MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

SOLVITA LEBECKAITĖ

MAŽŲ IR VIDUTINIŲ ĮMONIŲ RIZIKOS ANALIZĖS VERTINIMAS

Magistro baigiamasis darbas

Vadovas

Doc. dr. Ramūnas Vanagas

VILNIUS, 2022

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

MAŽŲ IR VIDUTINIŲ ĮMONIŲ RIZIKOS ANALIZĖS VERTINIMAS

Veiklos audito magistro baigiamasis darbas

Studijų programa 6211LX075

Vadovas

doc. dr. Ramūnas Vanagas

Atliko

VKAvmis20 gr. stud.

S. Lebeckaitė

VILNIUS, 2022

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Verslo pasaulyje rizikos faktorius yra neišvengiamas. Nesvarbu, kurią sritį atstovauja verslo subjektas - konkurencija, infliacija ar bendri rinkos paklausos pokyčiai nuolat keičia jo aplinką. Rizikos valdymo problemos ne tik Lietuvoje, bet ir visame pasaulyje tampa išskirtinio dėmesio objektu, kuris aktualus tiek plečiant nagrinėjamų rizikų įvairovę, tiek plėtojant jų pažinimą (Garbanovas, 2010).

Temos aktualumas. Verslo rizikos žinojimas ir valdymas yra neatsiejama kiekvieno sėkmingo verslo dalis, kuri vis labiau tampa pagrindiniu konkurencingumo veiksniu. Nepakankamas dėmesys verslo rizikai, netinkamas jos vertinimas ar valdymas gali turėti įtakos įmonės veiklai ar jos tęstinumui. Mokslinėje literatūroje Laskienė (2003), Rutkauskas (2009), Aleknavičienė (1997), Statytytė (2015), Kindurys (2011) ir kt. riziką apibūdina skirtingai ir vieno tikslaus apibrėžimo nėra, tačiau pagrindiniai rizikos apibrėžimo elementai - tai netikslumas, galimybė, neapibrėžtumas, nuostolis. Veiklos rizikos valdymas smulkiose ir vidutinėse organizacijose, kurios sukuria didelę pridėtinės vertės dalį Europos Sąjungoje, reikalauja atskiro dėmesio, suderintų sprendimų ir priemonių (Stasytytė, Aleksienė, 2015). Per pastarąjį dešimtmetį išaugęs susidomėjimas gerinti įmonių gebėjimą susidoroti su neapibrėžtumu, o ypač su neigiamu jos poveikiu organizacijos lygmeniu, paskatino rizikos valdymo priemonių, metodų, procesų ir metodikų kūrimą ir taikymą. Kadangi verslo pasaulyje rizikos išvengti neįmanoma, būtina ją išskirti, įvertinti ir minimizuoti.

Temos naujumas. Šiuolaikiniame verslo pasaulyje yra daug įvairių rizikos valdymo standartų, tokių kaip ISO31000, COSO, ISO27005 ir kt., kurie yra patikimi ir laiko išbandyti. Šie standartai yra platūs ir reikalaujantys nemažai finansinių ir žmogiškųjų išteklių. Tarptautinius standartus aprašo darbe nagrinėjami Alberts ir Dorofee (2001), Januta, Marozas ir Goranin (2011), Čepinskis ir Raškinis (2005), Jevsejev (2019) ir kt. Didėlėms organizacijoms tokie rizikos valdymo standartai yra priimtini, tačiau mažoms ir vidutinėms įmonės, dažnu atveju, per sunkūs. Atsižvelgiant į tai, šiame darbe kuriamas naujas, mažesnės apimties rizikos valdymo modelis, kuris leistų mažoms ir vidutinėms įmonėms be papildomų išteklių, naudojant esamus resursus, išanalizuoti galimas jų įmonės rizikas.

Darbo objektas – rizikos valdymas mažose ir vidutinėse įmonėse.

Darbo problema – kaip mažos ir vidutinės įmonės turi organizuoti rizikos vertinimą naudojant mažiau resursų?

Magistro darbo tikslas – remiantis esamais tarptautiniais standartais sukurti mažesnės apimties rizikos vertinimo metodą, pritaikant jį vidutinėje „X“ įmonėje.

Magistrinio darbo uždaviniai:

1. Išanalizuoti ir apibrėžti rizikos valdymo sampratą, aptarti rizikos valdymo ir vertinimo principus teoriniu aspektu.
2. Išanalizuoti esamus rizikos valdymo modelius.
3. Ištirti naudojamų tarptautinių standartų paklausumą bei tinkamumą mažoms ir vidutinėms įmonėms.
4. Sukurti rizikos valdymo metodą orientuotą į smulkias ir vidutines įmones.
5. Palyginti sukurtą modelį su „X“ įmonėje taikomu tarptautiniu standartu.

Darbo metodai:

1. Mokslinės literatūros analizės metodas.
2. Anketinė apklausa .
3. Modeliavimo metodas.
4. Lyginamosios analizės metodas.

Raktiniai žodžiai. Rizika, rizikos valdymo procesas, rizikos veiksniai, rizikos valdymo metodai, IT sektorius, mažos ir vidutinės įmonės.

Darbo struktūra ir apimtis: Bendra apimtis – 65 puslapių. Darbą sudaro įvadas, teorinė dalis, metodologinė ir analitinė dalys, išvados ir rekomendacijos, literatūros sąrašas, anotacija ir santrauka (lietuvių ir anglų kalbomis), priedai. Darbe pateiktos 11 lentelių, 23 paveikslai ir 2 priedai. Literatūros sąraše – 44 šaltiniai.

1. RIZIKOS VALDYMO TEORINIAI ASPEKTAI

1.1. Rizikos samprata

Šiuometiniame pasaulyje, kuris kiekvieną dieną tobulėja, rizikos valdymas yra neišvengiama kiekvieno verslo aplinkos dalis (Belanova, 2018). Tobulėjant technologijoms, keičiantis procesams atsiranda vis daugiau pavojų, kuriuos institucijos ar įmonės turi identifikuoti, įvertinti ir atlikti veiksmus, kurie ateityje užtikrintų sklandų darbą. Verslo rizika – tai verslo aplinkos dalis, su kuria kiekviena įmonė turi susidurti kiekvieną darbo dieną. Verslo aplinka parodo ir verslo sąlygų kokybę bei sąlygas savo ūkinei veiklai. Jei verslo aplinką sudarys kokybiškos sąlygos, tvarus ekonominis augimas ir tikslus rizikų valdymas, tai gali pagerinti įmonės konkurencingumą tarptautiniame lygmenyje (Virglerova, 2018).

Pasak Thompson (1996), žymiausiuose žodynuose rizika apibrėžiama kaip pavojaus, praradimo ar kitų neigiamų pasekmių galimybė ar atsiradęs šansas. Balkevičius (2017) išskiria tokias rizikos rūšis, kaip socialinė, psichologinė, ekonominė ir kt.. Taigi, esant įvairioms rizikos rūšims, rizikos sąvoka dažnai vartojama įvairiuose konceptuose ir nėra tiksliai apibrėžta. Lietuvių kalbos žodyne (LKZ) rizika apibrėžiama kaip su galimu pavojumi susijęs dalykas, pasiryžimas vykdyti ką nors pavojingą ir per daug didelis savęs vertinimas, įsivaizdavimas. Tarptautinių žodžių žodyne rizikos apibūdinimai nurodomi tokie:

1. „*Ryžimasis veikti, žinant, kad yra tam tikra tikimybė nepasiekti tikslo, arba ryžimasis nepaisyti galimų neigiamų atsitiktinių aplinkybių padarinių;*

2. Aplinkybės, kuriomis apsisprendimas imtis tam tikro veiksmo, priemonės arba jų nesiimti gali nepasiekti tikslo arba nepateisinti vilčių;

3. Nepasisekimo tikimybė“ (Tarptautinių žodžių žodynas).

Psichologijos žodynuose terminas „rizika“ aiškinamas kaip:

1. „veiklos situacinė ypatybė – žmogus veikia nežinodamas, kokia bus veiklos baigtis (sėkminga ar nesėkminga) (6, p. 857); <..>

2. tikėtinos nesėkmės ir jos neigiamo padarinio dydis (7, p. 259); <..>

3. veiksmas (gali būti motyvuotas arba nemotyvuotas), kurį atlikdamas žmogus gali ką nors prarasti (pralaimėti, gauti traumą, patirti nuostolį)“ (8, p. 344) (Psichologijos žodynas).

Darbe nagrinėjamų autorių Balkevičiaus (2017), Daujotaitės (2012), Aleknavičienės (1997), Statytytės (2008) ir kt. straipsniuose pastebima, kad rizikos sąvoka skiriasi priklausomai nuo autorių sukauptos patirties tam tikroje srityje ir tyrinėjamo objekto. 1 lentelėje pateikiami skirtingų autorių rizikos sąvokų apibrėžimai.

1 lentelė. Rizikos sampratos apibrėžimai

Autorius	Apibrėžimas
D. Daujotaitė	„Tikimybė, kad susiklosčius tam tikroms aplinkybėms nepalankus (neigiamai veikiantis auditą) įvykis gali realiai įvykti ir tai gali įvykti kiekviename veiklos audito proceso etape“ (Daujotaitė, Tarakavičiūtė, Puškorius, 2012).
G. E. Rejda	„Netikrumas dėl nuostolių atsiradimo“ (Rejda, 2008).
D. Laskienė	„Nepageidaujamo įvykio (poveikio) ar prarastos (maksimaliai neišnaudoto) naudos, pasireiškiančios konkrečiam subjektui, galimybė, sąlygojama aplinkos neapibrėžtumo“ (Laskienė, Snieška, 2003)
V. Rutkauskas	„Galimybė, kad pavojingoje situacijoje atsidūręs subjektas patirs neigiamą poveikį. Rizika – galima netektis, kuri priklauso ir nuo nepalankaus įvykio galimybių, ir nuo poveikio recipientų atsako būdo bei aplinkos įtakos poveikio procesui“ (Rutkauskas, A. V.; Stasytytė, V.; Borisova, J. 2009).
A. Lezgovko	„Įvykis, kuris gali įvykti, bet gali ir neįvykti“ (Lezgovko, Lastauskas, 2008).
V. Aleknavičienė	„Sprendimų situaciją, kurioje egzistuoja faktinių rezultatų nukrypimo nuo prognozuojamų rezultatų galimybė“ (Aleknevičienė, 1997).
J. Čepinskis, D. Raškinis	„Rizika gali būti apibrėžiama kaip nuostolių atsiradimo tikimybė, dispersija nuo matematinio vidurkio, tikimybė, kad faktinis rezultatas nesutaps su laukiamuoju“ (Čepinskis, Raškinis, 2005)
Z. Lydeka, B. Drilingas	„1) Tai galimi pavojai, gresianti žala, nuostoliai bei nelaimė vykdant kokius nors veiksmus; 2) tai įsitikinimas sėkme ir vykdymas veiksmų, kurių atlikimas priklauso nuo iš anksto nežinomų įvykių arba tiksliai neapibrėžtų aplinkybių“ (Lydeka, Drilingas, 2002).

Šaltinis: sudaryta autorės

Apibrėžimuose pastebima, kad autoriai išskiria tam tikras rizikos savybes. Merna, Al-Thani (2008) riziką aprašo, kaip tikimybę, kad per tam tikrą laiką įvyks kažkas nepageidaujamo. Daujotaitė (2012) rizikos apibrėžimą pažymi kaip tikimybę, Rejda (2008) – netikslumą, Laskienė (2003), Rutkauskas (2009) ir Aleknavičienė (1997) – galimybę, o Lezgovko (2008) – įvykį, kurio baigtis nėra aiški. „Rizikos sąvokos nagrinėjimas neatsiejamas nuo neapibrėžtumo sąvokos“ (Statytytė, 2015, p.141). Pasak Kindurio (2011) rizikos sąvokos apibrėžtumą apsunkina tai, kad jos taikymo sritis yra plati ir labai įvairi. Nagrinėjant literatūrą pastebima, kad Gegužis (2003) ir kt. autoriai taip pat pabrėžia netikrumo ir neapibrėžtumo sampratą, kurios yra savitas rizikos turinio elementas. Tokie autoriai kaip Čepinskis ir Raškinis (2004) neapibrėžtumą išskirstė lygiais:

1. Nėra neapibrėžtumo – galima numatyti tikslius rezultatus;

2. Pirmo lygio neapibrėžtumas – žinomi rezultatai ir jų tikimybės;
3. Antro lygio neapibrėžtumas – žinomi rezultatai, bet šių rezultatų tikimybės nėra žinomos;
4. Trečio lygio neapibrėžtumas – rezultatai nėra visiškai aiškūs, o jų tikimybės taip pat nėra žinomos.

Užsienio autoriaus atskiria riziką ir neapibrėžtumą teigdamas, kad neapibrėžtumas – didesnė nežinomybė nei rizika: „jei jūs nežinote, kas atsitiks, bet žinote galimybes, tai yra rizika, o jei nežinote netgi galimybių, tai yra neapibrėžtumas“ (Adams, 2001, p. 30). Pasak Kindurio (2011) „netikrumas yra objektyvi, nuo žmonių valios nepriklausoma situacija, kai konkretus padarinių rezultatas yra nežinomas“ (p. 43). Netikrumas taip pat gali pasireikšti atsižvelgiant ir į rizikos dydžius: maža rizika, vidutinė rizika, didelė rizika. Marchand (2009) teigia, „kad pats paprasčiausias, plačiai vartojamas rizikos apibrėžimas, kuriuo remiasi daugelis rizikos valdytojų, gali būti aprašomas lygtimi: rizika yra tikimybė įvykti įvykiui, padauginta iš jau įvykusio įvykio padarinių“ (p. 22) (padariniai gali būti išreikšti pinigais arba indeksu):

RIZIKA = TIKIMYBĖ x PADARINIAI

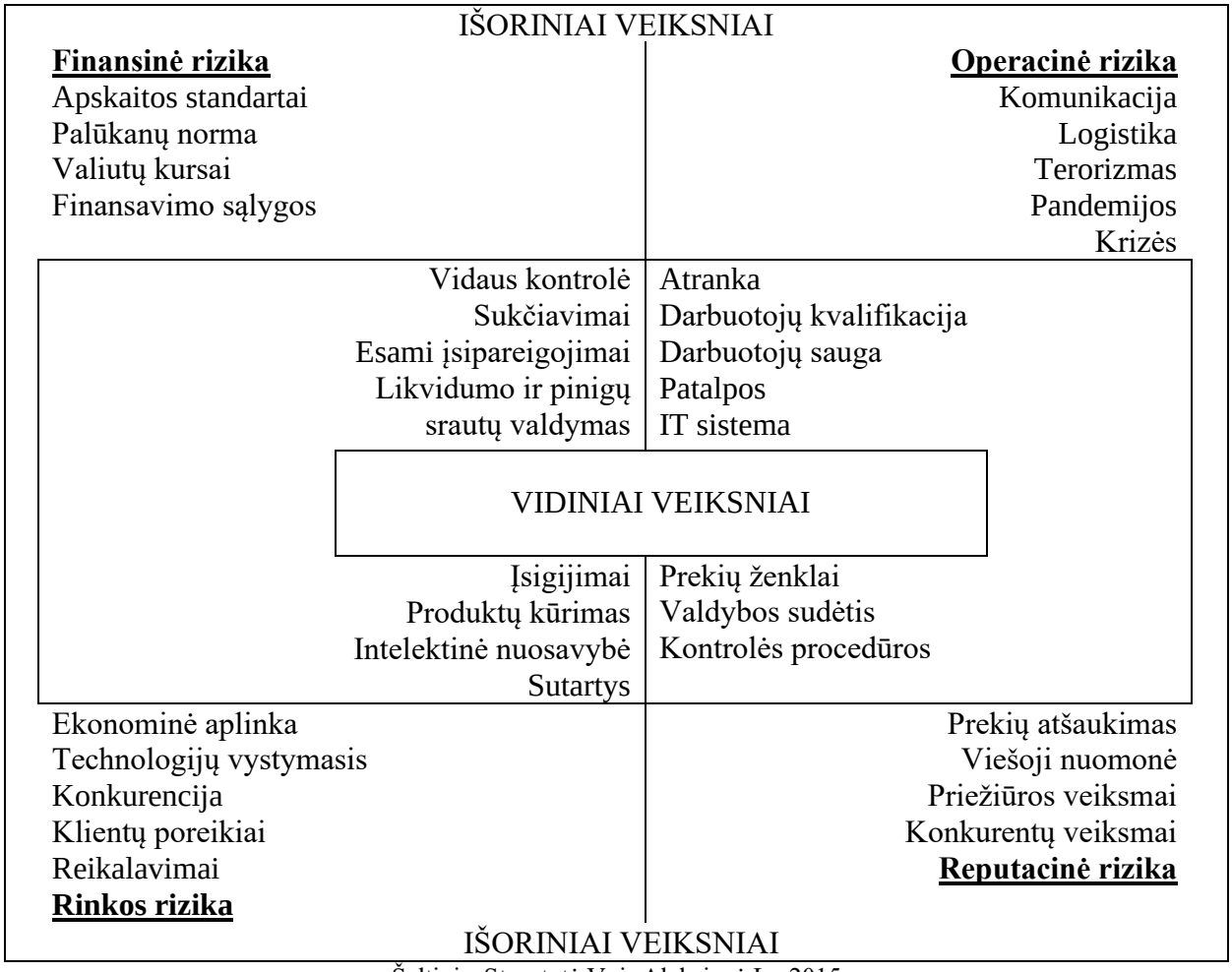
Taigi, praktikoje galima rasti ir susidurti su daug skirtingų rizikos apibrėžimų, tačiau galima pastebėti tai, kad visiems jiems yra būdingi keli elementai - tai netikslumas, galimybė, neapibrėžtumas, nuostolis.

1.2. Rizikos veiksniai

Rizika gali priklausyti nuo daug veiksnių, kurie skirstomi į išorinius ir vidinius (Mackevičius, Giriūnas, 2014). „Išoriniai rizikos veiksniai – įvykiai ir aplinkybės, staiga ir netikėtai veikiančios įmonę iš išorės, kurių negalima prognozuoti, užkirsti jiems kelio ar daryti esminės įtakos <...>, vidiniai veiksniai – tai rizikos, užprogramuotos organizacijos veikloje“ (Stasytytė ir Aleksienė, 2015, p. 142). Autorius Mackevičius (2005), taip pat pabrėžia, kad rizika skirstoma ir pagal veiklos sritis, kurios yra ūkinės (susijusios su įmonės ūkinės situacijos neapibrėžtumu), gamybinės (jų atsiradimą lemia technologinių procesų, technikos ar įrangos netobulumai ir kt.), komercinės (susijusios su įvairių sandorių sudarymu bei vykdymu), finansinės (susijusios su finansų tvarkymu ir pajamų ir sąnaudų kontrole), investicinės (susijusios su investicijų praradimu ir kt.). Pasak Stasytytė ir Aleksienė (2015) išorinę riziką taip pat galima skirstyti į tiesioginio ir netiesioginio poveikio veiksnius. Tiesioginio poveikio veiksniai yra mokesčių sistema, reketas, korupcija ir kt., o netiesioginio – stichinės nelaimės, rinkos pokyčiai, tarptautiniai įvykiai ir kt.

Autorės Stasytytė, L. ir Aleksienė L. (2015) straipsnyje pateikia pagal draudimo ir rizikos valdytojų pramonės ir prekybos asociaciją AIRMIC (2010), Rizikos valdymo institutą IRM (2002) ir Viešojo rizikos valdymo asociaciją ALARM (2010) rizikos veiksnių lentelę, kuri suskirstytą į išorinius ir vidinius veiksnius (žr. 1 pav.).

Išorinius veiksnius sudaro finansinė, operacinė, rinkos ir reputacijos rizika. Šios rizikos skaidomos dar smulkiau: į finansinę riziką įeina apskaitos standartai, palūkanų normos, valiutų kursai, finansavimo sąlygos, į operacinę riziką: komunikacija, logistika, terorizmas, pandemijos, krizės, į rinkos: ekonominė aplinka, technologijų vystymasis, konkurencija, klientų poreikiai, reikalavimai, į reputacijos: prekių atšaukimas, viešoji nuomonė, priežiūros veiksmai, konkurentų veiksmai.



