PATVIRTINTA
Valstybinės kainų ir energetikos kontrolės
komisijos pirmininko 2017 m. spalio 31 d.
įsakymu Nr. O1E-108

RIZIKOS VERTINIMO ATLIKIMO VALSTYBINĖJE KAINŲ IR ENERGETIKOS KONTROLĖS KOMISIJOJE TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklės (toliau – Taisyklės) reglamentuoja Valstybinės kainų ir energetikos kontrolės komisijos (toliau – Komisija) rizikos valdymo procesą: įtakos veiklai analizę, pažeidžiamumo, grėsmių, rizikos tikimybės ir lygio nustatymą, rizikos priimtinumo nustatymą, taikytinų valdymo priemonių parinkimą, rizikos valdymo priemonių plano rengimą ir jo priežiūrą, rizikos priežiūrą.

2. Taisyklės nustato rizikos vertinimo metodiką, kuri užtikrina rizikos identifikavimą ir tinkamų saugumo priemonių parinkimą.

3. Taisyklės taikomos atliekant visoje Komisijoje tvarkomos bet kokios formos (žodinės, rašytinės ir elektroninės) informacijos, naudojamos įgyvendinant teisės aktų nustatytas funkcijas, ir ją apdorojančių informacinių technologijų priemonių ir kitos infrastruktūros rizikos vertinimą.

4. Taisyklės parengtos, vadovaujantis:

4.1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

4.2. Lietuvos standartu LST ISO/IEC 27001 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai" (toliau – Lietuvos standartas LST ISO/IEC 27001);

4.3. Lietuvos standartu LST ISO/IEC 27005 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas";

4.4. kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais saugų duomenų valdymą ir jų tvarkymo teisėtumą.

5. Taisyklėse vartojamos tokios sąvokos:

Apsaugos priemonės – administracinės, teisinės, vadybos ir techninės priemonės, mažinančios riziką;

Agentūra – Energetikos reguliavimo institucijų bendradarbiavimo agentūra (angl. ACER);

Grėsmė – potenciali nepageidaujamų įvykių, išnaudojančių pažeidžiamumus ir galinčių padaryti žalą Komisijai ir Komisijos informacinėms sistemoms, galimybė;

Informaciniai ištekliai – Komisijos informacija, kurią tvarko Komisija, atlikdama teisės aktų nustatytas funkcijas, apdorojama informacinių technologijų priemonėmis, bei ją apdorojančios informacinių technologijų priemonės ir kita infrastruktūra;

ISVS – administracinių, teisinių, vadybos ir techninių priemonių visuma, skirta informacijos saugumo procesui valdyti, atsižvelgiant į nustatytą rizikos lygį ir bendrą Komisijos veiklos valdymo politiką;

Infrastruktūra – apima tarpsluoksnio programinę įrangą, duomenų bazių valdymo sistemas, operacines sistemas, techninę įrangą, kompiuterių tinklus, duomenų masyvus ir jų tinklus, patalpas ir įrengimus bei minėtiems ištekliams palaikyti reikalingas paslaugas;

Darbuotojas – Komisijos dirbantis valstybės pareigūnas, valstybės tarnautojas bei darbuotojas, dirbantis pagal darbo sutarti;

Informacinio ištekliaus savininkas – darbuotojas, atsakingas už informacinio ištekliaus priežiūrą ir informacijos saugumo reikalavimų nustatymą priskirtam informaciniam ištekliui;

IS – informacinė sistema;

Įtaka (poveikis veiklai) – teigiamas ar neigiamas poveikis Komisijos veiklai;

Įvykis – įvykis, susijęs su informaciniu ištekliu, rodantis galimą informacijos saugumo politikos spragą ar apsaugos priemonių triktį arba anksčiau nenumatytos situacijos, turinčios poveikio (teigiamą ar neigiamą) saugumo užtikrinimui, atsiradimą;

Konfidencialumas – informacijos savybė, reiškianti, kad su ja gali susipažinti tik tam įgalioti asmenys;

Liekamoji rizika – rizika, pritaikius rizikos valdymo priemones;

Naudotojas – darbuotojas, turintis teisę naudotis informaciniais ištekliais;

Nepriimtina rizika – rizika, kuri yra nepriimtina Komisijai, atsižvelgiant į grėsmės tikimybės laipsnį ir jos sukeltų padarinių dydį;

Pasiekiamumas – informacijos savybė, reiškianti, kad informacija gali būti tvarkoma reikiamu metu;

Pažeidžiamumas – turto ar turto dalies savybė, nurodanti pažeidžiamiausią vietą, dėl kurios gali kilti viena ar daugiau grėsmių šiam turtui;

Pagrindinis informacinis išteklius – su rizikos vertinimo objektu susijusi Komisijos informacija;

Pagalbinis informacinis išteklius – su rizikos vertinimo objektu susijusi infrastruktūra, nuo kurios priklauso pagrindiniai informaciniai ištekliai ir jų tinkamas veikimas;

Priimtina rizika – rizika, kuri yra priimtina Komisijai, atsižvelgiant į nustatytus kriterijus, pvz., veiklos ir teisinius reikalavimus, apsaugos priemonių kaštus;

