Kauno technologijos universitetas

Ekonomikos ir verslo fakultetas

Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas

Baigiamasis magistro studijų projektas

Edita Meištaitė

Projekto autorė

Prof. dr. Edita Gimžauskienė

Vadovė

Kaunas, 2021

Kauno technologijos universitetas
Ekonomikos ir verslo fakultetas

Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas

Baigiamasis magistro studijų projektas
Apskaita ir auditas (6211LX037)

Edita Meištaitė
Projekto autorė

Prof. dr. Edita Gimžauskienė
Vadovė

Doc. dr. Šviesa Leitonienė
Recenzentė

Kaunas, 2021

Kauno technologijos universitetas

Ekonomikos ir verslo fakultetas

Edita Meištaitė

Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama kitų asmenų autoriaus ar kitų teisių, laikydamasi Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjusi;

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Edita Meištaitė

Patvirtinta elektroniniu būdu

Meištaitė, Edita. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas. Magistro studijų baigiamasis projektas / vadovė prof. dr. Edita Gimžauskienė; Kauno technologijos universitetas, Ekonomikos ir verslo fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Apskaita, Verslas ir viešoji vadyba.

Reikšminiai žodžiai: *kibernetinis saugumas, kibernetinio saugumo rizika, kibernetinio saugumo rizikos vertinimas, vidaus auditas.*

Kaunas, 2021. 85 p.

Santrauka

Šiandien vis labiau kalbama apie tai, kad kibernetinio saugumo rizikos negalima išvengti, todėl tampa svarbu užtikrinti tinkamą jos valdymą. Įmonių intelektinė nuosavybė, pagrindiniai klientų ir organizacijos duomenys, organizacijos reputacija ir finansiniai ištekliai – tai tik dalis elementų, kurių praradimu rizikuoja organizacijos, tinkamai neužtikrinančios kibernetinio saugumo rizikos suvaldymo. Svarbu tai, kad bendrą kibernetinio saugumo rizikos poveikį organizacijos vadovai privalo vertinti kaip kompleksinę, visus verslo procesus neigiamai veikiančią, grėsmę. Norint užtikrinti visapusišką šios rizikos valdymą būtina įsivertinti pažeidžiamiausias organizacijos sritis, atlikti grėsmės poveikio analizę bei suplanuoti atsako priemonių taikymą. Vidaus audito, kaip nepriklausomo vertintojo, vaidmuo tampa būtinu siekiant užtikrinti kibernetinio saugumo rizikos nustatymo, tinkamo valdymo, atsparumo ir saugumo užtikrinimo priemonių taikymą. Šiame darbe siekiama įvertinti, kaip vidaus audito procedūrų ir kibernetinio saugumo rizikos vertinimo funkcijos galėtų būti derinamos tarpusavyje ir leistų užtikrinti privačių organizacijų duomenų konfidencialumą bei visiems verslo procesams saugią aplinką. Mokslinėje literatūroje pastebėtas metodų, kurie leistų įvertinti kibernetinio saugumo riziką, integruojant ją į organizacijos vidaus kontrolės vertinimo dalį, trūkumas. Būtent šią problemą siekiama padėti išspręsti pasiūlant kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį ir tuo pat metu paskatinti tolimesnius šios srities tyrimus.

Tyrimo objektas – kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas.

Tyrimo tikslas – pasiūlyti ir empiriškai patikrinti konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį.

Tyrimo uždaviniai:

1) Atskleisti kibernetinio saugumo rizikos sampratą ir jos vertinimo vidaus audito procedūrose problematiškumą;

2) Sudaryti konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį;

3) Pasiūlyti kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio empirinio tyrimo metodologiją;

4) Atlikti empirinį pasiūlyto kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio tyrimą, nustatyti organizacijų kibernetinio saugumo rizikos vertinimo lygį ir pateikti pasiūlymus dėl kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo.

Pagrindiniai tyrimo rezultatai. Mokslinės literatūros pagrindu buvo sudarytas konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelis. Modelio struktūrą sudaro dvi vertinimo sritys – kibernetinio saugumo rizikos vertinimas ir vidaus audito procedūrų užtikrinimo vertinimas. Šios sritys įvertintos nustatant atitinkamą šių sričių būklės lygmenį. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelis buvo empiriškai patikrintas atliekant kokybinį tyrimą – trijų organizacijų atvejo studijas. Tyrimo metu nustatyta, kad kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo konceptualus modelis gali būti naudojamas kaip praktinis įrankis, kurio pagrindu galima atlikti, o vėliau ir palyginti skirtingų įmonių kibernetinio saugumo rizikos vertinimo būklę ir vidaus audito procedūrų užtikrinimo būklę. Pagal empirinio tyrimo metu nustatytus trūkumus pateiktos konkrečios tobulintinų procedūrų rekomendacijos. Tyrimas patvirtino literatūros analizės metu keliamas prielaidas, kad kibernetinio saugumo rizika gali būti įvertina vidaus audito procedūrose, o su šiuo įvertinimu siejamas ir tinkamesnis kibernetinio saugumo užtikrinimas.

Meištaitė, Edita. Cyber Security Risk Assessment in Internal Audit Procedures. Master's Final Degree Project / supervisor prof. dr. Edita Gimžauskienė; School of Economics and Business, Kaunas University of Technology.

Study field and area (study field group): Accounting, Business and Public Management.

Keywords: *cyber security, cyber security risk, cyber security risk management, internal audit.*

Kaunas, 2021. 85 p.

Summary

Nowadays cyber security risks are unavoidable and it is important to ensure that they are properly managed. Corporate intellectual property, customer and organization data, reputation of organization and financial resources are some of the elements that organizations risk to lose if they do not adequately manage cyber security risks. Importantly, the overall impact of cyber security risks must be considered by the organization's management as a complex threat that negatively affects all business processes. In order to ensure comprehensive management of this risk, it is necessary to self-assess the most vulnerable areas of the organization, perform a threat impact analysis and plan response measures. The role of internal audit as an independent evaluator becomes essential to ensure the identification, good governance and resilience of cyber security risks, and also implementation of security measures. This study aims to assess how the internal audit procedures and the cyber security risk assessment procedures could be combined with each other and ensure the confidentiality of organizations private data and a secure environment for all business processes. In the academic literature there is a lack of methods to assess the risk of cyber security by integrating it into the organization's internal audit procedures. Therefore, the aim of this study is to address this issue by proposing a model for assessing the cyber security risk in internal audit procedures and also encourage further research in this field.

Research object – cyber security risk assessment in internal audit procedures.

Research aim – to propose and empirically investigate the conceptual model of cyber security risk assessment in internal audit procedures.

Research objectives:

1) To analyse the concept of cyber security risk and problems of cyber security risk assessment in internal audit procedures;

2) To develop conceptual model of cyber security risk assessment in internal audit procedures;

3) To propose the methodology of application of model of cyber security risk assessment in internal audit procedures;

4) To carry out an empirical research of the proposed model of cyber security risk assessment in internal audit procedures; to determine the level of cyber security risk assessment in organizations and to make suggestions for the improvement of cyber security risk assessment in internal audit procedures.

Results of the research. Based on the academic literature, the conceptual model of cyber security risk assessment in internal audit procedures was developed. The structure of the model consists of two main assessment areas – cyber security risk assessment and internal audit procedures assurance assessment. These areas have been assessed by determining the appropriate level of status for these areas. The model of cyber security risk assessment in internal audit procedures was empirically tested by performing a qualitative research – case studies of three organizations. Research results confirmed that a conceptual model of cyber security risks assessment in internal audit procedures can be used as a practical tool. On the basis of this practical tool, it is possible to perform and compare the state of cyber security risk assessment and the state of internal audit procedures assurance of different companies. Based on the shortcomings identified in the empirical research, specific recommendations for procedures to be improved are provided. The study confirmed the assumptions made from literature review that cyber security risks can be assessed in internal audit procedures, and this assessment is associated with more appropriate cyber security assurance.

Turinys

Lentelių sąrašas ... **9**

Paveikslų sąrašas ... **10**

Santrumpų ir terminų sąrašas ... **11**

Įvadas ... **12**

1. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo problemos analizė ... **16**

1.1. Kibernetinio saugumo rizikos samprata ir vidaus audito galimybės jos nustatymui ... 16

1.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo problematika ... 19

2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio teoriniai sprendimai ... **23**

2.1. Kibernetinio saugumo rizikos vertinimo mechanizmai ... 23

2.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo poreikis ... 25

2.3. Vidaus audito pokyčiai ir jų įtaka kibernetinio saugumo rizikos vertinimui ... 29

2.4. Vidaus audito procedūrų integravimas į kibernetinio saugumo rizikos vertinimą ... 33

2.5. Konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelis ... 36

3. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio tyrimo metodologija ... **40**

4. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tyrimo rezultatai ... **46**

4.1. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai A įmonėje ... 46

4.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai B įmonėje ... 56

4.3. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai C įmonėje ... 65

4.4. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatų aptarimas ir diskusija ... 74

Išvados ... **79**

Literatūros sąrašas ... **81**

Priedai ... **86**

1 priedas. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo klausimynas ir vertinimo kriterijų įverčių reikšmės ... 86

Lentelių sąrašas

1 lentelė. Kibernetinio saugumo ir kibernetinio saugumo rizikos sąvokų apibrėžimai 19
2 lentelė. Audito etapai ir analitiniai metodai 29
3 lentelė. Nuolatinio užtikrinimo (tęstinio audito) ir kibernetinio saugumo ypatybių palyginimas su tradiciniu audito modeliu 31
4 lentelė. Kibernetinio saugumo rizikos vertinimo kategorijų vertinimo kriterijai ir juos apibūdinantys veiksniai 41
5 lentelė. Vidaus audito procedūrų kategorijų vertinimo kriterijai ir juos apibūdinantys veiksniai . 43
6 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo sistema 45
7 lentelė. Kibernetinio saugumo rizikos vertinimo A įmonėje rezultatai 46
8 lentelė. Vidaus audito procedūrų vertinimo A įmonėje rezultatai 52
9 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos A įmonėje 55
10 lentelė. Kibernetinio saugumo rizikos vertinimo B įmonėje rezultatai 56
11 lentelė. Vidaus audito procedūrų vertinimo B įmonėje rezultatai 61
12 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos B įmonėje 64
13 lentelė. Kibernetinio saugumo rizikos vertinimo C įmonėje rezultatai 65
14 lentelė. Vidaus audito procedūrų vertinimo C įmonėje rezultatai 69
15 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos C įmonėje 73

Paveikslų sąrašas

1 pav. Hierarchinė literatūros žemėlapio schema 14
2 pav. Tyrimo struktūros schema 15
3 pav. Kibernetinio saugumo rizikos vertinimo sistema pagal tris apsaugos linijas 28
4 pav. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo teorinis modelis 37
5 pav. Kibernetinio saugumo rizikos vertinimo kategorijos 38
6 pav. Vidaus audito procedūrų vertinimo kategorijos 38
7 pav. Kibernetinio saugumo rizikos kategorijų vertinimas A įmonėje 48
8 pav. Kibernetinio saugumo rizikos kriterijų vertinimas A įmonėje 49
9 pav. Vidaus audito procedūrų vertinimas A įmonėje 53
10 pav. Vidaus audito procedūrų kriterijų vertinimas A įmonėje 54
11 pav. Kibernetinio saugumo rizikos kategorijų vertinimas B įmonėje 58
12 pav. Kibernetinio saugumo rizikos kriterijų vertinimas B įmonėje 59
13 pav. Vidaus audito procedūrų vertinimas B įmonėje 62
14 pav. Vidaus audito procedūrų kategorijų vertinimas B įmonėje 63
15 pav. Kibernetinio saugumo rizikos kategorijų vertinimas C įmonėje 67
16 pav. Kibernetinio saugumo rizikos kriterijų vertinimas C įmonėje 68
17 pav. Vidaus audito procedūrų vertinimas C įmonėje 71
18 pav. Vidaus audito procedūrų kategorijų vertinimas C įmonėje 72
19 pav. Kibernetinio saugumo rizikos vertinimo apibendrinamieji rezultatai 74
20 pav. Vidaus audito procedūrų vertinimo apibendrinamieji rezultatai 76
21 pav. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai 77

Santrumpų ir terminų sąrašas

Santrumpos:

A la – panašiai kaip; kaip.

Ex ante – iš anksto; prieš veiksmą.

Terminai:

Konvergencija *(angl. convergation)* – išorinių požymių, sandaros supanašėjimas.

Procesų „kasyba“ *(angl. process mining)* – analitinė disciplina, skirta atrasti, stebėti ir tobulinti procesus.

Ugniasienė *(angl. firewall)* –vidinė kompiuterio programa, atskiras serveris arba kompiuteris, kuris riboja išorinį ryšį su kitų kompiuterių programomis.

Įvadas

Temos aktualumas. Šiandien vis labiau kalbama apie tai, kad kibernetinio saugumo rizikos negalima išvengti, todėl tampa svarbu užtikrinti tinkamą jos valdymą. Internetinės erdvės augimas ir toliau didės, jei sąveika, atvirumas, stabilumas, atsparumas, ekonomikos augimas ir saugumu sušvelninta rizika paskatins jos plėtrą. Gausėjančios technologijos suteikia vis didesnę prieigą vartotojui prie organizacijų informacijos apie bendrą verslo tiekimo grandinę, klientus ir paslaugų teikėjus. Organizacijos dažnai kaupia didelius konfidencialios informacijos duomenų kiekius virtualioje infrastruktūroje, prieinamoje naudojant debesijos kompiuteriją ar serverinę sistemą, todėl informacija tampa lengvai prieinama (Ames ir kt., 2016). Kitas svarbus veiksnys yra vis didėjantis įrenginių skaičius, kuriuos galima prijungti ir kurie padeda keistis duomenimis tarpusavyje (reiškinys dar vadinamas „daiktų internetu“). Dėl šių priežasčių, tinklo saugumas tampa pagrindiniu politikos, pasaulio valstybių reguliacinių institucijų, organizacijų vadovų ir auditorių rūpesčiu visame pasaulyje (Kahyaoglu ir Caliyurt, 2018). Įmonių intelektinė nuosavybė, pagrindiniai klientų ir organizacijos duomenys, organizacijos reputacija ir finansiniai ištekliai – tai tik dalis elementų, kurių praradimu rizikuoja organizacijos, tinkamai neužtikrinančios kibernetinio saugumo rizikos suvaldymo.

Organizacijoms globalizuojantis ir plečiantis jų darbuotojų, klientų ir trečiųjų šalių tiekėjų tinklui, didėja ir nuolatinės prieigos prie organizacijų informacijos lūkesčiai, o su jais ir atitinkami šių duomenų saugumo užtikrinimo būdai bei metodai. Technologinei pažangai palaikant verslą, ji tuo pačiu skatina ir kibernetinio saugumo grėsmės raidą. Taip kaip tobulėja grėsmės sukėlėjai, taip ir organizacijos turi įvertinti savo kibernetinio saugumo rizikos apsaugos lauką. Dėl to labai svarbu suprasti bendrą organizacijos kibernetinės rizikos poveikį, kuris gali apimti ne tik turtinę ir finansinę organizacijų dalį, bet turėti reikšmingos įtakos veiklos vidaus kontrolei, visų procesų suvaržymui. Bendrą kibernetinio saugumo rizikos poveikį organizacijos vadovai privalo vertinti kaip kompleksinę, visus verslo procesus neigiamai veikiančią, grėsmę. Norint užtikrinti visapusišką šios rizikos valdymą būtina įsivertinti pažeidžiamiausias organizacijos sritis, atlikti grėsmės poveikio analizę bei suplanuoti atsako priemonių taikymą. Vidaus audito, kaip nepriklausomo vertintojo, vaidmuo tampa būtinu siekiant užtikrinti kibernetinio saugumo rizikos nustatymo, tinkamo valdymo, atsparumo ir saugumo užtikrinimo priemonių taikymą. Dėl vertinimo įgūdžių visuose organizacijų procesuose vidaus auditoriai yra svarbūs partneriai ir turėtų būti laikomi neatsiejama kibernetinio saugumo rizikos užtikrinimo proceso dalimi (Kahyaoglu ir Caliyurt, 2018).

Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo galimybės reikšmingai prisidėtų prie su verslo saugumu susijusių sprendimų ir tai atskleidžia šios temos aktualumą.

Tyrimo problematika. Poreikis tirti grindžiamas reikšmingu kibernetinio saugumo rizikos poveikiu visų verslo funkcijų valdymui technologinių transformacijų kontekste. Kadangi duomenų ir informacijos dalijimasis bei jungimasis į įvairius tinklus tampa viena iš verslo sėkmės prielaidų, kibernetinio saugumo rizikos valdymo problema negali būti sprendžiama lokalios organizacijos kontekste, nes dažna jų veikia tarpusavyje susijusiuose tinkluose. Kibernetinio saugumo rizikos problemą siūloma spręsti integruojant ją į vidaus kontrolės valdymo dalį, kurią geriausiai gali įvertinti įmonės vidaus auditas (Gordon ir kt., 2008; Haapamäki ir Sihvonen, 2019). Vidaus auditu, atsižvelgiant į kibernetinio saugumo rizikos suvaldymui skiriamų sąnaudų ir gaunamos naudos analizę, vidaus kontrolės vertinimą ir informacijos atskleidimo politiką galima objektyviai įvertinti kibernetinio saugumo rizikos būklę organizacijoje. Tai rodo Ahia ir Deloitte (2017) atliktas tyrimas, kuriame vidaus audito, kaip nepriklausomo užtikrinimo teikėjo, vaidmuo vertinamas būtinu patikimai

kibernetinio saugumo rizikai nustatyti ir valdyti bei užtikrinti įmonės saugumo ir atsparumo priemones. Mokslinėje literatūroje (Ghandge ir kt., 2020; Grody, 2020; Islam ir kt., 2018; Steinbart ir kt., 2013; Steinbart ir kt., 2018; Wallace ir kt., 2011) galima rasti pirmųjų tyrimų apie kibernetinio saugumo ir vidaus audito funkcijų bendradarbiavimo teikiamą naudą, tačiau šiuose tyrimuose pasigendama konkrečių metodų pavyzdžių, kurie leistų įvertinti esamą organizacijų kibernetinio saugumo rizikos būklę vidaus audito metu ir pagal ją nustatyti kibernetinio saugumo užtikrinimo galimybes bei tobulintinas sritis. Vadovybės atsakomybė už visų organizacijai keliamų rizikų supratimą ir suvaldymą bei rizikos poveikis verslo veiklos tęstinumui skatina mokslininkus ieškoti naujų sąsajų tarp kibernetinio saugumo rizikos ir vidaus audito. Vertinimo metodų trūkumas patvirtina šio tyrimo poreikį ir problematiką.

Tyrimo problema – kaip įvertinti organizacijų kibernetinio saugumo riziką vidaus audito procedūrose?

Tyrimo objektas – kibernetinio saugumo rizikos vertinimas vidaus audito procedūrose.

Tyrimo tikslas – pasiūlyti ir empiriškai patikrinti konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį.

Tyrimo uždaviniai:

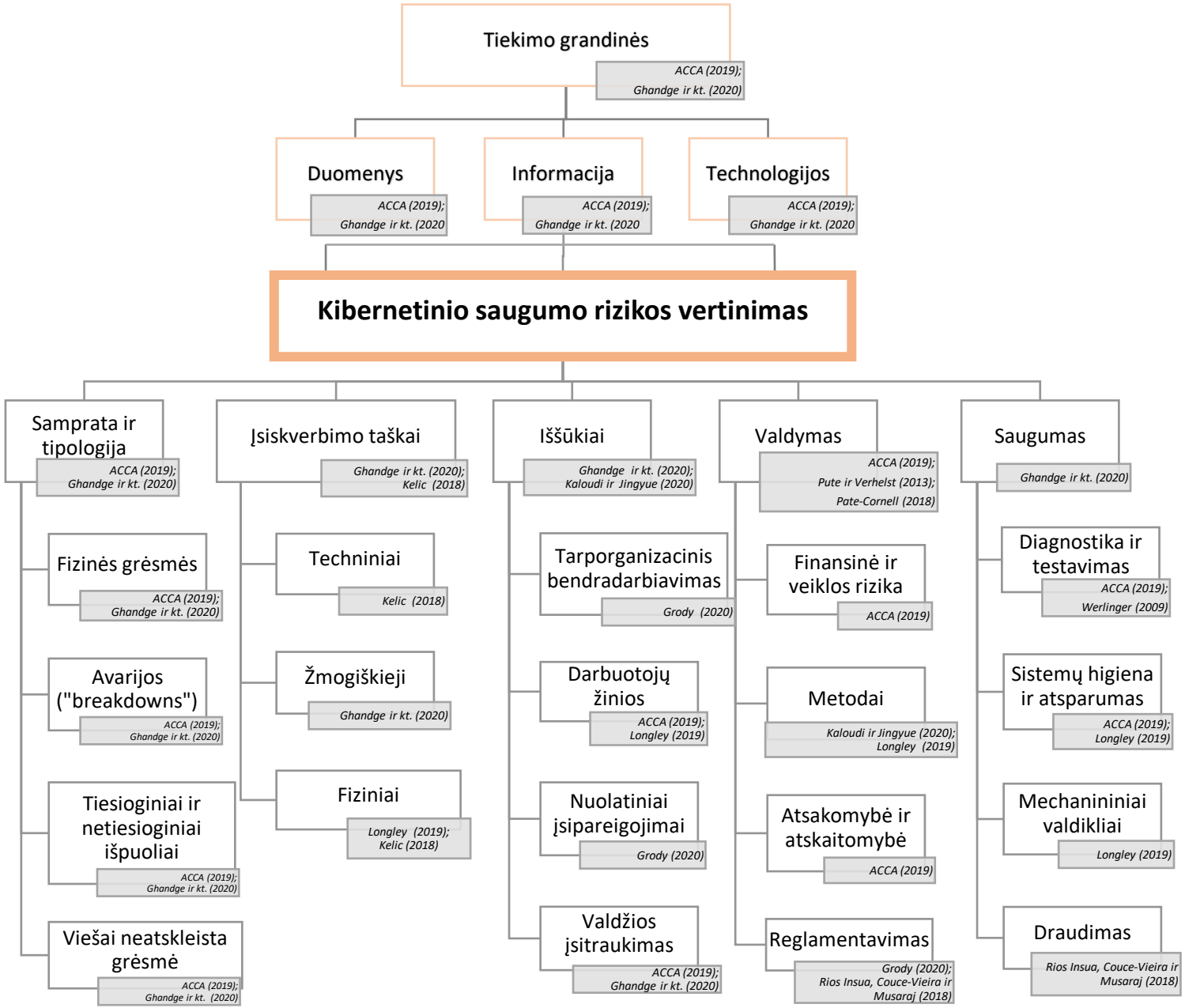
1) Atskleisti kibernetinio saugumo rizikos sampratą ir jos vertinimo vidaus audito procedūrose problematiškumą;

2) Sudaryti konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį;

3) Pasiūlyti kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio empirinio tyrimo metodologiją;

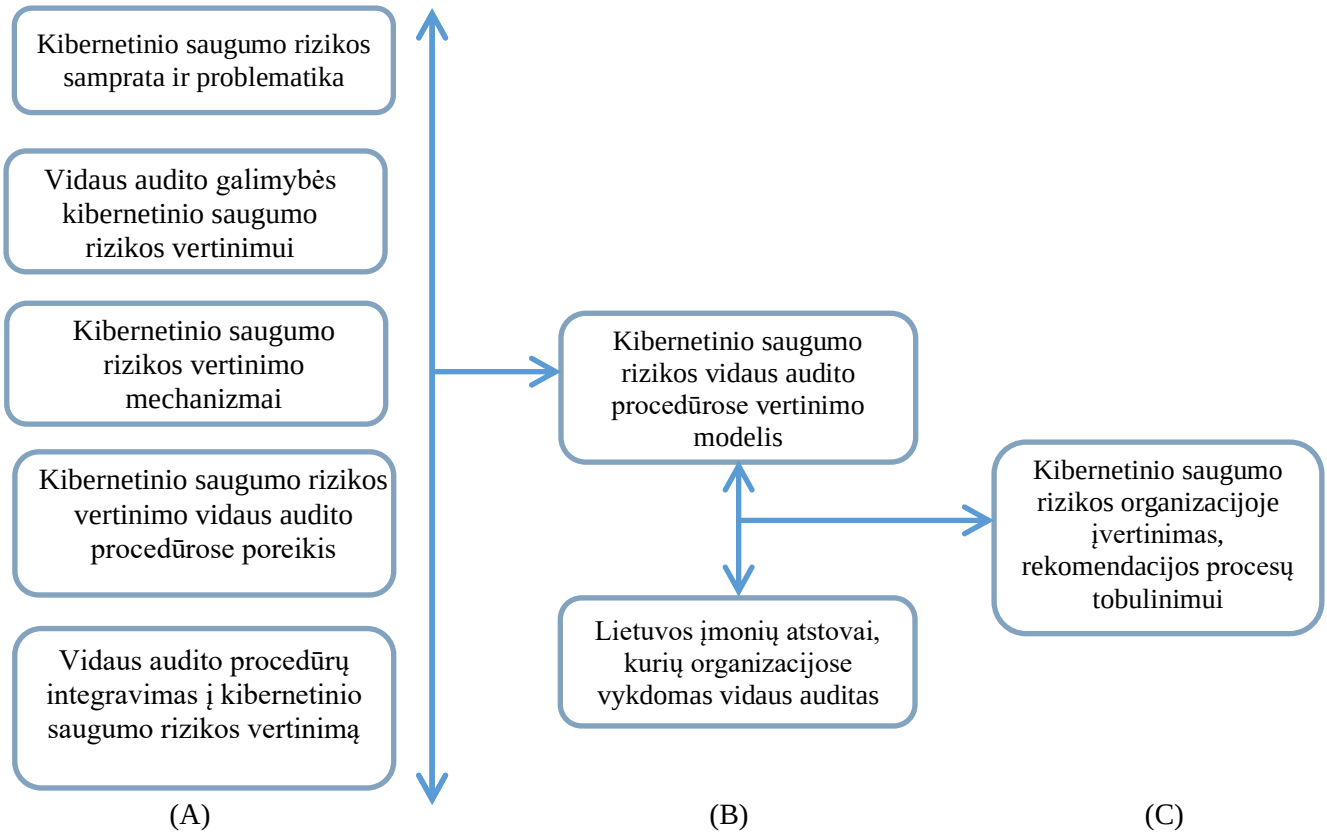
4) Atlikti empirinį pasiūlyto kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio tyrimą, nustatyti organizacijų kibernetinio saugumo rizikos lygį ir pateikti pasiūlymus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimui.

Darbo metodai. Mokslinės problemos suformulavimui ir konceptualaus teorinio modelio pagrindimui projekte naudojamas mokslinės literatūros analizės metodas. Praktinėje tyrimo dalyje konceptualaus modelio įvertinimui organizacijose naudojami pusiau struktūruoto interviu ir atvejų studijos metodai, gauti rezultatai analizuojami taikant lyginamąją analizę.



1 pav. Hierarchinė literatūros žemėlapio schema (sudaryta autorės)

Tyrimo struktūros schema: tyrimo struktūros schema sudaryta iš 3 dalių: A, B ir C (2 pav.).



2 pav. Tyrimo struktūros schema (sudaryta autorės)

1. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo problemos analizė

1.1. Kibernetinio saugumo rizikos samprata ir vidaus audito galimybės jos nustatymui

Šiandien pasaulinė verslo aplinka verčia organizacijas visuose pramonės sektoriuose turėti saugią skaitmeninę infrastruktūrą komerciniams sandoriams. Ši, tarpusavyje susijusi pasaulinė skaitmeninė infrastruktūra, yra vadinama kibernetine erdve, kurią sudaro internetas, kompiuterinės sistemos, mašininė, programinė įranga ir paslaugos bei visa organizacijų skaitmeninė informacija (Caliyurt, 2020). Šios priemonės leidžia sėkmingai veikti elektroninei prekybai, elektroninės valdžios vartų paslaugoms ir informacijos dalijimuisi (Kahyaoglu ir Caliyurt, 2018). Žvelgiant iš technologinės perspektyvos interneto ryšys, prietaisai ir jų naudojimo būdai – kompiuteriai, namų tinklai, išmanieji skaitikliai, debesijos kompiuterija ir socialiniai tinklai – šiandienos kibernetinę erdvę gerokai pakeitė nuo praeities (ACCA, 2019).

Didėjantis skaitmeninių technologijų naudojimas sukūrė naujos valdymo rizikos – kibernetinio saugumo – vaidmenį organizacijų veiklos procesams. Masiniai kibernetinio saugumo rizikos pažeidimai tapo įprastais, reguliariai aptariamais naujienų portalų antraštėse, nerimą keliančiais tiek vartotojams, tiek organizacijų vadovams (Amir, Levi ir Livne, 2018). Daugelis organizacijų visame pasaulyje vis dar stengiasi suvokti ir valdyti kylančias kibernetinio saugumo rizikas vis sudėtingesnėje skaitmeninėje visuomenėje. Kadangi priklausomybė nuo duomenų ir tarpusavio ryšiai bendrame tinkle nuolat plečiasi, atsparumo ugdymas, siekiant atlaikyti kibernetinius sukrėtimus – tai yra didelio masto įvykius, turinčius plačias trikdomas pasekmes – dar niekada nebuvo toks svarbus (AICPA, 2018). Didžiosios Britanijos vyriausybės saugumo pažeidimų tyrimas parodė, kad saugumo pažeidimų skaičius nuo 81 proc. didelėse organizacijose padidėjo iki 90 proc., nurodydamas, kodėl saugumo pažeidimai laikomi tęstiniais ir kurių negalima visiškai išnaikinti (PWC, 2017). Kita apklausa taip pat parodė, kad devynios iš dešimties apklaustų didelių organizacijų dabar kenčia nuo tam tikrų saugumo pažeidimų formų, o tai rodo, kad šie incidentai dabar yra beveik neišvengiami (Kahyaoglu ir Caliyurt, 2018).

Kibernetinio saugumo sąvoka dažnai naudojama kaip analogiškas informacijos saugumo terminas, tačiau reikėtų vertinti jį plačiau, kibernetinis saugumas – tai ne tik kibernetinės erdvės, bet ir joje veikiančių asmenų, bei jų valdomo turto, kurį galima pasiekti virtualioje erdvėje, apsauga (Von Solms ir Van Niekerk, 2013). ACCA (2019), Ghandge, Weiβ, Caldwell ir Wilding (2018) tyrimai atskleidė, kad kibernetinio saugumo rizikos grėsmė apima visus duomenis, informaciją ir technologijas, kurias galima rasti bet kurios organizacijos tiekimo grandinėse. Tradicinė tiekimo grandinė – tai kelias, kuriuo vyksta prekės, paslaugos, finansų ir informacijos judėjimas. Kibernetinė tiekimo grandinė – informacinių technologijų infrastruktūros ir technologijų tinklas, naudojamas duomenims sujungti, kurti ir dalintis virtualiuose tinkluose, todėl yra galimybė atsirasti naujiems pavojams, nesusijusiems su fiziniais produktais ar konkrečia fizine veikla (Ghandge ir kt., 2018). Pagrindinį skirtumą tarp kibernetinės ir įprastos rizikos Renauld ir kt. (2018) įvardina šios rizikos anonimiškumą, nes ji gali būti neaptinkama, kol nesutrikdys verslo funkcijų. Dėl šios priežasties galima daryti išvadą, kad kibernetinio saugumo rizika yra viso verslo rizika, todėl svarbu vertinti ne tik atskirus tiekimo grandinės elementus, bet ir jų sąveiką, bei daromą poveikį vienas kito ir visos grandinės atžvilgiu.

Minėtuose šaltiniuose – ACCA (2019), Ghandge ir kt. (2018) taip pat buvo apžvelgta kibernetinio saugumo samprata ir tipologija. Šioje sampratoje pokyčiai lėti – vis dar dauguma organizacijų mano, kad kibernetinis saugumas yra tik informacinių technologijų (IT) specialistų atsakomybė ir darbas,

nors dauguma nagrinėtų tyrimų literatūros šaltiniuose rodo, kad kibernetinė rizika daro įtaką visiems organizacijos nariams. Darbuose išskirti penki kibernetinės rizikos tipai:

- *fizinės grėsmės*, kurias sudaro materialūs daiktai (serveriai, maršrutizatoriai, kiti įrenginiai); taip pat stichinės nelaimės, teroristiniai išpuoliai ar tyčinis fizinės infrastruktūros sugadinimas arba vagystė;
- *avarijos* – dar kitaip vadinamos "nulaužimais", susiję su tinklapių netipine veikla, pasenusiais atnaujinimais, tinklų gedimais dėl duomenų srauto ir pan.;
- *tiesioginiai išpuoliai* – apima įsilaužimus, paslaugų atsisakymą, slaptažodžių šnipinėjimą siekiant finansinės naudos, kompromisų riziką intelektinei nuosavybei ar patyrus ataką;
- *netiesioginiai išpuoliai* – tai virusai, padirbti produktai, "minkšta" programinė įranga, kenkėjiški produktai;
- *viešai neatskleista (vidinė) grėsmė* – tai kibernetinė grėsmė, kylanti dėl darbuotojų kaltės, kuri gali būti vidinė, tyčinė arba atsitiktinė (slaptažodžių įsiminimas, slaptos informacijos aptarimas su kolegomis, sąmoningas neskelbtinos informacijos atskleidimas). Tiek aplaidi, tiek apgalvota darbuotojo sukelta kibernetinio saugumo grėsmė laikoma didžiausia ir labiausiai nenuspėjama.

Visos šios rizikos patekę į organizaciją per įsiskverbimo taškus (jie gali būti techniniai, žmogiškieji ir fiziniai) sukuria rizikos valdymo ir saugumo iššūkius, kuriems turi būti skiriamas vis didesnis ir daugiau išteklių reikalaujantis dėmesys. Pagal Anderson ir kt. (2017) penki labiausiai paplitę kibernetinių grėsmių šaltiniai yra šie:

- nacionalinės valstybės;
- kibernetiniai nusikaltėliai;
- įsilaužėliai;
- viešai neatskleista informacija;
- paslaugų teikėjai bei nekokybiškų produktų ir paslaugų kūrėjai.

Moksliniuose literatūros šaltiniuose kibernetinio saugumo ir kibernetinio saugumo rizikos apibrėžimai skiriasi, tačiau visi yra susiję su organizacijų vertės kūrimu arba jos išsaugojimu (1 lentelė). Įvairių priemonių taikymas saugumo užtikrinimui ir pagrindiniai procesai išorinei ir vidinei rizikai nustatyti yra integruotas procesų, susijusių su infrastruktūra, informacinių technologijų sistemomis ir organizacijos valdymu, derinimas. Sudarius pirminę hierarchinę literatūros žemėlapio schemą (1 pav.) buvo nustatyta, kad procesų derinimas yra labai svarbus kibernetinio saugumo užtikrinimui, o pavienės taikomos priemonės esminių rezultatų ir pokyčių rinkoje neduos. Tai, kad tiekimo grandinėse veikiančios susijusios šalys turėtų užtikrinti didesnį skaidrumą tarpusavio kibernetinio saugumo srityje ir kartu bendradarbiauti derinant turimas žinias ir išteklius patvirtino Rongping ir Yonggang (2014) tyrimas.

Apie tai, kad kibernetinio saugumo rizikos problemos negali būti lengvai išspręstos rinkos pastangomis ir reguliavimu teigiama ir Haapamäki ir Sihvonen (2019) literatūros analizės tyrime. Tam reikalingas suinteresuotųjų šalių (įmonėse dirbančių skirtingų sričių specialistų) grupės bendras sprendimų derinys, kuris turi potencialų vaidmenį koordinuojant saugumo funkcijų rinkinį pasiekti priemones, kurios bendrai lemtų veiksmingą kibernetinio saugumo politiką. Šiuo atžvilgiu, vidaus audito funkcija tampa labai svarbi ir turėtų būti vertinama, kaip neatsiejama kibernetinio saugumo užtikrinimo proceso dalis (Kahyaoglu ir Caliyurt, 2018). Tai patvirtina ir visuotiniame technologijų vadove pagal Anderson ir kt. (2017) aprašytos kibernetinio saugumo gynybos linijos:

1. *Duomenų, procesų, rizikos ir kontrolės valdymas*. Ši funkcija dažnai tenka sistemų administratoriams ir kitiems, už organizacijos turto apsaugą, atsakingiems darbuotojams;
2. *Rizikos, kontrolės ir priežiūros funkcijų užtikrinimas*. Atsakingos už tai, kad funkcionuotų pirmosios eilės procesai ir kontrolė. Šios funkcijos gali apimti grupes, atsakingas už efektyvaus rizikos valdymo užtikrinimą ir rizikų bei grėsmių stebėjimą kibernetinio saugumo erdvėje (Ames ir kt., 2016);
3. *Vidaus audito funkcija.* Ši suteikia organizacijos vadovybei nepriklausomą ir objektyvų valdymo, rizikos ir kontrolės užtikrinimą. Tai apima pirmosios ir antrosios gynybos linijų vykdomas veiklas, skirtas valdyti ir sumažinti kibernetinio saugumo riziką ir grėsmes bei bendrą veiksmingumą.

Apie tai, kokią įtaką vidaus audito funkcija gali turėti kibernetinio saugumo rizikos sumažinimui, nagrinėjo nedaug mokslininkų. Stafford ir kt. (2018), atliktame vartotojų elgsenos pažeidinėjant kibernetinio saugumo reguliavimo direktyvas tyrime, nustatė būdus, kuriais vidaus auditorius gali padėti užtikrinti su saugumu susijusias vartotojų pasitenkinimo problemas. Jų išvados parodė, kad įmonės kibernetinio saugumo rizikos valdymui naudingas auditas, kurio metu nustatomos technologijas naudojančių vartotojų žinios ir kompetencijos bei jų įtaka kibernetinio saugumo užtikrinimui. Vadovų įsitraukimas ir parama svarbi tiek kibernetinio saugumo rizikos vertinimui, tiek vidaus audito funkcijai organizacijoje užtikrinti (Islam ir kt., 2018). Jų teigimu, visapusiškas kibernetinio saugumo rizikos įvertinimas, atliekamas vidaus auditorių turi reikšmingą teigiamą poveikį kibernetinio saugumo užtikrinimui.

Steinbart ir kt. (2012) teigia, kad kibernetinio saugumo ir vidaus audito funkcijos organizacijose privalo veikti sinergiškai, nes kibernetiniu saugumu besirūpinantys darbuotojai kuria, įgyvendina ir taiko įvairias procedūras ir technologijas, siekdami apsaugoti organizacijos informacinius išteklius, o vidaus audito specialistai teikia periodinį grįžtamąjį ryšį apie šios veiklos efektyvumą bei siūlo pakeitimus ar tobulinimo pasiūlymus. Audito funkcija yra konsultuoti ir tobulinti, o valdymo funkcijos vaidmuo – ieškoti ir priimti vidaus audito rekomendacijas kibernetinio saugumo gerinimo klausimais (Stafford ir kt., 2018).

Tarp pagrindinių veiksnių, kurie daro įtaką vidaus audito ir kibernetinio saugumo funkcijų sąveikai, įvardijami šie: vidaus auditoriaus kompetencijų, susijusių su kibernetinio saugumo valdymu, rizika bei kontrole, lygis (Islam ir kt., 2018), bendravimo lygis, informacinių technologijų žinių kiekis, taip pat vidaus auditoriaus požiūris (vaidmens organizacijos visumoje suvokimas). Tęsdami ankstesnį tyrimą Steinbart ir kt. (2013) patvirtino, kad šių sričių bendradarbiavimo santykių užtikrinimas teigiamai susijęs su vidaus audito teikiamos vertės suvokimu ir bendro organizacijos kibernetinio saugumo efektyvumu. Paskutiniame Steinbart ir kt. (2018) šios temos tyrime teigiamai įvertintas bendradarbiavimo kokybės santykis su praneštų vidaus kontrolės trūkumų ir neatitikimų atvejų skaičiumi (vertinant pagal nustatytus kibernetinių incidentų skaičius prieš ir po to, kai buvo padaryta žala organizacijai).

Apibendrinant galima teigti, kad vidaus audito funkcija kibernetinio saugumo vertinime yra naujas saugumo aspektas ir nors šiuo metu trūksta platesnių atliktų mokslinių tyrimų šia tema, organizacijų vadovai turi įvertinti galimą jo naudą ir pagerinti jo procedūrų užtikrinimą. Poreikis vidaus audito metu įrodyti organizacinės kibernetinio saugumo politikos veiksmingumą ir vientisumą, išsaugoti duomenų konfidencialumą ir prieigos prieinamumą kuria prielaidas naujiems tyrimams, vertinantiems kibernetinio saugumo riziką vidaus audito procedūrose.

1 lentelė. Kibernetinio saugumo ir kibernetinio saugumo rizikos sąvokų apibrėžimai (sudaryta autorės)

Perspektyva	Sąvokos apibrėžimas	Autoriai
Kibernetinis saugumas *(*angl. *cyber security)*	Kibernetinis saugumas nėra tik turto apsaugos, programinės įrangos atnaujinimo ir naujausios apsaugos nuo virusų užtikrinimas, tai yra verslo problema, kuri gali sukelti didelę organizacijos reputacijos žalą ir finansinius nuostolius.	*ACCA (2019)*
	Kibernetinis saugumas – tai keturių pagrindinių tikslų – vientisumo, prieinamumo, konfidencialumo ir atskaitomybės – konkretus įgyvendinimas.	*Ghandge ir kt. (2018)*
	Kibernetinis saugumas – visuma, apimanti informacijos saugumą ir jos užtikrinimą. Informacijos saugumas yra susijęs su informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimu. Kibernetinis saugumas – technologijų, procesų ir praktikos rinkinys, saugantis ir užtikrinantis organizacijos turto, pavyzdžiui, informacijos ir sistemų, apsaugą.	*No ir Vasarhelyi, (2017)*
	Kibernetinis saugumas – informacijos ir jos kritinių savybių (konfidencialumo, vientisumo ir prieinamumo), įskaitant sistemas, apsaugą ir aparatinę įrangą, kuri naudoja, kaupia ir perduoda informaciją, taikydama politiką, mokymo ir informavimo programas bei technologijas.	*Whitman ir Mattord (2011)*
	Kibernetinis saugumas – apsauga nuo elektroninių išpuolių, vykdomų per kompiuterines sistemas, pradedant nedidelio masto elektroninio pašto suktybėmis ir baigiant sudėtingomis didelio masto atakomis, turinčiomis įvairių politinių ir ekonominių motyvų.	*Houses of Parliament (2011)*
	Kibernetinis saugumas – svarbiausia technologinė rizika, kuriai reikalinga vis didesnė kontrolė.	*Anderson ir kt. (2017)*
Kibernetinio saugumo rizika *(*angl. *cyber security risk)*	Kibernetinio saugumo rizika – tai finansinių nuostolių, veiklos sutrikimų ar žalos organizacijos reputacijai rizika, atsirandanti dėl tam tikrų jos informacinių technologijų sistemų gedimų. Kibernetinio saugumo rizika – rizika, susijusi su veikla internete, prekyba internetu, elektroninėmis sistemomis ir technologiniais tinklais, taip pat su asmens duomenų saugojimu.	*PWC (2017)*
	Kibernetinio saugumo rizika – rizika, turinti įtakos įmonės finansiniams nuostoliams, užsakymų vėlavimui ir trumpalaikiam klientų aptarnavimo praradimui, taip pat visai organizacijos rinkos vertei ir prekės ženklo reputacijai ilgalaikėje perspektyvoje.	*Ghandge ir kt. (2018)*

1.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo problematika

Technologijos vaidina svarbų vaidmenį pasaulio vyriausybių, bankų, valstybinių ir privačių organizacijų veikloje, siekdamos patenkinti kasdienius šių vartotojų poreikius. Technologijų dėka automatizuojami organizacijų veiklos procesai kuria geresnę darbo prieigą ir ryšį, mažina klaidų tikimybę, spartina informacijos mainus. Su šiomis vystymosi galimybėmis taip pat susijusi duomenų saugumo grėsmė – šios technologijos dažnai tampa kibernetinių atakų taikiniu. Dabartinėje rinkoje esantys kibernetinio saugumo užtikrinimo priemonių sprendimai yra sukurti žinomoms kibernetinių atakų rūšims ir suteikia „vieno taško“ gynybos mechanizmus, o tai reiškia, kad apsaugo vieną įrenginį arba jų sistemą. Norint apsaugoti visą organizaciją – reikalingi patyrę kibernetinio saugumo specialistai, kurie gali sukurti sudėtingus, visos organizacijos procesus apimančius, gynybos mechanizmus, skirtus kibernetinėms atakoms išvengti, aptikti ir pašalinti. (No ir Vasarhelyi, 2017). Kadangi kibernetinio saugumo grėsmę keliančios priemonės tobulėja kartu su reikalingų jos apsaugai

technologijų vystimusi, šis procesas turi būti nuolat peržiūrimas ir atnaujinamas, vystomos naujos priemonės, priimami kiti saugumo valdymo sprendimai.

