MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

JURGA KUPINĖ

KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIS

Magistro baigiamasis darbas

Vadovė:

Dr. Inga Malinauskaitė-van de Castel

VILNIUS, 2024

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIS

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų prorgama 6211LX066

Konsultantas

Vadovė
Dr. I. Malinauskaitė-van de Castel
2024

Recenzentas

Atliko:
KSVvmis22-1 gr. Stud.
J. Kupinė
2024

VILNIUS, 2024

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

SANTRUMPOS IR TERMINAI

CIA (ang. *Confidentiality* - konfidencialumas, *Integrity* - vientisumas, *Availability* - prieinamumas) - informacijos saugumas įvardijamas CIA, kuris yra šių trijų įrankių inicialų derinys.

COBIT (ang. *Control Objectives for Information and Related Technology*) - informacinių technologijų valdymo ir IT valdymo sistema

ENISA (ang. *European Union Agency for Cybersecurity*) - Europos Sąjungos kibernetinio saugumo agentūra

IEC (ang. *International Electrotechnical Commission*) - Tarptautinė elektrotechnikos komisija

ISO (ang. *International Organization for Standardization*) – Tarptautinė standartizacijos organizacija.

ISO/IEC 27001 - tarptautinis informacijos saugumo valdymo standartas, paskelbtas Tarptautinės standartizacijos organizacijos ir Tarptautinės elektrotechnikos komisijos

IRT (ang. *ICT – Information and Communications Technology*) – Informacinės ir Ryšių technologijos

IoT (ang. *Internet of Things*) – daiktų internetas

ISMS (ang. *Information Security Management System*) – Informacijos saugumo valdymo sistema

MVĮ – mažos ir vidutinės įmonės

NIST (ang. *National Institute of Standards and Technology*) - Nacionalinis standartų ir technologijų institutas. Šiame darbe taip pat vadinamas Nacionalinis standartų ir technologijų instituto sukurtas kibernetinio saugumo brandos modelis.

PCI DSS (ang. *Payment Card Industry Data Security Standard*) - Mokėjimo kortelių industrijos duomenų saugumo standartas

Phishing (*sukčiavimas*) - socialinės inžinerijos sukčiavimo forma, skirta išvilioti konfidencialius duomenis

ĮVADAS

Temos aktualumas. Nuolat didėjantis kibernetinių atakų skaičius, duomenų nutekinimo atvejai ir įvairios kibernetinės grėsmės rodo, kad valstybės, jų institucijos, organizacijos ir piliečiai nėra pasirengę apsisaugoti, tinkamai reaguoti ir atsistatyti įvykus kibernetinėms grėsmėms. Europos Sąjungos valstybėse susipažinti su kibernetiniu saugumu ir galimomis grėsmėmis skatina 2020 m. priimta naujoji ES Parlamento ir Komisijos ES kibernetinio saugumo strategija, kuri savo įvade konstatuoja kibernetinio saugumo aktualumą: „ES ekonomika, demokratija ir visuomenė labiau nei bet kada priklauso nuo saugių ir patikimų skaitmeninių priemonių ir ryšio[1].“ ENISA (Europos Sąjungos kibernetinio saugumo agentūros) 2022 m. spalio mėn. išleistame kibernetinio saugumo grėsmių žemėlapyje akcentuojama, kad „kibernetinio saugumo atakų 2021 m. ir 2022 m. antrąjį pusmetį ir toliau daugėjo ne tik kryptimi ir skaičiais, bet ir jų poveikio požiūriu[2].“ „Per 2022 antrąją pusę ir pirmąją 2023 pusę, pastebėtas staigus kibernetinių atakų pakilimas, nustatantis naujas incidentų įvairovės, skaičiaus bei jų pasekmių gaires; o 2023 m. pirmąjį pusmetį užfiksuotas precedento neturintis išpirkos reikalaujančių incidentų padidėjimas – tendencija, kuri nerodo mažėjimo ženklų.“[3]

Dažnėjantys kibernetiniai išpuoliai ir besikeičiančios kibernetinės grėsmės rodo, kad kibernetinis saugumas, kartu ir kibernetinis atsparumas bei branda tampa vienu svarbiausiu aspektu organizacijose. Kibernetinio saugumo brandos organizacijose vertinimo modeliai padeda organizacijoms įsivertinti esamą situaciją, nustatyti galimas grėsmes, rizikas, ir taip pasirengti gresiančioms kibernetinėms grėsmėms, tampant atsparioms ir išvengiant finansinių ir reputacinių nuostolių. Valdant kibernetinį saugumą, geroji praktika rekomenduoja įdiegti, valdyti ir stebėti informacijos saugumo valdymo sistemą (toliau – ISMS), kuri saugo informacijos konfidencialumą, vientisumą ir prieinamumą, taikydama rizikos valdymo procesą ir užtikrina suinteresuotąsias šalis, kad rizikos yra tinkamai valdomos.[4] Būtent kibernetinio saugumo brandos modeliai padeda organizacijoms įsidiegti ISMS ir įsivertinti esančią kibernetinio saugumo brandą, taip dinamiškai reaguoti bei keistis atsižvelgiant į naujus kibernetinių grėsmių tipus, besikeičiantį teisinį reguliavimą, naujas technologijas, darbuotojų mokymą, stebėti kibernetinius incidentus, rizikas, taip nuolat tobulintis bei didinti kibernetinį atsparumą.

---

[1] ES Parlamento ir Komisijos priimta ES kibernetinio saugumo strategija. Prieiga: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

[2] ENISA Threat Landscape 2022. P. 7 Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[3] ENISA Threat Landscape 2023. P. 6 Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[4] Valstybės Kontrolė. Kibernetinio saugumo užtikrinimas. Valstybinio audito ataskaita, 2022, P. 13. Prieiga: https://www.valstybeskontrole.lt/LT/Product/Download/4371

Mokslinis naujumas / teorinis reikšmingumas. Nuolat didėjantys kibernetinių atakų skaičiai ir besikeičiančios bei dažnėjančios kibernetinės grėsmės kelia nerimą valstybėms, organizacijoms ir piliečiams. Tampa svarbu apsaugoti informaciją, duomenis, serverius, sistemas, keistis ir tobulėti kartu su besikeičiančiomis technologijomis ir netapti kibernetinių nusikaltimų aukomis įgyjant kibernetinį atsparumą. Brandos modelis yra naudojamas kaip priemonė įvertinti organizacijos efektyvumą siekiant konkretaus tikslo. Tai taip pat gali palengvinti organizacijos gebėjimą nustatyti, kur jų praktika yra silpna arba jos nėra ir kur jų praktika yra tikrai įtvirtinta.[5] Brandos modelis organizacijoje prasideda nuo organizacinių priemonių, politikų sudarymo iki fizinės saugos praktinio įgyvendinimo bei nuolatinio atitikties stebėjimo, bei brandos išlaikymo. Brandos modelis patogus tuo, kad juo brandumo lygį gali nustatyti pati organizacija.[6] Kurii, Y., & Opirskyy, I. (2022) teigia, kad kibernetinio saugumo brandos modeliai yra organizacijos rizikos valdymo ir mažinimo planas. Informacijos saugos specialistai naudoja sistemas, kad apibrėžtų ir suskirstytų užduočių prioritetus, reikalingus organizacijos saugos programoms valdyti, o taip pat naudojami siekiant padėti pasiruošti atitikties ir kitiems IT ir saugos auditams. Lietuvoje Agafonov K. (2021) disertacijoje apžvelgė kibernetinio saugumo brandos modelius, jų specifikacijas bei atliko lyginamąją kibernetinio saugumo modelių analizę elektroninių rinkimų įgyvendinimo kontekste ir apibendrindamas teigė, „kad visi anksčiau aprašyti kibernetinio saugumo modeliai yra skirti kibernetiniam saugumui užtikrinti bet kokio sektoriaus ar veiklos organizacijoje: valstybinis sektorius, viešojo ar privataus verslo atstovai, gynybinės organizacijos ir kt., o pačias modeliuose aptariamas saugumo priemones galima išskirstyti į tris sritis: fizines saugos, technologinės saugos ir administracinės saugos priemones“. Tačiau moksliniuose šaltiniuose randama ir kita nuomonė - Stewart, Dr. (2022) nurodo priešingai ir nepaisant visų šiandien prieinamų standartų ir kitų įvairių tyrėjų siūlomų informacijos saugumo valdymo sistemų organizacijoms, jose kibernetinių nusikaltimų lygis vis dar didėja, nes mokslininkai ir vyriausybiniai institutai privertė organizacijas manyti, kad vieno iš turimų standartų laikymasis suteikia saugumo lygį. Mokslinė literatūra apžvelgia kibernetinio saugumo brandos modelių specifikacijas, kuo vienas ar kitas minėtas kibernetinio saugumo brandos vertinimo modelis naudingas, atliekama lyginamoji modelių analizė, kokiais kriterijais modeliai remiasi, kuo panašūs, ar skiriasi, tačiau pasigendama informacijos, o ypač lietuvių kalba, kuri vertintų kibernetinio saugumo brandos organizacijose vertinimo modelių efektyvumą organizacijose.

---

[5] Akinsanya, O. O., Papadaki, M., & Sun, L. (2019, March). Current cybersecurity maturity models: How effective in healthcare cloud?. In *CERC* (pp. 211-222). p. 211

[6] De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. "Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, p.5

Mokslinė problema. Didėjantis kibernetinių atakų skaičius priverčia nukentėti vis daugiau organizacijų, paveikiant jų veiklą, finansus ir reputaciją, todėl organizacijos pradeda ieškoti įvairių sprendimų, padedančių įgyti atsparumą kibernetinėms grėsmėms. Kibernetinio saugumo brandos modeliai yra viena iš priemonių, padedančių organizacijoms, nepriklausomai nuo jų dydžio ar veiklos srities, įgyti kibernetinį atsparumą, o taip pat identifikuoti, vertinti, valdyti ir tinkamai reaguoti į kibernetines grėsmes. Kibernetinio saugumo brandos organizacijose modelių nauda ir svarba yra pripažįstama, tačiau svarbu išsiaiškinti modelių veikimo principus, jų pritaikymą ir įgyvendinimą, bei kaip jie realiai gali padėti organizacijoms įgyti kibernetinį atsparumą. Siekiant išsiaiškinti kibernetinio saugumo brandos modelių metodikas kaip jos padeda organizacijoms priimti kibernetinio saugumo strategijas, atnaujinti dokumentaciją bei įvertinti ir įdiegti procesus, ir procedūras, leidžiančias organizacijai tapti atsparesnei kibernetinėms grėsmėms, keliama šio darbo mokslinė problema - išanalizuoti kibernetinio saugumo brandos vertinimo modelio efektyvumą organizacijoje ir brandos modelio praktinį veiksmingumą, sprendžiant organizacijose sukurtų saugumo politikų santykį su praktiniu taisyklių laikymusi, bei realiai mažėjančiu kibernetiniu pažeidžiamumu nagrinėjant du pagrindinius ir plačiausiai naudojamus kibernetinio saugumo modelius ISO 27001 ir NIST. Organizacijai renkantis kibernetinio saugumo brandos organizacijoje vertinimo modelį svarbiausias turėtų būti modelio efektyvumas, kad įdiegtas modelis organizacijai iš tiesų suteiktų saugumo lygį, brandą, padėtų apsisaugoti nuo kibernetinių įsilaužimų ir grėsmių, todėl papildomai bus siekiama atsakyti į klausimus – ar kibernetinio saugumo brandos organizacijoje vertinimo modeliai ir jų laikymasis iš tikrųjų užtikrina kibernetinį saugumą organizacijose; kaip organizacijos suvokia ir įgyvendina kibernetinio saugumo brandos modelius; kas iš tikrųjų lemia kibernetinio saugumo brandos modelio efektyvumą organizacijoje.

Tyrimo objektas: kibernetinio saugumo brandos vertinimo modelis.

Tyrimo dalykas: kibernetinio saugumo brandos organizacijoje vertinimo modelio efektyvumas.

Tyrimo tikslas: įvertinti kibernetinio saugumo brandos organizacijoje modelius, jų efektyvumą bei įgyvendinimo aspektus analizuojant UAB „XXX” atvejį bei pusiau struktūruoto interviu atsakymus.

Tyrimo uždaviniai:

1. Išanalizuoti populiariausius kibernetinio saugumo brandos vertinimo modelius.
2. Konceptualizuoti kibernetinio saugumo brandos vertinimo modelių vertinimo kriterijus išryškinant jų tendencijas.
3. Ištirti kibernetinio saugumo brandos organizacijoje vertinimo modelių įgyvendinimo aspektus analizuojant UAB „XXX“ bei interviu atsakymus.

4. Pateikti tyrimo metu gautas rekomendacijas organizacijoms kaip efektyviai įgyvendinti kibernetinio saugumo brandos organizacijoje vertinimo modelius

Duomenų rinkimo metodai:

1. Mokslinės literatūros sisteminimas, analizė, palyginimas.
2. Dokumentų analizė.
3. Atvejo analizė (*Case study analysis*) kokybinio turinio analizė.
4. Ekspertinis pusiau struktūruotas interviu.

Duomenų analizės metodai:

1. Kokybinė turinio (*Content*) analizė.
2. Atvejo studijos rezultatų analizė.
3. Pusiau struktūruoto interviu kokybinė turinio (*Content*) analizė ir interpretavimas.
4. Lyginamoji gautų duomenų analizė.

Magistrinio darbo struktūra:

Teorinė dalis, kurioje apžvelgiama, sisteminama ir analizuoja mokslinė literatūra ir dokumentai reglamentuojantys kibernetinį saugumą, kibernetinio saugumo brandos modeliai, jų pagrindiniai kriterijai, modelių palyginimas.

Metodologinė dalis, kurioje aprašomi kibernetinio saugumo brandos modelių vertinimo tyrimui taikyti metodai ir vertinimo kriterijai.

Analitinė dalis, kurioje analizuojami teorinėje dalyje ir atvejo analizės bei pusiau struktūrizuoto interviu yrimo metu gauti rezultatai ir jų palyginimas.

Pateiktos išvados ir rekomendacijos kaip efektyviai įgyvendinti kibernetinio saugumo brandos organizacijose vertinimo modelius.

Priedai, papildantys šio darbo teorinę, metodologinę ir analitinę dalis.

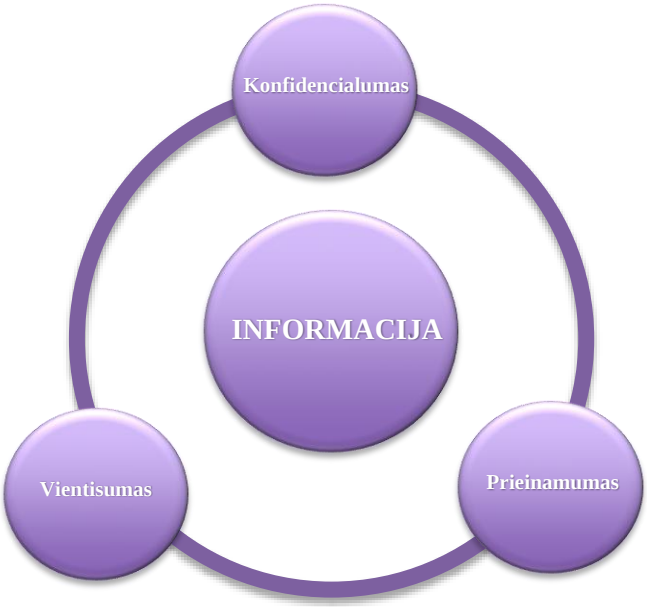
1. POPULIARIAUSI KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIAI

1.1. KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE SVARBA

Kibernetinio saugumo brandos svarba atsispindi ir valstybiniu bei tarptautiniu institucijų lygmeniu: priimami teisės aktai, rekomendacijos, gairės, kuriomis dažniausiai siekiama atkreipti dėmesį į kibernetinį saugumą, jo higieną bei poreikį imtis priemonių jam užtikrinti. Europos mastu kibernetinio saugumo brandą buvo siekta pakelti Europos Parlamento ir Tarybos direktyvomis, kurios ES valstybėms narėms nustatė pasitvirtinti reikalavimus siekiant didinti kibernetinį atsparumą, priimti kibernetinio saugumo strategijas, įstatymus.

Kibernetinis saugumas yra informacijos saugumo dalis, šių sąvokų definicijas ir santykį analizavo Taherdoost H.(2022) straipsnyje „Kibernetinis saugumas vs. Informacijos saugumas“. Tad remiantis ISO/IEC 27032:2012, kibernetinis saugumas apibrėžiamas kaip „informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas kibernetinėje erdvėje“. Be to, Merriam-Webster žodynas apibrėžia kibernetinį saugumą kaip „priemones, kurių imamasi, siekiant apsaugoti kompiuterį ar kompiuterinę sistemą nuo neteisėtos prieigos ar atakų“. Kita vertus, informacijos saugumas apibrėžiamas kaip „informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas“. Pagrindinis informacijos saugos tikslas – užtikrinti verslo procesų tęstinumą su mažiausia žala ir apriboti neigiamą incidentų poveikį. Taigi atsižvelgiant į apibrėžimus, galima daryti išvadą, kad informacijos sauga visiškai apima kibernetinį saugumą kaip vieną iš savo komponentų. Ibrahimova, A.N. (2021) teigia, kad informacijos saugumas iš esmės užtikrinamas trimis priemonėmis: konfidencialumu, vientisumu, ir prieinamumu. Daugelyje šaltinių informacijos saugumas įvardijamas CIA, kuris yra šių trijų įrankių inicialų derinys (ang. *Confidentiality* - konfidencialumas, *Integrity* - vientisumas, *Availability* - prieinamumas). Kiti šaltiniai prie šių trijų sąvokų prideda dvi sąvokas, kurios vadinamos atskaitomybės ir įgalinimo įrankiais. ISO Konfidencialumą apibrėžia kaip „prieiga prie informacijos tik įgaliotiems asmenims“. Šiandien daugelyje informacijos ir komunikacijos įmonių pagrindinis šifravimo naudojimo tikslas yra užtikrinti informacijos konfidencialumą. Tad **konfidencialumas**, kaip pagrindinė sąvoka, yra „neleisti neįgaliotiems asmenims atskleisti informacijos“. **Vientisumas** – tai duomenų ar informacijos apsauga nuo pašalinių asmenų padaryto pakeitimo ar sunaikinimo. Vientisumas – tai informacijos turinio apsauga nuo grėsmės jį bet kokiu būdu pakeisti, ištrinti ar sunaikinti pašalinių asmenų. Trumpai tariant, vientisumas yra atsitiktinio ar tyčinio informacijos vientisumo pažeidimo nebuvimas. Informacijos vientisumas turi atitikti šiuos tris kriterijus: apibrėžtumą, tikslumą ir patikimumą. **Prieinamumas** - reiškia, kad informacija yra prieinama tada, kai jos

reikia. Tokios informacijos prieinamumas iškilus bet kokiai problemai arba iškilus problemoms yra pagrindinė naudojimo ypatybė ir turėtų priklausyti vartotojo teisėms. Toliau pateikiamas informacinių sistemų saugumo aspektų modelis (1 Paveikslas) arba kitaip dar vadinama informacijos saugumo triada.



1 Paveikslas. Informacinių sistemų saugumo aspektų modelis. Šaltinis Fathurohman, A., & Witjaksono, R. W. (2020)

Lietuvoje Kibernetinio saugumo įstatymas priimtas 2014 m., 2 straipsnio 10 dalyje įtvirtino kibernetinio saugumo sąvoką taip pat įtraukdamas ir informacijos saugumo triadą: „kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.“[7] Pagal šią sąvoką galima išskirti kibernetinio saugumo brandos pagrindinius bruožus:

- Teisines, informacijos sklaidos, organizacines ir technines priemones, kuriomis siekiama išlaikyti kibernetinį atsparumą;
- Kibernetinis atsparumas veiksniams, kurie kibernetinėje erdvėje kelia grėsmę ryšių ir informacinėmis sistemose perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui,

[7] Lietuvos Respublikos Seimas (2014). Lietuvos Respublikos kibernetinio saugumo įstatymas. (2014 m. Gruodžio 11 d., Nr. XII-1428) https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

- Ryšių ir informacinių sistemų netrikdomas veikimas, valdymas arba paslaugų šiomis sistemomis teikimas, ir
- Sistemos, kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.

Informacijos saugumo triada yra neatsiejama kibernetinio saugumo ir kibernetinio saugumo brandos dalis, kuri padeda užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą organizacijose.

Straipsnio „Kibernetinio saugumo brandos modeliai ir SSGG analizė“ autorius Dietmar P. F. Möller teigia, kad kibernetiniam saugumui reikalingas organizacijų kibernetinio saugumo planas arba strategija, nes kibernetinis saugumas apima daugybę sričių, įskaitant duomenų saugumą, informacijos saugumą, veiklos saugumą ir kitas, bet tuo neapsiribojant. Nepaisant to, didžiuliai skaitmeninimo pokyčiai reikalauja metodų, leidžiančių organizacijoms kartoti esamą jų kibernetinio saugumo suvokimo ir (arba) kibernetinio saugumo strategijos būklę, kad galėtų apsiginti nuo kibernetinių atakų. Todėl reikalingos priemonės yra tikrosios kibernetinio saugumo supratimo ir (arba) kibernetinio saugumo gynybos strategijos būklės kiekybinis įvertinimas, siekiant nustatyti esminius veiksmus, kad būtų pasiekta tikslinė kibernetinio saugumo būsena[8]. Autorius Dietmar P. F. Möller (2023) pabrėžia, kad būtent šioje vietoje pradeda veikti kibernetinio saugumo brandos modeliai: „ Kibernetinio saugumo brandos modeliai apibūdina numatomą pageidaujamą arba būtiną kriterijų raidos kelią iš eilės atskirose eilėse, pradedant nuo pradinės būsenos iki visiško kibernetinio saugumo brandos lygio, pvz., penkių. Todėl brandos modelis yra tinkama metodika sistemingai plėtoti ir laipsniškai tobulinti įgūdžius, procesus, struktūras ir kitas esmines sąlygas organizacijoms kibernetinio saugumo suvokimo ir gynybos strategijos kontekste.“ Apibendrinant, galima išskirti kibernetinio saugumo brandos organizacijoje svarbos kriterijus, kurie užtikrina:

1. Organizacijos saugumo politikos, procedūros, darbuotojų mokymus, o su jais ir nuoseklų saugumo taisyklių įgyvendinimą atliekant kasdienines užduotis.
2. Techninių ir žmogiškųjų išteklių paskirstymą, ne tik sistemų saugumui, tačiau reagavimui į kibernetines grėsmes bei verslo tęstinumą, kuriam numatomas planas.
3. Sistemų saugumą ir jų darbo nenutrūkstamumą jas prižiūrint, atnaujinant ir apsaugant.
4. Reagavimą į kibernetines grėsmes jas identifikuojant, aptinkant, kad būtų padaryta mažiausia galima žala.

[8] Möller, D.P.F. (2023). Cybersecurity Maturity Models and SWOT Analysis. In: Guide to Cybersecurity in Digital Transformation. Advances in Information Security, vol 103 . Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_7

5. Nuolatinį atitikties su teisės aktais, vidaus politikomis, taisyklėmis ir pažeidžiamumų stebėjimą bei rizikų valdymą, o su jais ir procesų vientisumą, galimų rizikų numatymą, rizikų priėmimą arba korekcinių veiksmų nustatymą, bei išmoktų pamokų įgyvendinimą organizacijos veikloje.

Kibernetinio saugumo branda yra svarbus organizaciją apibūdinantis aspektas, parodantis organizacijos atsparumą kibernetinėms grėsmės. Skirtingos organizacijos susiduria su skirtingomis kibernetinėmis grėsmėmis ir turi tiesioginį ryšį su organizacijos dydžiu bei veiklos pobūdžiu. Kibernetinės atakos sukelia didelę ekonominę žalą ir gali sužlugdyti organizacijas. Todėl organizacijoms verta atkreipti dėmesį į kibernetinio saugumo brandos modelius, kurie padeda efektyvų pagrindą kibernetinio saugumo valdymui ir prisideda prie kibernetinio atsparumo. „2022 m. antroje pusėje ir 2023 m. pirmąjį pusmetį labai išaugo kibernetinių atakų kiekis, jų pasekmės ir įvairovė“[9] – teigia Europos Sąjungos kibernetinio saugumo agentūra (toliau – ENISA). ENISA tikslas – siekti aukšto bendro kibernetinio saugumo lygio visoje Europoje, 11-us metus leidžiamame ENISA grėsmių žemėlapyje, kuriame apibendrintos kibernetinės grėsmės, kurios buvo pasiekiamos renkant viešai prieinamą informaciją, pateikiamos nustatytos pagrindinės kibernetinės grėsmės, pagrindinės pastebėtos kibernetinių grėsmių tendencijos, grėsmių veikėjai ir atakų metodai, taip pat poveikio ir motyvacijos analizė.[10] 2023 m. ENISA Grėsmių žemėlapis apžvelgdamas minėtą laikotarpį apibūdina, kad haktyvizmas (*Hacktivism*[11]) išaugo atsiradus naujoms grupėms, o išpirkos reikalaujančios programos (*Ransomware*) incidentai išaugo 2023 m. pirmąjį pusmetį ir neparodė lėtėjimo požymių. ENISA grėsmių žemėlapio ataskaitoje per nagrinėjamą laikotarpį, nuo 2022 m. liepos 1 d. iki 2023 m. birželio 30 d., iš viso buvo užfiksuota 24 690 pažeidžiamumų, neįskaičiuojant tų, kurie buvo atmesti, užginčyti arba rezervuoti. Tai yra reikšmingas padidėjimas, palyginti su 21 920 pažeidžiamumų, nurodytų ankstesnėje ataskaitoje laikotarpiu nuo 2021 m. liepos 1 d. iki 2022 m. birželio 30 d.[12] Tuo tarpu Lietuvoje pagal Nacionalinio kibernetinio saugumo centro parengtą Nacionalinę kibernetinio saugumo būklės ataskaitą už 2022 metus nurodoma, kad 2022 NKSC CERT-LT iš viso užregistravo 4 080 kibernetinių incidentų, jų skaičius išliko panašus, kaip ir 2021 m.[13]

---

[9] ENISA Threat Landscape 2023. P. 4. Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[10] ENISA Threat Landscape research method. Prieiga: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-research-method
[11] Haktyvizmas - kompiuterinės sistemos griovimas politiniais ar socialiniais tikslais. Chandler D. and Munday R. A Dictionary of Social Media. Oxford University Press. Published online: 2016. eISBN: 9780191803093. Prieiga: https://www.oxfordreference.com/
[12] ENISA Threat Landscape 2023. P. 39. Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[13] Nacionalinis Kibernetinio Saugumo Centras. Nacionalinė kibernetinio saugumo būklės ataskaita 2022. P. 32 Prieiga: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf

Matomas didėjantis kibernetinių atakų skaičius kelia nerimą. ES institucijos į tai reagavo 2022 gruodžio 14 d. Priimant ir nuo 2023 m. Sausio 1 d. Įsigaliojant Europos Parlamento ir Tarybos direktyvai (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (toliau – NIS2), kuri pakeitė iki tol nuo 2018 m. Galiojančią direktyvą NIS. Iki 2024 m. Spalio 17 d. Lietuva įsipareigojo perkelti NIS2 į Lietuvos teisės aktus. Tikimasi, kad griežtesnius reikalavimus įvesianti NIS2 padidins organizacijų atsparumą kibernetinėms grėsmėms bei sumažins kibernetinio saugumo įgyvendinimo skirtumus tarp Europos Sąjungos valstybių narių. Taip pat NIS2 įtvirtina kibernetinio saugumo reikalavimus platesniam subjektų ratui: prie NIS įtvirtintų energetikos, transporto, bankininkystės, finansų rinkos infrastruktūros, sveikatos priežiūros, geriamo vandens tiekimo ir skaitmeninės infrastruktūros ypatingos svarbos sektorių, NIS2 pridėti nuotekų, IRT paslaugų valdymo (verslas verslui), viešojo administravimo ir kosmoso sektoriai. Pašto ir kurjerių paslaugos, atliekų tvarkymas, cheminių medžiagų gamyba ir platinimas, gamyba ir maisto gamyba, perdirbimas ir platinimas, skaitmeninių paslaugų tiekėjai bei mokslinių tyrimų organizacijos išskirti NIS2 trečiame priede kaip kiti svarbūs sektoriai.[14] NIS 2 preambulėje pabrėžiama, kad „į šios direktyvos taikymo sritį patenka tam tikros mažosios įmonės ir labai mažos įmonės, kurios atitinka specifinius kriterijus, pagal kuriuos parodomas jų esminis vaidmuo visuomenei, ekonomikai arba konkretiems sektoriams ar paslaugų rūšims“. Taigi NIS2 skatins kibernetinio saugumo pokyčius keliant kibernetinio saugumo brandą ne tik kritinės infrastruktūros ir didelėse organizacijose, tačiau ir mažose bei vidutinėse įmonėse (toliau – MVĮ).[15].

Remiantis NIS2 organizacijų skirstymu į MVĮ ir dideles įmones, taip pat siekiant įvertinti, kokios kibernetinės atakos būdingos organizacijoms, kurios yra brandžios kibernetinio saugumo prasme, ir kurios ne, taip pat siekiant išanalizuoti kibernetinio saugumo prasme brandžios organizacijos, pagrindinius iššūkius, ir, pasirinktas organizacijų skirstymas į dideles, mažas ir vidutines. ES yra daugiau kaip 23 mln. MVĮ, kurios sudaro 99 proc. įmonių ir suteikia dvi iš trijų privačiojo sektoriaus darbo vietų. Jos yra pagrindinis ekonomikos variklis.[16] NIS2 56-ajame preambulės punkte nurodoma, kai kurios MVĮ susiduria su konkrečiomis kibernetinio saugumo problemomis, pvz., mažu kibernetiniu sąmoningumu, nuotolinio IT saugumo trūkumu, didelėmis kibernetinio saugumo sprendimų sąnaudomis ir išaugusiu grėsmių lygiu, pvz.,

---

[14] Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti. Prieiga: https://eur-lex.europa.eu/eli/dir/2022/2555

[15] Pagrindiniai požymiai išskiriantys MVĮ yra darbuotojų skaičius ir apyvarta arba bendra balanso suma. ES narėse MVĮ kategorijai priskiriamos įmonės, kuriose dirba mažiau nei 250 darbuotojų bei kurių metinė apyvarta neviršija 50 mln. EUR ir (arba) metinis balansas neviršija 43 mln. EUR sumos. 2003 m. gegužės 6 d. Europos Komisijos rekomendacija dėl labai mažų, mažų ir vidutinių įmonių apibrėžimo 2003/361/EC 2 straipsnis. Prieiga: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

[16] EUR-Lex žodynas. Mažosios ir vidutinės įmonės. Prieiga: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=LEGISSUM:sme

išpirkos reikalavimo programinės įrangos grėsme, kurių klausimu jos turėtų gauti gaires ir pagalbą.[17] Daugelis MVĮ turi iliuziją, kad atakos aukos yra tik didelės įmonės ir remiantis šiuo pagrindu saugo savo vertingus duomenis labai silpnai.[18] MVĮ dažnai neturi žinių ir išteklių, kad galėtų taikyti informacijos saugumo priemones plačiai.[19] Tuo tarpu korporacijų informacijos ir technologijų paslaugos yra pažeidžiamos dėl įvairių saugumo pavojų šiuolaikinėje informacinėje aplinkoje, įskaitant neskelbtinų duomenų nutekėjimą ir užsitęsusius el. pašto ir interneto prieigos sutrikimus – visa tai daro didelę įtaką verslo tęstinumui.[20] Viešieji subjektai vis labiau priklauso nuo sudėtingų, tarpusavyje susijusių ir integruotų informacinių sistemų. Pagrindinės pramonės šakos sudaro pagrindinę valstybės infrastruktūrą, įskaitant telekomunikacijas, energetiką, sveikatos priežiūrą, žemės ūkį ir transportą. Ekonomika vis labiau priklauso nuo informacinės infrastruktūros, kuri yra esminis pramonės tęstinumo elementas.[21]

A. Chidukwani, S. Zander and P. Koutsakis straipsnyje „Apklausa apie mažų ir vidutinių įmonių kibernetinį saugumą: iššūkiai, tyrimų kryptis ir rekomendacijos“ (2022) teigia, kad užpuolikai renkasi lengvą taikinį – mažas ir vidutines įmones, kurios nežino arba neturi pakankamai išteklių sustiprinti savo tinklus ir informacijos išteklius. Nepaisant gerai žinomų priemonių verslui apsaugoti nuo kibernetinių atakų, mažos ir vidutinės įmonės ir toliau yra kibernetinių atakų aukos. Statistika rodo, kad 62 % Australijos mažų ir vidutinių įmonių pranešė, kad tapo kibernetinių atakų aukomis. Ši statistika yra glaudžiai susijusi su 2017 m. pasauline statistika, pagal kurią 66 % mažų ir vidutinių įmonių pranešė, kad per pastaruosius 12 mėnesių jų organizacija patyrė kibernetinę ataką. Ši statistika kelia susirūpinimą ne tik mažoms ir vidutinėms įmonėms, bet ir tiekėjams bei klientams, kurie dirba su jomis. Daugelis mažų įmonių neturi supratimo ir žinių apie kibernetinių atakų keliamas grėsmes. Dėl išteklių stokos, kadangi įmonės yra mažos, jos nekreipia dėmesio į kibernetinio saugumo grėsmes. Skelbtina verslo informacija kartu su kitais duomenimis yra prieinama kaip labai vertinamas skaitmeninis turtas. Tai tapo pelningu kibernetinių nusikaltėlių taikiniu. Pastebima, kad smulkusis verslas susiduria su kibernetinio saugumo iššūkiais ir nėra nei apsirūpinę įranga nuo jų apsiginti, nei pakankamai žino apie grėsmes, kylančias prisijungus prie interneto.[22] Kibernetinės

[17] Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti. Prieiga: https://eur-lex.europa.eu/eli/dir/2022/2555
[18] Teufel, S., Teufel, B., Aldabbas, M., Nguyen, M. (2020). Cyber Security Canvas for SMEs. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Botha, R. (eds) Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science, vol 1339. Springer, Cham. https://doi.org/10.1007/978-3-030-66039-0_2
[19] Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). A {Large-Scale} Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 1235-1252).
[20] Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. Authorea Preprints.
[21] Gorka, Marek. (2022). Cybersecurity culture in the public and private sector area in the central european region. Nowa Polityka Wschodnia, 2022(4), 51-71, p. 53
[22] Ullah, B., & Nab, S. I. (2022). Developing cyber security strategies for business organization to prevent data breaches. KASBIT Business Journal, 15(4), 62. P. 62-63

grėsmės nediskriminuoja pagal organizacijos dydį, o tai reiškia, kad mažos ir vidutinės įmonės yra jautrios toms pačioms grėsmėms kaip ir didelės organizacijos. Nors didesnės įmonės turi didesnį atakų plotą, daugiau darbuotojų ir įrenginių, didesnės organizacijos taip pat daugeliu atvejų turi žmogiškųjų ir finansinių išteklių, kad galėtų įdiegti kontrolę. Didesnėse organizacijose paprastai dirba specialūs kibernetinio saugumo darbuotojai, turintys atitinkamą išsilavinimą. Mažos ir vidutinės įmonės mažiau investuoja į kibernetinį saugumą, tačiau, kalbant apie sėkmingų kibernetinių atakų finansinį poveikį, jos patiria proporcingai didesnes išlaidas nei didelės įmonės. Mažos ir vidutinės įmonės turi potencialų pranašumą, nes yra mažos ir judrios su lankstesnėmis IT priemonėmis. [23]

Taigi galima išskirti pagrindinius kibernetinio saugumo iššūkius MVĮ ir didelėse organizacijose:

Mažos ir vidutinės įmonės (mažiau nei 250 darbuotojų)	***Didelės įmonės (daugiau nei 250 darbuotojų)***
mažas kibernetinis sąmoningumas nuotolinio IT saugumo trūkumas, didelės kibernetinio saugumo sprendimų sąnaudos, išaugęs kibernetinių atakų skaičius nežino arba neturi pakankamai išteklių sustiprinti savo tinklus ir informacijos išteklius neturi supratimo apie kibernetinių atakų keliamas grėsmes (kompetencijų stoka) išteklių stoka	pažeidžiamos dėl neskelbtinų duomenų nutekėjimo ir užsitęsusių el. pašto ir interneto prieigos sutrikimai didelis atakų plotas, daug darbuotojų ir jų įrenginių per kuriuos galima įsilaužti

1 Lentelė. Pagrindiniai kibernetinio saugumo iššūkiai MVĮ ir didelėse organizacijose.

Atsižvelgiant į 1 lentelėje išanalizuotus pagrindinius kibernetinio saugumo iššūkius MVĮ ir didelėse organizacijose, bei tai, kas išdėstyta, galima teigti, kad net jei su daugiau iššūkių susiduria MVĮ, didelėse įmonėse išlieka didesnė galimybė įsilaužti per didesnį kiekį įrenginių, paveikti didesnį skaičių darbuotojų. Didelių įmonių pranašumas yra kompetentingi specialistai ir finansiniai ištekliai, kurie reikalingi užtikrinti kibernetiniam saugumui organizacijose. Vadinasi, didelės įmonės yra linkusios labiau rūpintis kibernetiniu saugumu nei MVĮ, nes finansiniai ištekliai leidžia ne tik įdarbinti patyrusius kibernetinio saugumo specialistus, tačiau ir įdiegti kibernetinio saugumo sprendimus, todėl galima teigti, kad didelės organizacijos yra labiau brandžios kibernetinio saugumo prasme, nei MVĮ.

[23] A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," in IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899. Prieiga: https://ieeexplore.ieee.org/abstract/document/9853515

Vienos didžiausių komunikacijos technologijų kompanijos pasaulyje „Verizon“ 2023 metų Duomenų pažeidimo tyrimo ataskaitoje nurodoma, kad vis dažniau tiek MVĮ, tiek didelės įmonės naudojasi panašiomis paslaugomis ir infrastruktūra, o tai reiškia, kad jų atakų paviršiai turi daug daugiau bendro nei bet kada anksčiau. Tačiau labai skiriasi organizacijų gebėjimas reaguoti į grėsmes dėl išteklių, kuriuos jos gali panaudoti užpuolimo atveju, skaičiaus.

2020 m. „Verizon“ Duomenų pažeidimo tyrimo ataskaitoje palyginami mažų, vidutinių ir didelių organizacijų kibernetinių atakų duomenys:

	Mažos ir vidutinės įmonės (mažiau nei 1 000 darbuotojų)	***Didelės įmonės (daugiau nei 1 000 darbuotojų)***
Dažnis (*Frequency*)	407 incidentai, 221 su patvirtintu duomenų atskleidimu	8 666 incidentai, 576 su patvirtintu duomenų atskleidimu
Populiariausi modeliai (*Top patterns*)	Žiniatinklio programos, visa kita ir įvairios klaidos sudaro 70 % pažeidimų.	Visa kita, *Crimeware*[24] ir piktnaudžiavimas privilegijomis sudaro 70 % pažeidimų
Užpuolikai (*Threat actors*)	Išoriniai (74 %), vidaus (26 %), partneriai (1 %), keli (1 %) (pažeidimai)	Išoriniai (79 %), vidiniai (21 %), partneriai (1 %), keli (1 %) (pažeidimai)
Užpuoliko motyvai (*Actor motives*)	finansiniai (83 %), šnipinėjimas (8 %), linksmybės (3 %), pyktis (3 %)	finansiniai (79 %), šnipinėjimas (14 %), linksmybės (2 %), pyktis (2 %)
Pažeisti duomenys (*Data compromised*)	Kredencialai (52 %), asmeniniai (30 %), kiti (20 %), vidaus (14 %), medicininiai (14 %)	Kredencialai (64 %), kiti (26 %), asmeniniai (19 %), vidiniai (12 %)

2 Lentelė. Mažų ir vidutinių, ir didelių organizacijų kibernetinių atakos 2020 m.[25]

2023 metų „Verizon“ Duomenų pažeidimo tyrimo ataskaitoje pateikiamos lentelės iliustruojančios faktą, kad MVĮ ir didelės organizacijos tampa vis labiau panašios viena į kitą. Ataskaitoje teigiama, kad šis reiškinys prasidėjo prieš kelerius metus, o dabar liko labai mažai skirtumų, susijusių su organizacijos dydžiu.[26]

[24] *Crimeware* - bendras terminas, naudojamas apibūdinti bet kokią programinę įrangą, kuri naudojama nusikaltimui internete padaryti, pavyzdžiui, virusas gali būti apibūdintas kaip nusikalstama programinė įranga. Chandler D. and Munday R. A Dictionary of Social Media. Oxford University Press. Published online: 2016. eISBN: 9780191803093. Prieiga: https://www.oxfordreference.com/

[25] Verizon Data Breach Investigations Report 2020. P. 79. Prieiga: https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

[26] Verizon Data Breach Investigations Report 2023. P. 65. Prieiga: https://www.verizon.com/business/resources/reports/dbir/

	Mažos įmonės ***(mažiau nei 1 000 darbuotojų)***	***Didelės įmonės*** ***(daugiau nei 1 000 darbuotojų)***
Dažnis **(*Frequency*)**	699 incidentai, 381 su patvirtintu duomenų atskleidimu	496 incidentai, 227 su patvirtintu duomenų atskleidimu
Populiariausi modeliai **(*Top patterns*)**	Įsibrovimas į sistemą (*System intrusion*), socialinė inžinerija ir pagrindinės žiniatinklio taikomųjų programų atakos sudaro 92 % pažeidimų	Įsibrovimas į sistemą (*System intrusion*), socialinė inžinerija ir pagrindinės žiniatinklio taikomųjų programų atakos sudaro 85 % pažeidimų
Užpuolikai **(*Threat actors*)**	išoriniai (94 %), vidiniai (7 %), keli (2 %), partneriai (1 %).	Išoriniai (89 %), vidiniai (13 %), keli (2 %), partneriai (2 %)
Užpuoliko motyvai **(*Actor motives*)**	Finansiniai (98 %), šnipinėjimas (1 %), patogumas (1 %), pyktis (1 %)	Finansiniai (97 %), šnipinėjimas (3 %), ideologija (2 %), patogumas (1 %), linksmybės (1 %)
Pažeisti duomenys **(*Data compromised*)**	Kredencialai (54 %), vidiniai (37 %), kiti (22 %) , Sistema (11 %)	vidinis (41 %), įgaliojimai (37 %) , Kita (30 %), sistema (22 %)

3 Lentelė. Mažų ir vidutinių, ir didelių organizacijų kibernetinių atakos 2023 m.[27]

MVĮ kibernetinių atakų 2020 ir 2023 m., (2 ir 3 lentelių) palyginimas:

- Dažnis: bendras incidentų skaičius padidėjo beveik 300, 150 atakų daugiau su patvirtintu duomenų atskleidimu.
- Populiariausi modeliai: 2020 m. žiniatinklio programos sudarė 70% visų atakų, o 2023 m. be žiniatinklio taikomųjų programų, buvo naudojami ir įsibrovimai į sistemą, socialinė inžinerija ir visai tai sudarė 92% pažeidimų.
- Užpuolikai: 2020 m. Išoriniai sudarė 74 %, vidaus 26 %, tuo tarpu 2023 m. išoriniai jau sudaro 94 % įsilaužimų.
- Užpuoliko motyvai: finansiniai motyvai nuo 83% 2020 m., pakilo iki 98 % 2023 m., šnipinėjimas nuo 8% 2020 m. sumažėjo iki 1% 2023 m.
- Pažeisti duomenys: 2023 m. išliko panašus procentas kredencialų: 2020 - 52%, 2023 - 54%.

Didelių įmonių kibernetinių atakų 2020 ir 2023 m. (2 ir 3 lentelių) palyginimas:

- Dažnis: bendras incidentų skaičius sumažėjo aštuoniais tūkstančiais: nuo 8666 incidentų 2020 m. iki 496 incidentų 2023 m.

[27] Verizon Data Breach Investigations Report 2023. P. 65. Prieiga: https://www.verizon.com/business/resources/reports/dbir/

- Populiariausi modeliai: 2020 m. *Crimeware* ir piktnaudžiavimas privilegijomis sudaro 70 % pažeidimų, tuo tarpu 2023 m. Įsibrovimas į sistemą, socialinė inžinerija ir pagrindinės žiniatinklio taikomųjų programų atakos sudaro 85 % pažeidimų.
- Užpuolikai: 2020 m. Išoriniai sudarė 79 %, vidaus 21 %, tuo tarpu 2023 m. išoriniai jau sudaro 89 % įsilaužimų.
- Užpuoliko motyvai: finansiniai motyvai nuo 79 % 2020 m., pakilo iki 97 % 2023 m., šnipinėjimas nuo 14 % 2020 m. sumažėjo iki 3% 2023 m.
- Pažeisti duomenys: 2020 m. kredencialai sudarė 64 %, 2023 m. svarbūs tampa didelių įmonių vidiniai 41 % duomenys ir įgaliojimai 37 %.