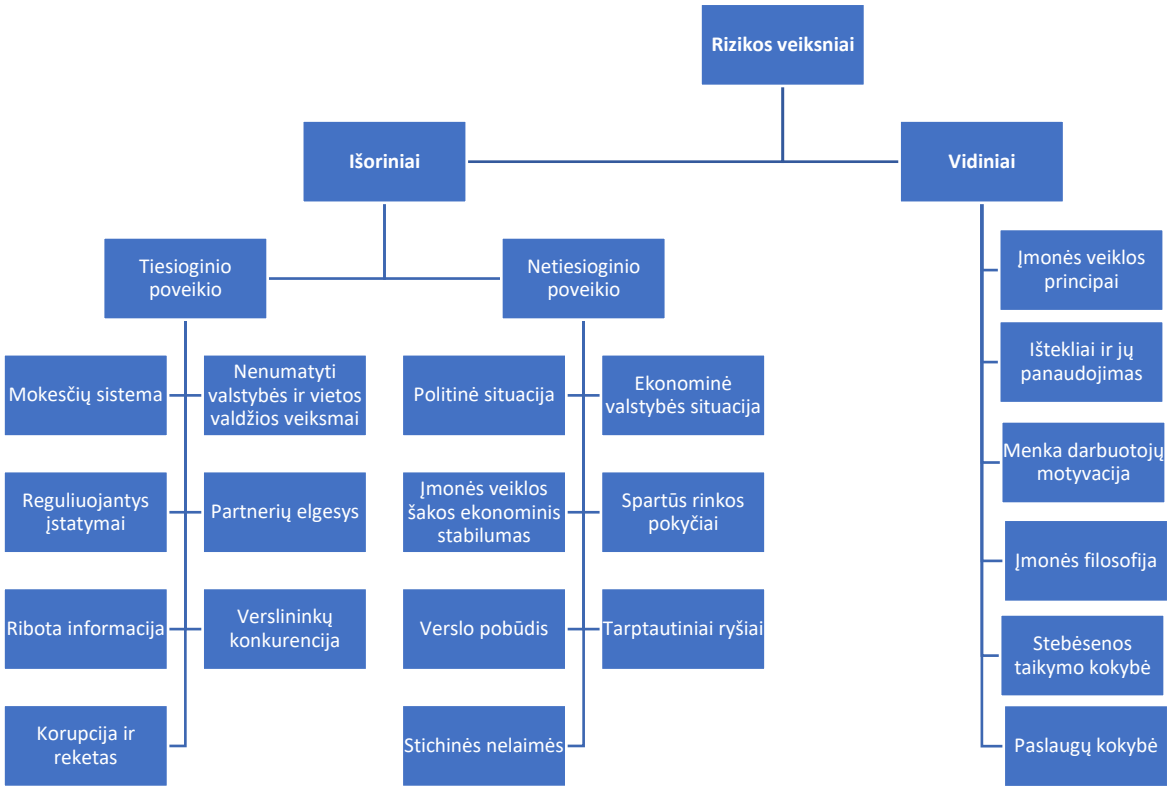
Šaltinis: Stasytytė V. ir Aleksienė L., 2015

1 pav. Rizikos veiksniai (AIRMIC, ALARM, IRM 2010)

Išoriniai ir vidiniai veiksniai yra susiję. Išorinis veiksnys - finansų riziką susijęs su vidiniais veiksniais: vidaus kontrole, sukčiavimais, įsipareigojimais, investiciniais sprendimais, likvidumu bei srautų

valdymu; operacinė rizika: atrankomis, darbuotojų kvalifikacija, darbo sauga, patalpomis, IT sistema; rinkos rizika: įsipareigojimais, produktų kūrimu, intelektine nuosavybe, sutartimis; reputacinė rizika: prekių ženklais, valdybos sudėtimi ir kontrolės procedūromis.

Taip pat, Valackienė (2012) išskiria, kad išoriniai veiksniai gali būti skirstomi dar smulkiau: tiesioginio ir netiesioginio poveikio ar netgi dar detaliau (žr. 2 pav.).



Šaltinis: Valackienė, 2012.

2 pav. Rizikos veiksnių klasifikavimas

Mackevičius (2005) pateikia šiek tiek platesnį rizikų klasifikavimo modelį, kuriame rizikos skirstomos:

- Politinės ir ekonominės (pagal atsiradimo pobūdis).
- Vidaus ir išorės (pagal poveikį).
- Ūkinė, gamybinė, investicinė, finansinė ir komercinė (pagal veiklos sritis).
- Einamoji, retrospektyvinė ir perspektyvinė (pagal laiką).
- Grynoji ir spekuliatyvinė (pagal rezultato tikimybę).

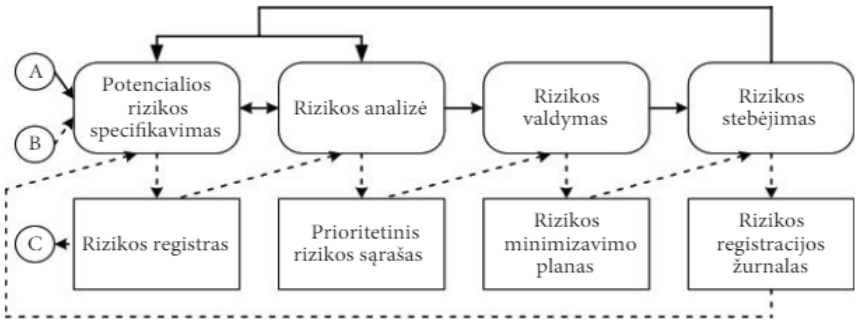
Šis autoriaus rizikų kvalifikavimo būdas yra bene plačiausiai klasifikuojamas. Kadangi šis būdas yra labai išsamus, jis yra naudingesnis atliekant rizikos vertinimą, o ne valdant riziką.

Apibendrinus galima teigti, kad rizika yra labai plati sąvoka ir kiekvienas ją gali suprasti skirtingai, todėl yra tiek daug rizikos apibrėžimų bei rizikos rūšių. Taigi, didžioji dalis 1 ir 2 paveiksluose nurodytų veiksnių yra tarpusavyje susiję ir gali daryti įtaką rizikos padariniams. Kadangi rizikos rūšys labiausiai priklauso nuo verslo pobūdžio, tai reiškia, kad kuo įmonės veikla yra įvairesnė, tuo atsiranda vis daugiau naujų rizikos rūšių.

Vienos rizikos rūšies pasikeitimas gali nulemti kitų rizikos rūšių pokyčius. Rizikos valdymo procese svarbiausia nustatyti didžiausią galimą poveikį veiklai darančius rizikos veiksnius ir tuo pačiu numatytų tų veiksnių patikimiausias valdymo priemones.

1.3. Rizikos valdymo metodai

Rizikos valdymas prasideda nuo įmonės veiklos ypatybių išgryninimo. Svarbiausia nusistatyti ne tik veiklos pobūdį, bet ir mastą, sezoniškumą, ūkinių operacijų sudėtingumą, problemiškumą. „Rizikos valdymas – tai galimos rizikos nustatymas ir planų, kurie minimizuotų rizikos įvykio padarinius projektui, sudarymas“ (Davidavičienė, 2012, 31 p.). Užsienio autoriai rizikos valdymą įvardina kaip „įmonės numatytos strategijos, procedūrų ir priemonių naudojimą rizikai minimizuoti“ (Davis, Jarvis, 2008). Kancerevyčius (2006) rizikos valdymą nurodo, kaip procesą, kurio metu identifikuojamos, stebimos, įvertinamos bei kontroliuojamos visos patiriamos rizikos. Senesniuose literatūros šaltiniuose minima, kad rizikos valdymas – tai nepertraukiamas procesas, leidžiantis įmonėms subalansuoti veiklos ir ekonomines apsaugos priemonių sąnaudas bei padidinti pajėgumus (Stoneburner, Goguen, Feringa, 2002). Autorė Davidavičienė (2012) knygoje apie informacinių technologijų valdymą pateikia rizikos valdymo schemą (žr. 3 pav.).



Šaltinis: Davidavičienė, 2012, p. 32

3 pav. Rizikos valdymo schema

Rizikos valdymas apima visas įmonės veiklos sritis siekiant išaiškinti nepalankius įvykius. Šiuolaikinis rizikos valdymas yra šiek tiek pasikeitęs, dėl daugelio veiksnių, įskaitant:

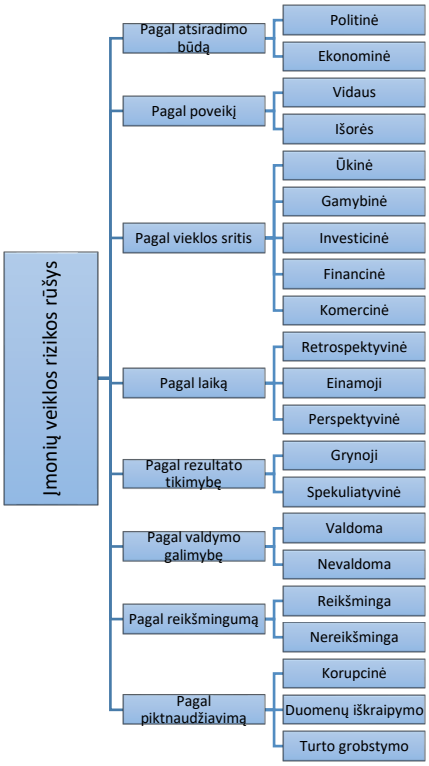
- Perėjimą nuo pavojingo fizinio darbo prie žinioms imlaus darbo;
- Išplėstas požiūris į organizaciją įvairių jos suinteresuotųjų šalių kontekste;
- Didėjantis projektų, kaip darbo planavimo ir vykdymo sistemos, svarbos klausimas organizacijose;
- Pagrindinis technologijos vaidmuo ir jai būdingas neapibrėžtumas;
- Nuolat didėjantis konkurencinis spaudimas sutrumpinti pristatymo laiką, todėl organizacijos pradeda veikti planuoti ir vykdyti savo veiklą turėdami neišsamią informaciją;
- Didėjantys neramumai verslo aplinkoje;
- Spartus verslo ir projektų sudėtingumo laipsnio augimas;
- Besitęsianti globalizacijos tendencija ir dėl to akcentuojamas virtualus verslas ir komandos;
- Didėjanti reguliavimo našta, kurios įmonės turi laikytis (Raz, Hillson, 2005, 53-66 p.).

Visi šie ir kiti veiksniai lėmė augantį knygų ir straipsnių skaičių, kurie skirti veiklos rizikos valdymui analizuoti. Ši sritis auga nuolatos, bet rizikos valdymo pradmenys lieka tie patys, tik yra tobulinami.

Šaltinis: Vageris, 2005, p. 10

4 pav. Sąvokų sąsajos, remiantis jų apibrėžimais ISO vadove 72

Pasak Vagerio (2005), ISO vadove 72 yra pateiktos tarpusavyje susijusios sąvokos, kurios atspindi rizikos valdymą ir rizikos analizę (žr. 4 pav.) Tai yra kaip rizikos valdymo planas, kuriuo vadovaujantis galėtų būti sudaromas įmonės rizikos valdymas.



Šaltinis: Mackevičius, Giriūnas, 2014, p. 54

5 pav. Įmonių veiklos rizikos rūšys

Verslo aplinkoje yra daugybė įvairių rizikos rūšių, kurie priklauso nuo skirtingų faktorių. Rizikos rūšys gali priklausyti nuo geografinės padėties, verslo apimties, sudėtingumo ir kitų veiksnių. „Tiek praktiniu, tiek teoriniu požiūriu tikslinga įmonių veiklos rizikas skirstyti pagal tam tikrus požymius“ (Mackevičius, Giriūnas, 2014). Kaip matoma 5 paveiksle, autoriai J. Mackevičius, ir L. Giriūnas, įmonių veiklos rizikos rūšis išskirstė pagal skirtingus faktorius. Rizikos faktorius pagal atsiradimo būdą skirstomas į politinį ir ekonominį, pagal poveikį – vidaus ir išorės, pagal veiklos sritis – ūkinį, investicinį, gamybinį, finansinį ir komercinį, pagal laiką – retrospektyvinį, einamąją ir perspektyvinį, pagal rezultato tikimybę – spekuliatyvinį ir grynąjį, pagal valdymo galimybę – valdomą ir nevaldomą, pagal reikšmingumą – reikšmingą ir nereikšmingą, pagal piktnaudžiavimą – korupcinį, duomenų iškraipymo ir turto grobstymo. „Vertinant bet kurią rizikos rūšį būtina atkreipti dėmesį į jos dualizmą:

1. Rizika – tai nuostolių tikimybė,
2. Rizika – tai pelno (ar naudos) tikimybė.“ (Mackevičius ir Giriūnas, 2014, p. 56).

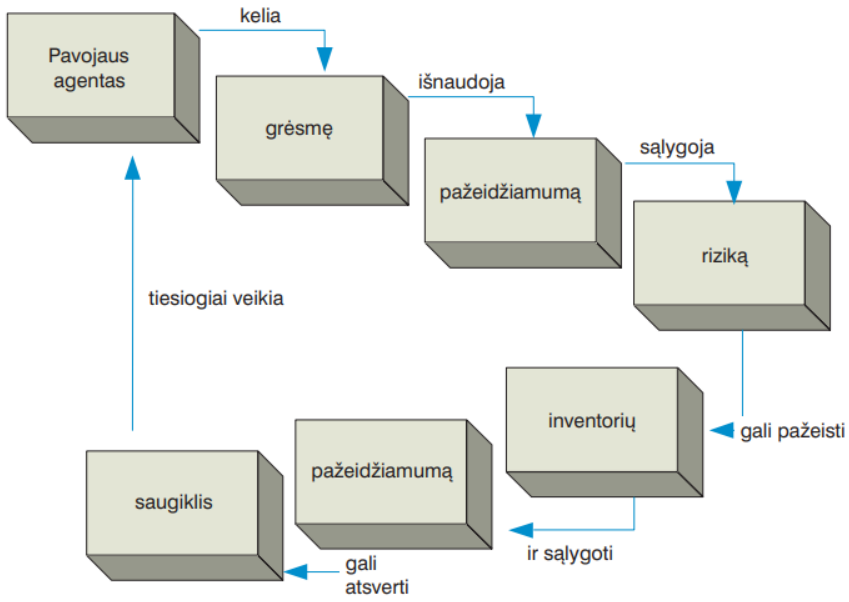
„Pagrindinis rizikos valdymo tikslas yra atskleisti ir sumažinti bet kurios rūšies riziką iki priimtino lygio“ (Mackevičius, Giriūnas, 2014, p. 57). Mills (2001) aprašo, kad rizikos valdymo tikslas – ne tik išvengti visų galimų rizikų, bet ir jas sėkmingai valdyti atsižvelgiant į finansinius bei laiko išteklius, nustatant rizikos neišvengiamumo, jos suvaldymą patiriant minimalius nuostolius. Panašiai teigia ir

Kanapickienė (2009), kad būtina nustatyti rizikos svarbą ir dydį, išnagrinėti atsiradimo tikimybę, nustatyti priimtinos rizikos galimybę, nes tinkamai identifikavus rizikos lygį, galima išvengti neigiamų padarinių, su kuriais įmonė susidurtų.

Rita Kanapickienė (2009) „rizikos valdymą siūlo išskirti į 4 etapus:

1. Įmonės tikslų nustatymas.
2. Rizikos tyrimas – rizikas būtina laiku identifikuoti ir analizuoti.
3. Reakcija į pastebėtą riziką.
4. Rizikos priėmimas – įmonėje sukuriamas toks valdymo procesas, kurio metu reaguojant į riziką ji sumažinama tiek, kad taptų priimtina.“

Rizikos analizės vadove pabrėžiama, kad atliekant rizikos analizę, būtinai reikia įvertinti rizikos pavojaus, saugos valdymo priemonių, pažeidžiamumo, verčių ir rizikos tarpusavio sąsajas (Vageris, 2005, 160 p). Kaip matoma 6 paveiksle, visi komponentai yra graudžiai susiję. Pavojaus agentas kelia tiesioginę grėsmę, grėsmė išnaudoja pažeidžiamumą, kuris sąlygoja riziką. Bet kokia riziką gali pažeisti inventorių ir taip sąlygoti pažeidžiamumą. Pažeidžiamumas gali atsverti saugiklį, kuris tiesiogiai veikia pavojaus agentą.



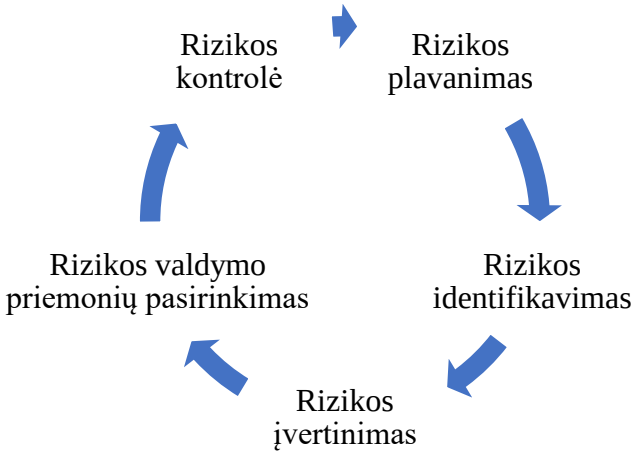
Šaltinis: Vageris R. Rizikos analizės vadovas, 2005

6 pav. Skirtingų saugos komponentų tarpusavio sąsajos

Taigi, visi šie komponentai turi būti išnagrinėti ir kiek įmanoma daugiau apsaugoti, kad atsiradus grėsmei, būtų galima atsaugoti ir sumažinti pažeidžiamas sritis.

Pasak Buškevičiūtės bei Leškevičiūtės (2008) rizikos valdymo procesą sudaro 5 pagrindiniai etapai (žr. 7 pav.):

1. *Rizikos planavimas*. Jis apima organizacijos pasirengimą rizikos valdymui, kai turėtų būti apibrėžiami veiksmų planai, užtikrinamos sąlygos vidiniams ir išoriniams duomenims rinkti, paskiriami atsakingi asmenys.
2. *Rizikos identifikavimą*. Pagrindinis šio etapo tikslas – galimybė nustačius problemas pereiti prie konkrečių veiksmų, kurie sudaromi atsižvelgiant į praeities duomenis, statistinę informaciją ir praktines žinias.
3. *Rizikos įvertinimas*. Jis gali būti kokybinis bei kiekybinis. Šio etapo metu nustatoma rizikos tikimybė, kad konkreti grėsmė gali paveikti tam tikras veiklos sritis ir sukelti nepageidaujamų padarinių.
4. *Rizikos valdymo priemonių pasirinkimas*. Atrenkamos toleruotinos ir netoleruotinos rizikos rūšys, kurios leidžia užtikrinti veiksmingą apsaugą.
5. *Rizikos kontrolės etapas*. Šiuo metu fiksuojami nukrypimai, kurie įvertinami prasidėjus kitam valdymo ciklui, arba atliekamas operatyvus koregavimas paties ciklo metu.



Šaltinis: sudaryta autorės pagal Buškevičiūtę ir Leškevičiūtę, 2008

7 pav. Rizikos valdymo etapai

Kaip teigia rizikos Buškevičiūtės ir Leškevičiūtės (2008): pagrindinis rizikos valdymo tikslas - tai rizikos išvengimas. Rizikos valdymo metodai yra sudėtingi ir jei įmonė netinkamai juos taikys – tai gali atnešti nuostolius.

Apibendrinus Mackevičiau, Giriūno (2014), Kanapickienės (2009), Mills (2001) ir kt. mokslinėje literatūroje nagrinėtų autorių darbus, galima teigti, kad siekiant išvengi rizikos, turi būti nustatytos visos potencialios rizikos, po to atliekama jų analizė, įvertinimas ir sudaromi aiškūs ir konkretūs rizikų valdymo planas.

1.4. Verslo rizikos vertinimo samprata

Rizikos vertinimas – tai bendras rizikos įvertinimo bei rizikos analizės procesas. Rizikos analizė sudaro pagrindą rizikos ir jos sukeltų nuostolių vertinimui, valdymui ir rizikos priėmimui. Pasak Vagerio (2005), siekiant priimti sprendimus dėl rizikos kontrolės yra vertinama rizika. Autorius išskiria rizikos analizę į dvi atšakas – tai kokybinę ir kiekybinę. Skirtumas tarp šių atšakų yra labai paprastas. Kokybinės rizikos analizė metu taikomos nematerialiosios verčių išraiškos (kaip pvz., duomenų praradimas), o kiekybinės – analizuojamiems potencialiems nuostoliams, komponentams siekiama suteikti skaitines vertes (kaip pvz., išreiškiant piniginiais vienetais - eurais).

Remiantis R. Vagerio (2005) teiginiais apibendrintai galima teigti, kad kokybinė rizikos analizė apima rizikos identifikavimą ir jos rūšių klasifikavimą, riziką sukeliančių veiksnių nustatymą, rizikos įvertinimo tikimybę bei rizikos galimų nuostolių įvertinimą.

Skirtingi autoriai, tokie kaip Čepinskis ir Raškinis (2005), Jordan (2013), Tepman (2002) ir kt., siūlo įvairius rizikos vertinimo proceso etapus. Bet lyginant minėtų autorių verslo rizikos vertinimo etapus galima teigti, kad rizikos vertinimas turi vykti tokiais etapais:

1. Atliekamas rizikos tyrimas.
2. Rizikos veiksnių identifikavimas.
3. Rizikos valdymo būdų nustatymas, kuris dažniausiai apima rizikos mažinimo būdų taikymą.

1.5. Rizikos valdymo standartai

1.5.1. COSO ERM standartas

Pagrindinis COSO ERM (angl. COSO Enterprise Risk Management – Integrated Framework, toliau – COSO ERM) standarto tikslas – taikantis prie organizacijos tikslų, padėti įmonės vadovams geriau susitvarkyti su rizika. COSO ERM akcentuojamas lankstus rizikos vertinimo modelis, pagal kurį vertinamas visas bendras įmonės rizikos valdymo procesas, o ne sutelkiamas dėmesys į konkrečias veiklos rizikos valdymo proceso dalis. Šio standarto dokumente nurodoma, kad įmonės rizikos valdymo sistemą sudaro

tiek galimybės, tiek rizika, kurios gali turėti įtakos vertės kūrimui ir jos palaikymui, ir yra apibūdinamas taip: „Organizacijos rizikos valdymas – tai organizacijos valdybos, vadovybės ir kitų darbuotojų vykdomas procesas, taikomas strategijai nustatyti. Procesu siekiama identifikuoti potencialius įvykius, galinčius turėti neigiamą įtaką įmonei, taip pat valdyti riziką, kad ji neviršytų rizikos toleravimo laipsnio bei pagrįstai užtikrinti organizacijos tikslų įgyvendinimą“ (COSO 2004).

