MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

LINA LEGYTĖ

IT PROJEKTŲ VALDYMO YPATUMAI KIBERNETINIO SAUGUMO SRITYJE

Magistro baigiamasis darbas

Vadovas
prof. dr. Tadas Limba

VILNIUS, 2021

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

IT PROJEKTŲ VALDYMO YPATUMAI KIBERNETINIO SAUGUMO SRITYJE

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas

prof. dr. T. Limba

2021 12

Atliko

KSVvmis19-1 gr. stud.

L. Legytė

2021 12

VILNIUS, 2021

TURINYS

LENTELĖS

PAVEIKSLAI

ĮVADAS

Temos aktualumas. Naujosioms technologijoms vystantis ir kintant neįtikėtinu tempu, kibernetinės grėsmės tampa vis labiau kompleksiškos, o kibernetinis saugumas tampa viena iš labiausiai eskaluojamų temų. Allianz organizacijos rizikų barometro duomenimis, kibernetinio saugumo incidentai užima trečią vietą 2021 metų globaliam verslui aktualiausių rizikų sąraše (Allianz Risk Barometer, 2021). Ne tik viešasis, bet ir privatusis sektorius stengiasi užtikrinti įvairiapusį duomenų ir kibernetinį saugumą kurdamas kibernetinio saugumo programas. Efektyvi kibernetinio saugumo programa susideda iš keletos komponentų, pavyzdžiui, strategijos, vidinių įmonės nuostatų, veiksmų plano (Barclay, 2013, Bermudez, 2020). Nuoseklus kibernetinio saugumo programos įgyvendinimas tampa išbandymu įmonėms ne tik dėl kompleksiškumo, bet ir dėl specialistų ar lėšų trūkumo. Žvelgiant į pasaulines tendencijas galima teigti, jog vieni iš pagrindinių iššūkių formuojant kibernetinio saugumo programas yra kibernetinės strategijos ir tikslų kūrimas (įskaitant rizikos faktorių identifikavimą), procesų standartizavimas, žmogiškųjų išteklių trūkumas, vadovybės parama (Swinton, S. ir Hedges, S., 2019). Smulkaus ir vidutinio verslo įmonėms kibernetinio saugumo iššūkiai dar aktualesni dėl lėšų ir specialistų stokos (Moskowitz, S. 2017, Hoppe F., Gatzert N., Gruner P., 2021). Dėl šių priežasčių smulkaus ir vidutinio verslo įmonės yra labiau pažeidžiamos iš kibernetinio saugumo pusės (Ozkan Y. B., Spruit M., 2020).

Temos naujumas. ENISA organizacijos 2021 metais atliktos apklausos ir analizės duomenimis, smulkaus ir vidutinio verslo sektorius Europos Sąjungos šalyse susiduria su 7 pagrindiniais iššūkiais bandydamas sudaryti kibernetinio saugumo planus, tarp kurių įvardijamos tokios problemos kaip IRT specialistų trūkumas, lėšų trūkumas, aiškių ir praktiškai pritaikomų kibernetinio saugumo gairių stoka (ENISA, 2021). Viena iš šiame pranešime pateiktų rekomendacijų ES šalių vyriausybėms – aiškių ir lengvai pritaikomų rizikos valdymo gairių kūrimo skatinimas. Teigiama, jog nors informacijos apie rizikos valdymo metodus yra daug, tačiau ji nėra lengvai suprantama ne specialistams, informacija fragmentuota, rizikų valdymo metodologijas sunku adaptuoti praktiškai (ENISA, 2021 p. 51). Pažvelgus į situaciją Lietuvos rinkoje per kibernetinio saugumo prevencijos prizmę galima daryti išvadas, jog sudėtingiausia situacija smulkaus ir vidutinio verslo sektoriuje. „Kurk Lietuvai“ projekto 2019 metais vykdytos apklausos duomenimis tarp labai smulkių įmonių tik 9 proc., smulkių – 39 proc., o vidutinių – 48 proc., teigė, kad turi kibernetinio saugumo politiką. Dauguma (72 %) įmonių teigė nemokančios arba nežinančios, ar moka įsivertini kibernetinio saugumo rizikas bei spragas (Bilevičiūtė, K., Kidykas, J. ir Beinoriūtė, R., 2019).

Atsižvelgdama į šios apklausos duomenis, Krašto apsaugos ministerija yra išsikėlusi tikslą didinti mažų ir vidutinių privataus verslo atstovų kibernetinio saugumo brandą. 2020 metais KAM inicijavo dokumento „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas“ išleidimą. Žvelgiant ne specialisto akimis, daugelis dokumente išvardintų gairių ir patarimų yra pateikti aiškiai ir suprantamai, tačiau skyriuje „Rizikų valdymas“ trūksta praktinės informacijos. Pateikiamos nuorodos į šaltinius užsienio kalba bei minima, jog rizikų valdymas yra sudėtingas ir brangus procesas: „Norint daugiau sužinoti apie rizikų vertinimo metodologijas ir susipažinti su gerosiomis užsienio kibernetinio ir informacinio saugumo valdymo praktikomis, rekomenduojama susipažinti su toliau nurodytais šaltiniais. Mažesnėms įmonėms šie standartai gali būti gana kompleksiški, o jų įgyvendinimas reikalauti daug kaštų, tačiau tai yra naudingi šaltiniai, padedantys verslui įvertinti pasiruošimą reaguoti į kibernetinius incidentus“ (Lietuvos Respublikos krašto apsaugos ministerija, 2021, p. 22). Publikacijoje pateikiama nuoroda į vienintelį šaltinį lietuvių kalba, supažindinanti su rizikų valdymu, t.y. 2005 metais išleistą „Rizikos analizės vadovą“.

Mokslinė problema. SVV įmonėms sudėtinga pačioms sudaryti ar praktiškai adaptuoti kibernetinio saugumo rizikų valdymo modelį dėl aiškių gairių stokos, fragmentuotos ir/ar kompleksinio turinio informacijos, susijusios su rizikų valdymu. Plačiąja prasme projektas yra individualios ar komandinės pastangos, kurios aiškiai suplanuotos, nukreiptos tikslui siekti. Taip pat projektas gali būti suprantamas kaip dokumentas, kuriame išdėstoma projekto esmė, organizacijos būklė, numatoma projekto įgyvendinimo strategija, ateities perspektyvos, prognozuojami projekto įgyvendinimo rezultatai (Tonchia, 2018). Pasitelkus projektų valdymo metodologijas siekiama optimizuoti tokius procesus kaip strateginis suderinamumas, rizikų valdymas, suinteresuotųjų šalių valdymas, rolių atsakomybė bei atskaitomybė, resursų valdymas ir pan. Lyginant kibernetinio saugumo programų formavimo ir įgyvendinimo iššūkius bei procesus, kuriuos siekiama suvaldyti projektų valdymo metodologijomis, galima teigti, jog sudarant KS rizikų valdymo modelį, galėtų būti pasitelkiamos IT projektų valdymo metodologijos.

Tyrimo objektas. Rizikų valdymo modeliai IT projektų valdymo metodologijose bei jų praktinis pritaikomumas sudarant kibernetinio saugumo rizikos valdymo modelį.

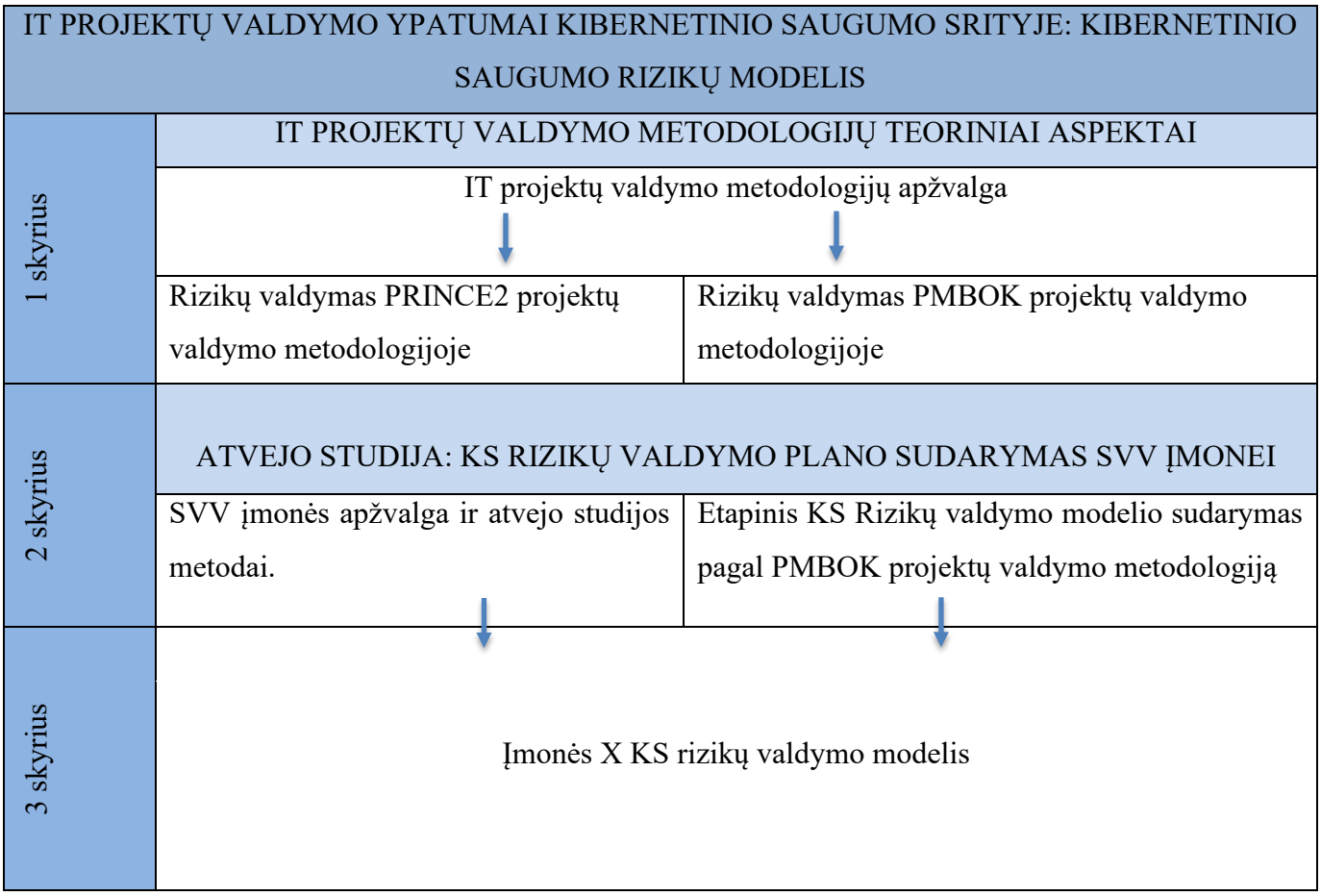
Tyrimo tikslas. Išanalizuoti IT projektų valdymo metodologijų teorinių aspektus bei praktinį pritaikomumą sudarant kibernetinio saugumo rizikos valdymo modelį SVV įmonei.

Uždaviniai:

- išanalizuoti teorinius IT projektų valdymo metodologijų teorinius aspektus;
- parinkti priimtiniausią IT projektų valdymo rizikos valdymo modelį;
- praktiškai pritaikyti priimtiniausią rizikos valdymo modelį sudarant kibernetinio saugumo rizikos valdymo modelį SVV įmonei.

Duomenų rinkimo metodai ir šaltiniai. Naudoti aprašomasis ir analitinis tyrimo metodai analizuojant teorinę literatūrą bei atvejo studija. Remiantis atvejo analizės metodu, siekta įvertinti pasirinkto rizikos valdymo modelio praktinio pritaikomumo galimybes sudarant kibernetinio saugumo rizikos valdymo modelį. Darbe daugiausia remiamasi „Project Management Institute“ organizacijos sudarytu vadovu „A Guide to the Project Management Body of Knowledge (PMBOK Guide)“ (2017) ir „Axelos“ organizacijos sudarytu vadovu „Managing Successful Projects with PRINCE2“ (2017).

Darbo struktūra. Darbą sudaro 2 pagrindinės dalys (žr. 1 pav.) – teorinė ir praktinė. Teorinėje dalyje aptariami IT projektų valdymo metodologijų ypatumai bei išsamiau aprašomos *waterfall* IT projektų valdymo metodologijose naudojami rizikų valdymo būdai. Antroje dalyje naudojant atvejo studijos metodą, analizuojamas praktinis IT pritaikomumas sudarant kibernetinio saugumo rizikos valdymo modelį SVV įmonei. Darbo pabaigoje pateikiamos išvados ir rekomendacijos.



pav. 1 Magistro baigiamojo darbo struktūros loginė schema

1. IT PROJEKTŲ VALDYMO METODOLOGIJŲ TEORINIAI ASPEKTAI

Pirmieji modernieji projektų valdymo principai pradėjo formuotis 20 amžiaus pradžioje, kurių pradininkais laikomi Henri Foyal ir Henry Gantt. Henri Foyal savo knygoje *Administration industrielle et générale* išskyrė penkis svarbiausius darbo organizavimo principus: planavimas, organizavimas, vadovavimas, koordinavimas ir kontrolė. Henry Gantt išplėtė H. Foyal teoriją ją papildymas įrankiu, padedančiu lengviau organizuoti planavimo ir kontrolės stadijas, žinomu kaip Gantto diagrama. Gantto diagrama turi svarbią reikšmę bendram projektų valdymo metodologijų vystymuisi, nes atskleidžiami privalumai skaldyti didelio masto projektus į mažesnius uždavinius (Chiu, 2010). Tiek H. Foyal, tiek H. Gantt įkvėpimo sėmėsi iš Frederic Winslow Taylor, kuris pradėjo formuotis moderniuosius vadovavimo principus, tokius kaip darbų pasiskirstymas, tinkamas resursų alokavimas ir pan (Taylor, 1911).

Terminas *projektų valdymas* pradėtas vartoti ir modernūs projektų valdymo įrankiai (tokie kaip CPM, PERT, WBS) pradėti plačiau vystyti šeštajame dešimtyje (Seymour, T. J. 2014). Pirmieji sektoriai, kurie pradėjo organizuoti darbus pasitelkę projektų valdymo metodologijas (žvelgiant iš darbartinės perspektyvos) buvo kariuomenė ir statybų sektorius. Vienas svarbiausių *projektų,* paskatinusiu projektų valdymo metodologijų raidą, buvo USAF (JAV Oro Pajėgos) projektas Atlas. Atlas tikslas – sukurti tarpkontinentinę balistinę raketą. 1954m. šį projektą paskirtas koordinuoti Bernard Schriever (Morris, 2013). Žvelgiant holistiškai, galima teigti, kad B. Schriever į šį projektą organizavo pasitelkdamas sistemų teorijos filosofiją. Remdamasis principu, jog organizmas yra viena sistema. Bendrosios sistemų teoriją sukūrė Ludwig von Bertalanffy XXa. viduryje. Pagrindinės Bendrosios sistemų teorijos idėja – mus supančių reiškinių, procesų matymas per integralumo ir visumos prizmę. Viskas yra tarpusavyje susiję; tam tikra sistema, reiškinys, susideda iš komponentų, kurie nėra autonomiški: pasikeitus vienam sistemos komponentui, pasikeis ir visa sistema (Emes, Griffiths, 2018).

Projektų valdymo metodologijos pradėtos formuoti 7-jame dešimtmetyje: įkurtos tokios organizacijos kaip PMI, APM, AIPM ir IMPA. Kitas projektų valdymo metodologijų raidos etapas siejamas su IT sektoriaus vystymųsi: naujųjų technologijų kūrimui buvo pasitelktos jau esamos projektų valdymo metodologijos, taip pat IT sektorius įnešė ir savo indėlį į projektų valdymo teorijas, susistemindamas projektų valdymo praktikas ir adaptuodamas jas savo sektoriui. Bandymai surasti universaliausią projektų valdymo metodologiją, tinkančią įvairiems sektoriams, baigėsi kelių metodologijų suformavimų taikant įvarius projekto valdymo įrankius.

Terminas *projektas* interpretuojamas ne vienodai, tačiau skiriami pagrindiniai kriterijai, nusakantys projekto konceptą: laikina veikla, skirta sukurti unikalų rezultatą (produktą, paslaugą). Projekto apimtis ar trukmė nėra niekaip ribojama, kitaip tariant projektą galima įvykdyti ir per dieną, tačiau galimi ir ilgalaikiai projektai, trunkantys metus (Gholamreza, J., Oveisi, M., 2016).

Projekto eigą riboją trys pagrindiniai faktoriai: apimtis, laikas ir išlaidos. Pasak kai kurių mokslinių šaltinių, plačiąja prasme projektų valdymas yra specifinis problemų sprendimo metodikos rinkinys, kurio tikslas – atnešti naudos verslui (Abbasi, Jaafari, 2018).

PMBOK® skiria 5 pagrindines projekto procesų grupes: inicijavimas, planavimas, vykdymas, stebėsena ir kontrolė, užbaigimas. Kiekvienas laukas turi tam tikrus įrankius ir metodikas. Pagal tai, kaip organizuojamos procesų grupės, projektų valdymo metodologijas galima skirti į tradicinę (linijinę) vykdančias projekto valdymo etapus iš eilės. Nepasibaigus vienam etapui, negalima pradėti kito. Tradicinio tipo projektų valdymo metodologijos tinkamiausios gerai organizuotiems, susiformavusiems sektoriams. Koncentruojamasi į projekto taikymo sritį (angl. *scope*), o projekto valdymo metodologijos siūlomais įrankiais siekiama nustatyti projekto trukmę ir išlaidas. Populiariausios tradicinės projektų valdymo metodologijos yra PMBOK ir PRINCE2.

