NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJOS KASMETINIAM RIZIKŲ VERTINIMUI

RUGSĖJIS
2025

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.

Turinys

NKSC rekomendacija

KASMETINIAM RIZIKŲ VERTINIMUI

Rekomendacijų tikslas

Šio informacinio leidinio tikslas – pateikti kibernetinio saugumo subjektams (toliau – organizacijoms) aiškias ir praktiškas rekomendacijas, skirtas kasmetiniam rizikų vertinimui atlikti.

Šiose rekomendacijose pateikta informacija leis geriau suprasti ir įgyvendinti rizikų valdymo reikalavimus, nustatytus Lietuvos Respublikos kibernetinio saugumo įstatyme (KSĮ) ir Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo reikalavimuose (KSRA), bei užtikrinti organizacijose įdiegtos rizikų valdymo sistemos atitiktį galiojantiems teisės aktams ir gerajai praktikai.

Rizika šiame dokumente yra apibūdinama kaip potencialus įvykis, aplinkybė ar neapibrėžtumo situacija, įvertinta pagal pasireiškimo tikimybę ir galimą neigiamą poveikį organizacijos strateginiams tikslams.

Grėsmė yra laikoma dar neįvertintu potencialiu įvykiu, galinčiu daryti neigiamą įtaką organizacijos veiklai.

Auditorija

Rekomendacijos yra orientuotos į kibernetinio saugumo subjektus, tačiau yra pritaikomos ir kitoms organizacijoms, kasmet vykdančioms rizikų vertinimus.

Organizacijos (atsižvelgiant į jų dydį, veiklos mastą bei specifiką) turi dėti adekvačias pastangas rekomendacijose pateiktiems gerosios praktikos pavyzdžiams įgyvendinti ir sukurti bei tobulinti veiksmingą rizikos valdymo sistemą, didinti rizikos valymo kultūrą, brandą bei tvarumą.

Problematika

Ne pagal standartus ar gerąją praktiką įdiegta rizikų valdymo sistema yra viena iš pagrindinių kliūčių, užtikrinant efektyvų tinklų ir informacinių sistemų (TIS) saugumą bei atitiktį KSĮ ir KSRA reikalavimams. Šios rekomendacijos yra skirtos padėti organizacijoms spręsti minėtą problematiką, suteikiant aiškias gaires apie rizikų valdymo sistemos pagrindinius elementus, būtinus tinkamam rizikos vertinimui atlikti bei KSĮ ir KSRA reikalavimams užtikrinti.

Pirmas skyrius

RIZIKOS KULTŪRA, VALDYSENA IR RIZIKŲ VALDYMO SISTEMOS

Rizikos kultūra yra organizacijos darbuotojų kompetencijų, požiūrio ir elgsenos visuma, atspindinti jų gebėjimą suvokti, įvertinti ir valdyti kasdienėje organizacijos veikloje kylančias grėsmes ir esančias rizikas. Tinkamai išvystyta rizikos kultūra užtikrina, kad darbuotojai kasdienėje veikloje priimtų rizika pagrįstus ir organizacijos strategiją atitinkančius sprendimus.

Stipri rizikos kultūra pasireiškia tuo, kad visi organizacijos darbuotojai aiškiai suvokia, kad:

bet kokia veikla yra susijusi su tam tikro lygio rizika, kuri gali turėti įtakos visai organizacijai, todėl darbuotojai yra skatinami apie rizikas kalbėti su kolegomis bei vadovais atvirai ir laiku;

darbuotojai turi būti pastabūs ir gebėti nustatyti galimas rizikas kasdienėje veikloje bei suprasti jų galimą poveikį įvairiems organizacijos procesams;

kiekvienas darbuotojas turi būti iniciatyvus, prisiimti atsakomybę už rizikų valdymą savo veiklos srityje bei, esant poreikiui, laiku eskaluoti rizikas atsakingiems asmenims.

Siekiant stiprinti rizikos kultūrą, organizacijai yra rekomenduojama aktyviai įtraukti darbuotojus į rizikų valdymo strategiją, o ją integruoti į kasdienius veiklos procesus. Kartu ugdyti darbuotojų rizikų valdymo kompetencijas ir skatinti elgesį, atitinkantį organizacijos pagrindines vertybes bei tikslus.