Šaltinis: sudaryta autorės remiantis Stasytytė V. ir Aleksienė L., 2015

8 pav. COSO ERM standartą sudarantys veiksniai

Stasytytė ir Aleksienė (2015) straipsnyje pažymi, kad remiantis COSO ERM modeliu, įmonių rizikos valdymą sudaro aštuoni tarpusavyje susiję veiksniai (žr. 8 pav.):

1. Vidinė aplinka – tai aplinka, kurioje įmonės darbuotojai vykdo savo įsipareigojimus siekdami bendrų tikslų.
2. Tikslų nustatymas – įmonė privalo nusistatyti tikslus, suderintus su jos misija ir rizikos apetitu, t. y. įvertinus, koks rizikos lygis jai priimtinas.
3. Įvykių identifikavimas – vidiniai ir išoriniai įvykiai, kurie gali turėti įtakos, siekiant įmonės numatytų tikslų. Įtaką gali būti išskirta kaip grėsmė ar galimybė įmonei.
4. Rizikos įvertinimas – rizika analizuojama atsižvelgiant į tikimybę bei poveikį įmonei.
5. Reagavimas į riziką – siekdama valdyti riziką įmonė turi nusistatyti, kaip reaguoti į ją – prisiimti, išvengti, sumažinti ar pasidalyti rizika.
6. Kontrolės veiksmai – kontrolės sistema, kuri užtikrina, kad procesai vykdomi siekiant įgyvendinti įmonės tikslus.

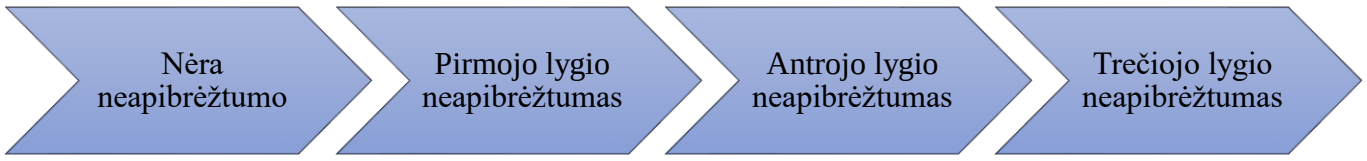
7. Informacija ir komunikavimas, kuri turi esminę reikšmę įmonės veiklos vykdymui bei valdymui. Vadovybei turi būti laiku pateikiama išsami, aktuali, patikima ir teisinga informacija.
8. Stebėsena – kontrolės sistema turi būti nuolatos stebima ir esant poreikiui - keičiama.

Kadangi šį modelį sudaro daug elementų, tai gali lemti sunkesnį pritaikymą ir įdiegimą praktikoje, ypač mažesnėse įmonėse.

Svarbiausias ir aktualiausias kontrolės elementas – rizikų vertinimas. Anksčiau rizikų vertinimas buvo atliekamas fragmentiškai, o šiuo metu, esant naujoms tendencijoms ekonomikoje, įmonių vadovybės naudoja naują paradigmą: rizikos valdymą, atliekamą integruotai, nuolatos bei visoje organizacijoje. Modelyje pateikiama sistema yra atvira, t. y. be grįžtamojo ryšio. COSO ERM modelyje reikalaujama tik įvertinti riziką, tačiau nėra tolesnių rizikos valdymo elementų.

COSO ERM modelyje pateikiama pagrindinė rizikų valdymo nuostata: kiekvienos įmonės veiklos tikslas – visoms suinteresuotoms šalims sukurti pridėtinę vertę. Tačiau įmonės veikloje nuolat susiduriama su neapibrėžtumais, todėl vadovybės užduotis yra patvirtinti sprendimus apie neapibrėžtumo lygį, kurį įmonė gali priimti. Pasak Čepinskio ir Raškinio (2005) išskiriami keturi neapibrėžtumo lygiai (žr. 9 pav.):

1. Nėra neapibrėžtumo – galima numatyti tikslius rezultatus;
2. Pirmojo lygio neapibrėžtumas – žinomi rezultatai bei šių rezultatų tikimybė;
3. Antrojo lygio neapibrėžtumas – kai žinomi rezultatai, bet nežinoma jų tikimybė;
4. Trečiojo lygio neapibrėžtumas – rezultatai nėra visiškai aiškūs, o jų tikimybė taip pat nežinoma.



Šaltinis: sudaryta pagal Čepinskis, Raškinis, 2005

9 pav. Neapibrėžtumo lygiai

Taip pat būtina pažymėti, kad neapibrėžtumas, viena vertus, gali turėti įtakos rizikai, kita vertus - atverti galimybes, todėl jis gali sukelti tiek vertės padidėjimą, tiek sumažėjimą. COSO ERM modelis atskleidžia šiuos momentus:

1. Rizikų valdymas yra platesnis procesas nei vidaus kontrolė, kuris apima bei išplečia vidaus kontrolės sistemą, kuri keičiama į efektyvesnę formą, labiau orientuotą į rizikas.

2. Vidaus kontrolė labiau skirta taktiniams tikslams siekti, o rizikos valdymas – užtikrinti tikslų pasiekimą strateginiu ir taktiniu lygmeniu.
3. COSO ERM išskirti trys nauji komponentai: *kriterijai*, vertinantys rizikos valdymo efektyvumą: tikslų nustatymas (tikslai turi būti nustatyti prieš tai, kai vadovybė pradės identifikuoti potencialius įvykius, kurie galimai turės įtakos tikslų pasiekimui); *įvykių identifikavimas* (turi būti nustatyti vidiniai ir išoriniai įvykiai, kurie gali turėti įtakos įmonės tikslų pasiekimui); *reakcija į riziką* (parenkamas toks reagavimo į riziką būdas, kuris sumažintų riziką iki leidžiamo rizikos lygio ir priimtinos rizikos).

Taigi, šis rizikos valdymo medelis išsiskiria lankstumu, požiūriu į įmonės strategiją ir procesus. Atsižvelgiant į jo lankstumą, modelį galima suderinti su kitais rizikos valdymo standartais, tokiais kaip ISO31000. COSO ERM pagrinde apima kontrolės aplinką, informacijos sistemas, kontrolės veiksmus ir jos stebėseną. Šį modelį sudaro daug elementų, kurie yra sunkiau pritaikomi mažesnėse įmonėse, tad reikia atsižvelgti į tai ir naudojant šį modelį, kaip buvo pastebėta nagrinėjant mokslinę literatūrą, jį koreguoti pagal įmonės poreikius, pavertus mažiau formaliu.

1.5.2. ISO 31000 standartas

ISO 31000 yra pripažintas tarptautinis rizikos valdymo standartas, kurį 2009 m. paskelbė Tarptautinė standartų organizacija. Jis gali būti naudojamas visoms organizacijoms, apima visų rūšių riziką bei taikomas neatsižvelgiant į jų tipą ar dydį, veiklą, vietą. Tarptautinis standartas rekomenduoja įmonėms kurti, diegti ir nuolat tobulinti sistemą, kurios tikslas - integruoti rizikos valdymo procesą į visą organizacijos struktūros valdymą, politika, vertybės ir kultūrą. Šis standartas sukurtas taip, kad galėtų būti naudojamas ir suprantamas ne tik profesionaliems rizikos valdytojams, bet ir visiems, kurie valdo riziką. ISO 31000 padeda organizacijoms sukurti rizikos valdymo strategiją, kad būtų galima veiksmingai nustatyti ir sumažinti riziką, taip padidinant tikimybę pasiekti savo numatytų tikslų ir padidinant įmonės turto apsaugą. Jo pagrindinis tikslas - sukurti rizikos valdymo kultūrą, kurioje darbuotojai ir suinteresuotos šalys suvoktų rizikos stebėjimo ir valdymo svarbą. ISO 31000 įdiegimas taip pat padeda organizacijoms matyti tiek teigiamas galimybės, tiek neigiamas pasekmes, kurios susijusios su rizikomis ir leidžia, paskirstant išteklius, priimti labiau veiksmingesnius sprendimus (International Organization for Standardization, 2018).

ISO 31000 verslo rizikos valdymo sistema turi daug pranašumų, tokių kaip laiko taupymas, sudėtingų situacijų valdymas, plati galimybių ir grėsmių analizė ir kt. (2 lentelė).

2 lentelė. „ISO 31000“ verslo rizikos valdymo sistemos pranašumai

1.	Suteikia veiklos efektyvumą ir padidina efektyvumą
2.	Ugdo pasitikėjimą akcininkų rizikos valdymu
3.	Pagerina valdymo sistemos našumą ir atsparumą
4.	Apsaugo įmonę augdamas ir efektyviai reaguodamas į pokyčius
5.	Padidina tikimybę pasiekti tikslus
6.	Iniciatyvus valdymas
7.	Padeda išgryninti žinojimą apie poreikį nustatyti ir pašalinti riziką visoje organizacijoje
8.	Pateikiama galimybių ir grėsmių analizė
9.	Padeda pagerinti suinteresuotųjų šalių pasitikėjimą ir pasitikėjimą
10.	Patikimų sprendimų priėmimo ir planavimo pagrindo suteikimas
11.	Numato sudėtingas situacijas ateityje
12.	Prevencija užtikrinama prieš kylant rizikai
13.	Laiko taupymas
14.	Apsaugo nuo suvirinimo atliekų
15.	Užtikrina, kad rizika būtų išlaikoma pagrįstu lygiu
16.	Verslo tęstinumo užtikrinimas

Taigi, ISO31000 standartas siūlo bendras rizikos valdymo gaires ir siekia tobulinti ir gerinti jau esamus rizikos valdymo procesus. Šis standartas nustato visų formų rizikos valdymo principus neatsižvelgiant į įmonės dydį.

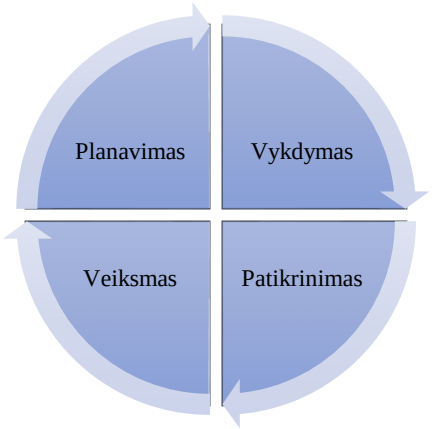
1.5.3. ISO 27005 standartas

„Informacinės saugos valdymo sistema (ISVS) gali būti suprantama kaip atitinkamų politikų rinkinys, kuris yra susietas su informacijos saugumo valdymu (priemonių). Sąvokos atsiradimas siejamas su ISO/IEC 27001 standartu“ (Januta, Marozas, Goranin, 2011, 110 p). Pagrindinis šios sistemos tikslas – organizacija turi sukurti, įgyvendinti bei palaikyti sistemas ir nuoseklius procesus. Šios sistemos turi būti skirtos informacinio turto rizikai valdyti ir tokiu būdu užtikrintų priimtiną organizacijoje saugumo lygi, kuris apimtų tiek konfidencialumą, tiek vientisumą bei prieinamumą. ISVS modelių yra ir daugiau, ne tik ISO/IEC 27000 šeimos standartai. Jie aprašomi ISF (Informacijos saugumo forumo) organizacijos „Standard of Good Practice (SOGP)” standarte ir kituose paplitusiuose standartuose, kaip COBIT ar ITIL.

ISO/IEC 27000 serija (taip pat vadinama „ISMS standartų šeima“ arba „ISO27K“) sudaro informacijos saugumo standartai. Juos paskelbė Tarptautinė standartizacijos organizacija (ISO) ir Tarptautinė elektrotechnikos komisija (IEC). Šie standartai apibrėžia rekomendacijas dėl informacijos saugumo valdymo, kurios sudarytos remiantis geriausiomis ISVS praktikomis. Straipsniuose Inter Cert (2017) nurodo, kad ISO 27001 turi daug privalumų, tokių kaip:

- Galimybė nustatyti rizikas bei priimti veiksmus jų optimizavimui ar pašalinimui;
- Adaptavimo lankstumas bet kuriai veiklos sričiai;
- Klientų ar suinteresuotų asmenų pasitikėjimas, jų duomenų saugumo užtikrinimo dėka;
- Privilegijuoto tiekėjo statusas, kuris garantuojamas standarto atitikimui;
- Lūkesčių patenkinimas standarto reikalavimams atitikimo dėka.

Serijos standartai yra plačios apimties. Jie gali būti taikomi tiek mažose, tiek didelėse įmonėse. Visos organizacijos yra skatinamos vertinti savo informacijos saugos riziką ir, jei reikia, įgyvendinti atitinkamą informacijos saugos kontrolę pagal organizacijos poreikius, naudojant gaires bei pasiūlymus. ISVS sąvoka apima nuolatinį grįžtamąjį ryšį ir veiklos tobulinimą, kuris paremtas W. Edvardo Demingo ciklu (žr. 10 pav.).



Šaltinis: A. Januta, 2011, p.110

10 pav. W. Esvardo Demingo ciklas

A. Januta (2011) išskiria 4 pagrindinius veiksnius:

- Planavimą – ką ir kada reikia padaryti, kas turi tai padaryti ir kokiomis priemonėmis;
- Vykdymą – suplanuotų darbų atlikimas;
- Patikrinimą – įvertinamas darbų atlikimas ir nustatoma ar pasiekti laukiami rezultatai.

- Veiksmą – koreguojami planai, įvertinant patikrinimo etape gautą informaciją.

Literatūros šaltiniuose pastebima, kad visos *planuok – veik – tikrink – vykdyk* ciklo būsenos gali veikti nesinchroniškai ir skirtingais laiko momentais. ISO/IEC 27002 (17799:2005) standarte yra nustatyti 133 saugumo valdymo svertai, kurie sudaryti iš 12 pagrindinių kategorijų:

1. Rizikos vertinimas.
2. Saugumo politika.
3. Organizacinės saugos priemonės.
4. Turto klasifikavimas ir priežiūra.
5. Personalo sauga.
6. Fizinė apsauga.
7. Ryšiai ir operacijų valdymas.
8. Priėjimo kontrolė.
9. Sistemos sukūrimas ir priežiūra.
10. Informacinės saugos incidentų valdymas.
11. Komercinės veiklos nepertraukiamumo valdymas.
12. Atitiktis.

Visos kategorijos turi tikslus ir papildomus saugumo kontrolės mechanizmus. Standarte taip pat yra pateikiamos valdymų svertų gairės ir aprašyta, kaip tai įgyvendinti. Kiekviena įmonė privalo įvykdyti struktūrinį informacinės saugos rizikos vertinimo procesą, kuris padėtų nustatyti konkrečius reikalavimus, prieš pasirenkant kontrolės mechanizmus ir atitiktų jų tam tikras iškylančias situacijas.

ISO/IEC 27000 standartų seriją sudaro šie, viešai publikuojami, standartai:

1. ISO/IEC 27000 – ISVS apžvalga ir žodynas.
2. ISO/IEC 27001 – ISVS reikalavimai.
3. ISO/IEC 27002 – Informacijos saugos valdymo praktikų rinkinys.
4. ISO/IEC 27003 – ISVS įgyvendinimo gairės.
5. ISO/IEC 27004 – Informacijos saugos valdymo priemonės.
6. ISO/IEC 27005 – Informacijos saugos incidentų valdymas.
7. ISO/IEC 27006 – Reikalavimai organizacijoms, atliekančioms auditą bei sertifikuojančioms informacijos saugos valdymo sistemas.

ISO/IEC 27005 standarto vadove pateikiamos gaires, kaip sukurti sisteminį informacijos saugumo rizikos valdymo metodą, kuris būtinas norint nustatyti organizacinius poreikius, susijusius su informacijos saugumo reikalavimais, ir sukurti efektyvią informacijos saugumo valdymo sistemą.

1.5.4. OCTAVE metodas

Octave - tai informacijos saugumo rizikos nustatymo ir valdymo sistema. Šis metodas apibrėžia išsamų vertinimo metodą, kuris leidžia organizacijai nustatyti informacijos turtą, kuris yra svarbus organizacijos misijai, grėsmes šiam turtui ir pažeidžiamumą, dėl kurio tam turtui gali kilti grėsmė. Pasak Roman Jevsejev (2019) metodas sukurtas „Carnegie Mellon“ universiteto Programinės įrangos inžinerijos institute. Autorius taip pat išskiria pagrindinius OCTAVE modelio elementus (Jevsejev, 2019):

- Kritinio informacijos turinio nustatymas;
- Kritinio informacijos turto grėsmių nustatymas;
- Pažeidžiamumų, kurie susiję su kritiniu informacijos turtu, nustatymas;
- Rizikos vertinimas, susijęs su kritiniu informacijos turtu.

OCTAVE yra lanksti ir savarankiška rizikos vertinimo metodika. Šis metodas gali būti pritaikytas daugumai organizacijų, tačiau labiau tinkamas didelėms įmonėms. Nedidelė (3 - 5) žmonių komanda iš operatyvinių, verslo padalinių ir IT skyriaus dirba kartu, kad patenkintų organizacijos saugumo poreikius. Komanda remiasi daugelio darbuotojų žiniomis, kad nustatytų esamą saugumo būklę, svarbių išteklių rizikas ir nustatytų saugumo strategiją. Šis metodas yra labai populiarus ir todėl yra sukurta paprastesnė jo versija, kuri yra skirta mažoms įmonės, tai OCTAVE-S versija. Nepaisant metodo žinomumo ir plataus naudojimo, autoriai Alberts ir Dorofee (2001) pažymi, kad nors ir OCTAVE metodas atitinka rizikos kriterijus, bet rizikų stebėjimas yra jo silpnoji pusė. „Metodas nesuteikia aiškaus nurodymo, kaip pastebėti pavojų, tačiau pabrėžia rizikos dėl pavojaus egzistavimo svarbą“ (Alberts ir Dorofee, 2001, p. 2).

1.5.5. ISO 31000 ir COSO metodų palyginimas

Išanalizavus vienus iš populiariausių literatūros šaltiniuose pateikiamų rizikos valdymo metodų (COSO ERM , ISO 31000, ISO 27005 , OCTAVE) pastebima, kad visi metodai turi panašumų ir skirtumų. ISO 27005 ir COSO ERM standartai yra daugiausiai aptarinėjami mokslinėje literatūroje, bet retai išskiriami šių dviejų standartų skirtumai ir panašumai.

ISO 31000 ir COSO standartus sukūrė skirtingos organizacijos, turinčios skirtingą profesinę kvalifikaciją. Tačiau abu standartai turi tiek panašumų, tiek skirtumų.

Galima išskirti šiuos panašumus:

- *Abu standartai išplečia rizikos valdymo sritį*. Užuot tik apribojęs neigiamą riziką, abu standartai padeda jomis vadovautis ir iš dalies skatina rizikuoti.

- *Abi versijos skirtos kaip gairės*. Nei ISO 31000, nei COSO nėra skirti organizacijai gauti atitikties sertifikatą. Ypač ISO 31000 modelis skirtas pateikti aukšto lygio nurodymus dėl rizikos valdymo sistemos komponentų. Kaip dažnai minima mokslinėje literatūroje, rizikos valdymas turėtų būti pritaikytas kiekvienai organizacijai, todėl logiška, kad standartai iš tikrųjų yra gairės. Organizacija yra atsakinga už standarto pritaikymą praktikoje, atsižvelgiant į įmonės poreikius.
- *Abi dabartinės versijos yra patobulintos*. Atnaujinta COSO versija buvo išleista 2017 m., o atnaujinta ISO 31000 – 2018 m.
- *Abu standartai į rizikos valdymą įtraukia sprendimų priėmimo procesus.* ISO 31000 ir COSO minima, kad rizikos įtraukimas į organizacijos sprendimų priėmimo procesą yra pagrindinė dalis siekiant užtikrinti, kad organizacija prisiima reikiamą riziką reikiamu kiekiu.

Išskirti standartų skirtumai:

- *Struktūra.* Naujausia ISO 31000 versija yra labiau standartizuota nei COSO. ISO standartas yra tik 16 puslapių, o COSO yra daugiau nei 100 puslapių. Iš to galima daryti išvadą, kad ISO 31000 yra lengviau suprantamas.
- *Geografija*. Kadangi COSO (organizacija, o ne standartas) ištakos yra orientuotos į vidaus kontrolės sistemos teikimą, COSO ERM standartas yra labiau skirtas apskaitos ir audito žmonėms. Nors 2017 m. atnaujintoje versijoje didesnis dėmesys skiriamas strategijai, ji vis dar labai nukreipta į audituojamą ERM pusę. ISO 31000 yra parašytas visiems, kurie domisi rizikos valdymu. Daugelis organizacijų pasirenka būtent šį standartą dėl daugybės kitų ISO standartų, kuriuos jos gali naudoti.
- *Pagrindinis dėmesys.* COSO daugiau dėmesio skiria bendram įmonės valdymui, o ISO daugiausia dėmesio skiria rizikai ir jos įtraukimui į strateginio planavimo procesą.
- *Sistema ir procesai*. ISO aiškiai atskiria sistemą ir procesą. Nors jame aprašytas procesas vis dar yra labai tradicinis, jame išsamiau aprašomas tikrasis rizikos nustatymo, vertinimo ir kt. pagrindas.
- *Rizikingas apetitas.* Pradiniame ISO rizikos valdymo standarte, rizikos apetito sąvoka nebuvo paminėta. 2018 m. versijoje trumpai paminėta rizikos „kriterijų“ tema, tačiau minima minimaliai. 2017 m. COSO versijoje apetitas rizikuoti aptariamas daug plačiau ir pateikiama daug vaizdinių rizikos sąvokų pavyzdžių.