XXI a. pradžioje išpopuliarinta Agile projektų valdymo metodologija, siūlanti kitokią projekto valdymo etapų eigą: greičiau įgyvendinamą, leidžiančią koreguoti projekto rezultatą projekto įgyvendinimo metu bei pasikeitus aplinkybėms bei prioritetams lengviau adaptuoti projekto eigą. Agile tipo projektas skirstomas į smulkesnius ciklus žinomus kaip sprintai. Kiekvieno sprinto pabaigoje galima tikėtis apčiuopiamo rezultato. Nors Agile metodologijos pritaikymo laukas gali būti platus, dėl jau išvardintų savybių (lankstumas, greitai apčiuopiamas rezultatas, galimybė lengvai koreguoti projekto eigą) Agile metodologija dažniausia taikoma kuriant programinę įrangą. Agile tipo metodologijos (kai kuriuose šaltiniuose vadinamos Agile technikomis) skiriamos į keletą rūšių pagal tai, kokie metodai taikomi kurti programinę įrangą bei valdyti projekto eigą. Patys populiariausi metodai yra Scrum, Kanban, Hybrid, Bimodal, Lean, XP (AltexSoft, 2018). Įvairių publikacijų duomenimis, Agile tipo projektų valdymo metodologijos neturi aiškiai apibrėžtos rizikų valdymų metodikos, projektų valdyme dažnai naudojamas hibridinis modelis pasitelkiant rizikos valdymo įrankius ir technikas iš tradicinių (angl. *waterfall*) projekto valdymo modelių (Zasa, P. F., Patrucco, A., Pellizzoni E., 2021, Buganováa, K., Šimíčkováa, J. 2019).

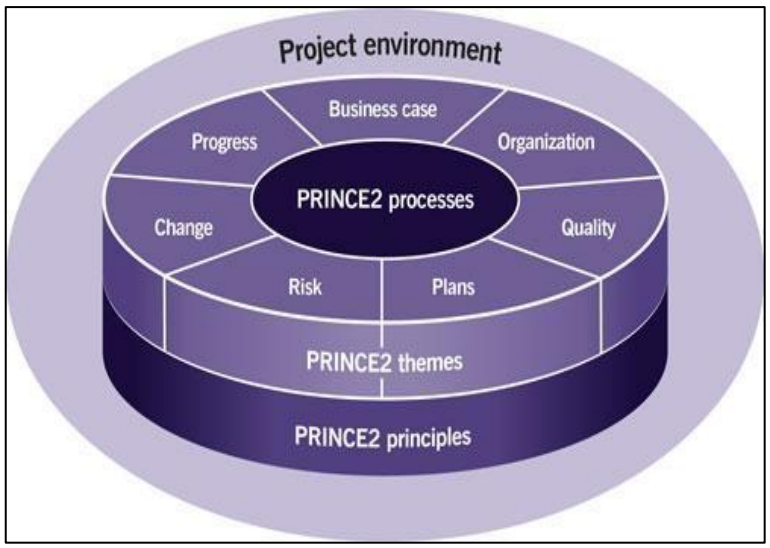
Šio darbo tikslas – išanalizuoti, ar rizikos valdymo technikos bei įrankiai, aptariami projektų valdymo metodologijose, galėtų pagelbėti įsivertinti rizikas kuriant kibernetinio saugumo planus, todėl Agile metodologija nebus plačiau aptariama ir toliau analizuojamos tradicinio tipo metodologijos PRINCE2 ir

PMBOK siekiant susisteminti rizikos valdymo įrankius bei praktiškai pritaikyti kuriant kibernetinio saugumo rizikos valdymo modelį SVV įmonėje.

1.1 PRINCE2 projektų valdymo metodologija

Ši projektų valdymo metodologija pradėta formuoti 8-jame dešimtmetyje Jungtinėje Karalystėje valdžios institucijoms pastebėjus, jog sunku įgyvendinti IT sektoriaus projektus ir iniciavus bendros metodologijos kūrimą. PRINCE2 metodologija dabartiniu savo pavidalu pilnai suformuota 1996 metais. Metodologija nuolat peržiūrima siekiant prisitaikyti prie nuolat kintančios aplinkos, paskutinį kartą PRINCE2 atnaujintas 2017 metais (ILX Group, 2017).

PRINCE2 metodologija susideda iš 4 pagrindinių elementų: 7 principų, 7 žinių sričių (angl. knowledge areas), 7 procesų ir projekto aplinkos. Teigiama, jog PRINCE2 projektų valdymo metodologiją galima pritaikyti įvairaus masto projektų įgyvendinimui nepriklausomai nuo sektoriaus.



Šaltinis: Axelos, 2017, p. 3

pav. 2 PRINCE2 projektų valdymo metodologijos stuktūros schema

7 principus sudaro šie elementai, teigiama, jog jei nors vienas principas yra praleidžiamas, projekto negalima laikyti atitinkančio PRINCE2 metodologijos standartų (Axelos, 2017):

1. projekto pagrindimas: aiški priežastis, kodėl projektas yra inicijuojamas ir vykdomas.

2. mokymasis iš patirties: PRINCE2 projektų valdymo komandos turi nuolatos mokytis iš prieš tai padarytų klaidų ir kaupti gerosios patirties bagažą.
3. rolių ir atsakomybių nustatymas: PRINCE2 projekto valdymo komanda turi nusistatyti aiškią organizacinę hierarchiją ir įtraukti tinkamus žmogiškuosius resursus.
4. valdymas etapais: PRINCE2 tipo projektai turi planuojami, stebimi ir vykdomi *etapas po etapo* principu.
5. valdymas išimties principu: PRINCE2 metodologijoje laikoma, jog išimtis reiškia didelę problemą su kuria susidūrė projekto vadovas. Didelė problema – atvejis, išeinantis iš anksčiau nusistatytų tolerancijos kriterijų ribų laikui, kaštams, kokybei, apimčiai, rizikoms ir naudai. Įprastai projekto vadovui suteikiami įgaliojimai pačiam priimti įvairius sprendimus be prieš tai sudarytos projekto valdymo tarybos pritarimo nebent atsiranda išimtinis atvejis t.y. susiduriama su didele problema. Tokiu atveju, sprendimą dėl tolimesnės projekto eigos priima projekto valdymo taryba.
6. susitelkimas ties produktais: PRINCE2 projektai turi sutelkti dėmesį į produkto apibrėžimą, pateikimą ir reikalavimus.
7. pritaikomumas projekto aplinkai: PRINCE2 turi atitikti projekto aplinką, dydį, sudėtingumą, svarbą, galimybes ir rizikas.

Skiriamos šios žinių sritys:

1. „verslo atvejis“ (angl. *business case*): projekto reikalingumo formulavimas ir pagrindimas.
2. organizavimas: žmogiškųjų išteklių bei jų rolių ir atsakomybių identifikavimas.
3. kokybė: kokybinių reikalavimų ir vertinimo rodiklių nustatymas.
4. planai: projekto etapai, reikalingi projekto eigai ir PRINCE2 metodologijos įrankiai.
5. rizika: efektyvus rizikų ir galimybių, galinčių paveikti projekto eigą, identifikavimas
6. pokyčiai: kaip projekto vadovas nustatys projekto pokyčius ir kaip elgis projekto valdymo procese.
7. progresas: tęstinis projekto perspektyvumo vertinimas.

Septynis PRINCE2 procesus sudaro:

1. Projekto pradžia
2. Projekto priežiūra
3. Projekto planavimas

4. Projekto kontrolė
5. Produkto įgyvendinimas
6. Etapų kontrolė
7. Projekto užbaigimas

Nors paties kibernetinio saugumo valdymo modelio kūrimas gali būti vykdomas kaip projektas, tačiau atsižvelgiant į darbo tikslus, išsamiau aptarti bus tik principai, procesai, žinių sritys, tiesiogiai susiję su rizikų valdymu.

1.1.1 Rizikų valdymas PRINCE2 projektų valdymo metodologijoje

PRINCE2 projektų valdymo metodologijoje rizika apibrėžiama kaip įvykių seka, galinti paveikti projekto tikslus. Kitas rizikos apibrėžimas - neužtikrintas įvykis, kuriam nutikus, projekto tikslai bus paveikti neigiamai arba teigiamai (Axelos, 2017). Taigi į rizikas žiūrima kaip į grėsmės arba kaip į galimybes.

Rizikų valdymas – sisteminis principų, procesų ir metodų taikymas siekiant identifikuoti ir įvertinti rizikas bei įgyvendinti atsakas į rizikas. Sėkmingas rizikų valdymas susideda iš šių komponentų (Axelos, 2017):

- rizikų identifikavimas bei apibūdinimas;
- rizikų supratimas bei prioritizavimas: tikimybė rizikai atsirasti, rizikos poveikio įvertinimas bei rizikos atsiradimo laikas (kada, tikėtina, rizika galėtų atsirasti, jog galėtų būti planuojamas bei prioritizuojamas atsakas į rizikas)
- atsako į rizikas implementavimas, stebėjimas ir kontrolė.

PRINCE2 metodologija reikalauja, jog bent minimaliai atitiktų rizikų valdymo standartus, projektas turi turėti šiuos komponentus:

- rizikų valdymo modelio apsibrėžimas. Projekto komanda turi nusistatyti metodus kaip a) rizikos yra nustatomos ir vertinamos; b) kaip bus planuojamas ir vykdomas atsakas į rizikas; c) kaip bus komunikuojamas rizikų valdymo modelis projekto valdymo laikotarpiu. Taip pat nurodoma, jog privaloma įvertinti, ar nusistatytos rizikos gali turėti reikšmingos įtakos verslo planui (angl. business justification).

- rizikų registro forma, t.y. dokumentas, kuris talpintų tokią informaciją kaip identifikuotų rizikų sąrašas bei priimti sprendimai, susiję su rizikų analize, valdymu ir peržiūra.
- užtikrinimas, jog projekto metu rizikos nuolat būtų peržiūrimos, vertinamos ir kontroliuojamos.
- naudojimasis organizacijos jau sukauptu gerosios patirties bagažu ir įgytomis patirtimis iš ankstenių projektų.

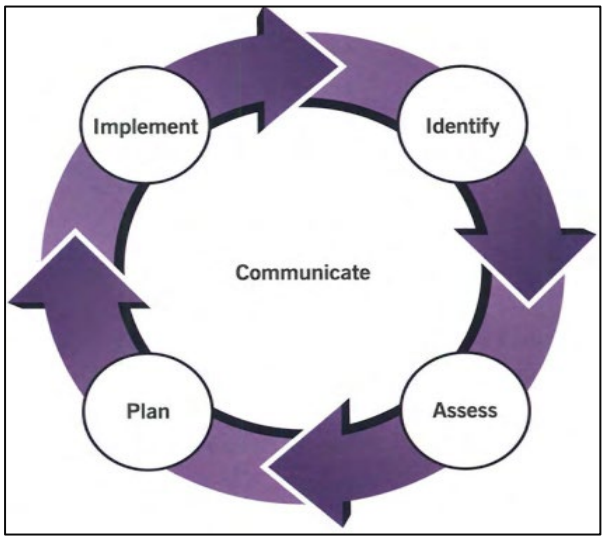
PRINCE2 metodologija reikalauja, jog rizikų valdymo etape būtų sukurti ir nuolat peržiūrimi du dokumentai: 1) rizikų valdymo gidas (dokumentas, kuriame nurodami įrankiai bei procesai, kurių pagalba organizuojamas rizikų valdymo etapas) 2) rizikų registras (dokumentas, kuriame nurodomos įsivertintos rizikos įtraukiant ir atnaujinant rizikų statusą, būseną ir istoriją) (Axelos, 2017). Šie dokumentai turi būti sudaryti projekto inicijavimo proceso metu. Rekomenduojama, jog rizikų valdymo metodika ir rizikų registras turi būti peržiūrimi bei galimai atnaujinami kiekvieno projekto valdymo etapo pabaigoje, tačiau kurdama rizikų valdymo metodika, projekto valdymo komanda turi pati nusistatyti kokiais būdais ir kaip dažnai šie dokumentai bus peržiūrimi bei atnaujinami.

Rizikų valdymo procedūra

Sudarant rizikų valdymo modelį, siūloma procesą skirtyti į 5 etapus:

1. konteksto ir rizikų identifikavimas
2. rizikų vertinimas
3. planavimas
4. implementacija
5. komunikacija

Pirmieji 4 etapai turėtų sekti chronologine tvarka (pabaigus pirmą etapą, pradedamas antras ir t.t.). Komunikacija turėtų būti vykdoma pagal poreikį visais etapais ir projektų valdymo komanda turėtų būti supažindinama su kiekvieno etapo rezultatais bei išvadomis. Jeigu atsiranda papildomos informacijos, rekomenduojama visus rizikų valdymo etapus kartoti iš naujo ir papildyti. Pažymima, jog rizikų valdymo modelis turi būti kuriamas atsižvelgiant į projekto aplinką (projekto mastą ir sudėtingumą bei rizikų keliamas grėsmes sėkmingam projektų vykdymui) siekiant išvengti užtikrinti efektyvų sprendimų priėmimo procesą.



Šaltinis: Axelos, 2017, p. 123

pav. 3 Rizikų valdymo procedūra

Konteksto vertinimo etape įvertinama bendra informacija apie projektą tokiais aspektais kaip kliento lūkesčiai; projekto sudėtingumas, svarba, kompleksiškumas ir kt. Pabrėžiama, jog rizikų identifikavimo etape svarbiausi aspektai yra rizikos įtraukimas į rizikos registrą iš karto ją indentifikavus bei gebėjimas aiškiai ir tiksliai apibūdinti rizikas tokiais aspektais: rizikos priežastingumas (galimi rizikos šaltiniai ar situacijos, leidžiančios rizikai atsirasti); rizikos poveikis (kokią įtaką rizikos išsipildymas turės projekto tikslams ir rezultatams). Siūloma į rizikos registrą įtraukti tokias kategorijas, kurios pildomos skirtingomis projekto rizikos valdymo procedūros etapais (Axelos, 2017):

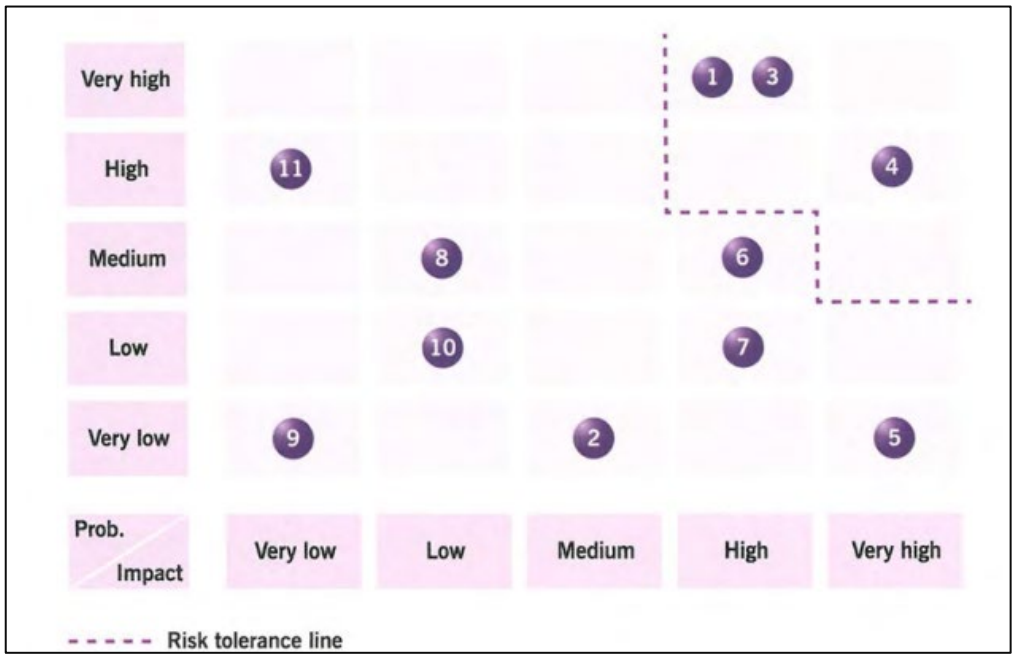
- rizikos identifikatorius (rizikai priskiriama unikali nuoroda, pavyzdžiui rizikos sunumeruojamos);
- rizikos autorius (asmuo, kuris identifikavo riziką);
- data (kada rizika buvo indentifikuota);
- rizikos kategorija (rizika įtraukiama į projekto komandos nustatytas kategorijas (projekto sritis, kurios bus paveiktos įvykus grėsmei/galimybei, pavyzdžiui projekto grafikas, kokybė ir pan.);
- rizikos aprašymas (nurodomas rizikos galimas priežastingumas, tipas (grėsmė ar galimybė) bei poveikis projektui);

- tikimybė, poveikis bei tikėtina vertė (siūloma projekto komandos pasirinktais metodais bei skalėmis nurodyti, kokia rizikos vertė, jeigu nebus įmamasi rizikos kontrolės veiksmų bei nurodyti vertę, jeigu rizika bus kontroliuojama);
- artumas (angl. proximity) (projekto komandos pasirinktais metodais ir skalėmis siūloma nurodyti, kokiu projekto valdymo etapu tikimasi, jog grėsmė/galimybė atsiras);
- atsakų į rizikas kategorijos (kaip projektų valdymo komanda skirstys atsakas į rizikas, pavyzdžiui galimos atsakų į grėsmes kategorijos: vengimas, mažinimas, perkėlimas ir pan.);
- atsakai į rizikas (kokių veiksmų, suderintų su atsakų į rizikas kategorijomis, bus imtąsi rizikai spręsti);
- rizikos statusas (nurodoma, ar rizika išspręsta ar ne);
- rizikos savininkas (asmuo, atsakingas už visus rizikos valdymo aspektus);
- rizikos vykdytojas (asmuo, atsakingas už veiksmų, nurodytų prie atsakų į rizikas įgyvendinimą. Rizikos vykdytojas gali būti arba nebūti tas pats asmuo kaip ir rizikos savininkas).