Didelės įmonės kaip brandžios organizacijos kibernetinio saugumo prasme, įsidiegusios kibernetinio saugumo brandos modelius tampa atsparios ir pajėgios reaguoti į kibernetines grėsmes, tai rodo ryškus kibernetinių atakų skaičius sumažėjimas 2023 m. lyginant su 2020 m. Tuo tarpu užpuolikų dėmesys nukreipiamas į MVĮ, nes jos dažniausiai nėra pritaikiusios kibernetinio saugumo priemonių, arba pritaikiusios labai siaura apimtimi. Matomas populiariausių įsibrovimo modelių kitimas tobulėjant technologijoms, o tai reiškia, kad organizacijoms reikalingas kibernetinio saugumo brandos modelis, kuris leidžia efektyviai reaguoti į besikeičiančias kibernetines grėsmes: veiksmingai identifikuoti, įgyvendinti saugumo priemones ir reaguoti į incidentus. Užpuolimo motyvai tampa labiau finansiniai ir tai tik rodo, kad visos organizacijos tampa svarbios, kaip finansinio pasipelnymo objektas bei taikinys kibernetinėms atakoms. Pažeistų duomenų analizė 2020 ir 2023 m. rodo, kad kredencialai išlieka pagrindiniu kibernetinių atakų tikslu nukreiptų prieš MVĮ, tuo tarpu kibernetinių atakų, nukreiptų prieš dideles įmones, pažeisti duomenys keičiasi, tampa svarbūs vidiniai duomenys, kurie turėtų būti konfidencialūs ir apsaugoti.

Analizuojant kibernetinio saugumo brandos svarbą organizacijose esminiu aspektu tampa tarptautiniu ir nacionaliniu lygmeniu priimami teisės akai, keliantys reikalavimus įsidiegti kibernetinio saugumo priemones, kurios yra kibernetinio saugumo brandos organizacijoje dalis: priimamos saugumo politikos ir taisyklės organizacijų viduje, paskirstomi finansiniai, techniniai ir žmogiškieji ištekliai, užtikrinant nenutrūkstamą sistemų saugumą ir tęstinumą, ir svarbiausia – atsparumą besikeičiančioms kibernetinėms grėsmėms, greitai reaguojant į jas ir minimalizuojant jų daromą žalą. Kibernetinio saugumo branda organizacijose užtikrina organizacijų nuolatinį tobulėjimą, kuris parengia organizacijas besikeičiančioms kibernetinėms grėsmėms nuolat tobulinant saugumo politikas, technologijas ir procesus, svarbu ne tik pasiekti, tačiau ir išlaikyti. Didelės organizacijos, kurios yra finansiškai pajėgios investuoti į kibernetinį saugumą, vis tiek išlieka pažeidžiamos ir tampa kibernetinių atakų taikiniais, taip gali būti ir dėl to, kad organizacijose įdiegti kibernetinio saugumo brandos modeliai yra neefektyvūs ir/ar

nefunkcionuojantys. Taip gali nutikti ir tada, kai organizacijos formaliai įsidiegia kibernetinio saugumo modelius kad taptų patrauklios investuotojams, tačiau po modelio įdiegimo organizacijoje išlieka žema kibernetinio saugumo kultūra. Tobulėjant technologijoms, o kartu ir kibernetinėms grėsmės tampa nebesvarbus organizacijos dydis, organizacija didelė, ar maža, ar vidutinė, kiekviena iš jų turi silpnųjų ir stipriųjų aspektų kibernetinio saugumo srityje, tad tik efektyvi kibernetinio saugumo branda organizacijose yra svarbiausia priemonė, leidžianti pasiekti ir užtikrinti aukštą kibernetinio saugumo lygį ne tik identifikuojant silpnąsias ir stipriąsias organizacijų sritis, tačiau ir bendrai keliant organizacijų saugumo kultūrą, jų darbuotojų sąmoningumą, prisidedant prie bendro organizacijų veiklos tęstinumo.

1.2. KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIŲ PASIRINKIMAS

Praktikoje yra išskiriami tiek visuotinai pripažinti kibernetinio saugumo brandos modeliai, kuriems dažniausiai reikalingas papildomas sertifikavimas, atitikimas standartui bei gerosios praktikos ir sistemos. Straipsnio autoriai Y.Maleh, A.Sahid & M.Belaissaoui (2021) literatūros apžvalgoje išskiria, kad organizacijos, vietoj to, kad kurtų savo kibernetinio saugumo vertinimo modelius, mieliau renkasi tarptautiniu mastu pripažintas sistemas bei išskiria gerąsias praktikas:

- Informacinių technologijų ir susijusių technologijų kontrolės tikslai (COBIT), padedantys sumažinti riziką, įvertinti strateginio suderinamumo brandą ir IT vertę (*Mataracioglu ir Ozkan, 2011; Raup-Kounovsky ir kt., 2010; Saetang ir Haider, 2011; Simonsson ir kt. al., 2008*)
- Nacionalinis standartų ir technologijos institutas (NIST) ITG, 2008 m.; (*Dlamini ir kt., 2009*).
- Tarptautinė standartizacijos organizacija (ISO) / Tarptautinė elektrotechnikos komisija (IEC) 27000 saugumo standartų šeima (*ITG, 2008*), pvz., ISO17799 (*Spafford, 2003*) ir ISO27001 (*Mataracioglu ir Ozkan, 2011*)
- Sertifikuotas informacinių sistemų saugumo profesionalas (CISSP) (*Harris, 2007 m.*)
- Oficialiai ISO/IEC 27032 sprendžia „kibernetinį saugumą“ arba „kibernetinės erdvės saugumą“, vadinamą „informacijos konfidencialumo, vientisumo ir prieinamumo palaikymu elektroninėje erdvėje“.[28]

Autoriai D. Sulistyowati, F.Handayani ir Y. Suryanto (2020) analizuoja:

- Kibernetinio saugumo brandos modelį (*Cybersecurity Capability Maturity Model (C2M2)*) – tai programa, kurią JAV Energetikos departamentas (DOE) išleido (2019 m.) ir pasižymi savybių, rodiklių rinkiniu, atspindinčiu tam tikros mokslo srities galimybes ir plėtrą.

[28] Yassine Maleh, Abdelkebir Sahid & Mustapha Belaissaoui (2021) A Maturity Framework for Cybersecurity Governance in Organizations, EDPACS, 63:6, 1-22, DOI: 10.1080/07366981.2020.1815354, p.6

- NIST, kurio dabartinė sistema suteikia išsamų vertinimą, kurį sudaro trys esminiai komponentai, o būtent branduolys *(core)*, įgyvendinimo lygis *(implementation level)* ir profilis *(profile).*
- ISO/IEC 27002, kuris pateikia sisteminį požiūrį į organizacinių informacinių sistemų valdymą ir kontrolę, siekiant išlaikyti tris pagrindinius aspektus, būtent konfidencialumą, vientisumą ir informacijos prieinamumą.
- COBIT, kuris yra valdžios, informacijos ir technologijų valdymo sistema, valdomas kaip visa įmonė.
- Mokėjimo kortelių pramonės duomenų saugumo standartas (PCI DSS) (*Payment Card Industry Data Security Standard (PCI DSS)*), kuris yra pasaulinis mokėjimo kortelių (kredito, debeto, bankomato) duomenų saugumo standartas, skirtas visiems subjektams, kurie apdoroja, saugo ar perduoda kortelės turėtojo duomenis ir (arba) slaptus autentifikavimo duomenis, perduodamus internetu.

K. Agafonov (2021) lygina šiuos kibernetinio saugumo brandos modelius:

- SANS, kuris yra sukurtas SANS instituto ir pažymi, kad egzistuoja penki esminės veiksmingos kibernetinės gynybos sistemos principai, kuriais yra grindžiama visa instituto parengta kibernetinio saugumo valdymo sistema: gynybinių mechanizmų parinkimas, prioritetų nustatymas, vertinimo sistemos nustatymas, nuolatinis situacijos vertinimas ir grėsmių mažinimas bei apsaugos priemonių automatizavimas.
- NIST, kuris yra sudarytas ir 3 sričių, kurių pagrindinis tikslas yra nusakyti ir užtikrinti organizacijos vykdomų funkcijų ir vidaus procesų sąsają su kibernetinio saugumo valdymu organizacijoje: kibernetinio saugumo modelio branduolys, kibernetinio saugumo įgyvendinimo pakopos, kibernetinio saugumo valdymo profilis.
- $(ISC)^2$ – Tarptautinio informacinių sistemų saugumo sertifikavimo konsorciumo (*International Information Systems Security Certification Consorcium)* sukurta sertifikuotų informacinių sistemų sugumo profesionalų *(Certified Information Systems Security Professionals (CISSP)*) mokymo programa, kuri dabartiniu laikotarpiu yra viena iš labiausiai paplitusių kibernetinio saugumo specialistų ruošimo ir sertifikavimo programų.
- ISO 27001/27002 standartas skirtas organizacijoms ir sudarytas kaip rekomendacinių priemonių rinkinys, kurio paskirtis užtikrinti organizacijos išteklių valdymą bei įgyvendinti visuotinai pripažintas informacijos saugumo valdymo priemones.

Moksliniuose šaltiniuose išskiriami modeliai ir gerosios praktikos, kurie padeda organizacijoms užtikrinti kibernetinį atsparumą. Pabrėžtina, kad kibernetinio saugumo brandos modeliai vertindami organizacijų brandą dažniausiai remiasi individualiais vertinimo kriterijais, tačiau galima išskirti keletą bendrų kriterijų visiems modeliams ir gerosioms praktikoms: tai organizacijų politikos, procedūros, saugumo technologijos, atnaujinimų, pažeidžiamumų, rizikos valdymas, darbuotojų mokymai, atsakas į incidentus, atitiktis galiojantiems teisės aktams.

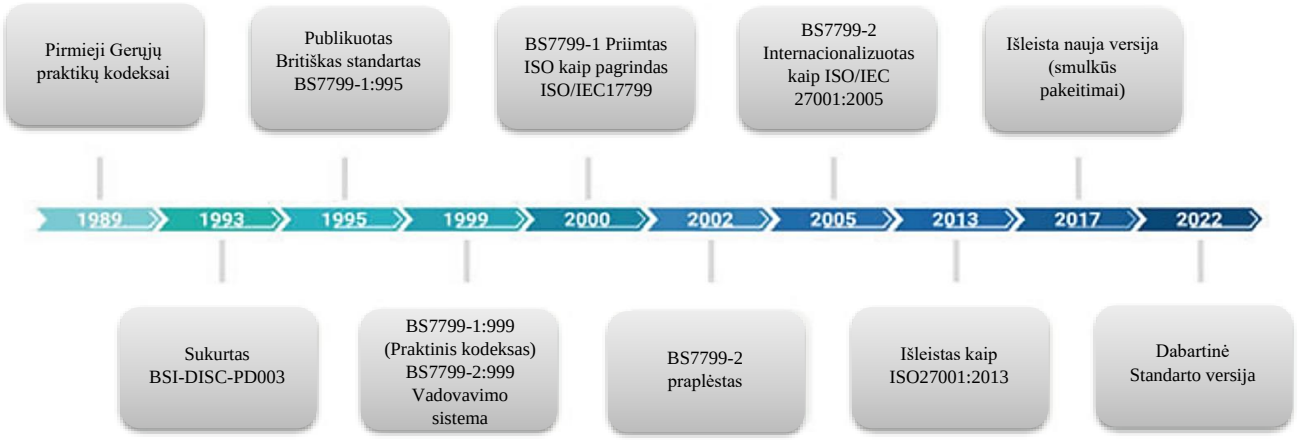
Šiame darbe bus nagrinėjami visuose aukščiau minėtuose šaltiniuose aptarti populiariausi pasaulyje kibernetinio saugumo brandos modeliai: ISO 27001:2013 ir NIST (2018 m.) 1.1versija.

1.3. ISO 27001 KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIS

Apžvalga

ISO 27001 Standartas buvo sukurtas Europoje bendradarbiaujant Tarptautinei standartizacijos organizacijai (ISO) ir Tarptautinei elektrotechnikos komisijai (IEC) ir 2005 m. paskelbtas kaip BS 7799 raida. Jis „[...] nustato steigimo, įgyvendinimo, priežiūros ir nuolatinius reikalavimus tobulinti informacijos saugumo valdymo sistemą (ISMS) atsižvelgiant į organizaciją“; reikalavimai „[...] yra bendrieji ir skirti taikyti visoms organizacijos, nepaisant tipo, dydžio ar pobūdžio“ (ISO/IEC 27001:2013).[29] Tarptautinis ISO/IEC 27001 standartas atsirado 1995 m. pavadinimu BS 7799 „Informacijos saugumo valdymas – Praktinis kodeksas informacijos saugumo valdymui“, – britų reguliavimą paskelbė Britų standartų institutas, atsižvelgdamas į Anglijos organizacijų poreikį kontroliuoti saugumą, susijusį su informacijos saugumu. [30]

2 paveikslas pateikia ISO 27001 standarto kūrimo detalią laiko juostą.



2 Paveikslas. ISO 27001 standarto kūrimo laiko juosta. Šaltinis: Alrehili, A. A., & Alhazmi, O. H. (2023)

[29] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. TQM Journal, 33(7), p. 77. https://doi-org.skaitykla.mruni.eu/10.1108/TQM-09-2020-0202

[30] Marco Sartor, & Guido Orzes. (2019). Quality Management : Tools, Methods and Standards: Vol. First edition. Emerald Publishing Limited., p. 246

ISO 27000 standartų šeima sukurta bendradarbiaujant Tarptautinei standartizacijos organizacijai (ISO) ir Tarptautinei elektrotechnikos komisijai (IEC) padėti organizacijoms užtikrinti privatumo saugumą, IT saugumą ir kibernetinį saugumą. ISO 27001 standartas yra pripažintas visame pasaulyje ir numato reikalavimus kuriant, diegiant, prižiūrint ir nuolat tobulinant informacijos saugumo valdymo sistemą (ISMS).[31] ISO 27000 standartų šeimą sudaro daugiau nei tuzinas standartų, kurie nuolat yra atnaujinami ir keičiami, dėl to tikslus skaičius nėra žinomas, tačiau yra išskiriami pagrindiniai:

- ISO 27000, numatantis informacijos saugumo valdymo sistemų (ISMS) apžvalgą, taip pat pateikia terminus ir apibrėžimus, dažniausiai naudojamus ISMS standartų šeimoje.
- ISO 27002, pateikiantis gaires organizacijoms, norinčioms sukurti, įdiegti ir tobulinti informacijos saugumo valdymo sistemą (ISMS), orientuotą į kibernetinį saugumą. ISO/IEC 27001 apibrėžia ISMS reikalavimus, ISO/IEC 27002 siūlo geriausią praktiką ir kontroles, susijusias su pagrindiniais kibernetinio saugumo aspektais.
- ISO 27004, nustatantis informacijos saugumo valdymo sistemos (ISMS), įskaitant jos procesus ir kontrolę, veiksmingumo stebėjimus ir matavimus, jų analizę ir vertinimą.
- ISO 27005, pateikia gaires, padedančias organizacijoms įvykdyti ISO/IEC 27001 reikalavimus dėl informacijos saugumo rizikos.
- ISO 27014, pateikia informacijos saugumo valdymo principų ir procesų gaires, pagal kurias organizacijos gali įvertinti, vadovauti ir stebėti informacijos saugumo valdymą.
- ISO 27036, apibūdina išorinių šalių tiek pirkėjų, tiek tiekėjų informacijos saugumą. Padeda organizacijoms diegti informacijos saugumo kontrolę, susijusią su tiekėjų santykiais.

Pats ISO 27001 padeda organizacijoms įsivertinti rizikas bei efektyviai pašalinti trūkumus, įtraukiant žmones, procesus ir technologijas. Dėl naujų technologijų įdiegimo ir didėjančio sistemos sudėtingumo ISO27001 standartas laikui bėgant vystėsi ir brendo. Šiuo metu naujausia ISO 27001 versija yra ISO/IEC 27001:2022, išleista 2022 m. spalį[32] su nauju pavadinimu „ISO/IEC27001:2022 Informacijos sauga, kibernetinis saugumas ir privatumo apsauga – informacijos saugumo valdymo sistemos – reikalavimai“. Pirmoji ISO 27001 versija (ISO/IEC 27001:2005) buvo paskelbta 2005 m. spalio mėn., veiksmingai pakeitusi BS77992 kaip audito standartą informacijos valdymo sistemų brandumui ir veiksmingumui

[31] Schiavone, M., & Kirk, B. (2023). Transitioning to ISO 27001:2022. Pennsylvania CPA Journal, 94(2), 21.
[32] Lietuvos Respublikos Vyriausybės Nacioanlinis Akreditacijos Biuras paskelbė, kad 2022 m. Spalio 25 d. Išleistas standartas 27001:2022 ir jam nustatytas trejų metų pereinamasis laikotarpis. Vadinasi, organizacijos trejų metų laikotarpyje bus sertifikuojamos pagal naująją standarto versiją. Prieiga: https://nab.lrv.lt/lt/naujienos/del-standarto-iso-iec-27001-2022-taikymo-atnaujinta-2023-02-27/

nustatyti. Dabartinė versija yra 2-osios versijos (ISO/IEC 27001:2013), kuri buvo paskelbta 2013 m., patobulinimas[33].

Tiek ISO 27001:2013, tiek ISO 27001:2022 standarto versijas sudaro 11 punktų, sunumeruotų nuo 0 iki 10:

0. Įvadas: pristatomas standartas ir jo paskirtis.

1. Taikymo sritis: suteikia labai aukšto lygio vaizdą apie ISMS ir rizikos valdymo reikalavimus, nurodytus likusioje standarto dalyje. Taip pat paaiškinama, kad standartas yra bendras ir taikomas įvairiose pramonės šakose ir įvairiose įmonėse.

2. Normatyvinės nuorodos: paaiškina ryšį tarp ISO 27000 ir 27001 standartų.

3. Terminai ir apibrėžimai: apima standarte vartojamą terminiją.[34]

Likę punktai (4–10) yra privalomi ISO 27001 reikalavimai ir, jei organizacijai reikia ISO 27001 sertifikato, ji turi atitikti ir išlaikyti visus tuos privalomus reikalavimus.

4. Organizacijos kontekstas, kuris apima pačios organizacijos supratimą, suinteresuotų šalių ir jų poreikių supratimą, ISMS apimties nustatymą ir sistemą.

5. Vadovavimas. Organizacija turi apibrėžti vadovybės įsipareigojimus, politiką, organizacinius vaidmenis, atsakomybes ir įgaliojimus. Pabrėžiamas vadovybės įsitraukimas į ISMS.

6. Planavimas apima veiksmus, skirtus spręsti rizikas ir galimybes, taip pat informacijos saugumo tikslus ir planavimą juos pasiekti.

7. Palaikymas. Standarto punktas apima išteklius, kompetencijas, sąmoningumą, komunikaciją, dokumentuotą informaciją ir eksploataciją, kurie būtini sėkmingam ISMS funkcionavimui.

8. Veikimas. Nustatoma, kad organizacija turi apsibrėžti, kaip atlieka veiklos planavimą ir kontrolę, informacijos saugumo rizikos vertinimą bei informacijos saugumo rizikos valdymą.

9. Veiklos įvertinimas apima stebėjimą, matavimą, analizę ir vertinimą, vidinius auditus ir valdymo peržiūrą.

10. Tobulinimas nurodo organizacijoms įgyvendinti nuolatinio tobulinimo kultūrą, stebėti ir apsibrėžti neatitiktis ir korekcinius veiksmus. [35]

[33] Junaid, T. S.(2023). ISO 27001: Information Security Management Systems. DOI: 10.13140/RG.2.2.36267.52005. Prieiga: https://www.researchgate.net/publication/367166657 p. 2-3
[34] Grimmick, R. (2022). ISO 27001 compliance: Essential tips and insights. Information & Records Management Society Bulletin, 229, p. 23, 28-29
[35] ISO/IEC 27001. Tarptautinis standartas. ISO/IEC FDIS 27001:2022(E)

ISO 27001:2013 versijos Priedas A (žr. 3 Priedas), kuris numatė 114 kontrolių, kurios buvo suskirstytos į 14 grupių:

A.5 Informacijos saugumo politika

A.6 Informacijos saugumo organizavimas

A.7 Žmogiškųjų išteklių saugumas

A.8 Turto tvarkymas

A.9 Prieigos valdymas

A.10 Kriptografija

A.11 Fizinis ir aplinkos saugumas

A.12 Darbo saugumas

A.13 Ryšių saugumas

A.14 Sistemų įsigijimas, kūrimas ir priežiūra

A.15 Santykiai su tiekėjais

A.16 Informacijos saugumo incidentų valdymas

A.17 Veiklos tęstinumo valdymo informacijos saugumo aspektai

A.18. Atitiktis

Svarbu paminėti, kad ISO 27001 standarto Priedas A nėra privalomas: taip pabrėžiamas standarto universalumas, leidžiantis kiekvienai įmonei prisitaikyti ir pasirinkti reikiamas kontroles.

Naujojoje ISO 27001:2022 Standarto versijoje atlikti nedideli dokumentacijos ir procesų pakeitimai, o didžiausi pakeitimai – standarto priede A – išsamiame kontrolės tikslų ir priemonių sąraše. Pats A priedo pavadinimas pakeistas iš „Nuorodos į kontrolių tikslus ir kontroles“ (*Reference control objectives and controls*) į „Informacijos saugumo kontrolės nuorodos“ (*Information security controls reference*). Taip pat matomos išskirtos 4 pagrindinės kontrolių grupės:

1) Organizacinės kontrolės priemonės (5 punktas);
2) Žmonių kontrolė (6 punktas);
3) Fizinė kontrolė (7 punktas);
4) Technologinė kontrolė (8 punktas). [36]

Buvo įtraukta 11 naujų valdiklių, nors bendras kontrolių skaičius sumažėjo nuo 114 iki 93: 57 kontroliniai elementai buvo sujungti į 24 kontroles; viena kontrolė buvo padalinta į dvi; 35 kontrolės liko nepakitę, o 23 buvo pervadintos, bei pridėta 11 naujų valdiklių. Schiavone, M., & Kirk, B. (2023) nurodo, kad naujosios

[36] ISO/IEC 27002. Tarptautinis standartas. ISO/IEC 27001:2022 (E), p.7

kontrolės susijusios su technologijų pažanga ir pasikeitusiomis rizikomis nuo ISO 27001:2013 išleidimo. Nauji valdikliai yra tokie:

• Grėsmės žvalgyba (*Threat intelligence*);

• Informacijos saugumas debesijos paslaugoms (*Information security for cloud services*);

• IRT (Informacijos ir ryšių technologijų) pasirengimas veiklos tęstinumui (*ICT readiness for business continuity*);

• Fizinio saugumo stebėjimas (*Physical security monitoring*);

• Konfigūracijos valdymas (*Configuration management*);

• Informacijos ištrynimas (*Information deletion*);

• Duomenų maskavimas (*Data masking*);

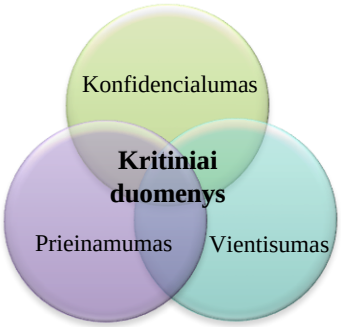
• Duomenų nutekėjimo prevencija (*Data leakage prevention*);

• Stebėsenos veikla (*Monitoring activities*);

• Interneto filtravimas (*Web filtering*);

• Saugus kodavimas (*Secure coding*).

Kaip matyti, standarto punktai įtraukia ne tik vadovybę ar už informacijos saugumą atsakingus asmenis organizacijoje, tačiau ir visus darbuotojus, jų atsakomybes, darbo procesus, o taip pat ir pateikia galimas kontroles norimiems tikslams pasiekti . P.J. Blount (2020) apie patį ISO standartą teigia, kad jis padeda nustatyti informacijos saugumui keliamas rizikos sritis ir nustatyti bei priimti priemones šiai rizikai sumažinti pasitelkiant valdymo priemonių, kurias galima pasirinkti, sąrašą. Calder, A. (2009) teigia, kad ISO 27001 apibrėžia ISMS, kaip bendros valdymo sistemos dalį, pagrįstą verslo rizikos požiūriu ir kuria siekiama sukurti, įgyvendinti, eksploatuoti, stebėti, peržiūrėti, palaikyti ir gerinti informacijos saugumą. ISMS egzistuoja siekiant išsaugoti organizacijos konfidencialumą, vientisumą ir prieinamumą. Kaip matyti 3 Paveiksle, ISMS užtikrina organizacijos informacijos ir informacijos išteklių konfidencialumą, vientisumą ir prieinamumą, o svarbiausi jos informacijos ištekliai yra tie, kuriuos apima visi trys požymiai.



3 Paveikslas. Informacinio turto požymiai. Šaltinis: Calder, A. (2009).

Atsižvelgiant į tai, kas išdėstyta, ISO 27001 standartas nustato griežtus reikalavimus apimančius visą organizaciją, vadinasi, kibernetinis saugumas yra užtikrinamas visuose lygiuose, o tai reiškia, kad ISO 27001 kaip kibernetinio saugumo brandos vertinimo modelis padeda organizacijoms valdyti su kibernetiniu saugumu susijusius procesus ir rizikas, juos nuolat tobulinti ir prisitaikyti prie besikeičiančių aplinkybių.

Pagrindiniai vertinimo kriterijai

Pagal pačio ISO 27001 standarto išskiriamas privalomas 4-10 sąlygas, išskirti pagrindiniai ISO 27001 standarto kaip kibernetinio saugumo brandos organizacijoje vertinimo kriterijai pateikti 4 Lentelėje.

Organizacijos kontekstas	Organizacinis kontekstas – nustatyti ISMS tikslai, vidinės ir išorinės problemos, kurios gali turėti įtakos jos efektyvumui; Trečiosios šalys - suinteresuotosios šalys, įskaitant taikomi įstatymai, reglamentai, sutartys ir kt. bei nustatyti su informacijos saugumu susiję jų reikalavimai, ir įsipareigojimai ISMS taikymo sritis - dokumentuota ISMS apimtis ISMS – sukurta, įgyvendinta ir nuolat atnaujinama
Vadovavimas	Lyderystė ir įsipareigojimas - aukščiausioji vadovybė rodo lyderystę ir įsipareigojimą ISMS Politika - dokumentuota ISMS politika Organizaciniai vaidmenys, pareigos ir įgaliojimai – priskirta informacijos saugumo pozicija
Planavimas	Veiksmai, skirti spręsti rizikas ir galimybes – sukurta / suplanuota ISMS, kad ji atitiktų reikalavimus, sprendžiant rizikas ir galimybes; apibrėžtas bei taikomas informacijos saugumo rizikos vertinimo procesas; dokumentuotas bei taikomas informacijos saugumo rizikos mažinimo procesas Informacijos saugumo tikslai ir planai – nustatykite informacijos saugumo tikslai ir planai
Palaikymas	Ištekliai – nustatyti ir paskirstyti būtinieji ištekliai ISMS Kompetencijos – nustatytos, dokumentuotos ir pateiktos reikiamos kompetencijos Informuotumas – sukurta saugumo informavimo programą Komunikacija – nustatytas ISMS susijusių vidinių ir išorinių ryšių poreikis Dokumentuota informacija – pateikti pagal standartą ir organizacijos reikalaujami dokumentai; pateikti dokumentų pavadinimai, autoriai ir pan.; peržiūrėta, patvirtinta ir tinkamai kontroliuojama dokumentacija
Veikimas	Veiklos planavimas ir kontrolė – planuoti, įgyvendinti, kontroliuojami ir dokumentuoti ISMS procesai, kad rizika būtų valdoma (rizikos valdymo planas) Informacijos saugumo rizikos vertinimas – (iš naujo) įvertintos ir dokumentuotos informacijos saugumo rizikos reguliariai ir per pokyčius Informacijos saugumo rizikos mažinimas – įgyvendintas rizikos valdymo planą (rizika mažinama ir dokumentuoti rezultatai
Veiklos įvertinimas	Stebėjimas, matavimas, analizė ir vertinimas – stebimos, matuojamos, analizuojamos ir vertinamos ISMS ir kontrolės priemonės Vidinis auditas – planuojamas ir atliekamas ISMS vidaus auditus Vadovybės peržiūra – reguliariai atliekama ISMS vadovybės peržiūra
Tobulinimas	Neatitikimas ir taisomieji veiksmai – nustatoma, pataisoma ir imamasi veiksmų siekiant užkirsti kelią neatitikimų pasikartojimui, dokumentuojant veiksmus Nuolatinis tobulinimas – nuolat tobulinama ISMS

4 Lentelė. ISO 27001 pagrindiniai vertinimo kriterijai. Šaltinis: ISO/IEC 27001.

Be 4 lentelėje pateiktų vertinimo kriterijų, svarbu paminėti ISO 27001 standarto Priede A esantį kontrolių sąrašą, kuris turi būti vertinamas paraleliai, kaip papildantis ir nurodantis konkrečias įgyvendinimo kontroles (3 Priedas).

ISO 27001 kaip kibernetinio saugumo brandos organizacijoje vertinimo modelio efektyvumas grindžiamas atitikimu minėtiems kriterijams, kurių yra laikomasi, bei stebint praktinį ISMS funkcionavimą per veiklos įrašus, dokumentaciją. Standartas taikomas visoje organizacijoje ir apima ne kažkurią dalį, tačiau visą organizaciją, todėl ir standarto keliami reikalavimai yra nuo dokumentacijos, įrodymų rinkimo, iki visų procesų įvertinimo ir tobulinimo.

Įdiegimas organizacijoje

Autorius Murphy, G. (2022) straipsnyje „Kelionė į ISO Sertifikavimą“ nurodo, kad keturi ISO etapai yra planuoti, daryti, patikrinti ir veikti. Šeši žingsniai iki projekto planavimo etapo yra tokie:

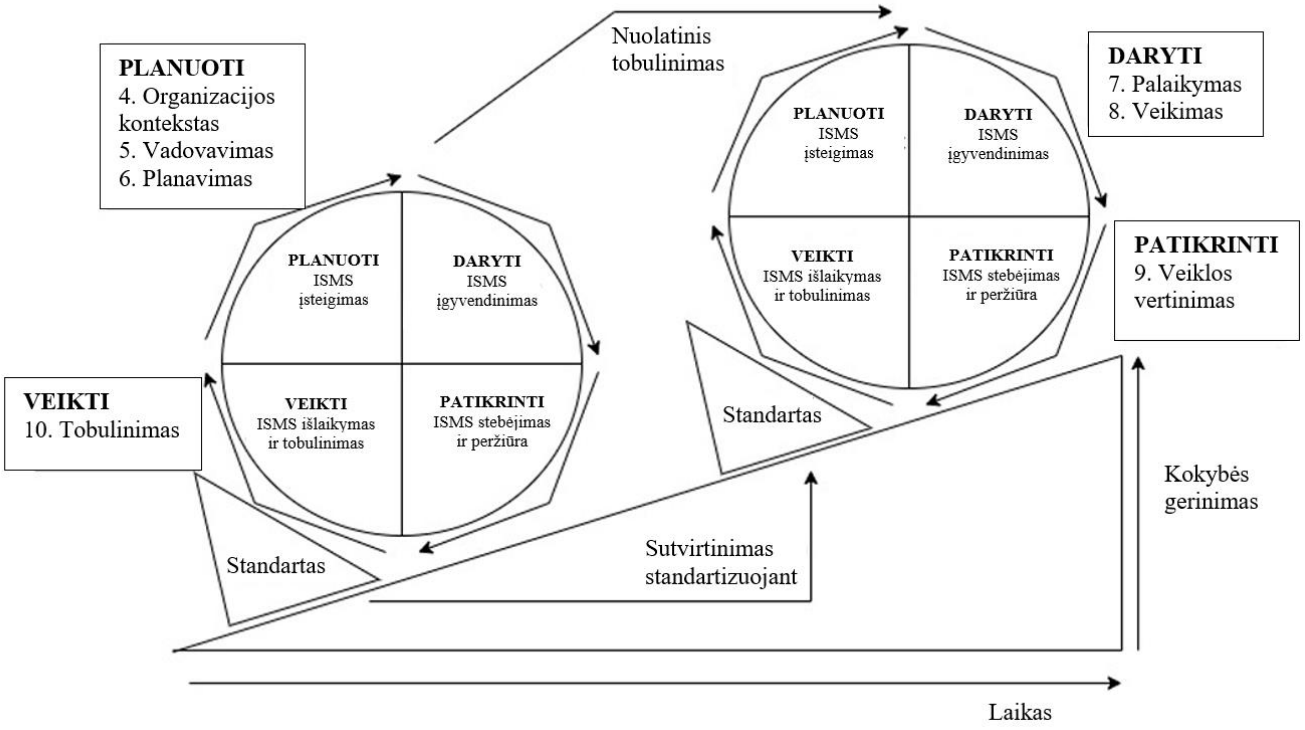
1. Priimti kibernetinio saugumo sistemą.
2. Gauti aukščiausios vadovybės įsipareigojimą ISMS.
3. Apibrėžti sisteminį požiūrį į informacijos saugumo rizikos vertinimą ir rizikos priėmimo kriterijus.
4. Atlikti rizikos vertinimą pagal ISMS taikymo sritį.
5. Nustatyti ir įvertinti šios rizikos valdymo galimybes, „susieti“ įmonės kontrolę su kibernetinio saugumo rizika.
6. Pagal ISO standartus parengti pritaikomumo pareiškimą ir rizikos valdymo planą.

Planavimo etapas apima rizikos vertinimą. Autorius nurodo, kad tiek vidinė, tiek išorinė rizika, kuri gali trukdyti pasiekti veiksmingos ISMS tikslą, turi būti nustatyta ir įtraukta į rizikos vertinimą. Konkrečiai organizacijai sukurtas rizikos vertinimas turėtų būti glaudžiai susijęs su ISO 27001 A priede nurodytais nuorodų valdymo ir kontrolės tikslais. Užbaigus pirminį rizikos vertinimą, rezultatai turi būti peržiūrimi kartu su vyresniąja vadovybe, kad jie galėtų įvertinti galimus veiksnius, į kuriuos rizikos savininkai galbūt neatsižvelgė. Sutariama dėl bet kokių būtinų atnaujinimų, o rizikos vertinimas užbaigiamas kaip oficialus ISO rizikos valdymo planas. **Daryti** etapo žingsniai yra šie:

1. Užbaigti rizikos valdymo planą ir jo dokumentaciją.
2. Įgyvendinti rizikos mažinimo planą ir suplanuotą kontrolę.
3. Surengti atitinkamus darbuotojų mokymus ir informavimo programas.
4. Valdyti operacijas ir išteklius pagal ISMS.
5. Įdiegti procedūras, leidžiančias greitai aptikti saugumo incidentus ir į juos reaguoti.

Patikrinimo etapas apima nuolatinį tobulėjimą stebint, peržiūrint, testuojant ir atliekant auditą. ISO reikalauja nepriklausomo audito, kuris gali būti atliktas naudojant vidinį auditą, bendradarbiaujant arba tam tikru jų deriniu. **Veikimo** etapas apima audito rezultatų / išvadų svarstymą, taip pat nuolatinį savo procesų atnaujinimą ir tobulinimą, pasimokius iš modeliavimo pratybų, incidentų, faktinių nustatytų grėsmių ir reakcijų į jas, informacijos saugumo pokyčių ir kitų patobulinimų.

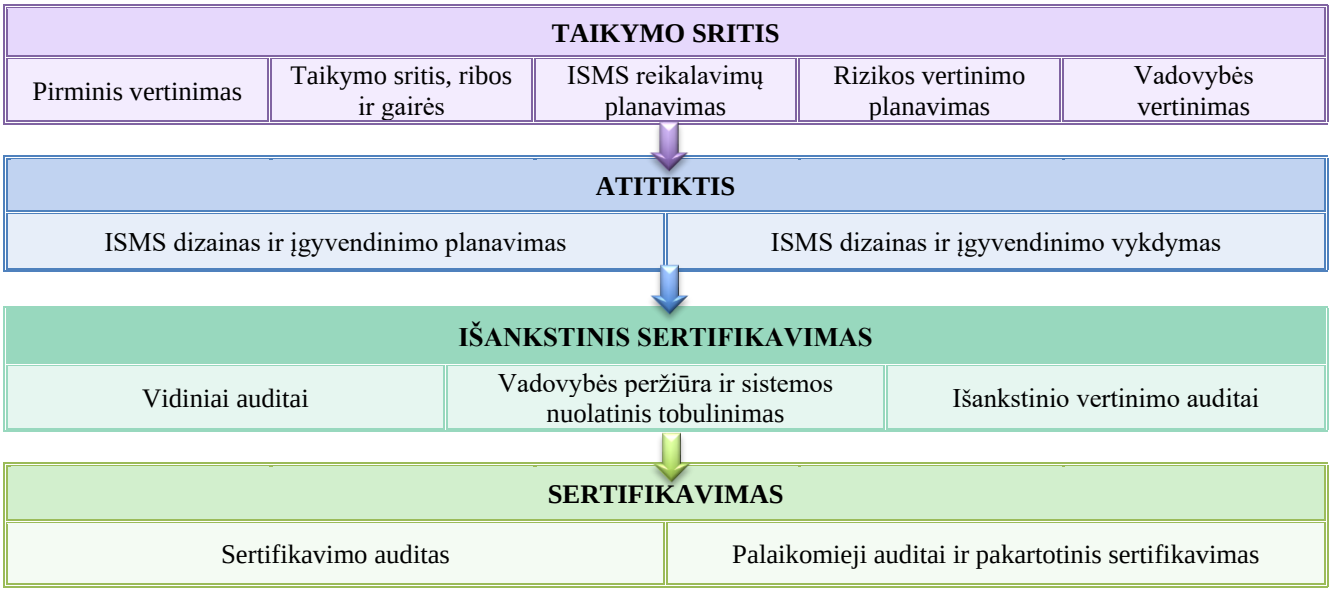
Junaid, T. S. (2023) taip pat teigia, kad ISO 27001 standartus galima nesunkiai įgyvendinti laikantis „Planuoti, Daryti, Patikrinti ir Veikti“ ciklo, kilusio iš kokybės užtikrinimo. ISMS kokybė gerės laikui bėgant laipsniškai pristatant laikantis minėto ciklo. 4 Paveikslas parodo, kaip ISO 27001 gali būti įdiegtas su „Planuoti, Daryti, Patikrinti ir Veikti“ ciklu, didinant valdymo procesų judrumą, aiškumą ir objektyvumą. Privalomi standarto 4, 5, 6 punktai (organizacijos kontekstas, vadovavimas, planavimas) pateks į Plano etapą su ISMS įsteigimu. ISMS bus įgyvendinta Daryti etape, kuris apima 7 ir 8 privalomus punktus. Patikrinimo etape bus atliktas ISMS stebėjimas ir peržiūra, kad būtų įvykdytas privalomas 9 punktas (veiksmingumo vertinimas). Paskutinė ciklo dalis yra Veikti, kuriame aptariama techninė priežiūra ir ISMS patobulinimas, laikantis ISMS sąlygos.



4 Paveikslas. Ciklas „Planuoti, Daryti, Patikrinti ir Veikti“. Šaltinis: Junaid, T. S. (2023).

Vadinasi, norint organizacijai įsidiegti ISO 27001 standartą, lengviausia tai padaryti vadovaujantis autorių minimais 4 etapais: Planuoti, Daryti, Patikrinti ir Veiki. Tačiau pirmiausia organizacijoje turėtų būti

vadovybės paskirtas atsakingas žmogus, kuris būtų atsakingas už organizacijos parengimą ISO 27001 auditui, išanalizuotų standarto reikalavimus, kaip ir kokia apimtimi jie taikomi organizacijoje. Dar iki planavimo stadijos organizacija turi apsibrėžti bei priimti savo informacijos saugumo strategiją, politiką ir rizikos valdymo procesus, atlikti informacijos saugumo auditą ar rizikos vertinimą, analizuojant organizacijos atitiktį standarto reikalavimams ir kontrolėms. Atkreiptinas dėmesys, kad prieš įdiegiant standartą, organizacija sertifikavimo įstaigai turi pateikti užpildytą tinkamumo pareiškimą, o tai yra ISO 27001 standarto Priedo A kontrolės, kurias organizacija nusprendžia taikyti. Tuomet **planavimo** etapas, apimantis ISMS įsteigimą, kurio metu kuriama organizacijos ISMS: dokumentacija, procesai, techninė bei programinė įranga reikalingi įgyvendinti siekiamiems informacijos saugumo tikslams, rizikos valdymo procesai ir kiti su informacijos saugumu susiję procesai. Tuomet, pagal Junaid, T. S. (2023), organizacija turi apibrėžti ISMS apimtį su pirminiu vertinimu, apimtimi, ribomis ir gairėmis, reikalavimų analize, rizikos valdymo planavimu, vadovybės vertinimu ir t.t. Kita dalis yra atitikties etapas, kai baigiamas ne tik projektavimas ir įgyvendinimo planavimas, bet ir šių planų vykdymas, kuris turi atitikti standartus. Prieš gaudama sertifikatą, organizacija turi atlikti išankstinį sertifikavimo auditą ir įvertinimą, kuris padės sužinoti, kurie procesai atitinka standartą ir kuriuos procesus reikia tobulinti. Tuomet jau sertifikavimo auditas. Svarbu paminėti, kad sertifikavimo auditui reikia atsakingai rinktis sertifikavimo organizaciją, nes tik įgaliotos sertifikavimo organizacijos gali išduoti galiojančius ISO 27001 sertifikatus. Po sėkmingo sertifikavimo audito, galiausiai organizacija gauna oficialų ISO 27001 sertifikatą, kurio galiojimo laikas yra treji metai, o kas metus – palaikomieji auditai. Pasibaigus sertifikato galiojimo laikui, organizacijai reikia kreiptis dėl pakartotinio sertifikavimo. 5 Paveikslas iliustruoja ISO 27001 sertifikato gavimo ir išlaikymo procesą:



5 Paveikslas. ISO 27001 sertifikato gavimas. Šaltinis: Junaid, T. S. (2023).

Murphy, G. (2022) rekomenduoja, gavus sertifikatą, pranešti apie tai savo suinteresuotosioms šalims, kad sertifikatas įkvėptų pasitikėjimo, pašalintų kibernetinio saugumo klausimynus, sumažintų draudimo įmokas ir labai sumažintų bet kokių būsimų kibernetinio saugumo įvykių riziką. Junaid, T. S. (2023) taip pat pabrėžia ISO27001 sertifikato naudą: jis turi didžiulę ekonominę ir reputacinę naudą, kuri ne tik sumažina saugumo atakų daromą žalą, bet ir įtikina partnerius, klientus, akcininkus, kad saugumo atakos atveju bus imtasi apsaugos veiksmų siekiant išsaugoti organizacijos turtą. Sertifikatas pagerina bendrą organizacijos struktūrą, padeda išvengti norminių baudų ir sumažina dažnų auditų poreikį. ISO 27000 standartų šeima pateikia geriausios praktikos rekomendacijas ir gaires, kaip įdiegti ISMS analizuojant riziką ir įdiegiant saugias apsaugos priemones su saugumo kontrole. Autorė pabrėžia ISO 27001 yra technologiškai agnostinė ir nuo pardavėjo nepriklausoma ISMS sistema, tinkanti bet kokio dydžio ir bet kokio tipo organizacijoms. ir prijungiamas prie kiekvieno jo sektoriaus.[37] P.J. Blount (2020) teigia, kad ISO 27001 turi du svarbius požymius, kurie yra svarbūs priimant įmonės kibernetinio saugumo planą. Pirma, pripažįstama, kad nėra kibernetinio saugumo, kuris tinkamas visiems. Vietoj to, tai yra individualus procesas, kurį lemia daugybė veiksnių, tokių kaip įmonės vieta, joje naudojamų informacinių sistemų tipai, tvarkomų duomenų tipai ir daugybė kitų veiksnių, turinčių įtakos konkrečios įmonės rizikos profiliui. subjektas. Tai reiškia, kad pats standartas yra lankstus ir pritaikomas konkretiems jį ketinančių įgyvendinti subjektų poreikiams. Antra, ji pripažįsta vertę kuriant ir įrodomąjį informacijos saugumo veiksmų įrašą. Neužtenka tik įmonei pasakyti, kad ji įdiegė ISO 27001, ta įmonė turės sugebėti per politiką, sutartis, žurnalus ir įvairius kitus įrodymus parodyti, kad ji iš tikrųjų įgyvendino reikiamas kontrolės priemones.

Jei ne vidinė organizacijų motyvacija išlaikyti ISMS, tai kasmetiniai priežiūros auditai skatina organizacijas vykdyti ir laikytis visų įsipareigojimų ISMS ir ISO 27001 standartui. Visi autoriai pabrėžia ISO 27001 standarto įdiegimo naudą organizacijoje, nes kaip kibernetinio saugumo brandos organizacijoje vertinimo modelis, jis yra universalus, pritaikomas bet kokio dydžio organizacijai, veikiantis ir naudingas. Finansinė ir reputacinė nauda ne tik visai organizacijai, tačiau ir akcininkams, prekių/paslaugų tiekėjams ir gavėjams, darbuotojams, pačios organizacijos fiziniam saugumui.