1.5.6. IT sektoriuje naudojami rizikos standartai

Informacinių sistemų ir technologijų plėtros intensyvumas vis labiau reikalauja kiek įmanoma lankstesnių ir adaptyvių kibernetinės saugos užtikrinimo metodų taikymo būdų. Vienas iš šių metodų yra

informacinių technologijų (IT) rizikos vertinimas. „IT rizika – tai neigiamą poveikį organizacijai ir jos sistemai turintis ir su informacinių technologijų naudojimu susijęs įvykis, kuris atsitinka tuomet, kai grėsmė realizuojasi dėl sistemoje esančių silpnų ir lengvai pažeidžiamų vietų“ (Stoneburner, Goguen, Fering, 2002, p. 46).

IT rizika yra tiesiogiai susijusi su informacinėmis technologijomis. Informacija vertinama kaip svarbus ir vertingas turtas: ekonomikos augimas, žinių tobulinimas ir skaitmeninė revoliucija paskatino organizacijas plačiau naudoti informacijos, apdorojimo ir informacinių technologijų priemones (Jevsejev, 2019). Pasak autoriaus Stulz (2008) rizikos valdytojai kartais daro klaidų vertindami nuostolių tikimybę ar dydį. Tai atsitinka dėl neteisingo rizikos veiksnių paskirstymo. Įstaigai, kuri turi daugybę rizikų ir skirtingų pozicijų gali būti neteisingai įvertinta.

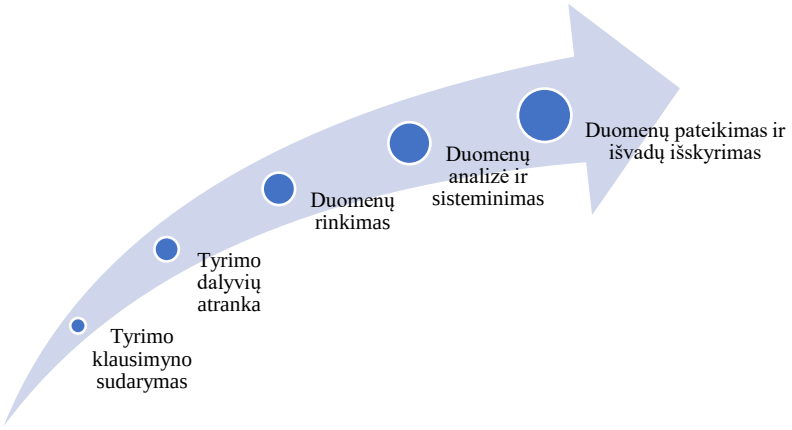
Daugumos įmonių rizikos vertinimą apsunkina tai, kad didelis programinės įrangos kiekis kuriamas nesivadovaujant IT rizikos vertinimo metodologija bei informacijos saugumo standartais. Dėl šios priežasties gali būti netinkamai nustatomas IT rizikos lygiai ir atitikties laipsnis konkrečiam standartui. Labiausiai naudojami metodai, kuriais remiantis vykdoma kibernetinės rizikos analizė (Chandrashekhar, Sachin Kumar ir Huded, 2015), yra CORAS, OCTAVE, CRAMM.

Kiekvienas metodas turi savo teigiamų ir neigiamų savybių. Skirtingoms organizacijoms metodai gali būti taikomi kaip atskira platforma, kuri adaptuojama pagal organizacijos poreikius, atsižvelgiant į organizacijos priklausomybę nuo informacijos.

Taigi, IT sektoriuje dažniausiai naudojami rizikos valdymo metodai yra CORAS, OCTAVE, CRAMM. Viena iš tokio pasirinkimo priežasčių yra, kad visi šie modeliai yra orientuoti į kibernetinį saugumą, kuris yra tiesiogiai susijęs su informacinėmis technologijomis.

2. MAŽŲ IR VIDUTINIŲ ĮMONIŲ RIZIKOS VERTINIMO TYRIMAS

Siekiant gauti tikslius duomenis, ar tarptautiniai rizikos valdymo modeliai yra sklandžiai naudojami, buvo pasirinktas kiekybinio tyrimo metodas – internetinė anketinė apklausa. Naudojant šį metodą ir norint sumažinti paklaidų ar netikslumų tikimybę, respondentai į klausimus atsakė anonimiškai, o apklausos laikas nebuvo ribojamas. Respondentams elektroniniu paštu buvo išsiųstos suformuotos anketos.



Šaltinis: sudaryta autorės

11 pav. Kiekybinio tyrimo procesas

Kiekybinio tyrimo tikslas – išsiaiškinti, ar siūlomi tarptautiniai standartai yra paklausūs bei tinkami naudoti mažoms ir vidutinėms įmonėms.

Duomenų rinkimo metodai. Siekiant ištirti, ar siūlomi tarptautiniai standartai yra paklausūs ir naudojami mažose ir vidutinėse įmonėse, atliktas kiekybinis tyrimas, o duomenų rinkimui pasirinktas anketinės apklausos metodas.

Šis apklausos metodas yra vienas iš populiariausių duomenų rinkimo metodų. Gaižauskienės ir Mikėnės (2014) klausimyną, kaip apklausos priemonę, išskirią kaip pagrindinį šio metodo privalumą. Anketinė apklausa padeda surinkti vertingą informaciją, kuri atskleisdama realybę, parodo reikšmių ryšius ir gauta informacija leidžia atskleisti tikrovę (Tijūnėlienė, Virbalienė, 2006).

Tyrimo respondentai. Atliekant tyrimą tikslinę respondentų grupę sudaro IT sektoriaus įmonių direktoriai, skyrių vadovai bei rizikos valdymo specialistai. Norint išvengti netikslumų ir sumažinti netikslumo riziką, respondentai buvo atrinkti remiantis šiais kriterijais:

- Įmonė įregistruota Lietuvoje.
- Teikia paslaugas, susijusias su informacinėmis technologijomis.

- Įmonė dirba iki 250 darbuotojų.

Tyrimas atliekamas visoje Lietuvoje, neišskiriant regionų ar miestų. Įmonė gali teikti paslaugas ne tik Lietuvos rinkoje, tačiau svarbu, kad verslo subjektas būtų registruotas Lietuvoje. Pasirinktos įmonės, kuriose dirba iki 250 darbuotojų, kadangi tyrimas akcentuotas į mažas ir vidutines įmones.

Imties dydžio nustatymas. Atliekant tyrimą, svarbu užtikrinti pakankamą imties reprezentatyvumą populiacijai. Tyrimo imtis apskaičiuota, remiantis Paniotto formule:

$$n = \frac{1}{\Delta^2 + \frac{1}{N}}$$

n – reprezentatyvios imties dydis

Δ - imties paklaidos dydis (10 proc.)

N – populiacijos dydis

Kiekybiniame tyrime populiacijos dydis (N) – mažos ir vidutinės įmonės, teikiančios IT paslaugas. Paklaidos dydis pasirinktas 10 proc. siekiant gauti kuo tikslesnius duomenis.

Naudojant Paniotto formulę:

$$n=1/(0.12+1/6948) = 98.$$

Gautas imties dydis yra 98. Tai reiškia, kad apklausoje būtina surinkti 98 respondentų atsakymus, norint, kad gauti rezultatai būtų reprezentatyvūs duomenų imčiai.

Tyrimo vykdymo laikotarpis. Internetinė apklausa buvo išsiųsta 2022 m. sausio 8 d. elektroniniu paštu. Apklausos nuoroda buvo aktyvi iki 2022 m. vasario 8 d. Internetinė apklausos nuoroda buvo išsiųsta 500 įmonių, kurios buvo atrinktos pagal aukščiau nurodytus kriterijus. Viso užpildytų anketų skaičius – 109 iš kurių 7 buvo užpildytos netinkamai, galimos naudoti – 101. Nustatytas imties dydis yra mažesnis už surinktų respondentų atsakymų skaičių, kas nustato, kad apklausos rezultatai yra reprezentatyvūs duomenų imčiai ir galimi analizuoti.

Gautų duomenų analizės metodas. Tyrimo metu gauti duomenys bus analizuojami naudojantis Microsoft Excel programa.

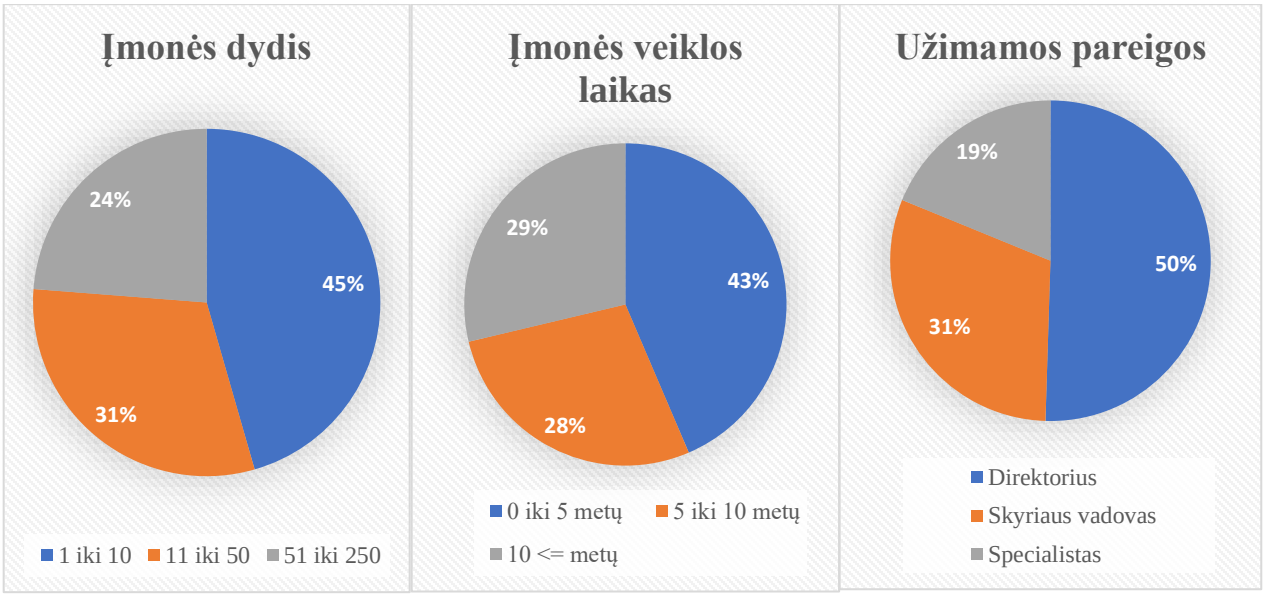
Atrinktų įmonių apklausos būdas. Netiesioginė įmonių apklausa, pateikiant jiems užpildyti elektroninę anketos versiją. Anketos talpinimo vieta – www.apklausos.lt internetinis puslapis. Anketos nuoroda buvo siunčiama atrinktoms įmonėms pagal anksčiau išvardintus kriterijus. Laiškuose su anketos nuoroda, buvo nurodyta, kad ši apklausa skirta įmonių direktoriams, skyrių vadovams ar rizikos valdymo

specialistams. Dalyvavusių ir nedalyvavusių, bet atrinktų tyrimui įmonių pavadinimai ar kiti duomenys, vadovaujantis duomenų apsaugos įstatymu ir profesinės etikos sumetimais, yra neatskleidžiami.

2.1.Kiekybinio tyrimo rezultatai

Tyrimo imties charakteristika. Respondentai anketoje nurodė įmonės dydį (žr. 12 pav.). Didžioji dalis respondentų (45 proc.) dirba labai mažose įmonėse (darbuotojų skaičius siekia iki 10 asmenų), 31 proc. sudaro mažos įmonės (darbuotojų skaičius iki 50 asmenų) ir 24 proc. sudaro vidutinės įmonės (darbuotojų skaičiuos nuo 51 iki 250 asmenų). Kadangi anketa buvo orientuota į būtent tokio dydžio įmones, manoma, kad anketos rezultatai bus patikimi ir galimi naudoti tolimesniuose šio darbo dalyse.

Taip pat, didžioji dalis apklausoje dalyvavusių įmonių yra jaunos, iki 5 metų veikiančios įmonės, jos sudarė 43 proc., 29 proc. Respondentų sudarė 10 ir daugiau metų turinčios įmonės, o likusius – nuo 5 iki 10 metų turinčios įmonės.

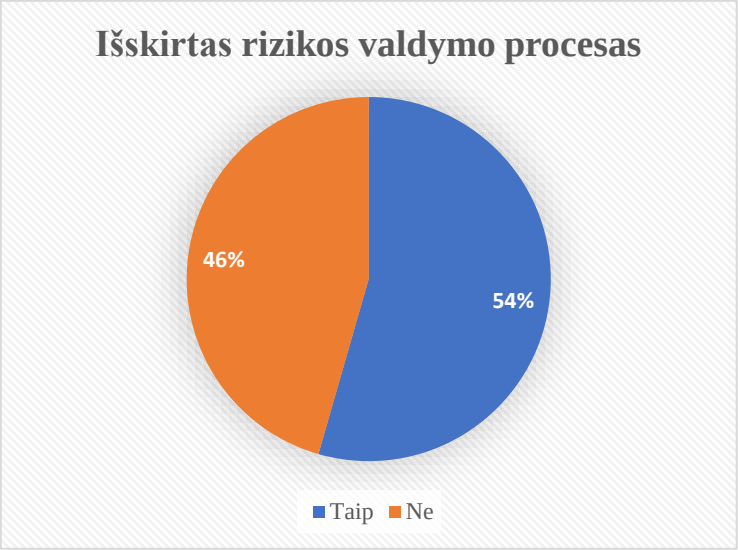


Šaltinis: sudaryta autorės

12 pav. Tyrimo charakteristika

Anketą pildė įmonių darbuotojai, iš jų 50 proc. sudarė įmonės direktoriai, 31 proc. – skyriaus vadovai, o tik 19 proc. – rizikos valdymo specialistai. Visi anketoje užduodami klausimai buvo susiję su rizikos veiklos ataskaitomis. Pirmas užduotas klausimo tikslas buvo išsiaiškinti, kiek įmonių išskiria veiklos rizikos valdymo procesus. Tyrime gauti rezultatai yra apylygiai: 55 įmonės, kad sudaro 54 proc. respondentų atsakė,

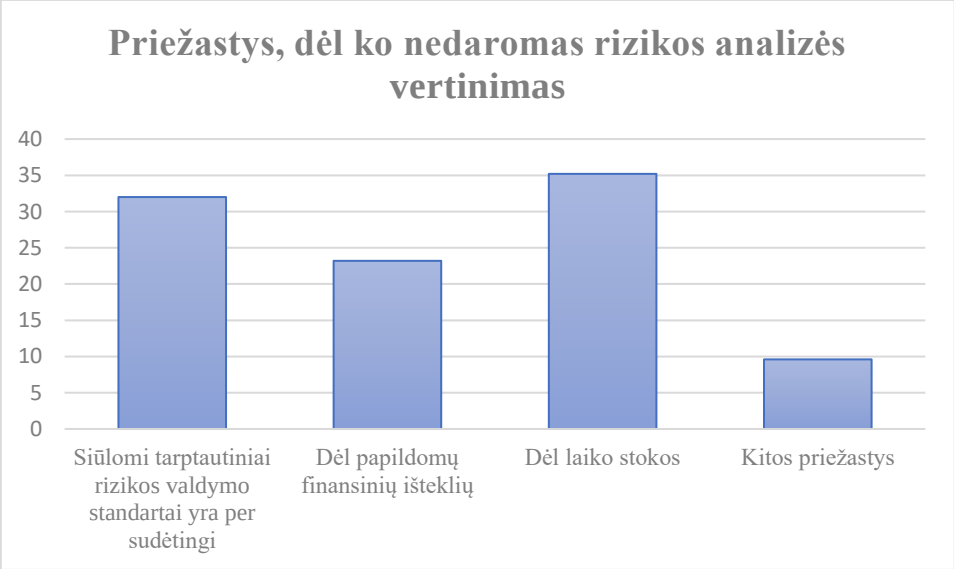
kad rizikos valdymo procesus išskiria, kas reiškia, kad yra sudaromos rizikos valdymo ataskaitos, o 46 proc. – kad ne (žr. 13 pav.).



Šaltinis: sudaryta autorės

13 pav. Rizikos valdymo proceso būvimas įmonėje

Anketoje buvo pateiktas klausimas, kurio tikslas išsiaiškinti, dėl kokių priežasčių įmonės nedaro rizikos valdymo ataskaitų. Respondentas galėjo pasirinkti vieną ar kelias priežastys, kurios buvo nurodytos apklausoje (žr. 14 pav.).



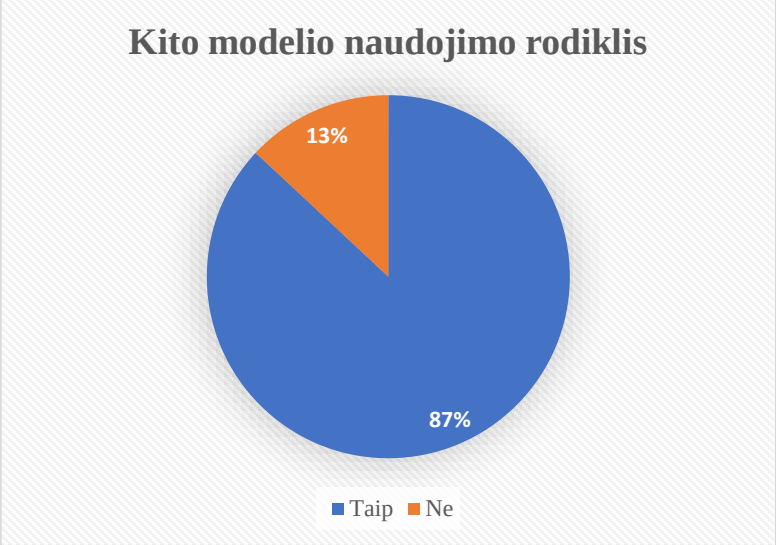
Šaltinis: sudaryta autorės

14 pav. Rizikos analizės nevykdymo priežastys

Didžioji dalis įmonių, kurios dalyvavo apklausoje – 35.2 proc. nurodė, kad rizikos valdymo ataskaitų neatlieka dėl laiko stokos, 32 proc. – pasirinko, kad siūlomi tarptautiniai rizikos valdymo standartai yra per sudėtingi, 23.2 proc. nurodė papildomų finansinių išteklių priežastį, o tik 9.6 proc. pasirinko kitas priežastis.

Apžvelgiant į apklausoje gautus rezultatus, buvo pastebėta, kad beveik 90 proc. įmonių, kurios neatlieka rizikos valdymo ataskaitų yra labai mažos arba mažos įmonės, kurios pasirinko laiko stokos ir tarptautinių rizikos valdymo standartų sudėtingumo priežastys.

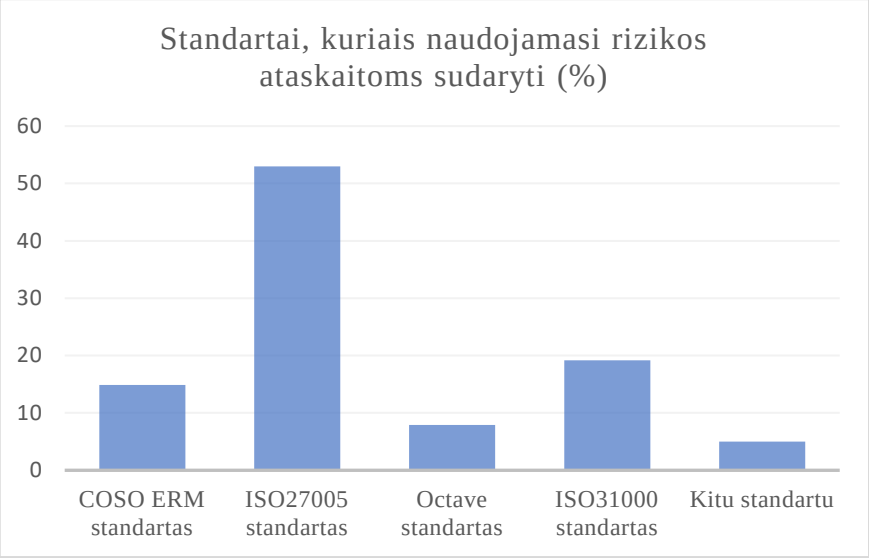
Norint įsitikinti, kad įmonės ne dėl nenorėjimo ar nesugebėjimo neatlieka rizikos valdymo analizių, buvo užduotas klausimas „Ar atliktumėte rizikos analizės vertinimą, jei būtų pasiūlytas lengvesnis vertinimo modelis?“ (žr. 15 pav.). Į šį klausimą atsakė visi respondentai, kurie buvo pasirinkę, kad neatlieką rizikos vertinimo ataskaitų. Rezultatuose matoma, kad net 87 proc. įmonių naudotų lengvesnį rizikos valdymo modelį savo įmonėse, o likę 13 proc. to nedarytų. Atsižvelgiant į šį rodiklį, analizuojant gautus rezultatus pastebėta, kad įmonės, kurios neturi ir nenorėtų turėti rizikos valdymo procedūrų nebuvo patyrusios nuostolių dėl galimų rizikų.