Informacijos saugos įgaliotinis – Komisijos pirmininko įgaliotas Komisijos valstybės tarnautojas ar darbuotojas, įgyvendinantis Taisyklių nustatyta tvarka jam pavestas funkcijas;

Respondentas – Komisijos administracijos padalinio vadovo paskirtas darbuotojas, turintis kompetencijos atsakyti į rizikos vertintojo pateiktus klausimus, priklausančius to administracijos padalinio kompetencijai;

Rizika – informacijos saugumo įvykio tikimybės ir jo padarinių derinys;

Rizikos analizė – sisteminis informacijos naudojimas, siekiant nustatyti rizikos priežastis ir ją įvertinti;

Rizikos mažinimas – veiksmai, skirti sumažinti grėsmės tikimybę ir (ar) neigiamas pasekmes;

Rizikos perdavimas – rizikos sąlygojamų nuostolių naštos pasidalijimas su trečiuoju asmeniu;

Rizikos prisiėmimas – sprendimas prisiimti riziką;

Rizikos vertinimas – rizikos analizės procesas, kurio metu galima rizika lyginama su numatytais kriterijais, siekiant nustatyti rizikos lygį;

Rizikos valdymas – darnūs veiksmai, kuriais, atsižvelgiant į riziką, siekiama koordinuoti ir kontroliuoti Komisijos veiklos riziką;

Rizikos vengimas – sprendimas nesiimti veiklos, susijusios su konkrečia rizika, ar ją nutraukti;

Rizikos vertinimas – bendrasis rizikos analizės ir rizikos įvertinimo procesas;

Rizikos vertintojas – informacijos saugos įgaliotinis ar kitas Komisijos pirmininko įgaliotas Komisijos darbuotojas, Taisyklių nustatyta tvarka atliekantis Komisijos informacinių sistemų rizikos vertinimą;

Tikimybė – tam tikro nepastovaus įvykio tikėtinumas, nustatomas pagal sutartus kriterijus;

Turtas – tai visas su informacinėmis sistemomis susijęs turtas: informacija, programinė ir techninė įranga bei informacinių sistemų paslaugos;

Vientisumas – informacijos savybė, reiškianti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

Kitos Taisyklėse vartojamos sąvokos atitinka Lietuvos Respublikos teisės aktuose, reglamentuojančiuose saugų duomenų valdymą ir jų tvarkymo teisėtumą, vartojamas sąvokas.

II SKYRIUS
ATSAKOMYBĖS

6. Informacijos saugos įgaliotinis organizuoja arba Komisijos pirmininko pavedimu pats atlieka šias veiklas:
- apibrėžia rizikos vertinimo objektą ir kriterijus;
- identifikuoja pažeidžiamumus ir galimas grėsmes;
- identifikuoja esamas valdymo priemones;
- nustato rizikos lygį;
- parengia rizikos valdymo priemonių planą ir kontroliuoja jo įgyvendinimą;
- atlieka rizikos stebėseną ir peržiūrą;
- komunikuoja rezultatus Komisijos vadovybei;
- prižiūri šių Taisyklių įgyvendinimą ir vykdymą;
- dokumentuoja pastebėtas neatitiktis, analizuoja jų priežastis ir koordinuoja jų šalinimą.

7. Informacinių išteklių savininkai (valdytojai):
- nustato informacinių išteklių įtaką;
- nustato galimas grėsmes ir jų tikimybes informaciniams ištekliams;
- nustato pažeidžiamumus.

8. Rizikos savininkai:
- vykdo nustatytos rizikos stebėseną;
- numato rizikos valdymo priemones rizikai valdyti;
- prižiūri rizikos valdymo priemonių įgyvendinimą.

III SKYRIUS
RIZIKOS VERTINIMO PROCESAS

9. Informacijos saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja Komisijos rizikos vertinimą ir pateikia rizikos vertinimo ataskaitą bei rizikos valdymo priemonių planą tvirtinimui vadovybinės vertinamosios analizės posėdžio metu. Prireikus gali būti organizuojamas neeilinis Komisijos rizikos vertinimas. Komisijos pirmininko sprendimu rizikos vertinimas gali būti atliekamas ir Tiekėjų. Rizikos vertinimo proceso schema pateikta šių Taisyklių 1 priede (1 priedas).

10. Neeilinį Komisijos rizikos vertinimą turi teisę inicijuoti informacinių išteklių savininkai ir rizikos savininkai, raštu kreipdamiesi į Informacijos saugos įgaliotinį.

11. Neeilinis Komisijos rizikos vertinimas turi būti atliekamas, kai:

11.1. pradedama kurti nauja arba modernizuojama jau veikianti Komisijos informacinė sistema;

11.2. užbaigiama kurti arba modernizuoti Komisijos informacinė sistema;

11.3. atlikus esminius Komisijos informacinės sistemos veiklą užtikrinančios programinės ir aparatinės įrangos pakeitimus;

11.4. pakeičiama patalpų ir / ar pastatų išdėstymo vieta;

11.5. įvyksta I kategorijos informacijos saugumo incidentas;

11.6. įvykus esminiams veiklos pokyčiams;

11.7. prieš vykdant ar įvykus kitiems esminiams pasikeitimams Komisijoje, dėl kurių galėjo pasikeisti informacinių išteklių įtaka, atsirasti pažeidžiamumų ir grėsmių pokyčių.