[37] Junaid, T. S.(2023). ISO 27001: Information Security Management Systems. DOI: 10.13140/RG.2.2.36267.52005. Prieiga: https://www.researchgate.net/publication/367166657 p. 2-3

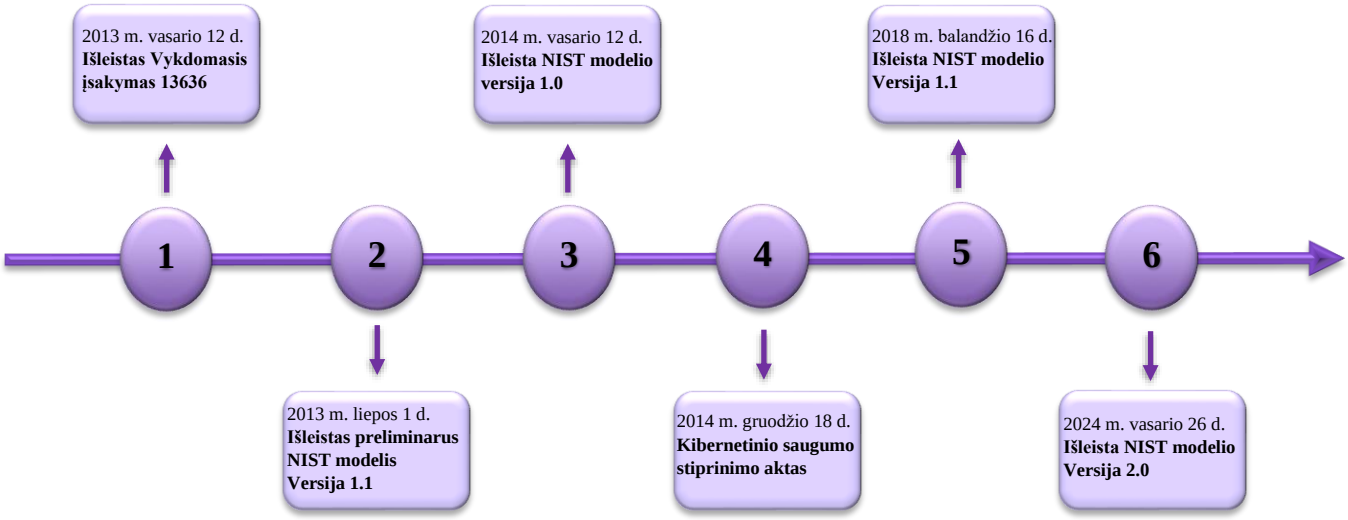
1.4. NIST KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIS

Apžvalga

Jungtinių Amerikos Valstijų Nacionalinis standartų ir technologijų institutas (toliau - NIST) yra atsakingas už standartų ir gairių, įskaitant minimalius reikalavimus, kūrimą, kad būtų užtikrintas tinkamas informacijos saugumas visoms agentūros operacijoms ir turtui. 2012 m. parengė Kompiuterių apsaugos Incidentų valdymo vadovą pagal Jungtinių Amerikos Valstijų Federalinį informacijos saugumo valdymo įstatymą (FISMA) 2002 m., tačiau tokie standartai ir gairės buvo netaikomos nacionalinėms saugumo sistemoms.[38] NIST reaguodamas į vykdomąjį įsakymą (EO) 13636, 2014 m. vasario mėn. paskelbė savo kibernetinio saugumo modelio (*CSF* arba *Framework*) 1.0 versiją kaip pagerinti ypatingos svarbos infrastruktūros objektų kibernetinį saugumą. Nuo to laiko šią sistemą visų pramonės šakų organizacijos priėmė kaip su kibernetiniu saugumu susijusios rizikos valdymo gaires.[39] 2014 m. Kibernetinio saugumo stiprinimo aktas (*Cybersecurity Enhancement Act of 2014*, toliau - CEA) atnaujino NIST vaidmenį, įtraukdamas kibernetinio saugumo rizikos sistemų, skirtų ypatingos svarbos infrastruktūros savininkams ir operatoriams, savanoriškam naudojimui, nustatymą ir plėtojimą. Pasitelkdama CEA, NIST turėjo nustatyti „prioritetinį, lankstų, pakartojamą, našumu pagrįstą ir ekonomiškai efektyvų metodą, įskaitant informacijos saugumo priemones ir kontrolę, kurias gali savanoriškai taikyti ypatingos svarbos infrastruktūros objektų savininkai ir operatoriai, kad padėtų jiems nustatyti, įvertinti ir valdyti kibernetinio ryšio rizikas“. Tai įformino ankstesnį NIST darbą kuriant 1.0 pagrindų versiją pagal vykdomąjį įsakymą (EO) 13636 „Kritinės infrastruktūros kibernetinio saugumo gerinimas“ (2013 m. vasario mėn.), ir buvo pateiktos gairės dėl būsimos NIST modelio evoliucijos. Modelyje, kuris buvo sukurtas pagal EO 13636 ir toliau tobulinama pagal CEA, naudojama bendra kalba, skirta spręsti ir valdyti kibernetinio saugumo riziką ekonomiškai efektyviu būdu, atsižvelgiant į verslo ir organizacinius poreikius, nenustatant įmonėms papildomų reguliavimo reikalavimų.[40] Be to, JAV prezidentas Trumpas 2017 m. gegužę išleido vykdomąjį įsakymą 13800, pavadintą „Federalinių tinklų ir ypatingos svarbos infrastruktūros stiprinimas“, kuris nukreipia federalines agentūras į NIST kibernetinio saugumo modelį, ir vadovas yra įpareigotas naudoti modelį kibernetinio saugumo rizikai valdyti ir pateikti rizikos valdymo ataskaitą Valstybės saugumo sekretoriatui. 2018 metais buvo išleistas NIST kibernetinio saugumo modelio leidinys, kuris papildo 2014 metų versiją. Kaip nurodoma leidinio pradžioje, „tai yra nuolatinio bendradarbiavimo, kuriame dalyvauja pramonė,

[38] Cichonski P., Millar T., Grance T., Scarfone K., Recommendations of the National Institute of Standards and Technology. Special Publication 800-61, Revision 2, 2012. Prieiga: http://dx.doi.org/10.6028/NIST.SP.800-61r2 , p. 4
[39] Hudson D., Macallister J., Pote M., A Guide to Assessing Security Maturity. Carbon black. White paper. 2019, p. 3
[40] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. Prieiga: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf , p. v

akademinė bendruomenė ir vyriausybė, rezultatas[41]“. 2024 m. vasario 26 d. NIST savo tinklapyje pranešė apie išleistą naują NIST modelio versiją 2.0, kuris sukurtas glaudžiai bendradarbiaujant su suinteresuotosiomis šalimis ir atspindintis naujausius kibernetinio saugumo iššūkius bei valdymo praktiką, šiuo atnaujinimu siekiama, kad sistema būtų dar tinkamesnė platesnei vartotojų grupei JAV ir užsienyje. NIST 2.0 yra išplėsta ir apima ne tik ypatingos svarbos infrastruktūros objektų, kaip ligoninių ir elektrinių, apsaugą, bet ir visas organizacijas bet kuriame sektoriuje. Taip pat naujas dėmesys skiriamas valdymui, kuris apima tai, kaip organizacijos priima ir vykdo pagrįstus sprendimus dėl kibernetinio saugumo strategijos.[42] 6 paveikslas pateikia NIST modelio laiko juostą:



6 Paveikslas. NIST modelio laiko juosta. Šaltinis: nist.gov

Taherdoost H.(2022) pateikia glaustą informaciją apie NIST specialiųjų publikacijų (toliau - SP) seriją SP800. SP 800 standartinė serija iš pradžių buvo sukurta siekiant patenkinti privatumo ir saugumo reikalavimus federalinėse informacinėse sistemose; tačiau vėliau juo naudojosi ir nefederalinės organizacijos. 5 Lentelėje pateikiami NIST SP-800 serijos standartai. Atkreiptinas dėmesys, kad šiame darbe yra nagrinėjamas 2018 metų NIST kibernetinio saugumo modelio versija 1.1.

[41] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. Prieiga: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf , p. iv

[42] NIST Releases Version 2.0 of Landmark Cybersecurity Framework. Prieiga: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

NIST SP-800
NIST rizikos valdymo sistema Kiekviena organizacija privalo laikytis septynių etapų, įskaitant pasirengimą, skirstymą į kategorijas, atranką, įgyvendinimą, vertinimą, leidimų suteikimą ir stebėjimą, procesą, kad būtų valdoma privatumo ir informacijos saugumo rizika. Šis procesas sukurtas kaip išsamus ir išmatuojamas procesas, kuris gali būti kartojamas skirtingu metu**.**
NIST kibernetinio saugumo modelis (NIST CSF) Padeda organizacijoms padidinti kibernetinio saugumo priemones ir suteikia integruotą organizacinę struktūrą įvairiems kibernetinio saugumo požiūriams, renkant geriausią praktiką, standartus ir rekomendacijas. Kitaip tariant, modelis, suteikia galimybę išreikšti kibernetinio saugumo reikalavimus, gali būti veiksminga siekiant atkreipti dėmesį į organizacijos kibernetinio saugumo praktikos spragas.
NIST privatumo sistema NIST privatumo sistemoje daugiausia dėmesio skiriama organizacijų susirūpinimui aptikti ir reaguoti į su privatumu susijusias problemas ir kurti naujoviškas paslaugas bei produktus, kartu atsižvelgiant į asmens privatumą. Ši sistema pagrįsta penkiomis pagrindinėmis funkcijomis, įskaitant identifikavimą, valdymą, kontrolę, bendravimą ir apsaugą.
NIST SP800-12 Pagrindiniai kibernetinio saugumo principai yra išsamiai aprašyti SP800-12 standartų serijoje, paaiškinančioje pagrindinius elementus, įskaitant kompiuterių saugumo vaidmenį palaikant verslo misiją, pabrėžiant kompiuterių saugumo vaidmenį patikimame valdyme, ekonomiškai efektyvaus veiklos svarbą. Aptariamos sąnaudos, svarbios sąvokos ir skirtingų saugos kontrolės priemonių koreliacija, galiausiai siūlomi sprendimai, užtikrinantys išteklių saugumą.
NIST SP 800-53 Šiame standarte daugiausia dėmesio skiriama privatumui ir informacinių sistemų ir organizacijų kontrolei, siekiant apsaugoti organizacijose turtą, asmenis ir operacijas nuo įvairių kibernetinių grėsmių, įskaitant žmogaus klaidas, priešiškas atakas, struktūros gedimus, stichines nelaimes, privatumo riziką ir grėsmes iš užsienio.
NIST SP 800-30 Šiame standarte daugiausia dėmesio skiriama informacinių sistemų rizikos vertinimo kūrimo gairėms. Rizikos vertinimo planai atliekami naudojant NIST SP 800-30, remiantis NIST standarto rekomendacijomis ir principais. Šis standartas padeda suprasti kibernetinę riziką organizacijos sprendimus priimantiems asmenims
NIST SP 800-37 Šiame standarte daugiausia dėmesio skiriama rizikos valdymo sistemos taikymo informacinėse sistemose ir organizacijose gairėms. Šiame standarte pateikiamos rekomendacijos organizacijoms, kaip įgyvendinti ir valdyti privatumo ir saugumo riziką, susijusią su geriausia informacinių sistemų praktika.
NIST SP 800-39 Šiame standarte daugiausia dėmesio skiriama vadovavimui organizacijoms sukurti programai, kuri yra integruota siekiant valdyti informacijos saugumo riziką, susijusią su organizacijos misija, operacijomis, reputacija, funkcijomis, asmenimis, įvaizdžiu ir organizacijos turtu. Šis struktūrizuotas ir lankstus metodas yra skirtas rizikos vertinimui ir stebėjimui bei atitinkamam atsakui. Be to, šis rizikos vadovas nėra skirtas pakeisti kitas su rizika susijusias priemones organizacijose.
NIST SP 800-14 Dažniausiai naudojami saugos principai aprašyti NIST SP 800-14, siekiant padėti vartotojams įgyvendinti kibernetinio saugumo politiką. Šis standartas organizacijoms pateikia reikalavimus, kurių jos turėtų laikytis, kad apsaugotų informacinių technologijų išteklius. NIST SP 800-14 naudojimas užtikrina organizacijų informacinių technologijų saugumo sprendimų pasirengimą kibernetinių grėsmių atveju.

5 Lentelė. NIST SP-800 serijos standartai. Šaltinis: Taherdoost H.(2022)

NIST (2018) nurodoma, kad NIST modelis gali būti pavyzdys tarptautiniam bendradarbiavimui stiprinant kibernetinį saugumą ypatingos svarbos infrastruktūros objektuose ir kituose sektoriuose bei bendruomenėse. Siūlomas lankstus būdas kibernetiniam saugumui spręsti, įskaitant kibernetinio saugumo poveikį fiziniam, kibernetiniam ir žmogiškajam aspektams. Jis taikomas organizacijoms, kurios remiasi technologijomis, nesvarbu, ar jų kibernetinio saugumo pagrindinis dėmesys skiriamas informacinėms technologijoms (IT), pramonės valdymo sistemoms (ICS), kibernetinėms fizinėms sistemoms (CPS) ar prijungtiems įrenginiams apskritai, įskaitant daiktų internetą (IoT). NIST modelis gali padėti organizacijoms

spręsti kibernetinio saugumo klausimus, nes tai turi įtakos klientų, darbuotojų ir kitų šalių privatumui. Be to, NIST modelio rezultatai naudojami kaip darbo jėgos plėtros ir evoliucijos veiklos tikslai. [43] Autoriai L. A.Gordon, M.P.Loeb, ir L. Zhou (2020) nurodo, kad NIST kibernetinio saugumo sistemą plačiai pritaikė JAV įmonės ir vyriausybinės agentūros, taip pat visame pasaulyje. Iš tiesų, NIST kibernetinio saugumo modelis greitai tapo vienu iš, jei ne, plačiausiai priimtų metodų, palengvinančių kibernetinio saugumo rizikos valdymą organizacijose. NIST kibernetinio saugumo sistema yra sąmoningai plati ir lanksti. Iš esmės ji suteikia nedidelę apžvalgą, kaip organizacijos turėtų taikyti kibernetinio saugumo rizikos valdymą, palikdamos išsamią informaciją apie modelio įgyvendinimą kiekvienai įmonei. Nors NIST modelis yra savanoriškas, jis yra pripažintas labai puikia platforma kibernetinio saugumo rizikai įvertinti ir valdyti. Kiekvienai NIST modelio versijai taikomas viešas komentavimo laikotarpis, per kurį įvairių pramonės šakų kibernetinio saugumo ekspertai pateikia grįžtamąjį ryšį ir tobulina, kad geriau atitiktų brandžios kibernetinio saugumo programos tikslus. NIST modelis yra bendra kalba, skirta spręsti ir suprasti kibernetinio saugumo rizikos valdymą, todėl ji ypač naudinga informuojant apie riziką suinteresuotąsias šalis. Aiškių komunikacijos linijų su aukštesne vadovybe nustatymas yra svarbus pirmasis žingsnis siekiant įtraukti kibernetinį saugumą į bendrą organizacijos misiją.[44]

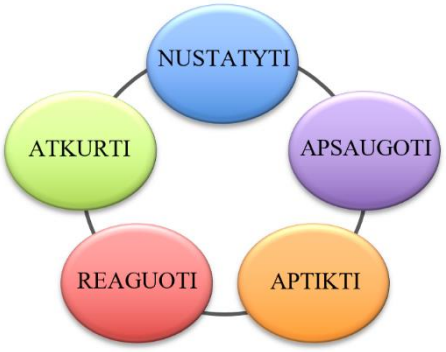
Pats NIST (2018) kibernetinio saugumo brandos vertinimo modelis yra rizika pagrįstas kibernetinio saugumo rizikos valdymo metodas ir susideda iš trijų dalių: branduolių, įgyvendinimo pakopų ir sistemos profilių. Kiekvienas NIST modelio komponentas sustiprina ryšį tarp verslo / misijos varomųjų jėgų ir kibernetinio saugumo veiklos.

- **NIST modelio branduoliai** yra kibernetinio saugumo veiklos, norimų rezultatų ir taikomų nuorodų rinkinys, būdingas ypatingos svarbos infrastruktūros sektoriams. Branduolys pateikia pramonės standartus, gaires ir praktiką tokiu būdu, kuris leidžia perduoti informaciją apie kibernetinio saugumo veiklą ir rezultatus visoje organizacijoje nuo vykdomojo lygio iki įgyvendinimo / operacijų lygio. Modelio branduoliai susideda iš penkių lygiagrečių ir nuolatinių funkcijų – nustatyti, apsaugoti, aptikti, reaguoti, atkurti:
    - *Nustatyti* – plėtoti organizacinį supratimą apie tai, kaip valdyti kibernetinio saugumo rizikas, gresiančias sistemoms, žmonėms, ištekliams, duomenims ir pajėgumams.
    - *Apsaugoti* – parengti ir įgyvendinti tinkamas apsaugos priemones, kad būtų užtikrinamas ypatingos svarbos paslaugų teikimas.

[43] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. Prieiga: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf , p. vi
[44] Hudson D., Macallister J., Pote M., A Guide to Assessing Security Maturity. Carbon black. White paper. 2019, p. 3

- *Aptikti* – plėsti ir įgyvendinti atitinkamą veiklą, kuria siekiama nustatyti kibernetinio saugumo įvykio faktą.
- *Reaguoti* – plėsti ir įgyvendinti atitinkamą veiklą, kad būtų imamasi veiksmų dėl nustatyto kibernetinio saugumo incidento.
- *Atkurti* – plėsti ir įgyvendinti tinkamą veiklą siekiant išlaikyti atsparumo planus ir atkurti visus dėl kibernetinio saugumo incidento sutrikusius pajėgumus ar paslaugas.[45]

Apsvarstytos kartu, šios funkcijos suteikia aukšto lygio strateginį organizacijos kibernetinio saugumo rizikos valdymo gyvavimo ciklo vaizdą (7 Paveikslas). Tada Sistemos branduoliai nustato pagrindines kiekvienos funkcijos pagrindines kategorijas ir subkategorijas, kurios yra atskiri rezultatai, ir suderina jas su pavyzdinėmis informacinėmis nuorodomis, pvz., esamais standartais, gairėmis ir kiekvienos subkategorijos praktika.



7 Paveikslas. NIST modelio branduolys. Šaltinis: NIST, 2018.

NIST (2018) nurodo, kaip branduoliai veikia tarpusavyje:

Funkcijos organizuoja pagrindinę kibernetinio saugumo veiklą aukščiausiu lygiu. Šios funkcijos yra nustatymas, apsauga, aptikimas, atsakymas ir atkūrimas. Jie padeda organizacijai išreikšti savo kibernetinio saugumo rizikos valdymą organizuojant informaciją, įgalinant priimti rizikos valdymo sprendimus, šalinant grėsmes ir tobulėjant mokantis iš ankstesnės veiklos. Šios penkios funkcijos yra suskirstytos į 23 kategorijas ir 108 subkategorijas. Kiekviena subkategorija yra išorinės informacinės medžiagos sąrašas.[46]

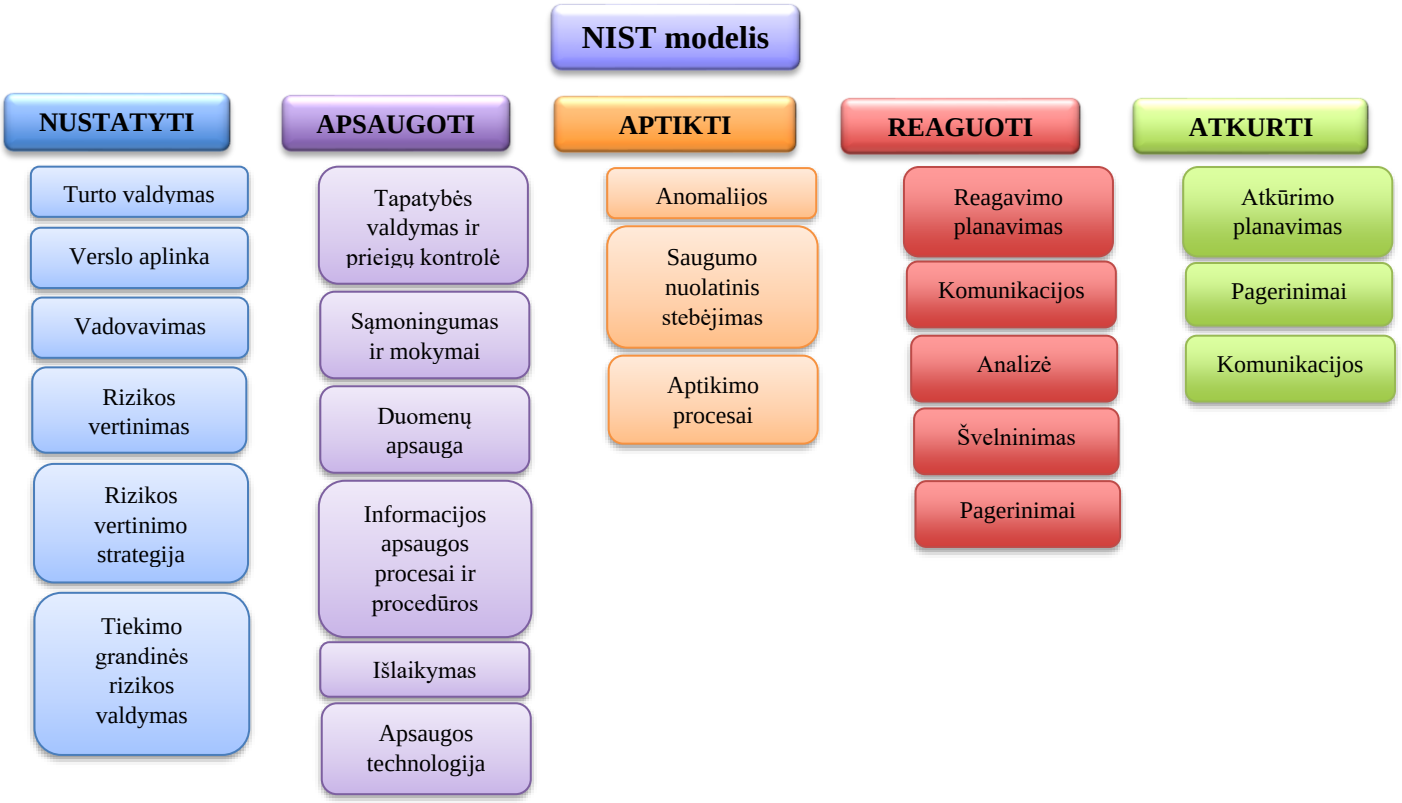
Kategorijos yra funkcijų suskirstymas į kibernetinio saugumo rezultatų grupes, glaudžiai susijusias su programiniais poreikiais ir konkrečia veikla. 8 Paveikslas iliustruoja funkcijas ir kategorijas.

[45] ENISA Nacionalinių pajėgumų vertinimo Sistema. 2020 m. Prieiga: https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-lt.pdf p. 63

[46] Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), p. 226

Subkategorijos toliau skirsto kategoriją į konkrečius techninės ir (arba) valdymo veiklos rezultatus. Jie pateikia rezultatų rinkinį, kuris, nors ir nėra išsamus, padeda siekti kiekvienos kategorijos rezultatų. Subkategorijos pavyzdys: „Išorinės informacinės sistemos yra kataloguojamos“.

Informacinės nuorodos yra specifinės kritinės infrastruktūros sektoriuose paplitusių standartų, gairių ir praktikos skyriai, iliustruojantys metodą, kaip pasiekti su kiekviena subkategorija susijusius rezultatus.



8 Paveikslas. NIST modelio branduolio funkcijos ir kategorijos. Šaltinis: Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020).

- **Modelio įgyvendinimo pakopos** pateikia kontekstą, kaip organizacija vertina kibernetinio saugumo riziką ir taikomus procesus šiai rizikai valdyti. Pakopos apibūdina organizacijos kibernetinio saugumo rizikos valdymo praktikos ypatybes, apibrėžtas struktūroje (pvz., suvokianti riziką ir grėsmes, pakartojama ir prisitaikanti). Pakopos apibūdina organizacijos praktiką įvairiuose diapazonuose: nuo dalinės (1 pakopa) iki prisitaikančios (4 pakopa). Šios pakopos atspindi progresavimą nuo neformalių, reaktyvių reakcijų prie metodų, kurie yra judrūs ir informuoti apie riziką. Pakopų atrankos metu organizacija turėtų atsižvelgti į esamą rizikos valdymo praktiką, grėsmės aplinką, teisinius ir reguliavimo reikalavimus, verslo/misijos tikslus ir organizacinius apribojimus. ENISA Nacionalinių pajėgumų vertinimo sistema (2020) apibūdindama NIST modelio pakopas nurodo, kad pakopas reikia vertinti ne kaip brandos lygius, o kaip sistemą, kuria organizacijoms suteikiama galimybė aplinkybėmis pagrįsti savo požiūrį į kibernetiniam saugumui

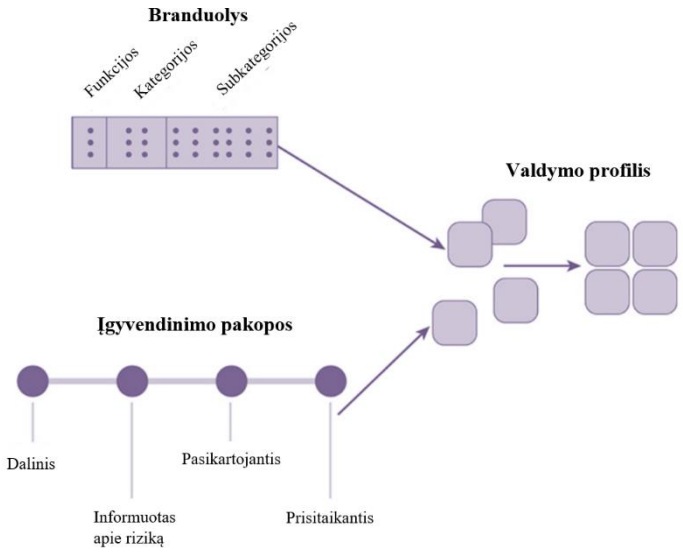
kylančią riziką ir į tai rizikai valdyti taikomus procesus. NIST (2018) teigiama, kad sėkmingas NIST modelio įgyvendinimas grindžiamas organizacijos tiksliniame profilyje(-iuose) aprašytų rezultatų pasiekimu, o ne pakopos nustatymu. Vis dėlto pakopos pasirinkimas ir paskyrimas natūraliai turi įtakos pagrindų profiliams. Verslo / procesų lygio vadovų pakopos rekomendacija, kurią patvirtino vyresniojo vadovo lygis, padės nustatyti bendrą toną, kaip organizacijoje bus valdoma kibernetinio saugumo rizika, ir turės įtakos prioritetų nustatymui tiksliniame profilyje bei pažangos, padarytos spragas, vertinimams. Pakopų apibrėžimai pateikiami 9 Paveiksle:

Rizikos valdymo procesas	**Integruota rizikos valdymo programa**	**Išorinis dalyvavimas**
1 pakopa: **dalinis**		
Organizacijos kibernetinio saugumo rizikos valdymo praktika nėra formalizuota, o rizika valdoma *ad hoc*, o kartais ir reaktyviu būdu. Kibernetinio saugumo veiklos prioritetų nustatymas negali būti tiesiogiai pagrįstas organizacijos rizikos tikslais, grėsmės aplinka ar verslo / misijos reikalavimais.	Organizaciniu lygmeniu apie kibernetinio saugumo riziką suvokiama ribotai. Organizacija kibernetinio saugumo rizikos valdymą įgyvendina nereguliariai, kiekvienu konkrečiu atveju dėl įvairios patirties ar informacijos, gautos iš išorės šaltinių.	Organizacija nesuvokia savo vaidmens didesnėje ekosistemoje nei jos priklausomybių, nei priklausomų asmenų atžvilgiu. Organizacija nebendradarbiauja ir negauna informacijos (pvz., grėsmių žvalgybos, geriausios praktikos, technologijų) iš kitų subjektų
2 pakopa: **informuotas apie riziką**		
Rizikos valdymo praktikas patvirtina vadovybė, tačiau ji negali būti nustatyta kaip visos organizacijos politika. Kibernetinio saugumo veiklos prioritetus ir apsaugos poreikius tiesiogiai lemia organizacijos rizikos tikslai, grėsmės aplinka arba verslo/misijos reikalavimai.	Organizacijos lygmeniu suvokiama kibernetinio saugumo rizika, tačiau nėra sukurtas visos organizacijos požiūris į kibernetinio saugumo rizikos valdymą.	Organizacija žino apie kibernetinės tiekimo grandinės rizikas, susijusias su jos teikiamais ir naudojamais produktais ir paslaugomis, tačiau nesiima veiksmų nuosekliai ar formaliai dėl tos rizikos.
3 pakopa: **pasikartojantis**		
Organizacijos rizikos valdymo praktika yra oficialiai patvirtinta ir išreiškiama kaip politika. Organizacijos kibernetinio saugumo praktika yra reguliariai atnaujinama, atsižvelgiant į rizikos valdymo procesų taikymą, atsižvelgiant į verslo / misijos reikalavimų pokyčius ir besikeičiančią grėsmę ir technologijų aplinką.	Kibernetinio saugumo rizikai valdyti taikomas visos organizacijos metodas. Į riziką orientuota politika, procesai ir procedūros yra apibrėžiamos, įgyvendinamos, kaip numatyta, ir peržiūrimos. Siekiant veiksmingai reaguoti į rizikos pokyčius, taikomi nuoseklūs metodai. Vyresnieji vadovai užtikrina, kad būtų atsižvelgta į kibernetinį saugumą visose organizacijos veiklos srityse.	Organizacija supranta savo vaidmenį, priklausomybes ir priklausomus asmenis didesnėje ekosistemoje ir gali padėti bendruomenei geriau suprasti riziką. Ji reguliariai bendradarbiauja su kitais subjektais ir iš jų gauna informaciją, kuri papildo viduje sugeneruotą informaciją, ir dalijasi informacija su kitais subjektais
4 pakopa: **prisitaikantis**		
Organizacija pritaiko savo kibernetinio saugumo praktiką, remdamasi ankstesne ir dabartine kibernetinio saugumo veikla, įskaitant išmoktas pamokas ir prognozuojamus rodiklius. Vykdydama nuolatinio tobulinimo procesą, įtraukdama pažangias kibernetinio saugumo technologijas ir praktiką, organizacija aktyviai prisitaiko prie kintančios grėsmės ir technologijų aplinkos ir laiku bei veiksmingai reaguoja į besikeičiančias sudėtingas grėsmes.	Kibernetinio saugumo rizikai valdyti taikomas visos organizacijos metodas, pagal kurį naudojama rizika pagrįsta politika, procesai ir procedūros galimiems kibernetinio saugumo įvykiams spręsti. Ryšys tarp kibernetinio saugumo rizikos ir organizacijos tikslų yra aiškiai suprantamas ir į jį atsižvelgiama priimant sprendimus.	Organizacija supranta savo vaidmenį, priklausomybes ir priklausomus asmenis didesnėje ekosistemoje ir prisideda prie platesnio bendruomenės rizikos supratimo. Ji gauna, generuoja ir peržiūri prioritetinę informaciją, kuri padeda nuolat analizuoti riziką, kai vystosi grėsmė ir technologijos.

9 Paveikslas. NIST pakopų apibrėžimai. Šaltinis: NIST (2018)

- **Valdymo Profilis** reiškia rezultatus, pagrįstus verslo poreikiais, kuriuos organizacija pasirinko iš pagrindų kategorijų ir subkategorijų. Profilis gali būti apibūdinamas kaip standartų, gairių ir praktikos suderinimas su pagrindų pagrindu konkrečiame įgyvendinimo scenarijuje. Profiliai gali būti naudojami siekiant nustatyti galimybes pagerinti kibernetinio saugumo laikyseną, lyginant „dabartinį“ profilį (būseną „toks, koks yra“) su „tiksliniu“ profiliu (būsena „būti“). Siekdama sukurti profilį, organizacija gali peržiūrėti visas kategorijas ir subkategorijas ir, remdamasi verslo/misijos veiksniais ir rizikos vertinimu, nustatyti, kurios yra svarbiausios; ji gali pridėti kategorijas ir subkategorijas, jei reikia, kad būtų pašalinta organizacijos rizika. Dabartinis profilis gali būti naudojamas siekiant padėti nustatyti prioritetus ir įvertinti pažangą siekiant tikslinio profilio, kartu atsižvelgiant į kitus verslo poreikius, įskaitant ekonomiškumą ir naujoves. Profiliai gali būti naudojami atliekant savęs vertinimą ir bendraujant organizacijos viduje arba tarp organizacijų.

Taigi branduoliai pateikia kibernetinio saugumo veiklos rinkinį, norimus rezultatus ir taikomas nuorodas, kurios yra bendros ypatingos svarbos infrastruktūros sektoriuose. Įgyvendinimo pakopos pateikia kontekstą, kaip organizacija vertina kibernetinio saugumo riziką ir taikomus procesus šiai rizikai valdyti. Profiliai atspindi rezultatus, pagrįstus verslo poreikiais, kuriuos organizacija pasirinko iš pagrindinių Modelio branduolio kategorijų ir subkategorijų. 10 Paveikslas iliustruoja kaip modelio komponentai veikia tarpusavyje:



10 Paveikslas. NIST modelio komponentai. Šaltinis: Stallings W. (2019).

Taigi NIST modelis veikia kaip instrukcija organizacijoms, pagal kurią įsidiegiant ir laikantis, jos bus saugios ir patikimos. Identifikuotos ir įvertintos informacijos saugumo rizikos, sukurtos ir įgyvendintos saugumo politikos, įdiegtos saugumo priemonės bei reguliariai tikrinami ir atnaujinami saugumo procesai padeda organizacijoms tapti brandžiomis kibernetinio saugumo prasme.

Pagrindiniai vertinimo kriterijai

NIST (2018) pateikia išsamias gaires pagal NIST branduolio funkciją, kategoriją, subkategoriją ir konkrečias nuorodas į kitus standartus, kurie padeda įgyvendinti konkretų punktą ir yra pasirinkti kaip pagrindiniai NIST modelio vertinimo kriterijai (6 Lentelė). Šiame darbe tikslingai paliktos nuorodos tik į ISO/IEC 27001:2013 standartą.

Funkcija	Kategorija	Subkategorija	Nuoroda į ISO/IEC 27001:2013
NUSTATYTI	**Turto valdymas (ID.AM):** duomenys, personalas, įrenginiai, sistemos ir įrenginiai, leidžiantys organizacijai pasiekti verslo tikslus, yra identifikuojami ir valdomi atsižvelgiant į jų santykinę svarbą organizacijos tikslams ir organizacijos rizikos strategijai.	ID.AM-1: Organizacijos fiziniai įrenginiai ir sistemos inventorizuojami	A.8.1.1, A.8.1.2
		ID.AM-2: Organizacijos programinės įrangos platformos ir programos yra inventorizuojamos	A.8.1.1, A.8.1.2, A.12.5.1
		ID.AM-3: Organizacinė komunikacija ir duomenų srautai yra sužymėti	A.13.2.1, A.13.2.2
		ID.AM-4: Išorinės informacinės sistemos yra kataloguojamos	A.11.2.6
		ID.AM-5: ištekliai (pvz., techninė įranga, įrenginiai, duomenys, laikas, personalas ir programinė įranga) teikiama pirmenybė pagal jų klasifikaciją, kritiškumą ir verslo vertę	A.8.2.1
		ID.AM-6: Nustatyti visos darbo jėgos ir trečiųjų šalių suinteresuotųjų šalių (pvz., tiekėjų, klientų, partnerių) kibernetinio saugumo rolės ir atsakomybės	A.6.1.1
	Verslo aplinka (ID.BE): suprantama organizacijos misija, tikslai, suinteresuotosios šalys ir veikla ir teikiama pirmenybė; ši informacija naudojama informuoti apie kibernetinio saugumo vaidmenis, atsakomybę ir rizikos valdymo sprendimus.	ID.BE-1: nustatomas organizacijos vaidmuo tiekimo grandinėje ir apie jį informuojama	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.BE-2: Organizacijos vieta kritinėje infrastruktūroje ir jos pramonės sektoriuje yra identifikuojama ir apie ją informuojama	Standarto 4.1 punktas
		ID.BE-3: Organizacinės misijos, tikslų ir veiklos prioritetai yra nustatomi ir apie juos informuojama	-
		ID.BE-4: Nustatomos kritinių paslaugų teikimo priklausomybės ir svarbiausios funkcijos	A.11.2.2, A.11.2.3, A.12.1.3
		ID.BE-5: Atsparumo reikalavimai kritinėms paslaugoms teikti yra nustatyti visoms veikimo būsenoms (pvz., per prievartą / užpuolimą, atsigavimo metu, normaliomis operacijomis).	A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	Valdymas (ID.GV): politika, procedūros ir procesai, skirti valdyti ir stebėti organizacijos reguliavimo, teisinius, rizikos, aplinkos ir veiklos reikalavimus, yra suprantami ir informuoja kibernetinio saugumo rizikos valdymą.	ID.GV-1: Sukurta organizacijos kibernetinio saugumo politika ir apie ją informuojama	A.5.1.1
		ID.GV-2: Kibernetinio saugumo rolės ir atsakomybės yra suderintos su vidaus kitomis pozicijomis ir išorės partneriais	A.6.1.1, A.7.2.1, A.15.1.1
		ID.GV-3: Su kibernetiniu saugumu susiję teisiniai ir reguliavimo reikalavimai, įskaitant privatumo ir pilietinių laisvių įsipareigojimus, suprantami ir tvarkomi	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
		ID.GV-4: Valdymo ir rizikos valdymo procesai sprendžia kibernetinio saugumo riziką	Standarto 6 punktas
	Rizikos įvertinimas (ID.RA): organizacija supranta kibernetinio saugumo riziką organizacijos operacijoms (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtui ir asmenims.	ID.RA-1: Turto pažeidžiamumas identifikuojamas ir dokumentuojamas	A.12.6.1, A.18.2.3
		ID.RA-2: Kibernetinių grėsmių žvalgyba gaunama iš dalijimosi informacija forumų ir šaltinių	A.6.1.4
		ID.RA-3: Vidinės ir išorinės grėsmės yra nustatomos ir dokumentuojamos	Standarto 6.1.2 punktas
		ID.RA-4: Nustatyti galimi verslo poveikiai ir tikimybės	A.16.1.6, Standarto 6.1.2 punktas
		ID.RA-5: grėsmės, pažeidžiamumas, tikimybė ir poveikis naudojami rizikai nustatyti	A.12.6.1
		ID.RA-6: Rizikos atsakai nustatomi ir pateikiami pagal prioritetus	Standarto 6.1.3 punktas
	Rizikos valdymo strategija (ID.RM): nustatomi organizacijos prioritetai, suvaržymai, rizikos tolerancijos ir prielaidos, kurios naudojamos operacinės rizikos sprendimams paremti.	ID.RM-1: rizikos valdymo procesus nustato, valdo ir jiems pritaria organizacijos suinteresuotosios šalys	Standarto 6.1.3, 8.3, 9.3 punktai
		ID.RM-2: Organizacinės rizikos tolerancija yra nustatyta ir aiškiai išreikšta	Standarto 6.1.3, 8.3 punktai
		ID.RM-3: Organizacijos rizikos tolerancijos nustatymas priklauso nuo jos vaidmens ypatingos svarbos infrastruktūros ir sektoriaus rizikos analizėje	Standarto 6.1.3, 8.3 punktai
	Tiekimo grandinės rizikos valdymas (ID.SC): Organizacijos prioritetai, apribojimai, rizikos tolerancijos ir prielaidos yra nustatomos ir naudojamos rizikos sprendimams, susijusiems su tiekimo grandinės rizikos valdymu, paremti. Organizacija sukūrė ir įdiegė procesus tiekimo grandinės rizikai nustatyti, įvertinti ir valdyti.	ID.SC-1: Kibernetinės tiekimo grandinės rizikos valdymo procesus nustato, nustato, vertina, valdo ir sutinka organizacijos suinteresuotosios šalys	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.SC-2: Informacinių sistemų, komponentų ir paslaugų tiekėjai ir trečiųjų šalių partneriai identifikuojami, nustatomi prioritetai ir vertinami naudojant kibernetinės tiekimo grandinės rizikos vertinimo procesą.	A.15.2.1, A.15.2.2
		ID.SC-3: Sutartys su tiekėjais ir trečiųjų šalių partneriais naudojamos įgyvendinant atitinkamas priemones, skirtas organizacijos kibernetinio saugumo programos ir kibernetinės tiekimo grandinės rizikos valdymo plano tikslams pasiekti.	A.15.1.1, A.15.1.2, A.15.1.3
		ID.SC-4: Tiekėjai ir trečiųjų šalių partneriai yra reguliariai vertinami naudojant auditą, bandymų rezultatus ar kitas vertinimo formas, siekiant patvirtinti, kad jie vykdo savo sutartinius įsipareigojimus.	A.15.2.1, A.15.2.2
		ID.SC-5: atsako ir atkūrimo planavimas bei bandymai atliekami kartu su tiekėjais ir trečiųjų šalių teikėjais	A.17.1.3

6 lentelė. NIST modelio pagrindiniai vertinimo kriterijai. Šaltinis: NIST (2018).

Funkcija	Kategorija	Subkategorija	Nuoroda į ISO/IEC 27001:2013
APSAUGOTI	**Tapatybės valdymas, autentifikavimas ir prieigos kontrolė (PR.AC)**: prieiga prie fizinio ir loginio turto ir susijusių įrenginių yra ribojama įgaliotiems vartotojams, procesams ir įrenginiams ir yra valdoma atsižvelgiant į įvertintą neteisėtos prieigos prie įgaliotos veiklos ir operacijų riziką.	PR.AC-1: Išduodamos, tvarkomos, tikrinamos, atšaukiamos ir tikrinamos įgaliotų įrenginių, vartotojų ir procesų tapatybės ir kredencialai.	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-2: fizinė prieiga prie turto yra valdoma ir apsaugota	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
		PR.AC-3: Valdoma nuotolinė prieiga	A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
		PR.AC-4: Prieigos leidimai ir įgaliojimai tvarkomi, atsižvelgiant į mažiausiųjų privilegijų ir pareigų atskyrimo principus	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
		PR.AC-5: apsaugotas tinklo vientisumas (pvz., tinklo atskyrimas, tinklo segmentavimas)	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
		PR.AC-6: tapatybės tikrinamos ir susietos su kredencialais bei tvirtinamos sąveikaujant	A.7.1.1, A.9.2.1
		PR.AC-7: naudotojų, įrenginių ir kitų išteklių autentiškumas patvirtinamas (pvz., vieno veiksnio, kelių veiksnių) proporcingai operacijos rizikai (pvz., asmenų saugumo ir privatumo rizikai ir kitai organizacinei rizikai).	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
	Informuotumas ir mokymas (PR.AT): organizacijos personalas ir partneriai yra mokomi informuotumo apie kibernetinį saugumą ir yra apmokyti atlikti su kibernetiniu saugumu susijusias pareigas ir įsipareigojimus, atitinkančius susijusią politiką, procedūras ir susitarimus.	PR.AT-1: Visi vartotojai yra informuoti ir apmokyti	A.7.2.2, A.12.2.1
		PR.AT-2: Privilegijuotieji vartotojai supranta savo roles ir atsakomybes	A.6.1.1, A.7.2.2
		PR.AT-3: trečiųjų šalių suinteresuotosios šalys (pvz., tiekėjai, klientai, partneriai) supranta savo roles ir atsakomybes	A.6.1.1, A.7.2.1, A.7.2.2
		PR.AT-4: Vyresnieji vadovai supranta savo roles ir atsakomybes	A.6.1.1, A.7.2.2
		PR.AT-5: fizinio ir kibernetinio saugumo darbuotojai supranta savo roles ir atsakomybes	A.6.1.1, A.7.2.2
	Duomenų saugumas (PR.DS): informacija ir įrašai (duomenys) tvarkomi laikantis organizacijos rizikos strategijos, siekiant apsaugoti informacijos konfidencialumą, vientisumą ir prieinamumą.	PR.DS-1: Duomenys ramybės būsenoje yra apsaugoti	A.8.2.3
		PR.DS-2: perduodami duomenys yra apsaugoti	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		PR.DS-3: Turtas oficialiai tvarkomas pašalinimo, perkėlimo ir disponavimo metu	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
		PR.DS-4: Pakankami pajėgumai, užtikrinantys prieinamumą	A.12.1.3, A.17.2.1
		PR.DS-5: Įdiegta apsauga nuo duomenų nutekėjimo	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		PR.DS-6: vientisumo tikrinimo mechanizmai naudojami programinės įrangos, programinės įrangos ir informacijos vientisumui patikrinti	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
		PR.DS-7: Kūrimo ir testavimo aplinka (-os) yra atskirtos nuo gamybos aplinkos	A.12.1.4
		PR.DS-8: vientisumo tikrinimo mechanizmai naudojami aparatinės įrangos vientisumui patikrinti	A.11.2.4
	Informacijos apsaugos procesai ir procedūros (PR.IP): saugos politika (kuri apima tikslą, apimtį, vaidmenis, atsakomybę, valdymo įsipareigojimus ir organizacijos subjektų koordinavimą), procesai ir procedūros yra palaikomos ir naudojamos informacinių sistemų ir turto apsaugai valdyti.	PR.IP-1: sukuriama ir prižiūrima informacinių technologijų/pramoninio valdymo sistemų bazinė konfigūracija, apimanti saugumo principus (pvz., mažiausio funkcionalumo koncepciją).	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		PR.IP-2: įdiegtas sistemos kūrimo gyvavimo ciklas sistemoms valdyti	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
		PR.IP-3: Įdiegti konfigūracijos keitimo valdymo procesai	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		PR.IP-4: Kuriamos, prižiūrimos ir tikrinamos informacijos atsarginės kopijos	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
		PR.IP-5: laikomasi politikos ir taisyklių, susijusių su organizacijos turto fizine veiklos aplinka	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
		PR.IP-6: Duomenys naikinami pagal politiką	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		PR.IP-7: patobulinti apsaugos procesai	A.16.1.6, Standarto 9 ir 10 punktai
		PR.IP-8: Apsaugos technologijų efektyvumas yra bendras	A.16.1.6
		PR.IP-9: Reagavimo į incidentus ir veiklos tęstinumo planai ir atkūrimo planai (atkūrimo iš incidentų ir atkūrimo po nelaimių) yra parengti ir tvarkomi	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
		PR.IP-10: Reagavimo ir atkūrimo planai išbandomi	A.17.1.3
		PR.IP-11: kibernetinis saugumas įtrauktas į žmogiškųjų išteklių praktiką (pvz., atšaukimas, personalo patikra)	A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
		PR.IP-12: Sukuriamas ir įgyvendinamas pažeidžiamumo valdymo planas	A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3
	Techninė priežiūra (PR.MA): Pramonės valdymo ir informacinių sistemų komponentų priežiūra ir remontas atliekami laikantis politikos ir procedūrų.	PR.MA-1: Organizacijos turto priežiūra ir remontas atliekami ir registruojami, patvirtintais ir kontroliuojamais įrankiais	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6
		PR.MA-2: Nuotolinė organizacijos turto priežiūra patvirtinama, registruojama ir atliekama taip, kad būtų išvengta neteisėtos prieigos	A.11.2.4, A.15.1.1, A.15.2.1
	Apsauginė technologija (PR.PT): Techniniai saugos sprendimai valdomi taip, kad būtų užtikrintas sistemų ir turto saugumas ir atsparumas, laikantis susijusių politikos krypčių, procedūrų ir susitarimų.	PR.PT-1: audito / žurnalo įrašai nustatomi, dokumentuojami, įgyvendinami ir peržiūrimi pagal politiką	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
		PR.PT-2: Išimama laikmena yra apsaugota ir jos naudojimas ribojamas pagal politiką	A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
		PR.PT-3: Mažiausio funkcionalumo principas įtrauktas konfigūruojant sistemas, kad būtų teikiamos tik esminės galimybės	A.9.1.2
		PR.PT-4: Ryšių ir valdymo tinklai yra apsaugoti	A.13.1.1, A.13.2.1, A.14.1.3
		PR.PT-5: Įdiegti mechanizmai (pvz., saugus gedimams, apkrovos balansavimas, karštasis apsikeitimas) siekiant užtikrinti atsparumo reikalavimus įprastomis ir nepalankiomis situacijomis	A.17.1.2, A.17.2.1

6 lentelė. NIST modelio pagrindiniai vertinimo kriterijai. Šaltinis: NIST (2018). Tęsinys.