Kahyaoglu ir Caliyurt (2018) savo ataskaitoje išskiria pastaruoju metu, organizacijose vyraujančius keturis pagrindinius reikalavimus, kuriais užtikrinami kibernetinio saugumo rizikos klausimai:

1. *Daugiašalis požiūris:* dėmesys skiriamas kibernetinio saugumo užtikrinimo reglamentavimui skirtingose šalyse, įskaitant iniciatyvas, kuriomis siekiama suderinti elektroninius nusikaltimus reglamentuojančius teisės aktus ir skatinti griežtesnes baudžiamąsias nuobaudas bei pagerinti elektroninės prekybos įstatymus visame pasaulyje. Atskiros šalys turėtų susitarti dėl bendrų principų ir normų saugumo gerinimui taikymo ir tinkamai jų laikytis (Butler ir Lachow, 2012);
2. *Saugi informacinė sistema:* saugios informacinės sistemos laikomos veiksminga kibernetinio saugumo rizikos atsparumo dalis. Galligan ir kt. (2015) informacinę sistemą apibūdina kaip žmonių, procesų, duomenų ir (arba) technologijų rinkinį, kuris organizacijai suteikia galimybę gauti ir teikti operacijas, tinkamai naudoti ir perduoti informaciją, išlaikyti reikiamą atskaitomybę ir įvertinti bei peržiūrėti įmonės veiklą ir pažangą. Pagal saugios informacinės sistemos reikalavimus, daugiašalės iniciatyvos siekia užkirsti kelią piktavališkam internetinės erdvės naudojimui, o organizacijų vadovai skatinami saugesnių sistemų pasirinkimui ir naudojimui bei geresniam saugumo valdymui organizacijos viduje. Saugios informacinės sistemos gerina informacijos saugumo valdymą tiek viešajame, tiek privačiame sektoriuose, kuria naujas teisines ir technologines iniciatyvas (Kahyaoglu ir Caliyurt, 2018);
3. *Bendradarbiavimo nauda*: aptinkami atskirų organizacijų bendradarbiavimo mechanizmai, kurie leidžia iš anksto įspėti apie galimą kibernetinio saugumo pavojų. Daugiašalės iniciatyvos, skirtos nustatyti kenksmingą kibernetinės erdvės naudojimą, apima sustiprintų bendradarbiavimo saugos mechanizmų sukūrimą, siekiant iš anksto įspėti apie kibernetines atakas keičiantis informacija tarp viešojo ir privataus sektorių;
4. *Krizių valdymo programa*: daugiašalės iniciatyvos, skirtos reaguoti į piktavališką kibernetinės erdvės naudojimą, apima pastangas sukurti tvirtą informacinę infrastruktūrą, krizių valdymo sistemą, gerinti policijos ir baudžiamosios teisėsaugos koordinavimą.

Yra keletas svarstymų, kodėl auditoriai turėtų būti įtraukti į kibernetinio saugumo rizikos valdymą. Pirmasis yra apie tai, kad kibernetinio saugumo rizika gali turėti didelį poveikį ekonominei organizacijos būklei. Tai gali būti plataus masto ataka, kuri, tikėtina, paveiks įmonės veiklos tęstinumą (No ir Vasarhelyi, 2017). Pagal prognozes yra skaičiuojama, kad kibernetinis nusikalstamumas 2021 metais pasaulio ekonomikai kainuos šešis trilijonus dolerių per metus. Lyginant su 2015 metais, tai trijų trilijonų padidėjimas, todėl kibernetinis saugumas tampa pelningesnis net už prekybą visais nelegaliais narkotikais kartu sudėjus. Įmonėms tai – reikšminga ir brangiai kainuojanti grėsmė. Kibernetinio nusikalstamumo kainą sudaro duomenų naikinimo, piniginių nuostolių, prarastos produkcijos, asmeninių ir finansinių duomenų vagysčių, išlaidų atsigavimui po išpuolio ir reputacijos žalos patirti nuostoliai (ACCA, 2019).

Antra, auditoriaus kompetencija techninėje srityje vis dar kelia klausimų. Teigiama, kad dabartiniai vidaus auditoriai nėra apmokyti ir išbandyti kibernetinio saugumo klausimais, tačiau jų turimos analitinės įžvalgos ir įmonės veiklos procesų suvokimas, pritaikius tinkamas kontrolės priemones, gali padėti laiku imtis rizikos saugumo priemonių (Amin ir Mohamed, 2016). Nemažai atestuotų auditorių turi papildomas kvalifikacijas patvirtinančius sertifikatus, tokius kaip – informacinių

sistemų auditoriaus (angl. *certified information system auditor (CISA)*) arba informacinių sistemų saugumo specialisto (angl. *certified information systems security professional (CISSP)*), tačiau auditorių, turinčių pakankamus įgūdžius organizacijose, skaičius nėra pakankamas (No ir Vasarhelyi, 2017).

Atitinkamų, kibernetinio saugumo ir vidaus audito, darbuotojų įgūdžių ir vadovų žinių trūkumas dar labiau pablogina kibernetinio saugumo rizikos vertinimo situaciją. Mokymo kursai, kuriuose daugiausia dėmesio skiriama naujų technologijų naudojimui, virtualių komandų kūrimui ir valdymui bei elektroninių nusikaltimų prevencijos priemonėms, turi tapti didesne šiuolaikinių verslo struktūrų dalimi (Lois ir kt., 2020). Longley (2019) savo tyrime aprašė darbuotojų žinių trūkumų pasekmes, kai daugelyje šalių trūksta tinkamos kvalifikacijos kibernetinio saugumo specialistų, tačiau atkreipiamas dėmesys, kad tai neturi būti pasiteisinimas neinvestuoti į reikalingus išteklius kibernetinei rizikai suvaldyti.

Trečia, vidaus auditoriai atlieka svarbiausią vadovo pagalbininko vaidmenį – vertina sistemos efektyvumą ir pateikia vadovui jos veikimo užtikrinimą, taip pat yra tarpininkai tarp darbuotojų ir vadovų, galintys siūlyti problemos sprendimų būdus. Kaip teigia savo tyrime No ir Vasarhelyi (2017) be vidaus auditorių nebūtų kam atlikti finansinės ir kibernetinio saugumo rizikos informacijos integravimo į tam tikrą saugumo užtikrinimo formą. Be to, būsimų auditų rizikos vertinimo dalies negalima atlikti neatsižvelgiant į kibernetinio saugumo riziką, todėl reikalingi išsamūs tyrimai, kaip integruoti bendrai kokybinius kibernetinio saugumo rizikos klausimus į tradicinį audito modelį.

Darbuotojų žinių trūkumas reikšmingai susijęs su atskaitomybe ir atsakomybe (ACCA, 2019), valdžios įsitraukimu (Ghandge ir kt., 2018) bei kibernetinio saugumo rizikos valdymo reglamentavimu (Grody, 2020; Rios Insua, Couce-Vieira ir Musaraj, 2018), kuris šiandien egzistuoja nedaugelyje šalių ir tik kaip vietinės – nacionalinės rekomendacijos ar standartai. Neteisingai paplitęs požiūris, susijęs su reguliavimo standartais yra tas, kad organizacijos mano, jog įgijus kibernetinio saugumo akreditaciją, organizacija visada atitiks reikalaujamus standartus, todėl įmonės skiria mažai dėmesio ir išteklių procesų tobulinimui. Naujosios technologijos taip pat keičia informacijos valdymo būdą, todėl reikalingi nauji ir nuolatiniai sprendimai valdymo sistemoms prižiūrėti. Šiandien kibernetinio saugumo rizika kelia pavojų organizacijų reputacijai, įmonės veiklos ir finansiniam stabilumui. Duomenų apsaugos poreikis formuoja naujų audito uždavinius, kuriuos įtvirtina Bendrasis duomenų apsaugos reglamentas (BDAR) bei Tarptautiniai Vidaus audito profesinės praktikos standartai (TVAPPS) (Lois ir kt., 2020).

Atskiros šalys ar net atskiros pramonės šakų grandinės turi savo sukurtus kibernetinio saugumo rizikos valdymo modelius, kurie galioja tik jiems vieniems. Tyrimai rodo, kad tai neturi teigiamos įtakos nei modelius taikančioms organizacijoms, nei bendram šalies kibernetiniam saugumui (Paté-Cornell ir kt.). Tai turėtų tapti viso pasaulio bendrais reglamentavimo dokumentais, kurie nurodytų kibernetinės saugumo rizikos valdymo vertinimą vienijančius metodus, kuriais būtų galima ne tik laiku diagnozuoti rizikas (Werlinger ir kt., 2009), tačiau jas palyginti tarp organizacijų ar skirtingų šalių bei padėtų saugumą užtikrinti atsparumą gerinančiomis priemonėmis (Longley, 2019).

Kibernetinio saugumo rizikos didėjimas tapo vienu svarbiausių iššūkių organizacijoms. Taip, kaip prieš dešimtmetį vidaus audito funkcijos prisitaikė prie informacinių technologijų (IT) poveikio verslo procesams pokyčių, taip šiandien vidaus auditas susiduria su būtinybe pašalinti su kibernetinio saugumo rizika kylančias grėsmes. Siekdama išvengti kibernetinių grėsmių kiekviena organizacija

turėtų įgyvendinti organizacijos kibernetinio saugumo programą arba kibernetinio saugumo strategiją, kuriai įvertinti, reikalingas vidaus audito procedūrų užtikrinimas.

2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio teoriniai sprendimai

2.1. Kibernetinio saugumo rizikos vertinimo mechanizmai

Mokslinėje literatūroje, analizuojančioje kibernetinio saugumo rizikos vertinimą, egzistuoja daugybė mechanizmų ir operacijų, kurios palaiko kibernetinio saugumo užtikrinimą. Kai kuriais atvejais, ypač mažesnėms įmonėms, atliekant kibernetinio saugumo rizikos vertinimą gali būti tinkama tam tikra išorės konsultacija, nes kibernetinio saugumo rizikos vertinimas dažnai priklauso nuo organizacijos turimos patirties interpretuojant reikalavimus, efektyviai apskaičiuojant rodiklius, kuriant saugumo užtikrinimo metodus ir įrankius bei galutinai pranešant apie kibernetinio saugumo būklę (Evans ir kt., 2016).

Tam, kad būtų išvengta didelių grėsmių, siekiama įvertinti pagrindines kibernetinio saugumo riziką apibūdinančias procedūras: kibernetinio saugumo rizikos nustatymą, valdymą, reagavimą , saugumo užtikrinimą ir vidaus auditą. Kibernetinio saugumo rizikos vertinimai turėtų būti reguliariai peržiūrimi vadovybės ir audito komiteto vadovų, siekiant užtikrinti, kad atsakomybė ir atskaitomybė būtų aiškiai suprantama, o grėsmės lygis – tinkamai valdomas ir jam skiriama pakankamai išteklių (Kahyaoglu ir Caliyurt, 2018).

Kibernetinio saugumo rizikos nustatymas. Tai pirmasis veiksmingos kibernetinio saugumo rizikos valdymo etapas (Chong, Y. Y., 2013). Pagal ACCA (2019), vertinant kibernetinio saugumo riziką visoje organizacijoje, reikia atsižvelgti į keletą veiksnių, kurie turi apimti:

- turto, kuriam reikia apsaugos, nustatymą – turėtų būti išskiriamas tas, kuris turi didžiausią strateginę vertę organizacijai;
- atitinkamų grėsmių ir silpnybių nustatymą;
- pažeidžiamumų (silpnųjų vietų) nustatymą;
- grėsmės lygio, kurį kelia tie, kurie nuotoliniu būdu naudojasi organizacijos sistemomis, įvertinimą;
- verslo poveikio nustatymą (jei grėsmės realizuojamos);
- saugumo rizikos vertinimo parengimą;
- organizacijos priimtino rizikos lygio įvertinimą;
- tinkamų kontrolės mechanizmų nustatymą.

Kibernetinio saugumo rizikos valdymas. Gordon ir kt. (2015) pasiūlė efektyvaus kibernetinio saugumo rizikos valdymo gaires. Šių gairių ekonominės naudos ataskaitoje buvo lyginamos organizacijų taikomos saugumo valdymo priemonės ir jų teikiama nauda. Tyrimas patvirtino, kad papildomos investicijos į kibernetinio saugumo rizikos valdymo priemones efektyvios tol, kol jų išlaidos neviršija saugumą užtikrinančios naudos. Vėliau, tą patį modelį tobulinę mokslininkai teigė, kad suma, kurią įmonė turėtų išleisti informacijos duomenų apsaugai, turėtų būti tik nedidelė tikėtinų kibernetinių nuostolių dalis

ACCA (2019), Grody (2020), Pate-Cornell ir kt. (2018) tyrimai patvirtino, jog dauguma organizacijų kibernetinį saugumą vertina taktiniu, grėsmėmis pagrįstu lygmeniu, o ne mato kaip strateginę riziką. Dėl šios priežasties, reguliarus ir atsitiktiniais atvejais pagrįstas ataskaitų teikimas dažnai nesugeba pasiekti vadovybės, o tai gali sukelti klaidingą vadovų saugumo jausmą ir požiūrį, jog kibernetinė grėsmė yra pašalinta, tačiau rizika ir pažeidžiamumas nebuvo tikrinami ir vertinami iš verslo perspektyvos. Ataskaitų teikimo svarbą taip pat pabrėžė AICPA (2018), kuri nurodė, kad šių ataskaitų

tikslas yra numatyti priemones, kuriomis organizacijos galėtų perduoti suinteresuotosioms šalims naudingą informaciją, susijusią su kibernetinio saugumo rizikos valdymo programomis. Ataskaitų rengimas vertinamas kaip pirmasis žingsnis, siekiant sudaryti nuoseklų, rinka ir verslo funkcijomis pagrįstą sprendimą, kuriuo organizacijos galėtų tarpusavyje bendradarbiauti.

Ataskaitų teikimo sistema taip pat galėtų padėti įvertinti kitą kibernetinio saugumo valdymo pavojų – „pakopinį“ požiūrį. Organizacijose, kuriose vadovai neskiria pakankamai dėmesio arba turi mažai žinių ir kompetencijų apie kibernetinio saugumo valdymą, įmonės kibernetinės būklės vertinimą gali formuoti trečio lygio asmenys. Šie asmenys dažniausiai yra atsakingi už duomenų saugumą ar finansus, tačiau sistemingai ir visapusiškai neįvertinus įmonės kibernetinio saugumo rizikos pavojaus per įvairias informacinių technologijų sistemas ir tinklus, jų informacinius išteklius, skaitmeninius ryšius, žmones, darbo kultūrą, spręsti apie tikrąją organizacijos kibernetinio saugumo būklę negalima. Proceso pažeidžiamumas (pvz. silpna slaptažodžių politika ar dalijimasis duomenimis su trečiosiomis šalimis) gali sukelti kibernetinio saugumo spragas, o geras kibernetinis valdymas apima visą duomenų gyvavimo ciklą ir įvairius duomenų naudojimo būdus (ACCA, 2019).

Didėjant kibernetinių atakų skaičiui ir augant grėsmės poveikiui reikia gerinti kibernetinio saugumo rizikos valdymą, tačiau didelis finansinių įmonių finansų specialistų kiekybinis tyrimas (ACCA, 2019) atskleidė, kad daugiau kaip pusė respondentų atsakė, jog neturi žinių apie kibernetinio saugumo rizikos valdymą, nežino, kas už tai atsakingas. Pagal Anderson ir kt. (2017) veiksminga kibernetinio saugumo kontrolė apima:

- tvirtą saugumo sistemą;
- didžiausios rizikos, susijusios su kibernetiniu saugumu, nustatymą ir kontroliavimą;
- informacijos apie kibernetinį saugumą programas, skirtas visiems darbuotojams;
- išorinių ir vidinių grėsmių įvertinimą planuojant kibernetinio saugumo programą;
- tvirtą informacijos saugumo valdymą organizacijoje;
- tvirtas reagavimo taisykles rimto kibernetinio saugumo pažeidimo atveju.

Reagavimas į kibernetinio saugumo riziką (atsparumas). Efektyvus valdymas susijęs su didėjančio pažeidžiamumo suvokimu (Lainhart, 2000), todėl kai kibernetinio saugumo rizika yra apsaugota nuo tolimesnio jos plitimo, organizacijos turi sutelkti dėmesį į atsparumo užtikrinimą. Reagavimas į kibernetinio saugumo riziką arba atsparumas sujungia tradicinio atkūrimo po nelaimių planavimo priemones ir verslo tęstinumo valdymą. Gebėjimas greitai reaguoti gali padėti sumažinti finansinę ir reputacijos žalą (ACCA, 2019). Pagal šios tyrimo ataskaitos autorius išskiriami keturi kibernetinio atsparumo nustatymo etapai:

- *Tvarkyti ir apsaugoti*. Daugiausiai dėmesio šiame etape skiriama duomenų ir turto valdymui informacinėse sistemose ir tinkluose. Todėl privaloma parengti organizacijos apsaugos nuo kibernetinių atakų, sistemos gedimų ir neteisėtos prieigos politiką, apimančią žmones, procesus ir technologijas;
- *Nustatyti ir atrasti.* Šiame etape nustatomos organizacijos silpnosios vietos ir jos apsaugojamos naudojant saugos testus bei atliekant pažeidžiamumo nuskaitymo ir įsibrovimo aptikimo procesų vertinimą;
- *Atsakyti ir atkurti*. Etapas apima organizacijos veiklos tęstinumo (užtikrinimo) planus ir reagavimo į kibernetinius incidentus priemones;
- *Valdyti ir užtikrinti.* Šiame etape organizacija turėtų patikrinti, ar ji atitinka teisinius ir norminius reikalavimus. Organizacija turėtų atlikti nuolatinį kibernetinio saugumo rizikos

vertinimą ir pagal šiuos vertinimus tobulinti organizacijos kibernetinio saugumo ilgalaikę programą.

Kibernetinio saugumo užtikrinimas. Kibernetinis saugumas apibūdinamas kaip keturių pagrindinių tikslų – vientisumo, prieinamumo, konfidencialumo ir atskaitomybės – įgyvendinimu (Ghandge ir kt., 2018), kuriuos apibūdina keturi užtikrinimo elementai. Šiais keturiais elementais laikomi vidinis užtikrinimas, išorinis užtikrinimas, įgyvendinimo užtikrinimas ir veiklos užtikrinimas. Kiekvienas elementas yra skirtas pasirinkti tinkamiausią ir subalansuotą procedūrų sprendimų rinkinį ir su jais susijusio patikimumo procesus (Kahyaoglu ir Caliyurt, 2018).

Vidinį užtikrinimą elementą lemia pasitikėjimas gamintojo kuriamo produkto ar teikiamos paslaugos taikomu procesu ir aplinka. Išorinis užtikrinimas apibūdina veiklą, kuri nepriklauso nuo kūrimo aplinkos, yra pasitikima tik produktu, paslauga ar sistema. Tokiu būdu galima analizuoti produktą, sistemą ar paslaugą per pripažintą, nepriklausomą vertinimo schemą, atitinkančią jos funkciją ir numatomą naudojimą. Įgyvendinimo užtikrinimas apima veiklą, užtikrinančią produktų, ar paslaugų diegimo procesus. Galiausiai, veiklos užtikrinimas vertina, kaip veikla, reikalinga produkto ar paslaugos saugos funkcionalumui palaikyti, užtikrinama, kai juo pradedama naudotis. Tai apima nuostatas dėl įmonės veiklos, kuri stebės pažeidžiamumo ir grėsmės pokyčius. Organizacijos pasitikėjimas kontrole turėtų atspindėti užtikrinimo elementų, kurie buvo naudojami užtikrinimui gauti, skaičių. Pavyzdžiui, organizacija labiau pasitikėtų ugniasienės efektyvumu, jei ji būtų gaunama iš patikimo pardavėjo (savaiminė), būtų išlaikiusi nepriklausomą saugumo vertinimą (išorinė) ir ją prižiūrėtų kompetentingi administracijos darbuotojai (įgyvendinimas), nei jei tik viena šių sąlygų būtų išpildoma (Kahyaoglu ir Caliyurt, 2018).

Kritinės infrastruktūros apsauga taip pat priklauso užtikrinimo sričiai. Tai apima sistemų konfigūravimo, kibernetinio saugumo informacijos politikos užtikrinimo ir visapusiško darbuotojų apmokymo užduotis.

2.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo poreikis

Vienintelį saugų būdą reaguoti į kibernetines grėsmes Kahyaoglu ir Caliyurt (2018) mato požiūrį, kurio pagrindu organizacijos kibernetinio saugumo strategija tampa pačio verslo strategija. Nebeužtenka kibernetinio saugumo strategijos laikyti tik informacinių technologijų funkcija. Tai privalo būti vertinama kaip įmonės rizikos problema, kuriai reikalingi visuotinai priimti sprendimai (AICPA, 2018). Reikalinga konsoliduoti verslo strategiją su organizacijos kibernetinio saugumo strategija. Tai labai svarbu, nes taikydamos aiškiai apibrėžtą kibernetinio saugumo strategiją, organizacijos gali efektyviau planuoti, kaip pašalinti dabartines ir būsimas grėsmes, atsižvelgiant į veiklą ribojančius įstatymus, reglamentavimą ir kibernetinio saugumo riziką, būdingą jų verslo šakai (Kahyaoglu ir Caliyurt, 2018). Dėl šios priežasties turi būti sukurta kibernetinio saugumo strategija ir jos valdymo sistema, kuri atitiktų verslą ir būtų pritaikyta jų rizikos pobūdžiui. Be to, turėtų būti apibrėžta verslui reikalingų technologijų kryptis ir nustatytos saugumo galimybės, siekiant pagerinti kritinių operacijų atsparumą, atsižvelgiant į darbuotojus, procesus ir technologijas. Tokiu būdu kuriamas bendras organizacijos požiūris, tenkinantis platesnės verslo misijos ir strateginės vizijos tikslus ir uždavinius. Pathak‘as (2005) vienas pirmųjų savo moksliniuose darbuose tyrė technologijų konvergencijos poveikį įmonės vidaus kontrolės mechanizmams ir nustatė, kad auditorius privalo žinoti apie įmonės saugumui kylančius pavojus, ypač jei jie susiję su finansine ar visa organizacijos

informacine sistema. Jis taip pat pabrėžė, kad technologijų rizikos valdymą ir jo poveikį įmonės vidaus kontrolei bei organizaciniams procesams taip pat turėtų vertinti auditorius.

Nuoseklumo ir aiškumo trūkumas saugumo užtikrinimo dalyje rodo, kad kibernetinio saugumo užtikrinimo programos nėra vienodos, o organizacijų valdymui reikalinga aiški normatyvinių normų hierarchija. Saugumo standartai turėtų suteikti organizacijoms daugiau praktinių patarimų ir numatyti aiškius pažeidžiamumo, susijusio su žmogaus kibernetinio saugumo veiksniais, sprendimų modelius. Šie veiksniai yra labai svarbūs, nes žmogiškumo faktorius laikomas esminiu kibernetinio saugumo elementu, nepaisant to, kad nuolat nesikeičiančios technologijos yra prieinamos užtikrinimo tikslams palaikyti. Žmogaus veikla apima įprastą elektroninių konfidencialių ar neskelbtinų duomenų apdorojimą iki reguliarių techninių pakeitimų diegimo ir patvirtinimo, kurį atlieka informacinių technologijų personalas. Tai – įvairi su kibernetiniu saugumu susijusi būtina veikla, tačiau atskirta nuo pastebimos priežiūros ir saugumo užtikrinimo. Pagrindinė priežastis, kodėl šiuo metu nėra nuoseklios kibernetinio saugumo metodikos, rizikos nustatymo technikos, susijusios su žmogaus elgesiu ir jo pažeidžiamumu yra tai, kad sunku įvertinti ir išmatuoti paslaugos kokybę. Žmogaus patikimumas – tai terminas, naudojamas apibūdinti žmogaus sugebėjimą atlikti tam tikrą užduotį be klaidų tam tikromis sąlygomis ir tam tikru metu (Evans ir kt., 2016).

Kahyaoglu ir Caliyurt (2018) savo tyrime teigia, kad organizacijos turėtų atsižvelgti į greitai besikeičiančios verslo padėties dinamiką, kad galėtų ne tik efektyviai prisitaikyti, bet ir veiksmingai taikyti integruotus požiūrius į kibernetinio saugumo užtikrinimo procesą, remdamosi toliau paaiškinta geriausia praktika:

- *Kibernetinio saugumo suderinimas atsižvelgiant į organizacijos prioritetus*: svarbu užtikrinti kibernetinio saugumo užtikrinimo proceso supratimą visuose verslo padaliniuose, kuris yra gyvybiškai svarbus siekiant organizacijos prioritetų. Norint sustiprinti strateginį bendradarbiavimą ir keitimąsi informacija tarp verslo padalinių ir susijusių darbuotojų kasdienėje darbo aplinkoje, reikia koordinuoti ir suderinti kibernetinio saugumo užtikrinimą su organizacine politika. Kibernetinio saugumo ir funkcijų, kategorijų, standartų ir gerosios praktikos suderinimas su verslo reikalavimais, rizikos tolerancija ir organizacijos ištekliais yra tai, kas lemia organizacijos sėkmę;
- *Kibernetinio saugumo kontrolės sistemos sukūrimas:* dabartinėje verslo aplinkoje organizacijos paprastai turi pasenusią arba neišsamią reagavimo į riziką sistemą ir labiausiai orientuojasi į informacines technologijas (IT). Organizacijos kibernetinio saugumo rizikos valdymą dažniausiai vykdo nereguliariai, kiekvienu atveju atskirai vertinant skirtingas technologines priemones. Remiantis KPMG (2017) tyrimo ataskaita užuot taikius technologinį požiūrį į kibernetinio saugumo įgyvendinimo priemones, rekomenduojama pradėti galvoti apie į vartotoją orientuotą dizainą. Žmogiškasis faktorius buvo, yra ir bus silpniausia grandis, todėl norint pagerinti vartotojų patirtį, reikia siūlyti vientisas, integruotas priemones.

  Kibernetiniai išpuoliai nėra nustatomi stebint vieną įvykį, dažniausiai tai vykdoma taikant kibernetinių duomenų taškų iš kelių šaltinių kaupimo ir koreliacijos procesą per tam tikrą laikotarpį (Galligan ir kt., 2019). Tai paaiškina, kokia svarbi yra rizikos ir kontrolės sistema, nes tokiu būdu organizacija galėtų identifikuoti rizikos modelį, kuris peraugtų į veiksmus prieš aptiktus kibernetinius įvykius. Pirmiausiai, neapdorojus duomenų į informaciją, kurią būtų galima naudoti automatizuotam ar rankiniam valdymui, organizacija negali tinkamai reaguoti į kibernetinę riziką, nes kontrolė priklauso nuo laiku pateikiamos svarbios, vientisos ir

kokybiškos informacijos. Šiuo atžvilgiu reikėtų sustiprinti tris apsaugos linijas, įtraukiant kibernetinio saugumo kontrolės sistemą (4 pav.) (Accenture ir Chartis Research, 2016);

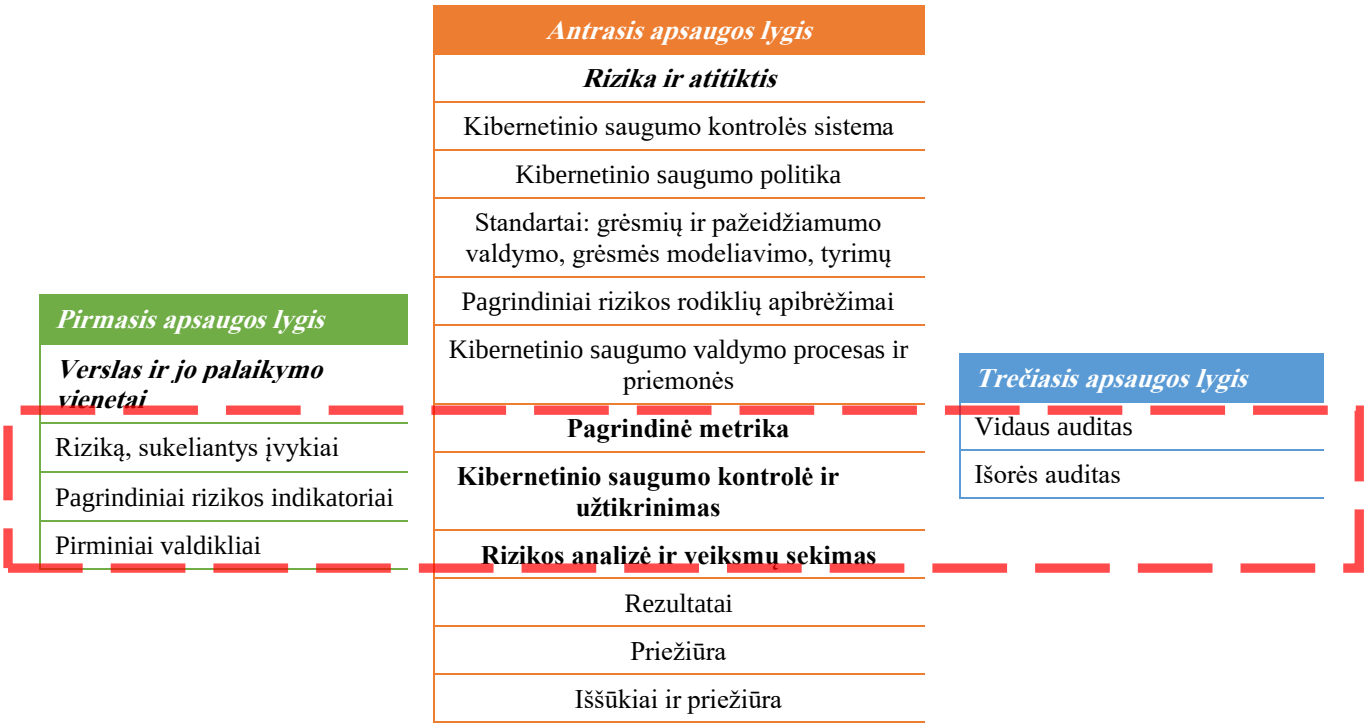
- *Didžiųjų duomenų analizė:* daugelis organizacijų atlieka didžiųjų duomenų analitiką, siekdamos stebėti slaptas kibernetinio saugumo grėsmes. Tokiu būdu jie geriau supranta besikeičiančią išorinę ir vidinę kibernetinio saugumo riziką, taip pat gali stebėti vartotojų elgseną ir tinklo veiklą. Organizacijos, kurios yra stiprios kaip duomenų analizės vartotojos, turi didesnį pasitikėjimą, kai reikia naudoti duomenų analizę kibernetinėms grėsmėms aptikti.. Kita vertus, dideli duomenys gali būti neveiksmingi grėsmių analizei, jei jie yra mažai naudojami siekiant pagerinti kibernetinį saugumą, taip pat sunku maksimaliai išnaudoti didžiųjų duomenų naudą. Kartais problema gali būti siejama su kvalifikuoto personalo – ekspertų, kurie žino, kaip išgauti duomenis apie kibernetinio saugumo riziką ir tendencijas. Šiuo metu didžiųjų duomenų analizė yra esminis būdas užtikrinti kibernetinį saugumą, o pagrindinis šios analizės tikslas yra organizacijų gebėjimas greitai perkelti informaciją, išlaikant aukštą kokybę ir saugumą (Kahyaoglu ir Caliyurt, 2018). Tam reikalingas judrus duomenų valdymas, kuris užtikrina, kad yra tinkama kontrolė, palaikanti šių programų tvarumą ir vertybinius pasiūlymus (International Professional Practices Framework, 2017);
- *Kontrolės aplinka ir kibernetinių grėsmių stebėjimas*: nors darbuotojų patirtis ir kompetencijos išlieka esminiu kibernetinio saugumo užtikrinimo faktoriumi, tik tada, kai kibernetinio saugumo rizika vertinama visoje organizacijos rizikos valdymo struktūroje, vadovybė gali patikėti, kad svarbiausias jų verslo turtas – informacija – yra pakankamai apsaugota nuo kylančių grėsmių. Organizacijų vadovai turi įgaliojimus ir atsakomybę nustatyti pagrindinius įmonės prioritetus, todėl labai svarbu saugumo ir atsparumo sritis nustatyti kaip pagrindines ir apie tai pranešti visos organizacijos nariams. Kitaip bus sunku pasiekti, kad organizacija panaudotų pakankamai išteklių savo informacinėms sistemoms apsaugoti ir tinkamai reaguotų į kibernetinius įvykius (Kahyaoglu, ir Caliyurt, 2018). Galligan ir kt. (2019) teigia, kad kibernetinio saugumo rizikos negalima išvengti, todėl ji turi būti tinkamai valdoma. Tam labai svarbu turėti paruoštą kibernetinio saugumo rizikos valdymo programą, kuri galėtų efektyviai įvertinti kontrolės struktūrą ir efektyvumą, siekiant apsaugoti organizacijos informacines sistemas. Neturint oficialaus dokumento, patvirtinančio vidaus kontrolės lūkesčius ir vidaus audito, kuris nuolat stebėtų ir vertintų organizacijos veiklos procesus, organizacijos galimybės efektyviai valdyti kibernetinio saugumo riziką žymiai sumažėja (Kahyaoglu ir Caliyurt, 2018).

No ir Vasarhelyi (2017) kibernetinio saugumo ir nuolatinio stebėjimo vertinime padarė išvadą, kad veiksmingų sprendimų priėmimui reikalinga papildoma informacija apie kontrolės aplinką, rizikos vertinimą ir rizikos poveikį. Lois ir kt. (2020) savo tyrime taip pat įvardina reikalavimus kibernetinio saugumo užtikrinimo modeliui, kurie, kaip galima matyti, visiškai atitinka vidaus audito funkcijas:

- Internetinis, realaus laiko kibernetinio saugumo stebėjimas;
- Nuolatinis tam tikros sistemos ar visos organizacijos saugos būklės įvertinimas automatiniais įrankiais;
- Pasirenkamas saugos įrankių, nustatymų ir saugos įvykių atskleidimas (pvz., saugumo pažeidimai);
- Bendros ir standartizuotos duomenų bazės apie nustatytus saugumo įvykius.

Galligan ir kt. (2015) taip pat nustatė efektyvios aplinkos kontrolės ir kibernetinės rizikos stebėjimo raktus:

– Vadovybės deklaruojama svarba informacinių sistemų apsaugai;
– Nuolatinio ar atskiro vertinimo programa, skirta įvertinti programos projektą ir veikimo efektyvumo kontrolę, kuria siekiama sumažinti galimą kibernetinį poveikį;
– Kvalifikuotų kibernetinio saugumo rizikos specialistų pagalba ir įtraukimas;
– Tinkamas kibernetinio saugumo rizikos stebėjimas ir su paslaugų teikėjais susijusių paslaugų teikėjų kontrolė;
– Tinkami ir savalaikiai pranešimai apie kibernetinio saugumo rizikos spragas;
– Už informacinių sistemų kontrolę atsakingų asmenų atskaitingumas



3 pav. Kibernetinio saugumo rizikos vertinimo sistema pagal tris apsaugos linijas (sudaryta autorės, pagal Accenture & Chartis Research, 2016 ir Ahia & Deloitte, 2017)

Kibernetinio saugumo grėsmių numatymas ir informacinių sistemų saugumo spragų vertinimas reikalauja ne tik visapusiško organizacijų požiūrio, bet ir nuolatinių pastangų, tačiau daugelis organizacijų kibernetinį saugumą dažnai laiko papildomomis išlaidomis, duodančiomis mažai grąžos. Šis klaidingas supratimas lemia nepakankamą programų valdymo palaikymą, o tai – blogai suprojektuotas apsaugos sistemas ir politiką. Todėl labai svarbu, kad organizacijos turėtų ilgalaikius kibernetinio saugumo iniciatyvų planus, kuriais apsaugotų kritines sistemas ir jų veikimą užtikrinančius išteklius. Ilgalaikiai kibernetinio saugumo sprendimai turėtų apimti visus organizacijos sistemų lygius ir užtikrinti šių sistemų bei įmonės valdomo turto apsaugą. Tiek kibernetinis saugumas, tiek vidaus auditas netelpa į visuotinai pripažintus juos reglamentuojančių standartų rėmus. Abi šios funkcijos organizacijose privalo būti susietos laiko periodu (veikti esamuoju laiku), taip pat turi niuansų, kurių negalima išreikšti tradicinių ataskaitų teikimo modeliais, joms netaikoma piniginė reikšmingumo riba, tiesiogiai susijusi su verte (No ir Vasarhelyi, 2017). Dėl šios priežasties organizacijų vadovai turi žinoti patys ir informuoti apie informacinių sistemų, suderintų su įmonės tikslais, vertę. Turėdami šią informaciją, jie gali apibrėžti kibernetinio saugumo rizikos tolerancijos lygį ir padėti užtikrinti, kad tinkamos investicijos būtų nukreiptos į kibernetinio saugumo sistemų, kurios yra labai svarbios organizacijos tikslams pasiekti, apsaugą (Kahyaoglu ir Caliyurt, 2018).

2.3. Vidaus audito pokyčiai ir jų įtaka kibernetinio saugumo rizikos vertinimui

Tradicinis audito modelis. Amerikos atestuotų valstybinių buhalterių instituto (AICPA) 2016 metais išleistame kibernetinio saugumo vadove yra trūkumų, dėl kurių dabartiniai ataskaitų teikimo ir atestavimo standartai yra netinkami. Šiame kibernetinio saugumo vadove atestavimo kriterijų rinkiniai pateikiami pagal dvi kategorijas: aprašymo kriterijai ir kontrolės kriterijai. Pirmieji kriterijai skirti parengti ir įvertinti organizacijos kibernetinio saugumo rizikos valdymo pristatymą ir aprašą, o vėlesni – kontrolės efektyvumui nustatyti, kad būtų pasiekti organizacijos kibernetinio saugumo tikslai. Šis tradicinis požiūris į kriterijų apibrėžimą neatsižvelgia į nuolat kintantį kibernetinio saugumo rizikos pavojaus pobūdį. Pavyzdžiui, į jį neįtrauktas galimas neigiamas poveikis, kurį gali sukelti kibernetinio saugumo sistemos gedimas konkrečiame verslo procedūrų etape. Be to, atsirado naujų analitinių technologijų ir procesų grupės, kurios padeda pagerinti atestaciją ar audito kokybę, tačiau tokios analitinės technologijos ir procesai nelabai atitinka tradicinių audito standartų (No ir Vasarhelyi, 2017).

2 lentelė. Audito etapai ir analitiniai metodai (sudaryta autorės remiantis No ir Vasarhelyi, 2017)

Audito etapai	Taikomi analitiniai metodai	Priežiūra, stebėjimas, pastabos	Svarbiausi akcentai
Kliento peržiūra	Žiniasklaidos stebėjimas; Socialinės žiniasklaidos stebėjimas	Didelis šaltinių rinkinys leidžia nuskaityti įvykių, su organizacijos vadovais aplinką, jų reputaciją, konkurencinę aplinką ir įvykius verslo šakoje.	
Audito planavimas	*Ex ante* rizikos vertinimas *a la* nuolatinis rizikos stebėjimas ir vertinimas; Santykinė analizė	Tarpusavio pramonės grupės veiklos vertinimas	Nuolatinio rizikos stebėjimo ir vertinimo procesai papildys audito planavimo procesą atlikdami pagrindinių rizikos rodiklių įvertinimą
Audito rizikos įvertinimas	Nuolatinis rizikos stebėjimas ir vertinimas	Esminis rizikos situacijos pokytis reikalauja nuolatinio stebėjimo, valdymo veiksmų ir nuolatinio audito parametrų pokyčių	Rizikos vertinimai padidins stebėjimo lygį ir apims tiesioginius programų bei kibernetinio saugumo „monitorius“, pagrįstus pagrindinių rizikos rodiklių ir stebėjimo duomenimis
Vidaus kontrolės vertinimas	Procesų „kasyba“; Analitinis modeliavimas	Pasikliaujama geriausia įmonės suprojektuota išteklių planavimo sistemos prigimtimi, tačiau tam trukdo tai, kad daugumos didelių organizacijų duomenys yra iš kitų įmonių išteklių planavimo tipų šaltinių derinio	
Atitikties testavimas	Procesų „kasyba“; Nuolatinis valdymo stebėjimas	Norint apsaugoti vartotojo konfigūruojamais valdikliais, reikia stebėti šiuos nustatymus naudojant nuolatinio valdymo stebėjimo metodiką	Bendrų rodiklių atitikties stebėjimas turės įtakos vidaus kontrolės vertinimui. **Kontrolės srityje audito ir kibernetiniai rodikliai sutaps ir bendradarbiaus**

Audito etapai	Taikomi analitiniai metodai	Priežiūra, stebėjimas, pastabos	Svarbiausi akcentai
Esminis testavimas	Klasterinė analizė; Patvirtinimai iš/į duomenų bazę; Tęstinumo lygtys[1]	Daugybės operacijų atsiradimas, galimybė jas saugoti internete, pasitikėjimas elektroniniais dokumentais ir įrašais, XML išvestinių kalbų kalbų naudojimas keičiantis duomenimis iš ankstesnių į tolimesnių laikotarpių sistemas stipriai pakeitė bandomus daiktus ir reikalauja naujų audito testų, kurių dar nėra	Esminius bandymus nuolat atliks programinės įrangos atstovai, ypač į sistemą patenkančių duomenų. Egzogeniniai duomenų šaltiniai, tokie kaip socialinė žiniasklaida, orai, regioninė mikroekonomika ir daiktų internetas (IoT) patvirtins ir papildys kibernetinius ir užtikrinimo duomenis. Šie duomenys bus šiek tiek pakeičiami.
Nuomonės suformulavimas	Oficialios ekspertų sistemos, skirtos įvertinti naujas audito įrodymų formas; Audito nesėkmės įvertinimo sistemos pagrįstos vidiniais įrodymais ir egzogeniniais kintamaisiais	Duomenų formų gausa ir apimtis bei tiesioginio duomenų stebėjimo trūkumas lems tai, kad audito sistemos turės būti iš esmės automatizuotos taikant simbiotinį nuomonės formulavimo procesą, iš dalies pasikliaujant mašininiu stebėjimu ir nuomonės formavimu	Kadangi turės būti suformuoti atspaudai, sistemos „įtarimo“ lygis turės būti ne intuityviai vertinamas, o formaliai nustatytas, nes tai priklausys nuo mašinos formuluotės. Labiausiai tikėtina, kad žmogaus sprendimas ilgą laiką bus būtinas. Skirtingiems audito produktams, tokiems kaip stebėjimo operacijų, finansinio užtikrinimo ir kibernetinio saugumo, gali būti pateikiamos skirtingos atskiros nuomonės

Pagal tradicinį audito modelį organizacijos audito komitetas reikalauja samdytis kvietinius (išorės) auditorius, taip pat priimti sprendimus dėl mokesčių, organizacijos išlaikymo, o kartais ir dėl įnašų į veiklos sritį. Be to, tradicinis audito modelis turi rimtų duomenų naudojimo apribojimų (No ir Vasarhelyi, 2017). Dabartiniame modelyje skelbiama nulinė arba viena audito išvada, ar ūkio subjekto finansinė atskaitomybė visais reikšmingais aspektais ir pagal visuotinai priimtus apskaitos principus (GAAP) (ang. *Generally Accepted Accounting Principles)* pateikiama sąžiningai, todėl mažai tikėtina, kad bus taikoma naujoms užtikrinimo paslaugoms, tokioms kaip kibernetinis saugumas ir nuolatinis užtikrinimas. Ši priežastis tampa kliūtimi draudikams, teikiantiems tokią finansinę atskaitomybę. Pavyzdžiui, užtikrinimo užduotis kibernetinio saugumo srityje labiausiai sutelkta į organizacijos kibernetinio saugumo rizikos valdymo efektyvumą (Lois ir kt., 2020).