1.1. Rizikos valdysena

Rizikos valdyseną organizacijoje yra rekomenduojama grįsti trijų gynybos linijų modeliu (angl. *Three Lines of Defence*). Šis modelis leidžia užtikrinti tinkamą atsakomybių atskyrimą ir efektyvų rizikos valdymo procesą. Šiuo modeliu yra paremta daugelis gerųjų praktikų bei standartų, jis suteikia sisteminį požiūrį į rizikų identifikavimą, vertinimą ir valdymą, mažina spragų riziką bei šalina galimą veiklos dubliavimą.

Tinkamai įgyvendintas trijų gynybos linijų modelis apima:

Pirmoji gynybos linija – operacijų ir procesų valdymas

- Už šią liniją atsakingi vadovai ir darbuotojai, tiesiogiai susiję su TIS, operacijų ir procesų vykdymu.
- Jie yra nustatomi kaip rizikų savininkai, kurie yra atsakingi už rizikų identifikavimą savo veiklos srityse, tinkamų kontrolės priemonių taikymą, rizikos ribų laikymąsi bei atitikties vidaus ir išoriniams reikalavimams užtikrinimą.
- Šios linijos vadovai taip pat prižiūri nustatytą ir toleruojamą rizikos lygį, kasdienius procesus ir užtikrina darbuotojų mokymus.

Antroji gynybos linija – rizikos valdymo priežiūra ir kontrolė

- Šią funkciją įprastai vykdo Rizikų valdymo pareigūnas (angl. *Risk Officer* - RO) arba mažesnėse organizacijose Informacijos saugumo pareigūnas (angl. Information Security Officer - ISO).
- Antroji linija užtikrina, kad visos organizacijai aktualios rizikos būtų tinkamai identifikuotos, vertinamos, valdomos ir stebimos.
- Šis vaidmuo taip pat yra atsakingas už rizikų valdymo sistemos veiksmingumo priežiūrą ir periodinių ataskaitų teikimą vadovybei.

Trečioji gynybos linija – nepriklausomas vidaus auditas

- Vidaus auditas atlieka nepriklausomą rizikos valdymo sistemos peržiūrą ir vertinimą.
- Auditoriai tiesiogiai atsiskaito aukščiausiam organizacijos valdymo organui (akcininkams arba valdybai), teikia objektyvias įžvalgas apie rizikos valdymo veiksmingumą ir nustato tobulintinas sritis.
- Nepriklausomas auditas taip pat padeda įvertinti organizacijos atitiktį galiojantiems teisės aktams, įdiegtiems standartams ir vidaus politikoms.

Organizacijos vadovybė privalo nuolat stebėti pagrindinius rizikos rodiklius (angl. *Key Risk Indicators* - KRI) ir gauti reguliarią informaciją apie rizikos situaciją organizacijoje (pvz., mėnesio ar ketvirčio ataskaitas). Vadovai taip pat privalo aktyviai tobulinti savo kompetencijas rizikos valdymo srityje, periodiškai dalyvauti mokymuose ir kituose kvalifikacijos kėlimo renginiuose.

1.2. Valdymo sistemos

Rizikų valdymo sistema organizacijose turėtų būti kuriama ir tobulinama vadovaujantis gerosiomis praktikomis, tarptautiniais standartais bei KSĮ ir KSRA reikalavimais. Organizacijoje diegiant rizikų valdymo sistemą ir vykdant kasmetinį rizikų vertinimą yra rekomenduojama remtis tarptautiniais standartais ir gairėmis, tokiomis kaip:

- ISO 31000:2018 „Rizikos valdymas - Gairės“.
- ISO/IEC 27001:2022 „Informacijos sauga, kibernetinė sauga ir privatumo apsauga - Informacijos saugos valdymo sistemos - Reikalavimai“.
- ISO/IEC 27005:2022 „Informacijos sauga, kibernetinė sauga ir privatumo apsauga - Informacijos saugos rizikos valdymo gairės“.
- NIST SP 800-30 Rev. 1 „Rizikos vertinimo atlikimo gairės“.

Siekiant užtikrinti rizikų valdymo sistemos veiksmingumą ir atitiktį galiojantiems reikalavimams, rekomenduojama reguliariai peržiūrėti naujausias gairių ir standartų versijas bei atitinkamai atnaujinti rizikų valdymo sistemą.