12. Sprendimą atlikti neeilinį rizikos vertinimą priima Informacijos saugos įgaliotinis.

13. Rizikos vertinimo procesą sudaro šios dalys:

13.1. rizikos vertinimo objekto apibrėžimas ir vertinimo kriterijų nustatymas;

13.2. rizikos vertinimas – informacinių išteklių analizė ir rizikos analizė;

13.3. rizikos valdymas – tinkamų rizikos valdymo priemonių, mažinančių riziką iki priimtino lygio, parinkimas.

14. Rizikos vertintojas, atlikęs rizikos vertinimą:

14.1. per 5 darbo dienas nuo rizikos vertinimo ataskaitos parengimo dienos Komisijos nustatyta tvarka rizikos vertinimo ataskaitą pateikia susipažinti ir derinti:

14.1.1. informacinių išteklių, kurių rizika buvo vertinama, savininkams;

14.1.2. Komisijos Turto valdymo ir viešųjų pirkimų skyriaus vedėjui;

14.2. per 10 darbo dienų nuo ataskaitos suderinimo su atsakingais asmenimis Komisijos nustatyta tvarka pateikia Komisijos pirmininkui tvirtinti.

IV SKYRIUS
RIZIKOS VERTINIMO OBJEKTO APIBRĖŽIMAS IR VERTINIMO KRITERIJŲ NUSTATYMAS

15. Rizikos vertintojas, pradėjęs rizikos vertinimą, turi apibrėžti rizikos vertinimo objektą (pvz., viena, kelios ar visos Komisijos informacinės sistemos) ir, atlikus interviu su Respondentais, nustatyti su rizikos vertinimo objektu susijusį Komisijos turtą. Turi būti sudaromas rizikos vertinimo apimtyje esančių informacinių išteklių sąrašas, kurio forma pateikiama šių Taisyklių 6 priede (6 priedas). Informaciniai ištekliai skirstomi į pagrindinius (informacija) ir pagalbinius, nuo kurių priklauso pagrindiniai informaciniai ištekliai ir jų veikimas (techninė įranga, programinė įranga, tinklo įranga, žmogiškieji ištekliai, patalpos ir įrengimai).

16. Nagrinėjamos informacinių išteklių tarpusavio sąsajos ir priklausomybės – kuo daugiau procesų priklauso nuo tam tikro informacinio ištekliaus, tuo didesnė jo įtaka.

17. Rizikos vertinimui naudojami ARSIS metodikoje numatyti kriterijai: poveikio veiklai kriterijai ir tikimybės kriterijai. Šie kriterijai pateikti Taisyklių 2 ir 3 Prieduose (2 priedas, 3 priedas).

18. Rizikos vertintojas rizikos vertinimo metu turi nustatyti, ar informacinių išteklių tvarkymas Komisijos informacinėse sistemose yra Lietuvos Respublikos teisės aktų nustatyta tvarka įteisintas.

V SKYRIUS
INFORMACINIŲ IŠTEKLIŲ IR RIZIKOS ANALIZĖ

19. Rizikos vertintojas, identifikavęs rizikos vertinimo objektą, turi nustatyti jo poveikį (įtaką) Komisijos veiklai. Rizikos vertinimo objekto poveikis turi būti nustatomas, atsižvelgiant į Taisyklių 2 priede nustatytus poveikio veiklai kriterijus, įvertinant poveikį informacijos konfidencialumui, prieinamumui ir vientisumui.

20. Rizikos vertintojas, apklausdamas Respondentus, turi įvertinti pasekmes Komisijos turtui, atsižvelgiant į Valdymo ir veiklos sutrikdymą, Asmenų saugumą, Gamtą ir aplinkos saugumą, Finansinius nuostolius, Viešąją tvarką, tarptautinius santykius bei padarinius valstybei ir institucijoms:

20.1. Komisijos ar atskirų Komisijos administracijos padalinių valdymo ir veiklos sutrikdymas;

20.2. asmenų saugumo pažeidimas, kai dėl informacijos neteisėto atskleidimo ar pakeitimo gali kilti pavojus asmens ar asmenų grupės gerovei ar saugumui (pvz., paviešinama informacija apie brangų turtą įsigijusius asmenis ir pan.);

20.3. gamta ir aplinkos saugumas, kai dėl informacijos atskleidimo, sunaikinimo ar neprieinamumo gali kilti grėsmė įvykti procesams, kurie gali sukelti pavojų gamtos ir aplinkos saugumui;

20.4. finansiniai nuostoliai, kai Komisija gali patirti tiesioginius finansinius nuostolius (pvz., tinkamai nepasirūpinus atsarginėmis kopijomis ir, praradus informaciją, gali tekti samdyti darbuotojus ir mokėti jiems už duomenų įvedimą ar, tinkamai nepasirūpinus priešgaisrine apsauga, gaisro atveju bus visiškai ar iš dalies sunaikintas Komisijos turtas, ir pan.);

20.5. viešosios tvarkos sutrikdymas, kai, įvykus informacijos paviešinimui, sugadinimui ar neprieinamumui, gali būti išprovokuoti pavieniai ar masiniai gyventojų neramumai;

20.6. įtaka tarptautiniams santykiams, kai, pvz., dėl neteisėto duomenų atkleidimo gali būti pareikštos Europos Sąjungos ar kitų šalių pretenzijos;

20.7. padariniai valstybei ir institucijoms, kai dėl informacijos konfidencialumo, vientisumo ar prieinamumo praradimo gali kilti padarinių valstybei ar jos gyventojams.