Šaltinis: sudaryta autorės

15 pav. Rizikos modelio naudojimo rodiklis

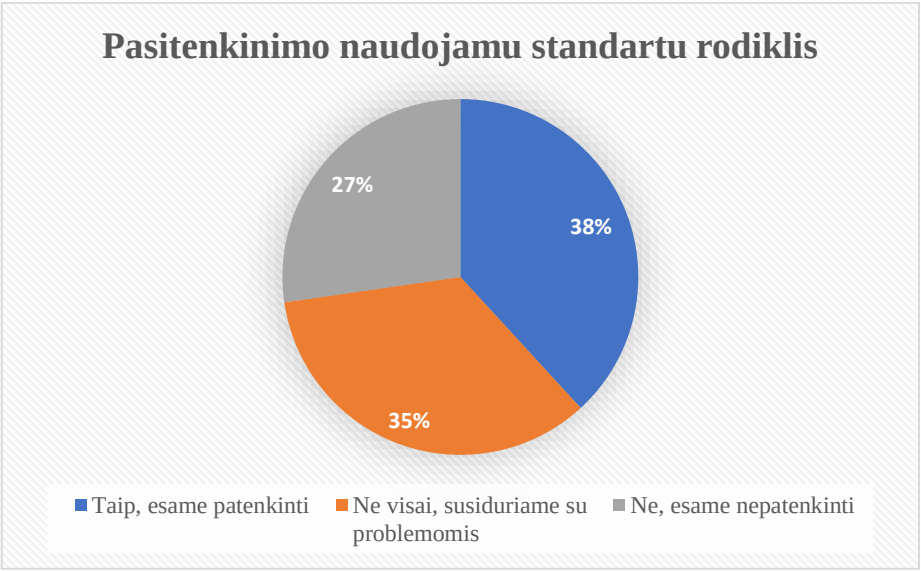
Tai patvirtina ir apklausoje matomi rezultatai, kad 58,4 proc. įmonėms teko susidurti su grėsmėmis, dėl kurių jos patyrė nuostolius, o 41,6 proc. – neteko. Iš to galima daryti išvada, kad būtent dėl šios priežasties, įmonės nemano, kad joms reikalingos rizikos analizės, tačiau daroma prielaida, kad ateityje tai gali pasikeisti.



Šaltinis: sudaryta autorės

16 pav. Rizikos valdymo analizės standartų naudojimas

Atsižvelgus į mokslinės literatūros analizėje pastebėtas rizikos valdymo modelių tendencijas, buvo užduotas klausimas, susijęs su įmonių pasirenkamais rizikos valdymo modeliais (žr. 16 pav.). Kadangi, net 54 proc. respondentų įmonėse išskiria rizikos valdymo procesus, buvo užduotas klausimas, kokiais rizikos valdymo modeliais remiantis, įmonės atlieka rizikos vertinimus. Didžioji dalis (53 proc.) apklaustųjų pasirinko, kad naudojasi ISO27005 standartu.



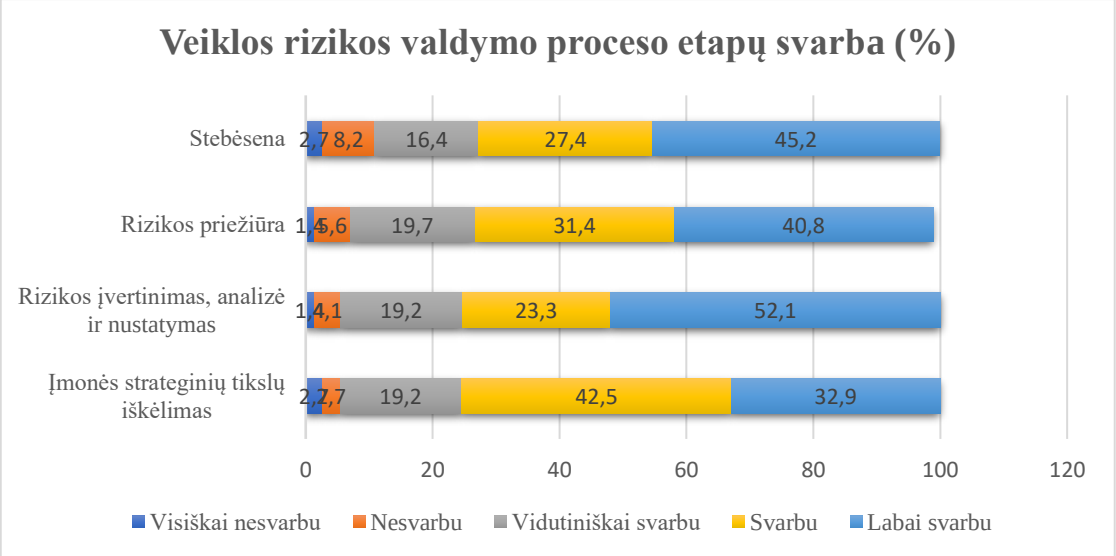
Šaltinis: sudaryta autorės

17 pav. Pasitenkinimo naudojamu standartu rodiklis

Tai galėjo turėti įtakos, kad apklausa buvo orientuota į IT įmones, o nagrinėjant literatūros šaltinius, pastebėta, kad šis modelis yra vienas iš dažniausiai naudojamų tokio tipo įmonėse. Kitų modelių pasirinkimas buvo panašus: 19,2 proc. naudoja ISO31000 standartą, 14,9 proc. – COSO ERM, 7,9 proc. – Octave, o 5 proc. respondentų pasirinko, kad naudojasi kitu standartu.

Naudojamu standartu ne visos įmonės yra pilnai patenkintos (žr. 17 pav.). Iš 55 įmonių, kurios išskiria rizikos vertinimą tik 21 įmonė juo yra patenkinta, o tai nesudaro net pusės bendro procento (38 proc.). 19 respondentų pasisakė, kad naudojamu standartu yra ne pilnai patenkinti ir susiduria su problemomis, o 15 atsakiusiųjų yra nepatenkinti naudojamu standartu. Bendroje sumoje nepasitenkinimo balas yra aukštesnis už pasitenkinimo: 62 nepasitenkinę ir 38 proc. – pasitenkinę naudojamu standartu.

Pagal gautus rezultatus matoma, kad ne visos įmonės išskiria rizikos valdymą, bet tai nereiškia, kad įmonėje šis procesas nevyksta. Pasitaiko atveju, kai įmonėse rizikos aptariamos žodžiu ir susitariama, ką reikėtų daryti, jei įvyktų vienas ar kitas įvykis. Klausimyne buvo paprašyta įvertinti nuo 1 iki 5 balų naudojamo tarptautinio standarto ataskaitos atlikimo sunkumo lygi: net 80 proc. respondentų pasirinko nuo 4-5 balų, kas reiškia, kad atlikimo sunkumo lygis yra aukštas. Taip pat vertino papildomų finansų ir papildomų žmogiškųjų išteklių reikalavimą – šie rezultatai buvo panašūs: apie 70 proc. respondentų pasirinko nuo 3 iki 5 balų, o ataskaitos sudarymo laiko sąnaudas nuo 4 iki 5 balų įvertino net 85 proc. apklaustų įmonių. Iš šių rezultatų galima daryti preliminarią išvadą, kad didžioji dalis įmonių, kurios naudojasi tarptautiniais ar kitais rizikos valdymo standartais, turi skirti papildomo laiko, žmogiškųjų ir finansinių išteklių, kas mažai įmonei jau būtų papildoma finansinė našta.



Šaltinis: sudaryta autorės

18 pav. Rizikos valdymo proceso etapų svarba

Respondentai taip pat vertino veiklos rizikos proceso etapų svarbą pagal Likerto skalę. Likerto skalėje reikėjo išskirti kiekvieno etapo svarbą kaip visiškai nesvarbu, nesvarbu, vidutiniškai svarbu, svarbu ir labai svarbu (žr. 18 pav.). Pagal gautus rezultatus matyti, kad visi etapai yra svarbūs. Mažoji dalis respondentų pasirinko, kad visi etapai yra visiškai nesvarbūs arba nesvarbūs. Didžiausia svarba išsiskyrė rizikos įvertinimo, analizės ir nustatymo rodiklis, jį kaip labai svarbų išskyrė 52 proc. respondentų, antras pagal „labai svarbų“ rodiklį išskirtas stebėsenos etapas.

Atlikus kiekybinį tyrimą, pastebėta, kad ne visos apklaustos mažos ir vidutinės įmonės išskiria rizikos valdymo ataskaitas. Didžioji dalis įmonių, šiuo metu neturinčių rizikos ataskaitų dėl laiko stygiaus, papildomų finansinių išlaidų, per sunkių siūlomų tarptautinių modelių ar kitų priežasčių, pažymėjo, kad atlikinėtų rizikos analizės vertinimą, jei būtų pasiūlytas lengvesnis vertinimo būdas. Atsižvelgus į visus gautus rezultatus, galima daryti išvadą, kad labai mažoms, mažoms ir vidutinėms įmonės pasiūlius lengvesnį ir patrauklesnį rizikos analizės valdymo modelį, dauguma įmonių jį išbandytų ir įsivertintų rizikas, ko pasekoje, naujai siūlomas modelis būtų paklausus ir naudojamas.

2.2. „X“ įmonės naudojamas rizikos valdymo standartas

Įmonė „X“ yra vidutinio dydžio IT įmonė, kuri teikia bankinių mokėjimų sprendimų paslaugas. Organizacija yra sukaupusi daugiau nei 15 metų patirtį rinkoje ir dirba ne tik Lietuvoje, bet Baltijos regione, Ukrainoje, Lenkijoje, Airijoje ir Rumunijoje.

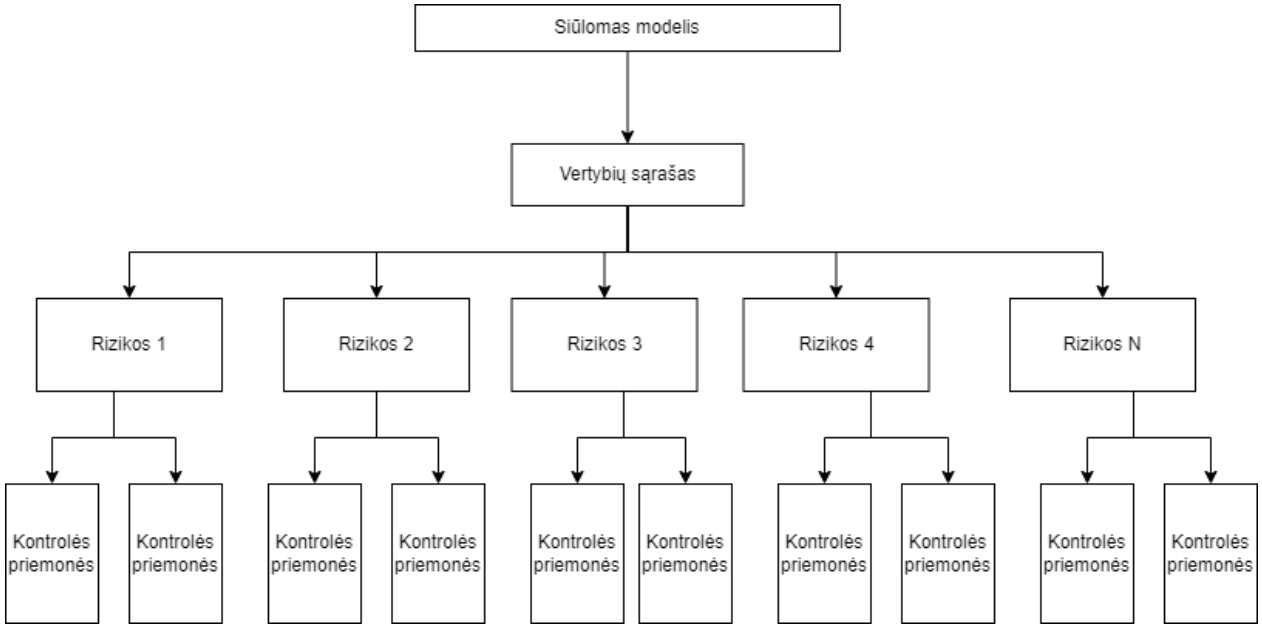
Įmonė visą veikimo laikotarpį rizikos ataskaitų sudarymui rinkosi ISO/IEC 27005 (Information technology – Security techniques – Information security risk management). Šiuo metodu kiekvienais metais vertindama įmonės rizikas organizacija „X“ užtikrina teikiamos paslaugos saugumą bei nenutraukiamą jos veikimą. Šios metodikos pasirinkimą lėmė tai, kad ISO 27005 metodiką yra tarptautinis standartas, vienas iš PCI DSS standarto rekomenduojamų metodikų bei suderinamas su kitais ISO/IEC 27000 serijos standartais ir ISO/IEC 27001 ISVS diegimo procesu.

Rizikos analizės vertinime dalyvauja 5 darbuotojai, kurie atstovauja skirtingus padalinius. Paskutinę 2020 m. ataskaitą (dėl įvesto karantino grupės narių skaičius buvo minimizuotas) vertino 3 darbuotojai. 2020 m. rizikos ataskaitą sudarė 72 puslapiai, kuriuose smulkiai išnagrinėtos šios įmonės galimos grėsmės. „X“ įmonė nesamdo išorinio darbuotojo sudaryti rizikos ataskaitas ir naudoja savo turimus resursus. Tokios apimties ataskaitai parengti skiriama daug laiko ir tai eikvoja įmonės finansinius resursus. Vidutinio dydžio įmonė galėtų rinktis ir paprastesnį rizikos ataskaitų valdymo standartą, kuris nereikalautų tiek laiko sąnaudų, bet taip pat užtikrintų tikslią rizikos valdymo procedūrą.

2.3. Naujas metodas, orientuotas į smulkias ir vidutines įmones, ir jo taikymas

Mažoms ir vidutinėms įmonėmis, kaip ir buvo pastebėta nagrinėjant mokslinę literatūrą bei atlikus empirinį tyrimą, standartiniai rizikos analizės standartai dažnai būna per sunkūs ir reikalauja papildomų tiek finansinių, tiek žmogiškųjų išteklių. Nereikia sudėtingos sistemos, norint pagerinti ar palaikyti organizacijos saugos aplinką, tačiau kiekvienam organizacijos vadovui reikia įrankių, kurie parodytų, kur skirti laiko ir išteklių, kad sumažintų galimą riziką įmonei. Taip rizikos vertinimai gali atskleisti pagrindinius šio sprendimų priėmimo proceso veiksnius. Supaprastinus ir išskyrus tik svarbiausias vertybes ir jų rizikos veiksnius, mažos ir vidutinės įmonės galėtų lengviau identifikuoti rizikas ir taip sutaupyti turimus finansus bei išgryninti įmonės turimas grėsmes ir jų kontrolės priemones.

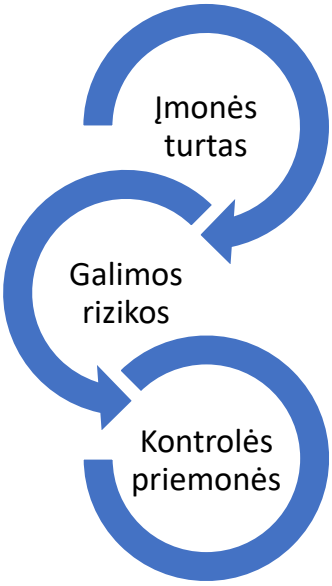
Siūlomas naujas metodas yra mažiau formalus ir struktūrizuotas bei lengviau pritaikomas. Jis sudarytas atsižvelgiant tik į svarbiausius rizikos valdymo veiksnius. Metodas yra mažesnės apimties, tikslus ir specialistų pagalbos nereikalaujantis standartas, kuris padėtų visoms mažoms ir vidutinės įmonės bei jų vadovams lengvai išanalizuoti rizikas. Naujas metodas būtų sudarytas iš trijų etapų: turtinių vertybių išskyrimo, jų rizikos veiksnių sąrašo ir kontrolės priemonių. Pateikiamoje schemoje aiškiai matoma trumpa ir lengvai suprantama schema, kuri parodo, kaip šis modelis veikia (žr. 19 pav.).



Šaltinis: sudarytas autorės

19 pav. Siūlomo metodikos modelio schema

Identifikuojant turimą turtą, vertybes ir rizikas, automatiškai išsiskirtų ir kontrolės priemonės. Tokią rizikos analizę galėtų atlikti įmonės vadovas, akcininkas ar kitas pareigas einantis darbuotojas, tad nereikėtų samdyti išorinių darbuotojų ar specialistų. Siūloma metodika parengta atsižvelgiant į pagrindinius rizikos analizės valdymo standartus, tik yra išgryninta, sutrumpinta ir labiau pritaikyta mažoms bei vidutinėms įmonės. Ji sudaryta iš įmonės turto identifikavimo sąrašo, galimų rizikų ir kontrolės priemonių (žr. 20 pav.).

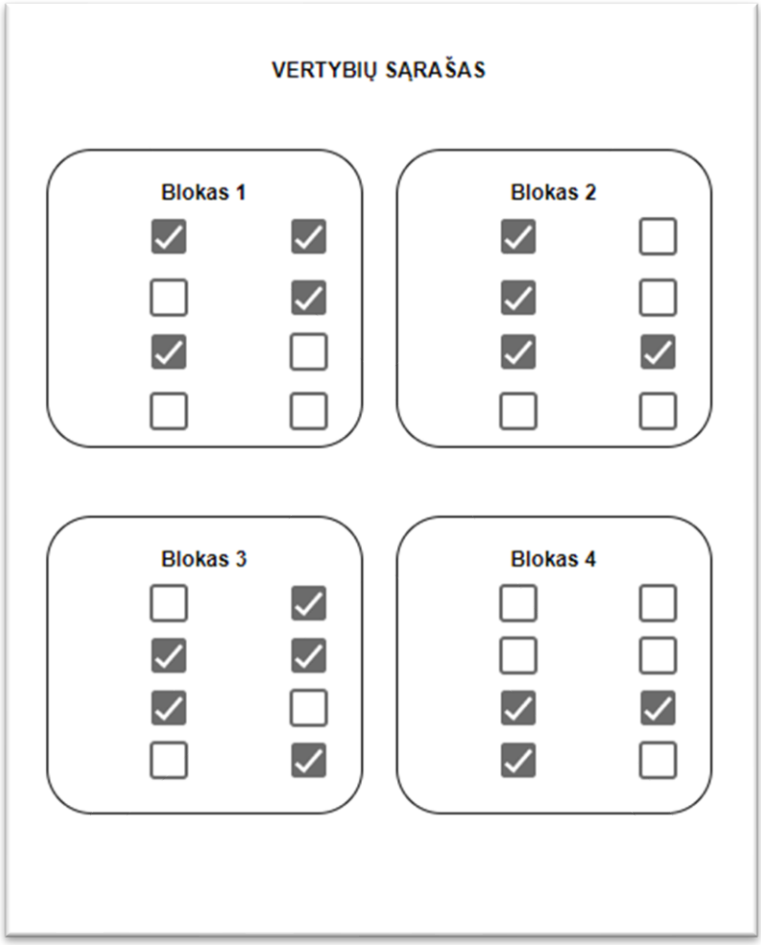


Šaltinis: sudaryta autorės

20 pav. Naujo metodo sandara

Darbuotojas, dirbantis įmonėje galėtų be papildomų vidinių ar išorinių konsultantų sužymėti sąrašuose jų įmonės turimą turtą, rizikas ir taip nusistatyti galimų rizikų kontrolės priemones. Toks metodas galėtų apsaugoti smulkias ir vidutines įmonės nuo galimų rizikų be papildomų išlaidų.

Darbuotojas ar įmonės vadovas, pradėdamas rizikos analizę pagal naująjį metodą, pradžioje turi sužymėti, kokios turimos turtinės vertybės yra toje įmonėje (žr. 21 pav.). Šis pirmas žingsnis (turto identifikavimas) yra bene svarbiausias, siekiant tinkamai sukurti saugos kontrolę. Kaip pastebėta nagrinėjant mokslinę literatūrą: blogai įsivertinus svarbias turtines vertybės rizikos valdymo proceso pradžioje – galimas netikslumas visoje rizikos valdymo ataskaitoje, ko pasekoje atsiranda tikimybė verslo tęstinumo trikdžiams. Vertingas turtas yra techninė įranga, programinė įranga, duomenys ir kt. Tai apima organizacijos verslo serverius, klientų duomenis, kredito kortelių informaciją, svetaines, programas, komercines paslaptis ir patentuotą informaciją, sutartis ir kt. Turėtų būti identifikuojamas toks turtas, kurio praradimas ar sugadinimas gali sukelti piniginių nuostolių arba sistemos prastovas.