PRINCE2 nesiūlo būdų, kaip rizikos registro informacija turėtų būti pavaizduojama konkrečiai. Nurodoma, jog tą turi pasirinkti projekto valdymo komanda atsižvelgdama į prieš tai vykdytus projektus, gerąsiais praktikas bei projekto valdymo įrankius, naudojamus įmonės viduje (Axelos, 2017).

Kaip jau minėta, PRINCE2 metodologija rizikas vertina tiek per neigiamą, tiek per teigiamą prizmę, t.y. mato rizikas arba kaip galimybes (darančias teigiamą įtaką projekto rezultatams), arba kaip grėsmės. Konkrečių metodų kaip rizikos gali būti identifikuojamos nesiūloma, tiesiog minima, jog gali būti naudojamos tokios technikos kaip smegenų šturmas (angl. *brainstorming*), naudojimasis viešai prieinamų rizikų identifikavimo šablonais, sukurtais kitų metodologijų arba organizacijų.

Pabaigus konteksto ir rizikų identifikavimo etapą, pradedamas rizikų vertinimo etapas, tai yra reikia įverti tikimybę rizikoms atsirasti bei jų poveikį. PRINCE2 rekomenduojama rizikas įsivertinti šiais aspektais: grėsmių ar tikimybių atsiradimo galimybė bei jų poveikis projekto tikslams įvariuose projekto planavimo etapuose; kaip greitai numatoma rizikų atsiradimo tikimybė bei ar projekto valdymo komanda pakankamai kompetetinga suvaldyti rizikas (ar reikėtų perduoti kitoms komandoms, resursams). Siūloma naudotis tokiais įrankiais kaip tikimybės poveikio matrica, galimybių medžiai, pareto analizė. Gautų rezultatų santrauką rekomenduojama pavaizduoti diagrama PRINCE2 vadinama rizikos profiliu (Axelos, 2017). Sunumeruotos figūros nurodo riziką įtrauktą ir išsamiau aprašytą rizikų registre bei pavaizduojama rizikos tolerancijos linija.



Šaltinis: Axelos, 2017, p. 130

pav. 4 Rizikos profilio pavyzdys

Įsivertinus kiekvieną riziką atskirai, kitas etapas – bendras rizikų poveikio vertinimas, tai yra rekomenduojama įvertinti, kokią įtaką rizikos turi projektui ir ar gauti rezultatai atitinka organizacijos rizikos apetito (ang. *risk appetite*) ribas. Jeigu rizikos turi didesnį poveikį nei numatytas rizikos apetitas, reikia nusistatyti kontrolės veiksmus. PRINCE2 teigimu yra 2 pagrindinės rizikos vertinimo technikos: rizikos modelių kūrimas (siūloma pasitelkti Monte Carlo metodą) bei tikėtina piniginė vertė.

Rizikų planavimo etape reikia suplanuoti atsakus į nusistatytas ir įvertintas grėsmės ar galimybes. PRINCE2 siūlomi atsakai į rizikas pavaizduoti 1 lentelėje. Jeigu pasirenkama grėsmes sumažinti, likusi rizika vadinama likutine (ang. *residual risk*). Jeigu likutinė rizika išlieka didelė, rekomenduojama pasirinkti kelis atsakų tipus. Kai kuriais atvejais atsakų į riziką implementavimas gali sumažinti ar pašalinti kitas susijusias rizikas. Taip pat gali būti, jog atsakai į rizikas gali turėti įtakos paties projekto eigai bei sukelti antrines rizikas. Antrines rizikas taip pat būtina įdentifikuoti, įvertinti ir kontroliuoti tais pačiais metodais kaip ir pirmines rizikas. Svarbu tinkamai subalansuoti atsakų į rizikas kaštus atsižvelgiant į tikimybę grėsmėms įvykti bei jų poveikį.

Galimi atsakai į rizikas	Atsakų naudojimo kontekstas
Vengti grėsmės. Pasinaudoti galimybe.	Grėsmės vengimas reiškia, jog rizika bei aplinkybės grėsmei atsirasti yra pašalinamos, o galimybė panaudojama projekto naudai. Šis atsakas gali būti įgyvendinamas be papildomų lėšų, pavyzdžiui kitaip suplanuojant projekto įgyvendinimo veiksmus, tačiau dažniau šis atsakas pareikalaus papildomų lėšų.
Sumažinti grėsmę. Sudaryti palankias sąlygas galimybei atsirasti.	Planuojami konkretūs veiksmai, leidžiantys sumažinti grėsmės atsiradimo tikimybę arba jos daromą žalą. Galimybių kontekste planuojami atvirkštiniai veiksmai, tai yra padidinama tikimybė galimybei ir/ar teigiamam jos poveikiui atsirasti.
Grėsmių ar galimybių perdavimas.	Tai reiškia, jog grėsmės perduodamos trečiųjų šalių valdymui (dažniausias tokio atvejo pavyzdys galėtų būti draudimas).
Pasidalinimas grėsmėmis ar galimybėmis	Grėsmės ar galimybės dalinai perduodamos kitoms komandoms (pavyzdžiui tiekimo grandinės komandoms).
Grėsmių ar galimybių priėmimas.	Tai reiškia, jog organizacija nesiima jokių veiksmų, jog būtų išvengta grėsmių bei jų galimai padaryto poveikio. Tikimasi, jog aplinkybės išnaudoti galimybes susidarys savaime, o palankios sąlygos pasirodyti grėsmėms nesusidarys.
Nenumatytų atvejų plano sukūrimas	Dažnai tokie planai kūriami, jeigu pasirenkamas grėsmių/galimybių priėmimas kaip atsakas į rizikas (t.y. pasirenkama nesiimti jokių veiksmų rizikoms pašalinti/išnaudoti, tačiau sukuriamas planas, kas bus daroma, jeigu projekto eigoje susidarys palanki terpė grėsmėms/galimybėms pasirodyti) arba kaip atsarginis planas, kuriame numatoma, kas bus daroma jeigu kiti rizikų atsakų planai nesuveiks.

Šaltinis: sudaryta pagal Axelos, 2017, p. 132

lentelė 1 Galimi atsakai į rizikas

Suplanuoti atsakai į rizikas turi būti įgyvendinami praktiškai, stebimas jų efektyvumas bei įmamasi veiksmų, jeigu atsakai nepateisina lūkesčių. Nurodoma, jog svarbus rolių paskirstymas: kiekviena

identifikuota rizika turi turėti priskirtą rizikos savininką bei vykdytoją (angl. *risk actionee*). Rizikos savininkas yra atsakingas už visus rizikos valdymo aspektus (priežiūrą, kontrolę, efektyviausio rizikos atsako parinkimą ir pan.). Rizikos vykdytojas yra pavaldus rizikos savininkui ir yra atsakingas už rizikos atsako įgyvendinimą praktiškai. Dažnai rizikos savininkas ir rizikos vykdytojas yra tas pats asmuo.

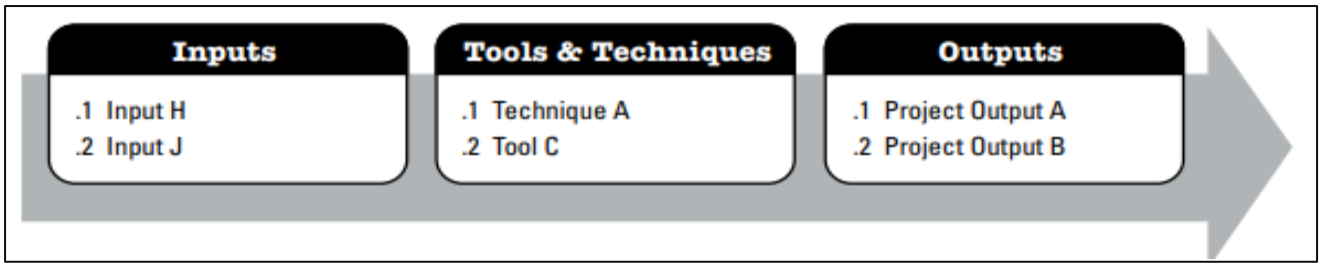
1.1.2 Apibendrinimas

PRINCE2 projektų valdymo metodologijoje akcentuojama rizikų valdymo procedūros svarba. Nurodoma, jog rizikų valdymas – tęstinis procesas, inicijuojamas projekto pradžioje bei vykdomas viso projekto metu. Vienas svarbiausiu rizikų valdymo aspektas – nuolatinė komunikacija apie rizikas bei jų statusą. Metodologijoje minimi įrankiai yra rekomendacinio pobūdžio, projektų valdymo komanda gali pati pasirinkti jiems priimtiną metodiką. Svarbiausia, jog rizikų valdymo praktika atitiktų PRINCE2 rizikų valdymo standartams keliamus reikalavimus. Kuriant rizikų valdymo modelį siūloma remtis *Management of Risk: Guidance for Practitioners (Office of Government Commerce, 2010)* knyga. Išsamiau apibūdinti tokie įrankiai: atsakai į rizikas (žr. lent. 1), rizikos profilis (žr. pav. 2) bei rizikų registras. Akcentuojama, jog rizikų valdymo proceso metu, svarbiausia sukurti rizikų valdymo planą bei rizikų registrą. PRINCE2 siūloma remtis organizacijos, įmonėmis gerosiomis praktikomis ir įgytomis pamokomis iš prieš tai vykdytų projektų. PRINCE2 metodologijoje siūloma vengti procesų, stabdančių proceso eigą. Rekomenduojama įsivertinti projekto kontekstą ir mastą, suteikti projekto vadovui galimybes savarankiškai priimti daugumą sprendimų siekiant užtikrinti, jog būtų išvengta biurokratijos bei procesai vyktų sklandžiai ir efektyviai.

1.2 PMBOK projektų valdymo metodologija

XX a. viduryje vykdant vis daugiau projektų įvairiose industrijose atsirado poreikis standartizuoti ir apibrėžti praktikas naudojamas projektų metu siekiant įtvirtinti projekto vadovo profesiją. US įkurta PMI (Project Management Institute) organizacija, kurios vienas iš tikslų ir buvo projekto valdymo metodikų standartizavimas (terminų, naudojamų projekto valdymo proseco metu, apibrėžimas ir metodikų bei geryjų praktikų aprašymas). 1996 metais išleistas pirmasis PMBOK (ang. *Project Management Body of Knowledge*) – geryjų projekto valdymo praktikų rinkinys, paremtas 1984 metais PMI išleista baltąja knyga (ang. *white paper*). PMBOK nuolat pildomas ir leidžiamos atnaujintos versijos. Paskutinį kartą PMBOK atnaujintas 2017 metais (Project Management Institute, 2017).

PMBOK pateikia tokį projekto apibrėžimą: laikinos pastangos siekiant sukurti unikalų produktą, paslaugą ar pasiekti tam tikrų rezultatų (Project Management Institute, 2017). Projekto gyvavimo ciklas – etapai per kuriuos turi pereiti projektas nuo projekto inicijavimo iki pabaigos. Projekto etapai yra tarpusavyje susiję: kiekvienas etapo metu pasitelkiant vieną ar kelis indėlius (ang. *input*) bei naudojantis įvariais įrankiais ir technikas sukuriamas tam tikras rezultatas (ang. *output*): indėlis, reikalingas kitam projekto etapui arba konkretus baigtinis proceso rezultatas.



Šaltinis: Project Management Institute, 2017, p.22

pav. 5 Projekto etapų ryšis

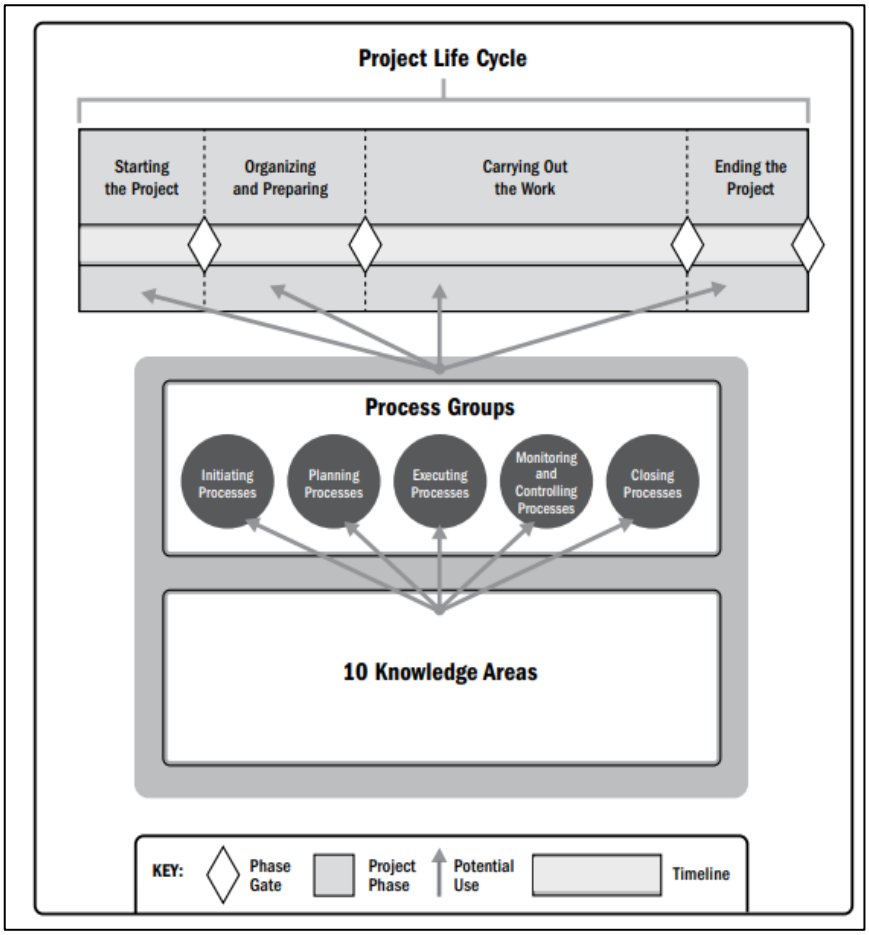
Projekto gyvavimo ciklas skirstomas į 5 procesų grupes:

1. inicijavimas
2. planavimas
3. vykdymas
4. stebėjimas ir kontrolė
5. užbaigimas

Papildomai procesai skirstomi į 10 žinių sričių. Kiekviena žinių sritis turi atskirus procesus, praktikas, indėlius, rezultatus bei įrankius ir metodikas. Skiriamos tokios žinių sritys:

1. projekto integravimo valdymas
2. projekto apimties valdymas
3. projekto tvarkaraščio valdymas
4. projekto kaštų valdymas
5. projekto kokybės valdymas
6. projekto resursų valdymas
7. projekto komunikacijos valdymas
8. projekto rizikų valdymas

9. projekto pirkimų valdymas
10. projekto suinteresuotų šalių valdymas



Šaltinis: Project Management Institute, 2017, p.18

pav. 6 Projekto gyvavimo ciklas

Atsižvelgiant į darbo tikslus, išsamiau bus aptariama projekto rizikų valdymo žinių sritis bei susiję procesai ir įrankiai.