21. Pasekmės Komisijos turtui, atsižvelgiant į informacijos saugumo incidentų poveikį, turi būti vertinamos penkių balų vertinimo skalėje: 1 (labai mažo lygio poveikis), 2 (mažo lygio poveikis), 3 (vidutinio lygio poveikis), 4 (didelio lygio poveikis), 5 (labai didelio lygio poveikis). Pasekmės nustatomos pagal Taisyklių 2 Priede (2 priedas) nurodytus poveikio veiklai kriterijus. Esant skirtingiems vertinimams, kiekvienoje iš pasekmių Komisijos turtui srityje visada turi būti įrašomas didžiausią vertę turintis balas.

22. Rizikos vertinimo metu nustatytas pasekmes Komisijos turtui Rizikos vertintojas turi įforminti Poveikio veiklai analizės dokumente (Taisyklių 7 priedas) ir pateikti rizikos vertinimo ataskaitoje, nurodant vieną iš daugiausiai balų surinkusių pasekmių Komisijos veiklai pavadinimą ir šių pasekmių vertinimą penkių balų skalėje. Įrašomos tik tos pasekmės Komisijos veiklai pavadinimas, kurios buvo įvertintas aukščiausiu balu. Jeigu didžiausiu balu buvo įvertintos kelios pasekmės Komisijos veiklai, turi būti įrašomi visi aukščiausiu balu įvertinti pasekmių Komisijos veiklai pavadinimai.

23. Rizikos vertintojas pagal Grėsmių sąrašą (Taisyklių 5 priedas) įvertina nustatytam Komisijos turtui grėsmių kilimo tikimybes dėl tikėtinų pažeidžiamumų, kai realizuosis atitinkamos grėsmės, naudodamasis pateiktais grėsmių tikimybės vertinimo kriterijais (Taisyklių 3 priedas).

24. Grėsmių tikimybės turi būti vertinamos penkių lygių skalėje: labai žema, žema, vidutinė, aukšta ir labai aukšta.

25. Grėsmių tikimybė vertinama, atsižvelgiant į buvusius informacijos saugumo incidentus bei esamus pažeidžiamumus, kurie gali padidinti grėsmės tikimybę.

26. Pažeidžiamumai gali būti nustatomi:

26.1. naudojant automatizuotą pažeidžiamumų skenavimo įrankį;

26.2. atliekant saugumo testavimus ir įvertinimus;

26.3. atliekant įsilaužimų testus;

26.4. apklausiant darbuotojus;

26.5. atliekant fizinę apžiūrą;

26.6. analizuojant dokumentus;

27. Pažeidžiamumai gali būti nustatyti šiose srityse:

27.1. procesai ir procedūros;

27.2. valdymo procedūros;

27.3. žmogiškieji ištekliai;

27.4. fizinė aplinka;

27.5. informacinių sistemų sąranka;

27.6. techninė, programinė ar tinklo įranga;

27.7. paslaugos, kurias teikia tretieji asmenys.

28. Pažeidžiamumų identifikavimo rezultatas – nustatytos vertinamų išteklių pažeidžiamos vietos, susijusios su esančiomis grėsmėmis ir naudojamomis apsaugos priemonėmis.

29. Rizikos vertintojas pagal Rizikos matricą (Taisyklių 4 priedas) nustato rizikos lygį, atsižvelgdamas į nustatytas Komisijos turto vertes ir šiam turtui nustatytus grėsmių lygius.

30. Rizikos vertinimo metu nustatytus grėsmių, pažeidžiamumų ir rizikos lygius rizikos vertintojas turi įforminti Rizikos sąraše (Taisyklių 8 priedas) ir pateikti rizikos vertinimo ataskaitoje.

31. Rizikos lygis gali būti vertinamas nuo 1 iki 5 balų.

32. Rizika gali būti priimtina arba nepriimtina. Nepriimtina rizika laikoma, kai jos lygis yra aukštesnis negu 3 balai. Rizika, įvertinta 1,2 ir 3 balais laikoma priimtina. Nepriimtinos rizikos atveju sudaromas priemonių, skirtų nepriimtinai rizikai mažinti, planas.

VI SKYRIUS
RIZIKOS VALDYMAS

33. Kiekvienai rizikai priskiriami rizikos savininkai – už rizikos tvarkymą atsakingi Komisijos darbuotojai. Rizikos savininkai nurodomi rizikos vertinimo ataskaitoje ir tvirtinami Komisijos pirmininko įsakymu.