Šaltinis: sudaryta autorės

21 pav. Vertybių sąrašo pavyzdys

Taigi, reikėtų apibrėžti, kas yra svarbus turtas ir kaip vadovybė jį skirsto pagal kategorijas (didelį, vidutinį ar nedidelį), atsižvelgdama į jo piniginę vertę arba teisinę padėtį. Norint tai padaryti, reikia apriboti, kuris turtas laikomas „kritiniu“. Naujame modelyje yra išskiriamas pagrindinis turtas, kurį gali turėti bet kuri įmonė. Turtas gali būti tiek neapčiuopiamas, tiek apčiuopiamas (Gregg, 2007). Apčiuopiamas turtas yra fiziniai įrenginiai (pvz. kompiuterinė įranga, informacinės sistemos, kt.), o neapčiuopiamas turtas – tai reputacija, slapta įmonės informacija ir kt. Modelyje jis yra suskirstytas blokais ir pateikiamas vertybių sąrašas, kurį sudaro:

Pirmas blokas. Į šį bloką įeina infrastruktūriniai veiksniai, dėl kurių neveikimo gali nutrūkti įmonės paslaugų tiekimas, vidinis darbas. Veiksniai:

- Interneto svetainė

- Ryšio linijos (Internet / ryšio linijos su klientais)
- Elektros tiekimas
- Elektroninis paštas
- Verslo valdymo sistema

Antras blokas. Antrą bloką sudaro techninė įranga. Išskiriamos pagrindinės techninės įrangos, kurių saugumas yra ypač svarbus ir atsitikus galimai rizikai, nuostoliai gali būti didžiuliai. Veiksniai:

- Serveriai
- Saugyklos
- Kondicionavimo sistema (fizines saugos priemones)
- Gesinimo sistema
- Video stebėjimo sistema
- Praėjimo kortelių sistema
- Tinklo įranga

Trečias blokas. Šį bloką sudaro pagrindiniai įmonės duomenys ir įmonės arba trečių šalių naudojama programinė įranga. Veiksniai:

- Techninė dokumentacija / sutartys
- Darbo tvarkos / Procedūros
- Įmonės programinė įranga
- Trečių šalių programinė įranga

Ketvirtas blokas. Šis blokas yra įvairus ir jame pateikiamos kitos vertybės, kurios gali turėti įtakos rizikai susidaryti. Įeinantys veiksniai:

- Patalpos (serverinė)
- Žmogiškieji ištekliai (darbuotojai/vadovai)
- Nedokumentuotos žinios
- Kompiuteriai ir jo priedai
- Nešiojami media (raktai, mob.telefonai)

Sužymėję, kokias turtines vertybės įmonė turi, antras žingsnis būtų tų vertybių rizikos (grėsmių) vertinimas. Grėsmė yra viskas, kas gali išnaudoti pažeidžiamumą, kad pažeistų įmonės saugumą ir pakenktų jos turtui. Dažniausiai pasitaikančios grėsmės gali būti fizinės (pvz., sena įranga), programinės įrangos projektavimo ar konfigūracijos problemos (pvz., per dideli prieigos leidimai), žmogiškieji veiksniai (pvz.,

neapmokyti ar neatsargūs darbuotojai, kišimasis, perėmimas ar apsimetimas), licencijų valdymas, gaisras ir kt. Modelyje rizikos sąrašai pateikiami labiau apibendrinti ir išskirstyti pagal vertybių grupes (1 vertybių blokas siejamas su "Rizika 1", 2 vertybių blokas - su „Rizika 2" ir pan.). Tokiu būtų, nepasirinktos vertybės nebebūtų analizuojamos darbuotojo ir sumažėtų netikslingos rizikos analizės galimybė bei būtų sutaupytas laikas. Rizikos sąrašai susidarytų iš kelių grupių, iš kurių sektų tų rizikų kontrolės priemonės. Kontrolės priemonių gali būti įvairių, nuo stebėjimo iki fizinių apsaugos priemonių, tačiau išanalizavus turimą turtą, jo grėsmes ir išskyrus kontrolės priemones, galima minimalizuoti arba iš viso eliminuoti galimą žalą. Pirminiame siūlomame modelyje pateikiamos keturios rizikos valdymo grupės (kontrolės priemonės įvardintos šalia rizikų):

„Rizika 1" (grėsmės susijusios su linijos ryšiu ir elektra):

3 lentelė. Rizikų pasirinkimas nr. 1

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Fizinis linijos pažeidimas	Dubliavimas
	Konfigūracijos klaida	Profilaktiniai darbai, monitoringas
	Ryšio linijos kokybė	Monitoringas, reguliari sutarčių peržiūra ir operatoriaus keitimas
	Priklausomybė nuo konkretaus fizinės ryšio linijos tiekėjo	Sąrašo sudarymas, „Provider Independant" IP gavimas
	Nepastebimas perjungimas į rezervinę liniją	Monitoringas
	Elektros šuoliai, elektros dingimas	UPS, profilaktiniai darbai, srovės lygintuvai
	Elektros įvado gedimas	Monitoringas, procedūros, įvado dubliavimas
	Šlamštas (ang. Spam) per e-paštą	SPAM filtrai, antivirusinės sistemos, vartotojų mokymai
	Pašto persipildymas	Monitoringas, resursų planavimas
	Pranešimų pametimas	Procedūros, rezervinis kopijavimas, mokymai
	Sukčiavimas (ang. Phishing) per e-paštą	Mokymai darbuotojams, antivirusinės sistemos, papildomi reguliarūs priminimai apie pavojaus svarbą

Šaltinis: sudaryta autorės.

Pasirinkus vertybes iš pirmo vertybių bloko, išsiskirtų šios rizikos. Dauguma išvardintų galimų rizikų kontrolės priemonių panašios, tai yra monitoringas, procedūros, dubliavimai. Šių galimų rizikų valdymo

priemonės reikalauja ir papildomų finansinių šaltinių: norint išvengti elektros šuolių ar elektros dingimo padarinių, reikėtų įsigyti UPS (nepertraukiamo maitinimo šaltinius), kurie palaikytų elektros tiekimą dingus elektrai ir nenutrauktų darbo. Taip pat papildomų išlaidų reikalauja ir antivirusinės, kurios sumažintų rizikas susijusias su el. paštu ar nesaugiomis svetainėmis. Kitos išvardintų rizikų valdymo priemonės, tokios kaip procedūrų aprašai ar monitoringas, nereikalauja papildomų išlaidų.

„Rizika 2“ (grėsmės susijusios su serverinėmis sistemomis):

4 lentelė. Rizikų pasirinkimas nr. 2

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	RAM gedimas	Atsarginės dalys, procedūros, monitoringas
	Maitinimo bloko gedimas	Atsarginės dalys, procedūros, monitoringas
	Gaisras	Gesintuvai, procedūros, veiklos atstatymas rezervinėje serverinėje, duomenų dubliavimas kitose patalpose, verslo atstatymo planas, draudimas
	Force majeure (nenugalima jėga)	Veiklos atstatymas rezervinėje serverinėje, draudimas
	Įrangos (serverių) nusidėvėjimas	Profilaktiniai darbai, monitoringas, įrangos atnaujinimas
	Dujų nutekėjimas	Procedūros, monitoringas
	Kamerų perdengimas kitomis kameromis	Papildomų kamerų montavimas
	Praėjimo kortelių pametimas	Procedūros (blokavimo), kontrolinė peržiūra

Šaltinis: sudaryta autorės.

Antrasis grėsmių blokas yra tiesiogiai susijęs su rizikomis nr. 2. Prie grėsmių dažnu atveju išsiskiria tokios pačios kontrolės priemonės kaip atsarginės dalys, procedūros ir jų aprašai bei monitoringas. Šios kontrolės priemonės skirtos rizikoms, kurioms galima ruoštis jau iš anksto. Tokios rizikos būtų – RAM gedimas, maitinimo bloko gedimas, dujų nutekėjimas. Šių rizikų valdymą galima apsirašyti ir greitai sustabdyti turint atsargines dalis ar iš anksto nusimatant veiksmų planą. Nors šios kontrolės priemonės gali būti sunkiau įvykdyti dėl reikalaujamų papildomų finansų, tačiau jų ignoravimas ateityje gali atnešti dar didesnius nuostolius.

„Rizikos 3” (grėsmės susijusios su duomenimis ir programine įranga):

5 lentelė. Rizikų pasirinkimas nr. 3

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Įsilaužimas	Tinklo segmentacija, griežta prieigos kontrolė iš išorės
	Netyčinis duomenų nutekinimas	Ryšių su klientais kontrolė, e-pašto ribojimas
	Užsakomosios paslaugos (ang. outsourcing) grėsmės: kodo vagystė, konkuruojančio verslo steigimas, kainų politika, vėlavimas, kompetencijos stoka	SLA, NDA, stebėjimas
	Licencijų valdymas	Centralizuoto sąrašo vedimas, procedūros
	Nusidėvėjimas	Testai
	Nereikalingas informacijos kopijavimas į asmenines laikmenas	Nešiojamų kaupiklių kontrolė
	Netyčinis dokumentų persiuntimas klientams/konkurentams	Ryšių su klientais kontrolė, e-pašto ribojimas
	Procedūrų aprašų trūkumas	Trūkstamų procedūrų sąrašo sudarymas, procesų apibrėžimas
	Darbo tvarkų iškomunikuotos	Mokymai

Šaltinis: sudaryta autorės.

Galimas grėsmes, susijusias su programine įranga suvaldyti yra šiek tiek sudėtingiau. Kontrolės priemonės numato ne tik stebėjimus, bet ir testų atlikimus ar griežtos tvarkos prie prieigų laikymąsi. Šias kontroles priemones įmonės gali apsirašyti ir vykdyti nuolatos, tokiu būtų mažindamos grėsmių lygį ir finansinius nuostolius.

„Rizikos 4” (grėsmės susijusios su patalpomis):

6 lentelė. Rizikų pasirinkimas nr. 4

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Gaisras	Gesintuvai, gesinimo sistema, signalizacija, mokymai
	Užpylimas	Nepratekančios lubos
	Fizinis įsilaužimas	Fizinės apsaugos priemonės

Šaltinis: sudaryta autorės.

Šios rizikos siejamos dalinai su 4 vertybių bloku. Jos apima tik patalpas. Norint apsaugoti patalpas nuo galimų grėsmių, reikia nuolatos daryti profilaktinius darbus, tai yra tikrinti gesintuvus, signalizacijas,

daryti mokymus. Taip pat, įmonės patalpos turi būti apsaugotos su praėjimo kortelėmis, papildomais signalizacijos kodais ir pan. Jei patalpos yra nuomojamos ir nuolat keičiamos – prieš įsikeliant į jas, reikėtų įsitikinti, kad patalpos atitinka rizikos vertinimo procesuose numatomus veiksnius.

„Rizikos 5“ (grėsmės susijusios su žmogiškaisiais ištekliais):

7 lentelė. Rizikų pasirinkimas nr. 5

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Darbuotojų neatėjimas į darbą	Pareigų dubliavimas
	Neteisingos informacijos skleidimas	Mokymai, procedūros
	Netinkamas bendravimas su klientais	Mokymai, procedūros
	Darbuotojų išėjimas	Žinių dokumentavimas, darbo sutarčių sąlygos

Šaltinis: sudaryta autorės.

Rizikos blokas susijęs su žmogiškaisiais ištekliais yra siejamas su 4 vertybių bloku. Pagrindinės rizikos kontrolės priemonės yra mokymai ir tinkamas dokumentavimas. Esant tinkamai supildytiems dokumentams, atsakomybėms ir mokymams, šias rizikas galima sumažinti iki nepastebimų ir darančių mažą įtaką įmonės veiklos tęstinumui.

Taip pat modelyje yra pateikiamos „Rizikos N“ (grėsmės susijusios su bet kokiomis kitomis įmonės vertybėmis ir turtu). Ši naujo modelio dalis nėra baigtinė, o tai reiškia, kad įmonė gali pridėti papildomų rizikos veiksnių ir joms valdyti reikalingų kontrolės priemonių. Pagrindinės vertybės, grėsmės ir kontrolės priemonės yra pateiktos modelyje, tad mažai įmonei gali neprireikti pačiai pildyti sąrašą ir ji gali tikslingai naudotis pateikiamais duomenimis. Esant pildymo poreikiui – reikėtų prie sudarytų blokų pridėti norimus punktus (vertybes, galimas rizikas ir kt.) ir toliau vadovautis modelio schema.

Trečias žingsnis – grėsmių atsiradimo tikimybės nustatymas. Kaip pavyzdys: jei yra žinomas saugos trūkumas senesnėse įmonės naudojamos programinės įrangos versijose, gali kilti grėsmė, kad įsilaužėliai pasinaudos šiuo konkrečiu pažeidžiamumu ir tai pakenks įmonės vidiniai sistemai. Bet, jei organizacija pritaikytų naujausius programinės įrangos pataisymus, kurie išspręstų problemą, pažeidžiamumo išnaudoti nepavyktų ir grėsmė būtų pašalinta. Poveikis parodo, su kiek trikdžių įmonė gali susidurti, jei grėsmė iš tikrųjų atsiras. Sujungus tikimybę ir poveikį, gaunamas liekamosios rizikos įvertinimas. Kiekvienos organizacijos likutinės rizikos įvertinimas gali skirtis atsižvelgiant į tikimybę ir poveikį, kurį sukelia kiekvienas kontrolės trūkumas. Siūlomame modelyje pateikiama, kad kiekvienai vertinamai sričiai gali būti nustatytas grėsmių atsiradimo tikimybės lygis:

- Žemas: mažai tikėtina, kad grėsmė pasitvirtins, rizika gali būti ignoruojama;

• Vidutinis: yra reali galimybė, kad grėsmė pasitvirtins;

• Aukštas: tikėtina, kad grėsmė pasitvirtins.

Pasinaudojus modelyje pateikiame lentele (žr. 8 lent.), galima paprastai nustatyti grėsmės atsiradimo tikimybę kiekvienai vertinamai sričiai.

8 lentelė. Grėsmių tikimybės nustatymas

Vertinimo sritis	Tikimybė	
	Lygis	Balas
Blokas 1	Žemas	1
	Vidutinis	2
	Aukštas	3
Blokas 2	Žemas	1
	Vidutinis	2
	Aukštas	3
Blokas 3	Žemas	1
	Vidutinis	2
	Aukštas	3
Blokas 4	Žemas	1
	Vidutinis	2
	Aukštas	3
Blokas 5	Žemas	1
	Vidutinis	2
	Aukštas	3

Šaltinis: sudaryta autorės.

Įvertinus tikimybę balais reikia sudėti keturis skirtinguose blokuose gautus balus ir susieti su grėsmės atsiradimo lentele. Kaip pvz.: blokas 1 – tikimybė **3**, blokas 2 – **1**, blokas 4 – **2**, o kituose blokuose rizikos buvo nenustatytos, tai bendras gaunamas balas – **6.** Bendra grėsmės atsiradimo balų suma nurodys grėsmės atsiradimo lygį (žr. 9 lentelė).

9 lentelė. Bendras grėsmės atsiradimo balo nustatymas

Bendra grėsmės atsiradimo tikimybės suma	Grėsmės atsiradimo tikimybės lygis
5-6	Žemas
7-9	Vidutinis
10-15	Aukštas

Šaltinis: sudaryta autorės

Jei bendras gautas balas siekia nuo 4 iki 5 balų, grėsmės atsiradimo tikimybė yra maža ir lygis vertinamas, kaip žemas. Gavus nuo 6 iki 8 balų – grėsmės lygis tampa vidutinis, o nuo 9 iki 13 balų – grėsmės lygis yra aukštas ir tai reiškia, kad įmonė turi skirti didelį dėmesį galimoms grėsmėms valdyti.

Nustačius tiek atskiruose blokuose, tiek bendrą grėsmės atsiradimo tikimybės lygį, įmonė gali tikslingai skirti dėmesį toms rizikos grupėms, kuriose rizikos atsiradimo tikimybės lygis yra aukščiausias. Su šiuo paprastu modeliu, kuris nereikalauja didelių pastangų ir papildomų resursų, bet gali apsaugoti įmonę nuo galimų rizikos atsiradimo veiksnių, organizacija sutaupo savo resursus.

Šis modelis, kaip ir buvo minėta anksčiau, labiausiai tinka mažoms ir vidutinėms įmonėms, kurios negali skirti papildomų finansų ir investuoti į rizikos valdymo metodus, kurie reikalautų papildomų išlaidų jų įdiegimui ir išorinių profesionalių darbuotojų samdymui.

2.4. Naujo modelio metodikos pritaikymas „X“ įmonėje

Norint įsitikinti, kad siūlomas rizikos vertinimo modelis, kuris orientuotas į smulkias ir vidutines įmones, veikia, jis išbandytas pritaikyti vidutinio dydžio, anksčiau minėtoje, „X“ įmonėje. Įmonei buvo pateiktas naujo modelio aprašymas ir duoti blankai, kuriuose „X“ įmonė turėjo sužymėti turimas vertybes, grėsmes, rizikos galimybes. Šią rizikos valdymo ataskaitą atliko IT saugos vadovas, kuris yra atsakingas už įmonės rizikos valdymą. Pasiūlymas naujas metodas sudomino įmonę, nes nori išbandyti naujoves ir papildomas privalumas – pasiteisinus modeliui, „X organizacija“ sutaupytų laiko sąnaudas ir greičiau nustatytų galimas rizikos, kurios gali paveikti įmonę. Darbuotojas atrinko, kokias pagrindines vertybės įmonė turi (žr. 2 priedas).

Įmonė pasirinko, kad turi interneto svetainę, ryšio linijas, elektros tiekimą, elektroninį paštą, serverius, kondicionavimo sistemą, video stebėjimo kameras, praėjimo kortelių sistemą, techninę dokumentaciją bei sutartis, įmonės ir trečių šalių programinę įrangą, patalpas, žmogiškuosius išteklius, kompiuterius ir jų priedus bei nešiojamą medią. Organizacija neišskyrė verslo valdymo sistemos, saugyklų, gesinimo sistemos, tinko įrangos ir nedokumentuotų žinių. Taigi, pirmojo žingsnio metu, įmonė pasirinko bent po 1 turimą vertybę iš skirtingų blokų.

Antras žingsnis, ką turėjo atlikti įmonė, tai pažymėti, kokios galimos rizikos jų įmonėje (žr. 2 priedas). Pirmajame bloke didžiąją dalį, t.y. 7/11, galimų grėsmių įmonė pasirinko, tačiau nepažymėjo fizinio linijos pažeidimo, konfigūracijos klaidų, nepastebimo perjungimo į rezervinę liniją ir elektros įvado gedimo. Darbuotojas išskyrė tokias galimas grėsmes (skliaustose pateikiama grėsmių kontrolės priemonės): ryšio linijos kokybė (monitoringas, reguliari sutarčių peržiūra ir operatoriaus keitimas), priklausomybė nuo

konkretaus fizinės ryšio linijos tiekėjo (sąrašo sudarymas, „Provider Independant“ IP gavimas), elektros šuoliai, elektros dingimas (UPS, profilaktiniai darbai, srovės lygintuvai), šlamštas (ang. Spam) (SPAM filtrai, antivirusinės sistemos, vartotojų mokymai), pašto persipildymas (monitoringas, resursų planavimas), pašto persipildymas (monitoringas, resursų planavimas), pranešimų pametimas (procedūros, rezervinis kopijavimas, mokymai), sukčiavimas(Ang. Phishing) per e-paštą (mokymai darbuotojams, antivirusinės sistemos, papildomi reguliarūs priminimai apie pavojaus svarbą).

Antrame bloke „X“ įmonė pasirinko 6/8 galimų rizikų. Kaip rizikomis nepalaikė dujų nutekėjimo ir kamerų perdengimo kitomis kameromis. Kitos galimos rizikos buvo pasirinktos, tai: RAM gedimas (atsarginės dalys, procedūros, monitoringas), maitinimo bloko gedimas (atsarginės dalys, procedūros, monitoringas), gaisras (gesintuvai, procedūros, veiklos atstatymas rezervinėje serverinėje, duomenų dubliavimas kitose patalpose, verslo atstatymo planas, draudimas), Force majeure – nenugalima jėga (veiklos atstatymas rezervinėje serverinėje, draudimas), įrangos (serverių) nusidėvėjimas (profilaktiniai darbai, monitoringas, įrangos atnaujinimas), praėjimo kortelių pametimas (procedūros (blokavimo), kontrolinė peržiūra).

Trečiajame bloke darbuotojas pažymėjo tik 4/9 galimų rizikų. Buvo išskirtas netyčinis duomenų naikinimas (ryšių su klientais kontrolė, e-pašto ribojimas), licencijų valdymas (centralizuoto sąrašo vedimas, procedūros), nusidėvėjimai (testai) ir netyčinis duomenų ar dokumentų perdavimas klientams ar konkurentams (ryšių su klientais kontrolė, e-pašto ribojimas). Įmonei nepasirinkus kitų galimų grėsmių, galima daryti išvadą, kad šiuo metu „X“ organizacija daro mokymus ir turi kitas kontrolės priemones, kurias nuolatos naudoja ir nemano, kad tai gali būti jų įmonės galimos grėsmės.

Ketvirtame bloke buvo pasirinktos 2/3 galimų grėsmių, tai: gaisras (gesintuvai, gesinimo sistema, signalizacija, mokymai), fizinis įsilaužimas (fizinės apsaugos priemonės). Neišskirta grėsmė – užpylimas. Taigi, galima daryti išvadą, kad patalpos, kuriomis naudojasi įmonė, jau yra su nepratekančiomis lubos ir papildomai į šią kontrolės priemonę įmonei nereikėtų investuoti.