Antras skyrius

RIZIKŲ VALDYMO PROCESAS

Rekomenduojama, kad organizacijos rizikų valdymo procesas būtų aiškiai apibūdintas, nuoseklus ir apimtų šiuos pagrindinius etapus:

- identifikuoti visus organizacijoje turimus išteklius – informacinius (duomenis, dokumentaciją, procesus), technologinius (TIS), žmogiškuosius ir fizinius (pastatus, įrangą ir kt.);
- atsižvelgiant į organizacijos strateginius tikslus ir vykdomą veiklą, nustatyti organizacijos rizikos apimtį;
- identifikuoti ir įvertinti visas reikšmingas vidines ir išorines grėsmes bei spragas;
- atlikti identifikuotų grėsmių analizę ir vertinimą bei nustatyti aktualių rizikų mastą;
- įvertintoms rizikoms pritaikyti rizikų valdymo kryptį bei kontrolės priemones;
- rizikoms su nepriimtinu rizikos lygiu sudaryti tolimesnį rizikų valdymo veiksmų planą, paskirstyti išteklius ir atsakomybes;
- nuolat stebėti rizikų kontrolės priemonių veiksmingumą, fiksuoti incidentus ir inicijuoti reikalingus tobulinimo veiksmus;
- reguliariai teikti ataskaitas vadovybei apie pagrindines rizikas, rizikų rodiklių vertes ir taikomų kontrolės priemonių efektyvumą;
- įvykus svarbiems pokyčiams organizacijoje ar incidentams, papildomai reikalinga apimtimi atlikti rizikų vertinimą.

Rizikos valdymo procesą yra rekomenduojama aprašyti ir nuolat tobulinti, atsižvelgiant į praktinio įgyvendinimo ir stebėsenos metu įgytas pamokas. Siekiant užtikrinti rizikų valdymo proceso aktualumą ir veiksmingumą, organizacijoms **rekomenduojama peržiūrėti jį ne rečiau kaip kartą per 12 mėn. arba esant reikšmingiems pokyčiams organizacijoje.**

2.1. Išteklių identifikavimas

Organizacija privalo tvarkyti išteklių registrą, jame registruoti identifikuotus veiklos vykdymui aktualius išteklius:

- veiklos funkcijas;
- technologinius išteklius;
- trečiąsias šalis ir jų subtiekėjus
- bei kitus organizacijos išteklius, esančius ne tik organizacijos centrinėje būstinėje, bet ir kituose padaliniuose.

Identifikuotus išteklius organizacija privalo klasifikuoti pagal jų kritiškumą organizacijos veiklai. Išteklių kritiškumą organizacijos veiklai yra rekomenduojama nustatyti atsižvelgiant į galimą tam tikrų išteklių sutrikimo poveikį organizacijos finansinei būklei, operaciniam tęstinumui ir reputacijai. Išteklių sutrikdymas yra vertinamas pagal galimus konfidencialumo, vientisumo ir prieinamumo pažeidimus.

Atitinkamai identifikavus išteklius ir nustačius jų kritiškumą, išteklių priežiūros ir valdymo atsakomybę priskirti atitinkamiems organizacijos darbuotojams. **Organizacijos išteklių registras privalo būti atnaujinamas reguliariai, ne rečiau kaip kartą per 12 mėn.**

Priimtino rizikos lygio (apetito) nustatymas

Rekomenduojama, kad organizacija, vadovaudamasi savo strateginiais tikslais, veiklos pobūdžiu, kapitalo dydžiu, reputacija ir kitais veiksniais, nusistatytų rizikos apetitą, t. y. didžiausią rizikos lygį, kurį yra pasirengusi prisiimti ir toleruoti, nepažeisdama savo finansinio stabilumo ar veiklos tęstinumo. Priimtinas rizikos lygis gali būti nustatytas tiek kiekybiškai (pvz., maksimalus galimas finansinis nuostolis per tam tikrą laikotarpį), tiek kokybiškai (pvz., toleruotinas reputacinės žalos mastas).

Pavyzdžiui, finansų įstaiga gali nusistatyti, kad jai priimtinas klientų nemokumo rizikos lygis yra toks, kuris neviršija 3 % viso paskolų portfelio per metus. Pastebėjus indikacijas, kad ši riba gali būti viršyta, organizacija imtųsi atitinkamų veiksmų, pavyzdžiui, sugriežtintų paskolų išdavimo politiką arba atsisakytų didesnę riziką keliančių klientų grupės.

Siekiant užtikrinti tikslesnę rizikų kontrolę ir valdymą, priimtiną rizikos lygį rekomenduojama nustatyti atskirai kiekvienai nustatytai rizikos kategorijai. O tam, kad būtų galima greičiau nustatyti rizikų lygio artėjimą prie nustatytų ribų, rekomenduojama įdiegti rodiklių sistemą, apimančią pamatuojamus rizikos įvykių slenksčius ir kitus ankstyvojo perspėjimo signalus.