34. Informacijos saugos įgaliotinis, atsižvelgdamas į rizikos vertinimo ataskaitą, ne vėliau kaip per 30 dienų nuo rizikos vertinimo ataskaitos patvirtinimo turi parengti rizikos valdymo priemonių planą.

35. Rizikos valdymo priemonių plane turi būti nurodytos rizikos valdymo priemonės, šių priemonių įgyvendinimo datos, išteklių poreikiai bei nurodomi už šių priemonių įgyvendinimą atsakingi Komisijos darbuotojai (Taisyklių 9 priedas).

36. Rizikos valdymo priemonių planas Komisijos nustatyta tvarka teikiamas tvirtinti Komisijos pirmininkui.

37. Rizikos valdymo priemonės turi būti parenkamos, atsižvelgiant į poveikį Komisijos veiklai ir turto, kurio apsaugai numatoma taikyti rizikos valdymo priemones, vertę. Rizikai valdyti turi būti apsvarstyti šie veiksmai:

37.1. siūlyti diegti rizikos apsaugos priemones, padedančias sumažinti rizikos lygį iki priimtino lygio;

37.2. siūlyti sąmoningai ir objektyviai priimti riziką, jeigu tai priimtina Komisijos veiklai;

37.3. vengti rizikos, iškeliant saugomą Komisijos turtą už rizikos zonos – iš fizinių zonų ar iš Komisijos veiklos procesų;

37.4. perduoti su Komisijos veikla susijusią riziką trečiosioms šalims.

38. Rizikos stebėsena, peržiūra ir komunikavimas.

38.1. Įgyvendinus rizikos valdymo priemonių planą, rizika nuolat stebima ir Taisyklių 9 punkte numatytu periodiškumu vertinama pakartotinai.

38.2. Turi būti stebima:

38.2.1. nauji informaciniai ištekliai, susiję su rizikos vertinimo objektu ir kontekstu;

38.2.2. informacinių išteklių įtakos pasikeitimai, susiję su pasikeitusiais veiklos reikalavimais;

38.2.3. naujai atsiradusios grėsmės;

38.2.4. informacijos saugumo įvykiai ir incidentai, susiję su nustatyta rizika.

VII SKYRIUS
TAIKOMUMO PAREIŠKIMAS

39. Įvertinus rizikas, po rizikos vertinimo ataskaitos ir rizikos valdymo priemonių plano patvirtinimo, rizikos vertintojas turi parengti Taikomumo pareiškimą (Taisyklių 10 priedas).

40. Taikomumo pareiškimo skiltyje „Ar taikomas?“ turi būti nurodoma:

40.1. „Taip“, jei reikalavimas taikomas Komisijoje;

40.2. „Ne“, jei reikalavimas netaikomas Komisijoje.

41. Taikomumo pareiškimo skiltyje „Reikalavimo taikymo ar netaikymo pagrindimas: mažinama rizika" reikia nurodyti reikalavimo taikymo ar netaikymo priežastis:

41.1. jei reikalavimas taikomas, nurodyti mažinamą riziką iš Rizikų sąrašo;

41.2. jei reikalavimas netaikomas, aprašyti netaikymo pagrindimą.

42. Taikomumo pareiškimo skiltyje „Ar įgyvendintas?" taikomiems reikalavimams turi būti nurodoma:

42.1. „Taip“, jei reikalavimas įgyvendintas;

42.2. „Ne“, jei reikalavimas neįgyvendintas.

43. Taikomumo pareiškimas Komisijos nustatyta tvarka teikiamas tvirtinti Komisijos pirmininkui.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Komisijos administracijos padalinių vadovai turi užtikrinti, kad Respondentais paskirtų kvalifikuotus Komisijos darbuotojus.

45. Jei rizikos vertinimą atlieka išorinių paslaugų teikėjas, viešojo pirkimo techninėje specifikacijoje turi būti numatyta prievolė riziką vertinti, vadovaujantis šiose Taisyklėse numatyta rizikos vertinimo metodika.