Funkcija	Kategorija	Subkategorija	Nuoroda į ISO/IEC 27001:2013
APTIKTI	**Anomalijos ir įvykiai (DE.AE):** aptinkama anomali veikla ir suprantamas galimas įvykių poveikis.	DE.AE-1: yra nustatytas ir valdomas tinklo operacijų ir numatomų duomenų srautų vartotojams ir sistemoms pagrindas.	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2
		DE.AE-2: aptikti įvykiai analizuojami siekiant suprasti atakos taikinius ir metodus	A.12.4.1, A.16.1.1, A.16.1.4
		DE.AE-3: įvykių duomenys renkami ir koreliuojami iš kelių šaltinių ir jutiklių	A.12.4.1, A.16.1.7
		DE.AE-4: Nustatomas įvykių poveikis	A.16.1.4
		DE.AE-5: yra nustatyti perspėjimo slenksčiai apie incidentus	A.16.1.4
	Saugumo nuolatinis stebėjimas (DE.CM): informacinė sistema ir turtas yra stebimi, siekiant nustatyti kibernetinio saugumo įvykius ir patikrinti apsaugos priemonių efektyvumą.	DE.CM-1: tinklas stebimas siekiant aptikti galimus kibernetinio saugumo įvykius	-
		DE.CM-2: fizinė aplinka stebima siekiant aptikti galimus kibernetinio saugumo įvykius	A.11.1.1, A.11.1.2
		DE.CM-3: personalo veikla stebima, siekiant aptikti galimus kibernetinio saugumo įvykius	A.12.4.1, A.12.4.3
		DE.CM-4: aptiktas kenkėjiškas kodas	A.12.2.1
		DE.CM-5: aptiktas neteisėtas mobiliojo ryšio kodas	A.12.5.1, A.12.6.2
		DE.CM-6: išorinio paslaugų teikėjo veikla stebima siekiant aptikti galimus kibernetinio saugumo įvykius	A.14.2.7, A.15.2.1
		DE.CM-7: Atliekamas neleistino personalo, jungčių, įrenginių ir programinės įrangos stebėjimas	A.12.4.1, A.14.2.7, A.15.2.1
		DE.CM-8: Atliekamas pažeidžiamumo nuskaitymas	A.12.6.1
	Aptikimo procesai (DE.DP): aptikimo procesai ir procedūros yra prižiūrimi ir tikrinami, siekiant užtikrinti informuotumą apie neįprastus įvykius.	DE.DP-1: Rolės ir atsakomybė už aptikimą yra tiksliai apibrėžti, siekiant užtikrinti atskaitomybę	A.6.1.1, A.7.2.2
		DE.DP-2: aptikimo veikla atitinka visus taikomus reikalavimus	A.18.1.4, A.18.2.2, A.18.2.3
		DE.DP-3: Testuojami aptikimo procesai	A.14.2.8
		DE.DP-4: perduodama įvykių aptikimo informacija	A.16.1.2, A.16.1.3
		DE.DP-5: aptikimo procesai nuolat tobulinami	A.16.1.6
REAGUOTI	**Reagavimo planavimas (RS.RP**): Reagavimo procesai ir procedūros yra vykdomi ir prižiūrimi, kad būtų užtikrintas atsakas į aptiktus kibernetinio saugumo incidentus.	RS.RP-1: Reagavimo planas vykdomas incidento metu arba po jo	A.16.1.5
	Ryšiai (RS.CO): reagavimo veikla koordinuojama su vidaus ir išorės suinteresuotosiomis šalimis (pvz., išorės parama iš teisėsaugos institucijų).	RS.CO-1: darbuotojai žino savo roles ir operacijų tvarką, kai reikia reaguoti	A.6.1.1, A.7.2.2, A.16.1.1
		RS.CO-2: apie incidentus pranešama laikantis nustatytų kriterijų	A.6.1.3, A.16.1.2
		RS.CO-3: Informacija dalijamasi pagal reagavimo planus	A.16.1.2, Standarto 7.4 punktas
		RS.CO-4: Koordinavimas su suinteresuotosiomis šalimis vyksta pagal reagavimo planus	Standarto 7.4 punktas
		RS.CO-5: Savanoriškas dalijimasis informacija vyksta su išorės suinteresuotosiomis šalimis, siekiant platesnio kibernetinio saugumo situacijos suvokimo	A.6.1.4
	Analizė (RS.AN): Analizė atliekama siekiant užtikrinti veiksmingą atsaką ir palaikyti atkūrimo veiklą.	RS.AN-1: tiriami aptikimo sistemų pranešimai	A.12.4.1, A.12.4.3, A.16.1.5
		RS.AN-2: Incidento poveikis suprantamas	A.16.1.4, A.16.1.6
		RS.AN-3: atliekama ekspertizė	A.16.1.7
		RS.AN-4: incidentai skirstomi į kategorijas pagal reagavimo planus	A.16.1.4
		RS.AN-5: sukurti procesai, skirti gauti, analizuoti ir reaguoti į pažeidžiamumą, atskleistą organizacijai iš vidinių ir išorinių šaltinių (pvz., vidinio testavimo, saugos biuletenių ar saugumo tyrinėtojų).	-
	Sušvelninimas (RS.MI): atliekami veiksmai, siekiant užkirsti kelią įvykio išplėtimui, sušvelninti jo padarinius ir išspręsti incidentą.	RS.MI-1: incidentai suvaldomi	A.12.2.1, A.16.1.5
		RS.MI-2: incidentai sušvelninami	A.12.2.1, A.16.1.5
		RS.MI-3: naujai nustatyti pažeidžiamumai sumažinami arba dokumentuojami kaip priimtina rizika	A.12.6.1
	Patobulinimai (RS.IM): Organizacinė reagavimo veikla patobulinta įtraukiant dabartinės ir ankstesnės aptikimo/reagavimo veiklos pamokas.	RS.IM-1: Reagavimo planai apima išmoktas pamokas	A.16.1.6, Standarto 10 punktas
		RS.IM-2: Reagavimo strategijos atnaujintos	A.16.1.6, Standarto 10 punktas
ATKURTI	**Atkūrimo planavimas (RC.RP**): atkūrimo procesai ir procedūros vykdomi ir prižiūrimi siekiant užtikrinti, kad būtų atkurtos sistemos arba turtas, paveiktas kibernetinio saugumo incidentų.	RC.RP-1: atkūrimo planas vykdomas kibernetinio saugumo incidento metu arba po jo	A.16.1.5
	Patobulinimai (RC.IM): atkūrimo planavimas ir procesai patobulinti įtraukiant išmoktas pamokas į būsimą veiklą.	RC.IM-1: į atkūrimo planus įtrauktos išmoktos pamokos	A.16.1.6, Standarto 10 punktas
		RC.IM-2: atnaujintos atkūrimo strategijos	A.16.1.6, Standarto 10 punktas
	Ryšiai (RC.CO): atkūrimo veikla derinama su vidinėmis ir išorinėmis šalimis (pvz., koordinavimo centrais, interneto paslaugų teikėjais, atakuojančių sistemų savininkais, aukomis, kitomis CSIRT grupėmis ir pardavėjais).	RC.CO-1: tvarkomi ryšiai su visuomene	A.6.1.4, Standarto 7.4 punktas
		RC.CO-2: reputacija pataisoma po incidento	Standarto 7.4 punktas
		RC.CO-3: apie atkūrimo veiklą pranešama vidinėms ir išorinėms suinteresuotosioms šalims, taip pat vykdomosioms ir valdymo komandoms	Standarto 7.4 punktas

6 lentelė. NIST modelio pagrindiniai vertinimo kriterijai. Šaltinis: NIST (2018). Tęsinys.

Įdiegimas organizacijoje

NIST (2018) nurodo, kad norint valdyti kibernetinio saugumo riziką, būtina aiškiai suprasti organizacijos verslo veiksnius ir saugumo sumetimus, susijusius su technologijų naudojimu. Kadangi kiekvienos organizacijos rizika, prioritetai ir sistemos yra unikalios, priemonės ir metodai, naudojami siekiant aprašytų rezultatų, skirsis. Daugelis organizacijų jau turi procesus, skirtus privatumui ir pilietinėms laisvėms spręsti. Metodika sukurta papildyti tokius procesus ir pateikti gaires, kaip palengvinti privatumo rizikos valdymą, atitinkantį organizacijos požiūrį į kibernetinio saugumo rizikos valdymą. Privatumo ir kibernetinio saugumo integravimas gali būti naudingas organizacijoms, nes padidina klientų pasitikėjimą, įgalina labiau standartizuotą dalijimąsi informacija ir supaprastina operacijas pagal teisinius režimus. Modelis išlieka veiksmingas ir palaiko technines naujoves, nes jis yra neutralus technologijoms.

Moskowitz D., Nichols D.M.(2022) teigia, kas organizacija pradeda kelionę tada, kai pasirenka kurti ir apsaugoti savo vertę įsidiegdama NIST modelį siekiant sumažinti kibernetinio saugumo riziką. Kelionė prasideda, kai aukščiausio lygio vadovybė priima strateginį sprendimą priimti įmonės rizikos valdymo sistemą ir NIST modelį. Autoriai Moskowitz D., Nichols D.M.(2022) siūlo atsakyti į pateiktus klausimus: Kur mes dabar? Kur mes einame? Kodėl mes einame? Kaip elgsimės su neišvengiamais įvykiais, kurių nesitikėjome ir kurių neplanuojame? Kaip žinosime, kad mums pasisekė?

Kelionė prasideda nustatant organizacijos kibernetinio saugumo viziją, nurodant priežastį, kodėl siekiama geresnių kibernetinio saugumo galimybių. Kad ir kaip gerai planuojama, nutinka nenumatytų dalykų. Kad būtų galima reaguoti į nenumatytus dalykus, kibernetinio saugumo pajėgumų tobulinimo kelionė gali paskatinti organizaciją tapti judresnę, nes ji internalizuoja prisitaikymą prie greitai kintančios aplinkos ir nuolat didina gebėjimą kurti, apsaugoti ir teikti skaitmeninio verslo vertę.

NIST (2018) pateikia 7 veiksmus, kaip organizacija gali naudotis NIST modeliu kurdama naują kibernetinio saugumo programą arba patobulindama esamą. Šie veiksmai turėtų būti kartojami, jei reikia, siekiant nuolat gerinti kibernetinį saugumą. 11 Paveikslas iliustruoja šiuos veiksmus.

1 veiksmas: nustatyti prioritetus ir apimtį. Organizacija nustato savo verslo/misijos tikslus ir aukšto lygio organizacijos prioritetus. Turėdama šią informaciją, organizacija priima strateginius sprendimus dėl kibernetinio saugumo diegimo ir nustato sistemų bei turto, palaikančių pasirinktą verslą ar procesą, apimtį. Struktūra gali būti pritaikyta įvairioms organizacijos verslo linijoms ar procesams palaikyti, kurių verslo poreikiai ir susiję rizikos tolerancija gali būti skirtingi. Rizikos tolerancija gali atsispindėti tikslinėje įgyvendinimo pakopoje.

2 žingsnis: orientuotis. Nustačius kibernetinio saugumo programos apimtį verslui arba procesui, organizacija nustato susijusias sistemas ir turtą, reguliavimo reikalavimus ir bendrą rizikos metodą. Tada organizacija konsultuojasi su šaltiniais, kad nustatytų toms sistemoms ir turtui taikomas grėsmes ir pažeidžiamumą.

3 veiksmas: sukurti dabartinį profilį. Organizacija sukuria dabartinį profilį, nurodydama, kurios kategorijos ir subkategorijų rezultatai iš pagrindų sistemos šiuo metu yra pasiekiami. Jei rezultatas pasiekiamas iš dalies, šio fakto pastebėjimas padės palaikyti tolesnius veiksmus, pateikiant pradinę informaciją.

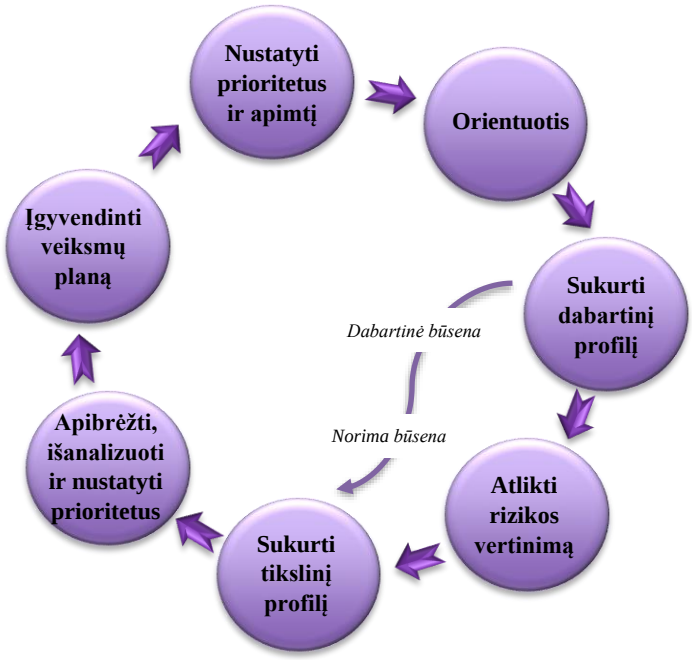
4 veiksmas: atlikti rizikos vertinimą. Šis vertinimas gali būti grindžiamas bendru organizacijos rizikos valdymo procesu arba ankstesne rizikos vertinimo veikla. Organizacija analizuoja veiklos aplinką, kad išsiaiškintų kibernetinio saugumo įvykio tikimybę ir poveikį, kurį įvykis gali turėti organizacijai. Svarbu, kad organizacijos nustatytų kylančias rizikas ir naudotų informaciją apie kibernetines grėsmes iš vidinių ir išorinių šaltinių, kad geriau suprastų kibernetinio saugumo įvykių tikimybę ir poveikį.

5 veiksmas: sukurti tikslinį profilį. Organizacija sukuria tikslinį profilį, kuriame pagrindinis dėmesys skiriamas pagrindų kategorijų ir subkategorijų, apibūdinančių norimus organizacijos kibernetinio saugumo rezultatus, vertinimui. Organizacijos taip pat gali sukurti savo papildomas kategorijas ir subkategorijas, kad atsižvelgtų į unikalią organizacinę riziką. Kurdama tikslinį profilį organizacija taip pat gali atsižvelgti į išorinių suinteresuotųjų šalių, tokių kaip sektoriaus subjektai, klientai ir verslo partneriai, įtaką ir reikalavimus. Tikslinis profilis turėtų tinkamai atspindėti tikslinės įgyvendinimo pakopos kriterijus.

6 veiksmas: apibrėžti, išanalizuoti ir nustatyti prioritetus. Organizacija lygina dabartinį profilį ir tikslinį profilį, kad nustatytų spragas. Tada sukuriamas prioritetinis veiksmų planas, skirtas pašalinti spragas, atspindinčias misijos veiksnius, išlaidas ir naudą bei riziką, kad būtų pasiekti tikslinio profilio rezultatai. Tada organizacija nustato išteklius, įskaitant finansavimą ir darbo jėgą, reikalingus spragoms pašalinti. Profilių naudojimas tokiu būdu skatina organizaciją priimti pagrįstus sprendimus dėl kibernetinio saugumo veiklos, palaiko rizikos valdymą ir leidžia organizacijai atlikti ekonomiškus, tikslingus patobulinimus.

7 veiksmas: įgyvendinti veiksmų planą. Organizacija nustato, kokių veiksmų imtis, kad pašalintų spragas, jei tokių buvo, nustatytas ankstesniame žingsnyje, ir tada pakoreguoja savo dabartinę kibernetinio saugumo praktiką, kad pasiektų tikslinį profilį. Modelyje pateikiami kategorijų ir subkategorijų informacinių nuorodų pavyzdžiai, tačiau organizacijos turėtų nustatyti, kurie standartai, gairės ir praktika, įskaitant sektoriui būdingus, geriausiai atitinka jų poreikius.

Organizacija kartoja veiksmus, jei reikia, kad nuolat įvertintų ir pagerintų savo kibernetinį saugumą. Pavyzdžiui, organizacijos gali pastebėti, kad dažnesnis orientavimo žingsnio kartojimas pagerina rizikos vertinimo kokybę. Be to, organizacijos gali stebėti pažangą pakartotinai atnaujindamos dabartinį profilį, vėliau lygindamos dabartinį profilį su tiksliniu profiliu. Organizacijos taip pat gali naudoti šį procesą, kad suderintų savo kibernetinio saugumo programas su norima pagrindų diegimo pakopa.



11 Paveikslas. NIST veiksmai kuriant ir tobulinant modelį organizacijoje. Šaltinis: Moskowitz D., Nichols D.M.(2022)

Šie NIST modelio nurodyti veiksmai, siekiant įgyvendinti ir nuolat tobulinti kibernetinio saugumo brandą organizacijoje, pradedant prioritetais ir apimtimi, baigiant jų įgyvendinimu, padeda nuosekliai įgyvendinti organizacijų kibernetinio saugumo strategijas bei pasiekti išsikeltus tikslus. Nuolatinis ciklas padeda organizacijos prisitaikyti prie besikeičiančių technologijų ir atakų pobūdžio bei kritiškai vertinti savo kibernetinio saugumo būklę.

NIST (2018) Kibernetinio saugumo sistema sukurta siekiant sumažinti riziką gerinant kibernetinio saugumo rizikos valdymą siekiant organizacijos tikslų. Idealiu atveju organizacijos, naudojančios sistemą, gali išmatuoti ir priskirti savo rizikos vertes kartu su veiksmų, kurių imtasi siekiant sumažinti riziką iki priimtino lygio, sąnaudas ir naudą. Kuo geriau organizacija galės įvertinti savo kibernetinio saugumo strategijų ir žingsnių riziką, išlaidas ir naudą, tuo racionalesnis, efektyvesnis ir vertingesnis bus jos požiūris į kibernetinį saugumą ir investicijas. Organizacijos ir toliau turės unikalias rizikas – skirtingas grėsmes, skirtingus pažeidžiamumus, skirtingą rizikos toleranciją. Jos taip pat skirsis dėl to, kaip jos pritaiko modelyje aprašytą praktiką. Galiausiai modelis yra skirtas sumažinti ir geriau valdyti kibernetinio saugumo

riziką. Autoriai Mahn A., Marron J., Quinn S., Topper D. (2021) teigia, kad NIST modelis gali padėti organizacijai pradėti arba tobulinti savo kibernetinio saugumo programą. Sukurta naudojant praktiką, kuri, kaip žinoma, yra veiksminga, gali padėti organizacijoms pagerinti kibernetinio saugumo poziciją. Tai skatina vidinių ir išorinių suinteresuotųjų šalių bendravimą apie kibernetinį saugumą ir padeda geriau integruoti, ir suderinti kibernetinio saugumo rizikos valdymą su platesnio masto įmonės rizikos valdymo procesais. NIST modelis ne tik kad parašytas bendra ir prieinama kalba, tačiau iš funkcijų, kategorijų ir subkategorijų matyti, kad jis pritaikomas daugeliui technologijų ir sektorių, o pats įgyvendinimo ir nuolatinio tobulinimo ciklas leidžia teigti, kad NIST modelis padeda organizacijoms tapti atsparesnėms ir brandesnėms kibernetinio saugumo prasme.

1.5. ISO 27001 IR NIST MODELIŲ PALYGINIMAS

Tiek ISO 27001, tiek NIST modeliais organizacijose yra pasiekiamas aukštas kibernetinio saugumo lygis bei užtikrinama organizacijos kibernetinio saugumo branda. Abu kibernetinio saugumo modeliai turi savo išskirtinumus, panašumus, privalumus ir trūkumus. Porch, A. M. (2020) teigia, kad NIST reklamuoja „kibernetinio saugumo sistemą“, pagrįstą penkiomis pagrindinėmis funkcijomis: identifikuoti, apsaugoti, aptikti, reaguoti ir atkurti. Šios funkcijos veikia kartu, kad sukurtų „sėkmingą ir visapusišką kibernetinio saugumo programą“. ISO sukūrė ISO 27001, kuriame pateikiami išsamūs informacijos saugos standartai, kurie tarptautiniu mastu pripažįstami kaip „*de facto*“ kibernetinio saugumo sistema. ISO standartas organizacijoms pateikia rekomendacijas, kaip peržiūrėti, matuoti ir tikrinti savo kibernetinio saugumo programas, kad galėtų imtis taisomųjų veiksmų ir tobulinti. Koza, E. (2022) teigia, kad esminis skirtumas tarp šių dviejų modelių slypi pagrindinėje jų metodikoje, skirtoje holistiniam požiūriui įgyvendinti. ISO/IEC 27001 taiko į procesą orientuotą metodą, naudojant informacijos saugumo aspektus kaip vidinių procesų įgyvendinimo kontrolės priemones. Kitaip tariant: ISO/IEC 27001 apibrėžia reikalavimus informacijos saugumo valdymo sistemai, kurios tikslas yra diegti, prižiūrėti ir nuolat tobulinti prevencines, reaktyviąsias ir detektyvines priemones. Kita vertus, NIST yra į riziką orientuotas metodas, padedantis nustatyti saugumo spragas ir nustatyti jų prioritetus, ir turi būti laikomas neatsiejama priemone arba naudinga priemone. Šių kibernetinio saugumo brandos modelių privalumai, trūkumai, panašumai ir skirtumai pateikti 7 Lentelėje:

PRIVALUMAI

ISO 27001	NIST
Plačiai vertinama ir naudojama kaip numatytoji kibernetinio saugumo ar rizikos valdymo sistema daugumoje organizacijų beveik visose pasaulio šalyse. Jame aprašoma informacijos saugumo valdymo sistema ir saugumas įtraukiamas į bendrą įmonės valdymo ir procesų kontekstą. Teikia didžiausią investicijų grąžą tarp įprastų kibernetinio saugumo sistemų ir pateikia metodologiją, kuri gali suteikti organizacijoms didžiausią konkurencinį pranašumą rinkoje dėl mažesnių išlaidų.	Savanoriškas, todėl ja gali tinkamai naudotis bet kuri organizacija Labiau tinka į technologijas orientuotoms įmonėms, nes jame akcentuojamas technologinis valdymas Apima įvairių standartų įstaigų praktiką, kuri pasirodė esanti sėkminga, kai ji buvo įgyvendinta, ir jis taip pat gali suteikti reguliavimo ir teisinių pranašumų. NIST branduolių suskirstymas į kategorijas ir subkategorijas suteikia daugiau lankstumo ir pritaikomumo, sklandžiai užpildo atotrūkį tarp techninių, administracinių ir su politika susijusių kontrolės priemonių, taip pat leidžia labai lengvai susieti įvairius valdiklius pagal skirtingus standartus su NIST modelio kategorijomis.

TRŪKUMAI

ISO 27001	NIST
• Kaina • Sudėtingumas • Reikalauja paskirti atsakingą darbuotoją, kuris valdys ISMS.	Savanoriškas sistemos pobūdis suteikia jai trūkumo, kad ji nepateikia tinkamo rizikos valdymo. Netinka būti diegiamas kaip ilgalaikis informacijos saugumo valdymo sistemų pakaitalas, o labiau gali būti naudojamas kaip gairės diegiant rizikos valdymo sistemas organizacijoms.

PANAŠUMAI

- Abu modeliai skirti su kibernetiniu saugumu susijusios rizikos valdymui.
- Daugelis su sistema susijusių valdiklių, taip pat apibrėžimai ir kodai, naudojami vienoje sistemoje, gali būti naudojami kitoje sistemoje. Tai pasakytina ir apie daugumą valdiklių.
- Abu modeliai naudoja visame pasaulyje žinomą žodyną, todėl įvairiose srityse dirbantiems specialistams lengviau aiškiai ir efektyviai bendrauti apie su kibernetiniu saugumu susijusius iššūkius.
- Abu siekia užtikrinti 3 ramsčius – konfidencialumą, vientisumą ir prieinamumą.
- Ir ISO 27001, ir NIST CSF padeda pateikti gaires, politiką ir procedūras kuriant struktūrizuotą informacijos saugos valdymo sistemą (ISMS), kurią galima papildyti kitomis gairėmis, tokiomis kaip CIS-20, SP 800-53 (saugos kontrolė), SP 800-37. (rizikos valdymo gairės), ISO 27002 (įgyvendinimo kontrolė), 27004 (metrika) ir 27005 (rizikos valdymas).
- Abi sistemos yra gana nepriklausomos nuo technologijų, nes jas galima įdiegti organizacijose, turinčiose skirtingą technologijos laipsnį,

SKIRTUMAI

Kaina: nors NIST ištekliai gali būti bet kuriuo metu pasiekiami nemokamai, ISO ištekliai – ne. Dauguma naujų ir besivystančių organizacijų nori pradėti savo kibernetinio saugumo rizikos valdymo programą su NIST, o augdamos jos norės padidinti investicijas į ISO 20071, kur jos norės valdyti savo kibernetinio saugumo riziką.

Sertifikatas: Yra galimybė gauti trečiosios šalies sertifikatą pagal ISO 20071, kuris bus pripažintas bet kuriame pasaulio regione. Nors tai gali kainuoti daug, yra tikimybė, kad tai gali padėti organizacijai įgyti suinteresuotųjų šalių ir vartotojų pasitikėjimą. Nepaisant to, NIST nesuteikia jokio tipo sertifikavimo.

Rizikos brandumas: organizacijai tik pradedant rengti planą, kaip sumažinti kibernetinės erdvės keliamus pavojus, ir norint įsitikinti, kad bus nepadaryta klaidų, NIST gali būti tinkamas pasirinkimas. Organizacijai, kuri jau yra gerai įsitvirtinusi ir pasirengusi siekti sertifikavimo, ISO 20071 yra tinkamas pasirinkimas.

ISO 27001 ir NIST sudėtingumas. ISO 27001 sudėtingumas priklauso nuo organizacijos dydžio ir tipo. Siekiant išlaikyti tinkamą pažeidžiamumo kontrolę, didesnė įmonė turės atsižvelgti į daugiau atsargumo priemonių, taisyklių ir procesų bei juos įgyvendinti. NIST sukurta sistema yra dar sudėtingesnė nei ISO sukurta sistema. NIST sistemą sunku įdiegti daugelyje įmonių, nes tokioms įmonėms trūksta vidinių NIST žinių, reikalingų tai padaryti.

7 Lentelė. ISO 27001 ir NIST modelių panašumai ir skirtumai. Šaltiniai: Alshar'e, M. (2023), Roy, P.P. (2020).

Roy, P.P. (2020) išskiria NIST pranašumą prieš ISO 27001 ir ISO 27001 pranašumą prieš NIST:

- NIST modelio pranašumas prieš ISO 27001:
    - Pagrindinis NIST kibernetinio saugumo sistemos pranašumas, palyginti su ISO 27001, yra jos struktūrizuotas ir suplanuotas formatas, todėl organizacijoms lengviau ją įgyvendinti įmonės lygiu. Šis struktūrizuotas NIST CSF formatas taip pat gali būti laikomas patogesniu vartotojui ir supaprastintu, ypač aukštesniam valdymui
    - Daugumoje kategorijų ir subkategorijų naudojamos nuorodos į kitas sistemas, tokias kaip ISO 27001, COBIT ir kt., kurios padeda CSF sujungti keletą svarbių įvairių struktūrų savybių.
    - Taip pat geriau tinka įgyvendinti tokiai kontrolės schemai kaip CIS-20 kontrolė, kurioje daug dėmesio skiriama nuodugniam požiūriui į saugumą.
    - Įgyvendina esamų ir tikslinių profilių koncepciją, skirtą įvertinti bendrą organizacijos saugumo padėtį.
- ISO 27001 modelio pranašumas prieš NIST:
    - Bet kuri šį standartą taikanti organizacija gali veiksmingai įtikinti savo klientus, partnerius ir kitas suinteresuotąsias šalis, kad ji gali sukurti saugią ir veiksmingą rizikos valdymo sistemą.
    - Organizacijos gali gauti sertifikatą pagal jį, taip įgydamos konkurentų pranašumą ir klientų pasitikėjimą, kuris gali būti naudojamas kaip didžiulis svertas sudarant verslo sandorius.
    - Itin griežtas ir struktūrizuotas dėmesys dokumentacijai, tiek privalomai, tiek neprivalomai, todėl ji yra labai supaprastinta vadovybei atlikti aukšto lygio analizę
    - Verčia organizacijas aiškiai apibrėžti atsakomybes, kas ir už kurį turtą bei informaciją atsakingas, o tai suteikia organizacijai ir jos informacijos saugumui aiškumo ir struktūros.

Lyginant kibernetinio saugumo brandos organizacijoje vertinimo modelius ISO 27001 ir NIST, išskiriami pagrindiniai modelių vertinimo kriterijai, kurie pateikiami 8 Lentelėje:

PALYGINIMAS	ISO 27001	NIST
Apibūdinimas	Tarptautinis standartas, apibūdinantis geriausią informacijos saugumo valdymo sistemos praktiką	Operacijų ir turto apsaugos saugumo modelis
Tikslinės organizacijos	Gali būti įgyvendinama bet kokios rūšies organizacijoje, pelno ar ne pelno siekiančioje, privačioje ar valstybinėje, mažoje ar didelėje	Pirmiausia buvo sukurtas siekiant padėti JAV ypatingos svarbos infrastruktūros organizacijoms
Struktūra	Standarto 11 punktų (0-4 – neprivalomi, 4-10 privalomi) ir priedas A (14 grupių, 114 kontrolių)	Branduolys suskirstytas į 5 funkcijas, 23 kategorijas ir 108 subkategorijas, įgyvendinimo pakopas bei profilius
Pagrindas	Rizikos valdymas	Rizikos valdymas
Privaloma dokumentacija	ISMS taikymo sritis, Informacijos saugumo politika ir tikslai, Rizikos vertinimo ir rizikos valdymo metodika, Taikomumo pareiškimas, Rizikos valdymo planas, Rizikos vertinimo ataskaita, Saugos vaidmenys ir atsakomybės, Turto aprašas, Prieigos kontrolės politikos dokumentas	Neapibūdinta
Mechanizmas	Nesavanoriškas, išorinis nepriklausomas auditas	Savanoriškas, savęs sertifikavimas
Kibernetinio saugumo brandos lygiai	Nenurodyti. Pasitelkiamos kitos metodikos, dažniausiai ISO 15504 arba Galimybių brandos modelio (*Capability Maturity Model*) lygiai: 0 – neatliekama, 1 – pradinis procesas, 2 – valdomas procesas, 3 – nustatytas procesas, 4 – nuspėjamas procesas, 5 – optimizuotas procesas.	Nenurodyti. Pasitelkiamos kitos metodikos, dažniausiai Galimybių brandos modelio (*Capability Maturity Model*) lygiai: 0 – neatliekama, 1 – pradinis procesas, 2 – valdomas procesas, 3 – nustatytas procesas, 4 – nuspėjamas procesas, 5 – optimizuotas procesas.
Diegimo organizacijoje procesas	Sudėtingas. Reikalingas paskirtas atsakingas asmuo už ISMS organizacijoje įdiegimą ir priežiūrą	Sudėtingas. Reikia papildomų žinių.
Sertifikavimas	Yra	Nėra
Apimtis	Informacijos saugumo standartas, aprašantis, kaip įdiegti ISMS	Neprivalomos kibernetinio saugumo programų įgyvendinimo ir tobulinimo gairės, geriausia praktika ir standartai
Neutralumas technologijoms	TAIP	TAIP
Prieinamumas	Platinama komerciniais pagrindais per oficialią svetainę	Nemokamai parsisiunčiamas iš oficialaus šaltinio
Integravimas su esamais saugumo procesais ir sistemomis	TAIP	TAIP
Darbuotojų įtraukimas	TAIP	TAIP
Nuolatinis tobulinimas	TAIP	TAIP

8 Lentelė. ISO 27001 ir NIST modelių palyginimas. Šaltiniai: Alshar'e, M. (2023), Roy, P.P. (2020), ISO 27001:2013, NIST (2018).

Lyginant bendraisiais kriterijais, ISO 27001 ir NIST modeliai skiriasi tik keletu apsektų: privaloma dokumentacija, sertifikavimas, apimtis, prieinamumas. Pagal šiuos kriterijus modeliai išsiskiria jau ir kitų autorių aptartais skirtumais: kaina ir įgyvendinimo sudėtingumu. Atkreiptinas dėmesys į šio darbo 1.3 ir 1.4 skyrius, kuriuose nagrinėjami ISO 27001 ir NIST modeliai, o būtent į išskirtus kiekvieno modelio pagrindinius vertinimo kriterijus. ISO 27001 išskirti kriterijai standartas ir Priedo A kontrolės (3 Priedas), NIST modelio kriterijai pagal NIST branduolio funkcijas, kategorijas, subkategorijas ir nuorodas. Kadangi NIST standarto nuorodos tikslingai buvo atrinktos tik į ISO 27001 standartą, šiuo apsektu taip pat lyginami ISO 27001 ir NIST kibernetinio saugumo brandos modeliai.

Pagal 6 Lentelę, kurioje apibūdinti NIST modelio pagrindiniai vertinimo kriterijai, galime matyti, kad NIST subkategorijos nepateikia nuorodų į ISO 27001 standartą ties šiais trimis punktais:

1) ID.BE-3: Identifikuoti. Organizacinės misijos, tikslų ir veiklos prioritetai yra nustatomi ir apie juos informuojama
2) DE.CM-1: Aptikti. Tinklas stebimas siekiant aptikti galimus kibernetinio saugumo įvykius.
3) RS.AN-5: Reaguoti. Sukurti procesai, skirti gauti, analizuoti ir reaguoti į pažeidžiamumą, atskleistą organizacijai iš vidinių ir išorinių šaltinių (pvz., vidinio testavimo, saugos biuletenių ar saugumo tyrinėtojų).

Vadinasi, lyginant ISO 27001 ir NIST kibernetinio saugumo modelius pagal ISO 27001 standartą ir kontroles, ir NIST branduolio subkategorijas, ISO 27001 neaprėpia tik aukščiau išvardintų trijų punktų, į kuriuos nepateikiamos nuorodos į ISO 27001 standartą. Tuo tarp ISO 27001 numato daugiau privalomos dokumentacijos ir reikalavimų, nukreiptų į organizacijos vadovybę. Abu kibernetinio saugumo brandos vertinimo modeliai turi savų aspektų, kurie gali būti įvardijami kaip teigiami ir, aspektų, kurie gali būti įvardijami kaip neigiami. Tačiau tai nereiškia, kad kažkuris modelis yra geresnis ar blogesnis – organizacijos, kurios renkasi kurį modelį įsidiegti turi įsivertinti savo finansines galimybes ir tikslus, bei pagal tai rinktis modelį, kuris padės pasiekti nustatytų tikslų.

Roy, P.P. (2020) teigia, kad užuot pasirinkus vieną sistemą, geriausia būtų derinti abiejų gerąją patirtį ir aspektus. Šiuolaikinis rizikos valdymas yra sudėtinga koncepcija, kai kenkėjiški užpuolikai turi prieigą prie naujausių išteklių ir daugybės atakų vektorių. Rizikos įvertinimas galbūt yra esminis bet kurios organizacijos ir projekto sėkmės komponentas. Riziką galima apibrėžti ne tik kaip nepageidaujamo įvykio tikimybę, bet ir kaip dažnumą, kuriuo jis gali įvykti. Taigi ISO 27001 ir NIST derinimas leidžia organizacijai geriau planuoti netikėtas katastrofas ir įvykius. NIST modelis yra geresnis, kai reikia struktūrizuoti saugumo sritis, kurias reikia įgyvendinti, ir kai reikia tiksliai apibrėžti saugos profilius, kuriuos reikia pasiekti, o ISO

27001 yra geresnis norint nubrėžti griežtai aiškiai apibrėžtą vaizdą, skirtą sukurti sistemą, kurioje saugumas gali būti valdomas ilgą laiką. Koza, E. (2022) antrina, kad abu modeliai turi gerą tarptautinę reputaciją dėl savo patikrinto, empiriškai pagrįsto ir tvirto požiūrio, o dėl modulinės konstrukcijos gali būti naudojami nuosekliai ir lygiagrečiai. Be to, abu metodai gali būti įgyvendinami ir naudojami nepriklausomai nuo sektoriaus. Dėl glaudaus ryšio tarp dviejų procedūrų, taip pat dėl tiesioginių NIST nuorodų į ISO/IEC 27001, abu modeliai gali būti įgyvendinami ir naudojami kartu. Į procesą orientuota ISO/IEC 27001 metodika ir susiję 114 gali būti sklandžiai integruoti į 5 NIST funkcijas. Ši integracija ypač svarbi, kai organizacijos turi tam tikrų išteklių, tiek žmogiškųjų, tiek finansinių, suvaržymų, todėl jos turi teikti pirmenybę savo saugumo procesams. Roy, P.P. (2020) nurodo, kad sujungus abu, būtų veiksmingai užpildyti kiekvieno trūkumai. Taigi, norėdami gauti geriausius įmanomus rezultatus, galime sukurti ir įdiegti ISMS pagal ISO 27001 ir naudoti NIST modelį, kad sudarytume turimas apsaugos priemones, įgyvendinamos pagal 5 funkcijas ir atitinkamas kategorijas bei subkategorijas. Tokiu būdu galima užtikrinti, kad visi aspektai būtų padengti.

Su didėjančiais kibernetinių incidentų skaičiais, kibernetinio saugumo branda organizacijose tampa vis aktualesnė. Organizacijos, priklausomai nuo jų dydžio bando taikyti įvairias kibernetinio saugumo praktikas, rekomendacijas ir kibernetinio saugumo brandos modelius. Organizacijoms siekiant tapti atsparesnėms kibernetiniams incidentams, kibernetinio saugumo brandos modeliai yra pagrindinė priemonė, kuri padeda įsivesti politikas, taisykles, atnaujinti procesus ir procedūras, apmokyti darbuotojus pagal konkrečios organizacijos tikslus ir strategiją. Nagrinėti pasaulyje populiariausi kibernetinio saugumo brandos vertinimo organizacijose modeliai - ISO 27001 ir NIST, kurie turi daug panašumų, tačiau išsiskiria įgyvendinimo sudėtingumu ir kaštais, o norint organizacijoje pasiekti maksimalių rezultatų kibernetinio saugumo srityje rekomenduojama turėti abu šiame darbe išnagrinėtus kibernetinio saugumo brandos modelius.

2. KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIO TYRIMO METODIKA

Siekiant ištirti ISO 27001 ir NIST kibernetinio saugumo brandos modelių efektyvumą UAB „XXX“ pasirinktas ***kokybinis tyrimas***.

Tyrimo geografija: Organizacija UAB „XXX“ - grupės skolų išieškojimo organizacijos, veikiančios 20-yje pasaulio valstybių, netiesioginio aptarnavimo operacijų padalinys. UAB „XXX“ veikia Lietuvoje kaip savarankiškas juridinis vienetas, savo veikloje vadovaujasi Lietuvos Respublikos teisės aktais, savo veiklos nuostatais, vidinėmis taisyklėmis, kurios priimamos organizacijos viduje pagal grupės organizacijos mastu priimtas taisykles, kiek tai neprieštarauja Lietuvos teisės aktams.

Tyrimo tikslas: teorinėje dalyje minėti autoriai Junaid, T. S.(2023), Grimmick, R. (2022), Murphy, G. (2022), Taherdoost H.(2022), Moskowitz D., Nichols D.M.(2022), Mahn A., Marron J., Quinn S., Topper D. (2021), Porch, A. M. (2020), Koza, E. (2022), Roy, P.P. (2020) aptaria nagrinėjamus kibernetinius saugumo brandos modelius ISO 27001ir NIST, juos lygina, aptaria jų privalumus, trūkumus, tačiau nepateikiamas praktinis šių modelių įgyvendinimas organizacijose, bei neaptariamas šių modelių efektyvumas. Taigi šio magistrinio darbo tyrimo tikslas yra - ***įvertinti ISO 27001 ir NIST kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumą analizuojant UAB „XXX” atvejį bei pusiau struktūruoto interviu atsakymus***.

Tyrimo uždaviniai:

1. Kibernetinio saugumo brandos modelių efektyvumo vertinimas UAB „XXX“ pagal ISO 27001 ir NIST kibernetinio saugumo brandos organizacijoje vertinimo modelius;
2. Pateikti pusiau struktūruoto interviu kibernetinio saugumo ekspertams atsakymus apie kibernetinio saugumo brandos modelių efektyvumą.
3. Identifikuoti vertinimo duomenų privalumus ir trūkumus.
4. Pateikti rekomendacijas organizacijoms apie kibernetinio saugumo brandos vertinimo organizacijoje modelius ir jų efektyvų pritaikymą.

Tyrimo metodai:

1. Dokumentų turinio (*Content*) analizė naudojama ES, nacionalinių ir kitų teisės aktų bei dokumentų esminių nuostatų reglamentuojančių kibernetinį saugumą, taip pat mokslinės literatūros turinio (*Content*) analizė padėjo susisteminti mokslinėje literatūroje pateiktas kibernetinio saugumo brandos vertinimo modelių ISO 27001 ir NIST koncepcijas.
2. Aprašomoji atvejo analizė (*Descriptive case study analysis*[47]) Valackienė, A. (2016) nurodo, kad aprašomasis atvejo tyrimo (*descriptive case study*) tipas naudojamas intervencijai ar reiškiniui ir realaus gyvenimo kontekstui, kuriame jis įvyko, apibūdinti. Šio tipo atvejo analizė gali būti naudojama tyrime, kuriuo siekiama ištirti mokslinę problemą; reikia apibrėžti pokyčius vienos organizacijos srityje, nustatyti ir patikrinti empirines dimensijas, kurios atspindi organizacijos pokyčius ir elementus. Aprašomasis atvejo tyrimas padeda nustatyti organizacijos silpnąsias vietas, turinčias reikšmės pokyčių rezultatams, ir padeda parengti atsargumo klausimus, pasikeitus pokyčių valdymo procese organizacijoje. Taigi aprašomoji atvejo analizė padėjo atskleisti praktinius ISO 27001 ir NIST modelių įgyvendinimo ir priežiūros aspektus bei siekti šio magistrinio darbo tikslo. Siekiant įvertinti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumą organizacijoje naudojant atvejo analizės tipą buvo nusistatyti kriterijai, kurie pateikti 3.1 šio darbo skyriuje 11 lentelėje, Atvejo analizės UAB „XXX“ vertinimo kriterijai ir vertinimas. Atvejo analizės metu buvo išanalizuota UAB „XXX“ dokumentacija, procesai, procedūros, kuriais remiantis pateikiamos argumentuotos išvados apie kriterijų (ne)efektyvumą.
3. Pusiau struktūruotas interviu. Mokslininkai ištyrė, kad nuo šešių iki dvylikos interviu visada pakaks norimam tyrimo tikslui pasiekti, o būtent - duomenų prisotinimą – tašką, kai iš duomenų nebeatsiranda naujos informacijos ar temų – nepaisant griežtų gairių nebuvimo. Kokybiniame tyrime kritinis veiksnys yra duomenų prisotinimas, o tai rodo, kad buvo pakankamai dalyvių, kad būtų galima visiškai suprasti dalyką.[48] Šiam tyrimui buvo siekiama gauti informaciją iš 8 kibernetinio saugumo ekspertų, ne mažiau nei 3 metus dirbančių kibernetinio saugumo srityje. Kokybiniam tyrimui ekspertai buvo ieškomi Linked IN socialiniame tinkle paieškos laukelyje įvedant „*informacijos saugumo pareigūnas*“ (ang. *information security officer),* gautuose rezultatuose nagrinėjant specialistų nurodytą patirtį kibernetinio saugumo srityje. Šis metodas pasirinktas tikslingai, siekiant sužinoti įvairių organizacijų kibernetinio saugumo

[47] Valackienė, A. (2016). Towards a framework for case study research: methodology and practical implementation. In D. Žostautienė, D. Susnienė, L. Leišytė (Eds.). CISABE'2016 : 6th international conference on Changes in social and business environment, April 28-29, 2016, Panevėžys, Lithuania (pp. 65-70). MEDIMOND, p. 4.