1.2.1 Rizikų valdymas PMBOK projektų valdymo metodologijoje

PMBOK skiria 2 rizikų tipus: 1) individuali projekto rizika ir 2) bendra projekto rizika. Individuali rizika – neapibrėžtas įvykis ar sąlyga, kuriai įvykus, bus neigiamai arba teigiamai paveikti vienas ar keli projekto tikslai (Project Management Institute, 2017). Bendra projekto rizika – neapibrėžtumo visuma, kylanti iš skirtingų šaltinių ar individualių rizikų bei turinti įtakos (teigiamos arba neigiamos) galutiniam projekto tikslui. Nurodoma, jog rizikų gali atsirasti viso projekto gyvavimo ciklo laikotarpiu, todėl rizikų

valdymo procesas turi būti vykdomas paraleliai su kitais projekto valdymo procesais. Rizikų valdymo procesas inicijuojamas projekto planavimo etape. Pabrėžiama, jog svarbu apsvarstyti įvairaus pobūdžio rizikas bei galima poveikį projekto baigtiniam rezultatui bei planuojant rizikų valdymo procesą įvertinti projekto kontekstą (mastą, svarbą, sudėtingumą ir pan.) Rizikų valdymas susideda iš šių procesų (Project Management Institute, 2017):

1. Rizikų valdymo planavimas
2. Rizikų indentifikavimas
3. Kiekybinė rizikų analizė
4. Kokybinė rizikų analizė
5. Atsakų į rizikas planavimas
6. Atsakų į rizikas įgyvendinimas
7. Rizikų stebėjimas

Rizikų valdymo planavimo proceso metu nusistatoma kaip projekto gyvavimo ciklo metu bus valdomos rizikos. Rizikų valdymo planą reikia sudaryti ankstyvose projekto valdymo stadijose peržiūrint projekto eigoje siekiant užtikrinti, jog rizikų valdymas atitinka projekto kontekstą bei su projektu susijusių šalių lūkesčius. Rizikų valdymo planavimui reikalingi indėliai: projekto planas (ang. *project chatter*), projekto valdymo planas (visi komponentai), projekto dokumentai (suinteresuotų šalių sąrašas), organizacijos konteksto supratimas, organizacijos vidinių procesų supratimas. Rizikų valdymo planavimo etape naudojami įrankiai ir technikos: ekspertų konsultacija, duomenų analizė (pagrinde suinteresuotų šalių analizė), susirinkimai (Project Management Institute, 2017). Rizikų valdymo planavimo rezultatas – rizikų valdymo plano sukūrimas, kuriame turėtų būti nurodyti tokie komponentai:

- rizikos strategija (apžvalga kaip projekto metu bus valdomos rizikos);
- metodologija (nurodomi konkretūs įrankiai, procesai, informaciniai šaltiniai, kurių pagalba bus valdomos rizikos);
- rolės ir atsakomybės;
- finansavimas;
- laikas;
- rizikų kategorijos (nurodoma kaip identifikuotos rizikos bus kategorizuojamos). Siūloma naudoti rizikų išskirstimo struktūrą (ang. *risk breakdown structure*, RBS, pav. 7) – hierarchine tvarka suskirstyti galimus rizikų šaltinius;
- suinteresuotų šalių rizikos apetitas;

- rizikos atsiradimo tikimybės ir poveikio apibrėžtis. Nurodoma kokiomis skalėmis ir kategorijomis bus vertinamos grėsmių ir galimybių tikimybė. Kategorijų kiekis ir tipas priklauso nuo organizacijos ir projekto konkeksto;
- ataskaitų formatas;
- rizikų stebėjimo formatas.

RBS LEVEL 0	RBS LEVEL 1	RBS LEVEL 2
0. ALL SOURCES OF PROJECT RISK	1. TECHNICAL RISK	1.1 Scope definition
		1.2 Requirements definition
		1.3 Estimates, assumptions, and constraints
		1.4 Technical processes
		1.5 Technology
		1.6 Technical interfaces
		Etc.
	2. MANAGEMENT RISK	2.1 Project management
		2.2 Program/portfolio management
		2.3 Operations management
		2.4 Organization
		2.5 Resourcing
		2.6 Communication
		Etc.
	3. COMMERCIAL RISK	3.1 Contractual terms and conditions
		3.2 Internal procurement
		3.3 Suppliers and vendors
		3.4 Subcontracts
		3.5 Client/customer stability
		3.6 Partnerships and joint ventures
		Etc.
	4. EXTERNAL RISK	4.1 Legislation
		4.2 Exchange rates
		4.3 Site/facilities
		4.4 Environmental/weather
		4.5 Competition
		4.6 Regulatory
		Etc.

Šaltinis: Project Management Institute, 2017, p.406

pav. 7 RBS

Rizikų identifikavimo etapu rizikos yra identifikuojamos ir aprašomos jų charakteristikos. Procesas yra tęstinis ir vykdomas viso projekto metu. Rizikas identifikuoti siūloma tokiais įrankiais ir metodais:

- ekspertų nuomonė. Rizikas identifikuoti kviečiami savo srities specialistai.
- informacijos rinkimas. Siūlomos tokios technikos kaip a) smegenų šturmas (angl. brainstorming): kviečiami specialistai, nesusiję su projekto valdymo komanda, gali būti naudojamos prieš tai

įsivardintos rizikų kategorijų grupės (arba pristatomas RBS planas). Kadangi ši technika yra laisvo formato, svarbu, jog sugeneruotos idėjos būtų tiksliai ir aiškiai įvardintos ir apibūdintos. b) Kontrolinis sąrašas: sąrašas galimų rizikų, identifikuotų ankstesnių projektų metu arba pasitelkiant istorinę panašių projektų išmoktų pamokų informaciją. Nurodoma, jog neįmanoma sudaryti baigtinio visų įmanomų rizikų sąrašo, todėl organizacijos viduje toks sąrašas turėtų būti nuolat peržiūrimas ir pildomas. Taip rekomenduojama pasitelkti ir kitas rizikų identifikavimo technikas. c) Interviu: patikimoje aplinkoje apklausiami savo srities ekspertai, suinteresuotos projekto šalys ir kiti projekto dalyviai išlaikant jų nuomonės konfidencialumą siekiant užtikrinti, jog asmenys pateiks objektyvią ir nešališką nuomonę.

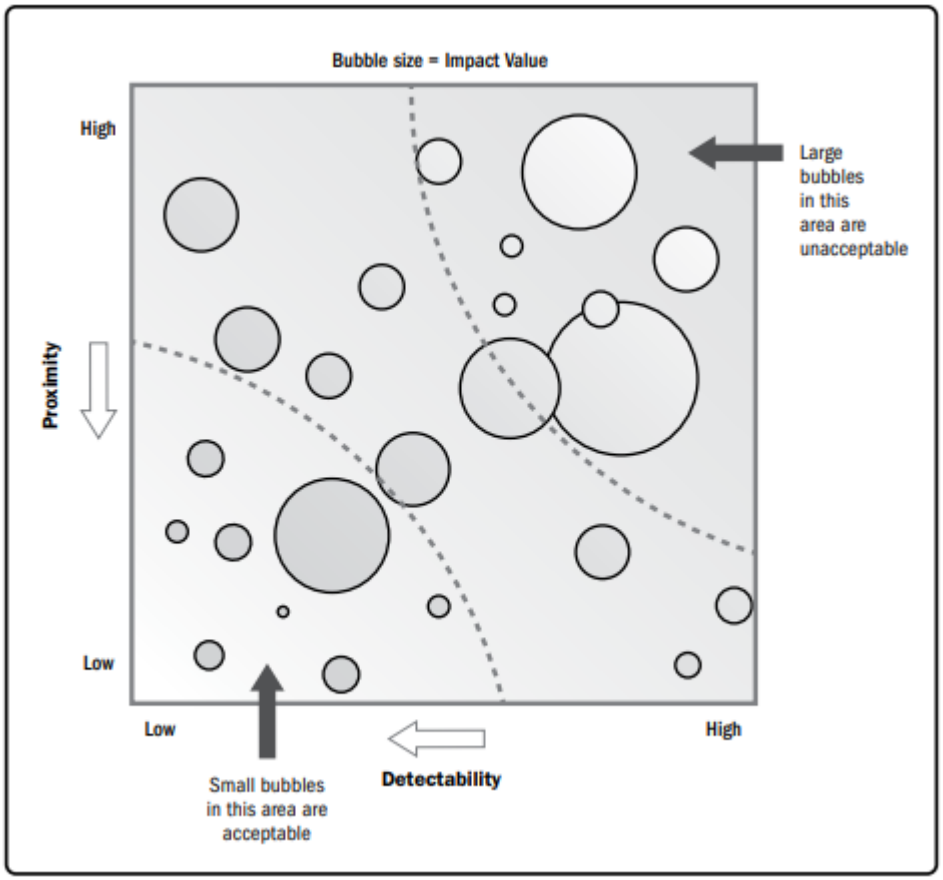
- informacijos analizė. Siūloma pasitelkti tokius įrankius kaip a) pagrindinių priežasčių analizė: grėsmės ir galimybės identifikuojamos nagrinėjant galimų problemų atsiradimo ar projektui naudą atnešančias priežastis (pvz. kaip problema identifikuojama vėlavimas užbaigti projektą, tuomet svarstoma, kokie veiksniai gali turėti tam įtakos). b) projekto apribojimų ir prielaidų analizė. c) SWOT analizė: įvertinamos projekto stipriosios, silpnosios pusės. Iš stipriųjų projektų pusių identifikuojamos projekto galimybės, iš silpnųjų – projekto grėsmės. d) Dokumentų analizė: nagrinėjami su projektų susiję dokumentai (planai, prieš tai buvusių projektų dokumentacija, kontraktai, techninė dokumentacija ir pan.) Neaiškios, dviprasmiškos dokumentų pusės, informacijos nesutapimas lyginant dokumentus gali padėti identifikuoti projekto rizikas.
- susirinkimai bei asmeniniai ir komandiniai įgūdžiai: gebėjimas efektyviai organizuoti grupės žmonių susitikimą, kurio metu būtų pasiekta susitarimų, sprendimų ir pan. Įgudęs tarpininkas gali pagelbėti grupei susikoncentruoti ties rizikų identifikavimo užduotimi, teisingai panaudoti rizikų identifikavimo technikas, užtikrinti, jog identifikuotos rizikos būtų aiškiai įvardinamos ir apibūdinamos.
- greitieji sąrašai (angl. prompt list): iš anksto sudarytų rizikos kategorijų sąrašų naudojimas (pvz. PESTLE, TECOP analizės įrankiai), galinčių padėti įsivertinti rizikas įvairiais rakursais.

Rizikų identifikavimo etapo pabaigoje inicijuojamas rizikų registro dokumentas, kuriame pateikiama tokia informacija: rizikų sąrašas (rizikai suteikiamas unikalus identifikatorius, rizika aiškiai aprašoma), potencialus rizikos savininkas, kuris galutinai bus patvirtintas įvykdžius kokybinę rizikos analizę, numatomi atsakai į rizikas, kurie galutinai patvirtinami atsakų į rizikas planavimo etape. Taip pat inicijuojamas rizikos ataskaitos dokumentas, kuris nuolat pildomas visos rizikos valdymo procedūros laikotarpiu. Rizikos indentifikavimo etapo pabaigoje, rizikos ataskaitos dokumente

nurodomi šaltiniai, keliantys riziką visam projektui bei nurodomas skaičius indentifikuotų individualių rizikų bei su jomis susijusios tendencijos.

Kokybinės rizikų analizės proceso metu individualios rizikos yra vertinamos rizikų atsiradimo tikimybės, poveikio ir kitais aspektais su tikslu rizikas prioritizuoti. Nurodoma, jog toks rizikų vertinimas yra subjektyvus ir priklauso nuo projekto valdymo komandos bei kitų suinteresuotų šalių teikiamų prioritetų (Project Management Institute, 2017). Jeigu kokybinė rizikų analizė vykdoma pasitelkiant tarpininką, vienas iš pagrindinių tarpininko tikslų turėtų būti subjektyvaus vertinimo tendencingumo nustatymas. Kokybinė rizikų analizė vykdoma pasinaudojant tokiais įrankiais bei technikomis:

- ekspertų vertinimas apklausiant specialistus ar vykdant grupinius susirinkimus;
- informacijos rinkimas;
- informacijos analizė įvertinant jau turimos informacijos apie rizikas tikslumą ir patikimumą susirinkimų su suinteresuotomis šalimi metu ar naudojant apklausos metodą kiek tiksli ir patikima jau turima informaciją apie rizikas;
- rizikų tikimybės ir poveikio vertinimas. Įvertinama kiekviena identifikuota rizika nustatant jos atsiradimo tikymybę bei poveikį tokioms sritims kaip laikas, kaštai, kokybė ir pan. Tikimybei ir poveikiui įvertinti gali būti naudojamos tokios technikos kaip ekspertų apklausą, susirinkimai su suinteresuotomis šalimis vertinant rizikos atsiradimo tikimybės ir poveikio apibrėžtimis, nusistatytomis rizikų valdymo planavimo etapu;
- kitų rizikų parametrų vertinimas: rizikas galima vertinti ir kitais aspektais (šalia tikimybės ir poveikio) pavyzdžiui gebėjimas kontroliuoti riziką, tikėtinas rizikos pasirodymo laikas projekto eigoje ir pan. Papildomų faktorių įsivertinimas gali padėti tiksliau prioritizuoti rizikas;
- rizikų kategorizavimas: indentifikuotas rizikas galima skirstyti į platesnes kategorijas (pavyzdžiui pagal rizikų atsiradimo priežastis, poveikio sritis). Toks rizikų grupavimas gali padėti efektyviau valdyti rizikų grupes bei identifikuoti problematiškiausias projekto sritis;
- informacijos atvaizdavimas: rekomenduojama pasitelkti tokias technikas kaip tikimybės ir poveikio matrica arba hierarchiją atspindys grafikai, jeigu rizikos vertinamos daugiau negu dvejomis kategorijomis. Tokio grafiko pavyzdys galėtų būti burbulinė diagrama (angl. *bubble chart*, pav. 8) reprezentuojanti 3 kategorijas x ir y ašimis bei burbulio dydžiu.



Šaltinis: Project Management Institute, 2017, p.426

pav. 8 Burbulinė diagrama

Kiekybinės rizikų analizės metu identifikuotos rizikos apskaičiuojamos siekiant išreikšti jų poveikį matematine reikšme bei efektyviau suplanuoti atsakas į rizikas (Project Management Institute, 2017). Kiekybiniai rizikų analizei atlikti reikia patikimos informacijos. Kiekybinė rizikų vertinimo analizė dažnai atliekama naudojantis tam skirta programine įranga, rezultatai interpretuojami pasitelkus ekspertus. Tokio tipo analizė reikalauja nemažai kaštų ir papildomo laiko, todėl nerekomenduojama vykdant mažos apimties ar ne kompleksiškus projektus. Kiekybinei analizei atlikti rekomenduojami tokie įrankiai kaip:

- ekspertų vertinimas. Rizikų vertinimo specialistai gali padėti parinkti tinkamus įrankius analizei atlikti bei padėti interpretuoti rezultatus;
- neapibrėžtumo faktoriaus vaizdavimas: atliekant kiekybinį rizikos vertinimą reikia kiekybinio rizikos vertinimo modelyje reikia pavaizduoti individualias projekto rizikas bei kitus nežinomuosius. Kai nėra aiški planuojamo veiksmo trukmė, kaštai ar resursai, galimybių skalę rizikos vertinimo modelyje galima pavaizduoti atsitiktinio dydžio reikšmių skirstiniais. Dažniausia naudojami

trikampio, normalus, beta, diskretusis skirstiniai. Skirstiniais galima pavaizduoti ir individualias projekto rizikas, taip pat šias rizikas galima rizikų vertinimo modelyje galima pavaizduoti medžio diagramos šakomis;

- informacijos analizė naudojant simuliacijas (viena populiariausiu - Monte Carlo analizė), jautrumo analizės metodą, sprendimo medžio analizės metodą ar įtakos diagramas.

Įvertinus rizikas sudaromi atsakų į rizikas planai. Parenkant optimalius atsakus į rizikas siūloma konsultuotis su ekspertais, patyrusiais bei savo srities specialistais, ypač planuojant atsakus į technines ar kompleksiškas rizikas. Skiriamos 5 strategijos planuojant atsakus į grėsmes/galimybes, efektyviausia rinktis strategiją, susidedančią iš kelių komponentų:

- eskalacija;
- grėsmės vengimas/pasinaudojimas galimybe;
- grėsmės perkėlimas/pasidalinimas galimybe;
- grėsmės sušvelnimas/galimybės padidinimas;
- priėmimas

Siūlomi ir alternatyvūs atsakų į rizikas sprendimai, pavyzdžiui išlaidų ir naudos analizė: jeigu riziką galima įvertinti piniginę išraiška, tuomet naudinga įsivertinti, ar sprendimas teiks daugiau naudos, negu kainuos jį įgyvendinti. Rekomenduojamos įvairios sprendimų priėmimo technikos pasirenkant atsakų į rizikas strategiją, pavyzdžiui daugiakriterinė sprendimų analizė, kuriai atlikti gali būti pasirenkami šie kriterijai analizei atlikti: atsakų į rizikas kaštai, numatomas sprendimų efektyvumas, resursų prieinamumas, laiko apribojimai, poveikio mastas įvykus rizikai ir pan.

Atsakų į rizikas įgyvendinimo etapas yra skirtas užtikrinti, jog suplanuoti atsakai yra rizikas įgyvendinami praktiškai. Siūloma remtis ekspertų patarimais nustatant efektyviausius įgyvendinimo metodus, taip pat asmeniniais ir komandiniais įgūdžiais siekiant užtikrinti, jog asmuo, indentifikuotas kaip rizikos savininkas imtųsi suplanuotų atsakų į rizikas veiksmų.

Rizikų stebėjimo proceso metu stebimas atsakų į rizikas įgyvendinimo progresas ir veiksmingumas, identifikuojamos ir analizuojamos galimos naujos rizikos siekiant užtikrinti viso projekto sprendimų priėmimo efektyvumą, remiantis nuolatos atnaujinama informaciją ir naudojantis šiais įrankiais:

- informacijos analizė: galima taikyti techninės veiklos analizę (techninės kategorijos rizikoms) ar rezervų analizę (rezervų, skirtų nenumatytiems atvejams lyginimas su likutinėmis rizikomis);
- auditas: rizikų auditas gali būti naudojamas užtikrinti rizikos valdymo proceso efektyvumą. Rizikos audito formatas ir tikslas turi būti aiškiai nurodomi prieš inicijuojant rizikos auditą;

- susirinkimai: siekiant nustatyti rizikų valdymo proceso efektyvumą galima reguliariai organizuoti rizikų peržiūrėjimo (angl. *risk review*) susirinkimus, kurių metu peržiūrima rizikų valdymo procesų dokumentacija, esant reikalui iš naujo įvertinamos identifikuotos rizikos, uždaromos nebeaktualios rizikos, identifikuojamos antrinės rizikos, galinčios kilti sudarius atsakų į rizikas strategijas.