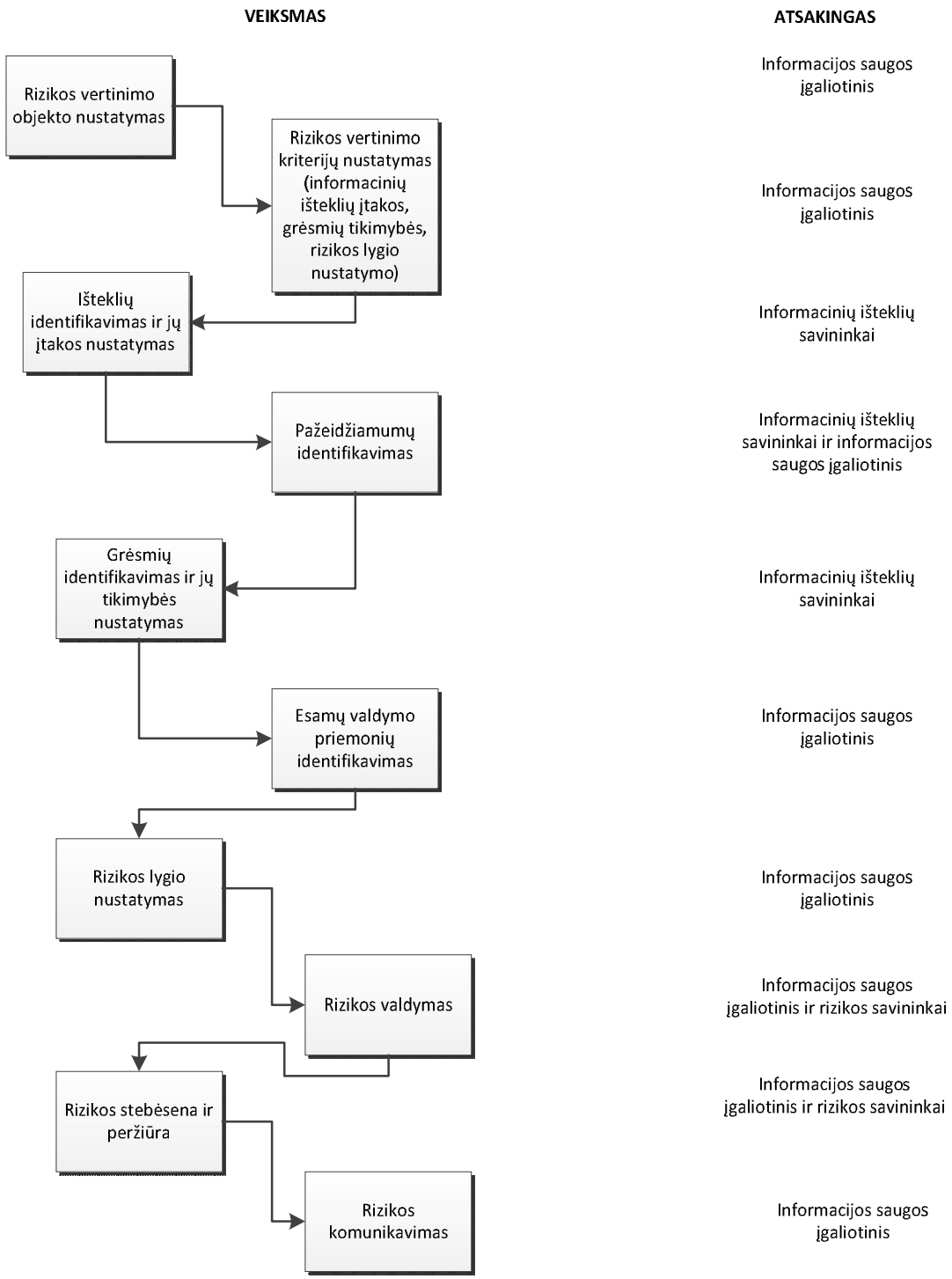
46. Taisyklėmis privalo vadovautis visi Komisijos darbuotojai, dalyvaujantys rizikos vertinimo procese: informacinių išteklių savininkai, Komisijos administracijos padalinių ir Komisijos administracijos padalinių, atsakingų už Komisijos informacinių sistemų priežiūrą, Komisijos patalpų fizinę apsaugą bei Komisijos infrastruktūros elementų tinkamą veikimą, Komisijos darbuotojai.

IX SKYRIUS
PRIEDAI

47. 1 priedas. Rizikos valdymo proceso srauto diagrama
48. 2 priedas. Poveikio veiklai vertinimo kriterijai
49. 3 priedas. Grėsmių tikimybės vertinimo kriterijai
50. 4 priedas. Rizikos matrica
51. 5 priedas. Grėsmių sąrašas
52. 6 priedas. Informacinių išteklių sąrašas
53. 7 priedas. Poveikio veiklai analizės dokumentas
54. 8 priedas. Rizikos sąrašas
55. 9 priedas. Rizikos valdymo priemonių planas
56. 10 priedas. Taikomumo pareiškimo lentelė

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
1 priedas

RIZIKOS VALDYMO PROCESO SRAUTO DIAGRAMA



Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
2 priedas

POVEIKIO VEIKLAI VERTINIMO KRITERIJAI

	Valdymo ir veiklos sutrikdymas	**Asmenų saugumas**	**Gamta ir aplinkos saugumas**	**Finansiniai nuostoliai**	**Viešoji tvarka**	**Tarptautiniai santykiai**	**Padariniai valstybei ir institucijoms**
Labai mažas (1)	Veikla nebus sutrikdyta	Netaikoma	Netaikoma	Nuostolių nebus	Netaikoma	Netaikoma	Padarinių valstybei ir institucijoms nebus
Mažas (2)	Gali kilti grėsmė įvykti procesams, kurie gali turėti neigiamų padarinių atskirų institucijos padalinių veiklai	Netaikoma	Netaikoma	Gali kilti grėsmė įvykti procesams, kurie vienai institucijai gali sukelti finansinius nuostolius ne didesnius nei 290 eurų	Netaikoma	Netaikoma	Gali kilti grėsmė įvykti procesams, kurie gali sukelti kitų neigiamų padarinių institucijai, atskirų institucijos padalinių veiklai
Vidutinis (3)	Gali kilti grėsmė įvykti procesams, kurie gali turėti neigiamų padarinių institucijos veiklai	Netaikoma	Netaikoma	Gali kilti grėsmė įvykti procesams, kurie vienai institucijai gali sukelti finansinius nuostolius ne didesnius nei 0,3 mln. eurų	Gali kilti grėsmė įvykti procesams, kurie gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų tretiesiems interesams, taip pat ir asmens duomenų apsaugai	Netaikoma	Gali kilti grėsmė įvykti procesams, kurie gali sukelti kitų neigiamų padarinių institucijai