Visas audito procesas, kuris aprašomas 2 lentelėje gali būti palaipsniui keičiamas, kaip nurodyta lentelės svarbiausiuose akcentuose. Atlikus šiuos pakeitimus, galima sukurti bendrus, pusiau

[1] Tęstinumo lygčių sąvoka pasiskolinta iš fizinių mokslų ir pritaikoma verslo scenarijuje. Kiekvienas verslo procesas laikomas kontroliniu kiekiu, kurį sudaro įvairūs sandorių srautai ar verslo veikla. Jei sandorių srautai į/ iš kiekvieno verslo proceso yra vienodi, verslo procesas pastovus, be anomalijų. Kitu atveju, jei sandorių srautuose atsiranda šuolių, verslo proceso pusiausvyros palaikyti negalima. Auditoriai, norėdami atlikti anomalijų priežasčių tyrimą, modeliuoja ryšius tarp skirtingų verslo procesų, naudodami tęstinumo lygtis (Alles ir kt., 2005).

autonomiškus, automatizuotus užtikrinimo procesus su kelių tipų tikslais ir galimais sprendimais, kurie pasitarnautų kibernetinio saugumo užtikrinimo procesuose.

Nuolatinio (tęstinio) vidaus audito poreikis kibernetinio saugumo rizikos vertinimui. Dėl technologinių naujovių dabartinėje audito aplinkoje vis labiau domimasi nuolatinio audito koncepcija. Nuolatinis arba tęstinis auditas užtikrina mažesnę klaidų tikimybę ir sustiprina audito išvadų patikimumą (Lois ir kt., 2020). Teigiama, kad nuolatinis auditas, integruojant tradicines audito procedūras ir naujas technologijas, ateityje taps viena iš organizacijų veiklos tęstinumą užtikrinančių priemonių (Woodroof ir Searcy, 2001).

Rikhardsson‘as ir Dull‘is (2016) tyrė tęstinio audito technologijas mažose įmonėse. Jų rezultatai parodė, kad technologijos dažniausiai buvo diegiamos siekiant padidinti išteklių efektyvumą, tačiau nebuvo suvokiamos kaip priemonė duomenų kokybės problemoms spręsti. Amin‘as ir Mohamed‘as (2016), tyrinėję Egipto auditorių požiūrį į internetinės finansinės informacijos kokybės iššūkius, nurodė, kad nuolatinis auditas gali kompensuoti iššūkius, susijusius su interneto finansine atskaitomybe. Chan, Chiu ir Vasarhelyi (2018), tyrinėdami įvairius nuolatinio audito būdus savo išleistoje knygoje padarė išvadą, jog metodologija reikalauja technologinių naujovių, kad sklandžiai veiktų su tradicine vidaus audito praktika. Atliekant nuolatinį auditą, galima nuolat tikrinti finansinius duomenis, siekiant išvengti klaidų ir sukčiavimo.

3 lentelė. Nuolatinio užtikrinimo (tęstinio audito) ir kibernetinio saugumo ypatybių palyginimas su tradiciniu audito modeliu (sudaryta autorės remiantis No ir Vasarhelyi, 2017)

Tradicinio audito modelio ypatybės	Nuolatinis užtikrinimas (tęstinis auditas)	Kibernetinis saugumas	Galimas sprendimas
Laiko taškas	Laiko intervalas yra ribotas ir artimas įvykio matavimui	Laiko intervalas yra ribotas ir artimas įvykio matavimui. Labiausiai tikėtina, kad visada yra tam tikrų pertraukų, kurių negalima aptikti/ nustatyti.	Visiška informacijos apsauga ir izoliavimas.
Viena nuomonė	Geresnis matavimas su keliais parametrais; Turi būti atsargus, kad ne visada pateiktų geriausius įvertinimus.	Geresnis matavimas su keliais parametrais; Turi būti atsargus, kad ne visada pateiktų geriausius įvertinimus. Brandos modelis siūlomas kaip reitingavimo schema.	Daugialypiai nuomonių reitingai pagal iš anksto nustatytus pramonės kriterijus, atskleistus su vidutiniais verslo linijų reitingų intervalais.
Skaitmeninis reikšmingumas	Nuolatinio stebėjimo procese sunku nustatyti kiekvienos operacijos skaitinį reikšmingumą; Paprastai, kiekvienam išimties tipui būdinga pavojaus riba	Kibernetinio lūžio pavojus priklauso nuo daugybės parametrų, kurie, greičiausiai, nėra skaitiniai.	Klausimynai ir kokybinis kiekvieno žinomo įsilaužimo pavojaus ir poveikio nustatymas bei nežinomų įsibrovimų nustatymo metodai.
Žodinė nuomonės išraiška	„sąžiningai atstovauja“ nėra tinkama; „atitinka kriterijus“ tinkamesnė forma, kaip nurodyta vadove.	„sąžiningai atstovauja“ nėra tinkama;	Įvairių tipų sakiniai , atspindintys daugialypės nuomonės vertinimo ypatybes.

Steinbart ir kt. (2013) informacijos saugumo efektyvumą apibrėžia kaip audito išvadų ir saugumo incidentų skaičiaus bei tendencijos visumą. Tai prasminga informacijos saugumo specialistų požiūriu, kuriems abi priemonės yra tai, ką reikia kuo labiau sumažinti. Apie tai, kad tradicinė audito sistema turėtų būti modifikuota, pritaria No ir Vasarhelyi (2017) atliktas tyrimas. Tai reikalinga tam, jog būtų galima užtikrinti patikimą paslaugų rinkinį ir apimti šiuos dalykus: nuolatinį auditą, nuolatinį kontrolės stebėjimą ir nuolatinį kibernetinio saugumo užtikrinimą. Tradicinio audito modelio, tęstinio audito ir kibernetinio saugumo ypatybių palyginimas pateikiamas 3 lentelėje.

Auditoriaus kvalifikacija ir žinios. Šiandien auditoriams labai svarbu įgyti profesinių įgūdžių, reikalingų geriau ir efektyviau reaguoti į savo darbe vykstančius procesus. Procesai praneša, kad naujos technologijos pakeis verslo audito metodus, todėl auditoriai turės tai suprasti, kad galėtų paaiškinti šių pokyčių poveikį bendrovės vadovams ir kitoms suinteresuotoms šalims. Taip pat pabrėžiamas žinių vaidmuo informacinėse technologijose, siekiant tiksliai įvertinti auditus. Apibendrinant galima teigti, kad norint tinkamai apsaugoti organizaciją nuo kibernetinių atakų, reikia kartu optimizuoti žinias, įgūdžius ir technologijas (Moorthy ir kt., 2011).

Kai kurių organizacijų valdybos nariams reikia aiškiai suprasti bendrą organizacijos kibernetinės rizikos poveikį, todėl kibernetinės rizikos valdymas turėtų būti bendro verslo rizikos valdymo procesų dalis, nes tai turi įtakos visai organizacijai. Dėl to valdybos ir audito komitetai reikalauja vidaus audito, kad užtikrintų organizacijos kibernetinės rizikos valdymą. Pasak Ahia ir Deloitte (2017), nors valdymo organai naudojasi kibernetinio saugumo mokymais, kuriuos teikia vyriausiasis informacijos pareigūnas (angl. *chief information officer (CIO)*), vyriausiasis technologijų pareigūnas (angl. *chief technical officer (CTO)*) ir vyriausiasis informacijos saugumo pareigūnas (angl. *chief information security officer (CISO)*), švietimo pastangos gali neatitikti valdybos aiškumo ir supratimo poreikių dėl trijų pagrindinių priežasčių:

- *Informacinių technologijų trūkumo*. Informacinių technologijų ir saugumo departamento ataskaitos ir pristatymai dažnai yra sudėtingi, juos sunku susieti su verslo tikslais, nes daugiausia dėmesio skiriama techninei rizikai, dėl kurios valdyba gali atsidurti aklavietėje. Šiuo metu į valdybą neprivaloma įtraukti kibernetinio saugumo techninių specialistų, dėl ko esamiems nariams galėtų būti patogiau vykdyti finansinę ar veiklos vidaus kontrolę ir taisykles;
- *Nepriklausomumo užtikrinimo trūkumas*. Faktas, kad daugumoje organizacijų informacinių technologijų ir saugumo funkcijos negali suteikti nepriklausomo, objektyvaus patikinimo, kurio reikalauja valdybos nariai, kalbėdami apie kibernetinį saugumą. Vidaus auditoriai yra nepriklausomi, o jų teikiamų užtikrinimo paslaugų vertę ir patikimumą lemia pagrindinės nepriklausomumo prielaidos. Mutchler (2003) nepriklausomumą apibūdina kaip audito aplinkos savybę, kurioje asmuo ar komanda teikia užtikrinimo paslaugas, kai pageidaujama, kad asmuo ar komanda būtų laisvi nuo materialinių interesų konfliktų, keliančių grėsmę objektyvumui. Susiduriant su nepriklausomumo pažeidžiamumu išskiriamos septynios pagrindinės grėsmės: savianalizė, socialinis spaudimas, ekonominis interesas, asmeniniai santykiai, familiarumas, kultūrinis, rasinis ir lyčių šališkumas bei pažinimo šališkumas;
- *Sąmoningumo trūkumas*. Remiantis naujienų pranešimais apie pažeidimus ir naujus reguliavimo, vyriausybių ir audito subjektų teisės aktus daugeliui valdybos narių reikia geriau suvokti kibernetinę riziką.

Vidaus auditoriai turėtų išplėsti informacinių technologijų audito galimybes, kad galėtų pateikti iniciatyvių įžvalgų ir tokiu būdu pateiktų vadovybei pridėtinės vertės rekomendacijų. Vidaus auditoriai turėtų gerai išmanyti būsimus susijusių reglamentų pokyčius, naujus reikalavimus ir kitas verslo tendencijas, taip pat užtikrinti, kad audito programose būtų į jas atsižvelgiama. Vadovybė turėtų atsargiai nustatyti CAE ir vidaus auditorių kibernetinio saugumo kompetencijas, naudodamiesi veiksmingomis talentų valdymo ir kvalifikacijos kėlimo programomis, pagrįstomis standartais, kad būtų užtikrinta, jog kompetencija yra reikalinga atsižvelgiant į organizacijos prioritetus (Haapamäki ir Sihvonen, 2019).

Žvelgiant iš rizikos valdymo perspektyvos, vidaus auditą atliekančių specialistų vertinimas ir analizė neapsiriboja tik rizikos vertinimu, siekiant nustatyti kibernetinio saugumo rizikos tikimybę ir poveikį. Šis poveikis turėtų būti vertinamas pagal tai, kaip organizacija sprendžia kibernetinį saugumą ir kokių veiksmų ėmėsi, kad sumažintų su juo susijusią riziką, peržiūrint trečiųjų šalių konsultacijas ir audito ataskaitas. Kahyaoglu ir Caliyurt (2018) teigia, kad vidaus auditoriai turėtų būti kompetentingi nustatyti kylančias kibernetinio saugumo rizikas ir suprasti visų kibernetinio saugumo grėsmių poveikį organizacijai. Šių procesų užtikrinimui teigiamos įtakos galėtų turėti nuolatinis vadovybės kibernetinio saugumo kontrolės audita. Vidaus auditoriai taip pat turėtų palaikyti tvirtą partnerystę su vyriausiu informacijos (CIO) arba vyriausiu informacijos saugumo (CISO) specialistais, kad įvertintų trečiųjų šalių paslaugų tiekėjų patikimumą (Kahyaoglu ir Caliyurt, 2018).

2.4. Vidaus audito procedūrų integravimas į kibernetinio saugumo rizikos vertinimą

Vidaus audito vaidmuo kibernetinio saugumo rizikos valdymui. Organizacijų vadovybė yra atsakinga už visų organizacijai keliamų pavojų supratimą ir apsaugojimą. Vidaus audito, kaip nepriklausomo užtikrinimo teikėjo, vaidmuo yra būtinas patikimam rizikos valdymui. Norėdami pasiekti šį pagrindinį vaidmenį organizacijose, vidaus auditoriai turėtų atsižvelgti į tarptautinius vidaus audito profesinės praktikos standartus (TVAPPS) ir tarptautinę profesinės praktikos sistemą (IPPF), kurią sudaro dviejų tipų – privalomos ir rekomenduojamos rekomendacijos. Šalia viso to, organizacijai reikalingas kibernetinio saugumo užtikrinimo planas, kuris pagal Kahyaoglu ir Caliyurt (2018), turėtų būti toks:

1) *sudarytas nuolatine rizika paremta saugumo užtikrinimo programa*: vidaus auditoriai turėtų taikyti vieningą ir išsamų sprendimą, pristatydami nuolatine rizika pagrįstą informacijos saugumo programą. Kad struktūruota rizika pagrįsta programa būtų išsami, ji turi pasiūlyti visapusiškas funkcijas, apimančias riziką, procesą, politiką, pažeidžiamumą, mokymą, auditą ir atitikties valdymą. Kitaip tariant, išsami programa leis nustatyti organizacijos riziką ir tinkamą kontrolę šiai rizikai sumažinti; reguliuoti kontrolės reikalavimus, siekiant palengvinti atitiktį; informuoti organizaciją, kurios funkcijos jau veikia; parengti trūkstamų kontrolių įgyvendinimo planą, pagrįstą jų ekonominiu efektyvumu; bei pranešti apie valdymo funkcijas ir atitikties procesą. Vidaus auditoriai turėtų reguliariai teikti ir kitas įžvalgas, susijusias su išoriniais rinkos duomenimis, kad įžvalgos būtų teikiamos su platesniu, rizika pagrįsto audito, požiūriu;
2) *sukurtas pagal kibernetinio užtikrinimo sistemą:* vidaus auditoriai turėtų naudoti panašias sistemas, pavyzdžius ir kalbą, kad būtų išvengta neatitikimų ir nenutrūktų vadovybės informavimas. Vidaus auditoriai galėtų derinti su vadovybe kibernetinį saugumo užtikrinimo klausimus, dalytis savo ištekliais ir (arba) bendrai naudoti informacinių technologijų partnerius. Kadangi įvairiuose verslą reglamentuojančiuose standartuose nurodoma arba

siūloma daugybė tų pačių saugumo rizikos analizių ir valdymo praktikų, vieningas požiūris supaprastina programą ir leidžia organizacijai laikytis visų jų vienu metu. Šis gebėjimas pašalina reikalingumą atsakyti į tuos pačius klausimus dėl kiekvieno reglamento;

3) *vykdomas užtikrinimo cikle*: svarbu turėti rizika pagrįstą informacijos saugumo požiūrį, kuriam reikalingas valdomas, bet drausmingas, tiesiogiai susijęs su verslo procesu ir supaprastinantis vykdomą programą, vertinimas. Tai reiškia informacinių sistemų efektyvumą ir didesnį organizacijos budrumą laikantis reikalavimų. Vidaus auditoriai turėtų parengti ilgalaikį nuolatinio audito planą, kuris nuosekliai atitiktų kibernetinio saugumo užtikrinimo planus. Taip pat turėtų palaikyti glaudžius santykius su kitomis organizacijomis ne audito metu, kad suprastų kibernetinio saugumo rizikos problemas ir trūkumus savo veikloje. Tokiu būdu vidaus auditoriai tampa patikimais kibernetinio saugumo patarėjais, prisidėdami prie kibernetinio saugumo užtikrinimo proceso, pateikdami kritines išvadas, kaip šio dalyko ekspertai. Vidaus auditoriai turėtų nustatyti audito rizika pagrįstus, tinkamai parengtus planus ir profesionaliai bendraujant teikti įžvalgas vadovybei, kad būtų užtikrinta, jog vidaus audito rezultatas sukuria pridėtinę vertę visoms suinteresuotosioms šalims.

Wallace ir kt. (2011) pateikia faktus, kad vidaus audito ir informacijos saugumo funkcijų bendradarbiavimo lygis yra teigiamai susijęs su organizacijos atitikimu organizacijos vidaus kontrolės reikalavimams.

Vidaus kontrolės sistema. Vidaus kontrolės sistemos vertinimas atlieka svarbų vaidmenį vidaus audite, nes vertinamas vidaus kontrolės sistemų efektyvumas, kuris taip pat apima vadovybės veiksmų, skirtų taisyti situacijas, kurios neatitinka planuotų rezultatų, vertinimą. Vidaus kontrolės sistemos apibrėžimą sudaro valdymo kontrolė, kuri apima planavimo, organizavimo, vadovavimo ir personalo funkcijų vertinimą. Organizacijų vadovybė ir audito komitetas paprastai tikisi, kad vyriausias audito vadovas (angl. *chief audit executive (CAE)*) per metus atliks pakankamą audito darbą ir surinks kitą turimą informaciją, jog susidarytų nuomonę apie kontrolės procesų tinkamumą ir veiksmingumą. Apibendrinus šiuos duomenis vyriausias audito vadovas turėtų perduoti vadovybei ir audito komitetui bendras vertinimo išvadas apie organizacijos vidaus kontrolės sistemos būklę. Tai būtina, nes vidaus auditoriai atlieka tarpininko vaidmenį ir padeda vykdyti audito komiteto priežiūros funkciją. Jei nurodytos vidaus audito funkcijos nėra, vadovybė turi taikyti kitus stebėsenos procesus, kad užtikrintų sau ir valdybai, jog vidaus kontrolės sistemos sistema veikia taip, kaip numatyta. Esant tokioms aplinkybėms, organizacijų vadovybė turės įvertinti, ar tokie procesai suteikia pakankamą ir objektyvų užtikrinimą, ar reguliariai tikrina ir vertina įmonės vidaus kontrolės sistemų tinkamumą ir vientisumą (Gramling ir Schneider, 2018).

Vidaus auditoriai, peržiūrėję ir įvertinę apskaitos, finansinės ir kitos veiklos kontrolės patikimumą ir tinkamumą turėtų išsiaiškinti, kaip laikomasi nustatytos organizacijos vidaus politikos, strateginių planų, procedūrų, jų veiklą ribojančių įstatymų ir kitų teisės aktų, nes tai gali turėti reikšmingos įtakos organizacijos veiklos procesų užtikrinimui. Tuomet vidaus auditoriai peržiūri organizacijos turto apsaugos priemones ir prireikus tikrina tokio turto egzistavimą bei įvertina išteklių panaudojimo ekonomiškumą ir efektyvumą. Galiausiai vidaus auditoriai atlieka stebėsenos kontrolę ir peržiūri, ar įmonės taikomi sprendimai ir priemonės atitinka nustatytus tikslus ir ar vykdomos taip, kaip buvo suplanuota (Fadzil, Haron ir Jantan, 2005).

Organizacijos vidaus kontrolės sistemos tinkamumo ir efektyvumo bei veiklos kokybės, atliekant priskirtas pareigas, peržiūra ir įvertinimas yra pagrindinis pirminis vidaus audito darbas. Vidaus

audito tinkamumo peržiūros tikslas yra išsiaiškinti, ar sukurta sistema suteikia pagrįstą patikinimą, kad organizacijos tikslai ir uždaviniai bus pasiekti efektyviai ir ekonomiškai. Laikoma, kad tinkama kontrolė yra, jei administracinis valdymas yra suplanuotas ir organizuotas taip, kad būtų pagrįstas užtikrinimas, jog organizacijos tikslai ir uždaviniai bus pasiekti efektyviai ir ekonomiškai. Pagrįstai užtikrinama, kai imamasi ekonomiškai efektyvių veiksmų, kad nukrypimai, pavyzdžiui, netinkami ar neteisėti veiksmai, būtų apriboti iki toleruotino lygio.

Vidaus kontrolės sistema veiksminga laikoma tada, kai administracinis valdymas vadovauja sistemai taip, kad užtikrintų pagrįstumą, jog organizacijos tikslai ir uždaviniai bus pasiekti. Veiklos kokybės apžvalgos tikslas yra išsiaiškinti, ar organizacijos tikslai ir uždaviniai buvo pasiekti. Pagrindiniai organizacijos vidaus kontrolės sistemos tikslai yra suteikti administraciniam valdymui pagrįstą patikinimą, kad finansinė informacija yra tiksli ir patikima; organizacija laikosi politikos, planų, procedūrų, įstatymų, taisyklių ir sutarčių; turtas yra apsaugotas nuo praradimo ir vagystės; ištekliai naudojami ekonomiškai ir efektyviai; ir nustatytus veiklos ar programų tikslus ir tikslus galima pasiekti (Fadzil, Haron ir Jantan, 2005). Antroji audito rūšis, kurią turi atlikti vidaus auditoriai, yra finansinės ir veiklos informacijos tikslumo ir patikimumo bei priemonių, naudojamų tokiai informacijai nustatyti, įvertinti, klasifikuoti ir pranešti, peržiūra. Informacinės sistemos teikia duomenis sprendimams priimti, kontroliuoti ir laikytis išorinių reikalavimų. Todėl vidaus auditoriai turėtų išnagrinėti informacines sistemas ir nustatyti, ar finansiniuose ir veiklos dokumentuose bei ataskaitose yra tiksli, patikima, laiku teikiama išsami ir naudinga informacija, o įrašų vedimo ir ataskaitų teikimo kontrolė yra tinkama ir veiksminga (Cheong ir kt., 2020).

Sistemų, sukurtų siekiant užtikrinti politikos, planų, procedūrų, įstatymų, reglamentų ir sutarčių laikymąsi, peržiūros atlikimas yra trečiasis audito veiklos elementas, aprašytas standartuose. Administracinis valdymas yra atsakingas už sistemų, skirtų užtikrinti, kad būtų laikomasi tokių reikalavimų kaip įstatymai, taisyklės, reglamentai, politika ir procedūros, sukūrimą. Vidaus auditorių vaidmuo yra nustatyti, ar vadovybės sukurtos sistemos yra tinkamos ir veiksmingos ir ar tikrinama veikla atitinka tinkamus reikalavimus (Be to, kaip aprašyta standartuose, vidaus auditoriaus vaidmuo apima vertinimų teikimą su rekomendacijomis dėl administracijos valdymo, nustatytų operacijų ir programų tikslų (Fadzil, Haron ir Jantan, 2005).

Steinbart ir kt. (2015) siūlo modelį, kaip vidaus auditas ir informacijos saugumo funkcijos galėtų veikti kartu, kad padėtų organizacijoms pasiekti ekonomiškai efektyvų informacijos saugumo lygį. Norint padidinti informacijos saugumo audito peržiūrų dažnumą, reikia investuoti papildomų išteklių. Daugumoje organizacijų vidaus auditas yra įpareigotas peržiūrėti kelis veiklos ir finansinės atskaitomybės aspektus. Valstybinių įmonių dideli vidaus audito ištekliai skiriami padėti vadovybei peržiūrėti ir įvertinti finansinės atskaitomybės vidaus kontrolę, todėl vadovybė turi būti įtikinta, kad papildomų investicijų, leidžiančių vidaus auditui atlikti dažnesnes informacijos saugumo peržiūras, atlikimas yra pagrįstas, nes tai pagerins organizacijos saugumo programos efektyvumą. Toks įsitikinimas galioja, jei abi šalys (vidaus auditas ir kibernetinis saugumas) sutinka, kad intensyvesnė sąveika yra naudinga ir būtina, todėl svarbu suprasti vidaus auditorių požiūrį į tai, kokią įtaką daro bendrai organizacijos informacijos saugumo programos kokybei.

Tarporganizacinio bendradarbiavimo iššūkiai, kurie svarbūs ne tik dalijantis duomenimis tose pačiose informacinių technologijų platformose, tačiau ir užtikrinant bendrą kibernetinę saugą tiekimo grandinėse. Bendra komunikacija, pagrįsta atvirais, sąžiningais ir pasitikėjimu grįstais santykiais bei

tiekimo grandinės integracija, suderinant sistemas ir procesus duos didesnę grąžą ir užtikrins bendrus saugumo tikslus (Ghandge ir kt., 2018).

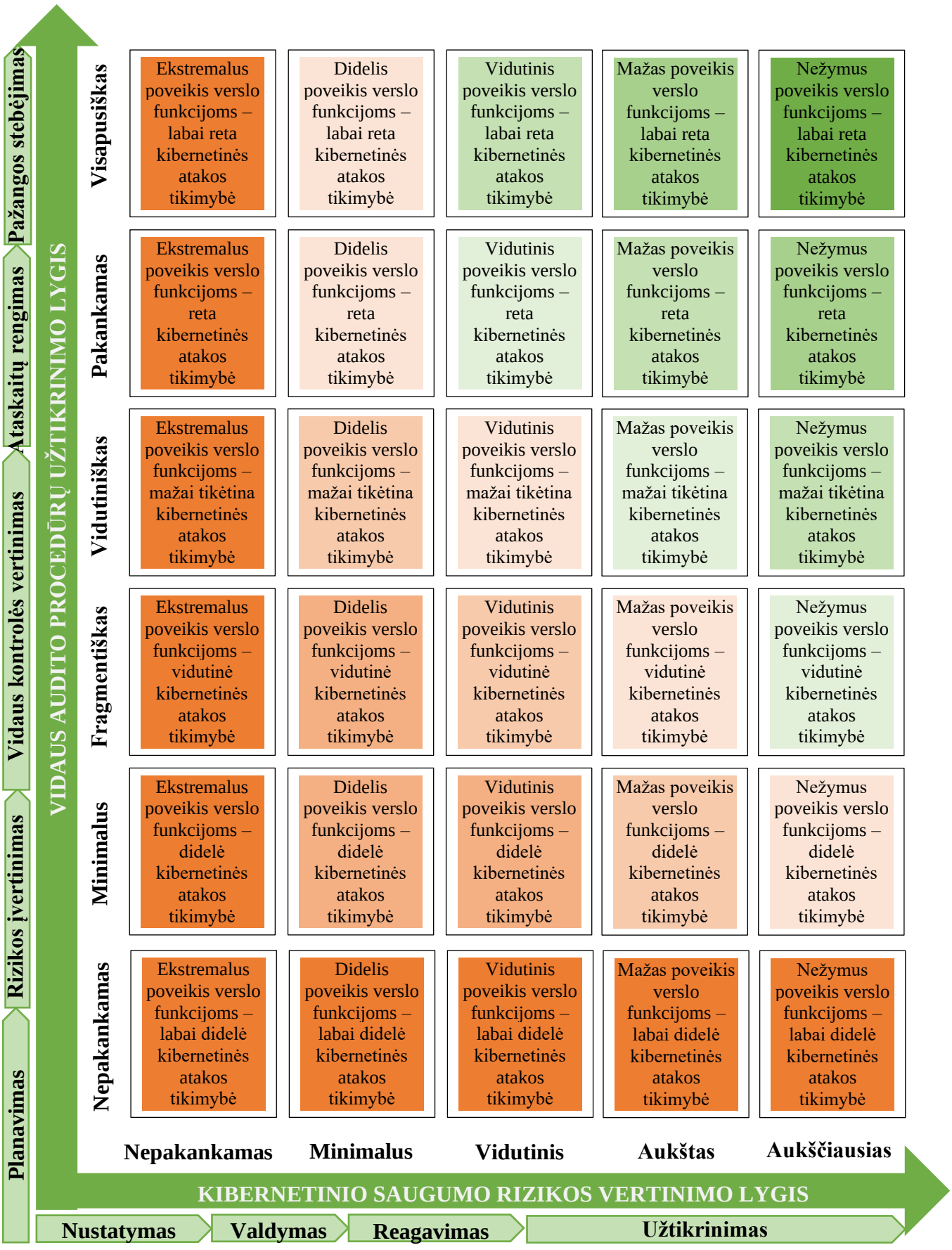
Tvirta vidaus audito sistema, sukurta organizacijų pridėtinei vertei kurti ir procedūroms tobulinti (Drogalas, Arampatzis ir Anagnostopoulou, 2016), vaidina pagrindinį vaidmenį užkertant kelią kibernetinėms atakoms ir įgyjant kvalifikuotų rizikos prevencijos vadovų (Abdullatif ir Kawuq, 2015). Nuolatinis auditas skatina tikralaikę (arba beveik realią) kontrolę ir dalijimąsi finansine informacija (Drogalas, Arampatzis ir Anagnostopoulou, 2016). Informacijos vientisumas gali būti vertinamas bet kuriuo metu ir nuolat tikrinamas siekiant išvengti klaidų ir nesąžiningos veiklos, tačiau vertinimo laikotarpis iš esmės priklauso nuo apskaitos informacinių sistemų atnaujinimo dažnumo, kuris gali būti nepakankamas dėl biudžeto suvaržymų (Lois ir kt., 2020).

Lois ir kt. (2020) savo tyrime išryškina tris pagrindinius vidaus audito tikslus: asmens duomenų apsaugą, kibernetinių atakų vengimą ir specializuoto personalo mokymą. Šiame tyrime, duomenų rinkimo laiko ir atsargumo technologijoms klausimai buvo ne tokie svarbūs, palyginti su darbuotojų noru atlikti nuolatinį auditą.

2.5. Konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelis

Mokslinės literatūros analizės metu nustatyta, kad vidaus audito metu atlikti tam tikri procedūrų kontrolės elementai ir patikrinimai gali turėti reikšmingą poveikį kibernetinio saugumo rizikos vertinimo kokybei ir grėsmės nustatymui. Nors kibernetinės grėsmės rizikos nustatymas vis labiau vertinamas kaip vienas pagrindinių verslo tęstinumą lemiančių veiksnių, organizacijų vadovams sunku įvertinti grėsmės poveikį, susijusį su visa įmonės veikla, ir jį susieti su kylančiais verslo valdymo iššūkiais. Vidaus auditas būdamas vidaus kontrolės sistemos dalis gali visapusiškai įvertinti rizikos valdymą ir kontrolės priežiūrą įmonės veiklos procesuose, padedant įmonei pasiekti savo numatytus strateginius tikslus. Todėl remiantis kibernetinio saugumo rizikos ir vidaus audito procedūrų vertinimo mokslinės literatūros tyrimų ir teorijų analize buvo sudarytas siūlomas konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose modelis. Jis rodo ryšį tarp vidaus audito procedūrų kontrolės elementų ir kibernetinio saugumo rizikos vertinimo organizacijų veiklos kontekste. Modelis sudarytas iš dviejų – kibernetinio saugumo rizikos vertinimo lygio ir vidaus audito procedūrų užtikrinimo lygio – kintamųjų. Šie kintamieji atvirkščiai proporcingai koreliuoja su poveikiu verslo funkcijoms bei kibernetinės atakos nepastebėjimo tikimybe. Pagal tai formuojami organizacijos kibernetinio saugumo rizikos vertinimo būklės rezultatai. Kibernetinio saugumo rizikos vertinimu siekiama nustatyti organizacijos kibernetinės saugumo rizikos lygį, jog tyrimo metu gautus rezultatus būtų galima palyginti tarpusavyje. Platesnis konceptualus vertinimo modelis pavaizduotas 4 paveiksle.

Pateiktame konceptualiame teoriniame modelyje kibernetinio saugumo rizikos vertinimo lygio vertinimas susideda iš keturių teorinėje dalyje išnagrinėtų kategorijų: kibernetinio saugumo rizikos **nustatymo**, su kibernetine saugumo rizika susijusio **valdymo**, atsparumą lemiančio **reagavimo** ir **užtikrinimo** (5 pav.). Kiekviena iš šių kategorijų dar yra išskaidoma į atskirus vertinimo kriterijus, o šie – į kriterijus apibūdinančius veiksnius, kurie pateikti 4 lentelėje ir bus vertinami tyrimo metu.



4 pav. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo teorinis modelis (sudaryta autorės)

Kibernetinio saugumo rizikos vertinimo kategorijos			
Kibernetinio saugumo rizikos nustatymo veiksniai	Kibernetinio saugumo rizikos valdymo veiksniai	Reagavimo į kibernetinio saugumo riziką veiksniai	Kibernetinio saugumo užtikrinimo veiksniai

5 pav. Kibernetinio saugumo rizikos vertinimo kategorijos (sudaryta autorės)

Kibernetinio saugumo rizikos nustatymo veiksniai leis identifikuoti organizacijų silpnąsias sritis ir poveikio grėsmės lygį, nustatyti esamos infrastruktūros ir turimų išteklių lygį, įvertinti taikomas saugumo stebėsenos priemones. Valdymo vertinimu siekiama atkreipti dėmesį, kad kibernetinę saugumo riziką būtina vertinti kaip strateginę, visam organizacijos strateginiam valdymui pavojingą riziką ir nustatyti, kurioje verslo dalyje kibernetinio saugumo pažeidžiamumai galėtų būti identifikuoti. Šioje kategorijoje siekiama įvertinti valdymo struktūros modelį ir kibernetinio saugumo rizikos reguliavimo ir teisinę aplinką, kokią įtaką jiems daro vadovybės požiūris į saugumo užtikrinimą. Atsparumo arba reagavimo į kibernetinio saugumo riziką vertinimas leis nustatyti organizacijos požiūrį į kibernetinių pažeidimų prevenciją – sistemų ir verslo atkūrimo po atakų pasirengimo priemones, verslo tęstinumo užtikrinimą, gebėjimą tinkamai ir greitai reaguoti. Organizacijos turimų duomenų analizė ir priežastinių ryšių tarp įmonės veiksmų ir pasekmių, susijusių su kibernetinio saugumo rizika, nustatymas leidžia formuoti elgsenos modelius, todėl svarbu įvertinti, ar organizacijos tokius duomenis tinkamai panaudoja.

Mokslinėje literatūroje daug dėmesio skiriama kibernetinio saugumo užtikrinimo būdams, priemonėms ir metodams, todėl šis vertinimas susideda iš daugiausiai kriterijų. Užtikrinimo vertinimas apima ne tik kibernetinio saugumo pagrindinių tikslų – vientisumo, prieinamumo, konfidencialumo ir atskaitomybės – kaip įgyvendinimo vertinimą, tačiau ir kibernetinės saugumo rizikos strategijos suderinamumą su rizikos ir kontrolės sistemomis. Žmogiškųjų išteklių, tarp kurių vertinamos darbuotojų kompetencijos ir kibernetinio saugumo rizikos žinios, bei trečiųjų šalių įtakos saugumo įgyvendinimui veiksniai taip pat bus vertinami kibernetinio saugumo užtikrinimo kategorijoje. Be to, kibernetinio saugumo užtikrinimo vertinime siekiama sužinoti organizacijos infrastruktūros, duomenų ir kitų veikloje naudojamų išteklių saugumo lygį, nustatyti, kokį poveikį jis daro bendram kibernetiniam saugumui.

Pagal mokslinę literatūrą sudarytame teoriniame vertinimo modelyje išskirtos antros vertinimo srities – vidaus audito procedūrų užtikrinimo lygio vertinimas susideda iš penkių kategorijų: audito planavimo, audito rizikos įvertinimo, vidaus kontrolės vertinimo, ataskaitų rengimo ir pažangos stebėjimo sričių (6 pav.).

Vidaus audito procedūrų vertinimo kategorijos				
Audito planavimas	Audito rizikos įvertinimas (pasiruošimas)	Vidaus kontrolės vertinimas (vykdymas)	Ataskaitų rengimas	Pažangos stebėjimas

6 pav. Vidaus audito procedūrų vertinimo kategorijos (sudaryta autorės)

Vidaus audito procedūrų integravimas kibernetinio saugumo rizikos vertinimo sprendimuose yra labai priklausomas nuo organizacijos vadovų sprendimų priėmimo užtikrinant visas vidaus audito procedūras, skiriant tam užtektinai išteklių ir siekiant tikslių analitinių įžvalgų, kurios galėtų turėti įtakos verslo tęstinumui ir tobulinimui. Todėl pirmasis svarbus vertinimas prasideda jau audito planavime, kurio metu organizacijos strateginiai tikslai, vadovų požiūris, verslo struktūra yra derinama su prioritetinių rizikų ir ilgalaikių vidaus audito tikslų nustatymu. Sudarytam ir vadovybės

patvirtintam vidaus audito planui reikalinga įvertinti galimą audito riziką, bei su ja susijusias priemones ir išteklius, kurie bus reikalingi vidaus auditui atlikti. Rizikos vertinimas – pasiruošimo auditui etapas, kuris leis nustatyti vertinimo sričių apimtis ir lygį, apims tiesioginius audito programų bei kibernetinio saugumo indikatorius, pagrįstus pagrindinių rizikos rodiklių ir stebėjimo duomenimis.

Vertinant vidaus kontrolės sistemą pagrindinis ir pirmasis vidaus audito darbas yra tinkamumo, efektyvumo bei veiklos kokybės, atliekant vidaus audito plane priskirtas užduotis, peržiūra ir įvertinimas. Vidaus audito tinkamumo peržiūros tikslas yra išsiaiškinti, ar sukurta vidaus kontrolės sistema, įvertinus jos aplinką, procedūras ir stebėseną, suteikia pagrįstą užtikrinimą, kad organizacijos tikslai ir uždaviniai bus pasiekti efektyviai ir ekonomiškai. Vidaus kontrolės vertinimo metu dėmesys taip pat skiriamas informavimo ir komunikacijos kriterijui, vidinių ir išorinių grėsmių vidaus kontrolėje identifikavimą.

Ataskaitų rengimo etape atliekamas bendrų rodiklių atitikties vertinimas turės įtakos svarbiausiam šio mokslinio tyrimo rezultatų nustatymui. Vidaus kontrolės vertinimo srityje nustatyti vidaus audito ir kibernetiniai rodikliai turėtų sutapti ir bendradarbiauti, o bendrų rodiklių ir veikimo taškų nustatymas turėtų tapti esminiais tyrimo rezultatais. Po rezultatų aptarimo ir galutinės nuomonės suformulavimo bei išvadų su pasiūlymais pristatymo organizacijos vadovybei prasideda pažangos stebėjimas, kurio metu grįžtama prie vidaus audito plano, analizuojamos gautos išvados, rengiami pasiūlymai ateities vidaus auditams, atliekama buvusių auditų pastabų ištaisymo analizė.

3. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio tyrimo metodologija

Tyrimo problema. Atlikus mokslinės literatūros analizę buvo nustatyta, jog kibernetinio saugumo rizikos vidaus audito procedūrose vertinimas gali turėti reikšmingą teigiamą įtaką vertinamų organizacijų vertės užtikrinimui, duomenų saugumui ir veiklos efektyvumo gerinimui. Kibernetinio saugumo rizikos vertinimo integravimui į organizacijų vidaus audito procedūras reikalingas kompleksiškas ir bendras visos organizacijos darbas, kurį užtikrinti padėtų papildomi ištekliai (tiek finansiniai, tiek žmogiškieji) bei tam tikri valdymo sprendimai. Dėl šios priežasties organizacijų vadovai privalo įvertinti vidaus audito procedūrų pritaikomumą kibernetinio saugumo rizikos kontekste, analizuoti tobulintinas vidaus audito procedūras tam, kad jos leistų ne tik įvertinti bendrą organizacijų valdymą ir vidaus kontrolę, tačiau ir tam, jog šios procedūros taptų įrankiu, leidžiančiu išvengti, arba iš anksto identifikuoti, kibernetinio saugumo grėsmes.

Analizuotos mokslinės literatūros dalyje aprašytos teorinės kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo gairės, tačiau pastebėtas praktinių tyrimų trūkumas. Šių tyrimų pagrindu organizacijų vadovybė galėtų analizuoti ir užtikrinti praktinį vidaus audito procedūrų pritaikymą kibernetinio saugumo rizikos vertinimo sprendimuose bei įvertinti esamą organizacijos kibernetinio saugumo rizikos būklę vidaus audito procedūrų kontekste. Šios atliktos analizės leistų organizacijų vadovybei atlikti valdymo sprendimus, susijusius su atitinkamų rizikų prisiėmimo ar išteklių jų sumažinimui skyrimo. Būsimu tyrimu siekiama patikrinti konceptualaus teorinio modelio praktinio taikymo galimybes, kuriomis organizacijos galėtų įvertinti kibernetinio saugumo rizikos vidaus audito procedūrose būklę. Šie vertinimai taptų ne tik metodika gretutinių organizacijos sričių apsaugos ir valdymo lygio gerinimui, tačiau taip pat leistų palyginti savo vertinimus su kitomis organizacijomis ir taip prisidėtų prie bendro sektoriaus ar šalies kibernetinio saugumo užtikrinimo.

Empirinio tyrimo tikslas – empiriškai patikrinti konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelį.

Empirinio tyrimo uždaviniai:

1) Nustatyti analizuojamų organizacijų esamą kibernetinio saugumo rizikos vidaus audito procedūrose būklę;

2) Išanalizuoti ir palyginti analizuojamų organizacijų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatus;

3) Pateikti rekomendacinius pasiūlymus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimui.

Tyrimo metodai. Siekiant empiriškai patikrinti konceptualaus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelio praktinio taikymo galimybes buvo atliktas kokybinio pobūdžio atvejo studijos metodo tyrimas. Šio metodo taikymas leidžia surinkti ir sujungti duomenis iš įvairių šaltinių ir taip išsamiai įvertinti tiriamą reiškinį, atsižvelgiant į kontekstą, kuriame jis yra arba kurio ribos, tarp reiškinio ir konteksto nėra aiškiai matomos (Yin, 2009). Atvejų studijos metodas yra sukurtas tam, kad būtų galima tyrime dalyvaujančių dalyvių požiūriu išsiaiškinti nagrinėjamos temos detales, naudojant kelis duomenų šaltinius (Tellis, 1997).

Pasirinkta atlikti daugybinė atvejų studijų analizė, kuri leido situaciją vertinti ne tik iš tyrime dalyvavusių, bet ir iš dalyvių atstovaujamų grupių perspektyvos (Tellis, 1997), taip pat paaiškinti teorinius priežastinius ryšius praktinėje situacijoje (Yin, 2009). Analitiniame apibendrinime sukurtas teorinis konceptualus modelis tyrime naudotas kaip šablonas, su kuriuo lyginti empirinių atvejų tyrimo rezultatai. Tai leido patvirtinti arba paneigti tiriamus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo kriterijus.

Šiame darbe atvejo studijos metodas padėjo išanalizuoti kibernetinio saugumo rizikos vidaus audito procedūrose vertinimą trijose organizacijose. Pagal mokslinę literatūrą sudarytas teorinis modelis leido įvertinti skirtingų organizacijų kibernetinio saugumo rizikos būklę vidaus audito procedūrose ir atskleidė šių procedūrų skirtumus ir poveikį, kurių pagrindu bus galima pateikti tolimesnes tyrimo rezultatų interpretacijas.

Duomenys tyrimui buvo renkami pusiau struktūruotu ekspertinio interviu metu, susitinkant su įmonių kibernetinio saugumo ir vidaus audito atstovais vaizdo skambučio pokalbiui. Prieš tai, pagal sudarytą konceptualų teorinį modelį, buvo parengtas išsamus interviu protokolas, kuriame numatyti konkretūs klausimai ir pilnas interviu planas. Respondentams buvo pateikiami atvirojo tipo klausimai, kuriems nebuvo pateikiami galimi atsakymo variantai, todėl buvo galima užduoti tikslinančius ar papildančius klausimus, kylančius pokalbio eigoje. Pirmasis vertinamo modelio kriterijų klausimas reikalavo atsakymo TAIP/NE, o antrasis buvo užduodamas kaip jį papildantis, kuriame atstovai galėjo plačiau pakomentuoti vertinamą situaciją ar turimas įžvalgas. Vėliau, interviu metu gauti rezultatai buvo susisteminti naudojant lyginamąją analizę – susisteminami kiekvienos organizacijos rezultatai pagal du atskirus vertinimus atskirai, o vėliau bendri įmonės rezultatai palyginami tarpusavyje su kitomis analizuotomis organizacijomis.