Rizikų kategorijų apetitą yra rekomenduojama nustatyti pagrindiniam organizacijos valdymo organui, o pavienių rizikų ribas - rizikų savininkams. Rizikų savininkai taip pat turėtų būti atsakingi už rizikų stebėjimą ir jų valdymą laiku, kad organizacijos veikla būtų vykdoma neviršijant nustatytų ribų.

Pagrindinių rizikos rodiklių stebėsena turėtų būti koordinuojama Rizikos valdymo pareigūno ar kitų paskirtų atsakingų asmenų. Reguliarios ataskaitos apie rizikos rodiklių būseną turėtų būti teikiamos organizacijos vadovybei. **Priimtinas rizikos lygis privalo būti periodiškai, ne rečiau kaip kartą per 12 mėn., peržiūrimas ir atnaujinimas, o esant reikšmingiems vidinės ar išorinės aplinkos pokyčiams ir dažniau.**

Grėsmių ir spragų identifikavimas

Organizacijoms yra rekomenduojama identifikuoti visus grėsmių šaltinius, įskaitant trečiųjų šalių keliamą grėsmę, kibernetines grėsmes, įvairius pažeidžiamumus, spragas ir kitus vidinius bei išorinius veiksnius, galinčius turėti įtakos organizacijos veiklos funkcijoms, informaciniams, technologiniams, žmogiškiesiems bei fiziniams ištekliams. Organizacijos privalo tvarkyti ir nuolat atnaujinti grėsmių sąrašą, šio sąrašo taksonomijai sudaryti rekomenduojame remtis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) parengta grėsmių taksonomija bei naujausiomis ENISA grėsmių apžvalgos ataskaitomis. Remiantis ENISA, yra apibrėžiamos šios pagrindinės grėsmių kategorijos:

- fizinės grėsmės;
- atsitiktinė žala;
- sistemų gedimai ir sutrikimai;
- kenkėjiška veikla;
- teisinės ir atitikties grėsmės;
- duomenų pažeidimai;
- grėsmės, kylančios iš trečiųjų šalių;
- sukčiavimas.

Kategorijas organizacijos gali koreguoti bei pritaikyti, atsižvelgdamos į vykdomą veiklą. Kiekviena kategorijoje identifikuota individuali grėsmė (vėliau rizika) privalo būti priskirta rizikų savininkui, kuris, atlikęs grėsmės vertinimą, toliau užtikrins šios rizikos stebėjimą ir valdymą.

Rizikų vertinimas

Siekiant laiku identifikuoti ir įvertinti galimą grėsmių pasireiškimą bei jų poveikį organizacijos veiklai ir ištekliams, organizacijai rizikų vertinimą yra privaloma atlikti ne rečiau kaip kas 12 mėn. Identifikavus grėsmes ir turint sudarytą grėsmių sąrašą, rizikų vertinimas turėtų būti vykdomas keliais pagrindiniais etapais:

Grėsmių analizės atlikimas.

Šiame etape siekiama nustatyti tikėtinų grėsmių pasireiškimo tikimybę ir galimo poveikio organizacijos veiklai mastą. Analizė gali būti grindžiama kokybiniais vertinimo metodais, tokiais kaip darbuotojų ar ekspertų apklausos, kurios leidžia subjektyviai įvertinti grėsmės aktualumą, poveikį ir galimą pasireiškimo tikimybę. Taip pat gali būti taikomi kiekybiniai metodai, pagrįsti statistiniais duomenimis, pavyzdžiui, vertinant šių grėsmių pasireiškimo dažnį kitose organizacijose ar sektoriuje. Tuo atveju, kai pagrįstai nustatoma, kad konkreti grėsmė organizacijos veiklai nėra reikšminga ar aktuali, ji gali būti nevertinama tolesniuose rizikos analizės etapuose;

Prigimtinio (angl. *inherent*) rizikos lygio nustatymas.