	Valdymo ir veiklos sutrikdymas	**Asmenų saugumas**	**Gamta ir aplinkos saugumas**	**Finansiniai nuostoliai**	**Viešoji tvarka**	**Tarptautiniai santykiai**	**Padariniai valstybei ir institucijoms**
Didelis (4)	Gali kilti grėsmė įvykti procesams, kurie gali sutrikdyti kelių institucijų veiklą ar viešųjų paslaugų teikimą daugiau kaip vienai dienai	Gali kilti grėsmė procesams, kurie gali turėti neigiamų padarinių Lietuvos Respublikos teritorijos gyventojų sveikatos apsaugai	Gali kilti grėsmė įvykti procesams, kurie gali sukelti pavojų gamtos ir aplinkos saugumui	Gali kilti grėsmė įvykti procesams, kelioms institucijoms gali sukelti finansinius nuostolius, didesnius nei 0,3 mln. eurų, bet ne didesnius nei 1,5 mln. Eurų	Gali kilti grėsmė įvykti procesams, kurie gali sukelti pavojų viešajai tvarkai ir gyventojų saugumui	Gali kilti grėsmė įvykti procesams, kurie gali sukelti kelių institucijų tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio pasekmių pašalinimas sukeltų didesnius nei 0,3 mln. eurų, bet ne didesnius nei 1,5 mln. eurų nuostolius	Gali kilti grėsmė įvykti procesams, kurie gali sukelti kitų sunkių padarinių kelioms institucijoms ar jų reguliavimo sričiai priskirtai ūkio šakai
Labai didelis (5)	Gali kilti grėsmė įvykti procesams, kurie gali turėti sunkių padarinių Lietuvos ūkiui - sukelti žymų, daugiau kaip 5 procentų, metinio nacionalinio produkto sumažėjimą ar kitus sunkius padarinius	Gali kilti grėsmė procesams, nuo kurių tiesiogiai priklauso Lietuvos Respublikos teritorijos gyventojų sveikata ir gyvybė	Gali kilti grėsmė įvykti procesams, nuo kurių tiesiogiai priklauso neigiami padariniai gamtai ir aplinkos saugumui	Gali kilti grėsmė įvykti procesams, kurie gali sukelti didesnius kaip 1,5 mln. eurų finansinius nuostolius valstybei	Gali kilti grėsmė įvykti procesams, kurie gali turėti neigiamų padarinių viešajai tvarkai ir gyventojų saugumui	Gali kilti grėsmė įvykti procesams, kurie gali sukelti valstybės tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio pasekmių pašalinimas sukeltų didesnius nei 1,5 mln. Eurų nuostolius	Gali kilti grėsmė įvykti procesams, kurie gali sukelti kitų sunkių padarinių valstybei ar jos gyventojams

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
3 priedas

GRĖSMIŲ TIKIMYBĖS VERTINIMO KRITERIJAI

Reikšmė	**Apibūdinimas**
Labai žema (1)	rečiau nei vieną kartą per 3 metus
Žema (2)	ne dažniau nei vieną kartą per 3 metus
Vidutinė (3)	vieną kartą per metus
Aukšta (4)	kelis kartus per metus
Labai aukšta (5)	vieną kartą per mėnesį ir dažniau

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
4 priedas

RIZIKOS MATRICA

Poveikis veiklai	**Labai didelis (5)**	1 (labai žemas)	2 (žemas)	3 (vidutinis)	4 (aukštas)	5 (labai aukštas)
	Didelis (4)	1 (labai žemas)	2 (žemas)	3 (vidutinis)	4 (aukštas)	4 (aukštas)
	Vidutinis (3)	1 (labai žemas)	2 (žemas)	3 (vidutinis)	3 (vidutinis)	3 (vidutinis)
	Mažas (2)	1 (labai žemas)	2 (žemas)	2 (žemas)	2 (žemas)	2 (žemas)
	Labai mažas (1)	1 (labai žemas)	1 (labai žemas)	1 (labai žemas)	1 (labai žemas)	1 (labai žemas)
		Labai žema (1)	**Žema (2)**	**Vidutinė (3)**	**Aukšta (4)**	**Labai aukšta (5)**
		Tikimybė				