Tyrimo instrumentas. Tyrimui atlikti buvo sudarytas interviu protokolas, kuris remiasi pagal mokslinę literatūrą sudarytame teoriniame konceptualiame modelyje numatytomis kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo kategorijomis. Interviu klausimynas sudarytas iš 35 kibernetinio saugumo riziką vidaus audito procedūrose vertinamų kriterijų aktualumą organizacijoje patvirtinančių/paneigiančių klausimų, kur kiekvienas klausimas atspindi vieną vertinamą kriterijų (kibernetinio saugumo rizikos vertinimą sudaro 20, vidaus audito procedūrų užtikrinimą – 15 klausimų). Klausimyne taip pat numatyti 47 papildantys klausimai, reikalingi plačiau apibūdinti organizacijoje vykdomus procesus, naudojamas priemones, sukauptą naudingąją patirtį, jei į pirmąjį klausimą buvo atsakyta teigiamai. Kibernetinio saugumo rizikos vertinimo procedūrų kategorijų kriterijai ir juos apibūdinantys veiksniai pateikiami 4 lentelėje.

4 lentelė. Kibernetinio saugumo rizikos vertinimo kategorijų vertinimo kriterijai ir juos apibūdinantys veiksniai (sudaryta autorės, remiantis ACCA, 2019; Ahia ir Deloitte, 2017)

Vertinimo kategorijos	**Vertinimo kriterijus**	**Vertinimo kriterijų apibūdinantys veiksniai**
Nustatymas	Grėsmių identifikavimas	– Išteklių poreikis identifikuoti rizikas; – Pagrindinių duomenų (įmonės informacijos) įvertinimas; – Kibernetinės rinkos stebėjimas ir analizė
	Infrastruktūros vertinimas	– IT turto įvertinimas; – Kritinės infrastruktūros nustatymas
	Poveikio analizė	– Grėsmės poveikio įvertinimas; – Kritinės infrastruktūros poveikio vertinimas

Vertinimo kategorijos	Vertinimo kriterijus	Vertinimo kriterijų apibūdinantys veiksniai
Nustatymas	Saugumo informacijos stebėsena	– Saugos žurnalų valdymas; – Įsiskverbimo bandymai; – Saugumo informacijos ir veiksmų valdymas; – Metrikos ir ataskaitos
Valdymas	Valdymo modelis ir struktūra	– Kibernetinio saugumo valdymo struktūra; – Valdymo komiteto struktūra; – Pareiginiai nuostatai
	Vadovybės įtaka	– Vadovų įsitraukimas; – Valdymo ir kibernetinės rizikos sąsaja
	Reguliavimo ir teisinė aplinka	– Kibernetinio saugumo strategija; – Įstatytų ir teisės aktų atitikties politika ir teisė
Reagavimas	Kibernetinės rizikos analitika	– Integracija į organizacijos veiklos kontrolės sistemas; – Atsakomybė ir atskaitingumas; – Kibernetinio saugumo rizikos aktualijos
	Prognozės ir elgsena	– Poveikio verslui analizė; – Verslo tęstinumo planavimas; – Krizių komunikacijos planas
	Priežastiniai ryšiai	– Duomenų pritaikomumas; – Veiksmai-pasekmės ryšio įvertinimas
	Atsako planavimas	– Atsako sprendimų modeliai; – Grėsmės ištaisymo mechanizmai (duomenų atkūrimas, pagalba, kompensacijos); – Grėsmės pratybos; – Incidentų valdymo planas
Užtikrinimas	Saugumo programų valdymas	– Strategijos, standartai, bazinės linijos, gairės ir procedūros; – Biudžeto valdymas; – Turto valdymas; – Pokyčių valdymas; – Programų ataskaitos; – Rizikos ir atitikties valdymas
	Duomenų apsauga	– Duomenų klasifikavimas; – Duomenų apsaugos strategija; – Informacijos įrašų valdymas; – Įmonės turinio valdymas; – Duomenų kokybės valdymas; – Duomenų praradimo prevencija
	Tapatybės ir prieigos valdymas	– Prieigos aprūpinimas; – Privilegijuotų vartotojų valdymas; – Prieigos identifikavimas; – Prieigos sertifikavimas; – Prieigos tvarkymas ir valdymas; – Bendrų prieigų valdymas
	Tinklo ir infrastruktūros apsauga	– "Grūdinimo" standartai; – Saugumo dizainas/ architektūra; – Konfigūracijų valdymas; – Tinklo apsauga; – Tinklo veiklos ir išorinių pranešimų apie atakas stebėjimas; – Saugumo operacijų valdymas
	Programinės įrangos apsauga	– Saugumo kūrimas ir nuolatinis testavimas; – Saugumo kodavimo gairės; – Programų prieiga ir dizainas; – Plėtros gyvavimo ciklas; – Saugumo „skylių" valdymas

Vertinimo kategorijos	Vertinimo kriterijus	Vertinimo kriterijų apibūdinantys veiksniai
Užtikrinimas	Trečiųjų šalių valdymas	– Vertinimas ir atranka; – Sutarčių ir paslaugų iniciacija; – Nuolatinis stebėjimas; – Paslaugų nutraukimas
	Debesijos sistemų valdymas	– Debesijos sistemų strategija; – Debesijos sistemų rizikos identifikavimas; – Debesijos teikimo inventorius; – Minimalios kontrolės saugumo riba; – Debesijos kontrolės atitiktis
	Darbuotojų kompetencijos	– Kibernetinės rizikos nustatymas; – Kibernetinės rizikos valdymas; – Reagavimas į kibernetinę riziką; – Kibernetinio saugumo užtikrinimas
	Personalo mokymai	– Fizinė apsauga; – Sukčiavimo simuliacijos pratimai; – Saugumo mokymai ir informavimas

Konceptualiame kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelyje pateiktų vidaus audito procedūrų vertinimo kategorijų kriterijai pateikiami 5 lentelėje.

5 lentelė. Vidaus audito procedūrų kategorijų vertinimo kriterijai ir juos apibūdinantys veiksniai (sudaryta autorės, remiantis ACCA, 2019; Ahia ir Deloitte, 2017)

Vertinimo kategorijos	Vertinimo kriterijus	Vertinimo kriterijų apibūdinantys veiksniai
Audito planavimas	Ilgalaikis planavimas	– Vidaus audito veiklos biudžeto sudarymas; – Išteklių paskirstymas; – Vidaus audito ilgalaikio plano atnaujinimas
	Apimties planavimas	– Audito subjektų prioritetų nustatymas; – Atsakingų padalinių ir procesų (darbų) paskirstymas; – Žmogiškųjų ir finansinių išteklių poreikio įvertinimas
	Vidaus audito plano sudarymas	– Audito rizikos vertinimas; – Organizacijos ir vadovybės indėlis; – Konsultavimo paslaugos; – Siūlomos audito procedūros pagrindas, tikslai, apimtis ir atsakomybė
	Patvirtinimas	– Reikalavimai ištekliams; – Reikšmingi tarpiniai pakeitimai; – Galimi išteklių apribojimų padariniai; – Bendradarbiavimas, apimantis visus valdymo lygius
Audito rizikos vertinimas (pasiruošimas)	Personalo/ žmogiškųjų išteklių strategija	– Darbuotojų hierarchiškumas organizacijos viduje; – Auditorių kvalifikacija (profesiniai sertifikatai); – Tinkamo dydžio specialistų komanda; – Personalo vertinimo programa; – Įdarbinimo praktikos; – Unikalių, nišinių specialistų poreikis (dalykinė kompetencija); – Profesinės priežiūros standartai; – Tobulinimosi programos
	Resursų valdymas	– Užsakomosios paslaugos; – Darbo valandų paskirstymas; – Darbo grupių sudarymas; – Resursų valdymo atsakomybė ir atskaitomybė

Vertinimo kategorijos	Vertinimo kriterijus	Vertinimo kriterijų apibūdinantys veiksniai
Vidaus kontrolės vertinimas (vykdymas)	Kontrolės aplinka	– Organizacijos darbinė aplinka; – Verslo etikos lygis; – Vadovų pavyzdžiu formuojama elgesio praktika; – Darbinės aplinkos gerinimo priemonės
	Informavimas ir komunikavimas	– Vidinių ir išorinių informacijos srautų priėmimas ir tinkamas jų pritaikymas; – Vadovų grįžtamasis ryšys, susijęs su praėjusių metų vidaus auditais
	Rizikos įvertinimas	– Vidinių grėsmių organizacijos tikslų pasiekimui identifikavimas ir analizė; – Išorinių grėsmių organizacijos tikslų pasiekimui identifikavimas ir analizė
	Kontrolės priemonės	– Rezultatų kontrolė; – Veiksmų kontrolė; – Personalo-motyvacinė kontrolė; – Organizacijos kultūra; – Pareigų atskyrimas
	Stebėsena	– Praėjusių vidaus auditų atsako į išvadas, pastabas ir rekomendacijas vertinimas ; – Praėjusių laikotarpių oauditinės veiklos vertinimas
Ataskaitų rengimas	Rezultatų aptarimas	– Vadovybės įtaka galutinei ataskaitai; – Koregavimų poreikis
	Atitikties testavimas	– Kibernetinio saugumo rizikos ir vidaus audito rodiklių sutapties vertinimas; – Rodiklių priklausomybių nustatymas
	Galutinė ataskaita	– Nuomonės suformulavimas; – Išvadų pateikimas skirtingoms sritims
Pažangos stebėjimas	Pažangos stebėjimo etapai	– Rekomendacijos rizikų suvaldymui

Tyrime dalyvavusių organizacijų atstovams buvo užduodami vertinimo klausimai (klausimynas pateikiamas priede Nr. 1). Pirmasis reikalauja atsakymo taip arba ne ir siekia nustatyti, ar vertinamas kriterijus aktualus organizacijos kontekste. Jei atsakymas teigiamas, užduodamas jį papildantis klausimas, kuriuo galima būtų įvertinti organizacijoje taikomus metodus, priemones ir sprendimus, susijusius su kibernetinio saugumo rizikos vidaus audito procedūrose vertinimu. Vertinant visus kibernetinio saugumo rizikos vidaus audito procedūrose kriterijus naudojama penkių balų įverčių sistema, su kuria tyrimo dalyviai nebuvo supažindinti, o įverčių balų reikšmės pritaikytos kiekvienam klausimui individualiai pagal vertinamą kriterijų. Apibendrinta įverčių reikšmių atitiktis su paaiškinimais nurodyta 6 lentelėje.

Pagal pateiktą kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo sistemą įverčiais buvo įvertintas kiekvienas tyrime vertinamą kriterijų apibūdinantis respondentų atsakymas. Bendra vertinimo sistemos įverčių suma atspinti kibernetinio saugumo rizikos ir vidaus audito procedūrų užtikrinimo lygius pagal anksčiau sudarytą teorinį modelį. Kibernetinio saugumo rizikos vertinimo didžiausia įverčių suma yra 100, jį sudarė 20 vertinimo kriterijų. Vidaus audito procedūrų užtikrinimo vertinimą sudarė 15 kriterijų, todėl bendra didžiausia šio vertinimo suma – 75 balai.

6 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo sistema (sudaryta autorės)

Įvertis	**Įverčio reikšmė**	**Paaiškinimas**
1	Kriterijus visiškai neatitinka	Organizacija nesiima jokių veiksmų, kuriais užtikrintų kibernetinio saugumo rizikos ar vidaus audito procedūrų užtikrinimo vertinimą.
2	Kriterijus neatitinka, tačiau vertinamas kaip svarbus	Organizacija šiuo metu nesiima veiksmų, kuriais užtikrintų kibernetinio saugumo rizikos ar vidaus audito procedūrų užtikrinimo vertinimą, tačiau planuoja tai daryti artimiausiu metu (arba vertina tai svarbiu vertinimo indėliu).
3	Kriterijus vidutiniškai atitinka	Organizacijoje kibernetinio saugumo rizikos ar vidaus audito procedūrų užtikrinimo vertinimas yra ribojamas.
4	Kriterijus atitinka	Organizacijoje kibernetinio saugumo rizikos ar vidaus audito procedūrų užtikrinimo vertinimas yra įmanomas.
5	Kriterijus visiškai atitinka	Organizacijoje kibernetinio saugumo rizikos ar vidaus audito procedūrų užtikrinimo vertinimas yra atliekamas, taikomos priemonės turi teigiamą įtaką visos organizacijos veiklai.

Tyrimo dalyviai. Tyrimo metu vertintos 3 organizacijos, kurios vykdo vidaus audito procedūras ir teikia vidaus audito ataskaitas vadovybei, siekiant efektyvesnio įmonės veikimo ir tinkamų kontrolės priemonių užtikrinimo. Platesniam modelio patikrinimui buvo atrinktos skirtingo dydžio organizacijos iš skirtingų verslo sektorių. Vidaus audito privalomas vykdymas nebuvo organizacijų atrankos kriterijus. Kadangi tyrimas susijęs tiek su kibernetinio saugumo rizikos vertinimu, tiek su vidaus audito procedūrų užtikrinimu, tyrimo metu buvo siekta apklausti analizuojamų organizacijų atstovus, kurie tiesiogiai dirba su kibernetinio saugumo užtikrinimu ir/arba atlieka vidaus auditą. Šie minėti organizacijų atstovai atsakinėdami į klausimus galėjo atskleisti tiksliausią įmonės informaciją.

Vertinime sutiko dalyvauti šios organizacijos:
1. Informacinių ir ryšių technologijų paslaugas teikianti organizacija (įmonė A);
2. Telekomunikacijų paslaugas teikianti organizacija (įmonė B);
3. Įvairias finansines paslaugas teikianti organizacija (įmonė C)

Duomenų rinkimas. Tyrimo duomenų rinkimas buvo atliktas 2021 m. balandžio mėnesį organizuojant individualius vaizdo skambučių susitikimus su analizuojamų organizacijų atstovais. Interviu su tyrimo dalyviais užtruko nuo 72 iki 89 minučių, priklausomai nuo atvirų klausimų išsamumo ir juos papildančių klausimų poreikio, buvo naudotas pusiau struktūruoto ekspertinio interviu metodas.

4. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tyrimo rezultatai

Teorinės baigiamojo projekto dalies pagrindu sudarytas konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo modelis tikrinamas atliekant tyrime sutikusių dalyvauti organizacijų, kuriose vykdomas vidaus auditas, atvejo analizę. Siekiant įvertinti organizacijų kibernetinio saugumo rizikos vidaus audito procedūrose lygį buvo prašoma įmonių vidaus audito ar kibernetinio saugumo užtikrinimo atstovų ne tik įvertinti, ar organizacija taiko modelio pagrindu išskirtus veiksnius, bet ir išsamiau apibūdinti taikomus metodus, priemones, pasidalinti patirtimi ir įžvalgomis. Toliau yra pateikiami analizuotų įmonių kibernetinio saugumo vidaus audito procedūrose vertinimai, šių vertinimų analizė bei rekomendacijos.

4.1. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai A įmonėje

A įmonė yra lietuviško kapitalo bendrovių grupė, save apibūdinanti kaip naujausias technologijas į Baltijos ir kitas pasaulio šalis atnešanti organizacija. Pagrindinė įmonės veikla – didmeninė įvairių elektronikos įrenginių prekyba ir remontas, saulės energetikos projektų vystymas ir jų valdymas. Pagrindine organizacijos kibernetinio saugumo rizika įmonė įvardina elektroninių paslaugų ir tinklo saugumo sutrikdymą, kuris taptų svarbus organizacijos, jos klientų, darbuotojų ir susijusių asmenų duomenų saugumui, nes beveik visi duomenys kaupiami serveriuose ir debesijos sistemose. Žemiau yra pristatomi kibernetinio saugumo rizikos vertinimo A įmonėje rezultatai (7 lentelė). Lentelėje pateikiamos interviu metu gautų atsakymų citatos, kurios patvirtina arba paneigia vertinimo metu tikrinto kriterijaus aktualumą organizacijos veikloje. Atsakymas taip pat įvertintas atitinkamu įverčiu pagal iš anksto paruoštą vertinimo rangų skalę (1 priedas).

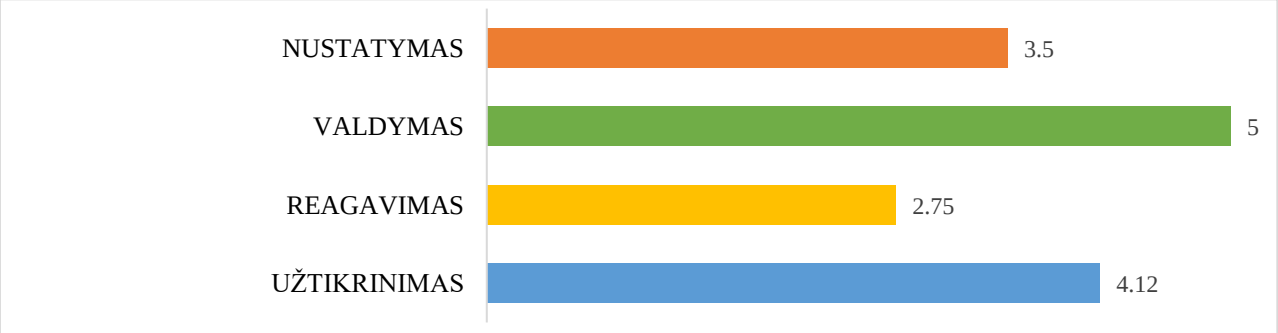
7 lentelė. Kibernetinio saugumo rizikos vertinimo A įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	**Citata, pagrindžianti arba paneigianti kriterijaus svarbumą**	**Įvertis, pagal sudarytus įverčio rangus**
Grėsmių identifikavimas	„**Taip**, nes yra IT skyriuje atsakingi žmonės už sistemas, kurie prižiūri ir kibernetinį saugumą [...] yra pasitvirtinę keletas, pvz. bandymas pasisavinti pinigus įsilaužiant į tiekėjo pašto dėžutę, nukopijuojant jų sąskaitos šabloną, bet pakeičiant banko sąskaitos numerį ir persiunčiant tokią sąskaitą prašant pamokėti į naują banko sąskaitą. Kadangi banko sąskaitų keitimai programoje yra neleidžiami, buvo imtasi papildomo patikrinimo ir nustatyta, kad tai buvo sukčiai. Taip pat siunčiami priminimai dėl neaiškių e'mailų atidarymo, kuriose būna prikabinti virusai“	5
Infrastruktūros vertinimas	„Manau, kad **taip**, infrastruktūra pakankama. Negaliu tiksliai pasakyti kas vertinama, bet stebimos sistemos, diegiami firewalls, reikalingi įvairūs patvirtinimai, tam tikrų teisių suteikimas ar veiksmų atlikimas galimas tik tam tikriems darbuotojams“	4
Poveikio analizė	„Tokia, kaip analizė, **nėra atliekama**, tačiau grėsmės žinomos ir su jomis yra supažindinami darbuotojai“	1
Saugumo informacijos stebėsena	„**Taip**, diegiami įvairūs sistemų naujinimai, saugumo sistemų naujinimai, atliekamas darbuotojų švietimas ir nuolat primenama dėl tam tikrų rizikingų situacijų“	4
Valdymo modelis ir struktūra	„**Taip**, kibernetinės rizikos valdymo analizei skiriamas didelis dėmesys, yra priimtos kibernetinio saugumo tvarkos ir paskirti atsakingi žmonės, suvaldyti šias rizikas. Sprendimus priima aukščiausio lygio vadovai remdamiesi rizikų valdymo komiteto patarimais“	5

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Vadovų požiūris	„**Taip**, vadovai tai identifikuoja kaip didelę riziką, ypač pastaruosius kelis metus, todėl į tai atsižvelgiama priimant valdymo sprendimus, skiriant biudžetą ir pan.“	5
Reguliavimo ir teisinė aplinka	„**Taip**, kibernetinio saugumo rizikos reguliavimo ir teisinė politika parengta vadovaujantis teisiniais aktais, įvairiomis gairėmis [...] yra sudaryti incidentų valdymo planai tam tikriems, dažniausiai sutinkamiems, incidentams atpažinti ir valdyti“	5
Kibernetinės rizikos analitika	„Analitika **vykdoma** ir integruota į bendras veiklos kontrolės sistemas, aktualijos visada analizuojamos ir atnaujinami procesai, susiję su jomis […] taip pat informuojami darbuotojai apie naujų rizikų atsiradimą”	5
Prognozės ir elgsena	„[...] įmonė tokių duomenų, kiek žinau, **nekaupia** ir **neanalizuoja**“	1
Priežastiniai ryšiai	„Atskira analizė būtent priežastiniams ryšiams ieškoti **tikrai nėra atliekama**, tiesiog organizacijos atsakingi žmonės tikrai žino veiksmus ir juos lydinčias pasekmes [...] organizacijos vadovybė deda daug pastangų į tai“	1
Atsako planavimas	„Manau, kad **taip**. Duomenų atkūrimas yra pagrindinis ir svarbiausias grėsmės ištaisymo mechanizmas”	4
Saugumo programų valdymas	„**Taip**, įmonė turi bendrą organizacijos kibernetinio saugumo programą su visais ją lydinčiais Europos Sąjungos standartais ir gairėmis. […] programa dalyvauja biudžeto valdyme, nes norint įdiegti tam tikrus saugos mechanizmus reikalingi piniginiai resursai, kuriuos reikia biudžetuoti. […] atsižvelgiama ir į turimą turtą, jo saugumą ir galimybes jį tobulinti”	5
Duomenų apsauga	„Duomenų apsaugos strategija taip pat **yra**. Kalbant apie asmens duomenis, yra pasamdytas žmogus, kuris atsakingas tik už BDAR klausimus ir jis stebi šiuos duomenis, identifikuoja rizikas ir leidžia tvarkas, kuriomis turime vadovautis. [...] dėl duomenų apskritai, tai visos kopijos yra saugomos serveriuose“	4
Tapatybės ir prieigos valdymas	„**Taip**, kiekvienas darbuotojas turi savo identifikacinį kodą, taip pat norint prisijungti reikia suvesti slaptažodį, kuris keičiamas kas kelis mėnesius. Norint prisijungti nuotoliu, kiekvienas darbuotojas suvedęs savo kodą ir slaptažodį į savo telefono numerį gauna kodą, kurį turi suvesti per minutę - kiekvienam prisijungimui generuojamas naujas kodas. […] ir tai, kad ribojamos teisės ir ne prie visų sistemų, dokumentų ar failų gali prieiti visi darbuotojai”	5
Infrastruktūros apsauga	„**Taip**, [...] įvairūs prisijungimo kodai, nuolat keičiami slaptažodžiai. Pritariu, kad prie infrastruktūros apsaugos gerinimo prisideda bendra tinklo apsauga, todėl, kad stebint naujienas ir atakas galima pasiruošti ir identifikuoti silpnas įmonės tinklo vietas [...] bet kokiu atveju, tiek tinklas, tiek infrastruktūra, tiek kitos veikloje naudojamos priemonės yra labai susiję“	5
Programinės įrangos apsauga	„Atskirų ar papildomų reikalavimų programinei įrangai **neturime**, manau, kad už tai atsakingi platintojai ar apsauginių programinių įrangų, tokių kaip pvz. antivirusinės, gamintojai ir platintojai. [...] įmonėje viskas vertinama pagal Europos Sąjungos reikalavimus“	3
Trečiųjų šalių valdymas	„**Taip**, pasirašomos sutartys, partneriai vertinami pagal "Partnerių patikimumo" tvarką, [...] taip pat didelį monitoringą atlieka ir bankai, todėl tai nėra tik iš įmonės vidaus kylantis poreikis, to nori ir išoriniai partneriai“	5

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Debesijos sistemų valdymas	„Papildomų reikalavimų ar valdymo stebėsenos debesų programoms **neatliekame**, tai paslaugas teikiančios įmonės atsakomybė [...] manau, kad jei atitinka bendrus Europos Sąjungos reikalavimus, tai yra pakankami“	2
Darbuotojų kompetencijos	„Manau, kad darbuotojų kompetencijos **yra pakankamos** atlikti darbus, už kuriuos jie yra atsakingi”	3
Mokymai	„**Taip**, kibernetinio saugumo mokymai vyksta bendrai visiems darbuotojams, reguliariai”	5

Toliau yra aptariami A įmonės kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai.

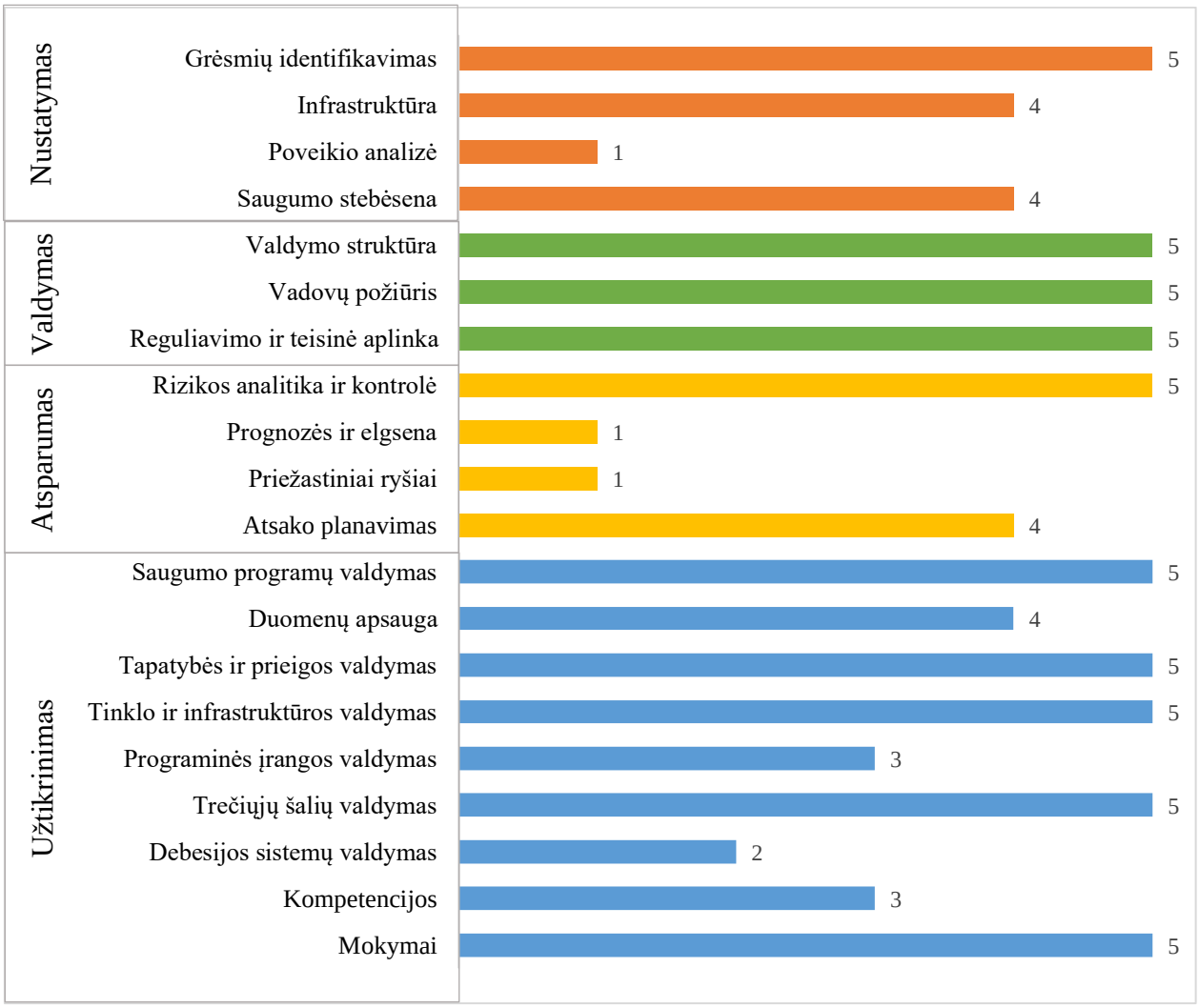


7 pav. Kibernetinio saugumo rizikos kategorijų vertinimas A įmonėje (sudaryta autorės)

Įvertinus kibernetinio saugumo rizikos kategorijų vertinimo įverčius A įmonėje gauti 77 balai iš 100 galimų. Pagal sudarytą konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose modelį toks vertinimas atitinka **aukštą** kibernetinio saugumo rizikos vertinimo lygį ir lemia žemą rizikos poveikį įmonės veiklos procesams. Pagal kibernetinio saugumo rizikos vertinimo kriterijų aritmetinius vidurkius (7 pav.) galima teigti, kad organizacija skiria pakankamai dėmesio visiems kibernetinio saugumo riziką vertinamoms kategorijoms, o patį didžiausią – valdymo kategorijos procesų užtikrinimui. Organizacija turi pakankamai kompetencijų ir išteklių apsaugoti fizinę ir tinklinę infrastruktūrą bei užtikrinti tinkamą jos valdymą, tačiau visiškai neatlieka įsilaužėlių elgsenos prognozavimo ir priežastinių ryšių tarp organizacijos atliekamų operacijų ir pasekmių, susijusių su kibernetinio saugumo rizika, vertinimo. Tai patvirtina ir kiti vertinimo rezultatai, kurie rodo, kad įmonė taip pat neskiria tinkamo dėmesio kibernetinio saugumo rizikos poveikio analizei, kuri teorinėje darbo dalyje įvardinta kaip viena pagrindinių verslo tęstinumo planavimą lemiančių veiksnių. Dėl šių priežasčių organizacija negali pasiekti aukščiausio kibernetinio saugumo rizikos vertinimo lygio ir gebėti įvertinti patį nežymiausią kibernetinio saugumo rizikos poveikį įmonės procesams.

Pagal atskirų kibernetinio saugumo rizikos kategorijų vertinimo rezultatus (8 pav.), kurie pagrįsti interviu metu gautais įmonių atstovų atsakymais (7 lentelė) galima teigti, kad organizacija gali pakankamai gerai nustatyti kibernetinio saugumo riziką savo įmonės procesuose. Grėsmių identifikavimui skiriamas didelis informacinių technologijų specialistų dėmesys, kurie atsakingi tiek už infrastruktūros vertinimo, tiek už saugumo stebėsenos funkcijas. Tai patvirtina teorinėje dalyje nagrinėtą organizacijų požiūrio problemą, kuri teigė, kad kibernetinio saugumo rizika yra suprantama kaip informacinių technologijų specialistų atsakomybė, nors nagrinėti mokslinių tyrimų literatūros

šaltiniai įrodė, kad kibernetinio saugumo rizika daro įtaką visiems organizacijos veiklos procesams. Infrastruktūros vertinimo funkcijoms užtikrinti organizacija naudoja kelių žingsnių autentifikavimo ir prieigos kontrolę, įmonėje yra patvirtinta slaptažodžių politika, nuolat atliekami automatiniai įrenginių atnaujinimai, daugumoje įrenginių įdiegtos antivirusinės programos su integruotomis ugniasienėmis. Saugumo informacijos stebėseną užtikrina nuolatiniai sistemų atnaujinimai, kibernetinio saugumo rizikos visų darbuotojų mokymai ir identifikuotų grėsmių patikra. Visos šios organizacijos naudojamos priemonės galėtų sėkmingai prisidėti prie kibernetinio saugumo rizikos duomenų rinkimo ir tolimesnės analizės, tačiau poveikio analizės vertinimas parodo, kad ji nėra atliekama. Kibernetinio saugumo rizikos poveikio analizė yra grindžiama pasitikėjimu kiekvieno darbuotojo žiniomis ir atsakomybėmis, todėl nėra atskirai analizuojama. Organizacija taip pat neturi nusistačiusi poveikio ribos, nuo kurios turi būti pradedama imtis papildomų saugumo rizikos veiksmų, todėl šiam kriterijui buvo suteiktas žemiausias įvertis.



8 pav. Kibernetinio saugumo rizikos kriterijų vertinimas A įmonėje (sudaryta autorės)

Vertinant valdymo kategorijos kriterijus – valdymo modelį ir struktūrą, vadovybės įtaką bei reguliavimo ir teisinę aplinką – visiems buvo suteikti aukščiausi balai. Įmonė A turi suformuotą rizikos valdymo komitetą, kurio rekomendacijomis yra parengtos bendros ir individualizuotos pagal veiklos sritis kibernetinio saugumo rizikos aprašų tvarkos, nurodymai, paskirti atsakingi juos užtikrinantys asmenys. Kibernetinio saugumo rizikos reguliavimo ir teisinę įmonės aplinką užtikrina kviestiniai teisės specialistai, kurie parengia reikalingus dokumentus pagal organizacijos rizikos

valdymo komiteto nurodymus ir šiuo metu Lietuvoje galiojančius teisinius aktus ir gaires. Parengtų tvarkų laikymąsi užtikrina rizikos valdymo komitetas, kuris kartu su informacinių technologijų specialistais parengia incidentų valdymo planus bei su jais supažindina atsakingus darbuotojus. Vadovybės įtakos vertinimas parodė, kad organizacijos vadovai suvokia didėjančią kibernetinio saugumo rizikos svarbą visos įmonės veiklos kontekste, todėl valdymo modelis ir sprendimai koreguojami priklausomai nuo rizikos komiteto analizės ir rekomendacijų. Tai, kad strateginius sprendimus, susijusius su kibernetinės saugumo rizikos vertinimu, priima aukščiausio lygio vadovai leidžia daryti išvadą, kad šios organizacijos vadovai turi pakankamai žinių apie savo veiklą ir jai kylančias rizikas. Vadovų įsitraukimas taip pat lemia greitesnę reakciją į kylančią grėsmę bei vadovų elgesiu formuojamą pavyzdį darbuotojams.

Kibernetinio saugumo rizikos vertinimo reagavimo kategorija surinko mažiausius įverčius, kadangi nėra atliekamas įsilaužėlių elgsenos prognozavimo ir priežastinių ryšių tarp organizacijos atliekamų operacijų ir pasekmių, susijusių su kibernetinio saugumo rizika, nustatymas. Elgsenos prognozavimo ir priežastinių ryšių duomenų nekaupimas glaudžiai susijęs su kibernetinio saugumo rizikos nustatymo kategorijos poveikio analizės kriterijaus vertinimu, nes nekaupiami duomenys neleidžia atlikti tolimesnės analizės. Įdomu tai, kad nors duomenys elgsenos prognozavimui ir priežastinių ryšių nustatymui nėra renkami, kibernetinio saugumo rizikos analitika organizacijoje yra atliekama. Ji integruota į visas veiklos kontrolės sistemas, siekiant padidinti kibernetinio saugumo rizikos atsparumą organizacijos procesuose, taip pat yra stebimos, analizuojamos ir pritaikomos su kibernetine saugumo rizika susiję aktualijos, o visa tai leidžia šį vertinamo kriterijų įvertinti aukščiausiu balu. Atsako į kibernetinę grėsmę planavimui įmonė A naudoja kviestinių kibernetinio saugumo specialistų teikiamas paslaugas ir produktus, kurie pritaiko sprendimų modelius pagal organizacijos turimą infrastruktūrą. Kadangi organizacijoje yra numatytas tik vienas grėsmės ištaisymo mechanizmas – duomenų atkūrimas, tai neleido šio kriterijaus įvertinti pačiu aukščiausiu lygiu. Įmonės A reagavimo į kibernetinio saugumo riziką kategorijos sritis yra labiausiai tobulintina, nes trūksta duomenų kaupimo ir platesnės analitikos. Ji galėtų padėti nustatyti tolimesnę veiksmų ir sprendimų eigą, o tai padidintų organizacijos atsparumą kibernetinio saugumo rizikai.

Kibernetinės saugumo rizikos užtikrinimui nagrinėtoje literatūroje buvo skiriamas didžiausias dėmesys. Įmonės A vertinimas parodė, kad šios kategorijos būklė yra pakankamai gera ir organizacija skiria pakankamai išteklių jai palaikyti ir užtikrinti. Patys aukščiausi įverčiai buvo skirti saugumo programų, tapatybės ir prieigos, tinklo ir infrastruktūros bei trečiųjų šalių valdymo kriterijų vertinime. Įmonėje patvirtintos ir visos organizacijos mastu vykdomos kibernetinio saugumo rizikos programos, parengtos pagal Europos Sąjungos standartus ir gaires. Šios programos vertinamos organizacijos biudžeto ir turto valdyme, nes naujiems saugumo mechanizmams įgyvendinti reikalinga išsami jų rizikos sumažinimo analizė, atsipirkimo laikas ir grąža. Tapatybės ir prieigos vertinimas įmonėje A atspindi Kibernetinio saugumo ir verslo vadove (2020) pateikiamas rekomendacijos, kuriose įmonėms nurodoma turėti „darbuotojų, duomenų valdytojų ir kitų asmenų prieigos teisių kontrolę“, o „darbuotojams turėtų būti suteikta prieiga tik prie konkrečių sistemų ar programų, kurių jiems reikia dirbant“. Prie šių taikomų prieigos teisių ir infrastruktūros apsaugos valdymo prisideda ir organizacijos naudojama slaptažodžių atnaujinimo politika, kuri užtikrina darbuotojų prisijungimus prie įmonės programų su autentifikavimo kodu, kuris gaunamas į kiekvieno darbuotojo telefoną. Belaidžio tinklo saugumą užtikrina informacinių technologijų specialistai, kurie rūpinasi maršrutizatorių saugumo administravimu, taip pat organizacija svečių prisijungimui prie interneto turi atskirą tinklą, kuris yra visiškai atskirtas nuo darbuotojų naudojamų prietaisų prieigų. Tai stipriai

sumažina kenkėjiškos veiklos, susijusios su infrastruktūra ir tinklu, riziką, todėl šių kriterijų vertinimui skirti didžiausi įverčiai.

Trečiųjų šalių valdymo vertinimas parodė, kad organizacija A šioje srityje yra sukaupusi didelę patirtį, nes vadovaujasi pačių sukurta „partnerių patikimumo tvarka“, o papildomą apsaugą nuo nepatikimų klientų ar tiekėjų įmonei suteikia pasirašomos sutartys ir išorės vertinimas, kurį atlieka finansinės įstaigos. Organizacijoje tinkamai vykdoma duomenų apsaugos strategija – įdarbintas specialistas, atsakingas už Bendrojo duomenų apsaugos reglamento (BDAR) keliamus reikalavimus. Šių duomenų apdorojimą, atsarginių kopijų saugojimą ir prieinamumą serveriuose, taip pat šių duomenų analizės metu identifikuojamos duomenų apsaugos rizikos ir pagal jas išleidžiamos tvarkos, kuriomis vadovaujasi visos organizacijos darbuotojai. Papildomų priemonių įmonė A duomenų praradimo prevencijai neatlieka, todėl su turimais negali visapusiškai užtikrinti duomenų apsaugos funkcijos. Programinės įrangos apsaugos vertinimo kriterijus įmonėje įvertintas vidutiniškai, nes įranga yra atnaujinama vadovaujantis tik gamintojo siūlomomis rekomendacijomis. Mokslinės literatūros dalyje minėtos programinės įrangos silpnosios vietos – kūrimo metu paliktos gamintojų saugumo skylės ar klaidos – dažnai įvardijamos kaip paprasčiausias būdas įsilaužėliams prieiti prie įmonės informacijos ir ją valdyti. Tai, kad organizacija A programinės įrangos saugumo užtikrinimą grindžia gamintojų keliamų reikalavimų pasitikėjimu, neužtikrina, jog yra laiku vykdomi programinės įrangos atnaujinimo procesai arba, jog atlikti atnaujinimai neturės neigiamos įtakos kitiems organizacijos veiklos procesams. Ši sritis turėtų būti tobulinama, nes visiškam programinės įrangos saugumo užtikrinimui reikalinga ne tik įrangos gamintojų atsakomybė, tačiau ir pačios organizacijos vertinimo ir kontrolės mechanizmai šioje srityje.

Vertinama organizacija į debesijos kompiuterines sistemas yra perkėlusi didžiąją dalį savo verslo veiklos informacijos, kurią apdoroja tiesiogiai debesijos paslaugų platformose. Įmonės atstovai patvirtina, kad šios platformos yra patogi dalijimosi failais sistema, kuri ne tik sumažina informacijos apdorojimo sąnaudas, bet ir užtikrina spartesnį visos organizacijos darbą. Kibernetinio saugumo ir verslo vadove (2020) yra atkreipiamas svarbus dėmesys į atsakomybės pasiskirstymą tarp debesijos paslaugų tiekėjo ir jų paslaugas užsakančios organizacijos. Tinkamam verslo informacijos saugumui debesijos platformose užtikrinti reikalingi informacinių technologijų saugos specialistų kompetencijas turintys darbuotojai, kurių vertinamoje A organizacijoje yra, tačiau tai nėra jų atsakomybių sritis, numatyta valdymo struktūroje. Iš to galima daryti išvadą, kad įmonė rinkdamasi debesijos paslaugų teikėją visą atsakomybės riziką, susijusią su šių paslaugų teikimu yra palikusi paslaugų teikėjui. Kadangi atsakomybės ir sąlygos, dėl kurių abi šalys yra susitarusios nebuvo vertinamos, bendras debesijos saugumo lygis vertinamas žemu ir reikalauja papildomų priemonių.

Įvertinus tai, kad žmogiškasis faktorius yra viena jautriausių ir pažeidžiamiausių kibernetinių grėsmių visoms organizacijoms, o vertinama įmonė skiria dideles investicijas reguliariems visų darbuotojų mokymams kibernetinio saugumo rizikos temomis (kibernetinės higienos, atsakomybės, darbo funkcijų saugumo užtikrinimo), šis tikrinamas kriterijus įvertintas aukščiausiu įverčiu. Mokymų metu darbuotojai išmoksta atpažinti apgaulingą informaciją, susipažįsta su metodais, kuriuos taiko įsilaužėliai, išgirsta naujausią informaciją apie saugumo priemones ir principus. Žvelgiant į darbuotojų kompetencijų vertinimo rezultatus, nors įmonė į darbuotojų mokymus deda dideles pastangas, darbuotojų kompetencijų pakanka tik atlikti savo darbo funkcijas, susijusias su kibernetinio saugumo rizika. Darbuotojų gebėjimai ir turima patirtis negali prisidėti prie kibernetinio saugumo rizikos mažinimo procesų.

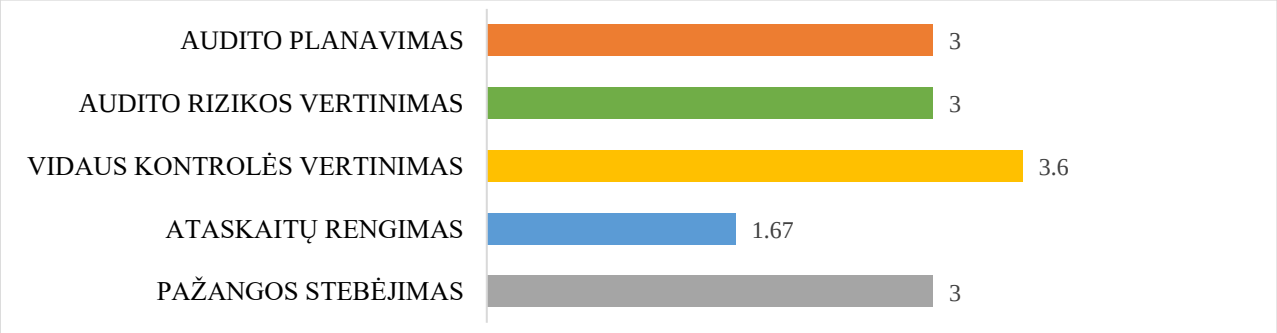
Toliau pateikiami vidaus audito procedūrų užtikrinimo vertinimo rezultatai A įmonėje.

