



Valstybinio audito ataskaita

VIDAUS REIKALŲ MINISTERIJOS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

2016 m. spalio 13 d. Nr. VA-P-90-2-19



Su valstybinio audito ataskaita galima susipažinti
Valstybės kontrolės interneto puslapyje
adresu www.vkontrole.lt

TURINYS

SANTRUMPOS IR SAVOKOS	3
SANTRAUKA	4
IŠVADOS	5
REKOMENDACIJOS	6
IŽANGA	8
AUDITO REZULTATAI	10
1. Informacinių technologijų planavimas turi trūkumų	10
1.1. Nerengiamas IT strateginis planas	11
1.2. Į ministerijos metinius veiklos planus įtrauktos ne visos svarbiausios IT srityje vykdomos veiklos	11
2. Vidaus reikalų ministerijos valdymo srities informacinė architektūra neapibrėžta	12
2.1. Ministerija neturi tikslių duomenų apie naudojamą programinę įrangą	13
2.2. Ne visų ministerijos valdomų informacinių išteklių nuostatai atnaujinti, parengtos ne visos specifikacijos	14
2.3. VRIS architektūra sudėtinga ir nelanksti	15
2.4. Duomenų klasifikavimas neatitinka reikalavimų	16
3. IT organizacinė struktūra neužtikrina efektyvaus informacinių išteklių valdymo	17
3.1. Aukščiausiu ministerijos valdymo lygmeniu nepakankamai dėmesio skiriama IT valdymo koordinavimui ir kontrolei	17
3.2. Neužtikrinamas ministerijai priskirtų valstybės informacinių išteklių valdytojo funkcijų įgyvendinimas	18
3.3. Daugeliui ministerijos valdomų IS ir registrų nėra paskirti duomenų valdymo įgaliotiniai	19
4. Nustatyta ne visų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarka	20
5. Informatikos ir ryšių departamento teikiamų IT paslaugų lygiai neapibrėžti	22
6. Ministerija nepakankamai pasirengusi užtikrinti IS saugą ir veiklos tęstinumą	23
6.1. Skiriama nepakankamai dėmesio organizuojant, koordinuojant ir kontroliuojant sistemų saugos užtikrinimo procesą	24
6.2. Atliekami ne visų IS rizikos ir saugos atitikties vertinimai, o atliktų vertinimų metu nustatyti trūkumai šalinami vangiai	25
6.3. IS ir registrų saugos politikos dokumentai laiku neatnaujinami	26
7. Vidaus kontrolės stebėsenos ir vertinimo procesas apibrėžtas, bet neįgyvendinamas	27
PRIEDAI	29

SANTRUMPOS IR SĄVOKOS

COBIT – ISACA¹ sukurta informacinių technologijų valdymo ir vadovavimo metodika

Informatikos ir ryšių departamentas – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

IS – informacinė sistema

IT – informacinės technologijos

Informaciniai ištekliai – valstybės IS ir registrai

N.SIS – Lietuvos nacionalinė Šengeno informacinė sistema

N.VIS – Lietuvos nacionalinė vizų informacinė sistema

PASIS – Viešųjų ir administracinių paslaugų stebėsenos ir analizės informacinė sistema

SVIS – Sertifikatų valdymo informacinė sistema

VRIS – Vidaus reikalų informacinė sistema

VRIS CDB – VRIS centrinis duomenų bankas

Vidaus reikalų ministerija – Lietuvos Respublikos vidaus reikalų ministerija

Kitos šioje ataskaitoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

¹ ISACA – Information Systems Audit and Control Association. Prieiga per internetą: <http://www.isaca.org/about-isaca/Pages/default.aspx> [žiūrėta 2015-06-10].

SANTRAUKA

Vidaus reikalų ministerijos veiklos tikslai² yra formuoti valstybės politiką, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą viešojo saugumo³, viešojo administravimo ir informacinių technologijų taikymo viešojo administravimo⁴, valstybės informacinių išteklių saugos srityje⁵, migracijos ir kūno kultūros bei sporto srityse.