Bendras rizikos pasireiškimo tikimybės ir galimų neigiamų pasekmių įvertinimas, dar prieš taikant bet kokias rizikos valdymo ar kontrolės priemones. Tai etapas, kuriame grėsmė yra klasifikuojama kaip rizika, kuri gali realizuotis ir turėti poveikį organizacijos veiklai. Prigimtinis rizikos lygis parodo, kiek organizacija būtų pažeidžiama, jei rizika nebūtų valdoma. Pavyzdžiui, jei organizacija teikia kredito paslaugas be jokio kliento kreditingumo vertinimo, tuomet prigimtinis kredito rizikos lygis dėl didelės nemokumo tikimybės ir galimų finansinių nuostolių būtų labai aukštas;

Atsižvelgiant į organizacijoje nustatytą rizikos apetitą, formuojamos rizikos valdymo kryptis.

t. y. ar rizika bus mažinama, perkeliama, priimama ar jos bus vengiama. Praktikoje tai reiškia, kad kiekvienai identifikuotai rizikai organizacija pasirenka tokią valdymo kryptį, kuri efektyviausiai leidžia suvaldyti prigimtinį rizikos lygį ir užtikrinti, kad likutinis rizikos lygis neviršytų nustatyto rizikos apetito ribų.

Pavyzdžiui, jeigu nustatoma, kad informacinių sistemų sutrikimų rizika viršija priimtiną ribą, gali būti taikoma rizikos mažinimo kryptis, diegiant papildomas prevencines kontrolės priemones, tokias kaip sugriežtinta prieigos kontrolė. Alternatyviai gali būti taikoma ir rizikos perkėlimo kryptis, pavyzdžiui, dalies IT paslaugų perdavimas patikimam išoriniam tiekėjui;

Po pritaikytos rizikos valdymo krypties ir atitinkamų kontrolės priemonių yra nustatomas likutinis (angl. residual) rizikos lygis.

Jeigu jis vis dar viršija organizacijos rizikos apetitą, tuomet yra privaloma parengti rizikos valdymo planą ir imtis papildomų veiksmų šį lygį sumažinant.

Apibendrinant, atliekant grėsmių analizę, kiekviena identifikuota grėsmė turi būti įvertinta pagal jos pasireiškimo tikimybę ir galimą poveikį organizacijos veiklai. Nustačius grėsmių riziką ir įvertinus prigimtinį rizikos lygį, jis turi būti palygintas su organizacijoje taikomu rizikos apetitu. Tai leidžia nustatyti, ar rizika yra priimtina, ar būtina peržiūrėti rizikos valdymo kryptį ir taikomas kontrolės priemones. Tais atvejais, kai rizikos lygis, taikant rizikos valdymo kontrolės priemones, viršija priimtinas rizikos apetito ribas, turi būti sudarytas rizikos valdymo planas, kuriame numatomi terminai ir atsakomybės įgyvendinti ir pritaikyti papildomas arba efektyvesnes kontrolės priemones.

Grėsmių analizės ir rizikų vertinimo metodikos apžvalga

Rizikų vertinimo metu analizuojamos tik tos grėsmės, kurios yra aktualios organizacijai, atsižvelgiant į jos veiklos pobūdį, vykdomas funkcijas ir turimus organizacinius išteklius. Toliau pateikiama grėsmių analizės ir rizikos vertinimo metodikos apžvalga, parengta vadovaujantis ISO/IEC 27005 standarto nuostatomis.

Siekiant nustatyti pagrįstą individualios rizikos lygį, rizikos grėsmės pasireiškimo ir poveikio vertinimas gali būti atliekamas, pasirinkus vieną iš kelių galimų vertinimo metodų – kiekybinį arba kokybinį. Šių rekomendacijų rizikų vertinimo metodikos apžvalgoje pateiktas pavyzdys iliustruoja galimus grėsmės pasireiškimo tikimybės ir poveikio lygius, taikant kokybinį vertinimo metodą. **Rekomenduojami lygiai grėsmės tikimybei nustatyti:**

Tikimybė	Aprašymas
Labai didelė / aukšta	Tikėtina, jog grėsmės įvykis įvyks, nes panašią veiklą vykdančiose organizacijose jis itin dažnai įvyksta.
Didelė / aukšta	Yra didelė tikimybė, jog grėsmės įvykis įvyks, nes panašią veiklą vykdančiose organizacijose jis dažnai pasikartoja.
Vidutinė	Yra tikėtina, jog grėsmės įvykis gali įvykti, nes panašią veiklą vykdančiose organizacijose yra buvę atvejų, kuomet jis įvyko.
Maža	Tikėtina, jog grėsmės įvykis neturėtų įvykti, tačiau yra nedidelė tikimybė, jog kada nors tai gali nutikti.
Labai maža	Labai tikėtina, jog grėsmės įvykis neturėtų įvykti, yra labai nedidelė tikimybė, jog kada nors tai gali nutikti.