[48] Guest, G. & Bunce, A. & Johnson, L. (2006). How Many Interviews Are Enough?. Field Methods - FIELD METHOD. 18. 59-82. 10.1177/1525822X05279903

specialistų patirtį ir nuomonę apie kibernetinio saugumo modelius ir jų efektyvumą. Deja, kai kuriuos respondentus saistė itin griežti konfidencialumo įsipareigojimai. Paieškos kriterijus atitikusiems asmenims buvo siunčiamas prašymas užpildyti klausimyną (žr. 2 Priedą). Gauti respondentų atsakymai buvo perkelti ir analizuoti naudojant Microsoft Excel programą.

4. Lyginamoji gautų duomenų analizė. Mokslinės literatūros, dokumentų turinio, aprašomojo atvejo analizės ir pusiau struktūruoto interviu gautų duomenų analizei atlikti, o pasitelkus analizės išvadas pateikti pasiūlymus ir rekomendacijas organizacijoms apie kibernetinio saugumo brandos vertinimo organizacijoje modelius ir jų efektyvų pritaikymą.

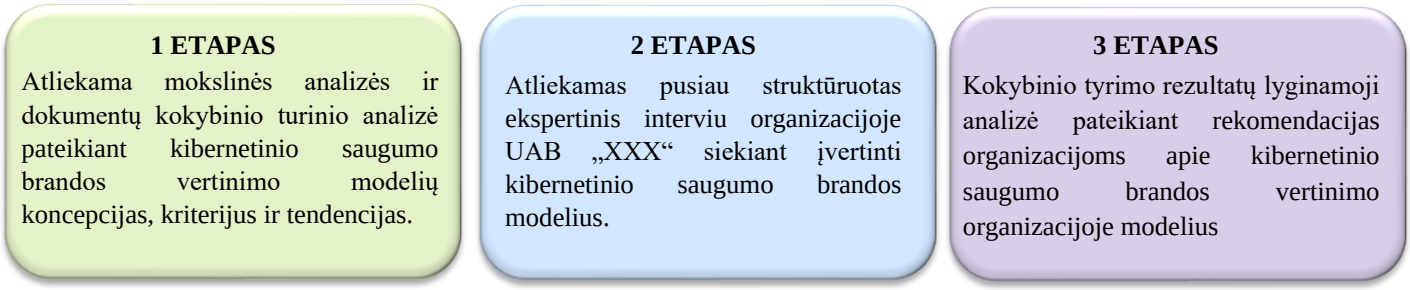
Tyrimo reprezentatyvumas:

Tyrimo imties sudarymui pasirinkta netikimybinė tikslinė atranka. Kibernetinio saugumo brandos organizacijose vertinimo modeliai atrinkti pagal populiarumą ir jų išskyrimą analizuojant mokslinius straipsnius.

Atvejo analizei organizacija UAB „XXX“ atrinkta pagal tris kriterijus: dydį, tipą, veikloje taikomus kibernetinio saugumo brandos vertinimo modelius. UAB „XXX“ tyrimo metu dirbo ~400 darbuotojų (didelė organizacija), tipas - netiesioginio aptarnavimo operacijų padalinys, kur operuojama didelio masto duomenų kiekiais, savo veikloje taikanti ISO 27001 ir NIST kibernetinio saugumo brandos modelius

Pusiau struktūruoto ekspertinio interviu respondentai atrinkti pagal atliekamas pareigas (kibernetinio saugumo specialistai ar jiems prilyginti asmenys), darbo stažą kibernetinio saugumo srityje – ne mažiau 3 metai.

Tyrimo loginis planas pateiktas 12 paveiksle:



12 Paveikslas. Tyrimo loginis planas. Šaltinis: autorius.

Tyrimo instrumentarijus pateiktas 9 lentelėje:

Tyrimo kriterijai	Tyrimo indikatoriai	Tyrimo metodai
Kibernetinio saugumo brandos vertinimo modelių kriterijai	1. Kibernetinio saugumo brandos vertinimo modelių koncepcijos mokslinėje literatūroje.	Mokslinės literatūros sisteminimas ir analizė.
	2. Kibernetinio saugumo brandos vertinimo modeliai dokumentuose	Dokumentų analizė.
Kibernetinio saugumo brandos organizacijoje tyrimas	1. Kibernetinio saugumo brandos organizacijoje vertinimas pagal ISO 27001 modelį	Atvejo analizė, Ekspertinis pusiau struktūruotas interviu
	2.Kibernetinio saugumo brandos organizacijoje vertinimas pagal NIST modelį	Atvejo analizė
Kibernetinio saugumo brandos organizacijoje analizė	1. Kibernetinio saugumo brandos vertinimo organizacijoje modeliai teorijoje.	Mokslinės literatūros analizė, dokumentų analizė, lyginamoji duomenų analizė
	2. Kibernetinio saugumo brandos vertinimo modeliai atlikus vertinimą organizacijoje	Atvejo studijos rezultatų analizė
	3. Kibernetinio saugumo brandos vertinimo modelių interviu	Ekspertinis pusiau struktūruotas interviu
Rekomendacijos organizacijoms apie kibernetinio saugumo brandos vertinimo organizacijoje modelius ir jų efektyvų pritaikymą.	1. Empirinio tyrimo duomenų analitinis ir kritinis vertinimas.	Mokslinės literatūros analizė, Atvejo studijos rezultatų analizė, Ekspertinio pusiau struktūruoto interviu analizė Lyginamoji gautų duomenų analizė.

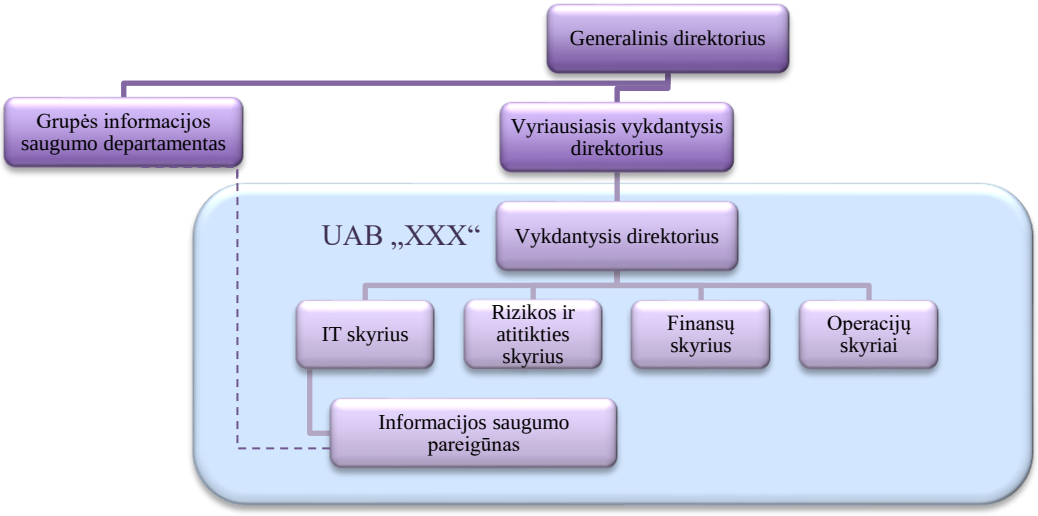
9 Lentelė. Tyrimo instrumentarijus. Šaltinis: autorius.

3. KIBERNETINIO SAUGUMO BRANDOS ORGANIZACIJOJE VERTINIMO MODELIO TYIMO ANALIZĖ

3.1. ATVEJO ANALIZĖ UAB „XXX“

Tyrimas atliktas dešimtus metus savo veiklą Lietuvoje vykdančioje tarptautinės skolų išieškojimo įmonės netiesioginio aptarnavimo padalinyje UAB „XXX“, kuriame tyrimo metu dirbo apie 400 darbuotojų. Siekiant pateikti kibernetinio saugumo brandos vertinimo modelių įgyvendinimo pasirinktos organizacijos pavyzdį ir atskleisti su modelių įgyvendinimu susijusius atliekamus organizacijos veiksmus, pasirinktas atvejo studijos metodas, kuris leido iš arčiausiai pamatyti, kaip kibernetinio saugumo modeliai veikia organizacijoje ir įsigilinti į procesus, vykstančius organizacijos viduje. Atvejo analizė buvo atliekama per laiko intervalą (2023 m. birželio-lapkričio mėn.), šio darbo autoriui dirbant UAB „XXX“ ir kooperuojantis su UAB „XXX“ Informacijos saugumo pareigūnu abu dirbo ties pasirengimu 2023 m. spalio pabaigoje vykusiam UAB „XXX“ ISO 27001 priežiūros auditui. Taip pat, darbo autorius turėjo galimybę išanalizuoti vidines struktūras, politikas ir visą dokumentaciją, procedūras ir procesus, susijusius su kibernetinio saugumo brandos modelių įgyvendinimu UAB „XXX“. Nuolatinis bendradarbiavimas su UAB „XXX“ Informacijos saugumo pareigūnu bei Rizikos ir atitikties vadove leido darbo autoriui sistemingai įsigilinti į UAB „XXX“ kibernetinio saugumo procesus, juos atnaujinti, o kai kuriuos visiškai pakeisti.

Apie UAB „XXX“. Jau minėta, kad tai tarptautinės skolų išieškojimo organizacijos netiesioginio aptarnavimo operacijų padalinys, tad organizacijos struktūra taip pat priklauso nuo grupės sprendimų.



13 Paveikslas. UAB „XXX“ organizacinė struktūra. Šaltinis: autorius.

13 Paveiksle matyti, kad UAB „XXX“ Informacijos saugumo pareigūnas priklauso IT skyriui, o taip pat atsakingas ir Grupės informacijos saugumo departamentui. Grupės informacijos saugumo departamentas

apima koordinavimo, paramos ir kontrolės funkcijas visoje 20 įmonių grupėje, kuriose prižiūri ir skatina informacijos saugumą. Šis departamentas yra rizikos ir atitikties funkcijos dalis, kuri yra atsakinga už rizikos ir atitikties valdymo įgyvendinimą verslo ir pagalbinėse funkcijose, taip pat už rizikos ir atitikties klausimų stebėjimą ir tolesnę veiklą. Globalaus informacijos saugumo departamento pareigos ir bendra veikla apima, tačiau (neapsiriboja):

- Grupės saugumo mokymų ir informavimo programų diegimas.
- Didelio saugumo incidento susijusios veiklos rėmimas.
- Saugumo patarimų teikimas paprašius ir, kai manoma, kad tai būtina.
- Privalomų grupės saugumo bazinių linijų, instrukcijų, standartų ir gairių vidaus taisyklėms nustatymas.
- Grupės trečiųjų šalių rizikos vertinimų vykdymas ir pagalbiniai vietiniai vertinimai.

Grupės informacijos saugumo departamentas sukūręs Informacijos saugumo kontrolių sistemą, remiantis: visos grupės informacijos saugos vidaus taisyklėmis, tarptautiniais standartais, tokiais kaip ISO 27001 ir ISO 27002, NIST modeliu ir PCI DSS, o taip pat teisiniais ir reguliaciniais reikalavimais bei geriausiomis praktikomis, įvardija minėtą sistemą kaip patikimą informacijos saugos valdiklių rinkinį. Kontrolės suskirstytos į 16 grupių pagal operatyvinį pajėgumą, įvertintos pagal kritiškumą ir yra vertinamos kiekviename grupės padalinyje pagal Gebėjimų brandos modelio (*ang. Capability Maturity Model (CMM)*), 5 brandos lygius – *ad hoc* (pagal situaciją), pasikartojantis, apibrėžtas, valdomas ir optimizuotas. Ši Informacijos saugumo kontrolių sistema yra peržiūrima bent kartą per metus ir pagal ją audituojamas kiekvienas grupės padalinys, atsižvelgiant į: atnaujintos ir naujas vidaus taisykles, atsiliepimus ir įvertinimus iš kitų grupės padalinių ir/ar grupės funkcijų, procesų patobulinimus, bet kokius naujus teisinius, reguliacinius ar atitikties reikalavimus, grėsmes ir IT aplinkos pokyčius, saugumo incidentų tendencijas.

Skolų išieškojimo organizacija savo veikloje vadovaujasi trimis gynybos linijomis, ir Grupės informacijos saugumo departamentas, kaip antroji gynybos linija, taip pat apima grupės atitiktį, grupės veiklos riziką, duomenų apsaugą ir kitas po - funkcijas. Taip pat Grupės informacijos saugumo departamentas yra atsakingas už informacijos ir IT saugumo bazinių reikalavimų, taikomų visai grupei (visoms pasaulinės ir vietinės rinkos dukterinėms įmonėms), apibrėžimą pagal instrukcijas, standartus ir gaires (vidaus taisykles), kurias patvirtina organizacijos valdyba ir paskelbia visiems darbuotojams. Grupės informacijos saugumo departamentas neatsako už konkrečių kontrolės priemonių, kurios būtinos, kad atitiktų vidinių taisyklių ir kitų šaltinių bazinius saugumo reikalavimus, parinkimą ir įgyvendinimą.

Atitinkamų saugumo kontrolės priemonių projektavimas, įgyvendinimas ir valdymas yra pirmoji kiekvienos organizacijos grupėje atsakomybė.

UAB „XXX“ Informacijos saugumo pareigūno atsakomybės yra užtikrinti, kad grupės organizacijoje būtų laikomasi taikomų su informacijos ir IT saugumu susijusių instrukcijų, įstatymų ir kitų teisės aktų bei kitų (dažnai sutartinių) su informacijos saugumu susijusių įsipareigojimų. Informacijos saugumo pareigūnas bendradarbiauja su grupės organizacijos IT vadovybe ir Grupės informacijos saugumo departamentu, kad užtikrintų, jog IT saugos kontrolė būtų įdiegta ir veiktų taip, kaip numatyta. Turėdami punktyrinę ataskaitų teikimo liniją (13 Paveikslas) Informacijos saugumo pareigūnas į Grupės informacijos saugumo departamentą, Informacijos saugumo pareigūnas yra kaip Grupės informacijos saugumo departamento komandos narys vienoje iš grupės organizacijų. Todėl Informacijos saugumo pareigūnas:

- Bent kartą per metus atlieka vidinės dokumentacijos spragų analizę, kad nustatytų galimas spragas arba konfliktus tarp vietoje valdomų saugos instrukcijų ir visos grupės saugumo instrukcijų. Grupės vidaus taisyklės visada pakeičia vietines instrukcijas, nebent grupės nurodymų savininkas patvirtintų raštu.
- Užtikrina, kad vietinė politika (jei taikoma) būtų atnaujinta, kad atitiktų vidaus taisykles ir būtų patvirtinta vietos vadovybės
- Užtikrina, kad būtų laikomasi privalomų saugos reikalavimų, ir pradėti tobulinimo veiklą, siekiant sumažinti nevykdomas saugumo kontrolės priemones ir nepriimtiną IT/IS riziką.
- Palaiko kokybės kontrolės audito seką, kad būtų galima atlikti vidaus ir išorės saugumo auditą;
- Praneša vietos ir grupės vadovybei apie kylančias rizikas, saugumo incidentus ir veiksmų (rizikos mažinimo) planus.

Taigi pagal visos skolų išieškojimo organizacijos struktūrą, UAB „XXX“ kaip grupės narys, privalo savo veikloje vadovautis grupės dokumentacija bei gairėmis, kiek tai neprieštarauja valstybės įstatymams, kur numatyta, pagal juos priimti vidines taisykles. Taip pat, organizacijos struktūra parodo ryšį, kaip Grupės informacijos saugumo departamentas prižiūri, padeda, o kartu ir reguliuoja kiekvienos grupės organizacijos nario veiklą. Taigi UAB „XXX“ savo veikloje vadovaujasi Lietuvos Respublikos įstatymais ir teisės aktais, grupės instrukcijomis, taisyklėmis bei gairėmis ir vidinėmis taisyklėmis, o Informacijos saugumo pareigūnas atsakingas su informacijos saugumu susijusios dokumentacijos kasmetinę peržiūrą bei kitas informacijos saugumo kontroles, ir taip būti pasiruošęs tiek vidaus, tiek išorės saugumo auditams.

Informacijos saugumo pareigūnas UAB „XXX“ tyrimo pradžioje buvo pradirbęs vos 4 mėnesius, todėl jam buvo naudingas šio darbo autoriaus prisijungimas prie pasirengimo ISO 27001 auditui ir buvo

sudėliotas veiksmų planas bei pasiskirstyta atsakomybėmis. Šio magistrinio darbo autoriui buvo suteiktos atsakomybės:

- Informacijos saugumą reglamentuojančios vidinės dokumentacijos auditas;
- ISO 27001 tinkamumo pareiškimo auditas;
- ISO 27001 susijusių ir sertifikavimo įmonei pateikiamų dokumentų ir priedų auditas;
- Anksčiau vykusių ISO 27001 išorinių auditų bei kitų UAB „XXX“ atitikties auditų išvadų ir jose pateiktų trūkumų analizė.

Taigi atvejo analizei UAB „XXX“ siekiant ištirti ISO 27001 ir NIST kibernetinio saugumo brandos modelių efektyvumą organizacijoje, buvo sudarytas planas, kuris pateiktas 14 paveiksle:

14 Paveikslas. Atvejo analizės planas. Šaltinis: autorius.

Įgyvendinus pirmą plano žingsnį ir atlikus UAB „XXX“ vidinės dokumentacijos, reglamentuojančios informacijos saugumą, analizę, buvo įžvelgtos spragos, kurios pateikiamos 10 lentelėje.

Informacijos saugumą reglamentuojančios vidinės dokumentacijos auditas	• **Neatnaujinta ISMS politika** ir kiti dokumentai daugiau nei vienerius metus (dokumentuose numatyta atnaujinti kas vienerius metus). • Pasikartojanti **informacij**a **su grupės dokumentacija**, kuri taikoma tiesiogiai • Susidėliotas veiksmų planas pagal dokumentaciją (neatliktas vidaus auditas, nesurengtas susitikimas su vadovybe)
ISO 27001 tinkamumo pareiškimo auditas	• Atnaujinus dokumentaciją pasikeitė kontrolių nuorodos į dokumentus
ISO 27001 susijusių ir sertifikavimo įmonei pateikiamų dokumentų ir priedų auditas	• Neatnaujinti ir neužpildyti sertifikavimo įmonei prieš auditą pateikiami priedai, pvz. Rizikų vertinimas.
Anksčiau vykusių ISO 27001 išorinių auditų bei kitų UAB „XXX“ atitikties auditų išvadų ir jose pateiktų trūkumų analizė	• Trūkumai nesuvesti į rizikos vertinimo ir korekcinių priemonių failus.

10 Lentelė. Atvejo analizės vidinės dokumentacijos spragos. Šaltinis: autorius.

Vidinių dokumentų, reglamentuojančių informacijos saugumą UAB „XXX“ analizė, atskleidė, kad grupės priimti dokumentai yra integruojami į vidinius dokumentus, reikalingi skyriai/poskyriai kopijuojami iš grupės taisyklių, tačiau atsinaujinus grupės taisyklėms, vidinės UAB „XXX“ taisyklės nebuvo

atnaujintos. Vidinė UAB „XXX“ dokumentacija labiau susijusi su ISO 27001 modeliu, o NIST modelis niekur neminimas.

Antrasis atvejo analizės žingsnis organizacijoje buvo atnaujinti dokumentaciją. Pirminis tikslas buvo pasiruošimas ISO 27001 auditui, tačiau vidinės UAB „XXX“ dokumentacijos atnaujinimui įtakos turėjo ir ankstesnių auditų trūkumai bei rekomendacijos. Dvejose Rizikos ir atitikties auditų ataskaitose buvo pabrėžtas fizinės saugos politikos nesilaikymas, taip pat ankstesnio išorinio ISO 27001 audito rekomendacija dėl fizinės saugos politikos bei praėjimo kortelių atnaujinimas, o taip pat tyrimo metu vyko grupės Informacijos saugumo kontrolių sistemos auditas, kuris vadovaujasi NIST žingsniais ir matuoja kiekvieno grupės padalinio kibernetinio saugumo brandą remiantis Gebėjimų brandos modelio metodika, pabrėžė fizinės saugos politikos prioritetą. Taigi UAB „XXX“ fizinės saugos politika buvo atnaujinama iš pagrindų, bendradarbiaujant Informacijos saugumo pareigūnui, Ofiso administratorei, Žmogiškųjų išteklių specialistei bei Rizikos ir atitikties vadovei. Fizinės saugos politika atnaujinta nustatant pozicijas ir atsakomybes darbuotojams, sukuriant praėjimo kortelių išdavimo/grąžinimo/registravimo procesus bei pačių kortelių atnaujinimą. Taip pat buvo sutvarkytas ir atnaujintas pagrindinis ISO 27001 dokumentas – ISMS politika.

Trečiasis atvejo analizės žingsnis apėmė auditą. Vidinis auditas apėmė jau minėtą fizinės saugos dokumentaciją, dėl kurios buvo gauta ir išorinių auditų trūkumų bei trečiųjų šalių rizikos vertinimą. Apie fizinės saugos politikos atnaujinimą jau aptarta antrajame atvejo analizės žingsnyje. Trečiųjų šalių rizikos vertinimas prasidėjo identifikuojant visus UAB „XXX“ tiekėjus. Kadangi UAB „XXX“ yra netiesioginio aptarnavimo padalinys, tad tiesioginių trečiųjų šalių, kurių nevaldytų grupė, buvo identifikuotos tiktai 6, iš kurių 3 nepasiekiančios jokių asmens duomenų, tad trečiųjų šalių rizikos vertinimas buvo atliekamas 3 tiekėjams. Tuo pačiu metu grupė pasidalino grupės Informacijos saugumo kontrolių sistemos audito ataskaita, kurioje taip pat buvo išskirti UAB „XXX“ trūkumai: fizinė sauga bei trečiųjų šalių rizikos vertinimas. Apie fizinę saugą grupei buvo pasidalinta vykdomais, tačiau dar nepatvirtintais pokyčiais, kurie buvo įvertinti kaip optimizuoti ir pakeliantys bendrą UAB „XXX“ kaip grupės padalinio brandą. Tad ši grupės Informacijos saugumo kontrolių sistemos audito ataskaita pateikė ir skaitinę organizacijos brandos išraišką - 3,2 iš 5 galimų, lygis - Apibrėžtas. Pagal UAB „XXX“ tai reiškia, kad pozicijos ir atsakomybės yra apibrėžtos, priskirtos ir išmokyta pagal užimamą poziciją; organizacijos politikos ir procedūros yra apibrėžtos ir standartizuotos bei paremiančios organizacijos strategiją; tinkamai įdiegtos atitinkamos technologijos. UAB „XXX“ ne tik pateikė sutvarkytą dokumentaciją, įrodymus apie vykdomas veiklas, taisė ankstesnius trūkumus, tačiau taip pat ir žengė papildomus žingsnius, kurie lėmė aukštesnį brandos lygį lyginant su kitomis grupės organizacijomis.

Ketvirtasis ir paskutinis atvejo analizės organizacijoje etapas buvo pagalba atstovaujant išoriniam ISO 27001 auditui. Išorinis ISO 27001 auditas vyko 2023 m. spalio mėn. į UAB „XXX“ patalpas atvykus sertifikuotos įmonės auditoriams. Tai buvo trečiasis ISO 27001 priežiūros auditas, taigi audito metu dėmesys buvo kreipiamas į prieš tai jau įžvelgtus UAB „XXX“ trūkumus, pateiktas rekomendacijas. Auditas praėjo sklandžiai, auditoriai įvertino įvykusį UAB „XXX“ dokumentacijos ir procesų progresą. Pastebėta, kad ISO sertifikavimo audito metu, auditoriai ieško bent minimalios atitikties su standarto ir kontrolių punktais, per daug nesigilinant į detales, tad tai labai palanku organizacijoms, siekiančioms formaliai atitikti ir gauti sertifikatą.

Taigi UAB „XXX“ NIST modelis taikomas tiek, kiek jį taiko grupė, o būtent Grupės informacijos saugumo departamentas, kuris NIST funkcijas, kategorijas ir subkategorijas yra įtraukęs ne tik į grupės padaliniams pateikiamą dokumentaciją, o taip pat ir į grupės Informacijos saugumo kontrolių sistemos auditą. Taigi NIST modelis yra integruotas ir į visas UAB „XXX“ vidines politikas ir procesus. Kadangi NIST modelis reikalauja tik savęs-įvertinimo, UAB „XXX“ tai daroma kasmet vertinant kiekvieną grupės padalinį pagal grupės Informacijos saugumo kontrolių sistemos parengtą audito planą. Skirtingai nei NIST modelį, ISO 27001 modelį kiekvienas grupės padalinys turi įsidiegti individualiai. Kaip ir kiekviename padalinyje, siekiančiam ISO 27001, turi būti paskirtas atsakingas asmuo, sukurta, priimta ir įgyvendinta ISMS politika bei visi kiti su ISO 27001 susiję reikalavimai. Tad UAB „XXX“ atitinkamai dėjo pastangas dėl ISO 27001 įdiegimo be grupės pagalbos.

Kriterijai, pagal kuriuos buvo vertinami kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumas atvejo analizės metu pateikti 11 lentelėje:

EFEKTYVUMO VERTINIMO KRITERIJAI	**UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS**
Valdymas. Kibernetinio saugumo politikos priimtos ir patvirtintos vadovybės bei iškomunikuotos visiems darbuotojams, paskirstytos atsakomybės. Vadovybės įsitraukimas į informacijos saugumo valdymą.	UAB „XXX“ būdama viena iš grupės padalinių savo veikloje tiesiogiai vadovaujasi grupės priimtomis politikomis, kiek jos neprieštarauja Lietuvos Respublikos įstatymams, ir vidinėmis politikomis. Visa dokumentacija parengta pagal grupės patvirtintą šabloną ir nustatytus kriterijus, numatant dokumento savininką bei patvirtinta atitinkamų vadovų. Apie politikas UAB „XXX“ darbuotojai sužino tik pradėję dirbti, su kai kuriais supažindinami pasirašytinai, o apie kai kuriuos net nesužino, taip pat apie atnaujintą dokumentaciją darbuotojai nebuvo informuojami. Tyrimo metu pradėta kas mėnesį UAB „XXX“ vidiniame socialiniame tinkle skelbti apie visiems privalomas, arba atnaujintas politikas, kurios tiesiogiai taikomos

EFEKTYVUMO VERTINIMO KRITERIJAI	UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS
	darbuotojams kasdieninėje veikloje. UAB „XXX“ vadovai įsitraukia į informacijos saugumo valdymą tiek, kiek atitinkamų skyrių vadovai pateikia jiems informacijos. Pagal ISO 27001 privalomi vadovybės susitikimai, kurių metu aptariama esama kibernetinio saugumo situacija, kylančios rizikos, įvykę pasikeitimai, santykiai su trečiosiomis šalimis. Ruošiantis ISO 27001 auditui buvo nustatyta, kad vienintelis susitikimas su vadovybe buvo 2021 metais, 2022 metais praleistas dėl besikeičiančių darbuotojų ir neperduotų atsakomybių, neužtikrintas tęstinumas, todėl nedelsiant buvo surengtas susitikimas su vadovybe ir aptarti visi būtini punktai, UAB „XXX“ informacijos saugumo strategija ir tikslai. Po šio susitikimo vadovybė paskyrė kas mėnesinius susitikimus su Informacijos saugumo pareigūnu apžvelgti UAB „XXX“ kibernetinio saugumo situaciją.
Atitiktis. Dokumentacija atitinka galiojančius Lietuvos Respublikos teisės aktus, saugojimo terminus, pranešimo apie incidentus terminus bei atitiktis sudarytoms sutartims su šalimis. Vidiniai auditai.	UAB „XXX“ Rizikos ir atitikties skyrius bendradarbiauja su Grupės rizikos ir atitikties skyriumi ir jeigu Grupės patvirtintos politikos prieštarauja ar kitaip skiriasi nuo Lietuvos Respublikos įstatymuose įtvirtintų normų, UAB „XXX“ priima vidinę politiką remdamasi Lietuvos Respublikos įstatymais. Grupė audituoja UAB „XXX“ padalinį: Atitikties kontrolių stebėjimo auditas trijų metų ciklu nustatytomis sritimis, Informacijos saugumo kontrolių sistemos auditas trijų metų ciklu nustatytomis sritimis bei vidiniai UAB „XXX“ Rizikos ir atitikties skyriaus auditai trijų metų ciklu nustatytomis sritimis. UAB „XXX“ kaip netiesioginio aptarnavimo padalinys bendradarbiauja su kitų valstybių padaliniais ir teikia jiems paslaugas pagal sutartį, tad kitų valstybių padaliniai taip pat daro kasmetinius auditus operacijų komandose, o kartu ir Rizikos ir atitikties skyriuje. Visų auditų ataskaitos UAB „XXX“ padeda identifikuoti rizikingas ar neatitinkančias sritis. Atitikties skyrius deda didžiules pastangas įvesti optimizuotus procesus, valdyti kylančias rizikas ir taip užtikrinti UAB „XXX“ atitiktį reglamentų, Lietuvos Respublikos įstatymų, grupės politikoms, vidinės taisyklėms bei sutartiniams įsipareigojimams.
Informacijos saugumo užtikrinimas. Darbuotojai laikosi organizacijos politikų, taisyklių, instrukcijų.	Informacijos saugumas UAB „XXX“ įtvirtintas tiesiogiai taikomoje grupės informacijos saugumo politikoje. Deja apie šią politiką mažai komunikuojama, tačiau 2 kartus per metus darbuotojai privalo dalyvauti nuotoliniuose mokymuose, atlikti testą. Kito padalinio audito metu buvo identifikuota, kad vienas operacijų skyrius elektroninio pašto dėžutėje

EFEKTYVUMO VERTINIMO KRITERIJAI	UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS
	archyvuoja laiškus su asmens duomenimis ilgesnį laiką nei būtina, ne visi darbuotojai dėvi vardo kortelę, ne visi darbuotojai trumpam palikdami darbo vietą užrakina kompiuterį. Tai tik keli pavyzdžiai, kurie atskleidžia, kad ne visi darbuotojai laikosi organizacijos politikų, taisyklių, instrukcijų.
Žmogiškųjų išteklių saugumas. Įdarbinimo metu, įdarbinus ir pasibaigus darbiniams santykiams laikomasi nustatytų patikrinimų, konfidencialumo įsipareigojimų.	UAB „XXX“ įdarbinimo metu siunčia anketą dėl patikrinimo, įdarbinus pasirašomas konfidencialumo susitarimas, o taip pat pati darbo sutartis numato, kad konfidencialumo įsipareigojimas galioja ir pasibaigus darbiniams santykiams.
Rizikos valdymas. Informacijos saugumo rizikos, trečiųjų šalių rizikos, turto valdymo rizikos bei asmens duomenų apsaugos rizikos yra įvertintos, nuolat stebimos, sudaryti rizikos valdymo/mažinimo planai. Rizikos valdymo strategija.	Rizikos valdymo strategija yra numatyta Grupės, ir UAB „XXX“ kiekvieną ketvirtį teikia ketvirčio rizikos ataskaitas Grupei. Tiek informacijos saugumo rizikos, tiek turto valdymo, bei atitikties rizikos buvo identifikuotos ir įvertintos. Tačiau UAB „XXX“ trečiųjų šalių rizikos buvo vertinamos likus keliems mėnesiams iki ISO 27001 audito, o paskutinė prieš tai buvusio vertinimo data buvo 2021 metais. Tad UAB „XXX“ ne visų sričių rizikos buvo tinkamai vertinamos ir pagrindinė priežastis – darbuotojų kaita bei neperduotos atsakomybės.
Informacijos apsauga. Duomenys yra naudojami ir perduodami pagal nustatytas organizacijos politikas ir taisykles, laikantis duomenų klasifikavimo ir duomenų nutekėjimo prevencijos. Atsarginių kopijų darymas.	Didžioji dalis duomenų yra naudojami ir perduodami pagal UAB „XXX“ ir Grupės nustatytas politikas bei taisykles, tačiau išskirtinas pavyzdys, kai užsienio kalba gautas skolininko dokumentas su itin jautriais asmens duomenimis yra išsiverčiamas naudojant UAB „XXX“ taisyklėse numatytą ir neleidžiamą naudoti vertėją. Kitas pavyzdys, kai gaunamas skolininko dokumentas yra siunčiamas ne pagal operacijų numatytą instrukciją ir išsiunčiamas ne tam gavėjui. Operacijų komandos fiksuoja tokius įvykius kurdami operacinės rizikos įvykį, jį analizuoja, taiko rizikos mažinimo veiksmus bei stengiasi išvengti panašių situacijų ateityje taikydami kokybės kontroles. Sistemų atsarginės kopijos yra daromos priklausomai nuo sistemų. Pati UAB „XXX“ savo turi tik vieną sistemą, kuri naudojama užsirezervuoti ofiso sėdėjimo vietą, ir jos atsarginė kopija nustatyta daryti automatiškai kiekvieną mėnesį. Visos kitos sistemos priklauso grupei ir taip pat su nustatytomis atsarginių kopijų darymais kas mėnesį, kaip nustato Grupės politikos, išskyrus atvejais, kai nustatyta atsarginių kopijų darymas kiekvienos darbo dienos pabaigoje.

EFEKTYVUMO VERTINIMO KRITERIJAI	UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS
Turto valdymas. Organizacijos naudojamos programos, sistemos bei fizinis turtas yra registruojamas ir prižiūrimas. Įrangos saugumas.	Fizinis UAB „XXX“ išduodamas turtas laikomas darbuotojams išduodama praėjimo kortelė ir darbui reikalinga įranga (kompiuteris, įkroviklis, ausinės), kurie yra registruojama ir prižiūrima IT skyriuje. Įrangos saugumas yra užtikrinamas antivirusinėmis programomis, ugniasienėmis. Be sistemos administratoriaus teisių darbuotojai negali įsirašyti papildomų programų, nebent yra vadovo leidimas ir patvirtinimas. Besiruošiant ISO 27001 auditui, UAB „XXX“ Informacijos saugumo pareigūnas identifikavo, kad keli darbuotojai savo kompiuteriuose turi daugiau programų nei leidžiama. Tad jis savo iniciatyva pradėjo daryti UAB „XXX“ naudojamų programų auditą, ir paaiškėjo, kad yra daugiau darbuotojų, turinčių įvairių papildomų programų, apie kurias IT skyrius net nebuvo informuotas. Informacijos saugumo pareigūnas savo ruožtu kreipėsi į darbuotojus ir tikslinosi, kokiomis aplinkybėmis ir kokiais tikslais papildomos programos buvo naudojamos.
Trečiųjų šalių informacijos saugumas. Trečiosios šalys, tiekėjai, su jais susijusi informacijos saugumo rizika yra nustatyta, įvertinta bei valdoma.	Jau minėta prie „Rizikos valdymo“ kriterijaus, kad trečiųjų šalių rizikos buvo vertinamos likus keliems mėnesiams iki ISO 27001 audito, o paskutinė prieš tai buvusio vertinimo data buvo 2021 metais. Buvo identifikuoti 6 UAB „XXX“ tiekėjai, iš kurių 3 turi priėjimą prie asmens duomenų ir privalo turėti rizikos vertinimą, tad buvo susisiekta su šiais tiekėjais, siunčiamas jiems klausimynas, identifikuotos ir įvertintos su jais susijusios rizikos.
Tapatybės ir prieigos valdymas. Stebimas tapatybės ir prieigos valdymas, nesuteikiant daugiau teisių negu reikia darbo funkcijoms atlikti.	Kiekvienam darbuotojui suteikiamos prieigos pagal darbo funkcijas. Pagal poreikį kiekvienas darbuotojas gali prašyti daugiau teisių, tačiau jo prašymą turi patvirtinti jo vadovas, apie būtinumą darbo funkcijoms atlikti. Dėl bet kurių kitų teisių suteikimo taip pat reikalingi atitinkamų atstovų patvirtinimai (pvz. IT skyriaus). Taip pat prisijungiant naudojama ir tapatybės patvirtinimas per darbuotojo mobilųjį įrenginį.
Grėsmių ir pažeidžiamumo valdymas. Grėsmės ir pažeidžiamumai yra stebimi, nustatomi bei pašalinami.	Grėsmes ir pažeidžiamumus prižiūri Informacijos saugumo pareigūnas, kuris kas savaitę įjungia sistemų grėsmių ir pažeidžiamumų skanavimą. Rastos grėsmės ir pažeidžiamumai yra įvertinami, jeigu jie kelia įtarimų, apie juos yra komunikuojama. Taip pat kiekvieną ketvirtį teikiama grėsmių ir pažeidžiamumų ataskaita Grupės informacijos saugumo departamentui.
Informacijos saugumo įvykių valdymas.	Informacijos saugumo įvykių valdymą reglamentuoja Grupės politika, kuri numato, komunikacijos ir reagavimo į incidentus, žingsnius. Tyrimo metu

EFEKTYVUMO VERTINIMO KRITERIJAI	UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS
Informacijos saugumo incidentai nustatomi, pranešami ir pašalinami.	UAB „XXX“ darbuotojas identifikavo galimą informacijos saugumo incidentą, kurio metu buvo pasinaudota prieiga prie sistemos per kurią siunčiamos SMS žinutės, kur finansinis nuostolis Grupei ~5000 EUR. UAB „XXX“ reagavo iškarto pagal minėtus Grupės politikos žingsnius ir pagrindinė UAB „XXX“ Informacijos saugumo pareigūno atsakomybė buvo komunikacija Grupės informacijos saugumo departamento darbuotojams.
Sistemos ir tinklo sauga. Sistemos ir tinklo sauga yra valdomi: tinklo atskyrimai, apsauga nuo kenkėjiškų programų.	UAB „XXX“ atskirti IT, svečių ir darbuotojų tinklai. Visada aktyvi ugniasienė o nuo kenkėjiškų programų įdiegtos antivirusinės, bei naudojama proaktyvi komunikacija.
Saugi konfigūracija Sistemų sugriežtinimas, naudojama kriptografija.	Visi slaptažodžiai, prisijungimas ir „bendravimas“ tarp serverių naudoja kriptografiją.
Programų saugumas. Sistemų tobulinimai, kūrimas, saugus kodavimas ir pokyčių valdymas.	Programos dažniausiai yra atnaujinamos / išleidžiamos per tris etapus: 1 etapas. Testavimas ir tobulinimai, kur tik kūrėjai testuoja su netikrais arba senais duomenimis. 2 etapas. Testavimas su pilotinėmis grupėmis, kurios dirba su sistemomis. 3 etapas. Išleidimas visiems. Taip yra užtikrinamas sklandus sistemų veikimas.
Fizinis saugumas. Fizinis patalpų ir aplinkos saugumas, švaraus stalo politika, darbuotojų kompiuterių rakinimas.	Fizinis saugumas UAB „XXX“ buvo pažymėtas keliose audito ataskaitose ir rekomendacijose. Svečių priėmimo tvarka, darbuotojų/svečių kortelių išdavimas/grąžinimas, jų nedėvėjimas, buvusių darbuotojų kvietimas į ofiso patalpas, kompiuterių nerakinimas trumpam paliekant darbo vietą, dokumentų su jautriais duomenimis laikymas bendruose stalčiuose. Tai tik keletas pavyzdžių, kurie akivaizdžiai buvo pastebimi atvejo analizės metu UAB „XXX“. Todėl daug dėmesio buvo skirta fizinės politikos atnaujinimui, darbuotojų praėjimo kortelių priskyrimui iš naujo, PIN kodų pakeitimu, svečiams ir darbuotojams praėjimo kortelių išdavimo/grąžinimo proceso atnaujinimu. Taip pat iš naujo paskleista informacija apie švaraus stalo politiką, kurioje pabrėžiamas kompiuterio rakinimas kiekvieną kartą trumpam paliekant darbo vietą, taip pat buvo paskleista komunikacija apie vardinių kortelių dėvėjimą matomoje vietoje, bei pašalinių žmonių nebuvimą ofiso patalpose. Po komunikacijos situacija šiek tiek pradėjo keistis, buvo stebimas ir svečių registras, bei komunikuojama su ofiso administratore, kuri pirmoji sužino apie svečius. Tad pasibaigus atvejo

EFEKTYVUMO VERTINIMO KRITERIJAI	UAB „XXX“ ATVEJO ANALIZĖS VERTINIMAS
	analizės tyrimui, daugiau darbuotojų dėvėjo darbuotojų korteles, nebebuvo matyti pašalinių žmonių ofiso patalpose.
Organizacijos darbuotojai. Jų supratimas apie kibernetinį saugumą. Įsitraukimas ir elgesys, darbuotojų požiūris į kibernetinį saugumą bei darbuotojų mokymai, „***PHISHING***“ simuliacijos.	Per kalendorinius metus kiekvienas darbuotojas gauna dvejus Grupės privalomus mokymus su testu: Tinkamas IT naudojimas ir Kibernetinis saugumas. Be šių dviejų, taip pat 2 kartus per metus yra mokymai susiję su Elektroninio pašto saugumu bei „*Phishing*“ mokymai. O taip pat, yra siunčiamos darbuotojams „*phishing*“ simuliacijos, bei visos Grupės mastu skaičiuojami darbuotojų paspaudimai bei visi padaliniai lyginami vieni su kitais. Dažniausiai darbuotojams šie privalomi mokymai yra tik laiko švaistymas, mokymai pasitinkami su nepasitenkinimu, nes ypač operacijų komandose svarbi kiekvieną minutė dėl itin didelio darbo krūvio. Jau minėta anksčiau, kad net ne visi darbuotojai trumpam palikdami darbo vietą užrakina kompiuterį, tad informacija lieka nesaugi. Taip pat siekia naudotis socialiniais tinklais, įsirašyti papildomą programinę įrangą, todėl pagrįstai galima teigti, kad UAB „XXX“ darbuotojų supratimas apie kibernetinį saugumą yra žemas. Tai įrodo ir „*phishing*“ simuliacijos rezultatai: 2023 metų ketvirto ketvirčio rezultatai buvo - 19 procentų UAB „XXX“ darbuotojų neidentifikavo „*phishing*“ elektroninio laiško paspausdami ant el. laiške buvusios nuorodos ar failo ir UAB „XXX“ užėmė 15 vietą iš 24 grupės padalinių. Tad net ir du kartus per metus vykstantys „*phishing*“ privalomi mokymai, kurie padaryti kaip itin įtraukūs, pasitelkus animaciją ir interaktyvius paspaudimus, tačiau išlieka labai didelė rizika, kad darbuotojai gavę ne simuliacijos laišką, paspaus ant el. laiške esančio failo ar nuorodos.
Tobulinimas. Nuolatinis organizacijos ir kibernetinio saugumo brandos tobulinimas organizacijoje.	UAB „XXX“ efektyviai veikiančią nuolatinio tobulinimo sistemą parodo tai, kad kiekviena komanda turi už nuolatinio tobulėjimo idėjas, jų registravimą ir priežiūrą atsakingą darbuotoją. UAB „XXX“ skatinama kultūra iš įvykusių klaidų ar siekiant prevenciškai apsisaugoti, kad jos nesikartotų, kurti nuolatinio tobulinimo idėjas ir jas įgyvendinti kartais net pasitelkiant kitų komandų darbuotojus. Skelbiamos ir mėnesio, ir ketvirčio daugiausiai laiko sutaupiusios idėjos. Ši kultūra aktyviai skleidžiama operacijų komandose siekiant pamažinti daromų klaidų skaičių, ir dažnai klaidos, užregistruotos kaip operacinės rizikos padeda sukurti nuolatinio tobulinimo idėjas, tačiau jos labai retais atvejais tėra susijusios su informacijos sauga.

11 Lentelė. Atvejo analizės UAB „XXX“ vertinimo kriterijai ir vertinimas. Šaltinis: autorius.

Atvejo analizė pagal parinktus efektyvumo kriterijus atskleidė, kad organizacija gali būti prižiūrima ir audituojama grupės, priėmusi kibernetinio saugumo organizacijoje politikas, skelbianti apie turimus standartus, audituojama išorinių auditorių, tačiau iš vidaus ji lieka pažeidžiama ir kibernetinio saugumo brandos organizacijoje vertinimo modeliai veikia neefektyviai. Atvejo analizė parodė, kad kibernetinio saugumo brandos organizacijoje vertinimo modeliai tėra didžiulė našta darbuotojams, nes visi nori išvengti papildomo darbo krūvio, o kibernetinio saugumo brandos modeliai reikalauja nuolatinio dėmesio ir įsitraukimo. UAB „XXX“ dėl darbuotojų kaitos, neperduotų atsakomybių naujiems darbuotojams, kompetencijų trūkumo, nutrūkus anksčiau vykdavusiems procesams, yra tik stengiamasi kuo minimalesniais resursais užpildyti atsiradusias spragas. Pavyzdžiui ISO 27001 modelis UAB „XXX“ tapo svarbus tik artėjant išoriniam auditui, ir tam trūko kompetentingų žmogiškųjų išteklių. Pabrėžtina, kad tapo svarbus pats pasiruošimas auditui, o ne reali situacija organizacijoje ir kaip būtų galima ją pagerinti. Sertifikavimo audito metu, auditoriai ieško bent minimalios organizacijos atitikties reikalavimams, nesigilinant, o pačiai organizacijai sertifikato gavimas niekaip nepagerina kibernetinio saugumo situacijos, kol nėra sistemingai dirbančių kompetentingų darbuotojų su informacijos saugumu. Modelių neefektyvumas labiausiai pastebimas iš operacijų padalinių specialistų, kurie savo veikloje nesivadovauja kibernetinio saugumo nustatytais reikalavimais, o taip pat mažas vadovybės įsitraukimas į kibernetinio saugumo skleidimą organizacijoje bei su kibernetinio saugumo brandos modeliais susijusiuose procesuose.