8 lentelė. Vidaus audito procedūrų vertinimo A įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	**Citata, pagrindžianti arba paneigianti kriterijaus svarbumą**	**Įvertis, pagal sudarytus įverčio rangus**
Ilgalaikis planas	„**Taip**, organizacija turi ilgalaikį audito planavimą. Jo metu sudaromas ilgalaikės audito veiklos biudžetas ir atitinkamai paskirstomas pagal poreikį visoms sritims“	5
Apimtis	„Manau, **ne**, audito apimties tai neįtakoja, nėra kažkokių minimalių ar maksimalių ribų, daroma kiek yra suplanuota [...] gal tai aktualiau išorės auditui, ten apimties klausimas gali būti svarbus pasirenkant auditorių“	2
Plano sudarymas	„Iš dalies **taip**, orientuojamasi į prioritetus ir pagrindines rizikas. [...], bet didžiausias dėmesys skiriamas procesų įvertinimui, taip pat darbų paskirstymui.“	3
Vadovų įsitraukimas	„**Ne**, patvirtinimas planui nereikalingas, planas yra skirtas mums, atliekantiems audito procedūras [...] supažindinama kartais, bet daugiau tai dėl reikalingų išteklių ar didesnio numatomo biudžeto, kuriam patvirtinimo vadovų jau reikia“	2
Žmogiškieji ištekliai	„Šiuo metu reikalingų **specialistų trūksta**, todėl yra įdarbinami specialistai iš išorės dalykinėms kompetencijoms vertinti. [...] įmonėje dirba vidaus audito vadovė, turinti jau beveik 20 metų darbo patirtį ir jai padeda po praktikos likusi trečius metus dirbanti auditoriaus asistentė, kuri šiemet siekia tapti auditore“	1
Resursų valdymas	„Manau, kad resursai valdomi **tinkamai**. Įmonėje turime atskirą, tik už rizikų valdymą atsakingą skyrių ir jo vadovę, kuri vertina ir su resursais susijusias rizikas, tai ji pateikia reikalingas išvadas vidaus audito skyriui.“	5
Kontrolės aplinka	„Tikrai **yra išlaikomas tinkamas** verslo etikos lygis. Manau, kad darbinė aplinka yra gera - užtikrinamas saugumas, geros darbo sąlygos, nediskriminuojama“	4
Informavimas ir komunikavimas	„**Negaliu atsakyti**, tikriausiai tai, kas būtina yra pranešama, o išsami viso to analizė nėra atliekama. Neteko susidurti, kad kažkokios informacijos, susijusios su vidaus auditu iš praeities neturėtume.”	2
Rizikos įvertinimas	„**Yra** nustatomos tiek vidinės, tiek išorinės grėsmės. [...] pati kibernetinė grėsmė vertinama kaip labai rimta ir siekiama apsaugoti nuo įvairių, su ja susijusių trikdžių“	4
Kontrolės priemonės	„Atrodo, kad priemonės **pakankamos** [...] tikriausiai visų išvardintų kontrolių rūšių nevertiname, [...] dėl veiksmų ir rezultatų kontrolės galėčiau pasakyti, kad jos tikrai yra vertinamos“	3
Stebėsena	„**Taip**, stebima, ar sukurti veiksmų planai ir tvarkos pasitvirtino, ar dirbama pagal patvirtintas tvarkas, [...] ar pritaikius patvirtintas tvarkas buvo išvengta rizikingų situacijų, taip pat periodinis įmonės darbo kokybės vertinimas”	5
Rezultatų aptarimas	„**Ne**, su pirmine ataskaita vadovybės supažindinti neprivaloma, ji, su savo išvadomis, pateikiama tik per visuotinį akcininkų susirinkimą. [...] kartais, galbūt kassavaitinio susirinkimo metu gali būti pristatomi tam tikri rezultatai, bet tai neturi įtakos galutinėms išvadoms.”	2
Atitikties testavimas	„Organizacijoje tai **nėra atliekama**”	1

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Galutinė ataskaita	„**Ne**, skirtingoms organizacijos veiklos sritims audito nuomonė nedetalizuojama, išvadose gali būti išskirta nebent sritis, pvz. finansai, su jai skirtais komentarais, tačiau tai nėra atskira nuomonė ar išvada, greičiau pastabos ”	2
Rekomendacijos	„**Ne**, atskirų rekomendacijų, nukreiptų į kibernetinės grėsmės suvaldymą nėra pateikiamos [..] kartais, bet tikrai ne visada pateikiamos bendro pobūdžio rekomendacijos visai audituotai veiklai, bet tai dažniausiai susiję su galutinėmis išvadomis“	3

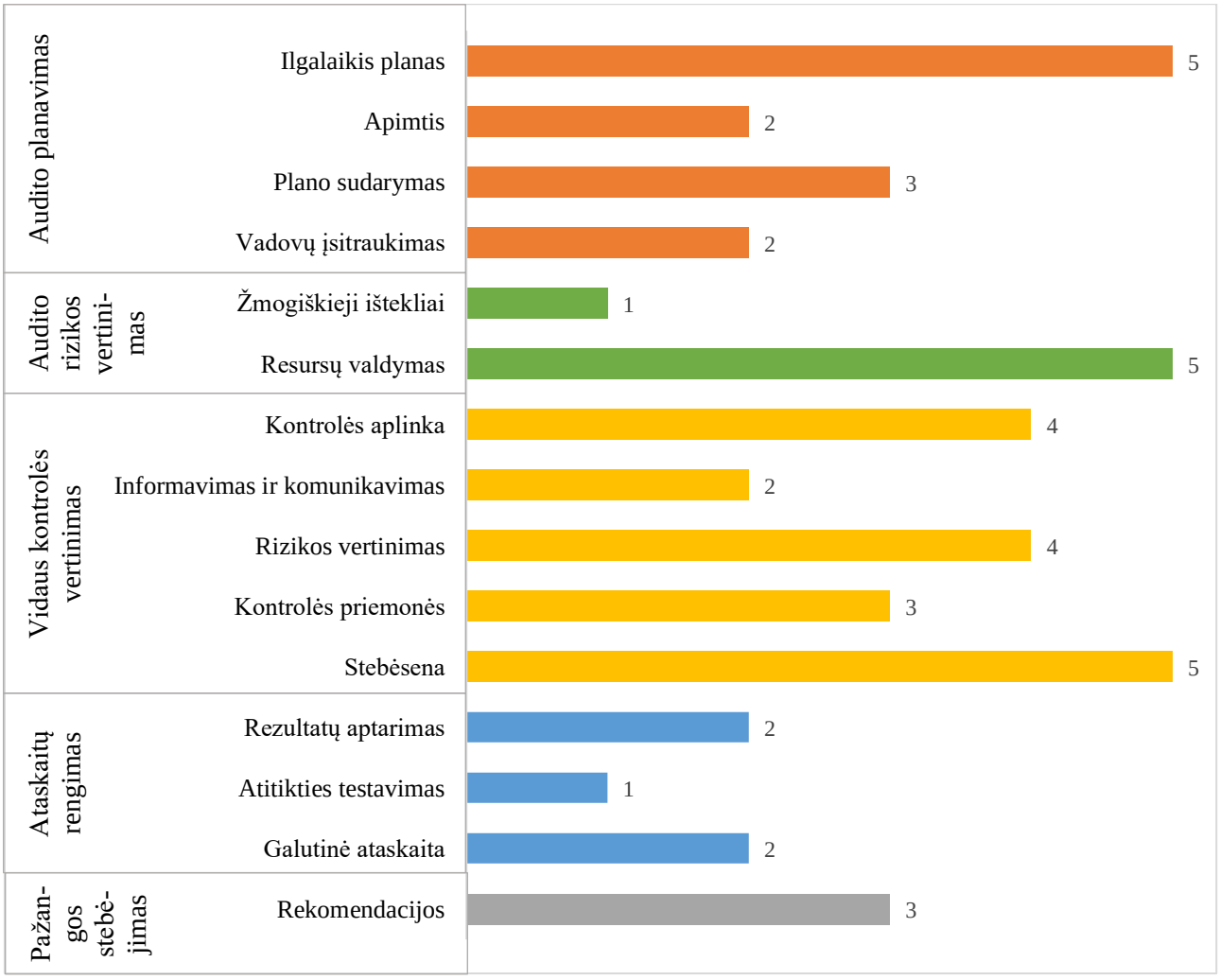
Vidaus audito procedūrų vertinimo įverčių suma A įmonėje lygi 44 balams iš 75 galimų, o tai lemia, kad įmonė atitinka **vidutinį** vidaus audito procedūrų užtikrinimo lygį, o kibernetinės atakos nepastebėjimo tikimybė yra **mažai tikėtina**. Aritmetinių vidurkių pagalba nustatyta, kad organizacija atlikdama vidaus auditą labiausiai užtikrina vidaus kontrolės vertinimo kategorijos kriterijus, o ataskaitų rengimo procedūrai skiria mažiausią dėmesį. Kitos procedūros – audito planavimas, audito rizikos vertinimas ir pažangos stebėjimas – užtikrinami vidutiniškai, todėl apibendrinus visus rezultatus galima teigti, kad įmonės A vidaus audito procedūros privalo būti peržiūrimos ir tobulinamos, plečiamos audito sritys, jog gauti rezultatai ne tik įvertintų buvusius organizacijos procesus, tačiau taptų įrankiu, galinčiu pasitarnauti organizacijos veiklos tęstinumui ir tobulinimo užtikrinimui.



9 pav. Vidaus audito procedūrų vertinimas A įmonėje (sudaryta autorės)

Vertinant atskirų vidaus audito procedūrų užtikrinimo kategorijų vertinimo rezultatus (10 pav.), kurie grindžiami pagal interviu surinktus atsakymus (8 lentelė) galima teigti, kad organizacija labai chaotiškai užtikrina vidaus audito procedūrų vertinimą: vienoms skiria labai didelį dėmesį, kitoms - jokio. Vidaus audito planavimo kategorijos vertinimai parodo, kad organizacija supranta ilgalaikio audito plano vykdymo svarbą, todėl siekia jo metu paskirstyti biudžeto išteklius, įvertinti ilgalaikius tikslus. Tačiau vidaus audito apimčių reguliavimui neskiriamas tinkamas dėmesys gali turėti įtakos audito prioritetų ir pagrindinių rizikų nepakankamam įvertinimui. Su tuo stipriai susijęs ir kitas tik vidutiniškai įvertintas veiksnys – plano sudarymas, kurio metu, organizacija tik iš dalies įvertindama pagrindines organizacijos rizikas gali netinkamai nustatyti bendrą vidaus audito riziką, nuo kurios priklauso planuojamos atlikti audito procedūros ir jų apimtys. Vadovų įsitraukimas į planavimo procesus įvertintas kaip minimalus, todėl įmonės vadovai, nereikalaudami vidaus audito plano patvirtinimo ir tik fragmentiškai su juo susipažindami, rizikuoja nepakankamai užtikrinti kontrolės procedūras.

Kaip teorinėje dalyje išnagrinėta, vidaus audito rizikų gali būti įvairių – pradedant įgimta rizika finansinėse ataskaitose, baigiant specifinėmis organizacijos veiklos rizikomis. Tinkamai įvertinęs šias rizikas planavimo etape – nustatęs reikalingą specialistų kiekį, procedūrų išsamumą ir apimtis, taikomus metodus ir įrankius, numatęs atlikimo laiką – auditorius gali iki minimumo sumažinti jų daromą poveikį. Šios kategorijos organizacijos A vertinimas parodė, kad įmonė negali visiškai užtikrinti audito rizikos įvertinimo, nes neturi pakankamai specialistų vidaus audito procedūroms užtikrinti ir keletą jų įdarbina iš išorės. Resursų valdymo kriterijui skiriamas aukščiausias įvertinimas, nes organizacija turi atskirą resursų valdymo skyrių su atsakingais darbuotojais, kurie sudarinėja darbo grupes, paskirsto darbo valandas, užsakinėja paslaugas iš išorės. Su resursų valdymo rizika siejami dalykai taip pat įvertinami ir pateikiami audito skyriui.



10 pav. Vidaus audito procedūrų kriterijų vertinimas A įmonėje (sudaryta autorės)

Vidaus kontrolės kategorijos vertinimui skiriamas didžiausias organizacijos A dėmesys, nors kriterijai vertinami nevienodai. Kontrolės aplinkos vertinimas, kuris laikomas vidaus kontrolės sistemos pagrindu, parodė, kad įmonėje A išlaikomas aukštas verslo etikos lygis, vadovų pavyzdžiu yra formuojama darbinė aplinka. Efektyvios kontrolės aplinkos turėjimas leidžia įmonei turėti tinkamą pagrindą, organizacijos rizikoms įvertinti (Paukštienė, 2012). Visgi, ankstesnių atliktų auditų įžvalgos ir naudingoji vidaus kontrolės valdymo patirtis nėra vertinami organizacijos ateities vidaus audito sprendimams įgyvendinti. Pagrindinėms rizikoms įvertinti ir strateginiams tikslams įgyvendinti organizacija prioritetą teikia vidinių ir išorinių grėsmių nustatymui, o tai ypač svarbu

tampa nustatant ir kibernetinę saugumo grėsmę. Kontrolės priemonių vertinimas parodė, kad įmonės A atliekamos veiksmų ir rezultatų kontrolės yra nepakankamos užtikrinti pagrindinių vidaus audito įrodymų savybių – pakankamumo ir patikimumo – atitiktį. Vidaus kontrolės stebėsena analizuojamoje A organizacijoje siekia įvertinti vidaus kontrolės procesų veiksmingumą, todėl tai svarbu gautų audito rezultatų patvirtinimui ir bendro vidaus audito darbo kokybės vertinimui.

Ataskaitų rengimo procesas vertinamoje A įmonėje turi būti iš esmės peržiūrimas ir tobulinamas. Gautų tarpinių vidaus audito rezultatų neaptarimas su įmonės vadovybe ir atskiroms audituotoms sritims nedetalizuojamos išvados gali būti rimta priežastis vidaus audito nepatikimumo pareiškimui, o tai taip pat siejama su jau anksčiau minėtu per mažu vadovų įsitraukimu į tinkamą vidaus audito kokybės valdymą. Atitikties testavimo neatlikimo atvejai gali būti reikšmingi teisingos galutinės vidaus audito nuomonės ir galutinių išvadų bei rekomendacijų suformulavimui, nes be jų negalima patvirtinti, ar buvo gauti tinkami vidaus audito įrodymai, ar buvo atliekami iškraipymų taisymai audito metu, ar jie yra reikšmingi. Be atitikties testavimo organizacijoje negali būti nustatyti bendri atliekamų įmonės veiklos procedūrų ir su jomis susijusių rizikos pasekmių bendri veikimo ir priežastiniai ryšiai, o tai neleidžia vidaus audito naudoti kaip įrankio visapusiškam rizikų įvertinimui. Stebėjimo pažangos vertinimas analizuojamoje įmonėje yra fragmentiškas, rekomendacijų ar procedūrų tobulinimo vertinimas atliekamas tam tikrais atvejais.

Aptarus visus A įmonės kibernetinio saugumo rizikos ir vidaus audito procedūrų vertinimo rezultatus (7 ir 8 lentelė) toliau pateikiamos rekomendacijos, kurios galėtų padėti organizacijai tobulinti kibernetinio saugumo rizikos vertinimo procesus vidaus audito procedūrose. Rekomendacijos pateikiamos 9 lentelėje.

9 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos A įmonėje (sudaryta autorės)

Siūloma tobulinimo priemonė/ sritis	**Rekomendacijos paaiškinimas**
Įtraukti atitikties testavimą į prioritetinių vidaus audito procedūrų sąrašą	Organizacijos A vidaus audito ataskaitų rengimo procesų vertinimas atskleidė, kad įmonė neatlikdama atitikties testavimo rizikuoja pateikti neteisingas vidaus audito išvadas. Atitikties testavimo procedūros leistų nustatyti asociaciją tarp bendrų organizacijai kylančių rizikų ir veikloje atliekamų veiksmų bei sprendimų. Priežastinių ryšių nustatymas padėtų vidaus auditui tapti įrankiu, galinčiu įvertinti kibernetinio saugumo riziką vidaus audito procedūrose.
Įdarbinti patyrusius kibernetinio saugumo ir vidaus audito specialistus	Organizacijos A žmogiškųjų išteklių vertinimas tiek kibernetinio saugumo rizikos, tiek vidaus audito procedūrose parodė, kad organizacija skiria per mažai dėmesio kompetencijų ir reikalingo specialistų kiekio užtikrinimui. Visiems darbuotojams vykdomi kibernetinio saugumo rizikos mokymai lemia bazines organizacijos darbuotojų žinias, tačiau reikalingi specializuoti, specifinius įgūdžius formuojantys nuolatiniai mokymai, kurie galėtų garantuoti kibernetinio saugumo užtikrinimo procesų tobulinimą visoje organizacijoje. Vidaus audito procedūrų užtikrinime darbuotojų trūkumas lemia papildomų išteklių poreikį, kuris susijęs su papildomomis vidaus auditui skiriamomis sąnaudomis. Be to, specialistų turėjimas įmonės viduje užtikrintų nuolatinį procesų stebėjimą ir kontrolę, leistų savo įžvalgomis tobulinti vidaus audito atlikimą.
Praeities vidaus audito kontrolės sprendimų informaciją panaudoti ateities sprendimams	Organizacijos A vidaus audito procedūrų užtikrinimo vertinimas parodė, kad įmonė neatlieka praeities auditų analitikos. Praėjusių vidaus audito procedūrų analizė galėtų padėti užtikrinti kokybiškesnius būsimų vidaus audito valdymo ir atlikimo sprendimus, turėtų teigiamos įtakos kokybiškesniam vidaus kontrolės vertinimui.

Siūloma tobulinimo priemonė/ sritis	Rekomendacijos paaiškinimas
Diegti įrankius, gebančius analizuoti turimus duomenis	Organizacijos A kibernetinio saugumo rizikos nustatymo vertinimas parodė, kad įmonė turi tinkamą infrastruktūrą bei reikiamas priemones kibernetinio saugumo rizikos duomenų rinkimui, todėl siekiant juos naudoti priežastinių ryšių ir prognozinių modelių kūrimui reikalingi įrankiai ar sistemos, galinčios šiuos duomenis apdoroti. Tikimasi, kad tai galėtų prisidėti prie įmonės kibernetinio atsparumo ir poveikio analizės nustatymo gerinimo.
Didinti vadovybės įsitraukimą į vidaus audito valdymo sprendimus	Organizacijos A vidaus audito valdymo vertinimas atskleidė, kad fragmentiškas vadovų įsitraukimas vertinant vidaus audito veiklą negali visiškai užtikrinti vidaus audito tikslų ir su jais susijusių verslo tęstinumo sprendimų. Teigiamas vadovų požiūris į vidaus auditą leistų efektyvinti procesus ir vertinti jį kaip verslo pridėtinės vertės kūrimo įrankį. Prie šio gerinimo aktyviau galėtų prisidėti ir įmonėje esantis vidaus audito padalinys, kuris vadovams gali suteikti daugiau žinių ir analitikos apie sritis, kuriose vidaus auditas gali būti panaudojamas organizacijoje ir kokius procesus galėtų įvertindamas pagerinti.

4.2. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai B įmonėje

B įmonė yra telekomunikacijų, informacinių technologijų ir televizijos paslaugas teikianti įmonė, veikianti Šiaurės ir Baltijos šalyse. Įmonės teikiamos paslaugos yra labai susiję su kibernetinių atakų taikinių priemonėmis, tokiomis kaip – tinklai, išmanieji įrenginiai, duomenų centrai, daiktų internetas, todėl įmonė jau kelerius metu teikia ir informacinių technologijų saugos paslaugas. Svarbu paminėti, kad organizacija yra su atliekamu tyrimu susijusių Lietuvoje veikiančių – vidaus auditorių ir Infobalt (informacijos ir ryšių technologijų sektoriaus) – asociacijų nariai, o tai reiškia, kad įmonė viena pirmųjų gauna vidaus audito atlikimo rekomendacijas ir naujienas bei gali turėti tinkamas sąlygas informacijos ir ryšių technologijų rinkos plėtrai. Toliau yra pateikiami B įmonės kibernetinio saugumo rizikos vertinimo rezultatai (10 lentelė).

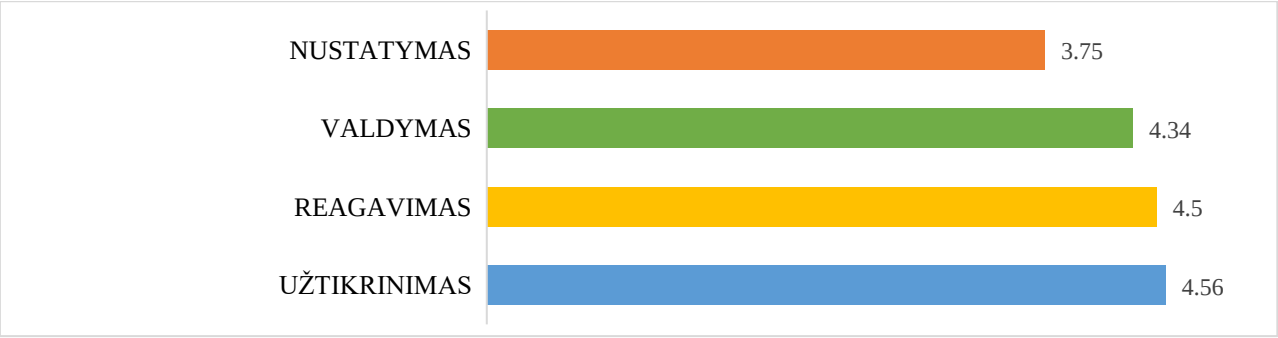
10 lentelė. Kibernetinio saugumo rizikos vertinimo B įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Grėsmių identifikavimas	„**Taip,** išteklių skiriama pakankamai, aišku, jie visada vertinami ir siekiama, kad iš jų būtų gauta maksimali nauda, kad jie atsipirktų [...] rizikos valdymo proceso metu yra nustatomos galimos grėsmės ir sudaromi planai joms valdyti [...] kiek esame turėję patvirtintų grėsmių tiksliai neįvardinsiu, bet pagal veiklos pobūdį tikriausiai galite įsivaizduoti, jog įmonė nuolat yra atakuojama ir ieškoma jos silpnųjų vietų“	4
Infrastruktūros vertinimas	„Infrastruktūros vertinimas **atliekamas** kartu su kitų informacinių sistemų kontrolės vertinimu, kuris yra vidinės kontrolės vertinimo dalis [...] šioje vietoje pagrindiniai organizacijos duomenys nėra vertinami, šis vertinimas apima IT turto ir kritinės infrastruktūros įvertinimą“	2
Poveikio analizė	„Tokia analizė **privaloma** atlikti nuolat, įmonė niekada negali manyti, kad yra pilnai apsisaugojusi, naujos grėsmės formos gimsta greičiau nei mes spėjame jas analizuoti “	5
Saugumo informacijos stebėsena	„**Taip,** stebėseną padeda įgyvendinti Infobalt asociacija, kurios nariais esame [...] o didžiausią dėmesį skiriame galimo atsparumo taktikoms analizuoti, atsako veiksmų efektyvumui gerinti, įsiskverbimo bandymams atlikti “	4

Tikrinamas kriterijus	**Citata, pagrindžianti arba paneigianti kriterijaus svarbumą**	**Įvertis, pagal sudarytus įverčio rangus**
Valdymo modelis ir struktūra	„**Taip**, valdymo struktūra aiški [...] valdymo analizei skiriamas pakankamas dėmesys, už kibernetinį saugumą atsakingas technologijų infrastruktūros padalinys ir jo vadovas“	5
Vadovų požiūris	„**Taip**, vadovybė tikrai priima valdymo sprendimus, atsižvelgiant į kibernetinio saugumo riziką, domisi šios rizikos suvaldymu [...] vertinama kaip viena didžiausių visoje organizacijoje“	3
Reguliavimo ir teisinė aplinka	„**Taip**, bendrovė turi Rizikos valdymo politiką, joje yra vertinamos visos įmonei reikšmingos grėsmės. [...] rizikos valdymas vykdomas pagal COSO reikalavimus ir tarptautinius standartus – ISO20000, ISO31000, ISO270001“	5
Kibernetinės rizikos analitika	„Analitika **vykdoma** ir yra pilnai integruota į įmonės verslo veiklos kontrolės procesus [...] kaip minėjau anksčiau klausime apie stebėseną, skiriame dėmesį atsparumo taktikoms analizuoti, atsako veiksmų efektyvumui gerinimui”	5
Prognozės ir elgsena	„Rizikos valdymo procese tai **yra atliekama** – nustatomos grėsmės, numatoma elgsena, sudaromi atsako planai [...] tikslinės grupės vertinamos“	5
Priežastiniai ryšiai	„Priežastinių ryšių analizė **nėra atliekama**, tačiau galima sakyti, kad priežastiniai ryšiai atrandami vertinant valdymo sritis, kurios atspindi vidinę (tokia kaip procesų valdymas, IT valdymas, informacijos ir išteklių valdymas) ir išorinę (pvz. konkurencinė ar vartotojų) įmonės aplinką“	3
Atsako planavimas	„**Tikrai taip**, įmonė prieš tris metus kartu su kibernetinės gynybos partneriais sukūrė kibernetinių pratybų centrą, kurių metu yra sukuriamos dirbtinės atakos pagal sektoriaus veiklos rizikas [..] pratybos būna naudingos tiek informacinių technologijų saugumo specialistams, tiek vadovams, tiek kitas funkcijas įmonėje atliekantiems darbuotojams”	5
Saugumo programų valdymas	„**Taip,** pagal minėtus anksčiau standartus sudarytos bendrovės kibernetinio saugumo strategijos, taip pat jau kelis metus atitinkame tarptautinį TIERIII saugumo standartą [..] biudžeto vertinime dalyvauja visi nauji sprendimai, visi pokyčiai susiję su jais taip pat vertinami valdybos taryboje ”	5
Duomenų apsauga	„Duomenų apsaugos politika visos įmonės mastu taip pat **yra**. Ji svarbi darbuotojų, klientų pasitikėjimui, taip pat susijusi su įmonės reputacijos vertinimu, nes valdant didelius kitų įmonių tinklus, svarbu užtikrinti vientisumo ir saugumo principus. [...] kaip prevencinė priemonė yra nuolat skiriami asmens duomenų apsaugos mokymai atsakingiems darbuotojams [...] kitą užtikrinimą garantuoja LR įstatymai ir ES Bendrasis asmens duomenų apsaugos reglamentas“	5
Tapatybės ir prieigos valdymas	„**Taip**, asmenų prieigos kontrolė griežtai reglamentuota bendrovės dokumentuose [...] naudojamos identifikavimo ir autentifikavimo priemonės, slaptažodžių politika”	4
Tinklo ir infrastruktūros apsauga	„Tinklo priemonių apsaugą siūlome net ir savo klientams, tai turėdami tiek patirties jau **išmokome tinkamai** juo rūpintis [...] tinkamai apsaugojus visą tinklą, pageriname ir infrastruktūros apsaugą, žinoma, tik tuo pasitikėti negalima“	5

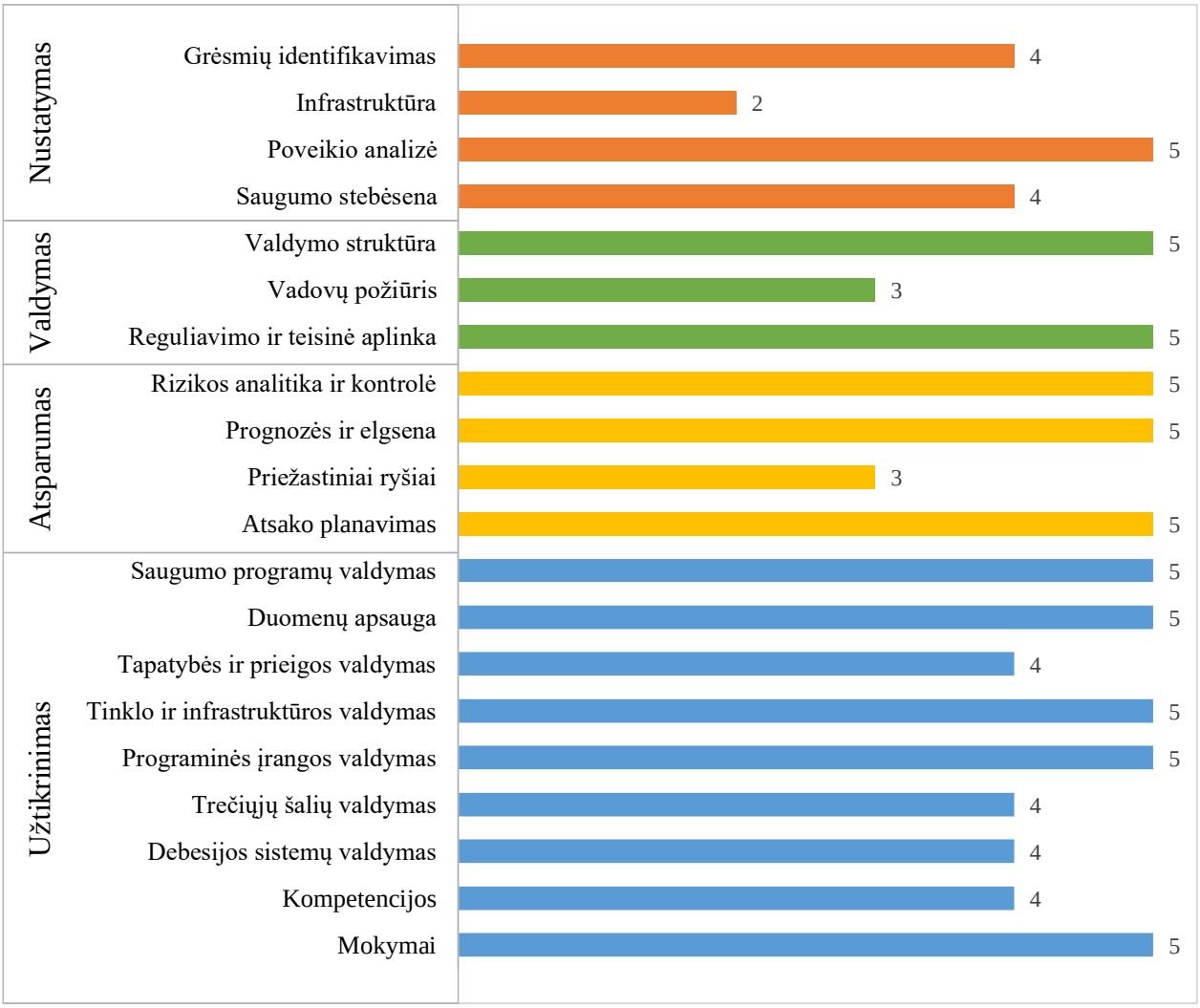
Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Programinės įrangos apsauga	„Kadangi patys siūlome tokią paslaugą kitoms įmonėms, tai tinkamą jų apsaugos valdymą **garantuojame** ne tik savo ūkio priežiūrai, bet ir kitiems [...] savo įmonėje nuolat atliekame automatinius programinės įrangos atnaujinimus, stebime įsigytų programinių įrangų gamintojų nurodymus, savo kurtas įrangas nuolat testuojame“	5
Trečiųjų šalių valdymas	„**Taip,** atranka atliekama, sutartys yra pasirašomos tiek su klientais, tiek su tiekėjais [...] rizika gal yra labiau susijusi su tais klientais, su kuriais turime paskolų sandorius, tai dalį šios rizikos prisiima bankas, taikydamas faktoringinį finansavimą “	4
Debesijos sistemų valdymas	„Su šia apsauga dirbame pakankamai neseniai, tačiau jau galime pasiūlyti virtualių serverių paslaugą kitiems, taip pat **ją taikome** ir savo įmonėje. Apsauga standartinė tokiai infrastruktūrai – slaptažodžiai, saugumo raktai, šifruotės, klientų serverius saugome prieigos kontrolės valdymu, gesinimo-užliejimo sistema, vaizdo stebėjimu “	4
Darbuotojų kompetencijos	„Darbuotojų kompetencijos **pakankamos** ir nuolat tobulinamos [...] bendrovė investuoja į mokymų programas, kurios rengia kibernetinio saugumo ir IT specialistus, geriausiems skiria stažuotes bendrovėje, kurios leidžia sukaupus patirtį tapti įmonės darbuotoju ”	4
Mokymai	„**Taip**, kaip jau ir minėjau anksčiau – tai yra mūsų įmonės prioritetas, kuo daugiau dirbančių žmonių būtų apmokyti atpažinti signalus, kurie bet kada gali virsti ataka [..] kuo daugiau darbuotojai supras apie kibernetinės atakos poveikį visai organizacijai, tuo geriau galėsime užtikrinti rizikos suvaldymą”	5

Kibernetinio saugumo rizikos kategorijų vertinime B įmonėje gauti 87 balai iš 100 galimų. Pagal sudarytą konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose modelį toks vertinimas atitinka **aukščiausią** kibernetinio saugumo rizikos vertinimo lygį ir lemia **nežymų** rizikos poveikį įmonės veiklos procesams. Pagal kibernetinio saugumo rizikos vertinimo kriterijų aritmetinius vidurkius (11 pav.) galima teigti, kad organizacija skiria didelį dėmesį valdymo, reagavimo ir užtikrinimo kategorijoms, kurios ir lemia aukščiausią saugumo rizikos vertinimą. Kiek žemesnį nustatymo kategorijų vertinimą lėmė organizacijos turimos infrastruktūros vertinimas. Jis atliekamas tik kaip vidinės kontrolės vertinimo dalis, apimanti informacinių technologijų turtą ir kritinės infrastruktūros nustatymą, tačiau nėra įtraukiamas pagrindinių organizacijos duomenų vertinimas. Nagrinėtos literatūros dalyje buvo teigiama, kad pagrindiniai organizacijos duomenys yra viena pagrindinių tinkamos infrastruktūros pagrindo dalis, kuri leidžia tinkamai nustatyti kylančias grėsmes.



11 pav. Kibernetinio saugumo rizikos kategorijų vertinimas B įmonėje (sudaryta autorės)

Pagal kibernetinio saugumo rizikos vertinimo atskirų kriterijų vertinimą (12 pav.) grėsmių identifikavimui skiriami dideli išteklių kiekiai yra pakankami, tačiau tai, kad įmonė kiekvienu sunaudotu ištekliu matuoja grėsmės suvaldymo naudą nėra teisingas požiūris. Grėsmių identifikavimui skiriami ištekliai yra tik maža dalis priemonių, reikalingų nustatyti organizacijai kylančias grėsmes, todėl ir vertinti reikėtų ne individualių, o kompleksinių priemonių taikymą. Infrastruktūros vertinimas, kaip ir buvo minėta apibendrinime, atliekamas kartu su kitų informacinių sistemų vertinimu, todėl tai neleidžia užtikrinti, kad surinktų duomenų saugumą lems konkreti infrastruktūra, o ne kartu su ja veikianti sistema. Todėl infrastruktūros vertinimas turėtų būti atskirtas, o norint turėti užtikrintą vertinimo pagrindą, turėtų būti įtraukiami ir organizacijos pagrindiniai duomenys. Kibernetinio saugumo rizikos poveikio analizė įmonėje B vertinama kaip būtina grėsmės nustatymo priemonė, kuri turi būti nuolatos atliekama, siekiant užtikrinti operatyvią reakciją į kylantį pavojų. Saugumo informacijos stebėseną analizuojamoje organizacijoje užtikrina atsparumo taktikų analizė, atsparumo gerinimas ir atliekami įsiskverbimo bandymai. Aktyvus dalyvavimas Informacijos ir ryšių technologijų sektoriaus (Infobalt) asociacijos veikloje taip pat prisideda prie saugumo informacijos stebėsenos.



12 pav. Kibernetinio saugumo rizikos kriterijų vertinimas B įmonėje (sudaryta autorės)

Vertinant valdymo kategorijos kriterijus – valdymo struktūrą bei reguliavimo ir teisinę politiką – organizacija buvo įvertinta aukščiausiais balais. Tai patvirtina įmonės B turima rizikos valdymo politika, kurioje rizikos valdymo etapai parengti pagal Tarptautinius standartus: ISO 20000

(informacinių technologijų paslaugų valdymo standartas), ISO 31000 *(verslo rizikos valdymo sistemos standartas)*, ISO 270001 *(informacijos saugumo vadybos sistemos standartas)* ir pagal COSO *(angl. The Committee of Sponsoring Organizations of the Treadway Commission)* įmonių rizikos valdymo metodiką. Šių standartų laikymasis užtikrina verslo valdymo funkcijų suderinamumą su informacinių technologijų priemonėmis, mažinant organizacijos kibernetinio saugumo riziką ir gerinant rinkoje veikiančių įmonių bendradarbiavimą. Vadovų požiūrio vertinimas parodė, kad organizacijos vadovai kibernetinio saugumo riziką vertina kaip vieną pavojingiausių įmonės veiklos tikslų įgyvendinimui ir skatina iniciatyvas, susijusias su šios rizikos suvaldymu, tačiau pačių vadovų įsitraukimas ir žinios neužtikrina vadovų elgesiu formuojamo pavyzdžio darbuotojams.

B įmonės kibernetinio saugumo rizikos vertinimo reagavimo kategorijos kriterijai – atliekama kibernetinės saugumo rizikos analitika, surinktais duomenimis prognozuojama įsilaužėlių elgsena bei kibernetinių atakų pratybų pagrindu kuriamas atsako planavimas – pasižymėjo aukščiausiais įverčiais, užtikrinančiais sėkmingą įmonės atsparumą kibernetinei grėsmei. Aukščiausią lygį šioje vertinimo kategorijoje neleido pasiekti priežastinių ryšių tarp organizacijos atliekamų operacijų ir pasekmių, susijusių su kibernetinio saugumo rizika, nustatymas. Nors įmonės B atstovas teigė, kad priežastinių ryšių nustatymas galimas atliekant valdymo sričių vertinimą, tačiau tai jau būtų labiau vidinės ir išorinės įmonės aplinkos sąsajų, o ne veiksmų ir juos lydinčių pasekmių analizė. Dėl šios priežasties įmonei verta pasvarstyti apie priežastinių ryšių nustatymo galimybė, įvertinant tai, jog atlikdama kibernetinės saugumo rizikos analitiką ji turi sukaupusi reikalingus tam duomenis.

Nors kibernetinės saugumo rizikos užtikrinimo vertinamas yra pats svarbiausias ir apima daugiausiai kriterijų, analizuojama įmonė B šioje kategorijoje įvertinta geriausiai. Aukščiausi įverčiai buvo skirti saugumo programų, duomenų apsaugos, tinklo ir infrastruktūros, programinės įrangos apsaugos valdymo kriterijų vertinimams. Kadangi įmonė atitinka Tarptautinius informacinių technologijų paslaugų valdymo standartus, šių kriterijų vertinimas leidžia įmonei teikti su šia veikla susijusias paslaugas išorės klientams. Šiuo pagrindu yra grindžiamas tinklo ir infrastruktūros bei programinės įrangos apsaugos užtikrinimas. Įmonės B kibernetinio saugumo strategija sudaryta pagal atitiktį Tarptautiniam TIERIII saugumo standartui, o duomenų apsaugos politika – pagal Lietuvos Respublikos Įstatymus ir Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą. Šių teisinių dokumentų atitiktis organizacijos veikloje šiame tyrime nebuvo analizuojama, tačiau tai vertinama kaip papildoma kontrolės priemonė kriterijaus įverčiui nustatyti.

Slaptažodžių politikos, identifikavimo ir autentifikavimo priemonių naudojimo reikalavimai, aprašyti organizacijos vidaus politikos dokumentuose, užtikrina aukštą tapatybės ir prieigos valdymo lygį. Su trečiųjų šalių saugos vertinimu susijusią riziką organizacija B dažniausiai dalinasi su finansų įstaigomis, kurios teikia faktoringo paslaugas. Papildomą apsaugą, kuri reikalauja dažno stebėjimo, įmonei suteikia pasirašomos sutartys, kurias rengia įmonės teisininkai.

Į virtualius serverius organizacijos operacines sistemas ir verslo veiklos informaciją perkėlusi įmonė B teikia šią paslaugą ir išorės vartotojams. Be reikiamo, savo įmonės veiklai skirtų sistemų, saugumo užtikrinimo, įmonės darbuotojai rūpinasi ir klientų serverių apsauga. Kadangi ši paslaugų sritis organizacijoje dar nauja, nors ir yra užtikrinamos tinkamos debesijos kontrolės priemonės – slaptažodžiai, saugumo raktai, šifruotės ir kitos fizinės priemonės – tai neleidžia šiam kriterijui skirti aukščiausią įvertį.

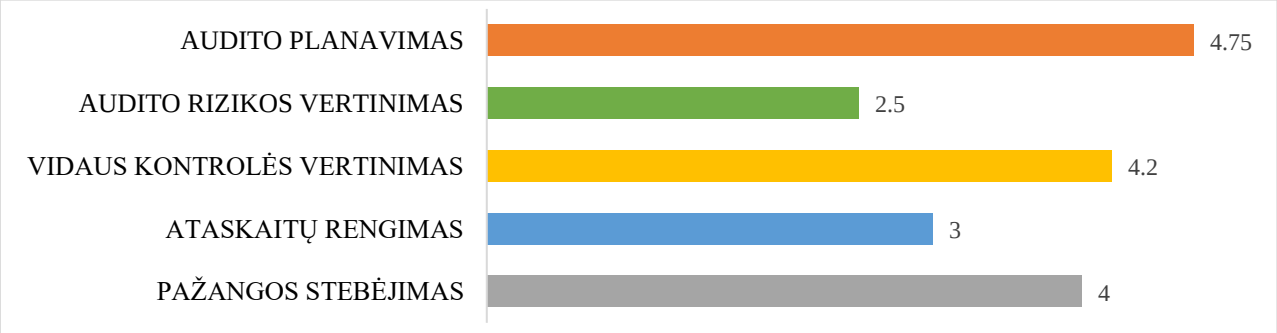
Kaip didžiausią pavojų organizacijos B veiklai respondentas įvertino techninę ar programinę įrangą naudojančius darbuotojus, todėl siekdami įvertinti kibernetinio saugumo riziką organizacija skiria dideles investicijas infrastruktūros gerinimui ir darbuotojų mokymams. Vertinant darbuotojų kompetencijas paaiškėjo, kad įmonė darbuotojų mokymų ir specialistų rengimo programomis siekia pateisinti nuolat augantį, kibernetinio saugumo rizikos ir informacinių technologijų specialistų, poreikį. Prie šio skaičiaus augimo iš esmės prisideda ne tik auganti organizacijos veikla, bet ir išorės klientams teikiamos paslaugos, kurios reikalauja tinkamo jų aptarnavimo ir užtikrinimo. Todėl galima teigti, kad nuolat vykdomų mokymų kriterijus yra išpildomas aukščiausiu įverčiu, o darbuotojų gebėjimai ir turimi įgūdžiai prisideda prie savo darbo srities procesų, susijusių su kibernetinio saugumo užtikrinimo tobulinimo organizacijoje. Toliau, 11 lentelėje, bus aptariami įmonės B vidaus audito procedūrų užtikrinimo vertinimo rezultatai.