1.2.2 Apibendrinimas

Rizikų valdymo procesai PMBOK išsamiai ir detaliai aprašytas. Teorijoje siūlomas platus spektras įrankių ir metodikų, galimai padedančių nuosekliai įgyvendinti rizikų valdymo proceso etapus praktikoje. Akcentuojama, jog kiekybinė rizikų valdymo analizės metodai turėtų būti taikomi tik sudėtingiems ar didelio masto projektams. Taip pat nurodoma, jog rizikų valdymas - tęstinis procesas: rekomenduojama rizikas nuolat peržiūrėti. Rizikų valdymo procesuose siūlomi 36 įrankiai ir metodikos. Kai kurie įrankiai detalizuoti ir papildyti specifinėmis technikomis, skirtomis įgyvendinti tam tikras procesų užduotis (žr. lent. 2).

Rizikų valdymo etapai	**Siūlomi įrankiai**
Rizikų valdymo planavimas	Ekspertų nuomonė, informacijos analizė, susirinkimai.
Rizikų indentifikavimas	Ekspertų nuomonė, informacijos rinkimas (smegenų šturmo technika, interviu), informacijos analizė (priežasčių analizė, SWOT analizė, dokumentų analizė), asmeniniai ir komandiniai įgūdžiai, susirinkimai, greitieji sąrašai (PESTLE, TECOP analizės įrankiai).
Kokybinė rizikų analizė	Ekspertų nuomonė, informacijos rinkimas (interviu), informacijos analizė (rizikos duomenų kokybinis vertinimas, rizikų atsiradimo tikimybės bei poveikio vertinimas, kitų rizikų veiksnių vertinimas), asmeniniai ir komandiniai įgūdžiai, rizikų kategorizavimas, informacijos vizualizavimas (tikimybės ir poveikio matrica, hierarchiją atspindintys grafikai), susirinkimai.
Kiekybinė rizikų analizė	Ekspertų nuomonė, informacijos rinkimas (interviu), asmeniniai ir komandiniai įgūdžiai, neapibrėžtumo faktoriaus vaizdavimas, informacijos analizė (simuliacijos, jautrumo analizė, sprendimo medžio analizė, įtakos diagramos).

Atsakų į rizikas planavimas	Ekspertų nuomonė, informacijos rinkimas (interviu), asmeniniai ir komandiniai įgūdžiai, grėsmių strategijos, galimybių strategijos, nepaprastosios padėties strategija, informacijos analizė (išlaidų ir naudos analizė), sprendimų priėmimo technikos (daugiakriterinė sprendimų analizė).
Atsakų į rizikas įgyvendinimas	Ekspertų nuomonė, asmeniniai ir komandiniai įgūdžiai (įtaka), projektų valdymo IT programos.
Rizikų stebėjimas	Informacijos analizė (rezervų analizė, techninės veiklos analizė), auditai, susirinkimai.

lentelė 2 PMBOK rizikų valdymo įrankiai

1.3 Skyriaus išvados

PRINCE2 ir PMBOK metodologijose į rizikos valdymo procesą žiūrima panašiai: rizikos skirstomos į grėsmes arba galimybes, akcentuojama vidinės komunikacijos svarba ir pabrėžiama, jog rizikų valdymas – tęstinis procesas, siūlomos identiškos atsakų į rizikas strategijos. Vienas iš esminių šių metodologijų skirtumų yra tas, jog PRINCE2 akcentuojama, jog nėra svarbu, kokiais praktiniais metodais bus vadovaujamasi rizikų valdymo procese (svarbiausia, kad rizikų valdymo praktika atitiktų PRINCE2 rizikų valdymo standartams keliamus reikalavimus). Kuriant rizikų valdymo modelį siūloma remtis *Management of Risk: Guidance for Practitioners (Office of Government Commerce, 2010)* knyga.

Įvertinus PRINCE2 ir PMBOK metodologijų siūlomus rizikų valdymo procesus, galima daryti išvadą, jog šios metodologijos vieną kitą papildo: PRINCE2 išsamiai aprašyta teorinė dalis, kai kuriems procesams įvykdyti aprašant galimus naudoti įrankius akcentuojant jų rekomendacinį pobūdį. Tuo tarpu PMBOK šalia teorinės dalies, savo esme sutampančia su PRINCE2 teorine dalimi, struktūruotai pateikiami įrankių rinkiniai, kurie galimai turėtų padėti pasiekti procesų užduotis, todėl atvejo studijai bus naudojamasi PMBOK metodologija.

Prielaidą, jog remiantis PMBOK siūloma rizikų valdymo metodologija galima sudaryti KS rizikų valdymo modelį SVV įmonei, papildo tarptautinio standarto ISO/IEC 27001 „Informacijos saugos vadybos sistema“ keliami rizikų valdymo reikalavimai bei gairės. ISO/IEC 27001 standarte nurodoma (ISO 27001,

2013), jog rizikų valdymo procedūra susideda iš 5 etapų: rizikų vertinimo plano sudarymas (nurodant tokius komponentus kaip rizikų apetitas, rizikų atsiradimo tikimybių ir poveikio apibrėžtys bei kt.), rizikų identifikavimas, rizikų analizė, rizikų valdymo strategijų parinkimas. Visi šie etapai yra apibūdinti PMBOK metodologijoje kartu pateikiant įrankių rinkinius.

2. RIZIKŲ VALDYMO PLANO KŪRIMAS SVV ĮMONEI: ATVEJO STUDIJA

Vienas iš šio darbo tikslų – praktiškai pritaikyti PMBOK rizikų valdymo strategijos metodologiją sudarant kibernetinio saugumo rizikų valdymo modelį smulkaus ir vidutinio verslo įmonei. Tam buvo pasirinkta SVV įmonė, įsikūrusi vakarų Lietuvoje ir teikianti dujotekių projektavimo paslaugas. Įmonės gyvavimo trukmė – daugiau negu 10 metų ir joje dirba 3 darbuotojai. Įmonės vadovas nenorėjo, jog įmonės pavadinimas būtų nurodytas bei įmonė galima identifikuota dėl saugumo priežasčių, todėl toliau vadinsime įmonę X. Įdomu pažymėti, jog šiuo atveju KS rizikų valdymo plano kūrimas gali būti traktuojamas kaip projektas (t.y. laikina veikla, skirta sukurti unikalų rezultatą - KS rizikų valdymo modelį) naudojant visus PMBOK metodologijoje nurodytus projekto valdymo etapus, tačiau atsižvelgiant į darbo tikslus, bus naudojamasi tik PMBOK rizikų valdymo plano kūrimo metodika. Kibernetinio saugumo rizikų valdymo modelis bus sudaromas iš eilės aprašant kiekvieną iš 7 PMBOK rizikų valdymo etapų ir pritaikant rekomenduojamus įrankius bei metodikas. KS rizikų valdymo modelis bus sudaromas šio darbo autoriaus konsultuojantis su įmonės X vadovu dėl šių specifinių aspektų bei prašant savarankiškai atlikti tam tikras užduotis:

- įmonei primtinos KS rizikų valdymo dokumento pateikimo formos;
- rizikų valdymo strategijos;
- rizikų atsiradimo tikimybių ir poveikio apibrėžčių vertinimo nustatymo;
- rizikų apetito;
- rizikų identifikavimo ir įvertinimo (atliko įmonės vadovas su personalu);
- atsakų į rizikas valdymo strategijų;
- atsakų į rizikas veiksmų (atliko įmonės vadovas);
- rizikų ir atsakų į rizikas veiksmų savininko priskyrimo;
- rizikų stebėsenos ir kontrolės periodiškumo.

Susitikimai su įmonės X vadovu buvo organizuojami nuotoliniu būdu naudojantis Zoom platforma. Iš viso organizuotos 7 sesijos: pirmosios sesijos metu, pristačius darbo tikslus bei veiksmų eigą, inicijuotas pirmasis KS rizikų valdymo modelio sudarymo etapas (rizikų valdymo planavimas). Tolimesnėse sesijose pristatomi ankstesnio etapai rezultatai, supažindinama su kito etapo teorine dalimi ir tikslais, konsultuojamasi su įmonės X vadovu dėl specifinių aspektų.

Įmonės X veiklos specifika - dujotiekių projektavimas AutoCad programine įrangą bei dujotiekio projekto plano derinimas su AB ESO privatiems asmenims, įmonėms ir viešojo sektoriaus įstaigoms. Įmonė daugiausia operuoja tokiais dokumentais kaip pastato nuosavybės dokumentai (namo kadastrinė byla, registro centro išrašas), už paslaugas klientai atsiskaito pavedimu arba grynaisiais pinigais. Buhalterija tvarkoma samdant išorinę buhalterijos įmonę. IT ūkį sudaro 4 kompiuteriai: 2 stacionarūs kompiuteriai (su XP ir Windows 10 programinėmis įrangomis), 2 nešiojamieji kompiuteriai (su Windows 10 programine įranga), braižytuvas (angl. plotter). Taip pat įmonė turi tokius periferinius įrenginius: 4 spausdintuvai su skanavimo funkcija, 4 mobilieji telefonai (Samsung Galaxy S 20 ir iPHONE 12). Mobilieji telefonai skirti ne tik komunikacijai, jais fotografuojamos objekto dalys (pastato, kuriam bus projektuojamas dujotekis), nuotraukos perkeliamos į kompiuterius. Įrenginiai sujungti į privatų tinklą: pagrindinė tinklo paskirtis - naudojamasi „shared drive“ funkcija dalintis dokumentais ir saugoti informacijai bei kompiuteriams komunikuoti su spausdintuvais bei skanavimo įrenginiais.

Įmonė taip pat naudojasi Google Drive platforma saugoti bei dalintis dokumentais, Gmail elektroniniu paštu komunikuoti su klientais ir tarpusavyje bei Messenger platforma komunikuoti įmonės viduje. 2 darbuotojai nuolat dirba įmonės biuro pastate, 1 darbuotojas dirba nuotoliniu būdu iš kito miesto.

Gavus užsakymą iš kliento standartinė įmonės X užsakymo vykdymo procesų schema atrodo šitaip: a) įmonės X darbuotojas nubraižo dujotiekio projektą AutoCad programinę įranga; b) projektas įkeliamas į AB ESO svetainę derinimui; c) AB ESO darbuotojas įvertiną projektą ir atsiunčia atsakymą įmonės X elektroniniu paštu; d) įmonės X darbuotojas atspausdina dujotiekio projektą ir fiziškai pristato užsakovui.

2.1 Rizikų valdymo planavimas

Šio etapo tikslas – rizikų valdymo plano inicijavimas nurodant tokius plano komponentus kaip rizikų valdymo strategija, rolės ir atsakomybės, rizikų kategorijos, suinteresuotų šalių rizikos apetitas, rizikų atsiradimo tikimybių ir poveikio apibrėžtys. PMBOK nesiūlomas rizikų valdymo plano šablonas, todėl jis bus sudaromas laisva forma nurodant reikiamus komponentus (priedas 1).

Valdymo strategija: įmonė nusistato pati. Pasirinkta kibernetinio saugumo rizikų valdymo modelį peržiūrėti kas ketvirtį.

Rolės ir atsakomybės: įmonė nusistato pati. Šiuo atveju už rizikų savininku pasirinko būti įmonės X vadovas.

Rizikų kategorijos: PMBOK pateikiamas toks rizikų kategorizavimo formatas (žr. lent. 3). Įdentifikuojant kategorijas, rekomenduojama remtis gerosios praktikomis, ekspertų patarimais.

Rizikos kategorija 0	**Rizikos kategorija 1**	**Rizikos kategorija 2**
Visos įmonės X kibernetinio saugumo rizikos	1. Technologijos	1.1. Techinė įranga
		1.2. Programinė įranga
		1.3. Infrastruktūra
	2. Žmogiškieji ištekliai	2.1. Įmonės darbuotojai
		2.2. Klientai
		2.3. Kiti trečiųjų šalių atstovai (įmonė, teikianti buhalterijos paslaugas bei AB ESO)
	3. Duomenys	3.1. Klientų kontaktiniai duomenys

		1.2. Istoriniai dujotekių projektai
		1.3. Įmonės praktinė patirtis

lentelė 3 Įmonės X rizikų kategorijų struktūra

Rizikų apetitas: įmonė X pasirinko valdyti rizikas, turinčias didelę tikimybę atsirasti ir turinčias didelį poveikį.

Rizikų atsiradimo tikimybių ir poveikio apibrėžtys: naudojamos PMBOK rekomenduojamos rizikų atsiradimo tikimybių ir poveikio apibrėžtys (žr. lent. 4), kurios vertinamos 3 kategorijų skale (maža, vidutinė ir didelė). Kadangi vertinamos kibernetinio saugumo rizikos, poveikį rekomenduojama matuoti atsižvelgiant į kibernetinio saugumo triados kontekstą, t.y. informacijos konfidencialumą, vientisumą ir prieinamumą (Kohke, Sigler, Shoemaker, 2017). Galimų rizikų atveju bent viename iš šių komponentų, tikėtinas tiesioginis poveikis įmonės materialiems (finansiniams) ar/ir nematerialiems (įmonės reputacija) ištekliams. Įmonės X vadovas nurodė, jog svarbiausias nematerialusis įmonės išteklius yra įmonės reputacija, t.y. klientų pasitenkinimas, kurį pagrinde lemia sutartas projektų padarymo ir suderinimo terminas (ar projektas įvykdomas sutartu laiku, ar terminas pratęsiamas), kuris rizikų atsiradimo tikimybių ir poveikio apibrėžties lentelėje bus įvardyjamas kaip laikas. Įmonės X vadovas nurodė, jog standartinė tikėtina projektų vėlavimo paklaida ~ 3 d.d.

Skalė	Tikimybė	Poveikis	
		Finansinis	Laikas
Didelė	66 – 100%	Didelis poveikis: finansiniai nuostoliai > 1000EUR.	Prarandami užsakovai arba > 6 d.d. vėluojama užbaigti projektą.
Vidutinė	30 – 66%	Vidutinis poveikis: finansiniai nuostoliai 500 – 1000 EUR.	Projekto užbaigimo terminas nukeliamas 3 - 6 d.d.
Maža	0 – 33%	Mažas poveikis: finansiniai nuostoliai <500 EUR.	Projektas užbaigiamas laiku arba vėluojama pristatyti iki 3 d.d.

lentelė 4 Įmonės X rizikų atsiradimo tikimybių ir poveikio apibrėžčių lentelė

2.2 Rizikų identifikavimas

Šiuo etapu vykdoma rizikų identifikacija ir inicijuojamas rizikų registro dokumentas, kuriame nurodomos ir aiškiai aprašomos identifikuotos rizikos, rizikų savininkas, PMBOK nurodoma, jog rizikų registras gali būti kuriamas laisva forma jame taip pat nurodant kitas reikiamas kategorijas, pavyzdžiui rizikos statusą, rizikos atsiradimo priežastis, detalesnį poveikio apibūdinimą ir panašiai (žr. pav 9).

Rizikos nr.	Rizikos kategorija	Rizikos pavadinimas	Tikimybė	Poveikis	Rizikos vertinimas	Atsakų į rizikas strategija	Rizikų vertinimo data	Rizikų atsiradimo priežastys	Atsakų į rizikas veiksmai	Atsakų į rizikas veiksmų įgyvendinimo data	Už riziką atsakingas asmuo	Už atsakų į rizikas veiksmus atsakingas asmuo	Atsakų į rizikas veiksmų statusas	Rizikos statusas
R14	Infrastruktūra	14. Vidinio įmonės tinklo sutrikimai.	1	2	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Techniniai gedimai	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R15		15. Mobilaus ryšio neprieinamumas.	2	1	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Trečiųjų šalių klaidos	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira

pav. 9 Rizikų registro kategorijų pavyzdys

PMBOK siūlomos rizikų identifikavimo technikos yra susijusios su informacijos rinkimu ir analize įvairiomis formomis (dokumentacijos peržiūrėjimas, mokymasis iš gerųjų patirčių, SWOT analizė). Pasirinktas pagrindinių priežasčių analizės metodas (angl. *root cause analysis*) kibernetinio saugumo kontekste (t.y. identifikuojant galimas problemas, keliančias grėsmę informacijos vientisumui, konfidencialumui ir prieinamumui) nurodant pagrindines galimas šių problemų atsiradimo priežastis.

KS Aspektas	**Problema**	**Galimos atsiradimo priežastys**
Informacijos prieinamumas	Žala įmonės techniniam inventoriui	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės programinei įrangai	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Duomenų praradimas, nepasiekiamumas	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės infrastruktūrai	Kibernetinės grėsmės
		Žmogiškieji ištekliai

		Nenugalima jėga
		Kitos priežastys
Informacijos konfidencialumas	Duomenų praradimas	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
Informacijos vientisumas	Duomenų praradimas, nepasiekiamumas	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės techniniam inventoriui	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės programinei įrangai	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys

lentelė 5 Įmonės X pagrindinių priežasčių analizė

Atlikus analizę identifikuotos 4 pagrindinės problemos (potencialios rizikos), kurioms atsiradus kiltų grėsmė informacijos konfidencialumui, saugumui ir vientisumui bei atsirastų potenciali grėsmė įmonės X veiklai taip pat kiltų galimų materialinių ir/ar nematerialinių nuostolių. Potencialios rizikos:

1. žala įmonės techninei įrangai
2. žala įmonės programinei įrangai
3. žala įmonės infrastruktūrai
4. duomenų praradimas.