Pagal analizuotus efektyvumo vertinimo kriterijus atvejo analizės metu paaiškėja, kad iš pirmo žvilgsnio organizacija, kuri savo veikloje vadovaujasi ISO 27001 standartu ir NIST modeliu, turi visas reikalingas kibernetinio saugumo politikas, procesus ir instrukcijas, taip pat technologiniu požiūriu viskas prižiūrima ir atitinka aukštus kibernetinio saugumo standartus, pažvelgus iš vidaus, kibernetinio saugumo brandos lygis yra žemas. Tai rodo tik formalią UAB „XXX“ atitiktį kibernetinio saugumo brandos modeliams NIST ir ISO 27001. Tai parodo, kad kibernetinio saugumo brandos organizacijoje vertinimo modeliai yra tik bendros gairės ir bandomos diegti kontrolės – kurios veikia, jei yra nuolat prižiūrimos. ISO 27001 išorinio sertifikavimo ar kito audito metu yra pateikiama, kaip viskas yra valdoma, priimama ir prižiūrima, o ir didžiausias dėmesys skiriamas turimai dokumentacijai. Deja, bet realybė šiek tiek nutolusi nuo dokumentacijos, kuri aktuali tik atitikties skyriui, ir būtent atvejo analizė atskleidė, kad visas kibernetinio saugumo priemonių taikymas prasideda nuo darbuotojų – kol darbuotojai neprisidės ir neįsitrauks bei savo kasdienybėje atliekant kiekvieną operaciją netaikys kibernetinio saugumo priemonių, tol kibernetinio saugumo brandos kultūra organizacijoje nedidės, o kartu ir organizacijos kibernetinio saugumo brandos lygis nesikeis. Kibernetinio saugumo organizacijoje užtikrinimas yra visų darbuotojų atsakomybė ir kiekvienas darbuotojas turi suprasti savo pareigas ir atsakomybes atliekant darbo funkcijas.

3.2 PUSIAU STRUKTŪRUOTO INTERVIU ANALIZĖ IR INTERPRETAVIMAS.

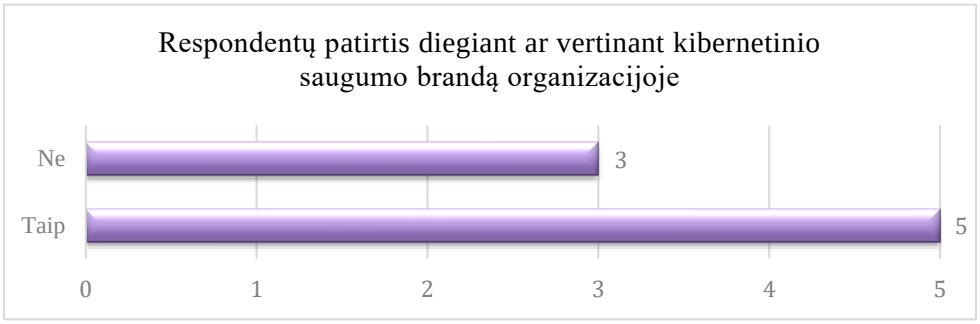
Pusiau struktūrizuoto interviu tikslas buvo papildyti tyrimą aštuoniomis įvairių organizacijų kibernetinio saugumo specialistų patirtimis ir sužinoti organizacijose dirbančių specialistų nuomonę apie kibernetinio saugumo modelius bei jų efektyvumą. Visiems respondentams buvo pateiktas tas pats klausimynas (2 priedas) ir šio darbo 4 priede pateikti visi respondentų atsakymai. Atsakymuose atsispindi ir tai, kad organizacijose dirbančius informacijos saugumo specialistus saisto konfidencialumo įsipareigojimas.

Į pirmą klausimą, apie respondentų išsilavinimą, poziciją ir pareigas organizacijoje, susisteminus gautus rezultatus, atsakymai pateikti 15 paveiksle:

15 Paveikslas. Respondentų pareigos organizacijoje. Šaltinis: 4 Priedas.

Jau minėta, kad respondentų paieška buvo atlikta naudojant socialinį tinklą „Linked IN“, paieškos laukelyje įvedus „informacijos saugumo specialistas“, o gautuose rezultatuose matyti, kad skirtingose organizacijose taikomi skirtingi pareigų pavadinimai.

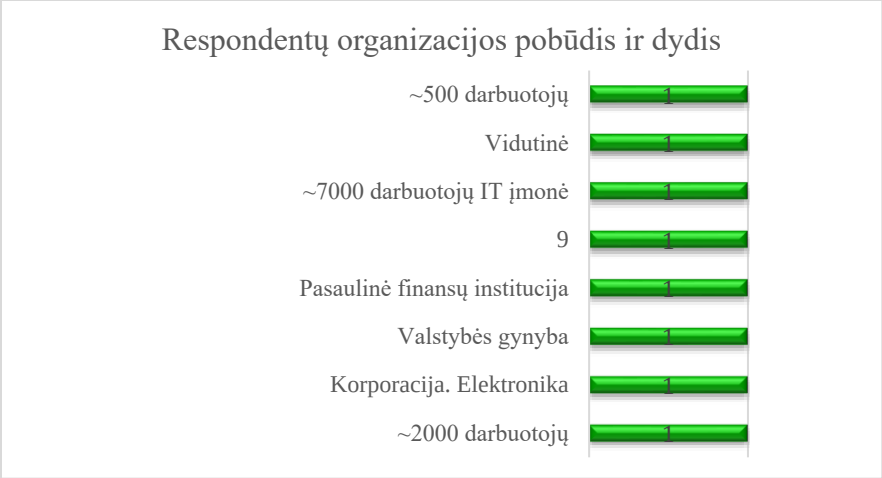
Antrasis klausimas buvo skirtas išsiaiškinti apie respondentų patirtį diegiant ar vertinant kibernetinio saugumo brandą organizacijoje. Susisteminti respondentų atsakymai pateikti 16 Paveiksle:



16 Paveikslas. Respondentų patirtis diegiant ar vertinant kibernetinio saugumo brandą organizacijoje. Šaltinis: 4 priedas.

5 iš 8 respondentų atsakė į šį klausimą teigiamai, kai kurie respondentai atsakydami į šį klausimą pateikė kibernetinio saugumo modelius su kuriais turėjo patirties dirbant, pvz. „ISO/IEC:27001/27002, NIST CSF, COBIT, NEN 7510, CMMI, CIS“, 3 iš 8 respondentai atvirai neigė apie patirtį su kibernetinio saugumo brandos modeliais.

Trečiasis klausimas labai svarbus dėl šio darbo teorinėje dalyje aptarto skirstymo į mažas, vidutines ir dideles įmones: apie organizacijos dydį ir pobūdį. Deja, ne visi respondentai atskleidė organizacijos pobūdį, tačiau keletas atsakymų atskleidė labai svarbios informacijos apie organizacijas: „*Dydis ~500 darbuotojų. Jokių kibernetinio saugumo tikslų ir prioritetų*“, „*Finansinių paslaugų įmonė, turinti 10 000 darbuotojų. Prioritetus apibrėžia 1-osios linijos organizacija, tačiau pagal 2-osios linijos perspektyvą dėmesys sutelkiamas į pagrindinius elementus, kurie gali būti laikomi pagrindine saugumo higiena*“, „*Pasaulinė finansų institucija, kuri specializuojasi skolų valdyme. Kibernetinio saugumo strategija ir programa nėra aiškiai apibrėžta arba nebuvo perteikta mano lygiui*.“, „*Elektronikos sritis, korporacija. Kibernetinio saugumo programos tikslai ir prioritetai mano organizacijoje: Apsaugoti organizacijos duomenis ir informaciją nuo neleistinos prieigos ar pakeitimų. Tinklo sauga ir perimetro apsauga. Užtikrinti duomenų saugą. Teisės aktų laikymasis. Užtikrinti organizacijos verslo tęstinumą ir atsparumą prieš kibernetinius įvykius. Nuolat atnaujinti saugumo strategiją ir prisitaikyti prie pokyčių. Darbuotojų mokymas ir supratimas apie saugumą. Prioritetai: nuolatinis stebėjimas ir priežiūra*.“ Susisteminti respondentų atsakymai pateikti 17Paveiksle



17 Paveikslas: Respondentų organizacijos pobūdis ir dydis. Šaltinis: 4 priedas.

Pateikti respondentų atsakymai rodo, kad 7 iš 8 respondentai atstovauja dideles įmones pagal Europos Komisijos 2003 m. gegužės 6 d. rekomendaciją 2003/361/EC dėl labai mažų, mažų ir vidutinių įmonių apibrėžimo, kur MVĮ kategorijai priskiriamos įmonės, kuriose dirba mažiau nei 250 darbuotojų. Pagal pateiktus atsakymus, tik 1 iš 8 respondentų atstovauja vidutinę įmonę. Valstybės gynybos ekspertas

nenurodė darbuotojų skaičiaus, tačiau tai yra valstybinis ypatingos svarbos sektorius, kuris prilygsta didelei organizacijai. Pasaulinė organizacija taip pat nenurodė darbuotojų skaičiaus, tačiau pasaulinė organizacija, vykdanti savo veiklą keliose valstybėse taip pat pagal darbuotojų skaičių priskiriama didelėms organizacijoms. toliau pateikti respondentų atsakymai išskirstyti į 3 dalis: vidutinė organizacija, didelė organizacija ir valstybinė.

Ketvirtasis klausimas respondentų prašė nurodyti pritaikytus kibernetinio saugumo brandos modelius atstovaujamose organizacijoje bei kas paskatino juos pasirinkti.

Vidutinė: šios organizacijos atstovas atsakydamas į trečiąjį klausimą, pabrėžė, kad „*Nėra jokių kibernetinio saugumo tikslų ir prioritetų*“, tad ir šiame klausime apie pritaikytus kibernetinio saugumo brandos modelius, atsakymas - „*nėra*“.

Didelė: net 4 iš 6 didelių organizacijų respondentai atsakydami į šį klausimą nurodė bendrai naudojamus ISO 27001 ir NIST modelius, viena iš šių organizacijų naudoja dar ir Gebėjimų vertinimo modelį (CMMI). Likę 2 respondentai nurodė „Logiška buvo pasirinkti modelius“, tačiau nenurodė naudojamų modelių, o kitas – „*Rizikos vertinimas*“.

Valstybinė: „*ISO 27001 ir NIST. Siekis pagerinti kibernetinio saugumo situacijos suvokimą*“

Taigi net 5 iš 8 organizacijų, iš kurių viena valstybinė, savo organizacijose naudoja tiek ir ISO 27001 ir NIST modelius. Tai patvirtinta, kad šie modeliai yra labiausiai paplitę pasaulyje, ir populiarūs didelėse organizacijose.

Sekantis, penktasis klausimas buvo susijęs su kibernetinio saugumo brandos modelio diegimo organizacijose procesu, prašant respondentų pasidalinti didžiausiais iššūkiais ir sėkmėmis, įgyvendinimo trukme bei kaštais. Deja į šį klausimą 2 iš 8 respondentų negalėjo atsakyti.

Vidutinė: „*Nėra*“.

Didelė: vienoje organizacijoje modelis vis dar yra diegiamas, o kiti respondentai pasidalino savo įžvalgomis ir patirtimis: „*Pakeisti žmonių nuomonę ir paaiškinti jiems saugumo svarbą, kaina yra laikas ir sąmoningumas*“; „*Kibernetinio saugumo brandos modelis, stabdo verslo sprendimą diegti naujus sprendimus ar produktus*“; „*Iššūkiai buvo ne tiek susiję su pasirinktomis sistemomis, bet kur kas daugiau: supažindinti žmones su pasirinktų kontrolės priemonių pagrįstumu ir jų atsakomybe. Iššūkių, susijusių su faktiniu kontrolės priemonių įgyvendinimu ir kasdieniu valdymu. Sėkmė: Žymiai išaugo informuotumas, ypač tarp su saugumu nesusijusių darbuotojų*“; „*Negalima sakyti, kad įgyvendinimas buvo projektas, tai buvo gana ilgas procesas, kad atitiktų reikalavimus*.“

.

Valstybinė: „*Negaliu atsakyti*“.

Iš pasidalintų respondentų įžvalgų, pažymėtini pagrindiniai iššūkiai organizacijose diegiant kibernetinio saugumo brandos vertinimo modelius: *pakeisti žmonių nuomonę, stabdo verslą, supažindinti žmones, faktinis kontrolių įgyvendinimas ir valdymas, ilgas procesas*. Pasidalinta ir viena sėkmė: „*Žymiai išaugo informuotumas, ypač tarp su saugumu nesusijusių darbuotojų“.* Čia darytina logiška išvada, kad kuo daugiau žmonės, organizacijų darbuotojai, supažindinami su informacijos saugumo reikalavimais, tuo labiau išauga organizacijoje informuotumas.

Respondentai buvo linkę labiau dalintis iššūkiais, negu sėkmėmis, tai rodo nuolat besikeičiančią ir gan sudėtingą kibernetinio saugumo brandos modelių diegimo procesą. Tuo tarpu, pasidalinta viena svarbiausių sėkmių didelėje organizacijoje – išaugo informuotumas, ir ypač tarp tų darbuotojų, kuriems informacijos saugumas nebuvo pagrindinė sritis. Tai rodo, kad organizacijos darbuotojų sąmoningumo didinimas yra esminis veiksnys norint užtikrinti organizacijos kibernetinio saugumo brandos modelių efektyvumą organizacijose ir taip organizacijoms tapti atsparioms kibernetinėms grėsmėms.

Šeštuoju klausimu buvo gilinamasi į kibernetinio saugumo brandos modelio efektyvumą, jo matavimą, kaip jį apibūdina respondentai jų atstovaujamoje organizacijoje.

Vidutinė: „*Nėra*“.

Didelė: Vienas iš respondentų nežino kaip organizacijoje yra matuojamas kibernetinio saugumo brandos modelių efektyvumas. Organizacijoje, kurioje modelis vis dar yra diegiamas, savo atsakymą papildo, kad „*Yra tam tikri veiklos rodikliai priklausomai nuo skirtingų apsaugos domenų, kategorijų, kontrolių“*. Kiti respondentai įvardijo jų atstovaujamų organizacijų praktikas: „*Sėkmingas vidinis ir išorinis auditas*“; „*Efektyvumas matuojamas naudojant dokumentais pagrįstą kontrolės sistemą, kurioje aprašomi kontrolės reikalavimai, rizika ir minimalus numatomas įgyvendinimas. Vertinama pagal 2 gynybos liniją su saugumo galimybėmis, apibrėžtomis sistemoje per 3 metų ciklą. Naudojamas Gebėjimų brandos vertinimo modelis (CMMI) siekiant įvertinti brandą ir neatitikimus (pvz., vidaus taisyklėms), jie registruojami ir antroji linija susisiekia su rizikos / kontrolės savininku. Be to, 3 gynybos linija (auditas) atlieka rizika pagrįstus auditus visoje organizacijoje ir periodiniai išoriniai auditai atliekami ištisus metus*“; „*Yra 3 metų vertinimo programa, pagal kurią nepriklausomi vertintojai tikrina esamą brandą.*“; „*Aukštas. Sugebėjimu atsilaikyti prieš atakas*.“

Valstybinė: respondentas nurodė: „*Incidentų kiekis. Kibernetinio saugumo situacijos suvokimas tarp organizacijos narių*“.

Taigi viena organizacija kibernetinio saugumo brandos modelio efektyvumą matuoja pagal veiklos rodiklius ir kontroles, viena organizacija pažymi vidinį ir išorinį auditą, dvi organizacijos pabrėžia incidentų kiekį ir gebėjimą atsilaikyti prieš atakas, ir dvi organizacijos vertina efektyvumą pagal 3 metų vertinimo programą. Kiekviena organizacija turi savo unikalų požiūrį į kibernetinio saugumo brandos organizacijose vertinimo modelių efektyvumą, svarbiausia, kad visos organizacijos siekia to pačio tikslo – apsaugoti savo turimą informaciją ir atitikti esamus bei nuolat besikeičiančius kibernetinio saugumo iššūkius.

Kitas, septintasis klausimas prašė pasidalinti respondentų apie kibernetinio saugumo modelio integravimą į organizacijos saugumo procesus ir sistemas.

Vidutinė: „*Nėra*“.

Didelė: Visi respondentai, atstovaujantys dideles organizacijas į šį klausimą atsakė teigiamai, kai kurie pridurdami, apie pilną integravimą, sėkmingą įgyvendinimą, pritaikymą pagal poreikius

Valstybinė: „*Procesai keičiami atsižvelgiant į poreikį*“.

Šio klausimo atsakymai leidžia daryti išvadą, kad didelės organizacijos savo veikloje besivadovaujančios ISO 27001 ir NIST modeliais, atitinkamai reaguoja į vykstančius pokyčius ir pagal tai atnaujina savo esamus saugumo procesus ir sistemas, siekiant nenukrypti nuo organizacijos strategijose įgyvendintų informacijos saugumo tikslų.

Aštuntasis klausimas pateiktas apie organizacijos darbuotojus, jų supratimą apie kibernetinio saugumo brandos modelius, įsitraukimas, elgesį bei požiūrį į kibernetinį saugumą.

Vidutinė: Respondentas, atstovaujantis vidutinę organizaciją, kurioje nėra įgyvendintų kibernetinio saugumo brandos modelių nurodo, kad darbuotojų suvokimas apie kibernetinį saugumą yra: „*Žemas. Kai kurie žmonės yra apgauti per kai kurias sukčiavimo atakas*“.

Didelė: respondentų, atstovaujančių dideles organizacijas, atsakymai: „*Tai keičiasi kiekvieną dieną ir visi nauji dalykai*“; „*Visi darbuotojai reguliariai lanko privalomus kibernetinio saugumo informuotumo mokymus*“; „*Tai galima išmatuoti tik ribotai ir apima subjektyvumo lygį, jei žiūrėsime į visą įmonę. Jei pažvelgtume tik į turimą informaciją, pvz., sukčiavimo simuliacijas, praneštus saugumo incidentus ir reagavimo į incidentus laiką ir t. t. Informuotumas ir įsitraukimas per pastaruosius porą metų labai išaugo, bet ne ten, kur norime.“*; „*Darbuotojai turi žinoti, ko tikimasi siekiant apsaugoti įmonės informaciją, ir apie*

tai pranešama pasitelkiant politiką, procedūras, el. mokymus ir kt.“; „*Lengvabūdiškas.*“; „*Brandos modelio supratimas skiriasi priklausomai nuo darbuotojų departamento*“.

Valstybinė: „*Geras suvokimas, kuris pastoviai didinamas atliekant incidentų imitavimo pratybas*“.

Didžiausias kontrastas matomas tarp vidutinės organizacijos, kurioje nėra įdiegto kibernetinio saugumo brandos modelio ir valstybinės didelės organizacijos, kuri savo veikloje vadovaujasi ISO 27001 ir NIST modeliais, kur darbuotojų suvokimas yra geras. Vienintelis respondentas, atstovaujantis valstybinę organizaciją ir pabrėžė gerą darbuotojų suvokimą. Nei vienas kitas respondentas, atstovaujantis didelę organizacija, taip pozityviai neįvardijo darbuotojų suvokimo apie kibernetinį saugumą. Vienoje organizacijoje nurodoma, kad supratimas skiriasi priklausomai nuo darbuotojo departamento, tad tikėtina, kad su informacijos saugumu dirbantys suvokia geriau, nei kituose departamentuose. Du respondentai išliko labiau neutralūs įvardindami priemones, kurias naudoja darbuotojų mokymams: „v*isi darbuotojai reguliariai lanko privalomus mokymus“* ir „*apie tai pranešama pasitelkiant politiką, procedūras, el. mokymus ir kt.*“. Tačiau reguliarus mokymų lankymas ar pranešimai darbuotojams apie informacinį saugumą per politikas, procedūras ar mokymus gali ir dažnai net nepasiekia bei nepadidina darbuotojo suvokimo praktiškai matant jų veiksmus organizacijoje. Rodikliai, kuriuos mini vienas didelės organizacijos respondentas, tokie kaip *sukčiavimo simuliacijos, pranešti saugumo incidentai ir reagavimo į incidentus laikas* geriausiai apibūdina darbuotojų suvokimą apie kibernetinį saugumą, o valstybinės didelės organizacijos respondento atsakymas pateikia geriausią būdą kelti darbuotojų suvokimą: *atlikti incidentų imitavimo pratybas*.

Devintasis klausimas buvo nukreiptas į nuolatinį kibernetinio saugumo tobulinimą organizacijoje.

Vidutinė: organizaciją atstovaujanti respondentas nurodė, kad vyksta „Periodiniai mokymai, skirti informuoti apie kibernetinį saugumą socialinės inžinerijos požiūriu.“.

Didelė: 5 iš 6 respondentų, atstovaujančių dideles organizacijas, į šį klausimą atsakė teigiamai: „*Aktyvi CISO valdyba iš kiekvienos šalies rengia reguliarius posėdžius, kuriuose aptaria dalykus, kuriuos galima tobulinti*; „*Siekiame nuolat gerinti savo bendrą saugumo padėtį įvairiais procesais, tokiais kaip rizikos valdymo programa, incidentų tinklo valdymas ir daug daugiau*“; „*Bendradarbiavimas su kitomis organizacijomis ir saugumo specialistais, investavimas į technologijas, darbuotojų mokymai, reguliarus auditas ir vertinimai*.“; „*Šis procesas vyksta nuolat*“; „*Taip*“. Išsiskiria vieno respondento atsakymas, kuris teigia, kad „*Sakyčiau, tai kitas žingsnis*“.

Valstybinė: „*Nuolat tobulinama*“.

Nuolatinis tobulinimas, kuris yra sudedamoji tiek ISO 27001, tiek NIST modelių dalis yra įgyvendinamas respondentų atstovaujamose organizacijose. Nustebino vienos didelės organizacijos, kuri yra įsidiegusi kibernetinio saugumo brandos modelius, respondento atsakymas kad „*Tai kitas žingsnis*“. Tad preziumuojama, kad šioje organizacijoje itin sudėtinga pastebėti realiai vykstančius nuolatinio tobulinimo procesus, arba jie vyksta tik formaliai, atnaujinant dokumentus, tačiau pratiškai nematomi. Vidutinės organizacijos atstovas teigia, kad vyksta periodiniai mokymai apie socialinę inžineriją. Organizacijoje, kurioje kibernetinio saugumo branda yra žema, nėra įgyvendintų kibernetinio saugumo brandos vertinimo modelių, vykstantys periodiniai mokymai, jau yra vertinama, kaip organizacijoje vykstantis tobulinimas. Tuo tarpu kitose organizacijose, kurios turi įsidiegusios tiek ISO 27001, tiek NIST modelius, tiek didelėse, tiek valstybinėje didelėje organizacijoje, nuolatinis tobulinimas yra nuolat vykstantis procesas .

Dešimtuoju klausimu buvo siekiama sužinoti ekspertų nuomonę apie didžiausius iššūkius išlaikant kibernetinio saugumo brandos modelį organizacijoje.

Vidutinė: „*Nėra*“.

Didelė: Respondentai dalijasi savo patirtimis: iššūkis „*Buvo atnaujinti, žinoti kiekvieną sistemą ir rasti kiekvienos problemos sprendimą*“, „"*Kibernetinio saugumo brandos modelis, stabdė verslą diegti naujus sprendimus ar produktus*.“; „*Didžiausios problemos yra įvairių veiklos funkcijų pajėgumai ir tinkamos informacijos pozicijos išlaikymas daugiau nei 20 šalių ir sudėtingas pasaulinis veiklos modelis. Tinklų kūrimas, žinojimas, su kuo kalbėtis ir užtikrinti, kad esame informacijos grandinėje, yra didžiausias dalykas. [..].*“; „*Manau, kad pirmiausia svarbu apibrėžti numatomą brandos lygį ir užtikrinti, kad visi verslo subjektai būtų tokio paties lygio. Tada kaip kitą žingsnį reikėtų apibrėžti, ar tas lygis yra tikslinis, ar jį reikėtų padidinti. Tai turėtų kilti iš kibernetinio saugumo strategijos.*“; „*Darbuotojų aplaidumas*.“; „*Gera komunikacija, manau, yra svarbiausias iššūkis norint įdiegti ar išlaikyti kibernetinio saugumo brandą*.“.

Valstybinė: „*Pastovus personalo mokymas ir budrumo tikrinimas*“.

Išskirtini iššūkiai, su kuriais susidūrė didelės organizacijos diegdamos kibernetinio saugumo brandos modelius: atnaujinti ir žinoti kiekvieną sistemą ir problemų sprendimus, dėl diegiamo modelio verslas sustabdė naujas veiklas, tinklų kūrimas ir komunikacija, kibernetinio saugumo strategijos laikymasis visiems įtrauktiems verslo subjektams, darbuotojų aplaidumas, komunikacijos nebuvimas, personalo mokymai. Siekiant organizacijoje įgyvendinti kibernetinio saugumo brandos vertinimo modelius, organizacijos turi būti pasiruošusios iššūkiams ir pagal kiekvieną modelio standarto reikalavimą, užtikrinti, kad bus kas, kaip ir kada jį vykdo. Du respondentai pažymi darbuotojus, jų aplaidumą ir mokymus. Tad

organizacijos, siekiančios įsidiegti kibernetinio saugumo brandos vertinimo modelį, turi būti pasiruošusios ne tik atnaujinti organizacijos dokumentaciją, politikas ar instrukcijas, aprūpinti organizaciją reikalinga technika ir programomis, o kartu ir informuoti bei apmokyti visus darbuotojus.

Vienuoliktuoju klausimu buvo kreipiamasi į respondentus sužinoti kas, jų nuomone, geriausiai apibūdina kibernetinio saugumo brandos modelio efektyvumą organizacijoje.

Vidutinė: „*Nėra*“.

Didelė: respondentai, atstovaujantys dideles organizacijas, atsakant į šį klausimą pateikė savo nuomones: „*Įrankiai ir žmonės*“; „*Kibernetinio saugumo brandos modelio efektyvumą organizacijoje geriausiai gali apibūdinti jos gebėjimas visapusiškai įvertinti organizacijos kibernetinio saugumo laikyseną, nustatyti stipriąsias ir silpnąsias puses, prioritetus skirti patobulinimams ir nukreipti organizaciją į aukštesnį atsparumo kibernetinėms grėsmėms lygį. [..] Apskritai kibernetinio saugumo brandos modelio veiksmingumas slypi jo gebėjime nuolat tobulėti ir būti atspariems kibernetinėms grėsmėms, derinant su organizacijos bendrais verslo tikslais ir rizikos tolerancija.*“; „*Įdiegtas brandos modelis, kaip mūsų visos grupės valdymo modelio dalis, leidžia mums geriau suprasti mūsų dabartinę brandą tiek kaip pasaulinei organizacijai, tiek atskiruose padaliniuose, tačiau taip pat leidžia taikyti nuoseklų metodą gerinimui laikui bėgant įvertinti. Tai leidžia vyresniajai vadovybei priimti rizika pagrįstus sprendimus ir atitinkamai paskirstyti išteklius.*“; „*Kiekviena organizacija turi sukurti savo apibrėžimą. Tai gali būti priemonės kritinėse srityse, pvz., incidentų skaičius, incidentų sunkumas, atitiktis pagrindų sistemai arba sertifikavimas pagal standartus, pvz., ISO.*“; „*Sugebėjimas apsaugoti duomenis, sistemas ir tinklus nuo kibernetinių atakų*“; „*Vadovų (aukštesniųjų) požiūris į investicijas šiuo klausimu.*“.

Valstybinė: „*Incidentų kiekio mažėjimas ir vartotojų pranešimų apie neaiškias situacijas didėjimas*.“

Pagal respondentų išreikštą nuomonę atsakant į šį klausimą, išskirtini požymiai geriausiai apibūdinantys kibernetinio saugumo brandos modelio efektyvumą organizacijoje: įrankiai ir žmonės, gebėjimas nuolat tobulėti ir būti atspariai, išteklių kibernetiniam saugumo brandos modeliui skyrimas, incidentų skaičius ir sunkumas, atitiktis standartams, sugebėjimas apsisaugoti nuo kibernetinių atakų, investicijos į kibernetinio saugumo brandos modelį, incidentų kiekio mažėjimas, vartotojų pranešimų didėjimas. Šie, pagal kiekvieno respondento nuomonę ir patirtį išskirti požymiai tik parodo, kokios skirtingos yra organizacijos, skirtingas požiūris ir strategija, bei kokia skirtinga kiekvienos organizacijos branda. Atsparumas kibernetinėms grėsmės, incidentų skaičius ir investicijų skyrimas kibernetiniam saugumui buvo įvardinti net po 2 kartus, tad šie efektyvumo požymiai geriausiai apibūdina organizacijos pasiryžimą ir gebėjimą efektyviai reaguoti į kibernetines grėsmes.

Paskutiniuoju, dvyliktu klausimu buvo siekiama sužinoti, kokie, respondentų nuomone, yra geriausi būdai išmatuoti kibernetinio saugumo brandos modelio efektyvumą organizacijoje.

Vidutinė: „*Naudojant gerai įgyvendintą standartizavimą / normalizavimą (pvz., ISO, SOC, PCI DSS...)*“.

Didelė: „*Vertinimas, testavimas*“; „*Kibernetinio saugumo brandos modelio veiksmingumo vertinimas organizacijoje yra labai svarbus siekiant užtikrinti, kad kibernetinio saugumo praktika laikui bėgant tobulėtų ir tinkamai reaguotų į riziką. Taikydamos spragų analizės, reagavimo į incidentus testavimo, saugumo supratimo ir mokymo vertinimo, atitikties audito, tiekėjų ir trečiųjų šalių vertinimo, nuolatinio tobulinimo, kaštų ir naudos analizės metodus, organizacijos gali efektyviai įvertinti savo kibernetinio saugumo brandos modelio efektyvumą ir priimti pagrįstus sprendimus, kad laikui bėgant pagerintų savo saugumą.*“; „*Sukurti aiškią, skaidrią ir dokumentais pagrįstą kontrolės sistemą, kurioje būtų aprašomi lūkesčiai, pagrindiniai reikalavimai (įskaitant numatomą brandos lygį), neatitikties rizika ir periodiškai, bet nuosekliai įvertinama renkant informaciją ir imant atranką (jei įmanoma ir taikoma). Kontrolės ir (arba) rizikos savininkai turi suprasti lūkesčius ir atsakomybę, tačiau taip pat turėtų sugebėti įrodyti, kad šiame kontekste taikomas „pasitikėk, bet tikrink“.*“; „*Geriausias būdas įvertinti yra auditas arba saugos įvertinimas, bet taip pat priemones galima apibrėžti kaip KPI ir KRI, kuriuos reikia stebėti kasdien.*“; „*Auditas, testavimai, ataskaitos ir vertinimai.*“; „*Reikia turėti aiškias procesų kontroles kurioms butu nustatyti aiškūs reikalavimai ir taip butu išmatuojamas kiekvienos kontrolės efektyvumas. Taip butu galima nustatyti bendrą saugumo vaizdą organizacijoje.*“.

Valstybinė: „*Nuolatinis incidentų imitavimas ir situacijų vertinimas.*“

Vidutinę organizaciją, kuri neturi įsidiegusi kibernetinio saugumo brandos modelio, atstovaujantis respondentas, atsakydamas į šį klausimą nurodo, kad „*Naudojant gerai įgyvendintą standartizavimą / normalizavimą (pvz., ISO, SOC, PCI DSS...)“* yra geriausias būdas išmatuoti kibernetinio saugumo brandos modelio efektyvumą organizacijoje. Tačiau didelės organizacijos, kurios savo veikloje vadovaujasi įdiegtais kibernetinio saugumo brandos modeliais, pateikia atsakymus nurodydamos konkrečius veiksmus, kuriais remiantis organizacijose yra matuojamas kibernetinio saugumo efektyvumas: *vertinimas, testavimas*“, „*veiksmingumo vertinimas“*, „*kontrolės sistema ir vertinimas pagal ją*“, „*auditas arba vertinimas*“, „*auditas*“, „*testavimai ir vertinimai*“, „*kontrolės*“. Dideles organizacijas atstovaujančių respondentų nuomone, nuolatinis vertinimas, testavimas ir kontrolės yra geriausias būdas išmatuoti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumą. Valstybinę organizaciją atstovaujantis respondentas nurodė nuolatinį incidentų imitavimą, kuris nukreiptas į visus darbuotojus ir darbuotojų

žinojimą kaip reaguoti į kibernetines grėsmes. Vadinasi, organizacijos, kurios nori sužinoti ar įsivertinti kibernetinio saugumo brandos modelio efektyvumą, turi pasidaryti vertinimą/auditą, kaip veikia organizacijoje įtvirtinti dokumentai, politikos, ar nustatyti procesai ir procedūros atitinka reikalavimus, ar jie veikia efektyviai ir pasiekia nustatytus tikslus bei atitinka organizacijos kibernetinio saugumo strategiją.

Vienas respondentas atsakydamas į paskutinį klausimą pridėjo pastabą anketai: „*Nelabai aišku ką norit paklausti. Trūksta konteksto. Siūlyčiau tobulinti. Labai abstraktūs klausimai.“* Abstraktūs klausimai buvo pasirinkti tikslingai, siekiant leisti respondentams pilnai išreikšti savo nuomonę ir, kiek įmanoma, atskleisti jų atstovaujamų organizacijų spragas, pasidalinti sėkmėmis bei iššūkiais.

Šiame tyrime buvo nagrinėjami klausimai, kurie papildė atvejo analizę organizacijoje ir leido pažvelgti į įvairių organizacijų kibernetinio saugumo brandos modelių įgyvendinimą. Atsakymų analizė parodė, kad priklausomai nuo organizacijos dydžio ir pobūdžio, labai skiriasi ir jose įgyvendinami procesai, susiję su kibernetiniu saugumu. Vidutinė organizacija, kuri savo veikloje nesivadovauja kibernetinio saugumo brandos modeliais, yra žemos brandos, darbuotojai yra apgaunami per sukčiavimo atakas, todėl visai organizacijai kyla grėsmė patirti vis daugiau atakų ir prarasti jiems svarbią informaciją. Net mokymai apie socialinę inžineriją tokioje organizacijoje vertinami kaip organizacijos tobulėjimas. Respondentų, atstovaujančių dideles organizacijas, ir kurios yra įsidiegusios kibernetinio saugumo modelius, buvo daugiausia, tačiau atsakymų analizė atskleidė, kokios skirtingos yra organizacijos, ne tik pasirinkdamos strategijas, tačiau ir įvairias kibernetinio saugumo priemones bei efektyvumo matavimo būdus. Didelės organizacijos patiria įvairių iššūkių tiek įdiegdamos, tiek stengdamos išlaikyti kibernetinio saugumo brandos vertinimo modelius. Diegiant kibernetinio saugumo brandos vertinimo modelius organizacijose, sunkiausia yra pakeisti ne tik darbuotojų nuomonę, tačiau ir vadovybės, nes diegimas stabdo verslą ir reikalauja nemažai investicijų, o kartu dar kontrolių įgyvendinimas, jų priežiūra ir valdymas. Taip pat organizacijos susiduria su iššūkiais išlaikyti kibernetinio saugumo brandos vertinimo modelį organizacijoje: sistemų atnaujinimas ir problemų sprendimas, tinklų kūrimas ir komunikacija, dėl diegiamo modelio sustabdytos verslo veiklos, kibernetinio saugumo strategijos laikymasis, darbuotojų aplaidumas. Kibernetinio saugumo brandos modeliai apima ne kažkurią organizacijos dalį, tačiau visą, nuo vadovybės iki darbuotojo, įtraukiant visus dokumentus, procesus ir instrukcijas, tad ir iššūkiai paliečia kiekvieną darbuotoją. Valstybinė didelė organizacija pateikė aukštos kibernetinio saugumo brandos pavyzdį, kur nuolatinis incidentų imitavimas bei situacijų simuliavimas daromas siekiant apmokyti darbuotojus, o kibernetinio saugumo brandos modelio efektyvumą rodo incidentų kiekio mažėjimas ir vartotojų pranešimų apie neaiškias situacijas didėjimas. Vienintelė valstybinė organizacija, pateikiant atsakymą apie darbuotojų mokymus ir įsitraukimą, atsakė teigiamai apie darbuotojų gerą suvokimą, tuo tarpu kitos didelės

organizacijos susiduria su iššūkiais keliant darbuotojų supratimą apie kibernetinio saugumą. Didelėse organizacijose, kuo daugiau, dažniau ir taikant įvairius metodus darbuotojai yra supažindinami su informacijos saugumo reikalavimais, tuo labiau išauga organizacijoje informuotumas. Valstybinėje organizacijoje yra atliekamos incidentų imitavimo pratybos, tad darbuotojų mokymui ir švietimui yra parinktas kitoks metodas, kuris veikia ir organizacija gali teigti tiek apie aukštą kibernetinio saugumo brandą, tiek apie gerą darbuotojų suvokimą apie kibernetinį saugumą. Tyrimas taip pat parodė, kad organizacijos, kurios įsidiegusios kibernetinio saugumo brandos modelius, nuolat reaguoja į vykstančius pokyčius ir pagal tai atnaujina organizacijų saugumo gaires, procesus ir sistemas bei nuolatinis tobulinimas yra nuolat vykstantis procesas. Šis tyrimas kartu atskleidė, kad organizacijoms rūpi ir kibernetinio saugumo brandos organizacijoje vertinimo modelio efektyvumas ir jo matavimas. Skirtingos organizacijos taiko skirtingus metodus efektyvumo matavimui, tačiau organizacijos dažniausiai naudoja: veiklos rodiklius ir kontroles, vidinius ir išorinius auditus, pagal incidentų kiekį ir gebėjimą atsilaikyti prieš atakas, ir pagal sudarytą 3 metų vertinimo programą. Svarbiausia, kad organizacijos matuoja, seka veiklos rodiklių, kontrolių ir incidentų dėsningumus, planuoja auditus ar sudaro vertinimo programas. Šie veiksmai patvirtina organizacijų kibernetinio saugumo brandą ir kibernetinio saugumo brandos modelių pozityvų poveikį. Atsparumas kibernetinėms grėsmėms, incidentų skaičius ir investicijų skyrimas kibernetiniam saugumui yra respondentų įvardinti kaip geriausiai apibūdinantys kibernetinio saugumo brandos organizacijoje vertinimo efektyvumo požymiai, o nuolatinis vertinimas, testavimas ir kontrolės yra geriausias būdas išmatuoti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumą didelėse organizacijose. Organizacijos įvairiais būdais vertina kibernetinio saugumo brandos modelius ir jų efektyvumą, o svarbiausias aspektas, kad visos organizacijos siekia apsaugoti jų svarbią informaciją ir tapti atspariomis prieš besikeičiančias kibernetines grėsmes.

3.3 TEORINĖS IR EMPIRINĖS DALIES LYGINAMOJI GAUTŲ DUOMENŲ ANALIZĖ IR KRITINIS VERTINIMAS.

Kibernetinio saugumo brandos vertinimo modeliai organizacijose įpareigoja organizacijas laikytis nustatytų reikalavimų, padeda nuolat tobulėti ir prisitaikyti prie besikeičiančių kibernetinių grėsmių. Organizacijos dydis tampa nereikšmingas su besikeičiančiomis technologijomis bei nuolat tobulėjančiomis kibernetinėmis grėsmėmis. Svarbiausiu tampa efektyvus kibernetinio saugumo brandos organizacijoje vertinimo modelis, apimantis visų organizacijos darbuotojų, procesų ir procedūrų įsitraukimą, keliant organizacijos kibernetinio saugumo kultūrą ir padedant jai pasiekti atsparumą kibernetinėms grėsmėms.

Šio darbo tikslas buvo išsiaiškinti ar kibernetinio saugumo brandos organizacijoje modeliai yra efektyvūs ir užtikrina organizacijų kibernetinį atsparumą. Kibernetinio saugumo brandos organizacijoje vertinimo modelio efektyvumas tai – organizacija atspari kibernetinėms grėsmėms, o modelis yra dinamiškas ir veikia atsižvelgiant į vykstančius nuolatinius socialinius bei technologinius pokyčius; tai modelis, kuris yra įgyvendinamas ir vykdomas – jo pagrindu nustatytos taisyklės taikomos kasdieninėje veikloje; tai modelio praktinis veiksmingumas – nuolatinis žmonių, dokumentacijos ir procesų stebėjimas, kaip organizacijos taisyklės yra realiai įgyvendinamos ir analizuojama, ar kibernetinio saugumo brandos organizacijoje vertinimo modelis prisideda prie organizacijos kibernetinio saugumo stiprinimo.

Tiek ISO 27001, tiek NIST kaip kibernetinio saugumo brandos organizacijoje vertinimo modeliai padeda pasiekti norimus kibernetinio saugumo brandos tikslus ir įgyvendinti organizacijų kibernetinio saugumo strategijas. ISO 27001 ir NIST modeliai tarpusavyje skiriasi, kad ISO 27001 numato privalomą dokumentaciją, sertifikavimą, skiriasi šių modelių apimtis ir prieinamumas, o taip pat kaina ir įgyvendinimo sudėtingumas. Norint pasiekti aukštesnį kibernetinio saugumo brandos lygį organizacijoje, rekomenduojama įsidiegti abu šiuos modelius kaip vienas kitą papildančius.

Atliktas tyrimas, apimantis atvejo analizę ir ekspertinį pusiau struktūrinį interviu, atskleidė, kad situacija organizacijose, kurios yra įsidiegusios ISO 27001 ar NIST, ar abu šiuos kibernetinio saugumo brandos organizacijoje vertinimo modelius, nėra tokia pozityvi. Įdiegti kibernetinio saugumo brandos organizacijoje vertinimo modeliai nepasiekia nustatytų organizacijų kibernetinio saugumo strategijų tikslų ir nėra efektyvūs. Atvejo analizė organizacijoje UAB „XXX“, kuri yra įsidiegusi tiek ISO 27001, tiek NIST modelį, parodė, kad net ir abu įdiegti modeliai nėra efektyvūs, organizacija išlieka pažeidžiama ir nėra pasiekiamas norimas kibernetinis atsparumas. UAB „XXX“ kibernetinio saugumo brandos modeliai yra prisimenami tik prieš auditus (vidinius ir ISO 27001 išorinį), ir tampa didžiuliu papildomu darbo krūviu darbuotojams. Dėl vykusios darbuotojų kaitos UAB „XXX“ bei kompetencijų trūkumo, buvo kuo greičiau ir minimaliausiomis pastangomis stengiamasi užpildyti esančias spragas. Tyrimo metu analizuoti efektyvumo kriterijai parodė, kad UAB „XXX“ yra organizacija, kuri priėmusi visą reikiamą dokumentaciją, apsirūpinusi pažangiais technologiniais saugumo sprendimais, tačiau analizuojant giliau, yra randama labai daug neatitikčių. Ir nors dokumentacija, procesai ir procedūros daugeliu atveju atitinka vidinių ir išorinių audito reikalavimus, jais vadovaujasi tik darbuotojai, kurie dirba su atitiktimi ir informacijos saugumu, o kiti darbuotojai visai nesilaiko esančių kibernetinio saugumo reikalavimų ir kitų organizacijos taisyklių. Tai rodo, kad UAB „XXX“ formaliai atitinka visus kibernetinio saugumo brandos organizacijoje vertinimo modelių reikalavimus, tačiau praktiškai jie nėra efektyvūs. Atvejo analizė atskleidė, kad kibernetinio saugumo branda prasideda nuo kibernetinio saugumo kultūros kėlimo ir

skleidimo darbuotojams, nes kibernetinio saugumo organizacijoje užtikrinimas yra kiekvieno darbuotojo atsakomybė.