11 lentelė. Vidaus audito procedūrų vertinimo B įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	**Citata, pagrindžianti arba paneigianti kriterijaus svarbumą**	**Įvertis, pagal sudarytus įverčio rangus**
Ilgalaikis planas	„**Taip** [...] audito veiklos biudžetas vis dar priklauso nuo bendro įmonės biudžeto, nelabai vidaus auditorius įtakoja biudžetą; planuojamas auditoriaus darbo laikas, vertinama pagal kompetencijas. Jei trūksta tam tikriems auditams kompetencijų, pvz. IT auditams, tai samdomos išorės paslaugos. Ilgalaikiai veiklos planai atnaujinami, planuojant siekiama "padengti" visas sritis/rizikas bent kartą per 3 metus. Kai kurie auditai ar bent jau jo dalys daromi kasmet.“	5
Apimtis	„**Taip**, ypač jei įmonės veikla tiesiogiai siejasi su paslaugomis elektroninėje erdvėje. [...] kadangi kibernetinė rizika yra viena pagrindinių rizikų ir vertinama periodiškai atskirai arba kaip sudėtinė dalis kitų auditų (pvz. pinigų plovimo prevencijos, mokėjimų ir t.t.)“	5
Plano sudarymas	„**Taip.** Kasmet atliekamas bendras įmonės rizikos vertinimas, kai kurios rizikos yra sisteminės ir audituojamos periodiškai dėl atitikties teisės aktams keliamų reikalavimų“	4
Vadovų įsitraukimas	„**Taip**, planas tvirtinamas valdyboje. [...] finansinėms įmonėms labai svarbi atitiktis visiems reguliaciniams reikalavimams, kad nekiltų rizika turimai licencijai, nebūtų baudų, nekiltų reputacinė rizika, todėl daug dėmesio skiriama vidaus audito ištekliams“	5
Žmogiškieji ištekliai	„**Ne**, nėra pakankamai, reikalingų išteklių šiek tiek trūksta, nes darbų, užduočių visada daugiau nei galima atlikti“	1
Resursų valdymas	„Manau, kad 80% resursų valdomi **tinkamai**. [...] darbo valandos nustatomos sudarant 3 metų ir 1 metų planą. Laikomasi profesinės priežiūros standartų. Kokybės vertinimui užsakomos paslaugos iš išorės maždaug kas 5 metai“	4
Kontrolės aplinka	„Vadovų verslo etikos lygis yra **tinkamas**. [...] darbinę aplinką vertinu gerai. Būdingas pagarbus elgesys, laikomasi įstatymų be jokių kompromisų“	3
Informavimas ir komunikavimas	„Grįžtamasis ryšys **juntamas**. [...] iš principo, vidaus auditorius turi prieigą prie visų duomenų bazių, dokumentų, gali vertinti anksčiau atliktus auditus, gauti informaciją kaip vykdomos rekomendacijos”	4
Rizikos įvertinimas	„**Yra** identifikuojamos tiek išorinės, tiek vidinės grėsmės. Mūsų organizacijai privalomas tiek vidaus, tiek išorės auditai dėl dalyvavimo vertybinių popierių biržos prekyboje. Todėl yra periodiškai sertifikuojama, tikrinama, audituojama.“	5

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Kontrolės priemonės	„Atrodo, kad priemonės tikrai **pakankamos** [...] visų išvardintų kontrolės rūšių vertinimas atliekamas, dar periodiškai atliekamas vidaus ir išorės veiklos auditai, saugumo sertifikavimas“	5
Stebėsena	„**Taip**, yra patvirtintos kontrolės procedūros, funkcijų atskyrimas”	4
Rezultatų aptarimas	„**Iš dalies,** tam rezultatai yra pristatomi, tačiau įtakos jiems vadovai neturi“	3
Atitikties testavimas	„**Yra** atliekama [...], periodiškai atliekamas testavimas ir jo metu atrandami bendrai veikiantys rodikliai”	4
Galutinė ataskaita	„ [...] labiau **ne**, nei taip, nors iš esmės tai priklauso nuo audito objekto, tikslų, uždavinių, pradinio plano, audituojamos srities ”	2
Rekomendacijos	„**Taip**, rekomendacijos yra pateikiamos“	4

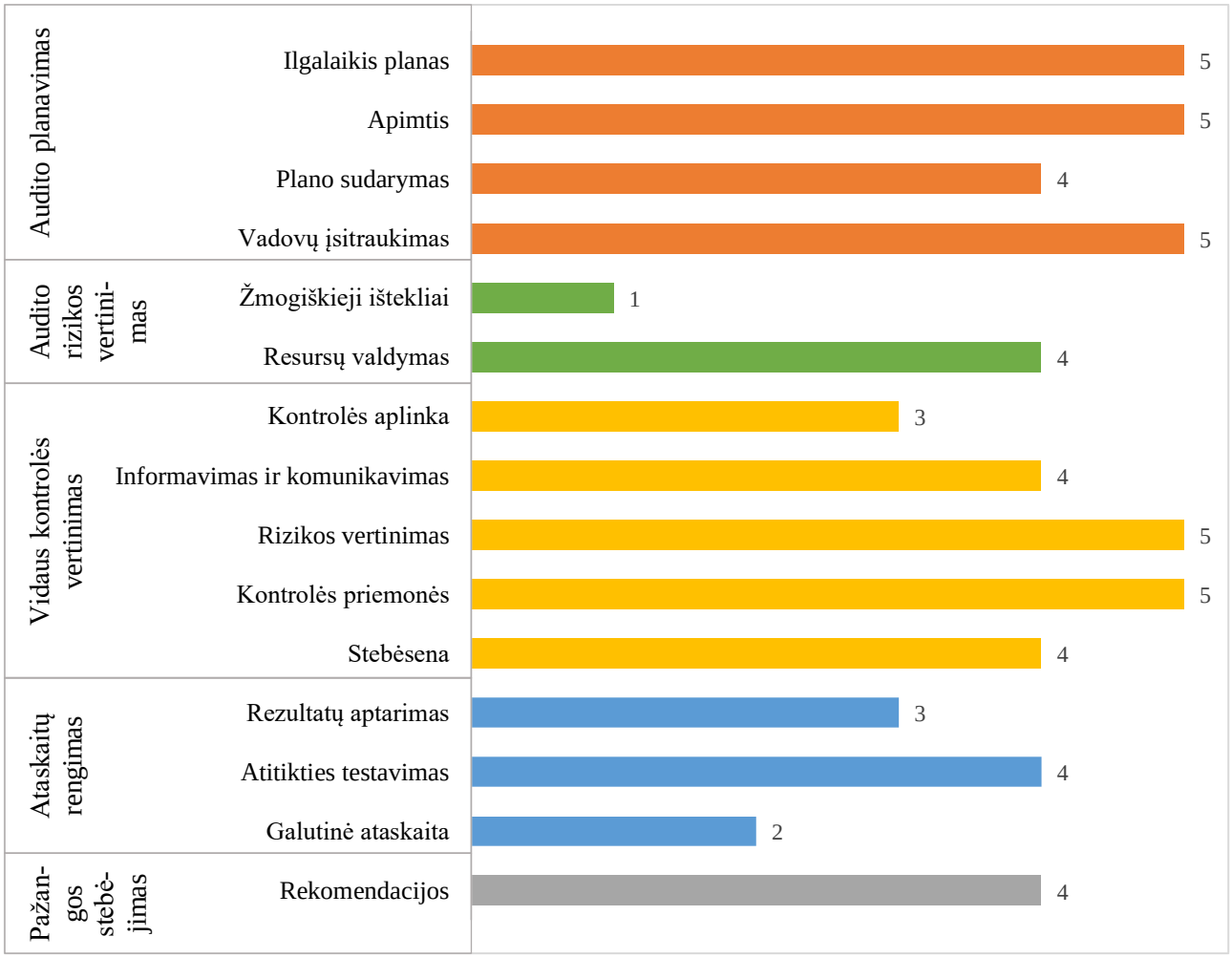
Vidaus audito procedūrų vertinimo įverčių suma B įmonėje parodo, kad įmonė atitinka **pakankamą** vidaus audito procedūrų užtikrinimo lygį, vertinimas surinko 58 balus. Šis balas kibernetinės atakos tikimybę sumažina iki retos. Pagal aritmetinius kiekvienos procedūros kriterijų vertinimo vidurkius (13 pav.) nustatyta, kad organizacija pakankamai gerai užtikrina trijų iš penkių vidaus audito procedūrų atlikimą. Žmogiškųjų išteklių trūkumas lemia tai, kad nėra užtikrinama audito rizikos vertinimo procedūra, kuri yra svarbiausias veiksnys, nustatantis vidaus audito objektą ir tolimesnę jo programą. Mažas dėmesys skiriamas ataskaitų rengimo procedūroms užtikrinti kelia riziką vidaus audito rezultatų patikimumui, o tai leidžia daryti išvadą, kad įmonės B vidaus audito procedūros privalo tobulinamos.



13 pav. Vidaus audito procedūrų vertinimas B įmonėje (sudaryta autorės)

14 paveiksle aptariamame atskirų kriterijų vertinime matoma, kad vidaus audito planavimo procedūroje organizacija užtikrina tinkamą pasirengimą vidaus auditui visuose vertinamuose kriterijuose. Ilgalaikio vidaus audito plano sudarymas organizacijoje B lemia optimalesnį bendro biudžeto paskirstymą reikalingiems ištekliams, audituojamų sričių planavimą, pagrindinių organizacijai kylančių rizikų vertinimą, numatomus audito tikslus ir lūkesčius. Vidaus audito procedūrų apimtys padidėja su tikslu įvertinti vidaus audito subjektų prioritetų ir pagrindinių rizikų nustatymą, o tai leidžia šį kriterijų vertinti aukščiausiu įverčiu. Tai, kad sudarydama būsimo vidaus audito planą įmonė atsižvelgia į visos organizacijos rizikos vertinimą, o kai kurios rizikos yra vertinamos „dėl atitikties teisės aktams keliamų reikalavimų“, leidžia teigti, kad organizacija B planavimo etape siekia atsakingai suformuluoti tinkamą audito požiūrį. Tik dėl to, kad įmonės atstovė negalėjo įvardinti, kuriems planavimo etapams (atsakingų padalinių, procesų ar darbų paskirstymui, žmogiškųjų ar finansinių išteklių įvertinimui) skiriamas didžiausias dėmesys, vertinimo kriterijui

nebuvo suteiktas aukščiausias įvertinimas. Vadovų požiūrio vertinimas parodė, kad vadovai yra susipažinę su vidaus audito teigiama įtaka organizacijos funkcinei ir reputacinei padėčiai, todėl vertindami ir skirdami išteklius, reikalauja vidaus audito plano patvirtinimo valdyboje.



14 pav. Vidaus audito procedūrų kategorijų vertinimas B įmonėje (sudaryta autorės)

Audito rizikos vertinimo etapas reikšmingas reikalingam žmogiškųjų išteklių ir resursų valdymo užtikrinimui. Įmonė susiduria su audito rizikos vertinimo problema, nes neturi pakankamai specialistų vidaus audito procedūroms atlikti, todėl yra įdarbinami darbuotojai iš išorės. Pagrindinis šių darbuotojų vertinimo kriterijus – turima patirtis ir atliktų vidaus audito dalių kiekis. Specialistų įdarbinimas dalykinėms kompetencijoms įvertinti nagrinėtoje literatūroje vertinamas teigiamai, tačiau pilnam vidaus audito procedūrų užtikrinimui reikalingi nuolatos įmonėje dirbantys specialistai. Jų žinios apie organizacijoje vykstančius procesus gali patikimiau įvertinti įmonei kylančias funkcines rizikas, o tai turės įtakos ir audito rizikos vertinimui. Resursų valdymo kriterijus gavo aukštą įvertį, nes organizacijos resursų kokybės valdymą periodiškai tikrina išorės vertinimas, o darbo valandų paskirstymas sudaromas laikantis profesinės priežiūros standartų bei planuojant jas vienerių ir trejų metų laikotarpiui.

Audito rizika, pagal 200-ąjį Tarptautinį audito standartą, priklauso nuo vidaus kontrolės, kuriai įtaką daro įmonės verslo tikslų siekimas ir organizacijos struktūros veikimo efektyvumas. Ši priklausomybė dažniausiai paremta organizacijos vidaus kontrolės vertinimu, kurio vertinimo kriterijai įmonėje B yra užtikrinami. Kontrolės aplinką apibūdinantis verslo etikos lygis vertinamoje

įmonėje yra pakankamas, tačiau nors ir juntamas vadovų grįžtamasis ryšys vertinant ankstesnių metų vidaus auditus, vadovų pavyzdžiu nėra formuojama darbinė aplinka. Ankstesnių auditų vidaus kontrolės valdymo patirtimi ir galimybe analizuoti pokyčius joje grindžiamas procedūrų detališkumas, kuris daro įtaką vidaus audito ateities sprendimams. Rizikoms įvertinti organizacija B skiria pagrindinį dėmesį vidinių ir išorinių grėsmių nustatymui, o tai padeda laiku nustatyti kylančias problemas ir pagal jas ieškoti tinkamų sprendimų, kibernetinio saugumo rizika vertinama tokius pačiu principu. Kontrolės priemonių vertinimas parodė, kad rizikų nustatymo patikimumą padeda įgyvendinti privalomi išorės ir vidaus auditai bei nuolat sertifikuojama ir standartizuojama pagrindinė organizacijos veikla – telekomunikacijų ir informacinių technologijų paslaugos. Efektyviam vidaus kontrolės valdymui privalo būti užtikrinama tinkama jos stebėsena, todėl vertinamoje B organizacijoje šiam tikslui naudojamos patvirtintos kontrolės procedūros ir funkcijų atskyrimas leidžia patikrinti gautus rezultatus apie kontrolės procesų tinkamumą ir veiksmingumą.

Ataskaitų rengimo procedūra vertinamoje B įmonėje įvertinta vidutiniškai. Tik tam tikrų vidaus audito rezultatų pristatymas įmonės vadovams leidžia manyti, kad vadovų žinios tiek apie vidaus auditą, tiek apie jo rezultatus yra nepakankamos. Vidaus auditorių dėmesys skiriamas atitikties testavimo procedūrai užtikrina, kad atliekamo periodinis testavimo metu yra atrandami bendri veiklos ir rezultatų peržiūros rodikliai. Šios priemonės leidžia organizacijai vidaus auditą naudoti kaip įrankį pagrindinių įmonės rizikų vertinimui. Nors pažangos stebėjimo etape dažniausiai pateikiamos rekomendacijos tolimesnei įmonės veiklai, susijusios su grėsmių suvaldymu, tačiau galutinei vidaus audito ataskaitai nėra užtikrinimas pakankamas detalumas. Šis kriterijus galėtų būti tobulinamas bendrą audito išvadą ir rezultatus detalizuojant atskiroms organizacijoms sritims, o tai prisidėtų ir prie poauditinės veiklos – pažangos stebėjimo – tobulinimo.

Įvertinus visus B įmonės kibernetinio saugumo rizikos ir vidaus audito procedūrų vertinimo rezultatus toliau pateikiamos rekomendacijos, kurios galėtų padėti organizacijai tobulinti kibernetinio saugumo rizikos vertinimo procesus vidaus audito procedūrose. Rekomendacijos pateikiamos 12 lentelėje.

12 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos B įmonėje (sudaryta autorės)

Siūloma tobulinimo priemonė/ sritis	**Rekomendacijos paaiškinimas**
Atskirti infrastruktūros vertinimą nuo bendro informacinių sistemų vertinimo	Organizacijos B kibernetinio saugumo rizikos nustatymo procedūros vertinimas parodė, kad bendra informacinių sistemų analizė negali užtikrinti infrastruktūros tinkamumo kibernetinio saugumo rizikos duomenų vertinimui. Kadangi šis vertinimas apima pagrindinių organizacijos duomenų, kritinės infrastruktūros ir informacinių technologijų vertimą, svarbu nustatyti, kiekvienos iš jų tinkamumą ir atitiktį tolimesniam vertinimui.
Didinti vadovybės įsitraukimą į kibernetinio saugumo rizikos valdymo ir vidaus audito ataskaitų rengimo procedūras	Organizacijos B kibernetinio saugumo rizikos valdymo ir vidaus audito ataskaitų rengimo vertinimas parodė, kad nors vadovai šias procedūras ir su jomis susijusias rizikas laiko svarbiomis, pačių vadovų įsitraukimas ir žinios neužtikrina tinkamo šių procedūrų valdymo. Atitinkamai, vadovų įžvalgos, grįžtamasis ryšys, žinios, kompetencijos ir nuolatinis bendradarbiavimas šiais klausimais galėtų lemti patikimesnius sprendimus kibernetinio saugumo rizikos vidaus audito procedūrose vertinime.

Siūloma tobulinimo priemonė/ sritis	Rekomendacijos paaiškinimas
Nuolatiniam darbui įdarbinti vidaus audito specialistus, užtikrinti jų kompetencijas	Organizacijos B žmogiškųjų išteklių vertinimas vidaus audito procedūrose parodė, kad organizacija skiria per mažai dėmesio kompetencijų ir reikalingo specialistų kiekio užtikrinimui. Specialistų trūkumas lemia papildomų išteklių poreikį įdarbinant juos iš išorės, o nepakankamas jų įsigilinimas į įmonės veiklą gali lemti vidaus audito klaidų galimybę, kuri įtakos ir bendras vidaus audito išvadas. Nuolatinis vidaus audito specialistų darbas įmonės viduje užtikrintų nuolatinį procesų stebėjimą ir kontrolę, leistų savo įžvalgomis tobulinti vidaus audito atlikimą.
Detalizuoti vidaus audito galutinės ataskaitos pateikimą	Organizacijos B vidaus audito ataskaitų rengimo procesų vertinimas atskleidė, kad įmonė galutinėje ataskaitoje pateikdama bendras išvadas ir rekomendacijas neužtikrina jų detalumo. Detalumas galėtų padėti atskiroms organizacijos sritims atkreipti dėmesį į tobulintinus procesų valdymo kriterijus, nuolat stebėti juose vykstančius pokyčius, efektyvintų organizacijos poauditinę veiklą ir užtikrintų pažangos stebėjimo etapus.

4.3. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai C įmonėje

C įmonė yra finansinių konsultacijų ir klientų aptarnavimo paslaugas teikianti įmonė, veikianti Lietuvos teritorijoje. Įmonės teikiamų paslaugų infrastruktūra bei turimi finansiniai klientų duomenys yra patraukliausia kibernetinių atakų rūšis, kelianti pavojų ne tik organizacijai, bet liečianti kiekvieno kliento finansinių duomenų atskleidimą ar praradimą. Skaitmeninių paslaugų ir įrankių plėtra organizacijoje yra prioritetinis tikslas, todėl tam reikalingos papildomos saugumą užtikrinančios priemonės. Siekiant gerinti organizacijos duomenų ir operacijų saugumą yra taikomi automatizuoti sprendiniai, užtikrinantys darbo sąnaudų mažėjimą, bei leidžiantys darbuotojams prisidėti prie organizacijos tobulinimo ir vystymo kitomis, pridėtinę vertę kuriančiomis užduotimis. Žemiau yra pateikiami C įmonės kibernetinio saugumo rizikos vertinimo rezultatai (13 lentelė).

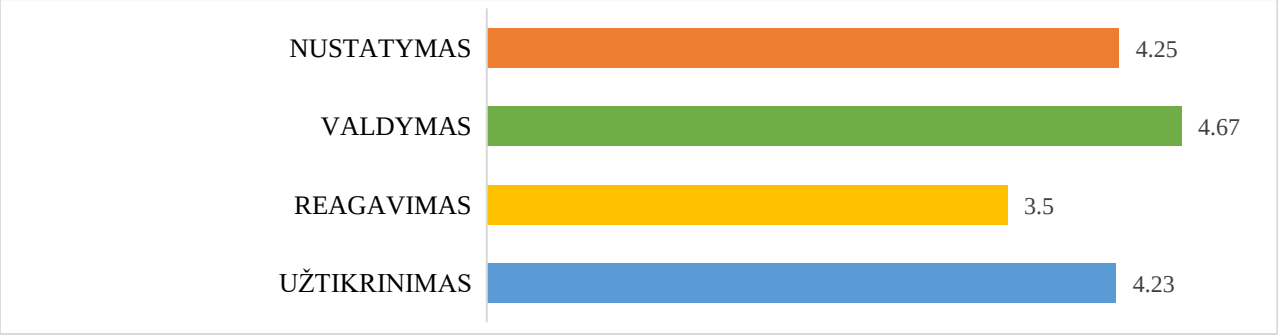
13 lentelė. Kibernetinio saugumo rizikos vertinimo C įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Grėsmių identifikavimas	„Reikalingų išteklių visoms grėsmės įvertinti reikia vis daugiau, todėl teigti, kad jų yra pakankamai – vertinant tai, kad didžiausia organizacijos grėsmė yra duomenų praradimas – matyt reiktų atsargesnio vertinimo [...] saugumo specialistai nuolat fiksuoja bandymus „įsilaužti“, tačiau kolkas pavyko su visomis grėsmėmis sukovoti“	4
Infrastruktūros vertinimas	„Manau, kad **taip**, infrastruktūra pakankama, nes kuo negalime pasirūpinti patys, tam užtikriname išorės paslaugas [...] tai IT paslaugomis ir su jomis susijusia infrastruktūra rūpinasi išorės įmonė, mūsų specialistai tik yra apmokyti, kokią informaciją turi perduoti [...] kita infrastruktūra rūpinamės patys“	4
Poveikio analizė	„poveikis vertinamas nuolat [...] poveikio minimali riba yra mažiausia grėsmė kylanti organizacijai [..] bendrai vertinant, viskas apie ką kalbame yra labai susiję ir tas poveikis turi būti vertinamas kompleksiškai ne tik nuo įmonėje taikomų saugumo priemonių, bet ir sektoriaus, ir susijusių šalių ir pan. “	5
Saugumo informacijos stebėsena	„**Taip [...]** atliekami saugumo sistemų naujinimai, dalyvavome KSC parengtose kibernetinio saugumo pratybose [...] bendradarbiaujame su kibernetinės žvalgybos institucijomis, kurie turi specialias prieigas bei gali analizuoti didelės apimties saugos duomenų žurnalus, patys tokių dokumentų nerengiame“	4

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Valdymo modelis ir struktūra	„**Taip**, kibernetinės rizikos valdymo analizei skiriamas didelis dėmesys [...] sprendimus priima valdybos įgalioti Rizikos departamento vadovai“	5
Vadovybės įtaka	„**Taip**, vadovų vertinimu tai viena skaudžiausių ir mažiausiai pažįstamų rizikų, vadovai todėl ieškoma naujų priemonių kaip kuo daugiau specialistų įtraukti į jos valdymą“	4
Reguliavimo ir teisinė aplinka	„**Taip**, kibernetinio saugumo rizikos reguliavimo ir teisinė politika parengta vadovaujantis Tarptautiniais reguliavimo standartais ir metodikomis, kurios reguliariai peržiūrimos dėl vykstančių pokyčių šioje srityje“	5
Kibernetinės rizikos analitika	„Jau minėjau anksčiau, kad tai susiję su poveikio analize ir stebėsena, nes specialistai nustatę grėsmę ieško priemonių jai įveikti, tam padeda atakų analitikos programos, galinčios detalizuoti tolimesnę elgseną [...] vykdomas dar padalinių, kurie susiję su operacine rizika reguliarus Rizikos ir kontrolės įsivertinimas““	3
Prognozės ir elgsena	„[...] taikiniu gali būti bet kuri organizacijos infrastruktūra arba jos žmonės[...] tolimesnė elgsena vertinama per rinkos, klientų ir partnerių prizmes, kur dauguma organizacijos veiklos sričių yra priskiriamos aukštos rizikos grupei“	4
Priežastiniai ryšiai	„procesų ir priežastinių ryšių modeliavimas leidžia nustatyti geresnius rezultatus analitikoje [...] procesų suvokimas – geriau pažinti galimą grėsmę“	3
Atsako planavimas	„**Taip**. Atsako planavimas susijęs su kibernetinės rizikos analitika, kuriai atliekamos atakų analizės (išmėginama Bitdefender programa) jau duoda rezultatų tikslingesnio atsako į grėsmę planavimui. Taip pat įmonė turi ištestuotus veiklos tęstinumo planus”	4
Saugumo programų valdymas	„**Taip**, organizacijos saugumo programa sudaryta pagal Tarptautinius standartus ir kitus juos lydinčius dokumentus […] visų, o ypatingai slaptų duomenų perdavimui tinkais ir duomenų saugojimui saugyklose naudojamos šifravimo priemonės [...] valdyba, kartu su finansinių išteklių skyriumi privalo tokio lygio programas patvirtinti”	5
Duomenų apsauga	„Tai užtikrina išorės įmonė, mes perkame duomenų apsaugos paslaugas. Šiuo metu įmonėje atliekamas asmens duomenų saugumo auditas, kurio metu duomenų saugumu besirūpinančiai įmonei siunčiamas pagal sutartį su jais sudarytas klausimynas, kuris vertina, ar tiekėjas tinkamai laikosi saugumo reikalavimų, tačiau patys kitų kontrolės testavimų neatliekame“	4
Tapatybės ir prieigos valdymas	„**Taip**, darbuotojams suteikiama tik ta prieiga prie sistemų, kuri yra reikalinga jų darbo funkcijoms atlikti [...] naujiems suteikiamos darbuotojo teisės, darbuotojo kodas ir laikinas slaptažodis, kurį per ribotą laiką turi pasikeisti [...] prieigos teises administruoja sistemą prižiūrintys specialistai”	5
Infrastruktūros apsauga	„**Taip**, turime nemažai tai užtikrinančių priemonių – visa įmonės veiklai naudojama įranga (kompiuteriai, telefonai, serveriai) turi įdiegtą „Bitlocker“ šifravimą. Taip pat darbuotojams draudžiama siųstis programinę ar panašią įrangą, jei ji nėra patvirtinta mūsų IT skyriaus“	5
Programinės įrangos apsauga	„Valdymas atliekamas mūsų IT specialistų, tačiau programinės įrangos apsaugą užtikrina išorės specialistai, nes ji reikalauja specifinių žinių ir patirties, mes tik vertiname atitiktį sudarytoms sutartims, ar užtikrina visus įsipareigojimus“	4

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Trečiųjų šalių valdymas	„**Taip**, ir vertinimas, ir atranka tiek kalbant apie klientus, tiek apie tiekėjus [...] kiekviena pasirašoma sutartis vertinama teisininkų ar atsakingos srities specialistų su sankcijų numatymu pažeidžiant nustatytus sutarčių punktus“	5
Debesų valdymas	„Tiek debesijos, tiek serverių valdymu rūpinasi išorės specialistai, šioje vietoje riziką dalijamės su paslaugų tiekėjais, nes suvaldyti procesų efektyvumą visose srityje patiems lemtų didesnes investicijas [...] kolkas toks pasirinkimas tenkina visus lūkesčius“	4
Darbuotojų kompetencijos	„Manau, kad darbuotojų kompetencijos **yra pakankamos** atlikti darbus pagal savo funkcijas šiai dienai, tačiau reikalingas nuolatinis žinių atnaujinimas”	3
Mokymai	„**Taip**, bendrus saugumo informacijos, pinigų plovimo, sukčiavimo prevencijos mokymus skatiname išklausyti visiems darbuotojams, pratybos rengiamos taip pat”	3

Kibernetinio saugumo rizikos apibendrintame kategorijų vertinime C organizacija įvertinta 81 balų iš 100 galimų. Pagal sudarytą konceptualų kibernetinio saugumo rizikos vidaus audito procedūrose modelį toks vertinimas atitinka **aukščiausią** kibernetinio saugumo rizikos vertinimo lygį ir lemia nežymų rizikos poveikį įmonės veiklos procesams. Pagal kibernetinio saugumo rizikos vertinimo kriterijų aritmetinius vidurkių diagramą (15 pav.) galima teigti, kad organizacija visapusiškai užtikrina nustatymo, valdymo ir užtikrinimo etapų kategorijas. Net aštuoni vertinimo kriterijai buvo įvertinti aukščiausiu įverčiu, o dar devyni atitiko aukštą kriterijaus išpildymo lygį. Kiek žemesnį reagavimo kategorijos vertinimą lėmė rizikos analitikos ir kontrolės bei priežastinių ryšių nustatymo taikomos priemonės ir metodai.



15 pav. Kibernetinio saugumo rizikos kategorijų vertinimas C įmonėje (sudaryta autorės)

Žemiau bus išsamiau aptariami atskirų kibernetinio saugumo rizikos lygį vertinantys kriterijai (16 pav.). Pagal kibernetinio saugumo rizikos nustatymo vertinimą, grėsmių identifikavimui ir infrastruktūros vertinimui skiriami ištekliai yra pakankami. Vertinant analizuojamos įmonės informacinių technologijų infrastruktūrą svarbu paminėti, kad ją sudaro programinė ir aparatinė įranga, tinklo komponentai, kurie tampa jungiamąja dalimi tarp įmonės sistemos ir jos vartotojų. Naujų produktų ar procesų vertinimas atliekamas pagal „Produkto ir veiklos tvirtinimo“ politiką, kurios tikslas yra įvertinti galimą operacinę riziką. Ir nors infrastruktūros užtikrinimo vertinime svarbu šias priemones vertinti kaip atskiras, duomenų saugojimui tinkamas priemones, atliekant poveikio analizę svarbu vertinti kompleksinį šių taikomų priemonių veikimą. Tai patvirtina ir organizacijos atstovas, kuris atvirai kalbėjo apie neįmanomą visišką kibernetinio saugumo grėsmės

suvaldymą, o tinkamą reakciją į ją įvertino ne tik per organizacijoje, tačiau ir verslo sektoriuose, o kai kuriais atvejais net ir valstybės taikomomis priemonėmis. Organizacijoje tai vertinama kaip būtina grėsmės nustatymo priemonė, kurios poveikis nuolat vertinamas. Saugumo informacijos stebėseną analizuojamoje organizacijoje užtikrina atliekami saugumo sistemų atnaujinimai ir dalyvavimas saugumo pratybose. Bendradarbiavimas su žvalgybos institucijomis leidžia įvertinti skelbtinus duomenis apie nacionalinį saugumą, o tai vertinama kaip papildoma saugumo informacijos stebėsenos priemonė.

16 pav. Kibernetinio saugumo rizikos kriterijų vertinimas C įmonėje (sudaryta autorės)

Kibernetinio saugumo rizikos valdymo vertinimas įmonėje C užtikrinamas Rizikos departamento veikla ir atsakomybėmis. Jis atsakingas už rizikos vertinimą ir privalo pateikti visą su saugumu susijusią informaciją valdybai, kuri kibernetinę riziką vertina prioritetine organizacijos sritimi. Įmonės C turima reguliavimo ir teisinė politika yra parengta pagal Tarptautinius reguliavimo standartus ir nuolat atnaujinama. Rizikos valdymo sistemos turėjimo būtinybę patvirtina ir Camillo, M. (2016) atliktas pasaulinio bankų ir finansinių institucijų tyrimas, kuriame apie kibernetinio saugumo rizikos valdymą autorius teigia, jog finansų įstaigos privalo parengti veiksmingą informacijos saugumo programą, pritaikytą jos operacijų sudėtingumui ir reikalauti išorinių šių paslaugų tiekėjų griežtai jos laikytis. Vadovų įsitraukimo vertinimas parodė, kad organizacijos vadovai kibernetinio saugumo riziką vertina kaip vieną pavojingiausių įmonės veiklos tikslų

įgyvendinimui, turi pakankamai žinių apie grėsmės poveikį, todėl skatina tiek pačių, tiek darbuotojų iniciatyvas, susijusias su šios rizikos suvaldymu. Tokiu įsitraukimu yra formuojama vadovų pavyzdžiu sektina darbinė aplinka.

C įmonės kibernetinio saugumo rizikos vertinimas parodė, kad pagal reagavimo procedūros kriterijus įmonė buvo įvertinta mažiausiai. Kibernetinės rizikos analitiką vadovai sieja su poveikio analizės ir saugumo stebėsenos atlikimu, tačiau analitikos integravimas į veiklos kontrolės sistemas padėtų didinti bendrą organizacijos atsparumą kibernetinei saugumo grėsmei. Interviu minimo atskirų, su operacine rizika susijusių, padalinių „Rizikos ir kontrolės įsivertinimas“ galėtų tapti visos veiklos vertinimo pagrindu. Atakų analitika ir jos pagrindu parengtas atsako planavimas – yra aukščiausio lygio reagavimo būdas, tačiau kol jis organizacijos C veikloje yra tik testuojamas, tai neleidžia šio kriterijaus vertinti aukščiausiu įverčiu. Priežastinių ryšių tarp atliekamų organizacijos veiksmų ir pasekmių nustatymas vertinamas fragmentiškai, nėra jais grindžiami tolimesnis sprendimų priėmimas. Organizacijos vykdoma švietėjiška visuomeninė veikla ir vykdoma informacinė kompanija apie saugumą, susijusį su internetiniais sukčiavimais, prisideda prie atsako į kibernetinę riziką planavimo ir veikia kaip papildoma išorės saugumą vertinanti priemonė. Apibendrinant galima teigti, kad nors reagavimo procedūrų užtikrinimas įmonėje C kol kas yra tik vidutinis, tačiau organizacijos dedamos pastangos ateityje gali turėti teigiamą įtaką kibernetinio atsparumo didinimui.

Net penki kibernetinės saugumo rizikos užtikrinimo vertinimo kriterijai – saugumo programų, tapatybės ir prieigos, infrastruktūros apsaugos ir trečiųjų šalių valdymas – surinko aukščiausius įverčius. Tai lemia įmonėje naudojamos duomenų šifravimo, kodavimo, prieigos, slaptažodžių politikos priemonės, prisideda valdymo atitiktis Tarptautiniams informacinių technologijų paslaugų valdymo standartams bei griežtų įsipareigojimų vykdymas pagal sudarytas trišales sutartis. Duomenų, programinės įrangos ir debesijos valdymo apsaugai užtikrinti organizacija C naudoja išorės specialistų paslaugas (ang. *outsourcing*). Nors išorės specialistai bendradarbiauja su įmonėje dirbančiais informacinių sistemų specialistais, juos apmoko prižiūrėti sistemas, pagal įsipareigojimus jas testuoja ir atnaujina, tačiau šios srities specialistų įdarbinimas organizacijos viduje padėtų užtikrinti nuolatinę sistemų apsaugą ir tolimesnį investicijų poreikį šiuo klausimu. Dėl šios priežasties vertinant darbuotojų kompetencijas galima teigti, kad jos yra pakankamos darbo funkcijoms įvykdyti, tačiau kibernetinio saugumo įgūdžiai turi būti tobulinami. Tai, kad įmonė rengia bendrinius kibernetinio saugumo mokymus ir pratybas padeda apsaugoti organizaciją nuo „nežinojimo“ rizikos, kuri susijusi su darbuotojų žinių trūkumu apie kibernetinio saugumo poveikį įmonės procesams. Tačiau kibernetinio saugumo analitikai, atsako modelių rengimui, naudojamų saugumo programų valdymui reikalingos specializuotos kibernetinio saugumo ekspertų žinios. Įvertinus tai, kokius duomenis kaupia C įmonė ir kokiais nuostoliais gali būti įvertinta kibernetinė ataka, papildomai apsaugai ir jos priežiūrai šioje organizacijoje būtų galimas taikyti teorinėje dalyje nagrinėtas Trijų linijų modelis (angl. *The Three Lines of Defense Model*).

14 lentelė. Vidaus audito procedūrų vertinimo C įmonėje rezultatai (sudaryta autorės)

Tikrinamas kriterijus	**Citata, pagrindžianti arba paneigianti kriterijaus svarbumą**	**Įvertis, pagal sudarytus įverčio rangus**
Ilgalaikis planas	„**Taip,** banke patvirtinama vidaus audito politika trejiems metams [...] joje nurodomi ilgalaikiai audito veiklos tikslai, vadovų požiūris ir indėlis siekiant įvertinti vidaus kontrolę, darbuotojų kompetencijų klausimas, audito rezultatų tęstinumas“	5

Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Apimtis	„Jei pasakyčiau, kad **banke yra 30 audituojamų sričių**, tikriausiai nereikės atsakinėti į klausimą, ar viskas yra vertinama [...] kibernetinio saugumo grėsmę galima vertinti per daugumą iš tų sričių, kaip pvz. saugumo skyriaus, pinigų plovimo prevencijos priemones, IT sistemų valdymą, mokėjimų pervedimus, likvidumo, rinkos rizikos valdymą ir t.t.“	5
Plano sudarymas	„**Taip**, ir tikriausiai galėčiau papildyti, kad ne tik mūsų organizacijos, bet ir viso finansinio sektoriaus galimomis rizikomis remiantis formuojamas būsimo audito požiūris. [...] didžiausias skiriamas dėmesys labai priklauso nuo konkrečių audito tikslų ir nustatytų rizikos veiksnių, būdingų būsimam auditui, tačiau visi jūsų išvardinti etapai yra vertinami, o jau atitinkamas procedūras jiems vertinti priima vidaus audito vadovas “	5
Vadovų įsitraukimas	„Priimdama sprendimus vadovybė **visada** gauna informaciją apie atskirų padalinių veiklą ir pokyčius juose iš atskirų skyrių ar sričių vadovų, vidaus audito padalinys – ne išimtis. Vidaus audito planui, su jam reikalingais ištekliais ir atsakomybėmis, reikalingas vidaus audito vadovo patvirtinimas. “	4
Žmogiškieji ištekliai	„Kiek man yra žinoma - pakanka darbuotojų ir jų kompetencijų visoms vidaus audito funkcijoms įvykdyti. Ne vienerius metus žmonės nesikeičia – skyriuje dirba vidaus audito vadovas, auditoriai ir jų asistentai, atsakingi už vidaus audito plane išdėstytus procesus [...] finansinėse institucijose vidaus auditoriaus tinkamumą vertina priežiūros institucijos, pvz. Lietuvos bankas. Jam siunčiami išsilavinimo dokumentai, gyvenimo aprašymas, kandidatas patikrinamas dėl teistumo. Kas 5 metai paprastai atliekamas išorės vertinimas vidaus auditui pagal Tarptautinius vidaus audito standartus“	3
Resursų valdymas	„**Tinkamai**. Jų tinkamas valdymas užtikrinamas įvertinant darbuotojų atlyginimus, specialistų konsultacijas, technologinius poreikius bei kitas pridėtines išlaidas “	4
Kontrolės aplinka	„**Taip** [...], etikos lygį apibrėžia Vidaus kontrolės ir rizikos vertinimo organizavimo reikalavimai, kurie nurodo visiems darbuotojams laikytis griežtų etikos taisyklių. Be jų, bankas turi pasitvirtinęs ir savo vidaus audito standartus [...]. Tai – nešališkumo, objektyvumo ir nepriklausomumo principai, paremti lojaliu ir profesionaliu darbuotojų darbu“	5
Informavimas ir komunikavimas	„Grįžtamajam ryšiui **skiriamas** labai didelis dėmesys, nes tai padeda reaguoti į organizacijos ar rinkos pokyčius, laiku nustatyti rizikas, tinkamai į jas reaguoti [...] efektyvi komunikacija yra esminė organizacijos veiklos užtikrinimo priemonė, todėl pritariu, kad šis vertinimas atliekamas nustatant informacijos srautus ir jų pritaikomumą [..] skatinama viduje tokia nuolatinių pokalbių su darbuotojais politika, tai apie kažkokius trūkstamą informaciją dažniausiai išgirstame ten”	4
Rizikos įvertinimas	„**Vienareikšmiškai**, toks yra rizikos vertinimo tikslas. Vertinant vidaus kontrolę grėsmės yra ne tik identifikuojamos, bet nustatomas ir jų poveikio lygis, kuris susiejamas su galimais organizacijos nuostoliais. [...] kadangi didžiąją dalį banko veiklos reguliuoja LR įstatymai ir teisės aktai, o už jų nesilaikymą skiriamos baudos ir grėsmė organizacijos reputacijai, tai čia yra mūsų prioritetinė sritis“	5

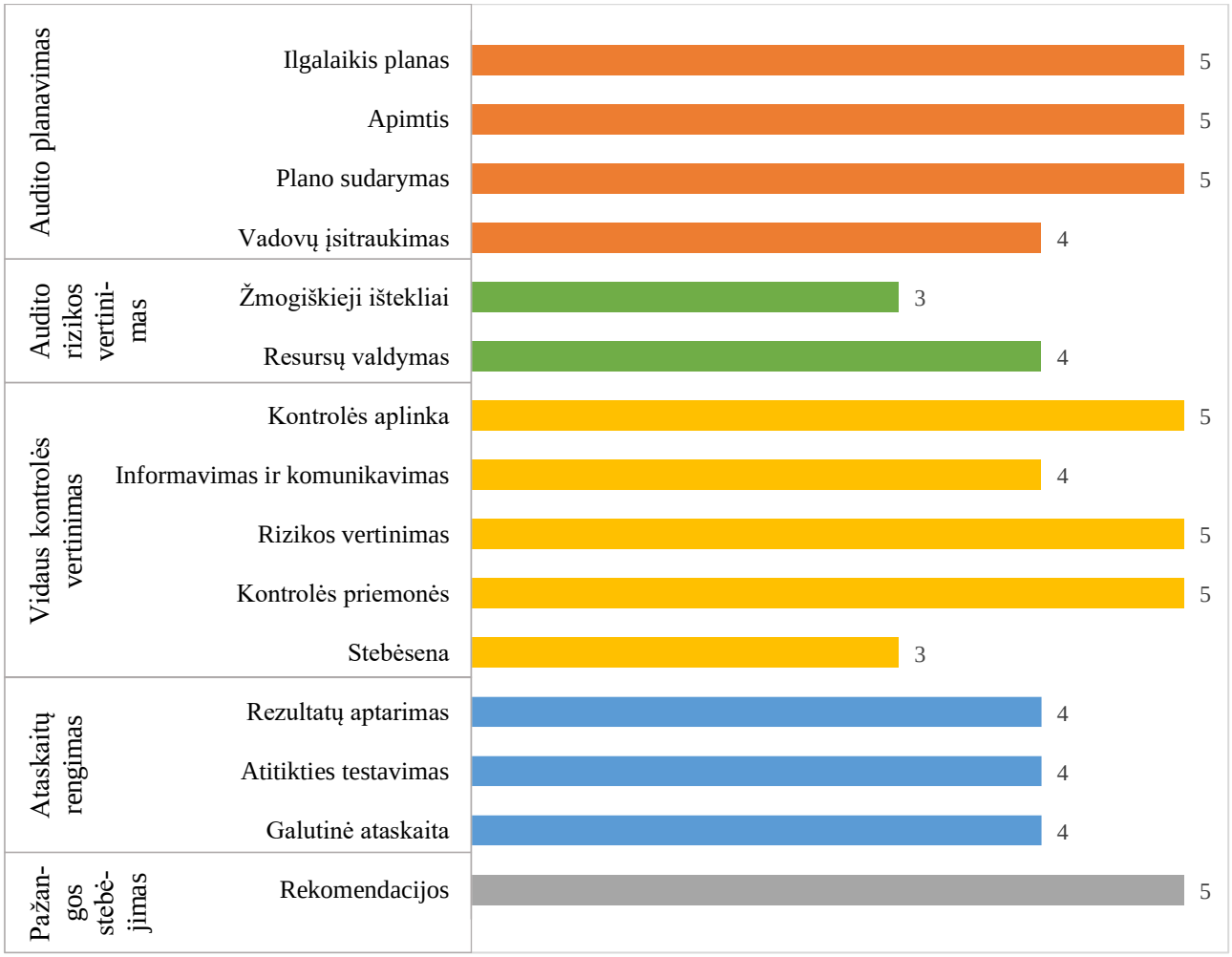
Tikrinamas kriterijus	Citata, pagrindžianti arba paneigianti kriterijaus svarbumą	Įvertis, pagal sudarytus įverčio rangus
Kontrolės priemonės	„Priemonės **pakankamos**, tačiau nėra baigtinės [...] šios išvardintos kontrolės rūšys yra atliekamos, o prie jų prisideda ankstesnių auditų vertinimas, poauditinės veiklos vertinimas. Kaip didžiausios kontrolės sistemos problemos dažniausiai įvardinami įvykę pasikeitimai kažkurioje vertinamoje srityje, taip pat pakartotinai nustatyti pažeidimai“	5
Stebėsena	„Stebėsenos atsakomybė taip pat priklauso vidaus auditoriams, jie po atlikto audito stebi, ar vadovai ir darbuotojai sureagavo į rekomendacijas ar laiku pašalino nustatytus trūkumus”	3
Rezultatų aptarimas	„**Taip**, rezultatai dažniausiai pristatomi vadovybei, nebent tai yra atskira audito dalis, kuri skirta tik papildyti buvusį auditą. [...] dažniausiai jie būna netgi detalesni nei galutinė ataskaita, nes vadovai reikalauja plataus požiūrio ir įvertinimo [...] rezultatams įtakos vadovai negali daryti, tačiau kartais galutinei ataskaitai yra reikalaujama naujų sąsajų įvertinimo, papildomo paskaičiavimo ar kito vertinamo objekto išvados“	4
Atitikties testavimas	„Atitikties testavimas atliekamas [...] periodiškai atliekama pagal vidaus audito nustatytus prioritetus”	4
Galutinė ataskaita	„Ataskaita būna detalizuojama pagal prioritetus, kurias problemas reikia spręsti ir kokia viso to nauda. Jei tas prioritetas reikalauja kažkokių paskaičiavimų, kurie audito metu buvo galimi įvertinti, tai pateikiami ir jie, kaip naudos pagrindimas [...] sritys priklauso nuo vertintų rizikų ir audito suformuluotų tikslų”	4
Rekomendacijos	„**Taip**, rekomendacijos visada pateikiamos kartu su galutine ataskaita“	5

Vidaus audito procedūrų vertinimo įverčių suma C įmonėje parodo, kad įmonė užtikrina **visapusišką** vidaus audito procedūrų lygį, vertinimas surinko 65 balus. Šio balo vertė kibernetinės atakos tikimybę sumažina iki labai retos. Pagal aritmetinius kiekvienos procedūros kriterijų vertinimo vidurkius (17 pav.) nustatyta, kad organizacija pakankamai gerai užtikrina keturių iš penkių – planavimo, vidaus kontrolės vertinimo, ataskaitų rengimo ir pažangos stebėjimo – vidaus audito procedūrų atlikimą. Žmogiškųjų išteklių trūkumas ir resursų valdymo sprendimai lemia tai, kad visapusiškai nėra užtikrinama tik audito rizikos vertinimo procedūra.