PMBOK metodologija pildant rizikų registrą reikalauja kuo detaliau ir tiksliau aprašyti galimas rizikas. Rekomenduojama nurodyti ir galimas aplinkybes ar priežastis rizikai išsipildyti. Įmonės X vadovas kartu su darbuotojais detalizavo rizikų kategorijas ir identifikavo rizikas, nurodytas 5 lentelėje, kurios nurodytos ir rizikų registre (priedas 1). Nepriklausomai nuo įmonės ar organizacijos dydžio, darbuotojai, t.y. žmogiškasis faktorius bei tyčinės ar netyčinės klaidos – viena pagrindinių priežasčių, suteikiančių galimybes atsirasti KS grėsmėms (Tareq, Nicholson, 2018, Joaquin, Kemp, 2019, Hodson, 2019).

Rizikos kategorija	**Rizika**	**Priežastys**
Techninė įranga	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	Darbuotojų klaidos, įrangos nepriežiūra, įrangos nusidėvėjimas, kibernetinės atakos, nenugalima jėga.
	2. Kompiuterių praradimas	Darbuotojų klaidos, vagystės, nenugalima jėga.
	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	Darbuotojų klaidos, įrangos nepriežiūra, įrangos nusidėvėjimas, kibernetinės atakos, nenugalima jėga.
	4. Spausdintuvų praradimas	Darbuotojų klaidos, vagystės, nenugalima jėga.
	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	Darbuotojų klaidos, įrangos nepriežiūra, įrangos nusidėvėjimas, kibernetinės atakos, nenugalima jėga.

	6. Mobiliųjų telefonų praradimas.	Darbuotojų klaidos, vagystės, nenugalima jėga.
Programinė įranga	7. Kompiuterių programinės įrangos gedimai.	Darbuotojų klaidos, įrangos nepriežiūra, kibernetinės atakos.
	8. Telefonų programinės įrangos gedimai.	Darbuotojų klaidos, įrangos nepriežiūra, kibernetinės atakos.
	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger).	Darbuotojų klaidos, trečiųjų šalių klaidos, kibernetinės atakos.
Duomenys	10. Istorinių projektų praradimas.	Darbuotojų klaidos, kibernetinės atakos, techniniai sutrikimai.
	11. Istorinių projektų nepasiekiamumas.	Darbuotojų klaidos, kibernetinės atakos, techniniai sutrikimai.
	12. Klientų duomenų praradimas.	Darbuotojų klaidos, kibernetinės atakos, trečiųjų šalių klaidos.
Infrastruktūra	13. Interneto ryšio neprieinamumas.	Darbuotojų klaidos, nenugalima jėga, trečiųjų šalių klaidos.
	14. Vidinio įmonės tinklo sutrikimai.	Darbuotojų klaidos, techniniai gedimai.
	15. Mobilaus ryšio neprieinamumas.	Darbuotojų klaidos, nenugalima jėga, trečiųjų šalių klaidos.

lentelė 6 Įmonės X rizikos

2.3 Kokybinis rizikų vertinimas

Siekiant sukurti kryptingą veiksmų planą bei įsivardinti prioritetines sritis, identifikuotos rizikos turi būti įvertinamos nustatant jų atsiradimo tikimybę, poveikį bei galimai kitus kriterijus (pavyzdžiui skubos tvarką, įgyvendinimo galimybių kriterijus ir pan.). Literatūroje išskiriamos dvi rizikų vertinimo kategorijos: kokybinė ir kiekybinė. PMBOK nurodoma, jog kiekybinis rizikų vertinimo metodas nėra privalomas, jis naudojamas kaip pagalbinė priemonė matematiškai įvertinti kokybinio rizikų vertinimo būdu identifikuotoms individualioms rizikoms, kurios galimai kelia grėsmių viso projekto tikslams (Project Management Institute, 2017). Teigiama, jog kiekybinis rizikų vertinimas reikalauja nemažai papildomo laiko, pastangų, specializuotos programinės įrangos, ekspertų patarimų, todėl kiekybinį rizikų vertinimą rekomenduojama atlikti tik vykdant plataus masto, sudėtingus ir kompleksinius projektus. Atsižvelgiant į darbo tikslą, apsiribojama rizikas vertinti tik kokybiniais rizikų vertinimo būdais. PMBOK metodologijoje atkreipiamas dėmesys, jog kokybinio rizikų vertinimo metodo ypatybė - galimas subjektyvumas, nes vertinant remiasi suinteresuotų šalių nuomone ir rizikų suvokimu (angl. *risk perception*). Kokybiniu rizikos vertinimu siekiama nustatyti individualių rizikų prioritetus, asmenis, atsakingus už rizikas bei atsakų į rizikas įgyvendinimą (Project Management Institute, 2017). Pasirinkta naudotis tokiais rizikų vertinimo įrankiais kaip rizikų atsiradimo tikimybės ir poveikio vertinimas bei atsiradimo tikimybės ir poveikio burbuline diagrama (žr. pav 11) vertinimo rezultatų vaizdavimui. Kokybinio rizikų vertinimo metodo ypatybė - galimas subjektyvumas, todėl paprašyta, jog rizikos atskirai būtų įvertintos (žr. lent. 7) įmonės vadovo bei ilgalaikio įmonės darbuotojo (įmonėje dirbančio 9 metus) naudojantis rizikų valdymo planavimo etapu sudaryta rizikų atsiradimo tikimybių ir poveikio apibrėžčių lentele (žr. lent. 4) poveikį ir tikimybę vertinant kategorijomis didelis (3), vidutinis (2), mažas (1). Iš gautų vertinimų išvestas vidurkis siekiant objektyvesnių rizikų vertinimo rezultatų (žr. lent. 8).

	Įmonės X vadovo vertinimas		**Įmonės X darbuotojo vertinimas**	
Rizika	**Poveikis**	**Tikimybė**	**Poveikis**	**Tikimybė**
1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	3	2	3	3
2. Kompiuterių praradimas	3	1	3	1
3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	3	1	3	2

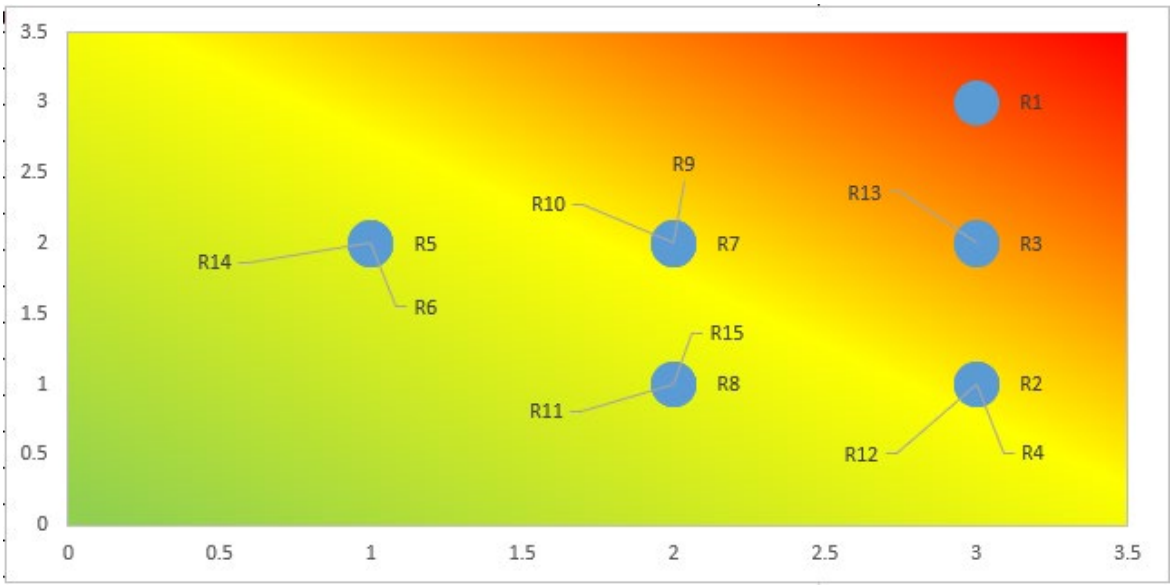
4. Spausdintuvų praradimas	3	1	3	1
5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	1	1	1	3
6. Mobiliųjų telefonų praradimas.	1	1	1	2
7. Kompiuterių programinės įrangos gedimai.	2	2	2	2
8. Telefonų programinės įrangos gedimai.	1	1	2	1
9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	2	1	2	2
10. Istorinių projektų praradimas.	2	1	2	2
11. Istorinių projektų nepasiekiamumas.	2	1	2	2
12. Klientų duomenų praradimas.	3	1	3	1
13. Interneto ryšio neprieinamumas.	3	1	1	2
14. Vidinio įmonės tinklo sutrikimai.	1	1	1	2
15. Mobilaus ryšio neprieinamumas.	2	1	2	1

lentelė 7 Įmonės X vadovo ir darbuotojo rizikų vertinimo rezultatai

Rizikos nr.	**Rizika**	**Poveikis**	**Tikimybė**	**Rizikos vertinimas**
R1	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	3	3	Didelis
R2	2. Kompiuterių praradimas	3	1	Vidutinis
R3	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	3	2	Vidutinis
R4	4. Spausdintuvų praradimas	3	1	Vidutinis
R5	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	1	2	Mažas

R6	6. Mobiliųjų telefonų praradimas.	1	2	Mažas
R7	7. Kompiuterių programinės įrangos gedimai.	2	2	Vidutinis
R8	8. Telefonų programinės įrangos gedimai.	2	1	Mažas
R9	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	2	2	Vidutinis
R10	10. Istorinių projektų praradimas.	2	2	Vidutinis
R11	11. Istorinių projektų nepasiekiamumas.	2	2	Mažas
R12	12. Klientų duomenų praradimas.	3	1	Vidutinis
R13	13. Interneto ryšio neprieinamumas.	2	2	Vidutinis
R14	14. Vidinio įmonės tinklo sutrikimai.	1	2	Mažas
R15	15. Mobilaus ryšio neprieinamumas.	2	1	Mažas

lentelė 8 Įmonės X rizikų vertinimo rezultatai



pav. 10 Įmonės X rizikų tikimybės ir poveikio vertinimo vaizdavimas

Gauti rezultatai parodė, jog įmonė X vieną grėsmę - kompiuterių gedimai (tyčiniai ir netyčiniai) įsivertino, kaip turinčią didelę tikimybę atsirasti ir turinčią didelį poveikį. Rizikų valdymo planavimo etapu nusistatyta, jog įmonės X imsis priemonių suvaldyti grėsmes, turinčias didelį poveikį ir didelę tikimybę atsirasti.

2.4 Atsakų į rizikas planavimas

Įsivertinus rizikas, kitas žingsnis - atsakų į rizikas planavimas ir strategijos kūrimas. PMBOK nurodoma, jog galimos 5 atsakų į rizikas strategijos: eskalavimas, vengimas, perkėlimas, sušvelninimas, priėmimas. Taip pat nurodoma, jog kai kurioms rizikoms atskirai arba visam projektui bendrai galima sudaryti grėsmių suvaldymo planus (angl. *contingency plan*), jeigu identifikuojami faktoriai, kuriais remiantis galima laiku (prieš išsipildant grėsmei) panaudoti šiuos planus. Įmonės X rizikų apetitas žemas, todėl 14 rizikų priskirta priėmimo strategija ir tik vienai rizikai priskirta sušvelninimo strategija, reiškianti, jog įmonė imsis priemonių, užkertančių kelią grėsmės atsiradimui ir/ar pašalintų galimą poveikį (žr. lent. 9).

Rizikos nr.	**Rizika**	**Rizikos vertinimas**	**Atsakų į rizikas strategija**
R1	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	Didelis	Sušvelninimas
R2	2. Kompiuterių praradimas	Vidutinis	Priėmimas
R3	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	Vidutinis	Priėmimas
R4	4. Spausdintuvų praradimas	Vidutinis	Priėmimas
R5	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	Mažas	Priėmimas
R6	6. Mobiliųjų telefonų praradimas.	Mažas	Priėmimas
R7	7. Kompiuterių programinės įrangos gedimai, sutrikimai.	Vidutinis	Priėmimas
R8	8. Telefonų programinės įrangos gedimai.	Mažas	Priėmimas
R9	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	Vidutinis	Priėmimas
R10	10. Istorinių projektų praradimas.	Vidutinis	Priėmimas

R11	11. Istorinių projektų nepasiekiamumas.	Mažas	Priėmimas
R12	12. Klientų duomenų praradimas.	Vidutinis	Priėmimas
R13	13. Interneto ryšio neprieinamumas.	Vidutinis	Priėmimas
R14	14. Vidinio įmonės tinklo sutrikimai.	Mažas	Priėmimas
R15	15. Mobilaus ryšio neprieinamumas.	Mažas	Priėmimas

lentelė 9 Įmonės X atsakų į rizikas strategijos

Rizikos priėmimo strategija gali būti pasyvi arba aktyvi. Pasyvios rizikos priėmimo strategijos atveju žinoma apie galimas grėsmes bei jų tikimybę, poveikį, tačiau pasirenkama nieko nedaryti, tik periodiškai peržiūrimos grėsmės iš naujo įvertinant jų tikimybę ir poveikį. Aktyvi rizikos priėmimo strategija yra tokia, kai rizikos savininkas pasirenka nieko nedaryti, tačiau numatyti finansiniai ir/ar nematerialūs ištekliai, kurie bus panaudoti grėsmės išsipildymo atveju. Įmonė X pasirinko aktyvios rizikos priėmimo strategijos būdą ir vidutinėms/mažoms grėsmėms nusimatė 1000 EUR rezervą grėsmių išsipildymo atvejams. Atskiras aktyvus rizikos priėmimo strategijos būdas bus taikomas R12 rizikai (klientų duomenų praradimas), nors rizikos vertinimo etapu ši grėsmė įvertinta kaip vidutinė, tačiau atsižvelgiant į galimas teisines bei įmonės reputacijai žalą keliančias pasekmes, buvo rekomenduoda sudaryti grėsmės suvaldymo planą, už kurį atsakingas įmonės X savininkas, siekiant sušvelninti galimus padarinius ir efektyviai suvaldyti riziką jos išsipildymo atveju.

Sušvelninimo strategijos tikslas - sumažinti rizikos atsiradimo tikimybę (pavyzdžiui sumažinant grėsmių atsiradimo priežastis) ir/arba sumažinti rizikos poveikį modifikuojant procesus, poveikio sritis (pavyzdžiui pratęsiant terminus). Įmonė X rizikų identifikavimo etapu įvardino šias galimas priežastis kompiuterių gedimams (tyčiniams ir netyčiniams) įvykti: darbuotojų klaidos, įrangos neprieţiūra, įrangos nusidėvėjimas, kibernetinės atakos, nenugalima jėga. Įmonės X vadovo nuomone nėra galimybės sumažinti šios rizikos poveikio (norint likti konkurencingiems rinkoje, projektų užbaigimo terminai negali būti ilginami), todėl buvo pasirinkta sumažinti rizikos atsiradimo tikimybę mažinant grėsmių atsiradimo priežastis. PMBOK nurodoma, jog konretūs atsakų į rizikas metodai gali būti parenkami tariantis su ekspertais, komandos nariais (Project Management Institute, 2017). Įmonė X neturi IT skyriaus ar specialisto, atsakingo už IT ūkį, todėl renkantis sušvelninimo veiksmus (žr. lent. 10) rekomenduota remtis

“Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas” pateiktomis gairėmis ir rekomendacijomis.

Rizikos nr.	**Rizikas**	**Priežastys**	**Atsakų į rizikas veiksmai**
R1	1. Kompiuterių gedimai, sutrikimai (tyčiniai ir netyčiniai)	Darbuotojų klaidos	Darbuotojų švietimas, kibernetinė higiena
		Įrangos nepriežiūra	Darbuotojų švietimas
		Įrangos nusidėvėjimas	Atsarginis kompiuteris
		Kibernetinės atakos	Darbuotojų švietimas Antivirusinių programų diegimas Saugių slaptažodžių politika Darbo ir asmeninių prietaisų atskyrimas Automatinių atnaujinimų įjungimas Atsarginis kompiuteris
		Nenugalima jėga	Atsarginis kompiuteris

lentelė 10 Įmonės X atsakų į riziką veiksmai

2.5 Atsakų į rizikas įgyvendinimas

PMBOK akcentuojama, jog dažnai pasitaiko atvejų, kai daug laiko ir pastangų skiriama rizikų analizei bei atsakų į rizikas strategijų kūrimui, tačiau atsakų į rizikas veiksmai lieka neįgyvendinti, dažniausia todėl, jog aiškiai nenurodomi atsakų į riziką veiksmų savininkai, veiksmų atlikimo terminai ar dėl nepakankamo rizikų savininko spaudimo atsakų į riziką veiksmų savininkams (Project Management Institute, 2017). PMBOK pateikiami šio etapo įrankiai - ekpertų vertinimas, asmeniniai ir komandiniai įgūdžiai (akcentuojami tokie įgūdžiai kaip įtaka komandai ir autoritetas). Pasirinktas asmeninis ir komandinių įgūdžių įrankis: dėl turimo autoriteto ir įtakos įmonės X vadovas pasirinko būti visų rizikų savininku bei daugelio atsakų į rizikas veiksmų savininku. 2 atsakų į rizikas veiksmai priskirti įmonės X darbuotojui (antivirusinių programų diegimas bei atsarginio kompiuterio paruošimas) dėl turimų

kompetencijų IT srityje. Visiems atsakų į rizikas veiksmams priskirti atlikimo terminai, už kurių progresą atsakingas įmonės X vadovas (t.y. rizikų savininkas).

