5 * blockPartial) / blockTotal * 100),
      total: blockTotal
    };
  });

  const existingHistory = getAssessmentHistory(organization) as AssessmentResult[];
  const maxVersion = existingHistory.length > 0 ? Math.max(...existingHistory.map(r => r.version)) : 0;

  return {
    id: `assessment_${Date.now()}_${Math.random().toString(36).substr(2, 9)}`,
    userId,
    organization,
    timestamp: new Date().toISOString(),
    version: maxVersion + 1,
    criticality,
    answers,
    score,
```

```
    blockResults
  };
};
```

**Įgyvendinimo plano modulis**

ImplementationPlan komponentas remiasi susiejimo lentele QUESTION_TO_MEASURE_MAPPING ir pagal atsakymus automatiškai nustato, kurios priemonės laikomos neįgyvendintomis. Užtikrinama, kad įgyvendinimo planas būtų **tiesiogiai susietas** su vertinimo rezultatais; naudojamas useMemo, kad skaičiavimai būtų atliekami tik pasikeitus atsakymams ar filtrams; priemonės gali būti filtruojamos pagal **reikalavimą**, **tipą**, **prioritetą** ir **subkategoriją**.

```
// Failas: frontend-v5/src/components/ImplementationPlan.tsx
const ImplementationPlan: React.FC<ImplementationPlanProps> = ({ answers }) => {
  const [selectedRequirement, setSelectedRequirement] = useState<string>('VISI');
  const [selectedType, setSelectedType] = useState<MeasureType>('VISI');
  const [selectedPriority, setSelectedPriority] = useState<FilterPriority>('VISI');
  const [selectedSubcategory, setSelectedSubcategory] = useState<string>('VISOS');
  const [expandedMeasures, setExpandedMeasures] = useState<Set<string>>(new Set());
  const [expandedActions, setExpandedActions] = useState<Set<string>>(new Set());
  const [expandedSteps, setExpandedSteps] = useState<Set<string>>(new Set());

  // Neįgyvendintos priemonės
  const unimplementedMeasures = useMemo(() => {
    const unimplementedMeasureIds = new Set<string>();

    Object.keys(QUESTION_TO_MEASURE_MAPPING).forEach(questionId => {
      const answer = answers[questionId];
      const measureId = QUESTION_TO_MEASURE_MAPPING[questionId];

      if (!answer || answer === 'NE' || answer === 'IŠ DALIES' || answer === 'NEŽINAU' || answer === 'PRALEISTI') {
        if (measureId) {
          unimplementedMeasureIds.add(measureId);
        }
      }
    });

    return IMPLEMENTATION_MEASURES.filter(m => unimplementedMeasureIds.has(m.id));
  }, [answers]);
```

```
  // Filtravimas
  const filteredMeasures = useMemo(() => {
    let filtered = unimplementedMeasures;

    if (selectedRequirement !== 'VISI') {
      filtered = filtered.filter(m => m.requirementId === selectedRequirement);
    }
    if (selectedType !== 'VISI') {
      filtered = filtered.filter(m => m.type === selectedType);
    }
    if (selectedPriority !== 'VISI') {
      filtered = filtered.filter(m => m.priority === selectedPriority);
    }
    if (selectedSubcategory !== 'VISOS') {
      filtered = filtered.filter(m => m.subcategory === selectedSubcategory);
    }

    return filtered;
  }, [unimplementedMeasures, selectedRequirement, selectedType, selectedPriority, selectedSubcategory]);
```

Kiekviena priemonė išskaidoma į veiksmus ir žingsnius, kuriuos galima atskirai išskleisti. Tokiu būdu įgyvendinimo planas tampa hierarchiškas ir papildytas metaduomenimis (trukmė, atsakingi asmenys, dalyvaujantys padaliniai, priklausomybės, rezultatų rodikliai, sprendimų klasės ir pavyzdžiai).