17 pav. Vidaus audito procedūrų vertinimas C įmonėje (sudaryta autorės)

Analizuojant atskirų vertinimo kategorijų kriterijus (18 pav.) vidaus audito planavimo procedūroje C įmonė užtikrina tinkamą pasirengimą vidaus auditui atlikti. Vidaus audito politika reikalauja ilgalaikio plano sudarymo, kuriame įvertinami ilgalaikiams tikslams įgyvendinti reikalingi ištekliai ir

su jais susiję atsakomybės. Vidaus audito procedūrų apimtys planuojamos kiekvienai audituojamai veiklos sričiai, todėl kibernetinio saugumo rizika yra įvertinama pagal atskiroms veiklos sritims kylančią riziką. Tai, kad sudarydama būsimo vidaus audito planą įmonė atsižvelgia ne tik į visos organizacijos rizikos vertinimą, bet ir finansiniam sektoriui galimas grėsmes, patvirtina apie kompleksinio vertinimo svarbą, plačiai aptartą literatūros analizės metu. Visos šios taikomos priemonės leidžia formuoti tinkamą audito požiūrį, prie kurio taip pat prisideda nuolatinis vadovų bendradarbiavimas ir ataskaitų patvirtinimų reikalavimas tinkamam kontrolės palaikymui.



18 pav. Vidaus audito procedūrų kategorijų vertinimas C įmonėje (sudaryta autorės)

Galimai vidaus audito rizikai nustatyti svarbus vertinimo etapas. Žmogiškųjų išteklių vertinimas nustatė pakankamą auditorių kvalifikacijos lygį, kurį nustato kontroliuojanti įstaiga – Lietuvos bankas. Jo vertinimas parengtas pagal Tarptautinius vidaus audito standartus, tačiau siekiant vidaus audito veiklos procesų tobulinimo organizacijos viduje šie reikalavimai turėtų būti derinami su organizacijos strateginių tikslų vertinimu, kuriems reikalingi aukščiausio lygio specialistai. Žmogiškųjų išteklių resursai organizacijoje C valdomi tinkamai – tam naudojamos darbuotojų darbo valandų paskirstymo ir darbo užmokesčio, specialistų konsultacijų, technologinio poreikio priemonės. Įmonės resursų kokybės valdymą kiekvienais metais tikrina išorės auditas.

Prie vidaus kontrolės vertinimo procedūros visapusiško užtikrinimo įmonėje C prisideda kontrolės aplinka, kuri organizacijoje formuojama „Vidaus kontrolės ir rizikos vertinimo“ bei „Vidaus audito standartų“ reikalavimų principais. Vidaus kontrolės metu organizacijos rizikų vertinimas siejamas su

galimais įmonės finansiniais nuostoliais bei atitiktimi Lietuvos Respublikos įstatymams, todėl skiriamų kontrolės priemonių užtikrinimas taip pat turi būti visapusiškas. Dėl šios priežasties kontrolės priemonėmis vertinama ne tik veiksmų-rezultatų kontrolė ar organizacijos kultūra, tačiau ir didžiausi pasikeitimai, įvykę organizacijos aplinkoje ar pakartotinai nustatomi pažeidimai. Jie įvardinami kaip didžiausios vidaus kontrolės sistemos problemos. Informavimo ir komunikavimo kriterijus įmonėje C vertinamas kaip viena iš reagavimo į organizacijoje ar rinkoje vykstančius pokyčius, priemonė, todėl jo užtikrinimui skiriamas didelis dėmesys. Sėkmingam vidaus kontrolės vertinimui užbaigti privalo būti užtikrinama tinkama stebėsena, tačiau šiam kriterijui skiriamas vidaus auditorių dėmesys negali patikrinti gautų rezultatų apie kontrolės procesų tinkamumą ir veiksmingumą.

Ataskaitų rengimo procedūra vertinamoje įmonėje C atliekama užtikrinant vadovų žinių apie audito rezultatus, atitikties testavimo ir galutinės ataskaitos išsamumo kriterijus. Detalus rezultatų pristatymas vadovybei, kuris reikalauja „plataus požiūrio ir vertinimo“ dar kartą patvirtina reikalingų aukštos kvalifikacijos specialistų poreikį bei tinkamą vadovų požiūrį į vidaus auditą. Vidaus auditorių dėmesys, skiriamas periodinei atitikties testavimo procedūrai pagal nustatytus vidaus audito prioritetus, leidžia manyti, kad atliekamo testavimo metu yra randami bendri vidaus audito ir organizacijos rizikų veikimo taškai. Bendrų rodiklių atitikties stebėjimas ne tik patvirtina vidaus kontrolės vertinimą, tačiau juo yra pagrindžiamos galutinės ataskaitos metu suformuotos išvados. Be to, šis vertinimas aktualus tampa ir bendradarbiavimo užtikrinimui tarp rizikas ir grėsmes vertinančių atsakingų padalinių bei vidaus audito specialistų, kurių indėlis kontrolės priežiūrai padėtų tinkamam kibernetinės saugumo rizikos vertinimui. Pažangos stebėjimo etape pateikiant rekomendacijas pagal rizikos vertinimo nustatytas prioritetines organizacijos sritis leidžia daryti išvadą, kad poauditinė veikla organizacijoje C yra užtikrinama.

Apibendrinus visus C įmonės kibernetinio saugumo rizikos ir vidaus audito procedūrų vertinimo rezultatus (13 ir 14 lentelės) toliau pateikiamos rekomendacijos, kurios galėtų padėti organizacijai tobulinti kibernetinio saugumo rizikos vertinimo procesus vidaus audito procedūrose. Rekomendacijos pateikiamos 15 lentelėje.

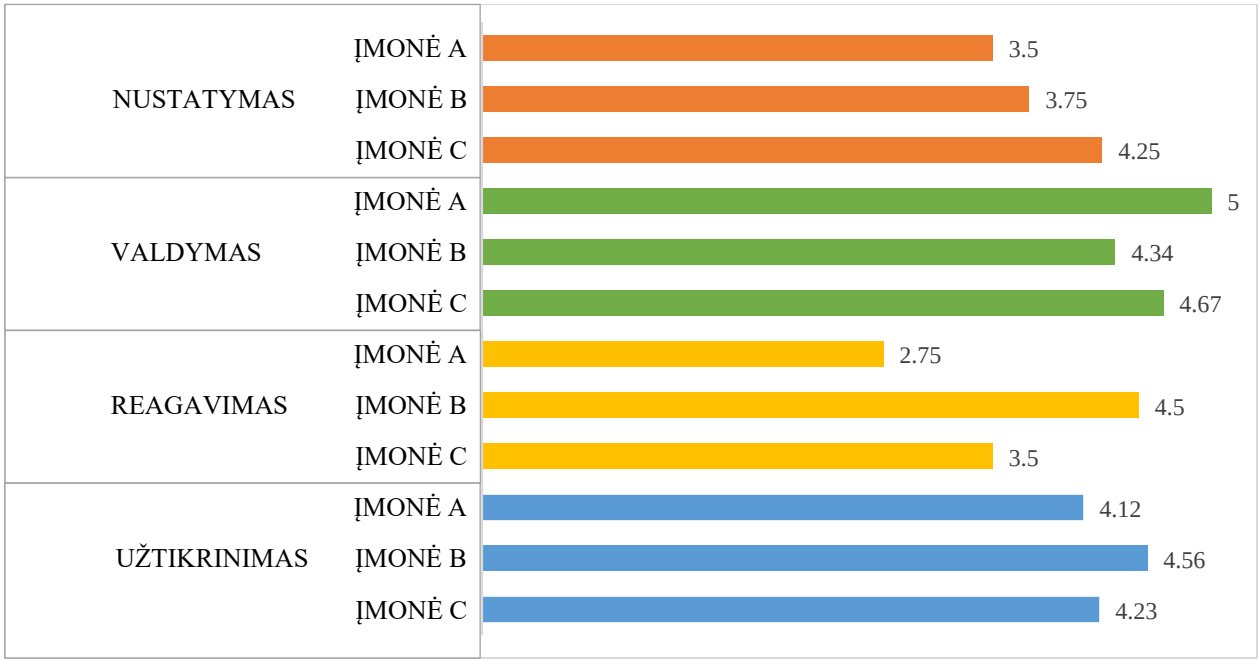
15 lentelė. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo tobulinimo rekomendacijos C įmonėje (sudaryta autorės)

Siūloma tobulinimo priemonė/ sritis	**Rekomendacijos paaiškinimas**
Įvertinti Trijų linijų modelio taikymą efektyviam kibernetinės rizikos valdymui ir kontrolės sistemai palaikyti	Organizacijos C kibernetinio saugumo rizikos vertimas parodė, kad įmonė taiko daugelį mokslinėje literatūroje vertintų rizikos planavimo, valdymo ir užtikrinimo priemonių, jos užtikrina aukštą kibernetinio saugumo rizikos lygį. Norint užtikrinti didesnį įmonės kibernetinį atsparumą, o ne tik taikomų priemonių kontrolę, reikalingas glaudus visų organizacijos funkcijų bendradarbiavimas bei išorės priežiūra, kuri dėl savo nepriklausomumo prisidėtų prie įmonės vertės kūrimo.
Įgalinti vidaus audito stebėsenos priemones	Organizacijos C vidaus kontrolės vertinimo procedūrą siūloma gerinti stebėsenos, kuri galėtų patvirtinti gautus rezultatus apie vidaus kontrolės procesų tinkamumą, vykdymą. Tam galėtų būti taikomas vidaus audito darbuotojų funkcijų atskyrimas, kuris sumažintų neatitikimų ir klaidų tikimybę, kylančią dėl skirtingų užduočių atlikimo. Efektyvus stebėsenos vykdymas taip pat galėtų prisidėti prie audito metu surinktų įrodymų patikimumo. Vadovybės dalyvavimas stebėsenos procedūroje padėtų užtikrinti vidaus kontrolės vertinimo suderinamumą su organizacijos tikslais.

Siūloma tobulinimo priemonė/ sritis	Rekomendacijos paaiškinimas
Nuolatiniam darbui įdarbinti kibernetinio saugumo ir vidaus audito specialistus, užtikrinti aukštas jų kompetencijas	Organizacijos C darbuotojų kompetencijų ir reikiamo jų kiekio vertinimas kibernetinio saugumo rizikos ir vidaus audito procedūrose parodė, kad organizacijoje šie kriterijai nėra užtikrinami. Visiems darbuotojams vykdomi kibernetinio saugumo rizikos mokymai lemia bazines organizacijos darbuotojų žinias, tačiau reikalingi kvalifikuoti, specifinius įgūdžius bei patirtį turinys specialistai, kurie galėtų garantuoti kibernetinio saugumo užtikrinimo procesų tobulinimą visoje organizacijoje. Dabar perkamos išorės paslaugos galėtų atlikti priežiūros funkcijas ir taip sustiprinti esamą kontrolės valdymo sistemą. Nuolatinis vidaus audito specialistų darbas įmonės viduje užtikrintų nuolatinį procesų stebėjimą ir kontrolę, leistų savo įžvalgomis tobulinti vidaus audito atlikimą, jį integruoti į kuo daugiau organizacijos veiklos sričių.

4.4. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatų aptarimas ir diskusija

Tyrimo metu buvo siekiama atlikti kibernetinio saugumo vertinimo vidaus audito procedūrose teorinio modelio, sudaryto pagal analizuotą literatūrą, praktinį pritaikymą. Trijų skirtingo sektoriaus ir dydžių organizacijų atvejų studijos metodo analize buvo nustatytas kiekvienos organizacijos kibernetinio saugumo rizikos vertinimo ir vidaus audito procedūrų užtikrinimo lygis. Pagal gautus rezultatus pasiūlytos tobulinimo priemonės ar sritys, aktualios organizacijos kibernetinio saugumo rizikos ar vidaus audito procedūrų vertinimui. Organizacijų vertinimų rezultatų analizė parodė, kad organizacijos atitinka skirtingus konceptualaus teorinio modelio vertinimo lygius, todėl kibernetinio saugumo vertinimo vidaus audito procedūrose esamos organizacijų būklės rezultatų palyginimui reikalingi žemiau pateikiami apibendrinti kibernetinio saugumo rizikos vertinimo (19 pav.) ir vidaus audito procedūrų vertinimo (20 pav.) rezultatai.



19 pav. Kibernetinio saugumo rizikos vertinimo apibendrinamieji rezultatai (sudaryta autorės)

Tyrimo metu nustatyta, kad visos analizuotos organizacijos kibernetinio saugumo riziką vertina kaip vieną didžiausių pavojų verslo tęstinumo užtikrinimui, todėl skiria pakankamus išteklius grėsmių identifikavimo bei saugumo stebėsenos priemonėms, kad galėtų tinkamai ją nustatyti. Tinkamą

grėsmių vertinimo duomenų saugojimo infrastruktūrą turi A ir C įmonės, o B įmonė siekia užtikrinti visų informacinių sistemų saugą, todėl atskirai infrastruktūros vertinimo neatlieka. Šie vertinimai rodo, kad visos organizacijos turi pakankamai duomenų kibernetinio saugumo rizikos nustatymo ir grėsmės poveikio analizei atlikti, tačiau tai iki šiol atlieka tik B ir C įmonės.

Kibernetinio saugumo rizikos valdymo vertinimas visose įmonėse patvirtino, kad tinkamos valdymo struktūros ir reguliavimo politikos sukūrimas yra vienas pirmųjų darbų įmonėje, kuriuo siekiama sumažinti šios kibernetinio saugumo rizikos poveikį. A organizacijos visi valdymo procedūros kriterijai įvertinti aukščiausiais balais, tačiau, svarbu paminėti, kad vadovų požiūris ir įsitraukimas į kibernetinio saugumo rizikos suvaldymą vis dar yra neužtikrinimas vertintose B ir C įmonėse ir ši problema, nors ir sprendžiama, vis dar yra labai aktuali.

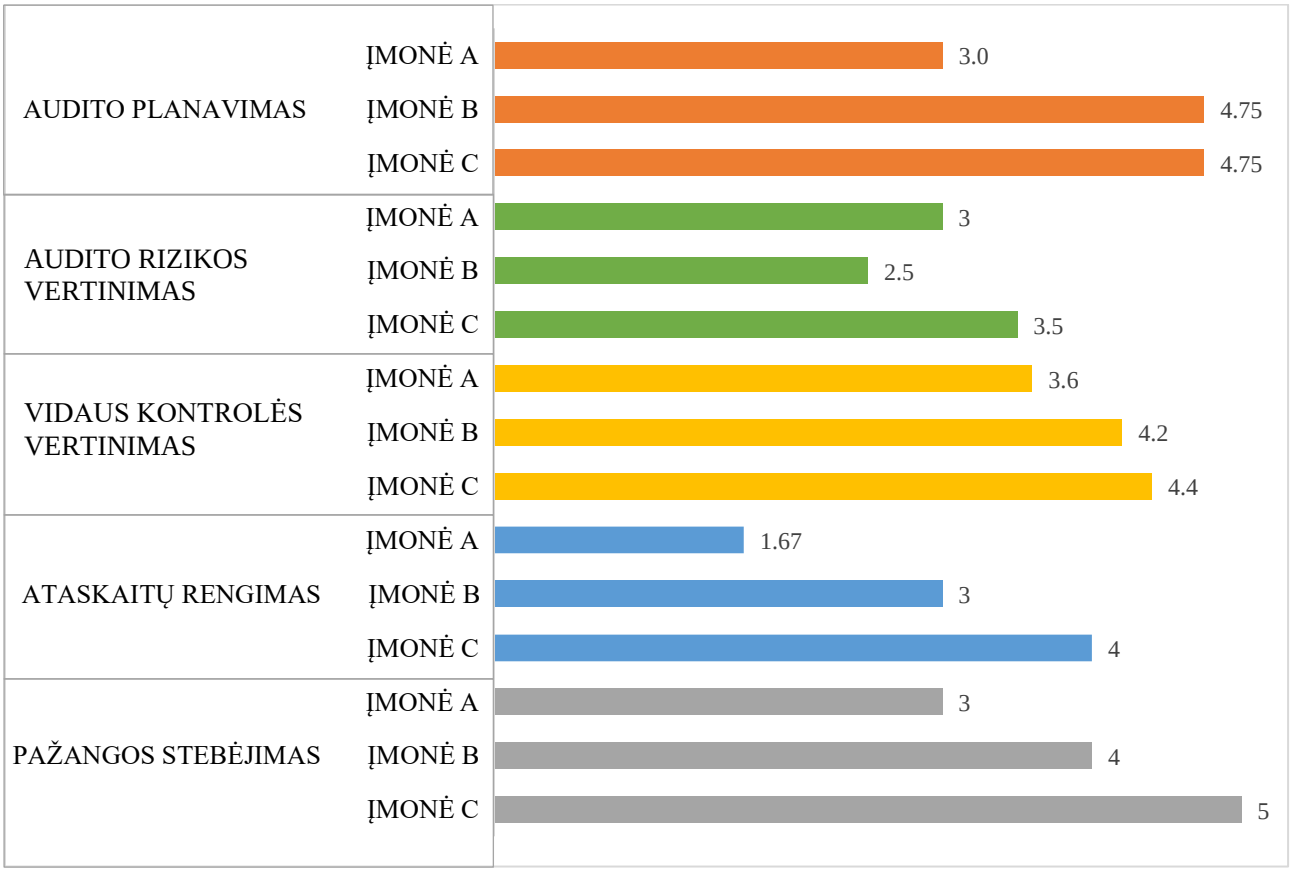
Pagal apibendrinamąjį vertinimą galima matyti, kad kibernetinio saugumo rizikos reagavimo procedūros A ir C įmonėse yra įvertinos mažiausiai, o tai lemia nepakankamą įmonių atsparumą kibernetinio saugumo rizikai. Nors rizikos analitika ir kontrolė yra integruota į visų organizacijų veiklos sistemas, o atsako planavimą užtikrina kibernetinio saugumo rizikos pratybos, atakų analitika ir duomenų atkūrimo užtikrinimas, tačiau šių priemonių nepakanka suformuoti tinkamą reakciją į rizikos grėsmę. Priežastinių ryšių nustatymo, tarp organizacijos veiklos funkcijų ir pasekmių, kurias gali turėti kibernetinio saugumo grėsmė, neužtikrina visos vertintos įmonės. Įmonė A taip pat turėtų įvertinti su „įsilaužėlių“ elgsenos modelių kūrimu susijusią naudą, nes visapusiškas grėsmės pažinimas užtikrina tinkamesnio reagavimo priemones.

Tyrimas patvirtino, kad kibernetinio saugumo užtikrinimo veiksniams organizacijos skiria didžiausią dėmesį, šie įvertinimai labai panašūs visose įmonėse. Tačiau svarbu tai, kad visose organizacijose trūksta kompetentingų kibernetinio saugumo specialistų, todėl įmonės susiduria su išorinių specialistų įdarbinimo problema. Ji atsiranda ne tik dėl specialistų trūkumo visoje rinkoje, tačiau ir mokslinėje literatūroje teigiamai vertinama tik tuo atžvilgiu, jei išorės kompetencijos yra papildoma kontrolės ir saugumo užtikrinimo priemonė. Pagrindinių, su saugumu susijusių, funkcijų atlikimui ir geresniam visos organizacijos verslo modelio supratimui yra naudingiau investuoti į vidaus specialistus. Su tuo glaudžiai susijęs nepakankamas mokymų kriterijaus vertinimas C įmonėje, kurioje užtikrinami tik bendriniai saugumo mokymai visiems darbuotojams. Kitų, A ir B įmonių atstovai patvirtino, kad darbuotojai šiandien yra išpuolikams patraukliausia ir kartu pažeidžiamiausia įmonės kibernetinė grėsmė, todėl investuoti į organizacijų darbuotojų įgūdžius yra būtina.

Empiriniame tyrime nustatyta, kad visų trijų tyrime dalyvavusių įmonių vidaus audito procedūros nėra visapusiškai užtikrinamos (20 pav.). Pagal atliktą tyrimą geriausiai įvertinta audito planavimo procedūra, kurią organizacijos užtikrina ilgalaikio plano sudarymu. Įvertindamos vidaus audito apimtis B ir C įmonės atsižvelgia į vidaus audito prioritetų ir pagrindinių rizikų (vertinant atskiras organizacijų sritis) nustatymą ir pagal jas sudaro būsimo audito planą. Įmonė A didžiausią dėmesį vidaus audito metu skiria procesų įvertinimui, darbų paskirstymui, todėl pagrindinės rizikos planavimo metu nėra nustatomos ir vidaus audito procedūrų apimtys nėra pagal tai vertinamos. Toks vadovų požiūris į vidaus auditą siejamas su kontrolės vertinimu ir neatspindi tikrųjų vidaus audito tikslų – stebėti organizacijos aplinką ir joje kylančias rizikas, laiku teikti įžvalgas apie jas, padėti jas tinkamai valdyti ir siekti kitų įmonės strateginių tikslų.

Tyrimo rezultatai rodo, kad audito rizikos vertinimo procedūroje visos įmonės susiduria su žmogiškųjų išteklių trūkumu, o tai tiesiogiai siejasi su vidaus audito kokybe ir patikimumu. Vertintas

resursų valdymas visose įmonėse yra užtikrinamas, tačiau atsižvelgiant į tai, kad vidaus audito specialistus reikia darbintis iš išorės, o joje vidaus audito specialistų trūksta, galima teigti, kad ilgainiui tinkamam resursų valdymui reikalingi ištekliai tik didės. Nors įmonė C įvertinta kaip turinti pakankamai darbuotojų vidaus audito procedūroms užtikrinti, tačiau darbuotojų darbo patirties ir kompetencijų trūkumas yra gaji visų įmonių problema.

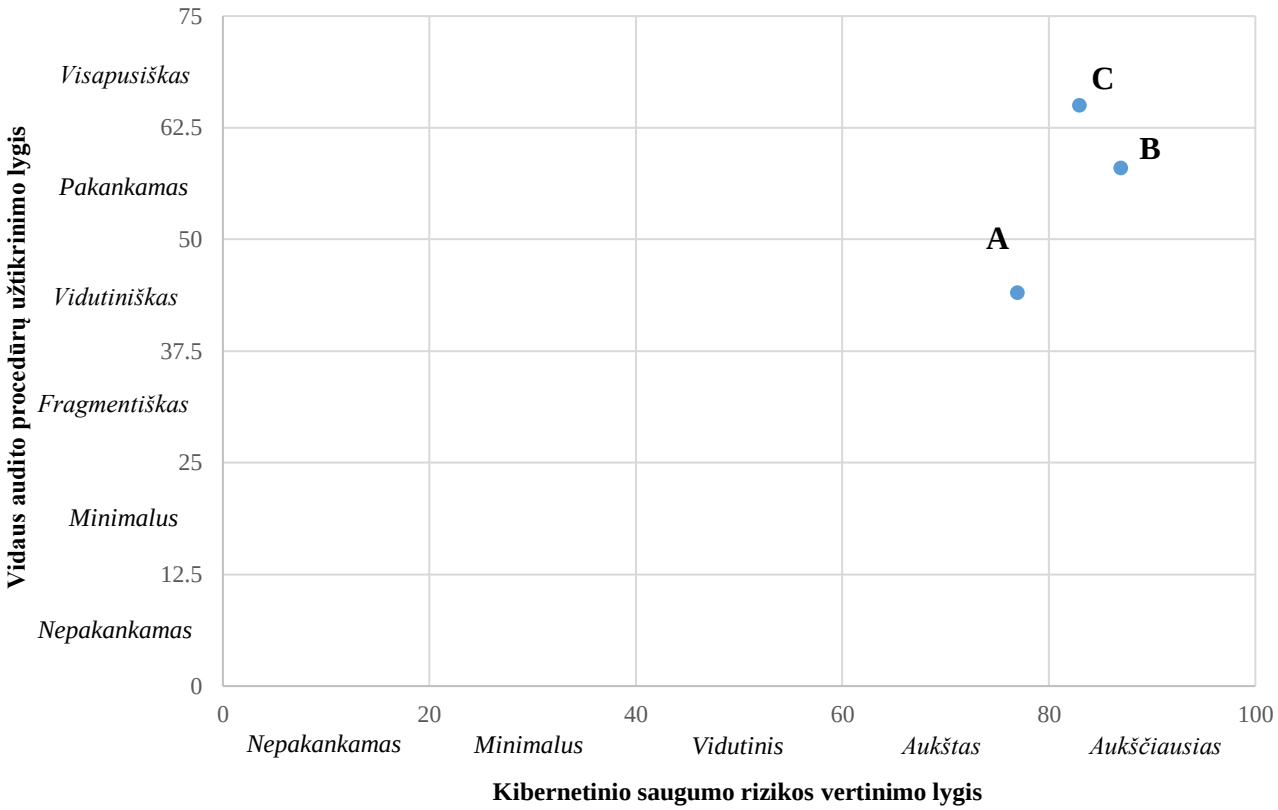


20 pav. Vidaus audito procedūrų vertinimo apibendrinamieji rezultatai (sudaryta autorės)

Pagal vidaus audito apibendrinamuosius rezultatus galima matyti, kad vidaus kontrolės vertinimą įmonės užtikrina nevienodai. Panašus vertinimo lygis būdingas B ir C įmonėms, jų vadovai užtikrina praėjusių auditų ir kitos susijusios informacijos perdavimą atsakingiems darbuotojams, taip pat rizikos vertinimą ir tinkamą kontrolės priemonių naudojimą. A įmonės vadovai nekuria grįžtamojo ryšio, susijusio su praeities vidaus kontrolės vertinimo sprendimais, todėl galima teigti, kad nors rizikos vertinimas atliekamas tinkamai, tačiau taikomos šiam vertinimui kontrolės priemonės ne visada yra pakankamos. Kontrolės aplinkos vertinimas grindžiamas etikos lygio organizacijoje išlaikymu, pagrindinių reguliavimo dokumentų atitikties vertinimu, kurių visos organizacijos turi dėl savo vykdomų veiklų rinkoje arba dėl poreikio vidaus politikoje.

Ataskaitų rengimo procedūros vertinimas parodė, kad tik C įmonė užtikrina tinkamą ataskaitų rengimo lygį. Įmonė B, nors ir vykdo atitikties testavimą, siekdama surasti bendrus vidaus kontrolės ir organizacijai kylančių rizikų veikimo taškus, tačiau gautų rezultatų neaptarinėja su įmonės vadovybe, o galutinę ataskaitą teikdama neužtikrina tinkamo jos detalumo lygio. A įmonė visos šios procedūros užtikrinimui skiria nepakankamas pastangas, todėl galutinėse vidaus audito išvadose gali būti neužtikrinamas ne tik detalumo, bet ir patikimumo principas. Su tuo glaudžiai susijęs ir pažangos stebėjimo vertinimas, kurio metu pateikiamų rekomendacijų išsamumas priklauso nuo galutinės

ataskaitos pateikimo. Poauditinės veiklos vertinimo metu vidaus auditorius gali įvertinti, ar įmonės vadovai atsižvelgė į gautas pastabas, ar ištaisė neatitikimus, o radus pasikartojančių neatitikimų - privalo supažindinti vadovus su jų prisiimama rizika, susijusia su pasyviu požiūriu į vidaus auditą.



21 pav. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo rezultatai (sudaryta autorės)

Empirinio tyrimo metu nustatytas vertinime dalyvavusių trijų organizacijų – A, B ir C – kibernetinio saugumo rizikos vertinimo ir vidaus audito procedūrų užtikrinimo lygis. Įmonės C ir B nustatytas kibernetinio saugumo rizikos vertinimo lygis yra aukščiausias, tačiau vidaus audito procedūrų užtikrinimo lygis B įmonėje yra pakankamas, o C įmonėje – visapusiškas. Pagal konceptualaus modelio atitikmenį, tai reiškia, kad C įmonės vidaus audito procedūrų metu galimas visapusiškas nežymios kibernetinio saugumo rizikos įvertinimas, o B įmonėje užtikrinamas pakankamas nežymios kibernetinio saugumo rizikos įvertinimas. B įmonė po šio vertinimo turėtų stiprinti vidaus audito procedūrų užtikrinimą ir tuomet galėtų pasižymėti aukščiausiu vertinimo lygiu. A įmonės vertinimas parodė, kad organizacija pasižymi aukštu kibernetinio saugumo rizikos vertinimo lygiu, o vidaus audito procedūros užtikrinamos vidutiniškai. Tai atitinka vidaus audito procedūrų metu galimą vidutinišką mažos kibernetinio saugumo rizikos įvertinimą. Siekiant pagerinti šį vertinimą organizacija A turėtų tobulinti ir kibernetinio saugumo rizikos vertinimą, ir vidaus audito procedūrų užtikrinimą.

Nustačius ir palyginus kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo lygį skirtingose organizacijose galima teigti, kad tyrimo rezultatai patvirtino teorinio konceptualaus modelio pritaikomumą praktikoje.

Tyrimo apribojimai. Šio empirinio tyrimo metu konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose modelis buvo praktiškai įvertintas tik trijose organizacijose, todėl nedidelė tyrime dalyvavusių organizacijų imtis mažina tyrimo validumą. Tyrime dalyvavusių organizacijų skaičių taip pat apribojo tai, kad vidaus auditas privalomas tik viešojo ir finansų sektoriaus organizacijoms, bei toms, kurių vertybiniais popieriais prekiaujama biržose, visose kitose – tai vadovų sprendimas. Platesnės vidaus audito funkcijos naudojimas ir pritaikymas organizacijoms strateginiams tikslams įmonėse taip pat yra tobulintina sritis. Tyrimo metu įmonių atstovai atsargiai dalinosi informacija apie kibernetinio saugumo ir vidaus audito procedūrų užtikrinimą savo atstovaujamose organizacijose, nes tai yra informacija, apribota organizacijų vidaus politikos reikalavimuose bei konfidencialumo sutartyse. Dėl šios priežasties dauguma organizacijų, kviestų dalyvauti tyrime – atsisakė.

Tolimesnės tyrimų kryptys ir perspektyvos. Kadangi tyrimo metu buvo vertintos tik trys Lietuvoje veiklą vykdančios vidutinės įmonės, tolimesniuose tyrimuose prasminga būtų vertinimą atlikti tiek mažose, tiek stambiose ar net valstybinėse įmonėse ir palyginti rezultatus tarp jų. Tikėtina, kad mažesnės įmonės skiria mažesnius išteklius kibernetinio saugumo rizikai valdyti, todėl šis organizacijos būklės vertinimas galėtų būti tinkamas paskatinimas įmonei atsižvelgti į kibernetinio saugumo rizikos keliamus pavojus. Atliekant atskirų sektorių vertinimus, taip pat būtų prasminga gauti išsamesnį organizacijų taikomų priemonių ir metodų sąrašą, o jis galėtų tapti visuotinėmis praktinėmis rekomendacijomis ir įmonių bendradarbiavimo pradžia, siekiant kartu išvengti kibernetinio saugumo rizikos pavojaus. Tolimesniems tyrimams, siekiant plačiau įvertinti modelio validumą, svarbu į vertinimą įtraukti daugiau įmonės darbuotojų, kurie ne tik tiesiogiai dirba su kibernetinio saugumo ar vidaus audito procedūrų užtikrinimu, bet ir darbuotojus, kurie atlieka vertinimo metu analizuojamas kasdienes operacijas. Įmonių vadovų, kaip sprendimų priėmėjų pozicijos atstovų vertinimas, taip pat padėtų gauti platesnių įžvalgų tolimesniame šio tyrimo vertinime. Bendradarbiaujant su kibernetinio saugumo ir vidaus audito specialistais ir ekspertais šį vertinimo modelį būtų galima praplėsti, tiksliau įvertinti ir dar labiau pritaikyti organizacijų kibernetinio saugumo rizikos būklei nustatyti.

Išvados

1. Atsižvelgus į kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo problematiką galima teigti, kad vidaus audito procedūrų užtikrinimas gali būti tinkamas įrankis kibernetinio saugumo rizikai organizacijoje nustatyti. Šis vertinimas gali padėti įmonių vadovams pasiekti organizacijos strateginius tikslus, įvertinus su jais susijusios kibernetinio saugumo rizikos poveikį, nustačius tinkamas, saugumą užtikrinančias priemones ir atliekant nuolatinę šių procesų stebėsenos kontrolę. Remiantis atlikta problematikos analize išskiriami šie, su kibernetinio saugumo rizikos vertinimu vidaus audito procedūrose, susiję iššūkiai:
   - Vidaus audito funkcija turi plačias kibernetinio saugumo rizikos vertinimui pritaikymo galimybes, tačiau organizacijų vadovams trūksta žinių ir visapusiško požiūrio į vidaus audito naudą, kurią gali suteikti tinkamas vadovų, kibernetinio saugumo specialistų ir vidaus auditorių bendradarbiavimas;
   - Svarbi organizacijų problema yra kompetentingų specialistų trūkumas ir neužtikrinama kvalifikacijos kėlimo bei nuolatinių mokymų sistema. Net turint tinkamą saugumo užtikrinimo infrastruktūrą, suformuotą reguliavimo politiką ar naujausias analitikai taikomas technologijas, saugumo rizikos nustatymui reikalingi specializuoti įmonės darbuotojai, todėl galima teigti, kad kibernetinio saugumo rizikos nustatymui vidaus audito procedūrose tik finansinių išteklių skyrimo nepakanka.

2. Pagal atliktą teorinę kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo literatūros analizę galima teigti, kad vidaus audito ir kibernetinio saugumo funkcijų bendradarbiavimas įmonėse gerina kibernetinio saugumo rizikos vertinimo lygį ir taip sumažina galimą neigiamą poveikį organizacijų verslo funkcijų tęstinumui. Atsižvelgiant į vidaus audito, kaip nepriklausomo vertintojo, galimybes ir naudą, kibernetinio saugumo rizikos vertinime, galima teigti, kad siūlomas konceptualus vertinimo modelis turi apimti tiek kibernetinio saugumo, tiek vidaus audito procedūrų vertinimą:
   - Kibernetinio saugumo rizika organizacijoje priklauso nuo tinkamo šios rizikos valdymo, taikomų prevencinių priemonių, technologinių sprendimų, atsako planavimo, turimų personalo kompetencijų ir mokymų, todėl organizacijų vadovybės turi skirti didelį dėmesį šios rizikos valdymui, vertinimui, stebėsenai ir kontrolei;
   - Vidaus auditas, kaip vidinės kontrolės dalis, kuriai būdingi nepriklausomumo ir objektyvumo pricipai gali užtikrinti tinkamą kibernetinio saugumo reikalavimų rizikos ir kontrolės valdymą. Auditorių atliktos analizės ir įžvalgos gali padėti pasiekti įmonei strateginius tikslus, optimizuoti taikomas saugumo priemones, užtikrinti efektyvesnius sprendimus kontrolės valdymui, laiku pastebėti rizikos indikatorius ir prisidėti prie saugumo sprendimų tobulinimo.

3. Pagal analizuotą mokslinę literatūrą parengta konceptualaus vertinimo modelio metodologija dėl savo išsamumo ir modelyje vertinamų procedūrų kriterijų detalumo vertinama kaip pakankama tam, kad empiriniame tyrime leistų nustatyti organizacijos kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo būklę:
   – Kibernetinio saugumo rizikos vertinimas apėmė rizikos nustatymo, valdymo, reagavimo į kibernetinę grėsmę ir saugumo užtikrinimo procesų vertinimą;
   – Vidaus audito vertinimas – audito planavimo, audito rizikos nustatymo ir vidaus kontrolės vertinimo, ataskaitų rengimo ir pažangos stebėsenos procedūrų užtikrinimą.

4. Remiantis atlikto tyrimo rezultatais galima teigti, kad pagal teorinę literatūros šaltinių analizę sudarytas konceptualus kibernetinio saugumo rizikos vidaus audito procedūrose modelis yra tinkamas praktiniam naudojimui, siekiant nustatyti organizacijų kibernetinio saugumo rizikos vertinimo galimybes vidaus audito procedūrose ir pasiūlyti šio vertinimo tobulinimo organizacijose galimybes:
   - Vertinimo modelio pagrindu įvertintas trijų organizacijų kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo lygis, kuris parodė, kad A įmonėje jis yra aukštas, o vidaus audito procedūrų užtikrinimo – vidutiniškas ir tuo remiantis galima teigti, kad įmonėje vidaus audito metu galima įvertinti mažai tikėtinos kibernetinės atakos tikimybę, turinčią mažą poveikį verslo funkcijų tęstinumui. Kitose – B ir C įmonėse nustatytas aukščiausias kibernetinio saugumo rizikos vertinimo lygis ir, atitinkamai, B įmonėje audito funkcijos užtikrinamos pakankamai, o C įmonėje – visapusiškai. Šiuo atžvilgiu vidaus audito procedūrose galima įvertini retos kibernetinės atakos tikimybę B įmonėje ir labai retos – C įmonėje, kurioms būdingas nežymus poveikis verslo funkcijoms;
   - Atliktas tyrimas taip pat leido įvertinti kiekvienos kibernetinio saugumo rizikos vertinimo ir vidaus audito procedūrų užtikrinimo procesus apibūdinančius kriterijus, todėl tai leido nustatyti problemines organizacijų sritis ir pateikti konkrečias procesų tobulinimo rekomendacijas vertintoms organizacijoms;
   - Vertinimo modelio galimybė palyginti vertinimo rezultatus su kitų organizacijų vertinimais gali užtikrinti bendradarbiavimo ir naudingosios patirties dalijimosi procesus, kurie ypač svarbūs tokiai neištirtai sričiai kaip kibernetinis saugumas ir tai leido numatyti tolimesnes tyrimo kryptis ir perspektyvas, kurios pateiktos empirinio tyrimo pabaigoje.

Literatūros sąrašas

1. Abdullatif, M., & Kawuq, S., (2015). The role of internal auditing risk management: evidence from banks in Jordan. *Journal of Economics and Administrative Sciences, 31*(1), 30–50. [žiūrėta 2020-12-29]. Prieiga per internetą: https://doi.org/10.1108/JEAS-08-2013-0025
2. ACCA (2019). Cyber and the CFO. *The Association of Chartered Certified Accountants* [žiūrėta 2020-03-27]. Prieiga per internetą: https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Cyber-cfo/pi-cyber-and-the-CFO.pdf
3. Accenture & Chartis Research (2016). The Convergence of Operational Risk and Cyber Security. [žiūrėta 2020-12-27]. Prieiga per internetą: https://www.accenture.com/t20170803T055319Z__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf
4. Ahia & Deloitte (2017). Cyber assurance: how internal audit, compliance and information technology can fight the good fight together. *Whitepaper, Guidance for Healthcare Internal Auditors and Compliance Professionals* [žiūrėta 2020-12-30]. Prieiga per internetą: http://www.ahia.org/assets/Uploads/pdfUpload/WhitePapers/CyberAssuranceWhitePaper.pdf
5. AICPA (2018). *Cybersecurity risk management reporting fact sheet*. [žiūrėta 2021-04-29]. Prieiga per internetą: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf
6. Alles, M., Kogan, A., Vasarhelyi, M., & Wu, J. (2005). Continuity Equations in Continuous Auditing: Detecting Anomalies in Buisness Processes. [žiūrėta 2021-01-16]. Prieiga per internetą: http://raw.rutgers.edu/docs/wcars/10wcars/CARutgersNov2005.pdf
7. Ames, B. C., Foster, F. R., Glynn, C., Lynn, M., Nakama, D., Penrose, T., & Rai S. (2016). *Assessing cybersecurity risk: roles of three lines of defence.* [žiūrėta 2021-05-13]. Prieiga per internetą: https://www.iia.nl/SiteFiles/vakpub/GTAG%20Assessing%20Cybersecurity%20Risk.pdf?cv=1
8. Amin, H. M. G., & Mohamed, E. K. A. (2016). Auditors‘ perceptions of the impact of continuous auditing on the quality of Internet reportes financial information in Egypt. *Managerial Auditing Journal, 31*(1), 111–132. doi: 10.1108/MAJ-01-2014-0989
9. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. doi: 10.1007/s11142-018-9452-4
10. Anderson, U. L., Head, M. J., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. J. (2017). *Internal Auditing: Assurance & Advisory Services* (4th ed.). Canada: Internal Audit Foundation.
11. Butler, R. J., & Lachow, I. (2012). Multilateral approaches for improving global security in cyberspace. *Georgetown Journal of International Affairs,* 5–14. . [žiūrėta 2021-04-16]. Prieiga per internetą: https://www.mitre.org/sites/default/files/pdf/12_3718.pdf
12. Caliyurt, K. T. (2020). Developing governance of procurement department in hospitals. In K. Caliyurt (Eds.), *Integrity, transparency and corruption in healthcare & research on health. Volume 1. Accounting, finance, sustainability, governance & fraud: theory and application*. Singapore: Springer.