2.6 Rizikų stebėjimas

Rizikų stebėjimas proceso metu stebimas atsakų į rizikas įgyvendinimo progresas ir veiksmingumas, identifikuojamos ir analizuojamos galimos naujos rizikos, kurių gali atsirasti įgyvendinus atsakų į rizikas veiksmus ar pasikeitus darbinei aplinkai (pavyzdžiui įsigijus naujų įrenginių, ar priėmus naujų darbuotojų). Įmonė X nusprendė reguliariai kas ketvirtį su darbuotojais organizuoti susirinkimus (*angl. risk review meetings*), kurių metu apžvelgs ir įsivertins esamas rizikas bei jų statusus. Pasikeitus darbinei aplinkai, esant poreikiui ar įgyvendinus atsakų į rizikas veiksmus rekomenduojama įsivertinti naujas rizikas bei peržiūrėti esamų riziką sąrašą nelaukiant ketvirtinio susirinkimo.

3. KIBERNETINIO SAUGUMO RIZIKŲ VALDYMO MODELIS

PMBOK metodologijoje akcentuojamas rizikų valdymo modelio bei rizikos registro formatų sudarymas laisva forma. Konkrečių šablonų ar pavyzdžių nepateikiama ir rekomenduojama naudotis organizacijoje naudojamais šablonais bei organizacijos gerosiomis praktikomis. Įmonė X darbinės veiklos neorganizuoja pagal projektų valdymo metodologijas bei nėra susidūrusi su rizikų valdymo modeliais, todėl neturi rizikų valdymo modelio dokumento pavyzdžių. Šis dokumentas buvo sudarytas laisva forma siekiant pateikti informaciją koncentruotai bei aiškiai nurodant svarbiausius komponentus tokius kaip rizikų valdymo strategija, atsakingi asmenys, rizikų registras ir pan. Rizikų registras – vienas svarbiausių KS saugumo modelio komponentų, kuris turi būti nuolatos atnaujinamas (Schreider, 2019, Moschovitis, 2018), todėl rekomenduojama jį sudaryti taip, jog būtų lengva koreguoti, atnaujinti ir papildyti (pvz. MS Excel ar Word formatu). KS rizikų valdymas – tęstinis procesas (Ruan, 2019, Davis, 2021), todėl siekta, jog dokumente atsispindėtų daryti pakeitimai, aiškiai identifikuojami dokumento pakeitimo autoriai bei daryti veiksmai, nurodytos suplanuotos atsakų į rizikas veiksmų datos, veiksmų ir rizikų statusai bei atsakingi asmenys. Taip pat buvo rekomenduota KS rizikų valdymo modelio dokumente kaip priedą turėti (ir esant reikalui atnaujinti) įmonės X turimo inventoriaus sąrašą, kadangi techninė, programinė įranga bei infrastruktūra yra pagrindiniai KS grėsmių atsiradimo komponentai (Reuvid, 2019, Brumfield, 2021).

UAB „Įmonė X”

KS RIZIKŲ VALDYMO PLANAS

Versija 1.0

2021 09

TURINYS

DOKUMENTO INFORMACIJA

	Informacija
Dokumento savininkas	Vardas Pavardė
Sudarymo data	2021 09
Paskutinių pataisymų data	*[Data]*

DOKUMENTO KOREKCIJŲ ISTORIJA

Versija	Data	Dokumento pakeitimai
1.0	*2021 09*	*KS Rizikų Modelio Sudarymas*

KS RIZIKŲ VALDYMO MODELIS

VALDYMO STRATEGIJA

Rizikų modelis peržiūrimas kas ketvirtį arba atsiradus poreikiui. Kas ketvirtį peržiūrimas inventoriaus sąrašas ir esant poreikui koreguojamas. Taip pat peržiūrimos identifikuotos rizikos ir jų statusas. Atsakai į rizikas planuojami rizikoms, įvertintoms kaip turinčias **didelę** tikimybę atsirasti ir turinčioms **didelį** poveikį.

ROLĖS IR ATSAKOMYBĖS

Rizikų savininkas ir asmuo atsakingas už rizikų valdymo modelio atnaujinimus *Vardas Pavardė*.

RIZIKŲ KATEGORIJOS (RK)

RK 0	RK 1	RK 2	RK 3
Visos KS rizikos	1. Technologijos	1.1. Techninė įranga	1.1.1. Kompiuteriai, spausdintuvai, mob. telefonai.
		1.2. Programinė įranga	1.2.1. Programinė įranga įdiegta ar pasiekiama naudojantis 1.1.1 išvardintais įrenginiais.
		1.3. Infrastruktūra	1.3.1. Interneto ryšys.
			1.3.2. Telefono ryšys.
			1.3.3. Vidinis įmonės tinklas.
	2. Žmogiškieji ištekliai	2.1. Įmonės darbuotojai	
		2.2. Klientai	
		2.3. Kiti trečiųjų šalių atstovai (įmonė, teikianti buhalterijos paslaugas bei AB ESO)	
	3. Duomenys	3.1. Klientų kontaktiniai duomenys	
		3.2 Istoriniai dujotekių projektai	
		3.3 Įmonės praktinė patirtis	

RIZIKŲ APETITAS

Atsakai į rizikas planuojami rizikoms, įvertintoms kaip turinčias **didelę** tikimybę atsirasti ir turinčioms **didelį** poveikį.

RIZIKŲ ATSIRADIMO TIKIMYBIŲ IR POVEIKIO APIBRĖŽTYS

Skalė	Tikimybė	Poveikis	
		Finansinis	Laikas
Didelė (3)	66 – 100%	Didelis poveikis: finansiniai nuostoliai > 1000EUR.	Prarandami užsakovai arba > 6 d.d. vėluojama užbaigti projektą.
Vidutinė (2)	30 – 66%	Vidutinis poveikis: finansiniai nuostoliai 500 – 1000 EUR.	Projekto užbaigimo terminas nukeliamas 3 - 6 d.d.
Maža (1)	0 – 33%	Mažas poveikis: finansiniai nuostoliai <500 EUR.	Projektas užbaigiamas laiku arba vėluojama pristatyti iki 3 d.d.

Rizikų vertinimas: Tikimybė * Poveikis	Didelis > 6	Vidutinis 4 - 6	Mažas ≤ 3

RIZIKŲ IDENTIFIKAVIMAS

RIZIKŲ INDENTIFIKAVIMO METODAS

Rizikos indentifikuojamos pagrindinių priežasčių analizės metodu kibernetinio saugumo kontekste, nurodant galimas problemas, keliančias grėsmę informacijos vientisumui, konfidencialumui ir prieinamumui bei identifikuojant pagrindines galimas šių problemų atsiradimo priežastis (žr. Pagrindinių priežasčių analizė). Įdentifikuotos 4 potencialių rizikų grupės, kurių atsiradimo priežastys tikslinamos rizikos registre.

1. Žala įmonės techninei įrangai
2. Žala įmonės programinei įrangai
3. Žala įmonės infrastruktūrai
4. Duomenų praradimas.

PAGRINDINIŲ PRIEŽASČIŲ ANALIZĖ

KS Aspektas	Problema	Galimos atsiradimo priežastys
Informacijos prieinamumas	Žala įmonės techniniam inventoriui	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės programinei įrangai	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Duomenų praradimas, nepasiekiamumas	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės infrastruktūrai	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
Informacijos konfidencialumas	Duomenų praradimas	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
		Kibernetinės grėsmės
		Žmogiškieji ištekliai

Informacijos vientisumas	Duomenų praradimas, nepasiekiamumas	Nenugalima jėga
		Kitos priežastys
	Žala įmonės techniniam inventoriui	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys
	Žala įmonės programinei įrangai	Kibernetinės grėsmės
		Žmogiškieji ištekliai
		Nenugalima jėga
		Kitos priežastys

IDENTIFIKUOTOS RIZIKOS

Rizikos nr.	Rizika
R1	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)
R2	2. Kompiuterių praradimas
R3	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)
R4	4. Spausdintuvų praradimas
R5	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)
R6	6. Mobiliųjų telefonų praradimas.
R7	7. Kompiuterių programinės įrangos gedimai.
R8	8. Telefonų programinės įrangos gedimai.
R9	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)
R10	10. Istorinių projektų praradimas.
R11	11. Istorinių projektų nepasiekiamumas.
R12	12. Klientų duomenų praradimas.
R13	13. Interneto ryšio neprieinamumas.
R14	14. Vidinio įmonės tinklo sutrikimai.
R15	15. Mobilaus ryšio neprieinamumas.

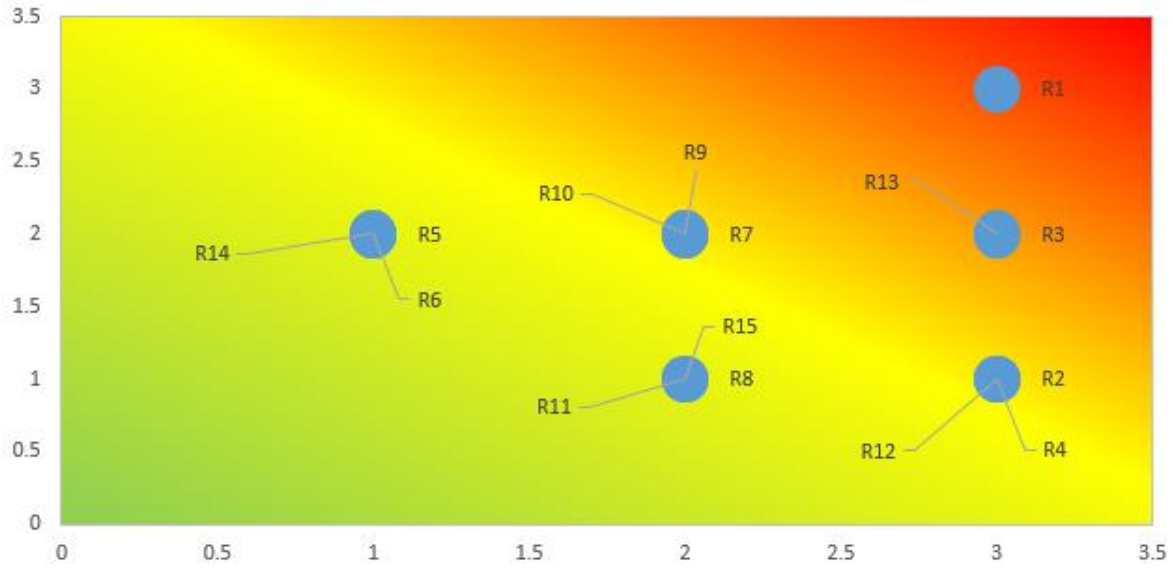
RIZIKŲ VERTINIMAS

RIZIKŲ VERTINIMO METODAS

Rizikų vertinimui naudojamas rizikų atsiradimo tikimybės ir poveikio vertinimas pagal rizikų atsiradimo tikimybių ir poveikio apibrėžčių lentelę. Rezultatai vizualizuojami diagrama.

RIZIKŲ VERTINIMAS

Rizikos nr.	Rizika	Poveikis	Tikimybė	Rizikos vertinimas
R1	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	3	3	Didelis
R2	2. Kompiuterių praradimas	3	1	Vidutinis
R3	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	3	2	Vidutinis
R4	4. Spausdintuvų praradimas	3	1	Vidutinis
R5	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	1	2	Mažas
R6	6. Mobiliųjų telefonų praradimas.	1	2	Mažas
R7	7. Kompiuterių programinės įrangos gedimai.	2	2	Vidutinis
R8	8. Telefonų programinės įrangos gedimai.	2	1	Mažas
R9	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	2	2	Vidutinis
R10	10. Istorinių projektų praradimas.	2	2	Vidutinis
R11	11. Istorinių projektų nepasiekiamumas.	2	2	Mažas
R12	12. Klientų duomenų praradimas.	3	1	Vidutinis
R13	13. Interneto ryšio neprieinamumas.	2	2	Vidutinis
R14	14. Vidinio įmonės tinklo sutrikimai.	1	2	Mažas
R15	15. Mobilaus ryšio neprieinamumas.	2	1	Mažas



ATSAKAI Į RIZIKAS

ATSAKŲ Į RIZIKAS STRATEGIJA

Atsižvelgiant į rizikų apetitą, R1 rizikai taikoma sušvelnimo strategija. R2 – R8 (mažoms ir vidutinio prioriteto) grėsmės taikoma aktyvi priėmimo strategija. R12 grėsmei taikoma atskiras aktyvios priėmimo strategijos būdas. Konkretūs atsakų į rizikas veiksmai detalizuoti rizikų registre.

Rizikos nr.	Rizika	Rizikos vertinimas	Atsakų į rizikas strategija
R1	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	Didelis	Sušvelninimas
R2	2. Kompiuterių praradimas	Vidutinis	Priėmimas
R3	3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	Vidutinis	Priėmimas
R4	4. Spausdintuvų praradimas	Vidutinis	Priėmimas
R5	5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	Mažas	Priėmimas
R6	6. Mobiliųjų telefonų praradimas.	Mažas	Priėmimas
R7	7. Kompiuterių programinės įrangos gedimai, sutrikimai.	Vidutinis	Priėmimas
R8	8. Telefonų programinės įrangos gedimai.	Mažas	Priėmimas

R9	9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	Vidutinis	Priėmimas
R10	10. Istorinių projektų praradimas.	Vidutinis	Priėmimas
R11	11. Istorinių projektų nepasiekiamumas.	Mažas	Priėmimas
R12	12. Klientų duomenų praradimas.	Vidutinis	Priėmimas
R13	13. Interneto ryšio neprieinamumas.	Vidutinis	Priėmimas
R14	14. Vidinio įmonės tinklo sutrikimai.	Mažas	Priėmimas
R15	15. Mobilaus ryšio neprieinamumas.	Mažas	Priėmimas

ATSAKŲ Į RIZIKAS ĮGYVENDINIMAS

Detalūs atsakų į rizikas įgyvendinimo būdai nurodomi rizikų registre. Už atsakų į rizikas įgyvendinimą atsakingas UAB „Įmonė X" savininkas *Vardas Pavardė*.

RIZIKŲ STEBĖJIMAS IR KONTROLĖ

Kas ketvirtį peržiūrimas inventoriaus sąrašas ir esant poreikui koreguojamas. Taip pat kas ketvirtį (ar esant poreikiui) peržiūrimos identifikuotos rizikos ir jų statusas. Už rizikų stebėjimą ir kontrolę atsakingas UAB „Įmonė X" savininkas *Vardas Pavardė*.

RIZIKŲ REGISTRAS

Rizikos nr.	Rizikos kategorija	Rizikos pavadinimas	Tikimybė	Poveikis	Rizikos vertinimas	Atsakų į rizikas strategija	Rizikų vertinimo data	Rizikų atsiradimo priežastys	Atsakų į rizikas veiksmai	Atsakų į rizikas veiksmų įgyvendinimo data	Už riziką atsakingas asmuo	Už atsakų į rizikas veiksmus atsakingas asmuo	Atsakų į rizikas veiksmų statusas	Rizikos statusas
R1	Techninė įranga	1. Kompiuterių gedimai (tyčiniai ir netyčiniai)	3	3	Didelis	Sušvelninimas	2021 08	Darbuotojų klaidos Įrangos nepriežiūra Įrangos nusidėvėjimas Kibernetinės atakos Nenugalima jėga	Darbuotojų švietimas	Iki 2022 02	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Vykdoma	Atvira
									Antivirusinių programų diegimas	Iki 2021 12	Įmonės vadovas Vardas Pavardė	Įmonės darbuotojas Vardas Pavardė	Vykdoma	Atvira
									Saugių slaptažodžių politika	Iki 2021 10	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Vykdoma	Atvira
									Darbo ir asmeninių prietaisų atskyrimas	Iki 2021 10	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Vykdoma	Atvira
									Automatinių atnaujinimų įjungimas	Iki 2021 10	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Vykdoma	Atvira
									Atsarginis kompiuteris	Iki 2021 12	Įmonės vadovas Vardas Pavardė	Įmonės darbuotojas Vardas Pavardė	Vykdoma	Atvira
R2		2. Kompiuterių praradimas	3	1	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Vagystės Nenugalima jėga		N/A	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Uždaryta	Atvira
R3		3. Spausdintuvų gedimai (tyčiniai ir netyčiniai)	3	2	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Įrangos nepriežiūra Įrangos nusidėvėjimas Kibernetinės atakos Nenugalima jėga		N/A	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Uždaryta	Atvira
R4		4. Spausdintuvų praradimas	3	1	Vidutinis	Priėmimas	2021 08	Vagystės Nenugalima jėga		N/A	Įmonės vadovas Vardas Pavardė	N/A	Uždaryta	Atvira