Pusiau struktūrinis interviu įtraukė 8 su informacijos saugumu dirbančius ekspertus įvairiose organizacijose, kurie pasidalino savo patirtimis ir nuomonėmis. Interviu atsakymai papildo ir patvirtina tyrimo duomenis kibernetinio saugumo brandos organizacijoje vertinimo modelių ir jų efektyvumo kontekste. Interviu atsakymai leido daryti išvadas, kad priklausomai nuo organizacijos dydžio ir pobūdžio, jose taikomi skirtingi kibernetinio saugumo sprendimai ir procesai. Pusiau struktūrinio interviu respondentai atstovavo vidutinę organizaciją neįsidiegusią kibernetinio saugumo brandos modelio (1), dideles (6) organizacijas, savo veikloje besivadovaujančiomis ISO 27001 ar/ir NIST modeliais ir valstybinę (1) didelę organizaciją, kuri, įsidiegusi ISO 27001 ir NIST modelius. Interviu atsakymai parodė, kad vidutinė organizacija yra žemos brandos, kur darbuotojai apgaunami per sukčiavimo atakas. Didelės organizacijos, kai kurios pasižyminčios aukštesne branda, kai kurios ne, įdiegdamos ir prižiūrėdamos kibernetinio saugumo brandos vertinimo modelius susiduria su iššūkiais, tokiais kaip: kibernetinio saugumo strategijos laikymasis, vadovybės nuomonės keitimas siekiant gauti investicijų organizacijos kibernetiniam saugumui, darbuotojų nuomonės keitimas, mokymai ir aplaidumas, o taip pat kontrolių įgyvendinimas, jų priežiūra ir valdymas, sistemų atnaujinimas ir problemų sprendimas, tinklų kūrimas ir komunikacija. Valstybinė organizacija nurodė, kad jos branda yra aukšta, darbuotojai gerai suvokia kibernetinio saugumo reikalavimus, nes yra apmokomi imituojant incidentus, o kibernetinio saugumo brandos modelio efektyvumą rodo incidentų kiekio mažėjimas ir vartotojų pranešimų apie neaiškias situacijas didėjimas. Kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumas, respondentų atsakymų duomenimis, yra matuojamas skirtingais metodais, tokiais kaip: veiklos rodikliai ir kontrolės, vidiniai ir išoriniai auditai, pagal incidentų kiekį ir gebėjimą atsilaikyti prieš kibernetines atakas, ir pagal sudarytą 3 metų vertinimo programą. Atsparumas kibernetinėms grėsmėms, incidentų skaičius ir investicijų skyrimas kibernetiniam saugumui yra respondentų įvardinti kaip geriausiai apibūdinantys kibernetinio saugumo brandos organizacijoje vertinimo efektyvumo požymiai, o nuolatinis vertinimas, testavimas ir kontrolės yra geriausias būdas išmatuoti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumą organizacijose.

Apibendrinant viso tyrimo rezultatus, kiekviena organizacija pasirenka jai priimtinus kibernetinio saugumo brandos modelius, jų įgyvendinimo principus ir efektyvumo matavimo kriterijus. Pusiau struktūrinio interviu atsakymų analizė patvirtino, kad kibernetinio saugumo brandos modelių diegimas organizacijoje yra sudėtingas procesas ir keliantis iššūkius tiek vadovybei, tiek specialistams, dirbantiems su modelio įgyvendinimu, tiek visiems organizacijos darbuotojams. Pagal respondentų atsakymus, kibernetinio saugumo brandos organizacijose vertinimo modeliai veikia, tačiau ne tiek, kiek jie to norėtų. Vienas negatyviausiai atsakytų klausimų apie darbuotojų mokymus organizacijose rodo, kad mokymai darbuotojams išlieka didžiausiu iššūkiu organizacijose, vadinasi kibernetinio saugumo kultūros skleidimas turėtų būti įvardijamas kaip vienu svarbiausiu kibernetinio saugumo strategijos tikslu.

Kibernetinio saugumo brandos vertinimo modeliai yra daugiau bendros gairės, kurios padeda organizacijoms struktūruotai ir sistemiškai parengti organizacijos kibernetinio saugumo dokumentaciją, pateikia praktiškai patikrintus reikalavimus organizacijų procesams ir procedūroms. Tačiau ar modeliai organizacijose bus efektyvūs, priklauso nuo juos prižiūrinčių darbuotojų bei visos organizacijų darbuotojų. Organizacijos, siekdamos pritraukti investuotojus dažnai nekreipia dėmesio į kibernetinio saugumo brandos vertinimo modelių efektyvumą, siekia kuo greičiau ir bent formaliai atitikti modelių keliamus reikalavimus, ir gauti sertifikatą. Tuo tarpu, kibernetinis saugumas, kuris susijęs su technologiniais sprendimais išlieka labiausiai pažeidžiamas per žmones, organizacijų darbuotojus, kurie valdo technologijas. Tinkamas darbuotojų mokymas, kibernetinio saugumo kultūros palaikymas organizacijose gali būti svarbiausiais veiksniais siekiant padidinti kibernetinio saugumo brandą organizacijose.

IŠVADOS IR REKOMENDACIJOS

Išvados:

1. Kibernetinio saugumo brandos organizacijoje vertinimo modeliai yra svarbūs organizacijų kibernetinio atsparumo pasiekimui, įpareigojantys organizacijas laikytis nustatytų reikalavimų ir padėdami organizacijoms struktūruotai bei sistemiškai pritaikyti saugumo reikalavimus organizacijų dokumentacijai, procesams ir procedūroms. Tačiau kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumas labiausiai priklauso tik nuo pačios organizacijos vadovybės požiūrio ir darbuotojų kibernetinio saugumo kultūros.
2. Ne visos organizacijos įsidiegusios kibernetinio saugumo brandos organizacijoje vertinimo modelius yra tikrai brandžios kibernetinio saugumo prasme, nes užtikrinama tik formali dokumentacijos, procesų ir procedūrų atitiktis, o darbuotojų elgesys prieštarauja organizacijos nustatytoms taisyklėms.
3. Kibernetinio saugumo brandos organizacijoje vertinimo modeliai ISO 27001:2013 ir NIST 1.1 (2018) padeda organizacijoms įgyvendinti kibernetinio saugumo reikalavimus, tapti atsparioms kibernetinėms grėsmėms ir pasiekti užsibrėžtus tikslus. Šie modeliai tarpusavyje skiriasi, kad ISO 27001 numato privalomą dokumentaciją, sertifikavimą, skiriasi šių modelių apimtis ir prieinamumas, o taip pat kaina ir įgyvendinimo sudėtingumas. Modelių analizė atskleidė, kad jie yra papildantys vienas kitą, todėl norint pasiekti aukštesnį kibernetinio saugumo brandos lygį organizacijoje, rekomenduojama įsidiegti abu šiuos modelius.
4. Kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumas matuojamas priklausomai nuo kiekvienos organizacijos pasirinktų vertinimo kriterijų. Šio darbo tyrimo rezultatai parodė, kad dažniausiai naudojami efektyvumo vertinimo kriterijai yra: veiklos rodikliai ir kontrolės, vidiniai ir išoriniai auditai, vertinimo programos, incidentų kiekis ir gebėjimas atsilaikyti prieš kibernetines atakas. Didžiausiu iššūkiu organizacijos įvardija tinkamą darbuotojų apmokymą ir jų sąmoningumo kėlimą.
5. Kibernetinio saugumo organizacijoje užtikrinimas yra kiekvieno darbuotojo atsakomybė, todėl ir kibernetinio saugumo kultūros kėlimas bei skleidimas yra viena esminių kibernetinio saugumo brandos organizacijoje kėlimo dalis. Todėl kibernetinio saugumo strategijose kibernetinio saugumo kultūros skleidimas turėtų būti įvardijamas kaip vienu svarbiausiu tikslu, o taip pat nuolat mokyti darbuotojus taikant įvairesnius metodus, pvz. simuliuojant situacijas, kelti darbuotojų sąmoningumą, kuo daugiau įtraukti ir skatinti dalyvauti kibernetinio saugumo procesuose.

Rekomendacijos:

1. Siekiant geriausių rezultatų įgyjant kibernetinį atsparumą, organizacijoms, nepaisant jų dydžio ir veiklos pobūdžio, rekomenduojama įsidiegti abu, tiek ISO 27001, tiek NIST kibernetinio saugumo brandos organizacijose vertinimo modelius. Šie modeliai papildo vienas kitą: ISO 27001 nukreipia į ISMS kūrimą, valdymą, dokumentaciją, o NIST padeda identifikuoti saugumo sritis ir sudaryti apsaugos priemones - taip užpildant vienas kito spragas sukuriamas itin aukštas organizacijos kibernetinis atsparumas.
2. Kadangi kibernetinis saugumas yra kiekvieno darbuotojo atsakomybė, o didžiausi iššūkiai organizacijose susiję darbuotojų mokymu į sąmoningumo skleidimu, rekomenduojama į organizacijos kibernetinio saugumo strategiją įtraukti kibernetinio saugumo kultūros kėlimą kaip vieną iš pagrindinių tikslų ir to sistemingai siekti, pvz. organizuojant reguliarius susitikimus įvykusiems kibernetiniams incidentams ir išmoktoms pamokoms aptarti.
3. Organizacijų vadovybėms rekomenduojama aktyviai rodyti kibernetinio sąmoningumo pavyzdį pvz. dalyvaujant kibernetinio saugumo mokymuose, pabrėžiant kibernetinio saugumo svarbą kasdieninėse užduotyse ar išsiunčiant pranešimą darbuotojams pažymint kibernetinio saugumo priemones.
4. Kibernetinio saugumo brandos organizacijose vertinimo modeliai numato darbuotojų mokymams kartotinumą, o tyrimas atskleidė, kad kuo įvairesni mokymų darbuotojams metodai, tuo geresnis darbuotojų suvokimas apie kibernetinį saugumą, todėl darbuotojų sąmoningumui kelti rekomenduojama pasitelkti įvairius metodus ir skirtingus formatus - nuo nuotolinių mokymų iki socialinės inžinerijos ir situacijų simuliavimo pratybų - jas vertinti, sekti jų rezultatus bei išmoktas pamokas
5. Įsidiegus kibernetinio saugumo brandos vertinimo modelius organizacijoje, rekomenduojama nusistatyti ir modelio efektyvumo vertinimo kriterijus. Be incidentų kiekio ir pobūdžio, kitų techninių kriterijų, organizacijoms rekomenduojama kibernetinio saugumo brandos modelių efektyvumą matuoti atsižvelgiant į žmogiškuosius kriterijus: kaip darbuotojai supranta ir taiko kibernetinio saugumo procedūras gali būti svarbiau nei formalūs techniniai vertinimo rodikliai, pavyzdžiui sekant darbuotojų sąmoningumą laikantis saugumo reikalavimų.

LITERATŪRA

1. Agafonov, K. (2021). *Kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti* (Daktaro disertacija, Mykolo Romerio universitetas). Prieiga: https://talpykla.elaba.lt/elaba-fedora/objects/elaba:108043004/datastreams/MAIN/content
2. Akinsanya, O. O., Papadaki, M., & Sun, L. (2019, March). *Current cybersecurity maturity models: How effective in healthcare cloud?*. In *CERC* (pp. 211-222). Prieiga: https://ceur-ws.org/Vol-2348/paper16.pdf
3. Alrehili, A. A., & Alhazmi, O. H. (2023, September). *ISO/IEC 27001 Standard: Analytical and Comparative Overview*. In International Conference on Advances in Data-driven Computing and Intelligent Systems (pp. 143-156). Singapore: Springer Nature Singapore. Prieiga: https://www.researchgate.net/publication/378486908_ISOIEC_27001_Standard_Analytical_and_Comparative_Overview
4. Alshar'e, M. (2023). *Cyber security framework selection: comparison of NIST and ISO27001*. Applied Computing Journal, 3(1), 245-255. https://doi.org/10.52098/acj.202364
5. Bendras komunikatas Europos Parlamentui ir Tarybai. *Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija*. Briuselis, 2020 12 16 JOIN(2020) 18 final. Prieiga: https://ec.europa.eu/newsroom/dae/redirection/document/72164
6. Blount, P. J. (2020). *CYA: Legal Perspective on How to Do Cybersecurity in Space*. Proceedings of the International Institute of Space Law, 63, 457-466. Prieiga: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=bsu&AN=174902925&site=ehost-live
7. Calder, A. (2009). *Information Security based on ISO 27001/ISO 27002*. Van Haren. Prieiga: https://www.google.lt/books/edition/Information_Security_based_on_ISO_27001/yhJADwAAQBAJ?hl=lt&gbpv=1
8. Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*. IT Governance Publishing Ltd. Prieiga: https://www.google.lt/books/edition/NIST_Cybersecurity_Framework_A_pocket_gu/rWxvDwAAQBAJ?hl=lt&gbpv=1&dq=NIST+Cybersecurity+Framework:+A+pocket+guide&printsec=frontcover
9. Chandler D. and Munday R. *A Dictionary of Social Media*. Oxford University Press. Published online: 2016. eISBN: 9780191803093. Prieiga: https://www.oxfordreference.com/

10. Chidukwani, A., Zander, S., and Koutsakis, P. (2022) "*A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations*," in IEEE Access, vol. 10, pp. 85701-85719, doi: 10.1109/ACCESS.2022.3197899. Prieiga: https://ieeexplore.ieee.org/abstract/document/9853515
11. Cichonski P., Millar T., Grance T., Scarfone K., *Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61, Revision 2, 2012. Prieiga: http://dx.doi.org/10.6028/NIST.SP.800-61r2
12. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*. TQM Journal, 33(7), p. 76-105. https://doi-org.skaitykla.mruni.eu/10.1108/TQM-09-2020-0202
13. De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). *COBIT as a Framework for Enterprise Governance of IT. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, 125-162. Prieiga: https://link.springer.com/chapter/10.1007/978-3-030-25918-1_5
14. *ENISA Nacionalinių pajėgumų vertinimo Sistema*. 2020 m. Prieiga: https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-lt.pdf
15. *ENISA Threat Landscape* 2022. Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
16. *ENISA Threat Landscape* 2023. Prieiga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
17. EUR-Lex žodynas. *Mažosios ir vidutinės įmonės*. Prieiga: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=LEGISSUM:sme
18. *Europos Komisijos 2003 m. gegužės 6 d. rekomendacija dėl labai mažų, mažų ir vidutinių įmonių apibrėžimo* 2003/361/EC. Prieiga: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361
19. Europos Parlamento ir Tarybos direktyva (ES) *2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti*. Prieiga: https://eur-lex.europa.eu/eli/dir/2022/2555
20. Fathurohman, A., & Witjaksono, R. W. (2020). *Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of*

Government of Bandung City). Bulletin of Computer Science and Electrical Engineering, 1(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

21. Ghelani, D. (2022). *Cyber security, cyber threats, implications and future perspectives: A Review*. Authorea Preprints. https://www.authorea.com/users/506161/articles/587239-cyber-security-cyber-threats-implications-and-future-perspectives-a-review
22. Gorka, Marek. (2022). *Cybersecurity culture in the public and private sector area in the Central European region.* Nowa Polityka Wschodnia, 2022(4), 51-71. Prieiga: https://czasopisma.marszalek.com.pl/images/pliki/npw/35/npw3503.pdf
23. Grimmick, R. (2022). *ISO 27001 compliance: Essential tips and insights*. Information & Records Management Society Bulletin, 229, 22–31. Prieiga: https://web-s-ebscohost-com.skaitykla.mruni.eu/ehost/pdfviewer/pdfviewer?vid=10&sid=54a0c0ae-ec31-4c75-b460-cd8270dd6870%40redis
24. Guest, G. & Bunce, A. & Johnson, L. (2006). *How Many Interviews Are Enough*?. Field Methods - Field Method. 18. 59-82. Prieiga: https://doi.org/10.1177/1525822X05279903
25. Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). *A {Large-Scale} Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises*. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 1235-1252). Prieiga: https://www.usenix.org/conference/usenixsecurity21/presentation/huaman
26. Hudson D., Macallister J., Pote M., *A Guide to Assessing Security Maturity*. Carbon black. White paper. 2019. Prieiga: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-a-guide-to-assessing-security-maturity.pdf
27. Yassine Maleh, Abdelkebir Sahid & Mustapha Belaissaoui (2021) *A maturity framework for cybersecurity governance in organizations*, EDPACS, 63:6, 1-22, https://doi.org/10.1080/07366981.2020.1815354
28. Ibrahimova, Aytakin Nazim. (2021). *Information security and influencing factors*. Law of Ukraine: Legal Journal (Ukrainian), 2021(11), 234-244. Prieiga: https://doi-org.skaitykla.mruni.eu/10.33498/louu-2021-11-234
29. *ISO/IEC 27001. Tarptautinis standartas*. ISO/IEC FDIS 27001:2013(E).
30. *ISO/IEC 27001. Tarptautinis standartas*. ISO/IEC FDIS 27001:2022(E)
31. *ISO/IEC 27002. Tarptautinis standartas*. ISO/IEC 27002:2022 (E).

32. Junaid, T. S.(2023). *ISO 27001: Information Security Management Systems*. DOI: 10.13140/RG.2.2.36267.52005. Prieiga: https://www.researchgate.net/publication/367166657
33. Koza, E. (2022). *Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security*. Med. Eng. Themes, 2, 26-39. Prieiga: https://themedicon.com/pdf/engineeringthemes/MCET-02-021.pdf
34. Kurii, Y., & Opirskyy, I. (2022). *Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013*. NIST Spec. Publ, 800(53), 10. Prieiga: https://ceur-ws.org/Vol-3288/paper3.pdf
35. Lawrence A Gordon, Martin P Loeb, Lei Zhou, *Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model*, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa005, https://doi.org/10.1093/cybsec/tyaa005
36. Le N. T., Hoang D. B., (2016). *Can maturity models support cyber security*?. IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 2016, pp. 1-7. Prieiga: https://doi.org/10.1109/PCCC.2016.7820663
37. Lietuvos Respublikos Seimas (2014). *Lietuvos Respublikos kibernetinio saugumo įstatymas*. (2014 m. Gruodžio 11 d., Nr. XII-1428) https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
38. Lietuvos Respublikos Vyriausybės Nacioanlinis Akreditacijos Biuras. *Dėl standarto ISO/IEC 27001:2022*. Prieiga: https://nab.lrv.lt/lt/naujienos/del-standarto-iso-iec-27001-2022-taikymo-atnaujinta-2023-02-27/
39. Mahn A., Marron J., Quinn S., Topper D. (2021) *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*. NIST Special Publication 1271. Prieiga: https://doi.org/10.6028/NIST.SP.1271
40. Marco Sartor, & Guido Orzes. (2019). *Quality Management : Tools, Methods and Standards*: Vol. First edition. Emerald Publishing Limited. Prieiga: https://doi.org/10.1108/978-1-78769-801-720191017
41. Möller, D.P.F. (2023). *Cybersecurity Maturity Models and SWOT Analysis. In: Guide to Cybersecurity in Digital Transformation*. Advances in Information Security, vol 103 . Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_7
42. Moskowitz D., Nichols D.M.(2022) *Fundamentals of Adopting the NIST Cybersecurity Framework*: Part of the Create, Protect, and Deliver Digital Business Value series. ISBN 9780117093706. Prieiga: https://books.google.com/books?id=HU7wzgEACAAJ&dq=Fundamentals+of+Adopting+the+NIST+

Cybersecurity+Framework&hl=lt&newbks=1&newbks_redir=1&sa=X&ved=2ahUKEwjZktW5yuCFAxVXQlUIHVSYAXUQ6AF6BAgFEAI

43. Murphy, G. (2022). *The Journey to ISO 27001 Certification*. Strategic Finance, 104(1), 62–63. Prieiga: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=bsu&AN=157583890&site=ehost-live
44. Nacionalinis Kibernetinio Saugumo Centras. *Nacionalinė kibernetinio saugumo būklės ataskaita 2022*. Prieiga: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf
45. National Institute of Standards and Technology (NIST 2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018. Prieiga: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
46. NIST (2020). *Approaches for Federal Agencies to use the Cybersecurity Framework*. NISTIR 8170. https://doi.org/10.6028/NIST.IR.8170
47. *NIST Releases Version 2.0 of Landmark Cybersecurity Framework*. Prieiga: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
48. Porch, A. M. (2020). *Spoiling for fight: hacking back with the Active Cyber Defense Certainty Act*. South Dakota Law Review, 65(3), 467-488. Prieiga: https://heinonline.org/HOL/P?h=hein.journals/sdlr65&i=525
49. Roy, P.P. (2020). *A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard*. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 1-3. Prieiga: https://doi.org/10.1109/NCETSTEA48365.2020.9119914
50. Schiavone, M., & Kirk, B. (2023). *Transitioning to ISO 27001:2022*. Pennsylvania CPA Journal, 94(2), 21. Prieiga: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=bsu&AN=164209796&site=ehost-live
51. Stallings W. (2019), *Effective Cybersecurity– Understanding and Using Standards and Best Practices*, Addison-Wesley, 2019, ISBN 013477292X, 9780134772929. Prieiga: https://books.google.lt/books/about/Effective_Cybersecurity.html?id=qBLFuQEACAAJ&redir_esc=y
52. Stewart, Dr. (2022). *Why ISO 27001 Certified Organizations Still Experience Data Leakage*?. Journal of Digital Information Management. 20. 90-103. Prieiga: http://dx.doi.org/10.6025/jdim/2022/20/3/90-103

53. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). *Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 AND PCI DSS.* JOIV: International Journal on Informatics Visualization, 4(4), 225-230. Prieiga: http://dx.doi.org/10.30630/joiv.4.4.482

54. Taherdoost H.(2022) *Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview*. Electronics.; 11(14):2181. https://doi.org/10.3390/electronics11142181

55. Taherdoost H.(2022). *Cybersecurity vs. Information Security*, Procedia Computer Science, Volume 215, Pages 483-487, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.050. Prieiga:https://www.sciencedirect.com/science/article/pii/S1877050922021214

56. Teufel, S., Teufel, B., Aldabbas, M., Nguyen, M. (2020). *Cyber Security Canvas for SMEs*. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Botha, R. (eds) Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science, vol 1339. Springer, Cham. https://doi.org/10.1007/978-3-030-66039-0_2

57. Ullah, B., & Nab, S. I. (2022). *Developing cyber security strategies for business organization to prevent data breaches*. KASBIT Business Journal, 15(4), 62. Prieiga: https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=bsu&AN=161417427&site=ehost-live

58. Vageris, R. *Rizikos analizės vadovas*, 2005. Prieiga: https://www.nksc.lt/doc/rizikos_analize.pdf

59. Valackienė, A. (2016). *Towards a framework for case study research: methodology and practical implementation*. In D. Žostautienė, D. Susnienė, L. Leišytė (Eds.). CISABE'2016 : 6th international conference on Changes in social and business environment, April 28-29, 2016, Panevėžys, Lithuania (pp. 65-70). MEDIMOND. Prieiga: https://www.lituanistika.lt/content/78308

60. Valstybės Kontrolė. *Kibernetinio saugumo užtikrinimas*. Valstybinio audito ataskaita, 2022, P. 13. Prieiga: https://www.valstybeskontrole.lt/LT/Product/Download/4371

61. *Verizon Data Breach Investigations Report* 2023. Prieiga: https://www.verizon.com/business/resources/reports/dbir/

62. *World Economic Forum: The global risks report 2020* (2020). Prieiga: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

63. Zammani, M., Razali, R., & Singh, D. (2021). *Organizational information security management maturity model*. International Journal of Advanced Computer Science and Applications, 12(9). Prieiga: http://dx.doi.org/10.14569/IJACSA.2021.0120974

Kupinė J. (2024). *Kibernetinio saugumo brandos organizacijoje vertinimo modelis* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Nuolat didėjant kibernetinių atakų skaičiui, kibernetinio saugumo brandos organizacijoje vertinimo modeliai tampa vis svarbesne priemone organizacijoms siekiant didinti kibernetinį atsparumą. Šio darbo pirmame skyriuje aptariama kibernetinio saugumo brandos organzacijose vertinimo modelių svarba, bei mažų, vidutinių ir didelių, daugiau ir mažiau brandžių organizacijų patiriamos kibernetinės atakos. Taip pat aptariami įvairūs kibernetinio saugumo brandos modeliai bei analizuojami populiariausi - ISO 27001 ir NIST - pateikiama jų išsami analizė bei palyginimas išryškinant kiekvieno privalumus, trūkumus, panašumus ir skirtumus. Antrasis skyrius skirtas tyrimo metodologijai, apibūdinant vykusio tyrimo detales. Trečiame skyriuje išsamiai aptarti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumo tyrimo rezultatai. Darbo pabaigoje ateiktos išvados ir rekomendacijos organizacijoms, kaip efektyviai įgyvendinti kibernetinio saugumo brandos organizacijoje vertinimo modelius.

Pagrindiniai žodžiai: kibernetinis saugumas, kibernetinio saugumo branda, organizacijų kibernetinis atsparumas, kibernetinio saugumo brandos modelis

Kupinė J. (2024). *Cyber security maturity assessment model in the organization* (master thesis). Vilnius: Mykolas Romeris University

ANNOTATION

As the number of cyber-attacks continues to increase, cyber security maturity assessment models in an organization are becoming an increasingly important tool for organizations to increase cyber resilience. The first chapter of this thesis discusses the importance of models for evaluating the maturity of cyber security in organizations, as well as the cyber attacks that are experienced by small, medium, and large, more and less mature organizations. It also discusses various cybersecurity maturity models and analyzes the most popular - ISO 27001 and NIST - their detailed analysis and comparison are provided, highlighting the advantages, disadvantages, similarities, and differences of each. The second chapter is dedicated to the research methodology, describing the details of the research that took place. The third chapter discusses in detail the results of the research on the effectiveness of the cyber security maturity assessment models in the organization. At the end of this paper, conclusions and recommendations for organizations on how to effectively implement cyber security maturity assessment models in the organization are presented.

Key words: cyber security, cyber security maturity, cyber resilience of organizations, cyber security maturity model

Kupinė J. (2024). *Kibernetinio saugumo brandos organizacijoje vertinimo modelis* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Nuolat didėjant kibernetinių atakų skaičiui, organizacijoms tampa svarbu įgyti kibernetinį atsparumą, tai ir kibernetinio saugumo brandos organizacijoje vertinimo modeliai tampa vis aktualesne priemone organizacijoms tapti atparioms nuolat besikeičiančioms kibernetinėms grėsmėms. Nors kibernetinio saugumo brandos organizacijose modelių svarba yra pripažįstama, yra svarbu išsiaiškinti modelių veikimo principus, jų pritaikymą ir realų įgyvendinimą, bei kaip jie gali padėti organizacijoms įgyti kibernetinį atsparumą. Šiame darbe iškelta mokslinė problema - išanalizuoti kibernetinio saugumo brandos vertinimo modelio efektyvumą organizacijoje ir brandos modelio praktinį veiksmingumą, nagrinėjant du pagrindinius ir plačiausiai naudojamus kibernetinio saugumo modelius ISO 27001 ir NIST. Šio darbo tyrimo tikslu įvardintas siekis įvertinti kibernetinio saugumo brandos organizacijoje modelius, jų efektyvumą bei įgyvendinimo aspektus analizuojant UAB „XXX" atvejį. Šiam tikslui pasiekti nustatyti tyrimo uždaviniai: išanalizuoti populiariausius kibernetinio saugumo brandos vertinimo modelius; konceptualizuoti kibernetinio saugumo brandos vertinimo modelių vertinimo kriterijus išryškinant jų tendencijas; ištirti kibernetinio saugumo brandos organizacijoje vertinimo modelių įgyvendinimo aspektus analizuojant UAB „XXX"; bei pateikti tyrimo metu gautas rekomendacijas organizacijoms kaip efektyviai įgyvendinti kibernetinio saugumo brandos organizacijoje vertinimo modelius. Tyrimui naudoti metodai: mokslinės literatūros sisteminimas, analizė, palyginimas; dokumentų analizė; atvejo analizė; kokybinio turinio analizė bei ekspertinis pusiau struktūruotas interviu. Tyrimo duomenų analizei naudoti metodai: kokybinė turinio analizė, atvejo studijos rezultatų analizė, pusiau struktūruoto interviu kokybinė turinio analizė ir interpretavimas bei lyginamoji gautų duomenų analizė.

Literatūros analizė išryškino kibernetinio saugumo brandos organizacijoje vertinimo modelių privalumus ir su jais didėjantį organizacijų kibernetinį atsparumą. Išsami populiariausių kibernetinio saugumo brandos organizacijoje vertinimo modelių analizė atskleidė, kad ISO 27001 ir NIST modeliai yra papildantys vienas kitą, todėl organizacijoms norinčioms geriausių rezultatų ir didesnio kibernetinio atsparumo, rekomenduojama įsidiegti abu modelius. Tačiau atvejo analizės tyrimas UAB „XXX" parodė, kad organizcija, formaliai atitinkanti kibernetinio saugumo modelių reikalavimus, nepasiekia modelių efektyvumo ir tai matyti iš darbuotojų aplaidaus elgesio. Todėl padaryta išvada, kad kibernetinio saugumo brandos organizacijoje vertinimo modelių efetyvumas priklauso visų pirmą nuo organizacijos požiūrio bei

visų darbuotojų kibernetinio sąmoningumo, o darbuotojų kibernetinio sąmoningumo ir kultūros kėlimas turėtų būti įtrauktas į organizacijų kibernetinio saugumo strategijas. Taip pat tyrimo metu nustatyti pagrindiniai kibernetinio saugumo brandos organizacijose vertinimo modelių efektyvumo matavimo kriterijai, ir be visų techninių veiklos rodiklių, taip pat rekomenduojama organizacijoms turėti veiklos rodiklius, matuojančius darbuotojų kibernetinį sąmoningumą. Tyrimo metu identifikavus organizacijų patiriamus iššūkius apmokant darbuotojus, rekomenduojama organizacijoms taikyti kuo įvairesnius kibernetinio saugumo mokymo metodus bei patikrinimus.

Magistro baigiamąjį darbo sudaro trys pagrindinės dalys: pirmojoje aptarta kibernetinio saugumo brandos organzacijose vertinimo modelių svarba, bei skirtingo dydžio ir brandos organizacijų patiriamos kibernetinės atakos. Taip pat aptarti įvairūs kibernetinio saugumo brandos modeliai bei išanalizuoti populiariausi - ISO 27001 ir NIST - pateikta jų išsami analizė bei palyginimas išryškinant kiekvieno privalumus, trūkumus, panašumus ir skirtumus. Antrasis skyrius skirtas tyrimo metodologijai, apibūdinant vykusio tyrimo detales. Trečiame skyriuje išsamiai aptarti kibernetinio saugumo brandos organizacijoje vertinimo modelių efektyvumo tyrimo UAB „XXX“ ir pusiau struktūruoto interviu rezultatai, jų analizė ir apibendrinimas. Magistrinio darbo pabaigoje pateiktos išvados ir rekomendacijos organizacijoms, kaip efektyviai įgyvendinti kibernetinio saugumo brandos organizacijoje vertinimo modelius.

Kupinė J. (2024). *Cyber security maturity assessment model in the organization* (master thesis). Vilnius: Mykolas Romeris University

SUMMARY

As the number of cyber-attacks continues to increase, it becomes more important for organizations to acquire cyber-resilience, that is why cyber security maturity assessment models in the organization are becoming an increasingly relevant tool for organizations to become resistant to ever-changing cyber threats. While the importance of cyber security maturity models in organizations is recognized, it is important to clarify the principles of operation of the models, their application and real-world implementation, and how they can help organizations acquire cyber resilience. The scientific problem raised in this master thesis is to analyze the effectiveness of the cyber security maturity assessment model in the organization and the practical effectiveness of the maturity model by examining the two main and most widely used cyber security models ISO 27001 and NIST. The goal of this study is to assess the maturity models of cyber security in the organization, their effectiveness, and implementation aspects by analyzing the case of JSC "XXX". To achieve this goal, the research tasks were set: to analyze the most popular cyber security maturity assessment models; conceptualize the evaluation criteria of cyber security maturity assessment models by highlighting their trends; to investigate the implementation aspects of cyber security maturity assessment models in the organization by analyzing JSC "XXX"; and present the recommendations obtained during the research to organizations on how to effectively implement cyber security maturity assessment models in the organization. Methods used for research: systematization, analysis, comparison of scientific literature; document analysis; case study; qualitative content analysis, and expert semi-structured interview. Methods used for research data analysis: qualitative content analysis, analysis of case study results, qualitative content analysis and interpretation of semi-structured interviews, and comparative analysis of the obtained data.

The literature analysis highlighted the advantages of the assessment models of cyber security maturity in the organization and with them the increasing cyber resilience of the organizations. A detailed analysis of the most popular cyber security maturity assessment models in the organization revealed that the ISO 27001 and NIST models are complementary to each other, so organizations that want the best results and greater cyber resilience are recommended to implement both models. However, the case study of JSC "XXX" showed that the organization, which formally meets the requirements of cyber security models, does not achieve the effectiveness of the models and this can be seen in the negligent behavior of employees. Therefore, it was concluded that the effectiveness of cyber security maturity assessment models in an

organization depends first of all on the organization's approach and the cyber awareness of all employees, and raising employees' cyber awareness and culture should be included in the organizations' cyber security strategies. Also, during the study, the main criteria for measuring the effectiveness of the evaluation models of cyber security maturity in organizations were determined, and in addition to all technical performance indicators, it is also recommended that organizations have performance indicators that measure employees' cyber awareness. During the research there were identified challenges faced by organizations in training employees, it is recommended that organizations apply as many different cyber security training methods and checks as possible.

The Master's thesis consists of three main parts: the first part discusses the importance of cyber security maturity assessment models in organizations, as well as the cyber attacks experienced by organizations of different sizes and maturity. Various cyber security maturity models are also discussed and the most popular - ISO 27001 and NIST - are analyzed - their detailed analysis and comparison is presented, highlighting the advantages, disadvantages, similarities and differences of each. The second chapter is dedicated to the research methodology, describing the details of the research that took place. In the third chapter, the results of the research on the effectiveness of cyber security maturity assessment models in the organization JSC "XXX" and the results of semi-structured interviews, their analysis and generalization are discussed in detail. At the end of the master's thesis, conclusions and recommendations for organizations are presented on how to effectively implement cyber security maturity assessment models in the organization.

1 PRIEDAS. Magistro baigiamojo darbo programa

II SEMESTRAS	III SEMESTRAS	IV SEMESTRAS
Magistrinio baigiamojo darbo plano, turinio, įvado parengimas bei mokslinės literatūros analizė.	Tikslinama teorinės ir metodologinės dalys. Tyrimo parengimas, jo analizė.	Teorinės, metodologinės bei analitinių dalių tikslinimas, išvadų, rekomendacijų ir kitų MBD sudėtinių dalių rengimas.
Parengti iki 2023-06-25	**Parengti iki 2024-01-28**	**Parengti iki 2024-04-25**

2 PRIEDAS. Ekspertinio interviu klausimynas

1.	**Jūsų pozicija ir pareigos organizacijoje, jūsų išsilavinimas kibernetinio saugumo srityje.**
2.	Susipažinimas su kibernetinio saugumo brandos modeliais: ar turėjote patirties diegiant ar vertinant kibernetinio saugumo brandą organizacijoje?
3.	Jūsų organizacijos pobūdis ir dydis. Jūsų organizacijos kibernetinio saugumo programos tikslai ir prioritetai.
4.	Pritaikyti kibernetinio saugumo brandos modeliai Jūsų organizacijoje. Kas paskatino sprendimą pasirinkti šį (šiuos) modelį (-ius)?
5.	Kibernetinio saugumo brandos modelio diegimo jūsų organizacijoje procesas. Kokie buvo didžiausi iššūkiai ir sėkmės? Įgyvendinimo trukmė ir kaštai.
6.	Koks kibernetinio saugumo brandos modelio efektyvumas jūsų organizacijoje? Kaip jis matuojamas?
7.	Kibernetinio saugumo modelio integravimas su jūsų organizacijos esamais saugos procesais ir sistemomis?
8.	Jūsų organizacijos darbuotojų supratimas apie kibernetinio saugumo brandos modelį. Įsitraukimas ir elgesys, darbuotojų požiūris į kibernetinį saugumą.
9.	Nuolatinis kibernetinio saugumo brandos tobulinimas jūsų organizacijoje.
10.	Kokie didžiausi iššūkiai išlaikant kibernetinio saugumo brandos modelį organizacijoje? Bet kokios išmoktos pamokos, kuriomis norėtumėte pasidalinti.
11.	Kas, Jūsų nuomone, geriausiai apibūdina kibernetinio saugumo brandos modelio efektyvumą organizacijoje?
12.	Kokie, Jūsų nuomone, yra geriausi būdai išmatuoti kibernetinio saugumo brandos modelio efektyvumą organizacijoje?

3 PRIEDAS. ISO 27001 standarto priedo A kontrolių priemonės.

A.5 Informacijos saugumo politika **A.5.1 Informacijos saugumo valdymo kryptys** Tikslas: nustatyti valdymo kryptį ir priemones užtikrinti informacijos saugumą atitinkančius veiklos reikalavimus bei atitinkamus įstatymus ir reglamentus	
A.5.1.1 Informacijos saugumo politika	Informacijos saugumo politikų rinkinys turi būti nustatytas, patvirtintas vadovybės, paskelbtas ir išsamiai paaiškintas visiems darbuotojams bei susijusioms išorinėms šalims
A.5.1.2 Informacijos saugumo politikos peržiūra	Informacijos saugumo politikos, siekiant užtikrinti jų nuolatinį tinkamumą, adekvatumą bei efektyvumą, turi būti peržiūrimos suplanuotu reguliarumu arba įvykus reikšmingiems pasikeitimams
A.6 Informacijos saugumo organizavimas **A.6.1 Vidinis organizavimas** Tikslas: sukurti valdymo struktūrą, skirtą organizacijos informacijos saugumo sukūrimui ir eksploatavimui inicijuoti ir kontroliuoti	
A.6.1.1 Su informacijos saugumu susijęs vaidmenys ir atsakomybės	Visos su informacijos saugumu susijusios atsakomybės turi būti nustatytos ir priskirtos
A.6.1.2 Pareigų atskyrimas	Siekiant sumažinti neteisėtų ar netyčinių pakeitimų arba organizacijos turto netinkamo naudojimo galimybę turi būti aiškiai atskirtos prieigos ir nustatytos atsakomybės ribos
A.6.1.3 Ryšiai su valdžios institucijomis	Turi būti palaikomi ryšiai su valdžios institucijomis
A.6.1.4 Ryšiai su specialiomis interesų grupėmis	Turi būti palaikomi ryšiai su specialių interesų grupėmis ar kitais specialistų saugumo forumais bei profesinėmis asociacijomis
A.6.1.5 Projekto valdymo informacijos saugumas	Į projektų valdymo informacijos saugumą turi būti atsižvelgiama nepriklausomai nuo projekto tipo
A.6.2 Mobilieji įrenginiai ir nuotolinis darbas	
A.6.2.1 Mobiliųjų įrenginių politika	Siekiant apsisaugoti nuo rizikų, susijusių su mobiliaisiais įrenginiais, turi būti taikoma oficiali politika ir palaikančios saugumo priemonės
A.6.2.2 Nuotolinis darbas	Siekiant apsaugoti nutolusiose vietovėse pasiekiamą, apdorojamą ir saugomą informaciją, turi būti numatyta ir įgyvendinta nuotolinio darbo politika ir ją palaikančios priemonės
A.7 Žmogiškųjų išteklių saugumas **A.7.1 Iki įdarbinimo** Tikslas: užtikrinti, kad darbuotojai ir rangovai suprastų savo atsakomybę ir būtų tinkami jiems paskirtoms užduotims atlikti	
A.7.1.1 Tikrinimas	Visų pretendentų į darbą praeitis turi būti tikrinama nepažeidžiant galiojančių įstatymų, reglamentų ir etikos bei tenkinant veiklos ir teikiamos informacijos bei nustatytų rizikų klasifikavimo reikalavimus
A.7.1.2 Įdarbinimo nuostatos ir sąlygos	Sutartiniai susitarimai su darbuotojais ir rangovais turi numatyti jų ir organizacijos atsakomybes dėl informacijos saugumo
A.7.2 Įdarbinimo laikotarpiu Tikslas: užtikrinti, kad darbuotojai ir rangovai būtų susipažinę su savo atsakomybe už informacijos saugumą ir ją vykdytų	
A.7.2.1 Vadovybės atsakomybė	Vadovybė turi reikalauti, kad visi darbuotojai ir rangovai vadovautųsi informacijos saugumo reikalavimais, nustatytais organizacijos nustatytose politikose ir procedūrose
A.7.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	Visi organizacijos darbuotojai ir, jeigu reikia rangovai turi būti tinkamai mokomi ir nuolat informuojami apie organizacijos politikos bei procedūrų, susijusių su jų darbu, pokyčius
A.7.2.3 Drausminė procedūra	Turi būti oficiali ir išsamiai paaiškinta drausminė procedūra, kuri taikoma darbuotojams, pažeidusiems informacijos saugumo reikalavimus
A.7.3 Darbo sutarties nutraukimas ir keitimas Tikslas: apsaugoti organizacijos interesus nutraukiant arba keičiant darbo sutartis	
A.7.3.1 Darbo sutartyje nustatytų atsakomybių pabaiga arba keitimas	Atsakomybės ir pareigos dėl informacijos saugumo, kurios galios ir nutraukus arba pakeitus darbo ar samdos sutartį, turi būti apibrėžtos, išsamiai paaiškintos darbuotojui arba rangovui ir turi būti užtikrinama, kad jų laikomasi
A.8 Turto tvarkymas **A.8.1 Atsakomybė už turtą** Tikslas: identifikuoti organizacijos turtą ir nustatyti atitinkamas atsakomybes už jo apsaugą	
A.8.1.1 Turto inventorizavimas	Informacija, kitas su informacija ir jos apdorojimo priemonėmis susijęs turtas turi būti aiškiai apibrėžtas bei turi būti sudarytas ir išlaikomas tokio turto aprašas
A.8.1.2 Atsakomybė už turtą	Visas inventorizuotas turtas turi būti paskirtas valdyti
A.8.1.3 Priimtinas turto naudojimas	Turi būti nustatytos, dokumentuotos ir įgyvendintos taisyklės, skirtos informacijos ir turto, susijusio su informacija ir jos apdorojimo priemonėmis, priimtinam naudojimui
A.8.1.4 Turto grąžinimas	Pasibaigus įdarbinimo ar samdos sutarčių arba kitų susitarimų galiojimo laikui, visi darbuotojai ir išoriniai naudotojai turi grąžinti visą jiems patikėtą organizacijos turtą
A.8.2 Informacijos klasifikavimas Tikslas: Užtikrinti informacijos apsaugos lygį, atsižvelgiant į informacijos svarbą	
A.8.2.1 Informacijos klasifikavimas	Informacija turi būti klasifikuojama atsižvelgiant į teisinius reikalavimus, jos vertę, svarbumą ir jautrumą neteisėtam atskleidimui ar pakeitimui
A.8.2.2 Informacijos žymėjimas	Turi būti parengtas ir įgyvendintas tinkamas informacijai žymėti skirtų procedūrų rinkinys, atitinkantis organizacijos priimtą klasifikavimo schemą
A.8.2.3 Turto priežiūra	Turi būti parengtas ir įgyvendintas tinkamas turtui prižiūrėti skirtų procedūrų rinkinys, atitinkantis organizacijos priimtą klasifikavimo schemą
A.8.3 Duomenų laikmenų tvarkymas Tikslas: išvengti neteisėto duomenų laikmenose saugomos informacijos atskleidimo, pakeitimo, pašalinimo ar sugadinimo	
A.8.3.1 Keičiamų duomenų laikmenų tvarkymas	Keičiamų duomenų laikmenoms valdyti turi būti įgyvendintos organizacijoje priimtą informacijos klasifikavimo schemą atitinkančios procedūros
A.8.3.2 Duomenų laikmenų naikinimas	Nebereikalingos laikmenos turi būti saugiai sunaikinamos vadovaujantis, oficialiomis procedūromis
A.8.3.3 Duomenų laikmenų perdavimas	Perdavimo metu duomenų laikmenos, kuriuose yra įrašyta informacija, turi būti apsaugotos nuo neteisėtos prieigos, netinkamo jų naudojimo ir sugadinimo
A.9 Prieigos valdymas **A.9.1 Veiklos reikalavimai prieigos valdymui** Tikslas: apriboti prieigą prie informacijos bei jos apribojimo priemonių	
A.9.1.1 Prieigos valdymo politika	Vadovaujantis veiklos ir informacijos saugumo reikalavimais turi būti numatyta, dokumentuota ir peržiūrima prieigos valdymo politika
A.9.1.2 Prieiga prie tinklų ir tinklo paslaugų	Naudotojams prieiga turi būti suteikiama tik prie tų tinklų ir tinklo paslaugų, kuriomis naudotis jiems buvo konkrečiai suteikta teisė
A.9.2 Naudotojų prieigos valdymas Tikslas: užtikrinti sankcionuotą naudotojų prieigą ir išvengti neteisėtos prieigos prie sistemų ir paslaugų	