13. Camillo, M. (2016). Cybersecurity: Risk and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions, 10*(2), 196–200 [žiūrėta 2021-05-08]. Prieiga per internetą: https://www-409.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf
14. Chan, D. Y., Chiu, V., & Vasarhelyi, M. A. (2018). *Continuous auditing: Theory and Application*. UK: Emerald Publishing Limited.
15. Cheong, A., Yoon, K., Cho, S., & No, W. G. (2020). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *The Journal of Information Systems*. doi: 10.2308/ISYS-2020-031
16. Chong, Y. Y. (2013). *Investment risk management.* England: John Wiley & Sons Ltd
17. Drogalas, G., Arampatzis, K., & Anagnostopoulou, E. (2016). The relationship between Corporate governance, internal audit and audit committee: empirical evidence from Greece. *Corporate Ownership and Control, 14*(1), 569–577. Prieiga per internetą: https://doi.org/10.22495/cocv14i1c4art3
18. Evans, M., Maglaras L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667–4679. doi: 10.1002/sec.1657
19. Fadzil, F. H., Haron, H., & Jantan, M. (2005). Internal auditing practices and internal control system. *Managerial Auditing Journal, 20*(8), 844–866. doi: 10.1108/02686900510619683
20. Galligan, M. E., Herrygers, S., & Rau, K. (2019). *Managing cyber risk in a digital age* [žiūrėta 2020-12-29]. Prieiga per internetą: https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf
21. Galligan, M. E., & Rau, K. (2015). *Coso in the cyber age* [žiūrėta 2020-12-28]. Prieiga per internetą: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-coso-in-the-cyber-age-final-01292015.pdf
22. Ghandge, A., Weiβ, M., Caldwell, N. D., & Wilding, R. (2018). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal, 25*(2), 223–240. doi: 10.1108/SCM-10-2018-0357
23. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015).The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy, 34*(5), 509–519. doi: 10.1016/j.jaccpubpol.2015.05.001
24. Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review, 17*(2), 215–241. doi: 10.1080/09638180701819972
25. Gramling, A., & Schneider, A. (2018). Effects of reporting relationship and type of internal control deficiency on internal auditors' internal control evaluations. *Managerial Auditing Journal, 33*(3), 318–335. doi: 10.1108/MAJ-07-2017-1606
26. Grody, A. D. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions, 13*(2), 155–162. [žiūrėta 2020-04-01]. Prieiga per internetą: https://web-b-ebscohost-com.ezproxy.ktu.edu/ehost/pdfviewer/pdfviewer?vid=9&sid=d6b7fe26-8262-4183-8bad-32bf0e1c2e00%40pdc-v-sessmgr02

27. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834. doi: 10.1108/MAJ-09-2018-2004
28. Houses of Parliament. (2011). *Cyber Security in the UK*. [žiūrėta 2021-01-23]. Prieiga per internetą: https://www.parliament.uk/globalassets/documents/post/postpn389_cyber-security-in-the-uk.pdf
29. Islam, M. S., Farah, N., & Stafford, T. S. (2018). Factors associated with security/cybersecurity audit by internal audit function: an international study. *Managerial Auditing Journal 33*(4), 377–409. doi: 10.1108/MAJ-07-2017-1595
30. Yin, R. (2009). *Case study research: Design and methods* (4th ed). Thousand Oaks, CA: Sage.
31. Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360–376. doi: 10.1108/MAJ-02-2018-1804
32. Kaloudi, N., & Jingyue, L. (2020). *The Al-Based Cyber Threat Landspace: A Survey* [žiūrėta 2020-04-04]. Prieiga per internetą: https://doi.org/10.1145/3372823
33. Kelic, A. (2018). Cyber Risk in Critical Infrastructure. *Performance Evaluation Review, 46*(2), 72–75. Prieiga per internetą: https://doi.org/10.1145/3305218.3305243
34. KPMG (2017). *Clarity on cyber security* [žiūrėta 2020-12-27]. Prieiga per internetą: https://assets.kpmg/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2017-en.pdf
35. Lainhart, J. W. (2000). Cobit™: a methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of information Systems, 14*(s-1), 21–25. doi: 10.2308/jis.2000.14.s-1.21
36. Lietuvos Respublikos krašto apsaugos ministerija. (2020). *Nacionalinė kibernetinio saugumo būklės ataskaita 2020* [žiūrėta 2021-04-13]. Prieiga per internetą: https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf
37. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Buisness, 15*(2), 205–217. doi: 10.1108/EMJB-07-2019-0097
38. Longley, A. (2019). Understanding and managing cyber security threats and countermeasures in the process industries. *Loss Prevention Bulletin*, 268, 2–6. [žiūrėta 2020-04-02]. Prieiga per internetą: https://web-b-ebscohost-com.ezproxy.ktu.edu/ehost/pdfviewer/pdfviewer?vid=9&sid=0872fb9e-1a36-47ec-bfdb-077987775b54%40pdc-v-sessmgr01
39. Moorthy, M. K., Mohamed, A. S. Z., Gopalan, M., & San, L. H. (2011). The impact of information technology in internal auditing. *African Journal of Business Management, 5*(9), 3523–3539. Prieiga per internetą: https://doi.org/10.5897/AJBM10.1047
40. Mutchler, J. F. (2003). Independence and objectivity: a framework for research opportunities in internal auditing. *The Institute of Internal Auditors, 7*, 231–268. [žiūrėta 2020-12-04]. Prieiga per internetą: https://global.theiia.org/iiarf/Public%20Documents/Chapter%207%20Independence%20and%20Objectivity%20A%20Framework%20for%20Research%20Opportunities%20in%20Internal%20Auditing.pdf
41. Nacionalinis kibernetinio saugumo centras (2020). *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas.* [žiūrėta 2021-04-01]. Prieiga per internetą: https://www.nksc.lt/naujienos/pristatytas_kibernetinio_saugumo_vadovas_smulkioms.html

42. No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and Continous Assurance. *Journal of Emerging Technologies in Accounting*, *14*(1), 1–12. doi: 10.2308/jeta-10539
43. Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis: An International Journal, 38*(2), 226–241. doi: 10.1111/risa.12844
44. Pathak, J. (2005). Risk management, internal controls and organizational vulnerabilities. *Managerial Auditing Journal 20*(6), 569–577. doi:10.1108/02686900510606065
45. Paukštienė, I. (2012) *Auditas. Vadovėlis.* Klaipėda: Viešoji įstaiga Socialinių mokslų kolegija.
46. Pute, D.V., & Verhelst, M. (2013). Cyber crime: Can a standart risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity & Emergency Planning*, *7*(2), 126–137 [žiūrėta 2020-04-02]. Prieiga per internetą: https://web-b-ebscohost-com.ezproxy.ktu.edu/ehost/pdfviewer/pdfviewer?vid=26&sid=baec8558-0226-46a7-bf8d-61bf2c5e978c%40pdc-v-sessmgr04
47. PWC (2017). Strengthening digital society against cyber shocks. *Key findings from The Global State of Information Security Survey* [žiūrėta 2020-12-02]. Prieiga per internetą: https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf
48. Renauld, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security, 78,* 198–211. doi: 10.1016/j.cose.2018.06.006
49. Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems, 20*, 26–37. doi: 10.1016/j.accinf.2016.01.003
50. Rios Insua, D., Couce-Vieira, A., & Musaraj, K. (2018). Some Risk Analysis Problems in Cyber Insurance Economics. *Estudios de Economia Aplicada*, *36*(1), 181–194 [žiūrėta 2020-04-03]. Prieiga per internetą: https://web-b-ebscohost-com.ezproxy.ktu.edu/ehost/pdfviewer/pdfviewer?vid=10&sid=baec8558-0226-46a7-bf8d-61bf2c5e978c%40pdc-v-sessmgr04
51. Rongping, M., & Yonggang, F. (2014). Security in cyber supply chain: a Chinese perspective. *Technovation 34*(7), 385–386. doi: 10.1016/j.technovation.2014.02.004
52. Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training information security policy compliance. *Managerial Auditing Journal 33*(4), 410–424. doi: 10.1108/MAJ-07-2017-1596
53. Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: an exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228–243. doi: 10.1016/j.accinf.2012.06.007
54. Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal if Information Systems, 27*(2), 65–86. doi: 10.2308/isys-50510
55. Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2015). The Influence of Internal Audit on Information System Effectiveness: Perceptions of Internal Auditors. [žiūrėta 2020-12-30]. Prieiga per internetą: https://doi.org/10.2139/ssrn.2685943

56. Vidaus auditorių institutas (2017). Tarptautiniai vidaus audito profesinės praktikos standartai. [žiūrėta 2020-12-03]. Prieiga per internetą: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Lithuanian.pdf
57. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. doi: 10.1016/j.cose.2013.04.004
58. Tellis, W. (1997). Appliccation of a Case Study Methodology. *The Qualitative Report, 3*(3), 1–19 [žiūrėta 2020-12-03]. Prieiga per internetą: https://nsuworks.nova.edu/tqr/vol3/iss3/1/?utm_source=nsuworks.nova.edu/tqr/vol3/iss3/1&utm_medium=PDF&utm_campaign=PDFCoverPages
59. The Institute of Internal Auditors. (2017). *Understanding and Auditing Bid Data* [žiūrėta 2020-12-27]. Prieiga per internetą: https://www.iia.nl/SiteFiles/Publicaties/GTAG-Understanding-and-Auditing-Big-Data.pdf
60. Toapanta, S. M. T., Peralta, N. A., & Gallegos, L. E. M. (2019). Definition of parameters to perform audit in cybersecurity for public one organization of Ecuador. *ICETM 2019: In Proceedings of the 2019 2nd International Conference on Education Technology Management* (pp. 91–96). Nex York: Association for Computing Machinery.
61. Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information Security and Sorbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems, 25*(1), 185–211. doi: 10.2308/jis.2011.25.1.185
62. Werlinger, R., Mulder, K., Hawkey, K., & Beznosov, K. (2009). Towards Understanding Diagnostic Work During the Detection and Investigation of Security Incidents. *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 119–132 [žiūrėta 2020-03-25]. Prieiga per internetą: http://lersse-dl.ece.ubc.ca/record/208/files/208.pdf
63. Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th ed). Mason: Centgage Learning.
64. Woodroof, J., & Searcy, D. (2001). Continuous audit: model development and implementation within a debt covenant compliance domain. *International Journal of Accounting Information Systems*, *2*(3), 169–191. doi: 10.1016/S1467-0895(01)00019-7

Priedai

1 priedas. Kibernetinio saugumo rizikos vidaus audito procedūrose vertinimo klausimynas ir vertinimo kriterijų įverčių reikšmės

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	**NUSTATYMAS**	Grėsmių identifikavimas	*Ištekliai*	Ar organizacija turi pakankamai išteklių, kurie leistų nustatyti organizacijai kylančias rizikas, susijusias su kibernetinėmis grėsmėmis?	Kiek vidutiniškai identifikuotų grėsmių yra pasitvirtinę ar pareikalavę kito, detalesnio grėsmės patikrinimo?	1 - grėsmių identifikavimui nėra pakankamai išteklių; 2 - grėsmių identifikavimas yra ribotas; 3 - grėsmių identifikavimas yra vidutinis; 4 - grėsmių identifikavimui ištekliai yra pakankami; 5 - grėsmių identifikavimui naudojami visapusiški ištekliai
		Infrastruktūros vertinimas	*Infrastruktūra*	Ar organizacija turi tinkamą infrastruktūrą, kuri leistų rinkti duomenis ir nustatyti kibernetinės grėsmės pavojų?	Kas sudaro vertinamos infrastruktūros pagrindą (pagrindinių organizacijos duomenys, IT turto vertinimas, kritinės infrastruktūros nustatymas)?	1 - infrastruktūra netinkama duomenų saugojimui ir kibernetinės grėsmės nustatymui; 2 - infrastruktūra iš dalies tinkama duomenų saugojimui; 3 - infrastruktūros vertinimas apima tik pagrindinių organizacijos duomenų vertinimą; 4 - infrastruktūros vertinimas apima pagrindinių organizacijos duomenų ir IT turto vertinimą; 5 - infrastruktūra tinkama, vertinimas apima pagrindinių organizacijos duomenų, IT turto vertinimą ir kritinės infrastruktūros įvertinimą
		Poveikio analizė	*Poveikis*	Ar ir kaip dažnai organizacijoje yra atliekama poveikio analizė, susijusi su kibernetinio saugumo grėsmės rizika?	Ar organizacija turi numačiusi, sau nusistačiusi poveikio ribą, nuo kurios pradedama imtis tam tikrų saugumo veiksmų? Kas yra ta riba?	1 - organizacijoje poveikio analizė neatliekama niekada; 2 - organizacijoje poveikio analizė dažniausiai neatliekama; 3 - organizacijoje poveikio analizė atliekama tam tikrais atvejais; 4 - organizacijoje poveikio analizė atliekama dažniausiai; 5 - organizacijoje poveikio analizė atliekama nuolat
		Saugumo informacijos stebėsena	*Saugumo priemonės*	Ar organizacijoje yra atliekama saugumo informacijos stebėsena?	Kokiomis priemonėmis yra atliekama saugumo informacijos stebėsena organizacijoje? (atliekami įsiskverbimo į sistemą bandymai, pildomi saugos žurnalai, metrikos, ataskaitos)?	1 - organizacijoje saugumo informacijos stebėsena nėra atliekama; 2 - organizacijoje saugumo informacijos stebėsena yra ribota; 3 - organizacijoje saugumo informacijos stebėsena yra vidutiniška; 4 - organizacijoje saugumo informacijos stebėsena yra pakankama; 5 - organizacijoje saugumo informacijos stebėsena yra visapusiška: atliekami įsiskverbimo į sistemą bandymai, pildomi saugos žurnalai, teikiamos ataskaitos

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	**VALDYMAS**	Valdymo modelis ir struktūra	*Struktūra*	Ar organizacijoje yra numatyta aiški kibernetinio saugumo valdymo struktūra, su jai reikalingais specialistais ir atsakomybėmis?	Koks dėmesys organizacijos valdymo sprendimuose yra skiriamas kibernetinės rizikos valdymo analizei? Kurio valdymo lygio atstovai dalyvauja priimant sprendimus, susijusius su šia rizika?	1 - organizacijos valdymo struktūroje nėra skiriamas dėmesys kibernetinės rizikos valdymo analizei; 2 - organizacijos valdymo struktūroje nėra skiriamas dėmesys kibernetinės rizikos valdymo analizei, tačiau planuojama tai daryti ateityje; 3 - organizacijos valdymo struktūroje skiriamas mažas dėmesys kibernetinės rizikos valdymo analizei; 4 - organizacijos valdymo struktūroje vidutinis dėmesys kibernetinės rizikos valdymo analizei; 5 - organizacijos valdymo struktūroje skiriamas didelis dėmesys kibernetinės rizikos valdymo analizei
		Vadovybės įtaka	*Požiūris*	Ar organizacijoje vadovybė sieja valdymo sprendimus su kibernetinės grėsmės rizika?	Koks yra Jūsų organizacijos vadovų požiūris į kibernetinės grėsmės riziką ir jos suvaldymą priimant valdymo sprendimus?	1 - organizacijos vadovybė valdymo sprendimų nesieja su kibernetinės grėsmės rizika; 2 - organizacijos vadovybė valdymo sprendimų nesieja su kibernetinės grėsmės rizika, tačiau planuoja tai daryti ateityje; 3 - organizacijos vadovybė skatina iniciatyvas, kuriose valdymo sprendimai priimami atsižvelgiant į kibernetinės grėsmės riziką; 4 - organizacijos vadovybė skatina ir patys kuria iniciatyvas, kuriose valdymo sprendimai priimami atsižvelgiant į kibernetinės grėsmės riziką; 5 - organizacijos vadovybė visus valdymo sprendimus priima ir įpareigoja organizacijos darbuotojus valdymo sprendimus priimti atsižvelgiant į kibernetinės grėsmės riziką
		Reguliavimo ir teisinė aplinka	*Politika*	Ar organizacijoje yra patvirtinta kibernetinio saugumo rizikos reguliavimo ir teisinė politika, kuri pritaikoma visiems įmonės procesams?	Jei taip, kokiais dokumentais vadovaujantis ji yra parengta?	1 - organizacijoje nėra patvirtintos kibernetinio saugumo rizikos reguliavimo ir teisinės politikos; 2 - organizacijoje nėra patvirtintos kibernetinio saugumo rizikos reguliavimo ir teisinės politikos, planuojama ją sukurti ateityje; 3 - organizacijoje nėra patvirtintos kibernetinio saugumo rizikos reguliavimo ir teisinės politikos, ji kuriama šiuo metu; 4 - organizacijoje yra patvirtintos kibernetinio saugumo rizikos reguliavimo ir teisinės politikos atskiruose padaliniuose; 5 - organizacijoje yra patvirtintos kibernetinio saugumo rizikos reguliavimo ir teisinės politikos visoje organizacijoje

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	**REAGAVIMAS**	Kibernetinės rizikos analitika	*Analizė ir kontrolė*	Ar organizacijoje yra vykdoma kibernetinės rizikos analitika?	Ar ši analitika yra integruota į veiklos kontrolės sistemas, siekiant padidinti kibernetinio saugumo atsparumą organizacijos procesuose? Ar analizuojamos su kibernetine rizika susiję aktualijos?	1 - organizacijoje nėra vykdoma kibernetinės rizikos analitika; 2 - organizacijoje yra vykdoma kibernetinės rizikos analitika, tačiau ji nėra integruota į veiklos kontrolės sistemas; 3 - organizacijoje yra vykdoma kibernetinės rizikos analitika, ji integruota į tam tikrų veiklų kontrolės sistemas; 4 - organizacijoje yra vykdoma kibernetinės rizikos analitika, ji integruota į daugumos veiklų kontrolės sistemas; 5 - organizacijoje yra vykdoma kibernetinės rizikos analitika, ji integruota į visų veiklų kontrolės sistemas
		Prognozės	*Elgsena*	Ar organizacija savo sistemoje turi duomenų, kurių pagrindu galėtų prognozuoti kibernetinės grėsmės „taikinius“?	Ar remiantis šiais duomenimis yra prognozuojama tolimesnė įsilaužėlių elgsena? Ar yra vertinamos atskiros tikslinės grupės (darbuotojai, klientai, trečiosios šalys)?	1 - organizacija neturi duomenų, kurių pagrindu galėtų prognozuoti kibernetinės grėsmės "taikinius" ir prognozuoti tolimesnę elgseną; 2 - organizacija neturi duomenų, kurių pagrindu galėtų prognozuoti kibernetinės grėsmės "taikinius" ir prognozuoti tolimesnę elgseną, tačiau planuoja tai daryti ateityje; 3 - organizacija turi duomenų, kurių pagrindu galėtų prognozuoti kibernetinės grėsmės "taikinius", tačiau tolimesnė tikslinių grupių elgsena nėra prognozuojama; 4 - organizacija turi duomenų, kurių pagrindu tam tikrais atvejais prognozuoja kibernetinės grėsmės "taikinius" ir tolimesnę tikslinių grupių elgseną; 5 - organizacija turi duomenų, kurių pagrindu visais atvejais prognozuoja kibernetinės grėsmės "taikinius" ir tolimesnę tikslinių grupių elgseną
		Priežastys	*Priežastiniai ryšiai*	Ar organizacija gali įvertinus duomenis iš visų organizacijos sričių nustatyti priežastinius ryšius tarp atliekamų organizacijos veiksmų ir pasekmių, susijusių su kibernetinio saugumo rizika?	Kaip priežastinių ryšių nustatymas lemia tolimesnę veiksmų ir sprendimų, susijusių su kibernetine rizika, eigą? Kaip dažnai tenka keisti veiksmų ar sprendimų eigą, susijusią su kibernetinio saugumo rizika, nustačius tam tikrus priežastinius ryšius?	1 - organizacija negali nustatyti priežastinių ryšių tarp atliekamų organizacijos veiksmų ir pasekmių; 2 - organizacija negali nustatyti priežastinių ryšių tarp atliekamų organizacijos veiksmų ir pasekmių, tačiau norėtų tai daryti ateityje; 3 - organizacija nustatinėja priežastinius ryšius tarp veiksmų ir pasekmių, susijusių su kibernetinio saugumo rizika, tačiau jie nelemia tolimesnių sprendimų priėmimo; 4 - organizacija dažnai nustatinėja priežastinius ryšius tarp veiksmų ir pasekmių, susijusių su kibernetinio saugumo rizika ir jie dažnai lemia tolimesnių sprendimų priėmimą; 5 - organizacija nuolat nustatinėja priežastinius ryšius tarp veiksmų ir pasekmių, susijusių su kibernetinio saugumo rizika ir jie lemia tolimesnių sprendimų priėmimą

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	**REAGAVIMAS**	Atsako planavimas	*Sprendimų modeliai*	Ar organizacijoje yra modeliuojami skirtingi galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai?	Kokie yra numatyti, galimi grėsmės ištaisymo mechanizmai (duomenų atkūrimas, kompensacijos, pagalba)? Ar yra sudarytas incidentų valdymo planas?	1 - organizacijoje nėra modeliuojami galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai; 2 - organizacijoje nėra modeliuojami galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai, planuojama tai daryti ateityje; 3 - organizacijoje tam tikrais atvejais yra modeliuojami galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai; 4 - organizacijoje yra modeliuojami galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai, tačiau nėra numatyti grėsmės ištaisymo mechanizmai; 5 - organizacijoje yra modeliuojami galimi atsako į kibernetinę grėsmę sprendimų modeliai ir rezultatai, yra numatyti grėsmės ištaisymo mechanizmai
	UŽTIKRINIMAS	Saugumo programų valdymas	*Reglamentavimas*	Ar organizacijoje yra vykdomos kibernetinio saugumo programos, t. y., ar yra numatytos strategijos, standartai, gairės visos organizacijos ar atskirų padalinių apsaugai?	Ar šios kibernetinio saugumo programos dalyvauja biudžeto ir turto bei su jais susijusių pokyčių sprendimų valdyme?	1 - organizacijoje nėra vykdomos kibernetinio saugumo programos; 2 - organizacijoje nėra vykdomos kibernetinio saugumo programos, tačiau planuojamos vykdyti ateityje; 3 - organizacijoje yra vykdomos kibernetinio saugumo programos, tačiau jos nedalyvauja biudžeto ir turto bei su jais susijusių pokyčių sprendimų valdyme; 4 - organizacijoje yra vykdomos kibernetinio saugumo programos tam tikruose padaliniuose ir jos dalyvauja biudžeto ir turto bei su jais susijusių pokyčių sprendimų valdyme; 5 - organizacijoje yra vykdomos kibernetinio saugumo programos visos organizacijos mastu ir jos dalyvauja biudžeto ir turto bei su jais susijusių pokyčių sprendimų valdyme
		Duomenų apsauga	*Duomenys*	Ar visoje organizacijoje ar jos padaliniuose yra vykdoma duomenų apsaugos strategija, t.y. ar yra tinkamai klasifikuojami, tikrinami ir vėliau saugomi gautini duomenys?	Kokiomis priemonėmis yra atliekama duomenų praradimo prevencija?	1 - organizacijoje nėra vykdoma duomenų apsaugos strategija; 2 - organizacijoje nėra vykdoma duomenų apsaugos strategija, tačiau planuojama turėti ateityje; 3 - organizacijoje yra vykdoma duomenų apsaugos strategija tam tikruose padaliniuose, tačiau duomenų praradimo prevencija nėra atliekama; 4 - organizacijoje yra vykdoma duomenų apsaugos strategija visos organizacijos mastu, tačiau duomenų praradimo prevencija nėra atliekama; 5 - organizacijoje yra vykdoma duomenų apsaugos strategija visos organizacijos mastu, taip pat atliekama duomenų praradimo prevencija

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	**UŽTIKRINIMAS**	Tapatybės ir prieigos valdymas	*Prieiga*	Ar organizacijoje yra tinkamas tapatybės nustatymo ir sistemos prieigų valdymas?	Kokiomis priemonėmis pasiekiamas tinkamas tapatybės nustatymo ir sistemos prieigų valdymas (identifikavimu, sertifikavimu, kitomis priemonėmis)?	1 - organizacijoje nėra tinkamas tapatybės nustatymo ir sistemos prieigų valdymas; 2 - organizacijoje yra žemas tapatybės nustatymo ir sistemos prieigų valdymo lygis, naudojama 1 priemonė tam pasiekti; 3 - organizacijoje yra vidutinis tapatybės nustatymo ir sistemos prieigų valdymo lygis, naudojama daugiau nei 1 skirtinga priemonė tam pasiekti; 4 - organizacijoje yra aukštas tapatybės nustatymo ir sistemos prieigų valdymo lygis, naudojamos daugiau nei 2 skirtingos priemonės tam pasiekti; 5 - organizacijoje yra labai aukštas tapatybės nustatymo ir sistemos prieigų valdymo lygis, naudojamos daugiau nei 3 skirtingos priemonės tam pasiekti
		Tinklo ir infrastruktūros apsauga	*Tinklas ir infrastruktūra*	Ar organizacijoje yra atliekamas tinkamas tinklo ir infrastruktūros apsaugos valdymas?	Kokie reikalavimai organizacijoje yra keliami tinklo ir infrastruktūros apsaugai? Ar pritariate, kad prie infrastruktūros apsaugos gerinimo prisideda bendra tinklo apsauga ir išorinių pranešimų apie atakas stebėjimas?	1 - organizacijoje nėra tinkamas tinklo ir infrastruktūros apsaugos valdymas; 2 - organizacijoje yra žemas tinklo ir infrastruktūros apsaugos valdymo lygis; 3 - organizacijoje yra vidutinis tinklo ir infrastruktūros apsaugos valdymo lygis; 4 - organizacijoje yra aukštas tinklo ir infrastruktūros apsaugos valdymo lygis; 5 - organizacijoje yra labai aukštas tinklo ir infrastruktūros apsaugos valdymo lygis
		Programinė įrangos apsauga	*Programinė įranga*	Ar organizacijoje yra atliekamas tinkamas programinės įrangos apsaugos valdymas?	Kokie reikalavimai organizacijoje yra keliami programinės įrangos apsaugai (numatytos saugumo kodavimo gairės, programų nuolatinis testavimas)?	1 - organizacijoje nėra tinkamas programinės įrangos apsaugos valdymas; 2 - organizacijoje yra žemas programinės įrangos apsaugos valdymo lygis; 3 - organizacijoje yra vidutinis programinės įrangos apsaugos valdymo lygis; 4 - organizacijoje yra aukštas programinės įrangos apsaugos valdymo lygis; 5 - organizacijoje yra labai aukštas programinės įrangos apsaugos valdymo lygis

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS	UŽTIKRINIMAS	Trečiųjų šalių valdymas	*Vertinimas ir atranka*	Ar organizacijoje yra atliekamas trečiųjų šalių valdymo vertinimas ir atranka?	Kokiais būdais yra atliekamas trečiųjų šalių vertinimas ir atranka? Ar vyrauja sutarčių pasirašymas, o po jų atliekamas nuolatinis trečiųjų šalių stebėjimas (ir sutarčių nutraukimas pažeidus susitarimo sąlygas)?	1 - organizacijoje nėra atliekami trečiųjų šalių valdymo vertinimas ir atranka; 2 - organizacijoje yra žemas trečiųjų šalių vertinimo ir atrankos lygis; 3 - organizacijoje yra vidutinis trečiųjų šalių vertinimo ir atrankos lygis, stebėjimas atliekamas retai; 4 - organizacijoje yra aukštas trečiųjų šalių vertinimo ir atrankos lygis, atliekamas dažnas stebėjimas; 5 - organizacijoje yra labai aukštas trečiųjų šalių vertinimo ir atrankos lygis, atliekamas nuolatinis stebėjimas
		Debesijos valdymas	*Debesijos saugyklos*	Ar organizacijoje yra atliekamas tinkamas debesijos apsaugos valdymas?	Kokie kriterijai lemia debesijos saugyklų, skirtų organizacijos veiklai, pasirinkimą? Ar yra identifikuota debesijos rizika su minimalia kontrolės saugumo riba, atitikties reikalavimais?	1 - organizacijoje nėra atliekamas tinkamas debesijos apsaugos valdymas; 2 - organizacijoje yra žemas debesijos apsaugos valdymo lygis; 3 - organizacijoje yra vidutinis debesijos apsaugos valdymo lygis; 4 - organizacijoje yra aukštas debesijos apsaugos valdymo lygis; 5 - organizacijoje yra labai aukštas debesijos apsaugos valdymo lygis
		Žmogiškųjų išteklių strategija	*Darbuotojų kompetencijos*	Kokius kibernetinio saugumo įgūdžius (kompetencijas) turi organizacijoje dirbantys specialistai?		1 - organizacija neturi kibernetinio saugumo specialistų; 2 - organizacijos specialistai turi specifinius kibernetinio saugumo įgūdžius, skirtus įvykdyti tam tikras užduotis; 3 - organizacijos specialistai turi pakankamus kibernetinio saugumo įgūdžius, skirtus įvykdyti savo darbo funkcijas; 4 - organizacijos specialistai turi aukštus kibernetinio saugumo įgūdžius, jie prisideda prie savo padalinio (veiklos, darbo) kibernetinio saugumo užtikrinimo procesų tobulinimo; 5 - organizacijos specialistai turi labai aukštus kibernetinio saugumo įgūdžius, jie prisideda prie visos organizacijos kibernetinio saugumo užtikrinimo procesų tobulinimo
			Personalo mokymai	Ar organizacijoje yra rengiami kibernetinio saugumo mokymai, sukčiavimo simuliacijos pratybos, kiti personalo apmokymai?		1 - organizacijoje nėra rengiami kibernetinio saugumo mokymai; 2 - organizacijoje yra rengiami kibernetinio saugumo mokymai tik keletui darbuotojų; 3 - organizacijoje yra rengiami bendriniai kibernetinio saugumo mokymai; 4 - organizacijoje yra rengiami kibernetinio saugumo mokymai, pagal nuolat vertinamą kibernetinio saugumo specialistų lygį; 5 - organizacijoje yra nuolat rengiami specializuoti kibernetinio saugumo mokymai visos organizacijos mastu

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai *(nustatyti, ar kriterijus aktualus organizacijos veikloje)*	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
VIDAUS AUDITO PROCEDŪRŲ UŽTIKRINIMO VERTINIMAS	**AUDITO PLANAVIMAS**	Ilgalaikis planavimas	*Audito strategija*	Ar organizacija atlieka ilgalaikį (metinį ar kelių metų) audito planavimą?	Ar planavimo metu yra sudaromas ilgalaikės audito veiklos biudžetas, paskirstomi ištekliai, atnaujinami ilgalaikiai planai?	1 - organizacijoje nėra atliekamas ilgalaikis audito planavimas; 2 - organizacijoje nėra atliekamas ilgalaikis audito planavimas, tačiau planuojama tai daryti ateityje; 3 - organizacijoje audito planavimas atliekamas pagal poreikį; 4 - organizacijoje kiekvienais metais atliekamas metinis audito planavimas, kurio metu sudaromas audito veiklos biudžetas, paskirstomi ištekliai, tačiau ilgamečio plano organizacija neturi; 4 - organizacijoje kiekvienais metais atliekamas metinis audito planavimas, kurio metu sudaromas audito veiklos biudžetas, paskirstomi ištekliai, tačiau ilgamečio plano organizacija neturi
		Apimties planavimas	*Procedūros*	Ar galite teigti, kad planuodama audito apimtis organizacija orientuojasi į vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymą?	Kiek kibernetinės rizikos nustatymas vidaus audite padidina vidaus audito apimtis?	1 - organizacija planuodama audito apimtis nesiorientuoja į vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymą; 2 - organizacija planuodama audito apimtis vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymui skiria ribotą dėmesį; 3 - organizacija, planuodama audito apimtis vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymui skiria pakankamą dėmesį; 4 - organizacija planuodama audito apimtis vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymui skiria didelį dėmesį; 5 - organizacija planuodama audito apimtis vidaus audito subjektų prioritetų ir pagrindinių rizikų, susijusių su kibernetine rizika, nustatymui skiria didžiausią dėmesį
		Vidaus audito plano sudarymas	*Audito požiūris*	Ar galite teigti, kad sudarydama vidaus audito planą organizacija remiasi visos organizacijos rizikos vertinimu?	Kuriuose planavimo etapuose skiriamas didžiausias dėmesys rizikos vertinimui (atsakingų padalinių, procesų darbų paskirstymui, žmogiškųjų ir finansinių išteklių įvertinimui)?	1 - organizacija sudarydama vidaus audito planą neskiria dėmesio visos organizacijos rizikos vertinimui; 2 - organizacija sudarydama vidaus audito planą skiria ribotą dėmesį visos organizacijos rizikos vertinimui; 3 - organizacija sudarydama vidaus audito planą skiria pakankamą dėmesį visos organizacijos rizikos vertinimui; 4 - organizacija sudarydama vidaus audito planą skiria didelį dėmesį visos organizacijos rizikos vertinimui; 5 - organizacija sudarydama vidaus audito planą skiria didžiausią dėmesį visos organizacijos rizikos vertinimui

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai (nustatyti, ar kriterijus aktualus organizacijos veikloje)	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
VIDAUS AUDITO PROCEDŪRŲ UŽTIKRINIMO VERTINIMAS	**AUDITO PLANAVIMAS**	Patvirtinimas	*Vadovų įsitraukimas*	Ar organizacijos vadovai ar kiti atsakingi asmenys yra supažindinami su vidaus audito planu ir yra reikalingas jų patvirtinimas?	Kokie organizacijoje keliami reikalavimai vidaus audito ištekliams ir jų apribojimų padariniams? Ar yra nustatytas bendradarbiavimas, apimantis visus valdymo lygius?	1 - organizacijos vadovai nėra supažindinami su vidaus audito planu, nėra reikalingas jų patvirtinimas; 2 - organizacijos vadovai supažindinami su vidaus audito planu, tačiau nėra reikalingas jų patvirtinimas; 3 - organizacijoje yra būtinas vadovų vidaus audito plano patvirtinimas, tačiau vidaus audito ištekliams ir bendradarbiavimui tarp visų valdymo lygių reikalavimų nėra; 4 - organizacijoje yra būtinas vadovų vidaus audito plano patvirtinimas, keliami aukšti vidaus audito išteklių ir bendradarbiavimo tarp visų valdymo lygių reikalavimai; 5 - organizacijoje yra būtinas vadovų vidaus audito plano patvirtinimas, keliami aukščiausi vidaus audito išteklių ir bendradarbiavimo tarp visų valdymo lygių reikalavimai
	AUDITO RIZIKOS VERTINIMAS	Žmogiškųjų išteklių strategija	*Kompetencijos*	Ar organizacija turi pakankamai reikalingų specialistų vidaus audito procedūroms užtikrinti (kalbant apie planavimą, rizikos ir vidaus kontrolės vertinimui, ataskaitų rengimui)?	Kokius vidaus audito įgūdžius (kvalifikaciją) turi organizacijoje dirbantys specialistai? Kokia jų hierarchija organizacijos viduje? Ar organizacijoje įdarbinami specialistai iš išorės dalykinėms kompetencijoms vertinti?	1 - organizacija neturi pakankamai specialistų vidaus audito procedūroms užtikrinti; 2 - organizacijos specialistai turi specifinius vidaus audito procedūrų užtikrinimo įgūdžius, skirtus įvykdyti tam tikras užduotis; 3 - organizacijos specialistai turi pakankamus vidaus audito procedūrų užtikrinimo įgūdžius, skirtus įvykdyti savo darbo funkcijas; 4 - organizacijos specialistai turi aukštus vidaus audito procedūrų užtikrinimo įgūdžius, jie prisideda prie savo padalinio (veiklos, darbo) procesų tobulinimo; 5 - organizacijos specialistai turi labai aukštus vidaus audito procedūrų užtikrinimo įgūdžius, jie prisideda prie visos organizacijos veiklos procesų tobulinimo
		Resursų valdymas	*Resursai*	Ar galite teigti, kad organizacijoje resursai, skirti vidaus audito rizikos vertinimui, valdomi tinkamai?	Kokios priemonės organizacijoje yra taikomos resursų valdymui (sudaromos darbo grupės, vykdomos tobulinimosi programos)? Ar atliekamos užsakomosios paslaugos iš išorės? Kas organizacijoje atsakingas už tinkamą resursų valdymą?	1 - organizacijoje resursai valdomi netinkamai; 2 - organizacijoje yra žemas resursų, skirtų vidaus audito rizikos vertinimui, valdymo lygis, naudojama 1 priemonė; 3 - organizacijoje yra vidutinis resursų, skirtų vidaus audito rizikos vertinimui, valdymo lygis, naudojama daugiau nei 1 skirtinga priemonė; 4 - organizacijoje yra aukštas resursų, skirtų vidaus audito rizikos vertinimui, valdymo lygis, naudojamos daugiau nei 2 skirtingos priemonės; 5 - organizacijoje yra labai aukštas resursų, skirtų vidaus audito rizikos vertinimui, valdymo lygis, naudojamos daugiau nei 3 skirtingos priemonės tam pasiekti

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai (nustatyti, ar kriterijus aktualus organizacijos veikloje)	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
VIDAUS AUDITO PROCEDŪRŲ UŽTIKRINIMO VERTINIMAS	**VIDAUS KONTROLĖS VERTINIMAS**	Kontrolės aplinka	*Etika ir darbinė aplinka*	Ar galite teigti, kad organizacijoje yra išlaikomas tinkamas verslo etikos lygis, vadovų pavyzdžiu formuojama elgesio praktika?	Kaip vertinate organizacijos darbinę aplinką? Kokiomis priemonėmis ji gerinama?	1 - organizacijoje nėra išlaikomas tinkamas verslo etikos lygis, vadovų pavyzdžiu nėra formuojama darbinė aplinka; 2 - organizacijoje išlaikomas žemas verslo etikos lygis, vadovų pavyzdžiu nėra formuojama darbinė aplinka; 3 - organizacijoje išlaikomas tinkamas verslo etikos lygis, tačiau vadovų pavyzdžiu nėra formuojama darbinė aplinka; 4 - organizacijoje išlaikomas aukštas verslo etikos lygis, vadovų pavyzdžiu formuojama darbinė aplinka; 5 - organizacijoje išlaikomas aukščiausias verslo etikos lygis, vadovų pavyzdžiu formuojama darbinė aplinka
		Informavimas ir komunikavimas	*Grįžtamasis ryšys*	Ar iš organizacijos vadovų jaučiamas grįžtamasis ryšys, susijęs su praeities sprendimais apie vidaus kontrolės valdymą, kuriais remiantis gali būti priimami ateities sprendimai?	Ar galite teigti, kad informavimo/ komunikavimo vertinimas atliekamas pagal tai, ar vidiniai ir išoriniai informacijos srautai yra priimami ir ar tinkamai pritaikomi?	1 - organizacijai nėra būdingas vadovų grįžtamasis ryšys; 2 - organizacijai būdingas vadovų grįžtamasis ryšys apie tam tikrus praeities sprendimus ir jie retai panaudojami priimant ateities sprendimus; 3 - organizacijai būdingas vadovų grįžtamasis ryšys apie daugumą praeities sprendimų, kurio pagrindu reti sprendimai grindžiami ateityje; 4 - organizacijai būdingas vadovų grįžtamasis ryšys apie praeities sprendimus, kurio pagrindu dažni sprendimai grindžiami ateityje; 5 - organizacijai būdingas vadovų grįžtamasis ryšys apie praeities sprendimus, kurio pagrindu visi sprendimai grindžiami ateityje
		Rizikos įvertinimas	*Vidinės ir išorinės grėsmės*	Ar atliekant vidaus kontrolės vertinimą organizacijoje yra identifikuojamos vidinės ir išorinės grėsmės, kurios gali turėti įtakos organizacijos tikslų pasiekimui?	Kaip organizacijoje yra vertinama kibernetinio saugumo grėsmė?	1 - organizacijoje vidinių ir išorinių grėsmių identifikavimui vertinant vidaus kontrolę nėra skiriamas dėmesys; 2 - organizacijoje vidinių ir išorinių grėsmių identifikavimui vertinant vidaus kontrolę skiriamas mažas dėmesys; 3 - organizacijoje vidinių ir išorinių grėsmių identifikavimui vertinant vidaus kontrolę skiriamas vidutinis dėmesys; 4 - organizacijoje vidinių ir išorinių grėsmių identifikavimui vertinant vidaus kontrolę skiriamas didelis dėmesys; 5 - organizacijoje vidinių ir išorinių grėsmių identifikavimui vertinant vidaus kontrolę skiriamas didžiausias dėmesys, tai padeda laiku nustatyti problemas ir pagal jas ieškoti sprendimų

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai (nustatyti, ar kriterijus aktualus organizacijos veikloje)	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
VIDAUS AUDITO PROCEDŪRŲ UŽTIKRINIMO VERTINIMAS	**VIDAUS KONTROLĖS VERTINIMAS**	Kontrolės priemonės	*Vertinimas*	Ar galite teigti, kad organizacijoje atliekant vidaus kontrolės vertinimą naudojama pakankamai kontrolės priemonių?	Kurios iš šių kontrolių rūšių yra vertinamos – veiksmų kontrolė, rezultatų kontrolė, personalo-motyvacinė kontrolė, organizacijos kultūra? Kaip atliekamas šių kontrolių vertinimas ir kur yra nustatomi didžiausi trūkumai?	1 - organizacijoje nėra pakankamas kontrolės priemonių naudojimas vertinant vidaus kontrolę; 2 - organizacijoje yra žemas kontrolės priemonių naudojimo lygis, vertinama 1 kontrolės rūšis; 3 - organizacijoje yra vidutinis kontrolės priemonių naudojimo lygis, vertinamos 2 kontrolės rūšys; 4 - organizacijoje yra aukštas kontrolės priemonių naudojimo lygis, vertinamos 3 kontrolės rūšys; 5 - organizacijoje yra labai aukštas kontrolės priemonių naudojimo lygis, vertinamos 4 ir daugiau kontrolės rūšys
		Stebėsena	*Kontrolės vertinimas*	Ar po vidaus kontrolės įvertinimo yra atliekama kontrolės vertinimo stebėsena, siekiant patvirtinti gautus rezultatus apie kontrolės procesų tinkamumą ir veiksmingumą?	Kokias būdais atliekama kontrolės vertinimo stebėsena?	1 - organizacijoje nėra atliekama kontrolės vertinimo stebėsena; 2 - organizacijoje nėra atliekama kontrolės vertinimo stebėsena, tačiau planuojama tai daryti ateityje; 3 - organizacijoje skiriamas mažas dėmesys kontrolės vertinimo stebėsenai; 4 - organizacijoje skiriamas vidutinis dėmesys kontrolės vertinimo stebėsenai; 5 - organizacijoje skiriamas didelis dėmesys kontrolės vertinimo stebėsenai
	ATASKAITŲ RENGIMAS	Rezultatų aptarimas	*Vadovų požiūris*	Ar organizacijoje prieš galutinės ataskaitos (pagrindinės nuomonės) rengimą yra pristatomi gauti vidaus audito rezultatai vadovybei?	Kokią įtaką turi vadovybės nuomonė apie šiuos rezultatus? Kaip dažnai po gautų rezultatų aptarimo reikalingi vidaus audito rezultatų patikslinimai?	1 - organizacijoje vadovams nėra pristatomi audito rezultatai prieš galutinės išvados suformulavimą; 2 - organizacijoje vadovams retai pristatomi audito rezultatai prieš galutinės išvados suformulavimą, vadovai įtakos tam neturi; 3 - organizacijoje vadovams dažniausiai pristatomi audito rezultatai prieš galutinės išvados suformulavimą, tačiau vadovai įtakos tam neturi; 4 - organizacijoje vadovams dažniausiai pristatomi audito rezultatai prieš galutinės išvados suformulavimą, vadovų įtaka yra; 5 - organizacijoje vadovams visada pristatomi audito rezultatai prieš galutinės išvados suformulavimą, vadovų įtaka didelė
		Atitikties testavimas	*Bendri veikimo taškai*	Ar organizacijoje vidaus audito metu yra atliekamas atitikties testavimas, siekiant nustatyti rodiklių priklausomybes, bendrus veikimo taškus?	Kaip dažnai yra atliekamas atitikties testavimas siekiant surasti kibernetinio saugumo ir vidaus audito rodiklių sutapimus ir bendrus jų veikimo taškus?	1 - organizacijoje nėra atliekamas atitikties testavimas; 2 - organizacijoje nėra atliekamas atitikties testavimas, tačiau planuojama tai daryti ateityje; 3 - organizacijoje atitikties testavimas atliekamas retai; 4 - organizacijoje atitikties testavimas atliekamas dažnai; 5 - organizacijoje atitikties testavimas atliekamas visada

	Kategorija	Kriterijus	Raktinis žodis	Vertinimo klausimai (nustatyti, ar kriterijus aktualus organizacijos veikloje)	Papildomi klausimai	Atsakymo įverčiai (būklės įvertinimui)
VIDAUS AUDITO PROCEDŪRŲ UŽTIKRINIMO VERTINIMAS	**ATASKAITŲ RENGIMAS**	Galutinė ataskaita	*Išvados*	Ar vidaus audito vadovas, formuojantis nuomonę ir galutines išvadas, skirtingoms organizacijos sritims pateikia atskiras nuomones (išvadas)?	Kokioms skirtingoms sritims yra pateikiamos atskiros nuomonės ir išvados (stebėjimo operacijų, finansinio užtikrinimo ir kibernetinio saugumo)?	1 - organizacijoje yra pateikiama viena bendra išvada ir galutinė nuomonė; 2 - organizacijoje pateikiamos bendros išvados visai veiklai, jos nedetalizuojamos; 3 - organizacijoje pateikiamos skirtingos nuomonės ir išvados pagrindinėms organizacijos sritims, vertinamos 2 sritys; 4 - organizacijoje pateikiamos skirtingos nuomonės ir išvados pagrindinėms organizacijos sritims, vertinamos 3 sritys; 5 - organizacijoje pateikiamos skirtingos nuomonės ir išvados visoms organizacijos sritims, vertinamos 4 sritys ir daugiau
	PAŽANGOS STEBĖJIMAS	Rekomendacijos	*Pažangos stebėjimas*	Ar po galutinės ataskaitos paskelbimo (nuomonės suformulavimo) pateikiamos rekomendacijos, susiję su organizacijos kibernetinės grėsmės suvaldymu?	Kokie yra vykdomi pažangos stebėjimo etapai?	1 - po galutinės ataskaitos paskelbimo nėra pateikiamos rekomendacijos; 2 - po galutinės ataskaitos paskelbimo nėra pateikiamos rekomendacijos, tačiau planuojama tai daryti ateityje; 3 - po galutinės ataskaitos paskelbimo tam tikrais atvejais pateikiamos rekomendacijos, susiję su visų grėsmių suvaldymu iš vidaus audito pusės; 4 - po galutinės ataskaitos paskelbimo dažniausiai pateikiamos rekomendacijos, susiję su visų grėsmių suvaldymu iš vidaus audito pusės; 5 - po galutinės ataskaitos paskelbimo visada pateikiamos rekomendacijos, susiję su visų grėsmių suvaldymu iš vidaus audito pusės