Grėsmės poveikio vertinimo ribos turėtų būti pritaikytos kiekvienos organizacijos individualiai pagal organizacijos veiklos pobūdį, finansines galimybes ir atsparumą. Rekomenduojama organizacijoms pačioms nustatyti, kokio dydžio finansiniai nuostoliai, reputaciniai ar veiklos sutrikimai joms laikytini reikšmingais, remiantis šiose gairėse pateiktais orientaciniais lygiais.

Rekomenduojami lygiai grėsmės poveikiui nustatyti:

Poveikis	Poveikis organizacijos veiklai
Labai didelis / aukštas	Poveikis, kuris peržengia organizacijos ribas ir daro reikšmingą poveikį visam sektoriui ar valstybei. Gali būti sutrikdytas organizacijos gebėjimas vykdyti esmines funkcijas ar užtikrinti kritinių paslaugų tęstinumą. Kritinis poveikis žmonių ir turto saugai, pavyzdžiui, reikšmingas sveikatos sutrikdymas, didelio masto aplinkos tarša, esminės infrastruktūros sunaikinimas. Pasekmės gali būti ilgalaikės ir negrįžtamos.
Didelis / aukštas	Draudimu nepadengti finansiniai nuostoliai. Klientų praradimas. Tęstinis kritinių sistemų nepasiekiamumas ar pasikartojantys ilgalaikiai veiklos sutrikimai. Ilgalaikis ir neigiamas nacionalinės žiniasklaidos dėmesys. Esminis poveikis organizacijos strateginiams tikslams, teisiniams įsipareigojimams, aplinkosaugai ar reputacijai.
Vidutinis	Draudimu nepadengti finansiniai nuostoliai. Klientų nepasitenkinimas. Ribotas kritinės sistemos pasiekiamumas. Ribotas neigiamas regioninės ar vietinės žiniasklaidos dėmesys. Reikšmingas, bet ne esminis poveikis organizacijos veiklos tęstinumui ar tikslų pasiekimui.
Mažas	Draudimu nepadengti finansiniai nuostoliai. Klientai patiria laikinus nepatogumus. Kritinės sistemos sutrinka ribotam laikui. Pavienė vietinės žiniasklaidos aprėptis. Nedidelis poveikis organizacijos tikslams ar reputacijai, kurį galima suvaldyti be reikšmingų pasekmių.
Labai mažas	Menko reikšmingumo pasekmės organizacijai. Nėra poveikio veiklos tęstinumui ar žmonių bei turto saugai. Organizacija gali lengvai įveikti situaciją, panaudodama vidinius rezervus arba turimas operacines priemones.

Rizikos lygio (įsk. likutinio) nustatymo skalė:

Grėsmės įvykio tikimybė						
	Labai didelė / aukšta	(V)	(A)	(A)	(LA)	(LA)
	Didelė / aukšta	(Ž)	(V)	(A)	(A)	(LA)
	Vidutinė	(Ž)	(Ž)	(V)	(A)	(A)
	Maža	(LŽ)	(Ž)	(Ž)	(V)	(V)
	Labai maža	(LŽ)	(LŽ)	(Ž)	(Ž)	(Ž)
		Labai mažas	Mažas	Vidutinis	Didelis / aukštas	Labai didelis / aukštas
	Grėsmės įvykio poveikis					

Rizikos lygio žymėjimas:

Žymėjimas	Lygis	Valdymo prioritetas
(LA)	Labai didelis / aukštas	(5) Aukščiausias
(A)	Didelis / aukštas	(4) Aukštas
(V)	Vidutinis	(3) Vidutinis
(Ž)	Žemas	(2) Žemas
(LŽ)	Labai žemas	(1) Žemiausias

Sudarius tikimybės ir poveikio veiksnių matricą, organizacijai yra rekomenduojama nustatyti kiekvienos rizikos prioritetą ir užtikrinti, kad aukštesnio lygio (prioriteto) rizikos būtų valdomos, taikant tinkamą rizikos valdymo kryptį.

Rizikų valdymo krypties pritaikymas ir priemonių parinkimas

Rekomenduojama, kad organizacija, įvertinusi prigimtinę riziką bei atsižvelgdama į organizacijoje nustatytą rizikos apetitą ir tolerancijos lygį, parinktų tinkamiausią rizikos valdymo kryptį:

Priimti riziką – kai rizikos mažinimo ar pašalinimo kaštai yra didesni negu galimas rizikos poveikis, riziką galima pagrįstai priimti ir toliau stebėti.