A.9.2.1 Naudotojų registravimas ir išregistravimas	Turi būti įgyvendinta oficiali naudotojų registravimo ir išregistravimo procedūra, siekiant suteikti prieigos teises
A.9.2.2 Prieigos naudotojams suteikimas	Turi būti įgyvendinta oficiali teisių naudotis visomis sistemomis ir jų paslaugomis suteikimo ir atšaukimo visų tipų naudotojams procedūra
A.9.2.3 Privilegijuotosios prieigos teisių valdymas	Privilegijuotosios prieigos teisių paskyrimas ir naudojimasis turi būti apribotas ir valdomas
A.9.2.4 Slaptos naudotojų autentiškumo patvirtinimo informacijos valdymas	Slaptos naudotojų autentiškumo patvirtinimo informacijos paskyrimas turi būti valdomas vadovaujantis oficialia valdymo procedūra
A.9.2.5 Naudotojų prieigos teisių peržiūra	Priskirtieji turto valdytojai turi nustatytu reguliarumu peržiūrėti naudotojų prieigos teises
A.9.2.6 Prieigos teisių pašalinimas arba keitimas	Pasibaigus įdarbinimo ar samdos sutarčių arba susitarimų galiojimo laikui ar jiems pasikeitus, visų darbuotojų ir išorinių naudotojų prieigos prie informacijos bei jos apdorojimo priemonių teises turi būti panaikintos
A.9.3 Naudotojų atsakomybė Tikslas: pasiektini, kad naudotojai būtų atsakingi už jų autentiškumo patvirtinimo informaciją	
A.9.3.1 Slaptos autentiškumo patvirtinimo informacijos naudojimas	Turi būti reikalaujama laikytis organizacijoje galiojančios tvarkos naudojantis slapta autentiškumo patvirtinimo informacija
A.9.4 Prieigos prie sistemų ir taikomųjų programų valdymas Tikslas: išvengti neteisėtos prieigos prie sistemų ir taikomųjų programų	
A.9.4.1 Prieigos prie informacijos ribojimas	Prieiga prie informacijos ir taikomųjų programų funkcijų turi būti apribota vadovaujantis prieigos valdymo politiką
A.9.4.2 Saugios prisijungimo procedūros	Ten, kur prieigos valdymo politika reikalauja, prieiga prie sistemų ir taikomųjų programų turi būti valdoma naudojant saugiąją prisijungimo procedūrą
A.9.4.3 Slaptažodžių tvarkymo sistema	Slaptažodžių tvarkymo sistemos turi būti interaktyvios ir užtikrinti kokybišką slaptažodžių naudojimą
A.9.4.4 Privilegijuotųjų paslaugų programų naudojimas	Paslaugų programų, kurios galėtu nepaisyti sistemoms ir taikomosioms programoms taikomų kontrolės priemonių, naudojimas turi būti apribotas ir griežtai valdomas
A.9.4.5 Prieigos prie pirminio programų teksto valdymas	Turi būti valdoma prieiga prie pirminio programų teksto
A.10 Kriptografija **A.10.1 Kriptografinės kontrolės priemonės** Tikslas: tinkamai ir veiksmingai panaudoti kriptografine priemones konfidencialumui, autentiškumui bei vientisumui apsaugoti	
A.10.1.1 Kriptografijos kontrolės priemonių naudojimo politika	Siekiant apsaugoti informaciją, turi būti numatyta ir įgyvendinta kriptografijos kontrolės priemonių naudojimo politika
A.10.1.2 Raktų valdymas	Turi būti numatyta ir įgyvendinta kriptografinių raktų naudojimo, apsaugojimo ir gyvavimo trukmės politika per visą jų gyvavimo ciklą
A.11 Fizinis ir aplinkos saugumas **A.11.1 Saugiosios vietos** Tikslas: išvengti neteisėtos fizinės prieigos, žalos bei trikdžių organizacijos informacijai ir informacijos apdorojimo priemonėms	
A.11.1.1 Fizinio perimetro apsauga	Perimetro apsaugos priemonės turi būti numatytos ir naudojamos, siekiant apsaugoti vietas, kuriose laikoma įslaptinta ar ypatingai svarbi informacija arba informacijos apdorojimo priemonės
A.11.1.2 Fizinė įėjimo kontrolė	Saugios vietos turi būti apsaugotos tinkamomis įėjimo mis, kurios užtikrintu tik įgalioto personalo įleidimą
A.11.1.3 Įstaigų, patalpų ir priemonių apsauga	Turi būti numatyta ir taikoma įstaigų, patalpų ir priemonių fizinė apsauga
A.11.1.4 Apsauga nuo išorinių ir aplinkos grėsmių	Turi būti numatytos ir pritaikytos fizinės apsaugos priemonės nuo nepalankių situacijų, tyčinių atakų ar nelaimingų atsitikimų
A.11.1.5 Darbas saugiose vietose	Turi būti numatytos ir pritaikytos procedūros, skirtos darbui saugiose vietose
A.11.1.6 Pristatymo ir krovimo vietos	Siekiant išvengti neteisėtos prieigos, prieigos vietos, pavyzdžiui, pristatymo ir krovimo zonos ar kitos vietos, pro kurias leidimo neturintys asmenys galėtu patekti į patalpas, turi būti kontroliuojamos ir, esant galimybei, atskiriamos nuo infrastruktūros, skirtos informacijai apdoroti
A.11.2 Įranga Tikslas: išvengti turto netekties, žalos, vagystės arba sugadinimo ir organizacijos veiklos pertrūkių	
A.11.2.1 Įrangos vietos parinkimas ir apsauga	Siekiant sumažinti aplinkos grėsmių ir pavojų rizika bei neteisėtos prieigos galimybę turi būti parinkta atitinkama įrangos laikymo vieta ir apsaugos priemonės
A.11.2.2 Komunalinės paslaugos	Įranga turi būti apsaugota nuo energijos tiekimo sutrikimų bei kitų nesklandumų, susijusių su komunalinių paslaugų tiekimu
A.11.2.3 Kabelių apsauga	Maitinimų ir telekomunikacijų kabeliai, kuriais perduodami duomenys arba teikiamos informacijos paslaugos, turi būti apsaugoti nuo slapto prisijungimo, trikdžių arba pažeidimo
A.11.2.4 Įrangos priežiūra	Įranga turi būti tinkamai prižiūrima, siekiant išlaikyti tolesnį jos prieinamumą ir vientisumą
A.11.2.5 Turto perkėlimas	Įranga, informacija arba programinė įranga neturi būti išnešama iš darbo vietos be atitinkamo leidimo
A.11.2.6 Įrangos ir turto, esančio ne organizacijos patalpose, saugumas	Turi būti apsaugotas ne organizacijos patalpose esantis turtas, atsižvelgiant į skirtingas dėl darbo ne organizacijos patalpose kylančias rizikas
A.11.2.7 Saugus įrangos naikinimas arba pakartotinis naudojimas	Prieš įrangą sunaikinant arba pakartotinai naudojant, visi jos elementai, kuriuose yra atmintinės, turi būti patikrinami, siekiant užtikrinti, kad visi slapti duomenys arba licencijuota programinė įranga būtų sunaikinta arba saugiai perrašyta
A.11.2.8 Be priežiūros paliekama naudotojo įranga	Naudotojai turi užtikrinti, kad jų be priežiūros paliekama įranga būtų tinkamai apsaugota
A.11.2.9 Švaraus stalo ir švaraus ekrano politika	Popieriniams dokumentams ir keičiamosioms laikmenoms turi būti taikoma švaraus stalo politika, o informacijos apdorojimo priemonėms – švaraus ekrano politika
A.12 Darbo saugumas **A.12.1 Darbo procedūros ir atsakomybė** Tikslas: užtikrinti teisingą ir saugų informacijos apdorojimo priemonių veikimą	
A.12.1.1 Darbo procedūrų įforminimas dokumentais	Darbo procedūros turėtų būti dokumentuotos ir prieinamos tiems naudotojams, kuriems jų reikia
A.12.1.2 Keitimo valdymas	Organizacijos, veiklos procesų, informacijos apdorojimo priemonių ir sistemų pakeitimai, kurie turi įtakos informacijos saugumui, turi būti kontroliuojami
A.12.1.3 Pajėgumų valdymas	Turi būti stebimas, derinamas išteklių naudojimas bei numatomi būsimo pajėgumo reikalavimai, skirti užtikrinti reikiamą sistemos veiksmingumo lygį
A.12.1.4 Kūrimo, bandymų ir eksploatavimo aplinkų atskyrimas	Kūrimo, bandymų ir operacinė sistema turi būti atskirta siekiant sumažinti neteisėtos prieigos prie operacinės sistemos arba jos pakeitimo riziką

A.12.2 Apsauga nuo kenkimo programų Tikslas: apsaugoti informaciją ir informacijos apdorojimo priemones nuo kenkimo programų	
A.12.2.1 Apsaugos nuo kenkimo programų s	Turi būti įgyvendintos tinkamos aptikimo, išvengimo bei atkūrimo priemonės, skirtos apsaugoti nuo kenkimo programų, o reikiami naudotojai turi būti supažindinti
A.12.3 Atsarginės kopijos Tikslas: apsaugoti nuo duomenų praradimo	
A.12.3.1 Atsarginės informacijos kopijos	Vadovaujantis numatyta atsarginių kopijų politika, turi būti reguliariai daromos ir išbandomos informacijos, programinės įrangos ir sistemų atsarginės kopijos
A.12.4 Įvykių registravimas ir stebėsena Tikslas: suregistruoti įvykius ir paruošti įrodymus	
A.12.4.1 Įvykių registravimas	Turi būti operacinių sistemų naudotojų veiklos, išimčių, trikčių ir informacijos saugumo įvykių žurnalai
A.12.4.2 Žurnalo duomenų apsauga	Registravimo priemonės ir užregistruota informacija turi būti apsaugota nuo klastojimo ir neteisėtos prieigos
A.12.4.3 Administratoriaus ir operatoriaus žurnalai	Sistemos administratorius ir sistemos operatoriaus veiksmai turi būti registruojami, o žurnalai turi būti saugomi ir reguliariai peržiūrimi
A.12.4.4 Laikrodžių sinchronizavimas	Visų organizacijoje ar saugumo vietoje esančių informacijos apdorojimo sistemų laikrodžiai turi būti sinchronizuoti pagal sutartą nuorodinį laiko šaltinį
A.12.5 Operacinių sistemų kontrolės priemonės Tikslas: užtikrinti operacinių sistemų vientisumą	
A.12.5.1 Programinės įrangos diegimas operacinėse sistemose	Turi būti įgyvendintos procedūros, skirtos programinės įrangos diegimui į operacinės sistemas valdyti
A.12.6 Techninių pažeidžiamumų valdymas Tikslas: išvengti techninių pažeidžiamumų išnaudojimo	
A.12.6.1 Techninių pažeidžiamumų valdymas	Turi būti laiku gaunama informacija, susijusi su informacinių sistemų techniniais pažeidžiamumais, įvertinama tokių pažeidžiamumų įtaka organizacijai bei imamasi atitinkamų priemonių susijusiai rizikai išvengti
A.12.6.2 Programinės įrangos diegimo apribojimai	Turi būti sukurtos ir įgyvendintos programinės įrangos diegimo, kurį atlieka naudotojai, taisykles
A.12.7 Informacinių sistemų auditas Tikslas: sumažinti audito veiklų poveikį operacinėms sistemoms	
A.12.7.1 Informacinių sistemų audito kontrolės priemonės	Siekiant sumažinti veiklos pertrūkių riziką, turi būti kruopščiai planuojami ir suderinami audito reikalavimai ir operacinių sistemų verifikavimo veiksmai
A.13 Ryšių saugumas **A.13.1 Tinklo apsaugos valdymas** Tikslas: užtikrinti informacijos apsaugą tinkluose ir pagalbinėse informacijos apdorojimo priemonėse	
A.13.1.1 Tinklo kontrolės priemonės	Tinklai turi būti valdomi ir prižiūrimi, siekiant apsaugoti informaciją sistemose ir taikomosiose programose
A.13.1.2 Tinklo paslaugų saugumas	Turi būti nustatytos ir kiekvieną su tinko paslaugomis susijusią sutartį įtraukiamos visų tinklo paslaugų saugumo priemonės, paslaugų lygiai ir valdymo reikalavimai, nepriklausomai nuo to, ar tos paslaugos teikiamos savo jėgomis, ar yra pasitelktos iš išorės paslaugos
A.13.1.3 Tinklų atskyrimas	Tinkluose turi būti atskirtos atskiros informacijos paslaugų, naudotojų ir informacijos sistemų grupės
A.13.2 Informacijos perdavimas Tikslas: išlaikyti informacijos perdavimo organizacijos viduje ar su bet kurio išoriniu subjektu	
A.13.2.1 Informacijos perdavimo politikos ir procedūros	Turi būti oficiali informacijos perdavimo politika, procedūros ir s, skirtos apsaugoti informaciją, naudojant visas įmanomas ryšių priemones jos perdavimui
A.13.2.2 Informacijos perdavimo sutartys	Tarp organizacijos ir išorės šalių turi būti sudaromos sutartys dėl saugaus veiklos informacijos perdavimo
A.13.2.3 Elektroninis susirašinėjimas	Elektroninio susirašinėjimo būdu siunčiama informacija turi būti tinkamai apsaugota
A.13.2.4 Konfidencialumo arba neatskleidimo sutartys	Atsižvelgiant į organizacijos informacijos apsaugos poreikius, turi būti identifikuojami, reguliariai peržiūrimi ir dokumentuojami konfidencialumo ir informacijos neatskleidimo sutarčių reikalavimai
A.14 Sistemų įsigijimas, kūrimas ir priežiūra **A.14.1 Informacijos sistemų saugumo reikalavimai** Tikslas: užtikrinti, kad informacijos saugumas būtų integrali informacinių sistemų dalis per visą gyvavimo ciklą. Taip pat apima reikalavimus informacinių sistemų, kurios teikia paslaugas per viešuosius tinklus	
A.14.1.1 Informacijos saugumo reikalavimų analizė ir specifikacija	Išdėstant naujoms informacinėms sistemoms arba esamų informacinių sistemų tobulinimui keliamus reikalavimus, turi būti nurodyti reikalavimai informacijos saugumui
A.14.1.2 Taikomųjų programų paslaugų apsaugojimas viešuosiuose tinkluose	Su per viešuosius tinklus teikiamų taikomųjų programų paslaugomis susijusi informacija turi būti apsaugota nuo kenkėjiškos veiklos, sutarčių užginčijimo bei neteisėto atskleidimo ar pakeitimo
A.14.1.3 Taikomųjų programų paslaugų transakcijų apsauga	Su taikomųjų programų paslaugų transakcijomis susijusi informacija turi būti apsaugota siekiant išvengti neužbaigto jos persiuntimo, išsiuntimo neteisingu adresu, neteisėto jos pakeitimo, atskleidimo, kopijavimo ar peradresavimo
A.14.2 Kūrimo ir priežiūros procesų saugumas Tikslas: Užtikrinti, kad kuriant informacijos sistemas visą laiką būtų taikomos informacijos saugumo priemonės	
A.14.2.1 Saugaus kūrimo politika	Organizacijoje turi būti nustatytos ir taikomos taisyklės programinei įrangai ir sistemoms kurti
A.14.2.2 Sistemų keitimo valdymo procedūros	Keitimų sistemose įgyvendinimas kūrimo fazėje turi būti valdomas vadovaujantis oficialiomis keitimų valdymo procedūromis
A.14.2.3 Techninė taikomosios programos peržiūra pakeitus operacinę sistemą	Pakeitus operacinę sistemą, vykdomai veiklai svarbios taikomosios programos turi būti peržiūrimos ir testuojamos, siekiant užtikrinti, kad organizacijos veiklai ir saugumui nebus padaryta neigiamos įtakos
A.14.2.4 Programinės įrangos paketų keitimų apribojimai	Programinės įrangos paketų keitimai neturi būti skatinami, jie turi būti ribojami, leidžiant atlikti tik būtinus pakeitimus, o visi pakeitimai turi būti griežtai kontroliuojami
A.14.2.5 Saugios sistemų inžinerijos principai	Saugios sistemų inžinerijos principai turi būti nustatyti, dokumentuoti, išlaikomi ir taikomi visoms informacinių sistemų įgyvendinimo iniciatyvoms
A.14.2.6 Saugi kūrimo aplinka	Organizacijos turi sukurti ir tinkamai visose sistemų kūrimo fazėse apsaugoti saugias kūrimo aplinkas, skirtas sistemoms kurti ir integruoti
A.14.2.7 Pasitelktas iš išorės programinės įrangos kūrimas	Organizacija turi prižiūrėti ir stebėti pasitelktus iš išorės sistemos kūrimo darbus
A.14.2.8 Sistemos saugos testavimas	Saugumo funkcionalumo testavimas turi būti atliekamas kūrimo metu
A.14.2.9 Sistemos priėmimo testavimas	Priėmimo testavimo programos ir susiję kriterijai turi būti nustatyti naujoms informacinėms sistemoms, jų atnaujinimui ir naujoms versijoms
A.14.3 Testavimo duomenys Tikslas: užtikrinti testuojant naudojamų duomenų apsaugą	
A.14.3.1 Testavimo duomenų apsauga	Testavimo duomenų turi būti parinkti apsaugoti ir valdomi
A.15 Santykiai su tiekėjais **A.15.1 Informacijos saugumas palaikant santykius su tiekėjais** Tikslas: Užtikrinti organizacijos turto, kuris prieinamas tiekėjams, apsaugą	

A.15.1.1 Informacijos saugumo politika palaikant santykius su tiekėjais	Turi būti su tiekėju suderinti ir dokumentuoti reikalavimai informacijos saugumui, skirti sumažinti rizikoms, susijusioms su tiekėjo prieiga prie organizacijos turto
A.15.1.2 Saugumo reglamentavimas sutartyse su tiekėju	Visi su informacijos saugumu susiję reikalavimai turi būti numatyti ir suderinti su kiekvienu tiekėju, galinčiu prieiti prie organizacijos informacijos, ja apdoroti, saugoti, keistis informacija ar teikti IT infrastruktūros komponentus
A.15.1.3 Informacijos ir ryšių technologijų tiekimo grandinė	Sutartyse su tiekėjais turi būti įtraukti reikalavimai dėl informacijos saugumo rizikų, susijusių su informacinių ir ryšių technologijų paslaugomis bei produktų tiekimo grandine
A.15.2 Tiekėjų paslaugų teikimo valdymas Tikslas: išlaikyti susitartą informacijos saugumo ir paslaugų teikimo lygį, atitinkantį sutartis su tiekėju	
A.15.2.1 Tiekėjų paslaugų stebėsena ir peržiūra	Organizacijos turi reguliariai stebėti, peržiūrėti ir audituoti tiekėjo teikia paslaugų teikimą
A.15.2.2 Tiekėjo paslaugų pakeitimų valdymas	Pakeitimai, susiję su tiekėjo paslaugų teikimu, įskaitant esamos informacijos saugumo politikos, procedūrų ir kontrolės priemonių išlaikymą ir tobulinimą, turi būti valdomi, atsižvelgiant į veiklos informacijos svarbą bei rizikoms pakartotinai įvertinti taikomas sistemas ir procesus
A.16 Informacijos saugumo incidentų valdymas **A.16.1 Informacijos saugumo incidentų ir gerinimo valdymas** Tikslas: užtikrinti, kad informacijos saugumo incidentų, įskaitant komunikavimą dėl saugumo įvykių ir silpnųjų vietų, valdymas butu nuoseklus ir efektyvus	
A.16.1.1 Atsakomybė ir procedūros	Siekiant užtikrinti greitą, efektyvų ir deramą atsaką į informacijos saugumo incidentus, turi būti numatytos valdymo atsakomybės ir procedūros
A.16.1.2 Pranešimas apie informacijos saugumo įvykius	Apie informacijos saugumo įvykius turi būti kaip galima greičiau pranešama per tinkamus vadovybės kanalus
A.16.1.3 Pranešimas apie silpnąsias informacijos saugumo vietas	Turi būti reikalaujama, kad visi darbuotojai ir rangovai, besinaudojantys organizacijos informacinėmis sistemomis ir paslaugomis, atkreiptu dėmesį į visas esamas ar galimas sistemos ar paslaugos saugumo silpnąsias vietas ir apie jas praneštu
A.16.1.4 Informacijos saugumo įvykių vertinimas ir sprendimų priėmimas	Informacijos saugumo įvykiai turi būti vertinami ir turi būti nuspręsta, ar jie yra informacijos saugumo incidentai
A.16.1.5 Reagavimas į informacijos saugumo incidentus	Į informacijos saugumo incidentus turi būti reaguojama taip, kaip numatyta dokumentuotose procedūrose
A.16.1.6 Mokymasis iš informacijos saugumo incidentų	Žinios, įgytos analizuojant ir šalinant informacijos saugumo incidentus, turi būti naudojamos būsimų incidentų tikimybei arba poveikiui sumažinti
A.16.1.7 Įrodymų rinkimas	Organizacija turėtu nustatyti ir taikyti procedūras informacijai, kuri galėtu būti panaudota kaip įrodymas, identifikuoti, surinkti, įsigyti ir išsaugoti
A.17 Veiklos tęstinumo valdymo informacijos saugumo aspektai **A.17.1 Informacijos saugumo tęstinumas** Tikslas: užtikrinti informacijos saugumo tęstinumą, įtraukiant jį į organizacijos veiklos tęstinumo valdymo sistemas	
A.17.1.1 Informacijos saugumo tęstinumo planavimas	Organizacija turi nustatyti savo reikalavimus informacijos saugumui ir informacijos saugumo valdymo tęstinumui nepalankiose situacijose, pavyzdžiui., krizės ar nelaimės metu
A.17.1.2 Informacijos saugumo tęstinumo įgyvendinimas	Organizacija turi sukurti, dokumentuoti, įgyvendinti ir išlaikyti procesus, procedūras ir kontrolės priemones, skirtas informacijos saugumo tęstinumui užtikrinti nepalankiose situacijose
A.17.1.3 Informacijos saugumo tęstinumo tikrinimas, peržiūra ir įvertinimas	Siekiant, kad sukurtos ir įgyvendintos informacijos tęstinumo s būtu tinkamos ir veiksmingos nepalankiose situacijose, organizacija turi jas reguliariai tikrinti
A.17.2. Perteklumas Tikslas: užtikrinti informacijos apdorojimo priemonių prieinamumą	
A.17.2.1Informacijos apdorojimo priemonių prieinamumas	Informacijos apdorojimo priemonės turi būti įdiegtos su prieinamumo reikalavimams patenkinti pakankamu perteklumu
A.18. Atitiktis **A.18.1 Atitiktis teisiniams ir sutartiniams reikalavimams** Tikslas: išvengti įstatymų, statuto, reglamentų arba sutartinių įsipareigojimų pažeidimų susijusių su informacijos saugumu ar kokiais nors saugumo reikalavimais	
A.18.1.1 Taikomų teisės aktų ir sutartinių reikalavimų identifikavimas	Kiekvienai informacinei sistemai ir organizacijai turi būti aiškiai identifikuoti, dokumentuoti ir naujinami visi susiję teisės aktų, statuto, reguliavimo ir sutartiniai reikalavimai bei organizacijos pasirinktas būdas jiems patenkinti
A.18.1.2 Intelektinės nuosavybės teisės	Siekiant užtikrinti, kad produktų, kuriems gali būti taikomos įgyvendinamos intelektinės nuosavybės teisės, ir nuosavybinės programinės įrangos naudojimas atitiktu įstatymų, reglamentų ir sutartinius reikalavimus, turi būti įgyvendintos atitinkamos procedūros
A.18.1.3 Įrašų apsauga	Įrašai pagal teisės aktų, reguliavimo, sutartinius ir veiklos reikalavimus turi būti saugomi, kad nebūtu prarasti, sunaikinti, iškraipyti, neteisėtai prieinami ir paviešinti
A.18.1.4 Privatumas ir asmens informacijos apsauga	Vadovaujantis galiojančiais įstatymais bei, kai reikia, reglamentais, turi būti užtikrintas privatumas ir asmeninės informacijos duomenų apsauga
A.18.1.5 Kriptografinių kontrolės priemonių reglamentavimas	Taikomos kriptografinės s turi būti naudojamos vadovaujantis visomis susijusiomis sutartimis, įstatymais ir reglamentais
A.18.2 Informacijos saugumo peržiūros Tikslas: užtikrinti informacijos saugumo įgyvendinamą ir taikymą taip, kaip numatyta organizacijos politikose ir procedūrose	
A.18.2.1 Nepriklausoma informacijos saugumo peržiūra	Organizacijos informacijos saugumo valdymas ir jo įgyvendinimo būdai (t. y. kontrolės priemonių tikslai, s, politikos, procesai ir informacijos saugumo procedūros) nepriklausomų specialistų turi būti tikrinami suplanuotu reguliarumu arba įvykus reikšmingiems pasikeitimams
A.18.2.2 Atitiktis saugumo politikoms ir standartams	Vadybininkai pagal savo atsakomybę turi reguliariai tikrinti informacijos apdorojimo ir procedūrų atitiktį atitinkamoms saugumo politikoms, standartams ir kitiems saugumo reikalavimams
A.18.2.3 Techninio suderinamumo tikrinimas	Turi būti periodiškai tikrinamas informacinių sistemų suderinamumas su organizacijos informacijos saugumo politikomis ir standartais

Šaltinis: ISO 27001:2013

4 PRIEDAS. Pusiau struktūruoto interviu rezultatai

1 klausimas. Jūsų pozicija ir pareigos organizacijoje, jūsų išsilavinimas kibernetinio saugumo srityje.

1	Vyriausiasis informacijos saugumo pareigūnas
2	Informacijos saugumo pareigūnas
3	Kibernetinio saugumo paramos skyriaus vadovas
4	Pradėjau saugos srityje dirbdamas kaip inžinierius, daugiausia atsakingas už techninių saugos priemonių, pvz., apsaugos nuo kenkėjiškų programų, žiniatinklio filtravimo, MDM ir kt., projektavimą, įgyvendinimą ir valdymą. Tada perėjau į duomenų centro saugos pareigūno pareigas, kurie buvo atsakingi ir už ISO 27001 ir PCI-DSS sertifikavimo įgyvendinimą ir palaikymą. 2020 m. sausio mėn. perėmiau Vyriausio informacijos saugumo pareigūno (CISO) pareigas. Esu atsakingas už antrosios gynybos linijos valdymo funkciją, kuri, be kita ko, apima bazinės informacijos (įskaitant kibernetinį) saugumo reikalavimų apibrėžimą ir užtikrinimą, kad atsakingos suinteresuotosios šalys laikytųsi vidinių ir išorinių reikalavimų bei valdytų riziką pagal organizacijų apetitą rizikuoti“
5	Aš dirbu informacijos saugumo pareigūnu ir mano pagrindinė pareiga – atlikti visų padalinių saugumo vertinimą. Turiu daugiau nei 20 metų profesinio darbo patirtį finansų institucijose IT, veiklos tęstinumo, kibernetinio saugumo ir informacijos saugumo srityse.
6	Ryšių sistemų specialistas
7	Elektronikos specialistė
8	Informacijos saugumo pareigūnas

2 klausimas. Susipažinimas su kibernetinio saugumo brandos modeliais: ar turėjote patirties diegiant ar vertinant kibernetinio saugumo brandą organizacijoje?

1	Žinau kai kuriuos modelius, bet, deja, negalėjau įdiegti savo darbo vietoje.
2	Žemas. Ne
3	Taip
4	ISO/IEC:27001/27002, NIST CSF, COBIT, NEN 7510, CMMI, CIS
5	Anksčiau naudojau modelius, pagrįstus ISO27001, o šiuo metu atlieku brandos vertinimą naudodamas viduje sukurtą sistemą.
6	Taip
7	Ne
8	Taip, turiu keletą metų patirties dirbant auditoriumi su įvairiais klientais skirtingose verslo sferose.

3 klausimas. Jūsų organizacijos pobūdis ir dydis. Jūsų organizacijos kibernetinio saugumo programos tikslai ir prioritetai.

1	Dydis ~500 darbuotojų. Nėra jokių kibernetinio saugumo tikslų ir prioritetų.
2	Vidutinė
3	IT įmonė, kurioje dirba virš 7000 darbuotojų
4	Finansinių paslaugų įmonė, turinti 10 000 darbuotojų. Prioritetus apibrėžia 1-osios linijos organizacija, tačiau pagal 2-osios linijos perspektyvą dėmesys sutelkiamas į pagrindinius elementus, kurie gali būti laikomi pagrindine saugumo higiena.
5	Pasaulinė finansų institucija, kuri specializuojasi skolų valdyme. Kibernetinio saugumo strategija ir programa nėra aiškiai apibrėžta arba nebuvo perteikta mano lygiui.
6	Valstybės gynyba
7	Elektronikos sritis, korporacija. Kibernetinio saugumo programos tikslai ir prioritetai mano organizacijoje: Apsaugoti organizacijos duomenis ir informaciją nuo neleistinos prieigos ar pakeitimų. Tinklo sauga ir perimetro apsauga. Užtikrinti duomenų saugą. Teisės aktų laikymasis. Užtikrinti organizacijos verslo tęstinumą ir atsparumą prieš kibernetinius įvykius. Nuolat atnaujinti saugumo strategiją ir prisitaikyti prie pokyčių. Darbuotojų mokymas ir supratimas apie saugumą. Prioritetai: nuolatinis stebėjimas ir priežiūra.

8	Organizacija apie ~2000 darbuotojų. Apsaugoti organizaciją nesulėtinant jos veiklos

4 klausimas. Pritaikyti kibernetinio saugumo brandos modeliai Jūsų organizacijoje. Kas paskatino sprendimą pasirinkti šį (šiuos) modelį (-ius)?

1	Logiška ir pan. Buvo pasirinkti modelius.
2	Nėra
3	Rizikos vertinimai
4	NIST CSF, ISO/IEC 27002:2022 kartu su CMMI ir pritaikyta pagal mūsų vidines taisykles ir reguliavimo įsipareigojimus. Pasirinkti dėl to, kad istoriškai mūsų ISMS yra pagrįsta ISO 27001, pasirinkti modeliai yra plačiai naudojami tarp mūsų klientų, o svarbiausios vidinės suinteresuotosios šalys dažnai jau turi pagrindinį supratimą apie lūkesčius.
5	IT saugumo, duomenų apsaugos ir kt. politika) + ISO27001 + NIST reikalavimai
6	ISO 27001 ir NIST. Siekis pagerinti kibernetinio saugumo situacijos suvokimą
7	ISO/IEC 27001 ir NIST CSF. Poreikis užtikrinti informacijos saugumą ir įgyti konkurencinį pranašumą rinkoje.
8	ISO 27001 ir NIST. Tikslios priežasties nežinau.

5 klausimas. Kibernetinio saugumo brandos modelio diegimo jūsų organizacijoje procesas. Kokie buvo didžiausi iššūkiai ir sėkmės? Įgyvendinimo trukmė ir kaštai.

1	Pakeisti žmonių nuomonę ir paaiškinti jiems saugumo svarbą, kaina yra laikas ir sąmoningumas
2	Nėra
3	Kibernetinio saugumo brandos modelis, stabdo verslo sprendimą diegti naujus sprendimus ar produktus.
4	Iššūkiai buvo ne tiek susiję su pasirinktomis sistemomis, bet kur kas daugiau: supažindinti žmones su pasirinktų kontrolės priemonių pagrįstumu ir jų atsakomybe. Iššūkių, susijusių su faktiniu kontrolės priemonių įgyvendinimu ir kasdieniu valdymu. Sėkmė: Žymiai išaugo informuotumas, ypač tarp su saugumu nesusijusių darbuotojų
5	Negalima sakyti, kad įgyvendinimas buvo projektas, tai buvo gana ilgas procesas, kad atitiktų reikalavimus.
6	Negaliu atsakyti
7	Negaliu atsakyti.
8	Vis dar yra diegiamas

6 klausimas. Koks kibernetinio saugumo brandos modelio efektyvumas jūsų organizacijoje? Kaip jis matuojamas?

1	Sėkmingas vidinis ir išorinis auditas
2	Nėra
3	Nežinau
4	Efektyvumas matuojamas naudojant dokumentais pagrįstą kontrolės sistemą, kurioje aprašomi kontrolės reikalavimai, rizika ir minimalus numatomas įgyvendinimas. Vertinama pagal 2 gynybos liniją su saugumo galimybėmis, apibrėžtomis sistemoje per 3 metų ciklą. Naudojamas Gebėjimų brandos vertinimo modelis (CMMI) siekiant įvertinti brandą ir neatitikimus (pvz., vidaus taisyklėms), jie registruojami ir antroji linija susisiekia su rizikos / kontrolės savininku. Be to, 3 gynybos linija (auditas) atlieka rizika pagrįstus auditus visoje organizacijoje ir periodiniai išoriniai auditai atliekami ištisus metus
5	Yra 3 metų vertinimo programa, pagal kurią nepriklausomi vertintojai tikrina esamą brandą.
6	Incidentų kiekis. Kibernetinio saugumo situacijos suvokimas tarp organizacijos narių
7	Aukštas. Sugebėjimu atsilaikyti prieš atakas.
8	Vis dar yra diegiama. Yra tam tikri veiklos rodikliai priklausomai nuo skirtingų apsaugos domenų, kategorijų, kontrolių.

7 klausimas. Kibernetinio saugumo modelio integravimas su jūsų organizacijos esamais saugos procesais ir sistemomis?

1	Taip
2	Nėra
3	Pilnai integruotas
4	Sėkmingai įgyvendinta
5	Sakyčiau taip, nes modelis turi būti esamų procesų dalis.
6	Procesai keičiami atsižvelgiant į poreikį
7	Nelabai galiu atsakyti. Viskas sklandu.
8	Modelis yra interpretuojamas ir pritaikomas atitinkamai nuo organizacijos poreikių.

8 klausimas. Jūsų organizacijos darbuotojų supratimas apie kibernetinio saugumo brandos modelį. Įsitraukimas ir elgesys, darbuotojų požiūris į kibernetinį saugumą.

1	Tai keičiasi kiekvieną dieną ir visi nauji dalykai
2	Žemas. Kai kurie žmonės yra apgauti per kai kurias sukčiavimo atakas.
3	Visi darbuotojai reguliariai lanko privalomus kibernetinio saugumo informuotumo mokymus
4	Tai galima išmatuoti tik ribotai ir apima subjektyvumo lygį, jei žiūrėsime į visą įmonę. Jei pažvelgtume tik į turimą informaciją, pvz., sukčiavimo simuliacijas, praneštus saugumo incidentus ir reagavimo į incidentus laiką ir t. t. Informuotumas ir įsitraukimas per pastaruosius porą metų labai išaugo, bet ne ten, kur norime.
5	Darbuotojai turi žinoti, ko tikimasi siekiant apsaugoti įmonės informaciją, ir apie tai pranešama pasitelkiant politiką, procedūras, el. mokymus ir kt.
6	Geras suvokimas, kuris pastoviai didinamas atliekant incidentų imitavimo pratybas
7	Lengvabūdiškas.
8	Brandos modelio supratimas skiriasi priklausomai nuo darbuotojų departamento.

9 klausimas. Nuolatinis kibernetinio saugumo brandos tobulinimas jūsų organizacijoje.

1	Taip
2	Periodiniai mokymai, skirti informuoti apie kibernetinį saugumą socialinės inžinerijos požiūriu.
3	Aktyvi CISO valdyba iš kiekvienos šalies rengia reguliarius posėdžius, kuriuose aptaria dalykus, kuriuos galima tobulinti.
4	Siekiame nuolat gerinti savo bendrą saugumo padėtį įvairiais procesais, tokiais kaip rizikos valdymo programa, BCCM/DR/CM, incidentų tinklo valdymas ir daug daugiau
5	Sakyčiau, tai kitas žingsnis.
6	Nuolat tobulinama
7	Bendradarbiavimas su kitomis organizacijomis ir saugumo specialistais, investavimas į technologijas, darbuotojų mokymai, reguliarus auditas ir vertinimai.
8	Šis procesas vyksta nuolatos

10 klausimas. Kokie didžiausi iššūkiai išlaikant kibernetinio saugumo brandos modelį organizacijoje? Bet kokios išmoktos pamokos, kuriomis norėtumėte pasidalinti.

1	Buvo atnaujinti, žinoti kiekvieną sistemą ir rasti kiekvienos problemos sprendimą
2	Nėra
3	Kibernetinio saugumo brandos modelis, stabdė verslo sprendimus diegti naujus sprendimus ar produktus.
4	Didžiausios problemos yra įvairių veiklos funkcijų pajėgumai ir tinkamos informacijos pozicijos išlaikymas daugiau nei 20 šalių ir sudėtingas pasaulinis veiklos modelis. Tinklų kūrimas, žinojimas, su kuo kalbėtis ir užtikrinti, kad esame informacijos grandinėje, yra didžiausias dalykas Svarbus mano kasdieninio darbo aspektas, antrasis, yra iš tikrųjų pašalinti visas galimas kontrolės spragas, riziką ir pan.
5	Manau, kad pirmiausia svarbu apibrėžti numatomą brandos lygį ir užtikrinti, kad visi verslo subjektai būtų tokio paties lygio. Tada kaip kitą žingsnį reikėtų apibrėžti, ar tas lygis yra tikslinis, ar jį reikėtų padidinti. Tai turėtų kilti iš kibernetinio saugumo strategijos.
6	Pastovus personalo mokymas ir budrumo tikrinimas
7	Darbuotojų aplaidumas.
8	Gera komunikacija, manau, yra svarbiausias iššūkis norint įdiegti ar išlaikyti kibernetinio saugumo branda.

11 klausimas. Kas, Jūsų nuomone, geriausiai apibūdina kibernetinio saugumo brandos modelio efektyvumą organizacijoje?

1	Įrankiai ir žmonės
2	Nėra
3	Kibernetinio saugumo brandos modelio efektyvumą organizacijoje geriausiai gali apibūdinti jos gebėjimas visapusiškai įvertinti organizacijos kibernetinio saugumo laikyseną, nustatyti stipriąsias ir silpnąsias puses, prioritetus skirti patobulinimams ir nukreipti organizaciją į aukštesnį atsparumo kibernetinėms grėsmėms lygį. Kibernetinio saugumo modelis turėtų leisti organizacijai: - Įvertinti dabartinę būklę: įvertinti esamą organizacijos kibernetinio saugumo praktiką, politiką ir technologijas įvairiose srityse, tokiose kaip valdymas, rizikos valdymas, atitiktis ir techninė kontrolė. - Nustatyti tikslus ir nustatyti prioritetus: nustatyti aiškius tikslus ir prioritetines sritis tobulėjimui, remiantis organizacijos rizikos profiliu, reguliavimo reikalavimais ir verslo tikslais. - Vadovas tobulinimo pastangoms: pateikti gaires ir rekomendacijas, kaip įgyvendinti būtinus kibernetinio saugumo procesų, kontrolės priemonių ir technologijų pakeitimus ir patobulinimus. - Išmatuoti pažangą: stebėti organizacijos pažangą laikui bėgant , įvertinti patobulinimus ir prireikus koreguoti strategijas, kad būtų pašalintos kylančios grėsmės ir kintantys verslo poreikiai. Palengvinti bendravimą: tarnauja kaip bendra suinteresuotųjų šalių, įskaitant vadovus, IT specialistus, saugos komandas ir išorės partnerius, bendravimo ir bendradarbiavimo sistema. Palaikyti sprendimų priėmimą: informuoti apie sprendimų priėmimo procesus, susijusius su išteklių paskirstymu, investicijų prioritetų nustatymu ir rizikos valdymu, pateikiant struktūrinį kibernetinio saugumo rizikos vertinimo ir mažinimo metodą. Pritaikymas ir mastelio keitimas: būti lankstiems ir keistis, kad laikui bėgant prisitaikyti prie organizacijos technologijų aplinkos, reguliavimo aplinkos ir grėsmių aplinkos pokyčių. Skatinti kultūros pokyčius: propaguoti kibernetinio saugumo supratimo ir atsakomybės kultūrą visoje organizacijoje, nuo vadovavimo lygio iki atskirų darbuotojų. Apskritai kibernetinio saugumo brandos modelio veiksmingumas slypi jo gebėjime nuolat tobulėti ir būti atspariems kibernetinėms grėsmėms, derinant su organizacijos bendrais verslo tikslais ir rizikos tolerancija.
4	Įdiegtas brandos modelis, kaip mūsų visos grupės valdymo modelio dalis, leidžia mums geriau suprasti mūsų dabartinę brandą tiek kaip pasaulinei organizacijai, tiek atskiruose padaliniuose, tačiau taip pat leidžia taikyti nuoseklų metodą gerinimui laikui bėgant įvertinti. Tai leidžia vyresniajai vadovybei priimti rizika pagrįstus sprendimus ir atitinkamai paskirstyti išteklius.
5	Kiekviena organizacija turi sukurti savo apibrėžimą. Tai gali būti priemonės kritinėse srityse, pvz., incidentų skaičius, incidentų sunkumas, atitiktis pagrindų sistemai arba sertifikavimas pagal standartus, pvz., ISO.
6	Incidentų kiekio mažėjimas ir vartotojų pranešimų apie neaiškias situacijas didėjimas
7	Sugebėjimas apsaugoti duomenis, sistemas ir tinklus nuo kibernetinių atakų.
8	Vadovų (upper management) požiuris į investicijas šiuo klausimu.

12 klausimas. Kokie, Jūsų nuomone, yra geriausi būdai išmatuoti kibernetinio saugumo brandos modelio efektyvumą organizacijoje?

1	Vertinimas, testavimas.
2	Naudojant gerai įgyvendintą standartizavimą / normalizavimą (pvz., ISO, SOC, PCI DSS...)
3	Kibernetinio saugumo brandos modelio veiksmingumo vertinimas organizacijoje yra labai svarbus siekiant užtikrinti, kad kibernetinio saugumo praktika laikui bėgant tobulėtų ir tinkamai reaguotų į riziką. Štai keletas pagrindinių metodų, kaip įvertinti jo efektyvumą: - Spragų analizė: atlikti išsamų vertinimą, kad nustatyti visus skirtumus tarp dabartinės kibernetinio saugumo brandos būsenos ir brandos modelyje nurodytos norimos būsenos. Ši analizė gali padėti nustatyti prioritetus tobulintinoms sritims. - Metrikos stebėjimas: apibrėžti pagrindinius veiklos rodiklius (KPI), suderintus su kibernetinio saugumo brandos modelio tikslais. Ši metrika gali apimti tokius dalykus kaip saugumo incidentų skaičius, laikas aptikti ir reaguoti į grėsmes, pataisų dažnis, darbuotojų mokymų baigimo rodikliai ir t.t. Reguliariai stebėti ir analizuoti šiuos rodiklius, kad stebėti pažangą ir nustatyti sritis, kurioms reikia dėmesio. - Reagavimo į incidentus testavimas: įvertinti organizacijos reagavimo į incidentus galimybes per imituojamus kibernetinių atakų scenarijus. Tai gali padėti nustatyti, ar organizacija yra gerai pasirengusi aptikti saugumo incidentus, reaguoti į juos ir atsigauti po jų, išryškinant bet kokius kibernetinio saugumo brandos modelio įgyvendinimo trūkumus. - Saugumo supratimo ir mokymo vertinimai: išmatuoti supratimo apie saugumą programų ir mokymo iniciatyvų efektyvumą atliekant vertinimus arba apklausas, kad įvertinti darbuotojų supratimą apie geriausią kibernetinio saugumo praktiką. Tai gali padėti užtikrinti, kad darbuotojai būtų susipažinę su savo vaidmenimis ir atsakomybe užtikrinant saugumą. - Atitikties auditas: reguliariai vertinti, kaip organizacija laikosi atitinkamų kibernetinio saugumo taisyklių, standartų ir sistemų (pvz., GDPR, NIST kibernetinio saugumo sistemos, ISO 27001). Atitiktis gali būti rodiklis, rodantis, kaip kibernetinio saugumo brandos modelis atitinka geriausią pramonės praktiką ir reguliavimo reikalavimus. - Tiekėjų ir trečiųjų šalių vertinimai: įvertinti pardavėjų ir trečiųjų šalių partnerių kibernetinio saugumo riziką, kad įsitikinti, jog jie atitinka tuos pačius standartus, nurodytus organizacijos kibernetinio saugumo brandos modelyje. Trečiųjų šalių saugos praktikos trūkumai gali kelti didelę riziką organizacijai. - Nuolatinio tobulinimo grįžtamojo ryšio ciklas: nustatyti grįžtamojo ryšio iš suinteresuotųjų šalių, įskaitant IT komandas, verslo padalinius ir vyresniąją vadovybę, rinkimo procesą. Naudoti šį atsiliepimą, kad nustatytumėte sritis, kurias reikia tobulinti kibernetinio saugumo brandos modelyje, ir atitinkamai pakoreguoti strategijas. - Kaštų ir naudos analizė: įvertinti investicijų į kibernetinį saugumą ir iniciatyvų rentabilumą, susijusį su organizacijos rizikos mažinimu ir atsparumu. Ši analizė gali padėti parodyti kibernetinio saugumo brandos modelio vertę suinteresuotosioms šalims ir pagrįsti išteklių paskirstymą. Taikydamos šiuos metodus, organizacijos gali efektyviai įvertinti savo kibernetinio saugumo brandos modelio efektyvumą ir priimti pagrįstus sprendimus, kad laikui bėgant pagerintų savo saugumą.
4	Sukurti aiškią, skaidrią ir dokumentais pagrįstą kontrolės sistemą, kurioje būtų aprašomi lūkesčiai, pagrindiniai reikalavimai (įskaitant numatomą brandos lygį), neatitikties rizika ir periodiškai, bet nuosekliai įvertinama renkant informaciją ir imant atranką (jei įmanoma ir taikoma). Kontrolės ir (arba) rizikos savininkai turi suprasti lūkesčius ir atsakomybę, tačiau taip pat turėtų sugebėti įrodyti, kad šiame kontekste taikomas „pasitikėk, bet tikrink“.
5	Geriausias būdas įvertinti yra auditas arba saugos įvertinimas, bet taip pat priemones galima apibrėžti kaip KPI ir KRI, kuriuos reikia stebėti kasdien.
6	Nuolatinis incidentų imitavimas ir situacijų vertinimas. Papildoma pastaba anketai. Nelabai aišku ką norit paklausti. Trūksta konteksto. Siūlyčiau tobulinti. Labai abstraktus klausimai. Geros dienos ir sekmingo apsiginimo.
7	Auditas, testavimai, ataskaitos ir vertinimai.
8	Reikia turėti aiškias procesų kontroles kurioms butu nustatyti aiškūs reikalavimai ir taip butu išmatuojamas kiekvienos kontrolės efektyvumas. Taip butu galima nustatyti bendrą saugumo vaizdą organizacijoje.