```
// Failas: frontend-v5/src/components/ImplementationPlan.tsx
{isExpanded && (
  <div style={{ padding: '20px', background: '#f8f9fa' }}>
    {measure.actions.map(action => {
      const isActionExpanded = expandedActions.has(action.id);

      return (
        <div key={action.id}>
          <div onClick={() => toggleAction(action.id)}>
            <h4>Veiksmas {action.number}: {action.title}</h4>
            <p>{action.description.substring(0, 100)}...</p>
          </div>
```

```
{isActionExpanded && (
 <div>
  <p>{action.description}</p>
  {action.steps.map(step => {
   const isStepExpanded = expandedSteps.has(step.id);

   return (
    <div key={step.id}>
     <div onClick={() => toggleStep(step.id)}>
      <strong>Žingsnis {step.number}: {step.description}</strong>
     </div>

     {isStepExpanded && (
      <div>
       {step.duration && (
        <div>Trukmė: {step.duration} savaitės</div>
       )}
       {step.responsible && (
        <div>Atsakingas: {step.responsible}</div>
       )}
       {step.participatingDepartments && (
        <div>Dalyvaujantys: {step.participatingDepartments}</div>
       )}
       {step.dependencies && (
        <div>Priklausomybės: {step.dependencies}</div>
       )}
       {step.resultIndicator && (
        <div>Rezultato rodiklis: {step.resultIndicator}</div>
       )}
       {step.solutionClass && (
        <div>Sprendimo klasė: {step.solutionClass}</div>
       )}
       {step.solutionExamples && (
        <div>Pavyzdžiai: {step.solutionExamples}</div>
       )}
```

```
                </div>
              )}
            </div>
          );
        })}
      </div>
    )}
  </div>
);
  })}
 </div>
)}
```

Priklausomai nuo tipo, žingsniai turi skirtingą detalumo struktūrą. technologiniuose žingsniuose organizacija gautų **konkrečių gamintojų ir produktų** pavyzdžių; procesiniuose žingsniuose akcentuojama **procesų seka**; mokymų žingsniuose – temos, trukmė, dažnumas, dalyviai; personalo žingsniuose – rolės, reikalavimai ir aiškiai apibrėžtos atsakomybės.

```
// Failas: frontend-v5/src/components/ImplementationDetails.tsx

// Technologiniai žingsniai: gamintojai ir produktai
{step.type === 'TECHNICAL' && step.vendors && (
 <div>
  <strong>Rekomenduojami gamintojai:</strong>
  {step.vendors.map((vendor, idx) => (
   <div key={idx}>
    <h5>{vendor.name}</h5>
    <div><strong>Produktas:</strong> {vendor.product}</div>
    <div>{vendor.description}</div>
    <a href={vendor.website} target="_blank" rel="noopener noreferrer">
     Apsilankyti svetainėje →
    </a>
   </div>
  ))}
 </div>
)}

// Procesiniai žingsniai
```

```
{step.type === 'PROCESS' && step.processSteps && (
  <div>
    <strong>Procesiniai žingsniai:</strong>
    <ol>
      {step.processSteps.map((processStep, idx) => (
        <li key={idx}>{processStep}</li>
      ))}
    </ol>
  </div>
)}

// Mokymų detalės
{step.type === 'TRAINING' && step.trainingDetails && (
  <div>
    <strong>Mokymų detalės:</strong>
    {/* temos, trukmė, dažnumas, dalyviai */}
  </div>
)}

// Personalo detalės
{step.type === 'PERSONNEL' && step.personnelDetails && (
  <div>
    <strong>Personalo detalės:</strong>
    {/* rolės, reikalavimai, atsakomybės */}
  </div>
)}
```

**Duomenų saugojimas ir rezultatų skaičiavimas**

Vertinimo rezultatai saugomi naršyklės localStorage objektuose, grupuojant duomenis pagal organizaciją ir versiją. leidžia saugoti **vertinimų istoriją** kiekvienai organizacijai.

```
// Failas: frontend-v5/src/App.tsx
const STORAGE_KEY = 'nis2_assessment_history';

const saveAssessmentResult = (result: AssessmentResult) => {
  try {
    const existingData = localStorage.getItem(STORAGE_KEY);
```

```
    const history: AssessmentHistory = existingData ? JSON.parse(existingData) : {};

    if (!history[result.organization]) {
      history[result.organization] = [];
    }

    history[result.organization].push(result);

    // Paliekamos tik paskutinės 10 versijų
    if (history[result.organization].length > 10) {
      history[result.organization] = history[result.organization].slice(-10);
    }

    localStorage.setItem(STORAGE_KEY, JSON.stringify(history));
    return true;
  } catch (error) {
    console.error('Failed to save assessment result:', error);
    return false;
  }
};

const getAssessmentHistory = (organization?: string): AssessmentHistory | AssessmentResult[] => {
  try {
    const data = localStorage.getItem(STORAGE_KEY);
    if (!data) return organization ? [] : {};

    const history: AssessmentHistory = JSON.parse(data);
        if (organization) {
      return history[organization] || [];
    }
        return history;
  } catch (error) {
    console.error('Failed to get assessment history:', error);
    return organization ? [] : {};
  }
};
```