Mažinti riziką – taikant kontrolės ar kitas priemones, galima sumažinti rizikos tikimybę arba poveikį iki priimtino lygio.

Perkelti riziką – perduoti rizikos valdymą trečiajai šaliai (pvz., draudimo bendrovei ar partneriui), jei jie gali ją efektyviau suvaldyti.

Vengti rizikos – visiškai atsisakyti veiklos ar sprendimo, kuri organizaciją padarytų pažeidžiamą nepriimtinai rizikai.

Žemiau lentelėje yra iliustruotos rekomenduojamos taikyti rizikos valdymo kryptys pagal nustatytą rizikos lygį.

Rizikos lygis	Rizikos lygio aprašymas	Rizikos valdymo kryptis
Labai didelis / aukštas	Kritinis neigiamas poveikis organizacijai, jos ištekliams, klientams, sektoriui ar partneriams.	**Vengti**
Didelis / aukštas	Didelis neigiamas poveikis organizacijai, jos ištekliams ar klientams.	**Mažinti, perkelti, vengti**
Vidutinis	Vidutinis neigiamas poveikis organizacijai, jos ištekliams ar klientams.	**Perkelti, vengti**
Žemas	Ribotas neigiamas poveikis organizacijai, jos ištekliams ar klientams.	**Priimti**
Labai žemas	Nereikšmingas neigiamas poveikis organizacijai, jos ištekliams ar klientams.	**Priimti**

Pasirinkus rizikų mažinimo kryptį, svarbu identifikuoti ir taikyti tinkamas kontrolės priemones, kurios sumažintų nepriimtiną rizikos lygį iki organizacijos rizikos apetitą atitinkančio lygio. Pagal ISO/IEC 27005 standartą, kontrolės priemonės gali būti klasifikuojamos į tris pagrindines grupes:

1. Prevencinės priemonės yra skirtos tam, kad grėsmė nepasireikštų (pvz., prieigos kontrolė, vartotojų autentifikavimas).
2. Identifikuojančios priemonės leidžia pastebėti grėsmės pasireiškimą (pvz., veiklos stebėsenos sistemos, įsibrovimų aptikimo sistemos).
3. Kompensacinės (korekcinės) priemonės padeda atkurti veiklą ar sumažinti poveikį pasireiškus rizikai (pvz., atsarginių kopijų atkūrimas, incidentų valdymo procedūros).

Rekomenduojama, kad visos taikomos kontrolės ar kitos priemonės būtų aprašytos ir periodiškai peržiūrimos. Siekiant užtikrinti, kad priemonės būtų aktualios, veiksmingos ir prisidėtų prie organizacijos atsparumo stiprinimo, rekomenduojama reguliariai, ne rečiau kaip kartą per 12 mėn. arba dažniau, jei to reikalauja situacija, vertinti jų veiksmingumą.

Likutinės rizikos valdymo planas ir tolimesni veiksmai

Atlikus prigimtinės rizikos vertinimą ir pritaikius atitinkamą rizikos valdymo kryptį bei atitinkamas priemones, yra nustatomas likutinis rizikos lygis, t. y. rizika, kuri išlieka po visų taikomų priemonių. Tais atvejais, kai likutinis rizikos lygis vis dar viršija organizacijos rizikos apetitą, turi būti parengtas tolesnis rizikos valdymo planas, kuriame nustatomos:

- papildomos priemonės, kurios valdys rizikas su nepriimtinu likutiniu rizikos lygiu;
- šių priemonių įgyvendinimui reikalingi ištekliai;
- atsakingi asmenys;
- įgyvendinimo terminai.

Rizikos valdymo planas turi būti realistiškas ir pritaikytas prie organizacijos veiklos pobūdžio bei suderintas su jos strateginiais tikslais. Jį įgyvendinus, rizika turi būti dar kartą įvertinama, užtikrinant, kad ji būtų tinkamai valdoma ir jos likutinis rizikos lygis atitiktų nustatytą organizacijos rizikos apetitą.

Siekiant ilgalaikio rizikos valdymo efektyvumo, rekomenduojama nuolat stebėti likutinės rizikos lygį, periodiškai peržiūrėti taikomą valdymo kryptį ir kontrolės priemones, prireikus ar reaguojant į pokyčius organizacijos vidinėje ar išorinėje aplinkoje, jas tobulinti ar keisti.