Penktame, žmogiškųjų išteklių rizikos galimybių bloke, įmonė pasirinko visas galimas rizikas, t.y. 4/4: darbuotojų neatėjimas į darbą (pareigų dubliavimas), neteisingos informacijos skleidimas (mokymai, procedūros), netinkamas bendravimas su klientais (mokymai, procedūros), darbuotojų išėjimas (žinių dokumentavimas, darbo sutarčių sąlygos). Remiantis nagrinėta moksline literatūra, buvo pastebėta, kad žmogiškieji ištekliai yra labai svarbi galimos rizikos atšaka, tad toks pasirinkimas yra visiškai normalus, norint užtikrinti galimų rizikų valdymo procesą.

Paskutinis siūlomo modelio žingsnis – galimos grėsmių atsiradimo rizikos vertinimo balas. Įmonė „X“ 1, 3, 4 ir 5 grėsmių atsiradimo blokus įvertino kaip žemą (1 balas), o 2 bloką išskyrė kaip vidutinės rizikos (2 balai) (žr. 22 pav.).

Šaltinis: sudaryta autorės

22 pav. „X“ įmonės grėsmių atsiradimo lygis pagal blokus

Sudėjus bendrą grėsmių atsiradimo lygi gautas rezultatas yra 6 ir tai patenka į žemos grėsmės atsiradimo tikimybės lygį. Iš šio gauto balo galime daryti išvadą, kad įmonės „X“ šiuo metu taikomos kontrolės priemonės yra patikimos ir galimos grėsmės valdomos efektyviai. Organizacija turėtų didžiausią dėmesį skirti antrajam - su technine įranga susijusiam blokui. Atsižvengus į tai, kad įmonė atstovauja IT sritį ir yra susijusiu su bankinių mokėjimų sprendimais, tai yra normalu, kad pagrindinės ir didžiausios rizikos gali iškilti būtent šiame bloke ir jam yra reikalingi didžiausia priežiūra.

„X“ įmonė siūlomą rizikos analizės modelį užtruko atlikti per mažiau nei 1 val., kas sutaupė įmonės laiko resursus. Modelio analizė sudarė 5 lapai. Įmonei užteko modelyje siūlomu vertybių ir galimų rizikų sąrašo, tad nereikėjo nieko pridėti.

2.5. Rizikos valdymo ataskaitų palyginimas

Norint įsitikinti, kad siūlomas modelis atskleidė galimas įmonės rizikas taip pat, kaip ir jau naudojamas tarptautinis standartas, buvo pasirinktas lyginamasis metodas. „Lyginimo metodas – sociologinis tyrimas, kai derinama informacija, gauta:

- įvairiais istorinio vystymosi laikotarpiais;

- įvairių socialinių sistemų (institutų, grupių, teritorijų, administracinių vienetų, šalių ir t. t.);
- skirtingų autorių ar tyrimo kolektyvų;
- įvairiais rinkimo ar matavimo metodais“ (Tidikis, R., 2003).

Lyginamojo metodo metu suderinami du ar daugiau objektai ir nustatomi jų panašumai ar skirtumai. Panašiai aprašo ir Jūraitė (2005). Ji savo straipsnyje šią metodą apibūdino taip: „Lyginimas - lyginamojo tyrimo metodologinė esmė – tai metodas, grindžiantis teiginius apie objektų, reiškinių panašumus ir skirtumus. <...> Lyginant nustatomos reiškinių kiekybinės ir kokybinės charakteristikos, konstruojamos analogijos ir klasifikacijos, įvertinamas būties ir pažinimo turinys“ (Juraitė, K., 2005). Pasak Morkevičiaus (2012) „apibendrintai moksle lyginamasis metodas suvokiamas:

- Ryšių (priežastinių sąryšių) tarp reiškinių analizės metodas, kuris remiasi alternatyvių hipotezių apie priežasties ir pasekmės ryšius tikrinimu pasitelkiant empirinius įrodymus;
- Indukcinių išvadų darymo metodas, kurio pagalba atrandami kintamųjų tarpusavio ryšių dėsningumai (reguliarumai)“ (Morkevičius, 2012).

Šiame darbe naudojamos lyginamosios analizės metu lyginama „X“ įmonės rizikos valdymo ataskaita, kuri atlikta su nauju, siūlomu rizikos valdymo modeliu, su jau naudojamu ISO rizikos valdymo modeliu. Esama ataskaita nėra pridedama prie šio darbo priedų, nes tai yra „X“ įmonės konfidenciali informacija, kuri yra naudojama tik vidiniams procesams, norint išvengti trečiųjų šalių galimų kenkėjiškų veiksmų. Siūlomas valdymo modelis, kaip ir minėta anksčiau, taip pat parengtas remiantis lyginimo principu lyginant jau esamus standartus ir išskiriant jų gerąsias praktikas bei atsižvelgiant į empirinio tyrimo rezultatus.

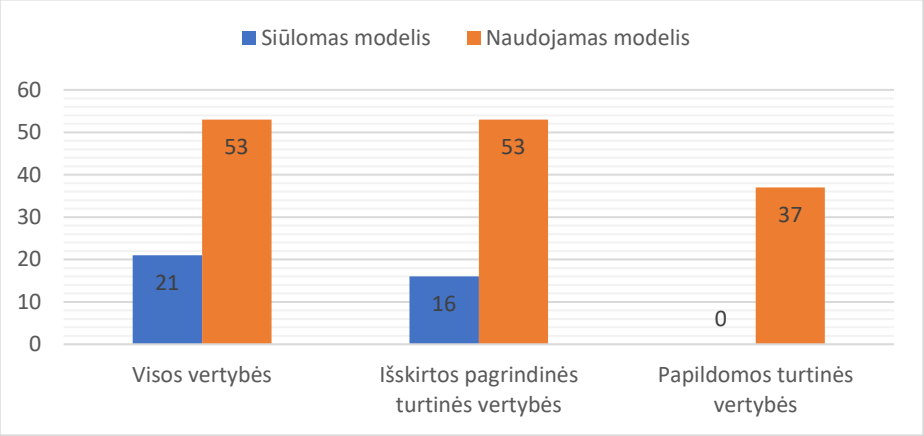
10 lentelė. „X“ įmonės ataskaitos parengimo skirtumai

	Naujas modelis	ISO27005 standartas
Laikas/trukmė	Apie 1 val.	Apie 16 val. (dvi darbo dienos)
Papildomi finansiniai kaštai	Nėra	Nėra
Žmogiškieji ištekliai	1 darbuotojas	3-5 darbuotojų
Profesinis išsilavinimas	Nesvarbu	Rizikos valdymo specialistas

Šaltinis: sudarytas autorės

Lyginant ataskaitų parengimo pagrindinius punktus, matoma, kad siūlomo modelio atlikimo trukmė yra žymiai trumpesnė nei naudojamo ISO modelio. Pagal siūlomą modelį įmonė rizikos ataskaitą parengė per 1 val., o pagal ISO – vidutiniškai užtrunka iki 2 darbo dienų. Abu modeliai nereikalauja papildomų finansinių šaltinių, nes „X“ įmonė turi rizikos valdymo specialistą. Matomas ryškus skirtumas ataskaitų

parengime – siūlomas modelis reikalauja tik 1 darbuotojo darbo, kurio profesinis išsilavinimas nėra svarbus. Šią analizę gali atlikti tiek vadovas, tiek su IT sistemomis dirbantis darbuotojas, o atliekant analizę pagal ISO standartą – įmonė turi paskirti 3 ar daugiau darbuotojus, kurie padėtų ir prisidėtų prie rizikų analizavimo, o bent vienas darbuotojas turėtų būti rizikos valdymo specialistas. Iš dalies – tai ir neigiama naujo modelio savybė, nes rizikos analizavime dalyvauja tik 1 asmuo, tad atsiranda šališkumo tikimybė ar žmogiškoji klaida – praleistos vertybės ar rizikos pasirinkimas.



Šaltinis: sudaryta autorės

23 pav. Rizikos modelių vertybių skirtumai

Siūlomame modelyje pateikiamos 21 vertybės, iš kurių įmonė išskyrė 16 vertybių. Naudojamoje ataskaitoje buvo aprašytos 53 vertybės. Abiejų ataskaitų pagrindinių vertybių sąrašas sutapo, nors turtinių vertybių kiekis skiriasi. Įmonė, siūlomame modelyje, papildomų turtinių vertybių neišskyrė, iš ko galima daryti išvadą, kad ataskaitoje, ruoštoje pagal tarptautinį standartą, įmonė yra apsirašiusi ne tik svarbiausiais vertybes, bet ir smulkesnes, tokias kaip darbo vietos, testiniai duomenys, testinės kortelės, Log failai ir kt. Šių vertybių įmonė neišskiria kaip pagrindinių, o labiau papildomas, nes jų praradimas neatneštų žymių finansinių nuostolių. Be to, įmonė pamini, kad visur yra daromos atsarginės kopijos, tad šių vertybių aprašai nėra dažnai naudojami. Taigi, naujas modelis neišskirdamas papildomo galimų rizikų veiksnių ir kontrolės priemonių gali šiek tiek apriboti rizikos valdymo procesą. Dėl šios priežasties modelis siūlomas mažoms ir vidutinės įmonėms, kur papildomų rizikos veiksnių, dažnu atveju, pasitaiko retai.

Siūlomame modelyje išskiriami penki galimų grėsmių blokai. Pirmame bloke išskiriama 11 galimų grėsmių, antrame – 8, trečiame – 9, ketvirtame – 3, penktame – 4. Kadangi įmonė iš kiekvieno vertybių bloko pasirinko bent po vieną vertybę, ji turėjo peržiūrėti ir visas galimas grėsmes. Kaip jau buvo minėta ankščiau – jei darbuotojas butų praleidęs vieną ar kelis vertybių blokus, jam tolimesnėje ataskaitoje

nereikėtų pildyti su tuo bloku susijusių laukų. Naudojamoje ataskaitoje viso yra išskirta daugiau nei 160 galimų grėsmių, kurias įmonė apsirašo. Dauguma aprašomų galimų grėsmių yra labai žemo rizikos balo. Kaip pati įmonėje teigia, tokios smulkios ataskaitos jai nereikia, ji praktikoje naudoja tik svarbiausius ir didžiausią vertę turinčius rodiklius. Grėsmių ataskaitoje išskiriamos tokios smulkios grėsmės, kaip vandalizmai, nesinaudojimas testavimo istorija, ataskaitų praleidimas ir pan. Šios visos galimos grėsmės įmonės ataskaitoje pažymėtos kaip visiškai toleruojama rizika.

Tiek viename, tiek kitame modelyje pagrindinės kontrolės priemonės prie galimų grėsmių išskiriamos tokios pačios, tačiau jau naudojamame ISO27005 modelyje – jų yra daugiau. Tai galėjo lemti faktas, kad pats standartas yra platesnis ir apima smulkesnes rizikas. Tai yra privalumas lyginant su naujame modelyje esančiomis kontrolėmis. Mažas kontrolinių priemonių buvimas gali sąlygoti rizikos eliminavimo laiką, o tai yra vienas iš neigiamų naujo modelio savybių.

Taigi, abi ataskaitos išskiria tas pačias turtines vertybes ir jų galimas rizikas. Tarptautinis standartas apima ne tik pagrindines galimas grėsmes, bet ir papildomas, tad automatiškai išskiriama daugiau galimų grėsmių ir jų kontrolės priemonių. Naujo modelių pagrindinės teigiamos savybės: laiko, žmogiškųjų išteklių ir finansų taupymas, tačiau atsiskleidė ir neigiama modelio pusė. Kaip neigiamą savybę galima išskirti vieno asmens dalyvavimą rizikų nustatymo etape, o tai gali sąlygoti svarbių turtinių vertybių neišskyrimą, ko pasekoje atsirastų papildomos rizikos grėsmė. Taip pat modelis apima tik pagrindines turtines vertybes, nenustatydamas papildomų. Apžvelgus į naujo modeliu rezultatus, „X“ įmonė patvirtino, kad šis modelis yra lengvesnis ir labai paprastai pritaikomas, o tai reiškia, kad siūlomas modelis yra patikimas ir tinkamas naudoti.

IŠVADOS IR SIŪLYMAI

1. Mokslinės literatūros analizė leidžia teigti, kad rizika yra sudedamoji verslo dalis, ji yra neišvengiama, ko pasekoje ją reikia nuolat vertinti ir analizuoti. Literatūroje rizikos sampratų įvairovė yra didžiulė, kas ir daro įtaką jos sudėtingumui ar prieštaringumui. Išanalizavus mokslinę literatūrą, nustatyta, kad nors ir praktikoje daug skirtingų rizikos apibrėžimų, tačiau visiems jiems yra būdingi keli elementai - tai netikslumas, galimybė, neapibrėžtumas, nuostolis. Taigi, riziką galima apibrėžti kaip reiškinį, kuris atsiranda tokioje situacijoje, kurioje yra galimybė teigiamai arba neigiamai pasikeisti veiklos rezultatams. Rizika susideda iš daugybės veiksnių, kurie skirstomi į vidinius ir išorinius, o išoriniai rizikos veiksniai skirstomi į tiesioginius ir netiesioginius. Šie visi veiksniai yra tiesiogiai susiję ir vienos rizikos rūšies pasikeitimas gali nulemti kitų jos rūšių nuokrypius. Taigi, norint sėkmingai suvaldyti rizikas, įmonės turi susidaryti ir nusistatyti valdymo procesus. Pagrindinį rizikos valdymo procesą sudaro keli etapai: rizikos planavimas, rizikos identifikavimas, rizikos įvertinimas, rizikos valdymo priemonių pasirinkimas, rizikos kontrolės valdymas.
2. Darbe aptarti populiariausi ir dažniausiai naudojami rizikos valdymo standartai: COSO ERM, ISO 31000, ISO 27005 ir Octave metodas. COSO ERM modelį sudaro stebėsenos procesas, vidinė aplinka, tikslų nustatymas, įvykių identifikavimas, rizikos įvertinimas, reagavimas į riziką, kontrolės veiksniai ir komunikavimas. ISO 31000 standarto didžiausias tikslas yra sukurti tokią rizikos valdymo kultūrą, kurioje įmonės darbuotojai suprastų rizikos valdymo svarbą. ISO 27005 – vienas iš „ISMS standartų šeimos“ narių. Šis standartas akcentuoja planuok – veik – tikrink – vykdyk veiksnius. Octave metodas - tai yra sistema, kuri skirta nustatyti informacijos saugumo rizikai. Šis metodas pasižymi lankstumu, bet labiau tinkantis didesnėms įmonėms. Kadangi, informacinių technologijų įmonėse rizikos vertinimas yra labai svarbus, nagrinėjant mokslinę literatūrą nustatyta, kad IT srityje dirbančios įmonės dažniausiai renkasi tokius rizikos valdymo standartus kaip CORAS, OCTAVE, CRAMM. Šių metodų pasirinkimo priežastis – jie remiasi kibernetinės rizikos valdymu.
3. Atlikus kiekybinį tyrimą, kurio tikslas išsiaiškinti, ar siūlomi tarptautiniai standartai yra paklausūs bei tinkami naudoti mažoms ir vidutinėms įmonėms, gauti apklausos rezultatai parodė, kad 54 proc. respondentų išskiria rizikos valdymo procesus, bet iš jų didžioji dalis nėra patenkinti naudojamu tarptautiniu rizikos valdymo standartu. Taip pat kiekybinio tyrimo metu nustatyta, kad net 87 proc. respondentų sutiktų ir naudotų lengvesnį rizikos valdymo modelį savo įmonėse. Taigi, naujas rizikos valdymo modelis, kuris pritaikytas mažoms ir vidutinėms įmonėms, būtų reikalingas ir naudojamas IT įmonėse.

4. Atlikus teorinę analizę ir empirinį tyrimą buvo sukurtas naujas rizikos valdymo modelis, kuris yra pritaikytas mažoms ir vidutinėms įmonėms. Kuriant šį metodą buvo naudotasi mokslinėje literatūroje pateikiamais tarptautinių standartų privalumus ir trūkumus ir kiekybinio tyrimo rezultatais. Naujas modelis sudarytas sąrašo ir žymėjimo principu, kurio pagrindinis tikslas – įmonės sąnaudų taupymas. Organizacijos savininkas, direktorius ar skyriaus vadovas gali atlikti analizę užpildydamas šį sąrašą ir taip sudarydamas rizikos valdymo ataskaitą. Modelio pagrindinės teigiamos savybės: papildomų specialistų ne reikalavimas, laiko ir žmogiškųjų išteklių taupymas. Modelis nėra baigtinis, o tai reiškia, kad kiekviena įmonė pagal save gali pridėti norimas vertybes, iš kurių išsiskirtų galimos grėsmės ir jų kontrolės priemonės. Neigiamos modelio savybės: jis apima tik svarbiausias įmones vertybes ir jų rizikas, analizę gali atlikti įmonės darbuotojai, kurie neturi patirties rizikos valdyme, o tai gali išprovokuoti kitų galimų rizikų atsiradimą.
5. Naujas rizikos valdymo modelis pritaikytas „X“ įmonėje, kuri yra vidutinio dydžio ir priklauso IT sektoriui. Įmonė iki šiol naudojo tarptautinį ISO27005 standartą, kuriuo taip pat nėra pilnai patenkinta dėl papildomų laiko sąnaudų resursų. Sulyginus gautus rezultatus, nustatyta, kad abu rizikos valdymo modeliai išskyrė tas pačias svarbiausias įmonės vertybes ir galimas grėsmes bei kontrolės priemones. Pagrindinis modelių skirtumas – tarptautinis standartas daug smulkiau padėjo išanalizuoti galimas įmonės grėsmes, tačiau atsižvelgiant į tai, kad įmonė yra vidutinio dydžio, jai užtektų rizikos ataskaitos, kuri išskirtų pagrindines ir finansiškai svarbiausias rizikos grėsmes.

Pasiūlymai įmonių vadovams. Įmonėms, kurios dar neturi rizikos valdymo standarto, siūloma išbandyti lengvesnį modelį, su kuriuo galės išskirti pagrindines vertybes, rizikos grėsmes ir kontrolės priemonės. Kadangi pagrindinė priežastis, dėl ko mažos ir vidutinės įmonės neturi rizikos valdymo ataskaitų, yra laiko ir papildomų resursų stygius, šis standartas tai išspręstų, nes nereikalauja papildomų resursų – bet kuris įmonės vadovas tai galės atlikti. Turint rizikos valdymo ataskaitą, organizacija bus labiau užtikrinti jos veiklos tęstinumu ir sklandžiu rizikos valdymo procesu.

Tolimesnių tyrimų kryptys. Naują rizikos valdymo modelį pritaikyti dar bent 2 įmonėse. Tokiu būdu išsiskirtų daugiau modelio teigiamų ir neigiamų savybių, kurias ateityje galima tobulinti. Taip pat, empirinis tyrimas atliktas tik Lietuvoje registruotose įmonėse, tad tikslinga jį atlikti kaimyninėse šalyse, tokiu būtų išsiaiškinant platesnį naujo modelio reikalingumą.

LITERATŪRA

1. ADAMS, John. (2001) *Rizika*. Kaunas: Poligrafija ir informatika. ISBN 9986-850-33-9.
2. AIRMIC, ALARM, IRM, (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. UK [interaktyvus]. Prieiga per internetą: http://www.airmic.com/system/files/ERM_ISO31000_guide.pdf
3. Alberts, C. J., & Dorofee, A. J. (2001). OCTAVE method implementation guide version 2.0. Carnegie Mellon University.
4. Aleknevičienė V. (1997). *Investicijų rizikos valdymas*. Kaunas: Lietuvos žemės ūkio universiteto Leidybos centras.
5. Banevičius, Š. (2020). *Rizikos veiksnių valdymas medicinos turizmo organizacijose*, ISSN 2351-6712
6. Čepinskis J., Raškinis D. (2004). *Draudimo veikla.* Kaunas: Vytauto Didţiojo universitetas,
7. Čepinskis, J., Raškinis, D. (2005). *Draudimo veikla*. Vadovėlis. Vytauto Didžiojo universitetas
8. Daujotaitė D., Tarakavičiūtė I. ir Puškorius S. (2012). *Veiklos audito teorija ir praktika*. Vilnius: Mykolo Romerio universitetas.
9. Davidavičienė, V. (2012). *Verslo procesų vertinimas ir informacinių technologijų rizikos valdymas*. Vilnius. eISBN 9786094572067.
10. Davis, A. E., Jarvis, D. R. (2008). *Risk management – survival tools for law firms*. American Bar Association.
11. Duckert, G. H. (2011). *Practical Enterprise Risk Management: A Business Process Approach.* John Wiley & Sons, p. 275. ISBN 978-0-470-89251-0
12. Ebrahimnejad S., Mousavi S. M., Seyrafianpour H. (2010). *Risk identification and assessment for build–operate–transfer projects: A fuzzy multi attribute decision making model*. Expert Systems with Applications, 37 p. 575–586. doi: 10.1016/j.eswa.2009.05.037.
13. Epstein M. J., Buhovac A. R. (2006). *The reporting of organizational risks for internal and external decision-making*. The Society of Management Accountants of Canada (CMA-Canada). ISBN 0-87051-655-8.
14. Gaižauskaitė I., Mikėnė S. (2014). *Socialinių tyrimų metodai: apklausa.* Vilnius: Mykolo Romerio universitetas.
15. Haimes, Y. Y. (2009). *Risk Analysis*, Vol. 29, No. 12, p. 1647-1654.