Rizikos nr.	Rizikos kategorija	Rizikos pavadinimas	Tikimybė	Poveikis	Rizikos vertinimas	Atsakų į rizikas strategija	Rizikų vertinimo data	Rizikų atsiradimo priežastys	Atsakų į rizikas veiksmai	Atsakų į rizikas veiksmų įgyvendinimo data	Už riziką atsakingas asmuo	Už atsakų į rizikas veiksmus atsakingas asmuo	Atsakų į rizikas veiksmų statusas	Rizikos statusas
R5		5. Mobiliųjų telefonų gedimai (tyčiniai ir netyčiniai)	1	2	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Įrangos nepriežiūra Įrangos nusidėvėjimas Kibernetinės atakos Nenugalima jėga	Numatytas 1000EUR rezervas rizikų išsipildymo atveju	N/A	Įmonės vadovas Vardas Pavardė	N/A	Uždaryta	Atvira
R6		6. Mobiliųjų telefonų praradimas.	1	2	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Vagystės Nenugalima jėga		N/A	Įmonės vadovas Vardas Pavardė	N/A	Uždaryta	Atvira
R7	Programinė įranga	7. Kompiuterių programinės įrangos gedimai.	2	2	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Įrangos nepriežiūra Kibernetinės atakos		N/A	Įmonės vadovas Vardas Pavardė	N/A	Uždaryta	Atvira
R8		8. Telefonų programinės įrangos gedimai.	2	1	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Įrangos nepriežiūra Kibernetinės atakos		N/A	Įmonės vadovas Vardas Pavardė	N/A	Uždaryta	Atvira
R9		9. Komunikacijai skirtų programų sutrikimai ir nepasiekiamumas (Gmail, Messenger)	2	2	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Trečiųjų šalių klaidos Kibernetinės atakos	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R10	Duomenys	10. Istorinių projektų praradimas.	2	2	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Techniniai sutrikimai	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R11		11. Istorinių projektų nepasiekiamumas.	2	2	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Techniniai sutrikimai	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R12		12. Klientų duomenų praradimas.	3	1	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Trečiųjų šalių klaidos	Grėsmės suvaldymo plano sudarymas	Iki 2022 02	Įmonės vadovas Vardas Pavardė	Įmonės vadovas Vardas Pavardė	Vykdoma	Atvira
R13	Infrastruktūra	13. Interneto ryšio neprieinamumas.	2	2	Vidutinis	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Trečiųjų šalių klaidos	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R14		14. Vidinio įmonės tinklo sutrikimai.	1	2	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Techniniai gedimai	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira
R15		15. Mobilaus ryšio neprieinamumas.	2	1	Mažas	Priėmimas	2021 08	Darbuotojų klaidos Kibernetinės atakos Trečiųjų šalių klaidos	N/A	N/A	Įmonės vadovas Vardas Pavardė	N/A	N/A	Atvira

PRIEDAS 1. INVENTORIAUS SĄRAŠAS

	Inventorius	Kiekis	Papildoma informacija
Techninė įranga	Stacionarus kompiuteris	2	
	Nešiojamas kompiuteris HP ProBook 640	2	
	Spausdintuvas	4	
	Mobilusis telefonas Samsung Galaxy S 20	2	
	Mobilusis telefonas iPHONE 12	2	
	Braižytuvas	1	
Darbui skirta programinė įranga	Windows 10 OS su Office 2019 paketu	3	
	AutoCad 2017	3	
	Adobe Acrobat Reader DC	3	
	Google Drive		
Komunikacijai skirtos e- programos	Gmail elektronins paštas		
	Messenger		
Infrastruktūra	Interneto tiekėjas "Telia"		
	Mobilaus ryšio tiekėjas "Tele 2"		
	Vidinis tinklas		

IŠVADOS IR REKOMENDACIJOS

1. PRINCE2 ir PMBOK siūlomos rizikų valdymo metodologijos viena kitą papildo: PRINCE2 išsamiai aprašyta teorinė dalis, tik kai kuriems procesams įvykdyti aprašant galimus naudoti įrankius akcentuojant jų rekomendacinį pobūdį. Tuo tarpu PMBOK šalia teorinės dalies, savo esme sutampančia su PRINCE2 teorine dalimi, struktūruotai pateikiami įrankių rinkiniai, kurie turėtų padėti pasiekti procesų užduotis.

2. Naudojantis PMBOK rizikų valdymo metodologija galima sudaryti KS rizikų valdymo planą SVV įmonėms, atitinkantį ISO/IEC 27001 „Informacijos saugos vadybos sistema“ standartu keliamus reikalavimus, tačiau įmonėms, kurios neturi PMBOK projektų valdymo patirties ar šioje srityje kompetetingų žmogiškųjų išteklių, savarankiškai sudaryti KS rizikų valdymo planus sudėtinga: trūksta lengvai pasiekiamų šaltinių lietuvių kalba, kai kurie procesų įrankiai abstraktūs (susirinkimai, interviu), sunkiai prieinami bei reikalaujantys 3-čiųjų šalių įsitraukimo (pavyzdžiui ekspertų nuomonė) ar neaktualūs SVV įmonėms.

3. PMBOK akcentuojamas informacijos pateikimo formatas laisva forma sudarant patį rizikų valdymo modelį ar rizikos registrą. Siūloma remtis organizacijose naudojamais šablonais ar geręja patirtimi. SVV įmonės, neturinčios projektų valdymo patirties ir pirmą kartą sudarančios rizikų valdymo modelį, neturės galimybės pasinaudoti bei konkrečių pavyzdžių kaip galėtų atrodyti toks rizikų valdymo modelis ar rizikų registras.

Rekomendacijos ir gairės tolimesniems tyrimams

- Siekiant, jog SVV įmonės turėtų galimybę savarankiškai susidaryti KS rizikų valdymo planus, naudojantis PMBOK metodologija, procesą reikėtų adaptuoti pritaikant Lietuvos rinkai, automatizuoti ir galimai pasiūlyti virtualaus asistento paslaugą (jeigu toks įrankis būtų pasiekiamas internetinėje svetainėje) ar galimybe susisiekti su konsultantu gyvai. Įmonėms, kuriose nenaudojama projektų valdymo metodologija tam tikri aspekti gali būti painūs ar reikalauti išsamesnių paaiškinimų.
- Kibernetinis saugumas – valstybinės svarbos klausimas. KS rizikų valdymo modelio sudarymą SVV įmonėms (ir ne tik) turėtų skatinti bei įrankių bei šablonų kūrimą turėtų inicijuoti vyriausybė kaip ir

rekomenduojama ENISA organizacijos pateiktose gairėse (ENISA, 2021) bei kitose mokslinėse studijose bei šaltiniuose (Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., 2020, OECD, 2021).

- ENISA organizacijose pateiktose išvadose kaip pavyzdinė valstybė, turinti KS rizikų valdymo modeliui SVV įmonėms kurti tinkamus įrankius, minima Olandija (ENISA, 2021 p. 51). Tolimesniuose su šia tema susijuose tyrimuose rekomenduojama nagrinėti Olandijos bei kitų šalių praktiką galbūt leisiančią adaptuoti įrankius Lietuvos rinkai.
- Svarbu paminėti, jog 2021 rugpjūčio mėnesį išleistas atnaujintas 7tas PMBOK metodologijos vadovas. Vykdant tolimesnius su šia tema susijusius tyrimus vertėtų nagrinėti pokyčius (jeigu tokių yra), susijusius su rizikų valdymo metodika.

LITERATŪRA

1. Barclay, C. (2013). *Creating an effective cybersecurity program for your organization*. Prieiga per internetą: URL: https://www.researchgate.net/publication/259146505_Creating_An_Effective_Cybersecurity_Program_For_Your_Organization

2. Swinton, S. ir Hedges, S. (2019). *Cybersecurity governance, part 1: 5 fundamental challenges*. Carnegie Mellon University's Software Engineering Institute Blog. Prieiga per internetą: URL: http://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/

3. European Union Agency for Cybersecurity, ENISA (2021). *Cybersecurity for SMEs - challenges and recommendations.* Prieiga per internetą: URL: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

4. Bilevičiūtė, K., Kidykas, J. ir Beinoriūtė, R. (2019). *SVV įmonių kibernetinio saugumo sąmoningumo apklausa. Rezultatai ir įžvalgos*. Prieiga per internetą: URL: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

5. Lietuvos Respublikos krašto apsaugos ministerija, (2020). Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas. Prieiga per internetą: URL: https://kam.lt/download/68737/kibernetinio%20saugumo%20vadovas%20verslui.pdf

6. Tonchia, S. (2018). *Industrial Project Management*. Springer

7. Mashiloane, E. R. ir Jokonya, O. (2018). Investigating the Challenges of Project Governance Processes of IT Projects. *Procedia Computer Science, 138, 875-882*.

8. Chiu, Y. S. (2010). *An Introduction to the History of Project Management: From the Earliest Times to A.D. 1900*. Goodreads

9. Taylor, F. W. (1911). *The Principles of Scientific Management.* Harper & Brothers

10. Morris, P.W.G. (2013). *Reconstructing Project Management*. Wiley-Blackwell

11. Emes, M. ir Griffiths, W. (2018). *Systems thinking: How is it used in project management*. Prieiga per internetą: URL: https://www.apm.org.uk/media/17308/systems-thinking_final.pdf

12. Abbasi, A. ir Alireza, J. (2018). Evolution of Project Management as a Scientific Discipline. *Data and Information Management, Volume 2, 91 – 102.* Prieiga per internetą: URL: https://content.sciendo.com/view/journals/dim/2/2/article-p91.xml?language=en

13. Altexsoft (2018). Agile Project Management: Best Practices and Methodologies. Prieiga per internetą: URL: https://www.altexsoft.com/whitepapers/agile-project-management-best-practices-and-methodologies/

14. Project Management Institute (2017). *A guide to the Project Management Body of Knowledge* (PMBOK guide) (6th ed.). Project Management Institute

15. Axelos (2017). Managing successful projects with PRINCE2. The Stationery Office

16. Hodson C. J. (2019). *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls*. Kogan Page Publishers

17. Kohke A., Sigler K., Shoemaker D. (2017). *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework.* CRC Press

18. Allianz Global Corporate & Specialty (2021). Allianz Risk Barometer. Identifying The Major Business Risks For 2021. Prieiga per internetą: URL:
19. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

20. Moskowitz, S. (2017). *Cybercrime and Business: Strategies for Global Corporate Security.* Butterworth-Heinemann

21. Reuvid, J. (2019). *Managing Cybersecurity Risk: Book 3*. Legend Press Ltd

22. Ruan, K. (2019). *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomic*. Academic Press

23. Davis, R. E. (2021). *Auditing Information and Cyber Security Governance: A Controls-Based Approach.* CRC Press

24. ILX Group (2017). *The History of PRINCE2*. Prieiga per internetą: URL: https://www.prince2.com/eur/blog/the-history-of-prince2

25. Joaquin III, J. G., Kemp, R. (2019). *Cybersecurity: Current Writings on Threats and Protection*. McFarland

26. Tareq, A.Z., Nicholson D. (2018). *Advances in Human Factors in Cybersecurity*. Springer

27. Schreider, T (2019). *Building an Effective Cybersecurity Program, 2nd Edition*. Rothstein Publishing

28. Refsdal, A., Solhaug, B., Stølen (2015). *Cyber-Risk Management*. Springer

29. OECD (2021). *Studies on SMEs and Entrepreneurship The Digital Transformation of SMEs*. OECD

30. Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (2020). Information and Cyber Security: 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings.

31. Moschovitis, C. (2018). *Cybersecurity Program Development for Business: The Essential Planning Guide*. John Wiley & Sons

32. Brumfield, C. (2021). *Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*. John Wiley & Son

33. Bermudez, M. (2020). *Cybersecurity for Small and Midsize Businesses*. BookBaby

34. Hoppe F., Gatzert N., Gruner P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance, Vol. 22 No. 3/4, 240-260*.

35. Ozkan Y. B., Spruit M. (2020). Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects.

36. Zasa, P. F., Patrucco, A., Pellizzoni E. (2021). Managing the Hybrid Organization: How Can Agile and Traditional Project Management Coexist? *Research-Technology Management*, 64:1, p. 54-63

37. Buganováa, K., Šimíčkováa, J. (2019). Risk management in traditional and agile project management. *Transportation Research Procedia, Volume 40, 2019, p. 986-993.*

38. Gholamreza, J., Oveisi, M. (2016). A Study on Project Management Based on PMBOK and PRINCE2. *Modern Applied Science, Vol. 10-6, p. 142 - 146.*

39. Seymour, T. J. (2014). The History Of Project Management. *International Journal of Management & Information Systems* (IJMIS) 18:233. Prieiga per internetą: URL: https://www.researchgate.net/publication/298341808_The_History_Of_Project_Management

Legytė L. IT projektų valdymo ypatumai kibernetinio saugumo srityje / Kibernetinio saugumo valdymomagistro baigiamasis darbas. Vadovas prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Viešojo valdymo ir verslo fakultetas, 2021. – 62 p.

ANOTACIJA

Magistro baigiamajame darbe nagrinėjamas IT projektų valdymo metodologijų pritaikomumas kibernetinio saugumo srityje kuriant kibernetinio saugumo rizikų valdymo modelį smulkaus ir vidutinio verslo įmonėms. Pirmoje darbo dalyje pristatomos IT projektų valdymo metodologijos bei supažindinama su rizikų valdymo modeliais tradicinėse (ang. *waterfall*) IT projektų valdymo metodologijose (PMBOK, PRINCE2). Antroje dalyje, taikant atvejo studija ir praktiškai pritaikant PMBOK siūlomą rizikų valdymo modelį, sudaromas kibernetinio saugumo rizikų valdymo modelis SSV įmonei analizuojant bei detaliai aprašant kiekvieną rizikų valdymo kūrimo etapą. Trečioje dalyje pateikiamas kibernetinio saugumo planas sudarytas konkrečiai SVV įmonei.

Pagrindiniai žodžiai: kibernetinis saugumas, rizikų valdymas, IT projektų valdymas, smulkus ir vidutnis verslas (SVV).

Legytė L. IT Project Management In Cybersecurity Field / Master‘s Work in Cybersecurity management. Supervisor full professor T. Limba. – Vilnius: Faculty of Public Governance and Business, Mykolas Romeris University, 2021. – 62 p.

ANNOTATION

In this Master‘s Work the adaptibility of IT project management within Cybersecurity field is being analyzed while composing cybersecurity risk management framework for a small and medium size enterprise (SME). The first part is dedicated to discuss theoritical aspects of IT project management as well as introduces with risk management frameworks within waterfall type of IT project management methodologies (PMBOK, PRINCE2). The second part via case study method is dedicated to create and demonstrate in detail the process of cybersecurity risk management plan creation for SME by applying PMBOK’s risk management framework. Third part demonstrates cybersecurity risk management plan for a particular SME.

Pagrindiniai žodžiai: cybersecurity, risk management, IT project management, small and medium enterprises.

Legytė L. IT projektų valdymo ypatumai kibernetinio saugumo srityje / Kibernetinio saugumo valdymomagistro baigiamasis darbas. Vadovas prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Viešojo valdymo ir verslo fakultetas, 2021. – 62 p.

SANTRAUKA

Magistro baigiamojo darbo tikslas - IT projektų valdymo metodologijų teorinių aspektų analizė bei praktinis pritaikomumas sudarant kibernetinio saugumo rizikos valdymo modelį smulkaus ir vidutinio verslo įmonei.

ENISA organizacijos 2021 metais atliktos apklausos ir analizės duomenimis, smulkaus ir vidutinio verslo sektorius Europos Sąjungos šalyse susiduria su 7 pagrindiniais iššūkiais bandydamas sudaryti kibernetinio saugumo planus, tarp kurių įvardijamos tokios problemos kaip IRT specialistų trūkumas, lėšų trūkumas, aiškių ir praktiškai pritaikomų kibernetinio saugumo gairių stoka (ENISA, 2021). Lyginant kibernetinio saugumo programų formavimo ir įgyvendinimo iššūkius bei procesus, kuriuos siekiama suvaldyti projektų valdymo metodologijomis, galima teigti, jog sudarant KS rizikų valdymo modelį, galėtų būti pasitelkiamos IT projektų valdymo metodologijos.

Darbą sudaro 3 dalys: pirmoje dalyje dalyje pristatomos IT projektų valdymo metodologijos bei supažindinama su rizikų valdymo modeliais tradicinėse (ang. *waterfall*) IT projektų valdymo metodologijose (PMBOK, PRINCE2). Antroje dalyje, taikant atvejo studija ir praktiškai pritaikant PMBOK siūlomą rizikų valdymo modelį, sudaromas kibernetinio saugumo rizikų valdymo modelis SSV įmonei analizuojant bei detaliai aprašant kiekvieną rizikų valdymo kūrimo etapą. Trečioje dalyje pateikiamas kibernetinio saugumo planas sudarytas konkrečiai SVV įmonei.

.

Legytė L. IT Project Management In Cybersecurity Field / Master‘s Work in Cybersecurity management. Supervisor full professor T. Limba. – Vilnius: Faculty of Public Governance and Business, Mykolas Romeris University, 2021. – 62 p.

SUMMARY

The purpose of this Master‘s thesis is to analyze the theoritacl aspects of IT project management methodologies and practical adaptability within Cybersecurity field while composing cybersecurity risk management framework for a small and medium size enterprise (SME).

Based on survey results and analysis contucted by ENISA organization in 2021, SMEs in EU countries run into challenges in their attempts to create cybersecurity risk management plans due to lack of financial and human resources, unclear and fragmented guidelines on cybersecurity risk management creation processes. Risk management frameworks within IT project management methodologies deal with similar issues and processes in comparison with cybersecurity management models, therefore it can be claimed that while creating cybersecurity risk management model, IT project management methodologies can be applied.

Master‘s thesis consists of three parts. The first part is dedicated to discuss theoritical aspects of IT project management as well as introduces with risk management frameworks within waterfall type of IT project management methodologies (PMBOK, PRINCE2). The second part via case study method is dedicated to create and demonstrate in detail the process of cybersecurity risk management plan creation for SME by applying PMBOK’s risk management framework. Third part demonstrates cybersecurity risk management plan for a particular SME.