Periodinis rizikos vertinimas

Rizikų vertinimą yra privaloma atlikti ir dokumentuoti reguliariai, ne rečiau kaip kartą per 12 mėn. arba dažniau, jei to reikalauja situacija. Atliekant periodinį rizikų vertinimą yra tikslinga peržiūrėti ir organizacijos išteklių kritiškumo klasifikacijos tinkamumą ir susijusią dokumentaciją, siekiant užtikrinti, kad klasifikacija atitiktų esamą situaciją ir organizacijos poreikius.

Kibernetinio saugumo subjektas (organizacija) Nacionaliniam kibernetinio saugumo centrui (NKSC) privalo pateikti rizikos vertinimo ataskaitos ir rizikos valdymo plano patvirtinimo duomenis, nurodydamas patvirtinimo datą, registracijos numerį bei rizikos vertinimo metu nustatytus apibendrintus rezultatus: identifikuotas grėsmes, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemones. Šie duomenys turi būti pateikiami per kibernetinio saugumo informacinę sistemą (KSIS) ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo organizacijoje.

Kibernetinio saugumo subjekto (organizacijos) vadovo arba jo įgalioto asmens patvirtintos rizikos vertinimo ataskaitos ir rizikos valdymo planai turi būti saugomi ne trumpiau kaip 3 metus.

NKSC, atlikdamas kibernetinio saugumo subjekto (organizacijos) patikrinimą, turi teisę pareikalauti kibernetinio saugumo subjekto (organizacijos) pateikti rizikos vertinimo ataskaitos ir rizikos valdymo priemonių plano kopijas. Kibernetinio saugumo subjektas šiuos dokumentus turi pateikti per KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

Rizikų stebėjimas

Siekiant užtikrinti veiksmingą reagavimą į besikeičiančias vidinės ir išorinės aplinkos sąlygas, organizacijai rekomenduojama sukurti ir įgyvendinti rizikų stebėsenos procesą, kurio metu rizikų savininkai reguliariai analizuotų tiek vidinius, tiek išorinius veiksnius, galinčius turėti įtakos organizacijos pažeidžiamumui ar veiklos tęstinumui. **Rizikų stebėsenos procesas turėtų apimti šiuos pagrindinius elementus:**

- nustatytų rizikų rodiklių (KRI) peržiūros periodiškumą (pvz., ketvirčio ar metų);
- atsakingus asmenis ar padalinius;
- pokyčių identifikavimo mechanizmus (pvz., incidentų analizė, vidinio audito išvados, tiekėjų vertinimai);
- slenkstinius indikatorius, kada būtina iš naujo vertinti rizikas ar peržiūrėti rizikų valdymo kryptis bei nustatytus planus.

Siekiant išlaikyti efektyvią rizikų stebėseną taip pat yra svarbu reguliariai vertinti ir organizacijos gebėjimą laiku atpažinti naujas grėsmes ar pažeidžiamumus, galinčius turėti poveikį organizacijai. Todėl rizikų stebėsenos procesą ir jo efektyvumą yra rekomenduojama peržiūrėti ne rečiau kaip kartą per 12 mėn. arba dažniau, jei to reikalauja situacija.

RIZIKŲ VALDYMO SISTEMOS PERŽIŪRA IR TOBULINIMAS

Vadovaujantis gerąja praktika, rizikų valdymas yra tęstinis procesas, apimantis ne tik rizikų vertinimą bei stebėseną, bet ir periodinį rizikų valdymo sistemos atnaujinimą. Organizacijos vadovybei ar už rizikų valdymą paskirtam atsakingam asmeniui rekomenduojama reguliariai peržiūrėti bei tobulinti įdiegtą rizikų valdymo sistemą, įskaitant ir rizikų valdymo priemones.

Peržiūros metu rekomenduojama atsižvelgti į šiuos aspektus:

- vidinių ir išorinių auditų ataskaitas, jų rezultatus ir išvadas;
- informacijos saugumo incidentų statistiką, priežastis ir jų analizę;
- rizikos įvykių dažnį bei nustatytų rizikos valdymo tikslų pasiekimo lygį;
- taikomų teisės aktų, reguliavimo reikalavimų ir gerosios praktikos pokyčius.
- naujai atsiradusius verslo partnerius, klientų segmentus ar siūlomus produktus ir paslaugas;
- pokyčius organizacijos strateginiuose tikslusose, veiklos modeliuose ar struktūroje;

Rizikų valdymo sistemos peržiūrą yra rekomenduojama atlikti ne rečiau kaip kartą per 12 mėn. arba dažniau, jei organizacijoje įvyksta reikšmingų pokyčių.