16. International Organization for Standardization (2018). *Risk management ISO 31000*. ISBN 978-92-67-10784-44. Prieiga per internetą: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf
17. Januta, A., Marozas, L. ir Goranin, N. (2011). *Informacinės saugos audito vykdymas remiantis ISO/IEC 27000 šeimos Standartų reikalavimais*.
18. Jevsejev, R. (2019). *Informacinių technologijų rizikos vertinimo metodai ir tobulinimo sprendimai*, , ISSN 2029-2341
19. Juraitė K., (2005). *Lyginamieji tyrimo metodai: nuo intensyvaus ir ekstensyvaus prie visapusiško tyrimo*. Vilnius: ISM Vadybos ir ekonomikos universitetas.
20. Kaleininkaitė L., Trumpaitė I. (2007). *Verslas: teorija ir praktika,* Verslo rizikos valdymas ir jo tobulinimas. ISSN 1822-4202.
21. Kancerevyčius G. (2006). *Finansai ir investicijos / II atnaujintas leidimas*. Kaunas: „Smaltijos“ leidykla.
22. Kardelis, K. (2002). *Mokslinių tyrimų metodologija ir metodai*. Kaunas. ISBN: 9986948657.
23. Laskienė D., Snieška V. (2003). *Verslo rizikos samprata ir struktūra // Inžinerinė ekonomika.*
24. Lezgovko A., Lastauskas P. (2008). *Draudimo verslo plėtra: teoriniai aspektai ir rinkosplėtros prielaidos.*
25. Lydeka, Z., Drilingas, B. (2002). *Firmos ekonomikos pagrindai. 2-oji papild. ir patais. laida.* Vilnius: Pačiolis, p. 311. ISBN 9955-04-054-8
26. Mackevičius J., Giriūnas L. (2014). *Įmonių veiklos rizikų valdymo ir vertinimo modelis*, ISSN 1822-8682
27. Mackevičius, J. (2005). *Įmonių veiklos rizikų rūšys ir jų vertinimo būtinumas* // Ekonomika ir vadyba: aktualijos ir perspektyvos.
28. Marchand, M. (2009). *Modeling Coastal Vulnerability: Design and Evaluation of Vulnerability Model*. IOS Pres. Amsterdam, NLD, p. 239.
29. Merna T., Al-Thani F. (2008). *Corporate risk management / 2nd edition*. West Sssex: John Wiley& Sons.
30. Mikes, A. (2009). *Risk management and calculative cultures*. Management Accounting Research.
31. Morkevičius V., (2012). *Kokybinės lyginamosios analizės (KLA) pagrindai*. Kaunas.
32. Kardelis, K, (2005). *Mokslinių tyrimų metodologija ir metodai*. Šiauliai: Liucijus
33. Psichologijos žodynas (1993). Vilnius: Mokslo ir enciklopedijų leidykla.

34. Raz, T., Hillson, D., A (2005). *Comparative Review of Risk Management Standard*s, Risk Management: An International Journal . 7 (4), p. 53-66.
35. Rejda G.E. (2008). *Principles of risk management and insurance*. Boston: Pearson education.
36. Risk management standart. Prieiga per internetą: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf
37. Rutkauskas, A. V., Stasytytė, V. & Borisova, J. (2009). *Adequate portfolio as a conceptual model of investment profitability, risk and reliability adjustment to investor's interests*. Economics & Management 14: 1170–1174.
38. Stasytytė, V. (2008). *Continuous optimization and knowledgebased technologies*. ISBN 9789955282839.
39. Stoneburner G., Goguen A. & Feringa A. (2002). *Risk Management Guide for Information Technology Systems*.
40. Stulz, M. (2008). *Risk management failures: what are they and when do they happen?* Journal of Applied Corporate Finance, 4, 58-67.
41. Tarptautinių žodžių žodynas (1985). Vyriausioji enciklopedijų redakcija.
42. Thompson, D. (1996). *The Oxford Modern English Dictionary. 2nd edition*. USA: Oxford University Press. 1248. ISBN 978-0198600640.
43. Tidikis, R. (2003). *Socialinių mokslų tyrimų metodologija*. Vilnius. ISBN 9955-563-26-5.
44. Vageris R. (2005). *Rizikos analizės vadovas*. Vilnius: Vaga. ISBN 5-415-01827-1.
45. Virglerová, Z. (2018). *Differences in the Concept of Risk Management in V4 Countries*. International Journal ofEntrepreneurial Knowledge.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Lebeckaitė S. (2022). *Mažų ir vidutinių įmonių rizikos analizės vertinimas* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

Magistro baigiamajame darbe išanalizuota rizikos samprata, rizikos valdymo analizių metodai, atliktas kiekybinis mažų ir vidutinių įmonių tarptautinių rizikos standartų pasitenkinimo vertinimas ir sukurtas naujas rizikos valdymo metodas, pritaikymas mažoms ir vidutinėms įmonėms. Pirmame skyriuje nagrinėjama rizikos samprata, jos veiksniai bei rizikos valdymo tarptautiniai standartai. Antrame darbo skyriuje pateikiamas kiekybinis tyrimas, kuris skirtas išsiaiškinti ar mažoms ir vidutinėms įmonėms siūlomi tarptautiniai standartai yra tinkami naudoti ir yra paklausūs, pateikiami tyrimo rezultatai. Taip pat pateikiami pagrindiniai „X“ įmonės aspektai ir naudojamas rizikos valdymo modelis. Darbe pateikiamas naujas rizikos valdymo modelis, jo struktūra. Antro skyriaus ketvirtoje ir penktoje dalyse pateikiamas naujo rizikos valdymo modelio pritaikymas „X“ įmonėje ir įmonės rizikos valdymo ataskaitų palyginimas. Trečiame darbo skyriuje yra pateikiamos išvados ir siūlymai, kaip toliau tobulinti naują rizikos valdymo modelį.

Pagrindiniai žodžiai: Rizika, rizikos procesas, rizikos valdymas, rizikos valdymo metodai, mažos ir vidutinės įmonės.

ANNOTATION IN ENGLISH

Lebeckaitė S. (2022). *Assessment of risk management in small and medium-sized enterprises* (master's thesis). Vilnius: Mykolas Romeris University

The Master's thesis analyses the concept of risk, the methods of risk management analysis, introduces the results of performed quantitative research of the satisfaction of small and medium-sized enterprises with international risk standards and a new risk management method for small and medium sized businesses is developed. The first chapter examines the concept of risk, its factors and international standards of risk management. The second chapter of the thesis presents a quantitative study and it’s results out of whether the international standards offered for small and medium-sized businesses are suitable and in demand. What is more, he master's thesis presents the main aspects of Company „X“ and used model for risk management. The master‘s thesis presents a new risk management model and its structure. In the fourth and fifth parts of the second chapter the application of the new risk management method in company „X“ and a comparison of the company's risk management reports is presented. The third chapter presents conclusions and suggestions for further development of the new risk management method.

Key words: Risk, risk process, risk management, risk management methods, small and medium enterprises

Lebeckaitė S. (2022). *Mažų ir vidutinių įmonių rizikos analizės vertinimas* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA LIETUVIŲ KALBA

Rizikos valdymo baigiamojo darbo tema aktuali mažoms ir vidutinėms įmonėms, kurios negali skirti pakankamai lėšų ar resursų rizikos valdymo procesams išgryninti. Rizikos valdymo problemos tampa vis aktualesnės, nes netinkamas rizikos valdymo procesas arba visiškas jo neturėjimas gali daryti įtaką įmonės veiklos tęstinumui.

Rizikos analizės vertinimui, kuris atliekamas remiantis tarptautiniais standartais, reikia skirti daug laiko, finansinių ir žmogiškųjų resursų, dėl šios priežasties buvo iškelta pagrindinė tyrimo problema - kaip mažos ir vidutinės įmonės turi organizuoti rizikos vertinimą naudojant mažiau resursų? Tyrimo objektas - rizikos valdymas mažose ir vidutinėse įmonėse. Magistro darbo tikslas – remiantis esamais tarptautiniais standartais sukurti mažesnės apimties rizikos vertinimo metodą, pritaikant jį vidutinėje „X“ įmonėje. Taip pat buvo iškelti 5 tyrimo uždaviniai: išanalizuoti ir apibrėžti rizikos valdymo sampratą, aptarti rizikos valdymo ir vertinimo principus teoriniu aspektu, išanalizuoti esamus rizikos valdymo modelius, ištirti naudojamų tarptautinių standartų paklausumą bei tinkamumą mažoms ir vidutinėms įmonėms, sukurti rizikos valdymo metodą orientuotą į smulkias ir vidutines įmones, palyginti sukurtą modelį su „X“ įmonėje taikomu tarptautiniu standartu. Taikyti tyrimo metodai: mokslinės literatūros analizės metodas, anketinė apklausa, modeliavimo metodas, lyginamosios analizės metodas.

Empirinio tyrimo metu iškeltas pagrindinis tikslas – išsiaiškinti, ar siūlomi tarptautiniai standartai yra paklausūs bei tinkami naudoti mažoms ir vidutinėms įmonėms. Kiekybinio tyrimo metu nustatyta, kad mažos įmonės neturi nusistačiusios rizikos valdymo procedūrų dėl finansinių, laiko ir žmogiškųjų resursų. Taip pat, didžioji dalis įmonių, kurios šiuo metu neturi rizikos valdymo procedūrų, ateityje norėtų išbandyti lengvesnį ir papildomų išteklių nereikalaujantį modelį. Atsižvengus į tai, darbe, remiantis modeliavimo metodu, sukurtas naujas rizikos valdymo modelis, kuris pritaikytas mažoms ir vidutinėms įmonėms. Pagrindinis modelio principas – sąrašuose esančių turtinių vertybių bei galimų grėsmių žymėjimas. Šis modelis buvo išbandytas „X“ vidutinio dydžio įmonėje, kurios veiklos sritis yra susijusi su IT sektoriumi. Išbandžius ir palyginus naują modelį su įmonėje naudojamu standartu, buvo išskirti pagrindiniai skirtumai. Po abiejų standartų palyginimo, nustatyta, kad naujas modelis atskleidė tas pačias pagrindines galimas rizikas.

Magistro darbas susideda iš 3 pagrindinių dalių. Pirmoje dalyje analizuojama mokslinė literatūra rizikos, jos valdymo, procesų, tarptautinių rizikos valdymo standartų aspektais. Antroje dalyje pateikiama empirinio tyrimo metodologija, tyrimo rezultatai. Taip pat pristatomas naujas rizikos valdymo modelis

akcentuotas į mažas ir vidutines įmones ir jo pritaikymas „X“ įmonėje. Magistro baigiamojo darbo paskutinėje dalyje pateikiamos išvados bei siūlymai, kurie susyja su nauju rizikos valdymo modeliu mažoms ir vidutinėms įmonėms.

SANTRAUKA ANGLŲ KALBA

Lebeckaitė S. (2022). *Assessment of risk management in small and medium-sized enterprises* (master's thesis). Vilnius: Mykolas Romeris University

SUMMARY

The thesis topic of risk management is relevant for small and medium-sized enterprises that cannot allocate sufficient funds or resources to define their risk management processes. Risk management issues are becoming more and more important, as insufficient and incomplete risk management process can affect the business continuity.

Assessing risk analysis in accordance with international standards requires a lot of time, financial and human resources, which is why the main problem of the study is: how should small and medium-sized enterprises organize risk assessment with fewer resources. The object of the research is risk management in small and medium enterprises. The aim of the master's thesis is to develop a smaller-scale risk assessment method based on the existing international standards, applying it to the average "X" company. 5 research objectives were chosen: to analyze and define the concept of risk management, to discuss the principles of risk management and assessment from a theoretical point of view, to analyze existing risk management models, to study the demand and eligibility of used international standards for small and medium-sized enterprises, to develop a risk management approach focused on small and medium-sized enterprises, comparing the developed model with the international standard applied in company X. Applied research methods: analysis of scientific literature, questionnaire survey, modeling method, comparative analysis.

The main goal of the empirical study is to find out whether the proposed international standards are popular and suitable for small and medium-sized enterprises to use. The quantitative study found that small businesses do not possess risk management procedures because of lack of financial, time and human resources. The vast majority of companies that do not currently have risk management procedures would be willing to try a simpler model that does not require additional resources. Taking this into account, a new risk management model has been developed for small and medium-sized enterprises based on a modeling approach. The main principle of the model is listing the assets of company assets and potential threats. This model has been tested in the medium-sized company X, which is active in the IT sector. After testing and comparing the new model with the standard used in the company, the main differences were identified. After comparing the two standards, the results show that the new model discovered same key potential risks.

The Master's thesis consists of 3 main parts. The first part analyzes the scientific literature on the aspects of risk, its management, processes, international risk management standards. The second part presents the methodology of the empirical research and the key findings of the research, introduces a new risk management model focused on small and medium-sized enterprises and its application in company X. The last part of the master's thesis presents the conclusions and suggestions related to the new risk management model for small and medium-sized enterprises.

PRIEDAI

1 PRIEDAS. KIEKYBINIO EMPIRINIO TYRIMO APKLAUSA

Anketos tikslas - išsiaiškinti, ar siūlomi tarptautiniai standartai yra paklausūs bei tinkami naudoti mažoms ir vidutinėms įmonėms. Anketa yra anoniminė ir pateikti atsakymai bus publikuojami mokslo tikslams. Ačiū už skirtą laiką.

1. **Ar įmonėje yra išskirtas veiklos rizikos valdymo procesas?**
   - Taip
   - Ne

2. **Jei atsakėte ne, dėl kokių priežasčių nedarote rizikos analizės vertinimo?**
   - Siūlomi tarptautiniai rizikos valdymo standartai yra per sudėtingi
   - Dėl papildomų finansinių išteklių
   - Dėl laiko stokos
   - Kitos priežastys

3. **Ar atliktumėte rizikos analizės vertinimą, jei būtų pasiūlytas lengvesnis vertinimo modelis?**
   - Taip
   - Ne
   - Neatsakė į klausimą

4. **Kokiu standartu remiantis sudarote rizikos ataskaitas?**
   - COSO ERM standartu
   - ISO27005 standartu
   - Octave standartu
   - ISO31000 standartu
   - Kitu standartu
   - Neatsakė į klausimą

5. **Ar esate pilnai patenkinti naudojamu rizikos valdymo standartu?**
   - Taip, esame patenkinti
   - Ne visai, susiduriame su problemomis
   - Ne, esame nepatenkinti

- ○ Neatsakė į klausimą

6. Ar teko susidurti su grėsme, dėl kurios Jūsų įmonė patirtų nuostolius??

- ○ Taip
- ○ Ne

7. Įvertinkite veiklos rizikos valdymo proceso etapų svarbą Jūsų įmonėje

	Visiškai nesvarbu	Nesvarbu	Vidutiniškai svarbu	Svarbu	Labai svarbu
Įmonės strateginių tikslų iškėlimas	○	○	○	○	○
Rizikos įvertinimas, analizė ir nustatymas	○	○	○	○	○
Rizikos priežiūra	○	○	○	○	○
Stebėsena	○	○	○	○	○

8. Nuo 1 iki 5 balų įvertinkite naudojamo tarptautinio rizikos standarto:

	1	2	3	4	5
Ataskaitos atlikimo sunkumo lygis	○	○	○	○	○
Papildomų finansų reikalavimas	○	○	○	○	○
Papildomų žmogiškųjų išteklių reikalavimas	○	○	○	○	○
Ataskaitos sudarymo laiko sąnaudos	○	○	○	○	○

9. Jūsų užimamos pareigos:

- ○ Direktorius
- ○ Skyriaus vadovas
- ○ Specialistas

10. Kiek darbuotojų dirba Jūsų įmonėje?

- ○ 1 - 10
- ○ 11 - 50
- ○ 51 – 250

11. Įmonės veiklos laikas:

- ○ 0 – 5 metai

- 5 – 10 metų
- 10 < metų

2 PRIEDAS. „X“ ĮMONĖS RIZIKOS ANALIZĖS VERTINIMO REZULTATAI

Bendras grėsmės atsiradimo balo nustatymas

Blokas 1		Blokas 2		Blokas 3		Blokas 4	
✓	Interneto svetainė	✓	Serveriai	✓	Techninė dokumentacija/sutartys	✓	Patalpos (serverinė)
✓	Ryšio linijos (Interneto/ryšio linijos su klientais)		Saugyklos	✓	Darbo tvarkos/procedūros	✓	Žmogiškieji ištekliai (darbuotojai/vadovai)
✓	Elektros tiekimas	✓	Kondicionavimo sistema	✓	Įmonės programinė įranga		Nedokumentuotos žinios
✓	Elektroninis paštas		Gesinimo sistema	✓	Trečių šalių programinė įranga	✓	Kompiuteriai ir jo priedai
	Verslo valdymo sistema	✓	Video stebėjimo sistema			✓	Nešiojami media (raktai, mob. telefonai)
		✓	Praėjimo kortelių sistema				
			Tinklo įranga				

Galimų grėsmių pasirinkimas, blokas 1

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Fizinis linijos pažeidimas	Dubliavimas
	Konfigūracijos klaida	Profilaktiniai darbai, monitoringas
✓	Ryšio linijos kokybė	Monitoringas, reguliari sutarčių peržiūra ir operatoriaus keitimas
✓	Priklausomybė nuo konkretaus fizinės ryšio linijos tiekėjo	Sąrašo sudarymas, „Provider Independant“ IP gavimas
	Nepastebimas perjungimas į rezervinę liniją	Monitoringas
✓	Elektros šuoliai, elektros dingimas	UPS, profilaktiniai darbai, srovės lygintuvai
	Elektros įvado gedimas	Monitoringas, procedūros, įvado dubliavimas
✓	Šlamštas (ang. Spam)	SPAM filtrai, antivirusinės sistemos, vartotojų mokymai
✓	Pašto persipildymas	Monitoringas, resursų planavimas

✓	Pranešimų pametimas	Procedūros, rezervinis kopijavimas, mokymai
✓	Sukčiavimas	Ang. Phishing) per e-paštą (mokymai darbuotojams, antivirusinės sistemos, papildomi reguliarūs priminimai apie pavojaus svarbą

Galimų grėsmių pasirinkimas, blokas 2

Yra/nėra	Galimos rizikos	Kontrolės priemonės
✓	RAM gedimas	Atsarginės dalys, procedūros, monitoringas
✓	Maitinimo bloko gedimas	Atsarginės dalys, procedūros, monitoringas
✓	Gaisras	Gesintuvai, procedūros, veiklos atstatymas rezervinėje serverinėje, duomenų dubliavimas kitose patalpose, verslo atstatymo planas, draudimas
✓	*Force majeure (nenugalima jėga)*	Veiklos atstatymas rezervinėje serverinėje, draudimas
✓	Įrangos (serverių) nusidėvėjimas	Profilaktiniai darbai, monitoringas, įrangos atnaujinimas
	Dujų nutekėjimas	Procedūros, monitoringas
	Kamerų perdengimas kitomis kameromis	Papildomų kamerų montavimas
✓	Praėjimo kortelių pametimas	Procedūros (blokavimo), kontrolinė peržiūra

Galimų grėsmių pasirinkimas, blokas 3

Yra/nėra	Galimos rizikos	Kontrolės priemonės
	Įsilaužimas	Tinklo segmentacija, griežta prieigos kontrolė iš išorės
✓	Netyčinis duomenų nutekinimas	Ryšių su klientais kontrolė, e-pašto ribojimas
	užsakomosios paslaugos (ang. outsourcing) grėsmės: kodo vagystė,	SLA, NDA, stebėjimas

	konkuruojančio verslo steigimas, kainų politika, vėlavimas, kompetencijos stoka	
✓	Licencijų valdymas	Centralizuoto sąrašo vedimas, procedūros
✓	Nusidėvėjimas	Testai
	Nereikalingas informacijos kopijavimas į asmenines laikmenas	Nešiojamų kaupiklių kontrolė
✓	Netyčinis dokumentų persiuntimas klientams/konkurentams	Ryšių su klientais kontrolė, e-pašto ribojimas
	Procedūrų aprašų trūkumas	Trūkstamų procedūrų sąrašo sudarymas, procesų apibrėžimas
	Darbo tvarkų iškomunikuotos	Mokymai

Galimų grėsmių pasirinkimas, blokas 4

Yra/nėra	Galimos rizikos	Kontrolės priemonės
✓	Gaisras	Gesintuvai, gesinimo sistema, signalizacija, mokymai
	Užpylimas	Nepratekančios lubos
✓	Fizinis įsilaužimas	Fizinės apsaugos priemonės

Galimų grėsmių pasirinkimas, blokas 5

Yra/nėra	Galimos rizikos	Kontrolės priemonės
✓	Darbuotojų neatėjimas į darbą	Pareigų dubliavimas
✓	Neteisingos informacijos skleidimas	Mokymai, procedūros
✓	Netinkamas bendravimas su klientais	Mokymai, procedūros
✓	Darbuotojų išėjimas	Žinių dokumentavimas, darbo sutarčių sąlygos