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
5 priedas

GRĖSMIŲ SĄRAŠAS

ID	GRĖSMĖ
G01	Gaisras
G02	Nepalankios oro sąlygos
G03	Vanduo
G04	Tarša, dulkės, korozija
G05	Stichinės nelaimės
G06	Aplinkos nelaimės
G07	Dideli įvykiai aplinkoje
G08	Elektros tiekimo gedimas ar sutrikimas
G09	Ryšių tinklų gedimas ar sutrikimas
G10	Magistralinio tiekimo gedimas ar sutrikimas
G11	Paslaugų teikėjų patiriamas gedimas ar sutrikimas
G12	Įsiterpianti spinduliuotė
G13	Informatyvi spinduliuotė
G14	Informacijos perėmimas/ šnipinėjimas
G15	Slaptas klausymasis
G16	Įrangos, duomenų laikmenų ir dokumentų vagystė
G17	Įrangos, duomenų laikmenų ir dokumentų praradimas
G18	Netinkamas planavimas arba suderinamumo trūkumas
G19	Konfidencialios informacijos atskleidimas
G20	Informacija ar produktai iš nepatikimų šaltinių
G21	Manipuliavimas aparatine ir programine įranga
G22	informacijos klastojimas
G23	neleistina prieiga prie IT sistemų
G24	Įrangos ar duomenų laikmenų sunaikinimas
G25	Įrangos ar sistemų gedimas
G26	Įrangos ar sistemų sutrikimas
G27	Išteklių trūkumas
G28	Programinės įrangos pažeidžiamumai ir klaidos
G29	Teisės aktų ir taisyklių pažeidimai
G30	Nesankcionuotas įrangos ir sistemų naudojimas ar administravimas
G31	Netinkamas įrangos ir sistemų naudojimas ar administravimas
G32	Piktnaudžiavimas įgaliojimais
G33	Darbuotojų stygius
G34	Ataka
G35	Prievarta, plėšimas arba korupcija
G36	Tapatybės vagystė
G37	Veiksmų išsižadėjimas
G38	Piktnaudžiavimas asmens duomenimis
G39	Kenkėjiška programinė įranga
G40	Paslaugos atkirtimas
G41	Sabotažas
G42	Socialinė inžinerija
G43	Pranešimų persiuntimas

G44	Neleistinas patekimas į patalpas
G45	Duomenų praradimas
G46	Svarbios informacijos vientisumo praradimas

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
6 priedas

INFORMACINIŲ IŠTEKLIŲ SARAŠAS

Eil. Nr.	Informacinių išteklių klasifikacija		Informacinis išteklius	Informacinio ištekliaus savininkas	Informacinio ištekliaus vieta	Informacinio ištekliaus forma (taikoma tik informacijai)	Konfidencialumas	Vientisumas	Prieinamumas
	Tipas: Pagrindinis /pagalbinis	Rūšis							

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
7 priedas

POVEIKIO VEIKLAI ANALIZĖS DOKUMENTAS

Informacinio ištekliaus pavadinimas	
Informacinio ištekliaus savininko vardas, pavardė, pareigos	
Trumpa informacinio ištekliaus paskirties ar vykdomų funkcijų santrauka (pagrindiniai tikslai, saugomi duomenys, naudotojų skaičius)	
Konfidencialumo įvertinimas (užduoti klausimus apie tai, kokie duomenys yra tvarkomi, kam jie prieinami, kokia galima žala dėl jų paviešinimo).	
Vientisumo įvertinimas (užduoti klausimus apie tvarkomų duomenų tikslumo svarbą, įtaką veiklai dėl atsiradusių neteisingų arba pakeistų duomenų, reikalingą laiką, sąnaudas ir priemones neteisingų arba pakeistų duomenų atstatymui)	
Prieinamumo įvertinimas (užduoti klausimus apie toleruotiną neveikimo (neprieinamumo) laiką, buvusius prieinamumo sutrikimus praeityje, tokių sutrikimų įtaką veiklai, galimą žalą informaciniam ištekliui esant neprieinamam ilgesniam laikui)	

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
8 priedas

RIZIKOS SĄRAŠAS

Informacinis išteklius	Poveikis veiklai	Grėsmė	Tikimybė	Rizikos lygis	Priimtinumas	Rizikos valdymas	Liekamoji rizika	Rizikos savininkas

Rizikos vertinimo atlikimo Valstybinėje kainų
ir energetikos kontrolės komisijoje taisyklių
9 priedas

RIZIKOS VALDYMO PRIEMONIŲ PLANAS

Eil. Nr.	Rizikos valdymo priemonė	Susijusios grėsmės	Mažinamų rizikų ID	Planuojamas įgyvendinimo terminas	Išteklių poreikiai	Atsakingas asmuo (skyrius)	Įdiegimo statusas

Rizikos vertinimo atlikimo Valstybinėje kainų ir energetikos kontrolės komisijoje taisyklių
10 priedas

TAIKOMUMO PAREIŠKIMO LENTELĖ

Priemonė	**Valdymo priemonės pavadinimas**	**Valdymas**	**Ar taikomas? (Taip/Ne)**	**Taikomumo /netaikymo pagrindimas: mažinama rizika**	**Ar įgyvendintas? (Taip/Ne)**	**Taikomos priemonės aprašas (įdiegimo lygis, naudojamos techninės ir organizacinės apsaugos priemonės, reglamentuojantys dokumentai)**