Daugelyje Vidaus reikalų ministerijos veiklos sričių naudojami visai valstybei didelę svarbą turintys informaciniai išteklių: valstybės ir žinybiniai registrai, valstybės informacinės sistemos. Kadangi ministerija įgyvendino ne visas 2007 ir 2010⁶ m. valstybinių auditų rekomendacijas, analizavome, ar esama teigiamų IT valdymo pokyčių. Jų poveikis svarbus ne tik dėl to, kad ministerija valdo 16 informacinių išteklių, kurie užtikrina duomenų pasiekiamumą gyventojams, operatyvią tarnybų veiklą ir Šengeno bendradarbiavimo įrankių veikimą. Ministerijos IT valdymo kokybė turės įtakos ir kitų valstybės institucijų veiklai: nuo 2016-01-05 įgyvendinant valstybės informacinių išteklių konsolidavimo darbų sąrašą⁷ Informatikos ir ryšių departamentas prie Vidaus reikalų ministerijos paskirtas vienu iš keturių valstybės IT paslaugų teikėju⁸.

Audito tikslas – įvertinti Vidaus reikalų ministerijos informacinių išteklių valdymą. Vertinome, kaip ministerija užtikrina jų tvarkymo planavimą ir organizavimą, stebėseną, vertinimą ir koordinavimą, įvertinome ministerijos IT valdymo procesų brandą. Analizavome ministerijos valdomus informacinius išteklius (penkis valstybės registrus, aštuonias valstybės IS ir tris žinybinius registrus), kuriuos naudoja ir tvarko ne tik ministerija, bet ir jos valdymo sričiai priskirtos institucijos ir kitos įstaigos.

Audituojamas laikotarpis – 2013–2016 m. I ketvirtis. Duomenų analizei atlikti buvo naudojami kitų laikotarpių duomenys. Auditą atlikome Vidaus reikalų ministerijoje. Informaciją taip pat rinkome Informatikos ir ryšių departamente ir VĮ „Regitra“, kurie atsakingi už ministerijos valdomų informacinių išteklių administravimą, duomenų saugos užtikrinimą ir plėtrą.

Audito metu nustatėme, kad aukščiausiu ministerijos vadovybės lygmeniu nepakankamai dėmesio skiriama IT valdymo koordinavimui ir kontrolei, todėl Vidaus reikalų ministerijos IT valdymo procesų branda per devynerius metus nepasikeitė ir apibrėžiama kaip pirminis (*Ad Hoc*) procesas. Tai reiškia, kad yra faktų, rodančių, kad ministerijos vadovybė supranta, jog yra problemų, kurias reikia spręsti, tačiau procesai nestandartizuoti (neapibrėžtas informacinės architektūros modelis, nenustatyti teikiamų IT paslaugų lygiai). Be to, nustatėme 24 teisės aktų reikalavimų nesilaikymo atvejus (3 priedas). Bendras požiūris į IT valdymą ministerijoje nesistemiškas (nerengiamas strateginis IT planas, tobulintina IT valdymo organizacinė struktūra, nepakankamas stebėsenos ir vertinimo procesas), o vietoj standartizuotų procesų paprastai taikomi *Ad Hoc* metodai, skirtingai kiekvienu individualiu atveju.

² Lietuvos Respublikos Vyriausybės 2001-03-14 nutarimu Nr. 291 (nauja redakcija nuo 2010-10-19) patvirtinti Lietuvos Respublikos vidaus reikalų ministerijos nuostatai, 8 p.

³ Viešosios tvarkos, vidaus tarnybos, priešgaisrinės bei civilinės saugos ir gelbėjimo darbų, valstybės sienos apsaugos, ginklų, šaudmenų, sprogmenų ir specialiųjų priemonių apyvartos, saugomo asmens statusą turinčių asmenų apsaugos.

⁴ Elektroninės valdžios, vietos savivaldos, regionų plėtros, valstybės tarnybos.

⁵ Tiek, kiek tai neapima kibernetinio saugumo.

⁶ 2007-11-10 valstybinio audito ataskaita Nr. IA-9000-2-4 „Vidaus reikalų ministerijos informacinių sistemų bendrosios kontrolės vertinimas“ ir 2010-12-31 valstybinio audito ataskaita Nr. VA-900-1-27 „Valstybės tarnautojų panaudojimas elektroninėje erdvėje“.

⁷ Lietuvos Respublikos Vyriausybės 2015-05-13 nutarimas Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“, 11 p.

⁸ Lietuvos Respublikos vidaus reikalų ministro 2016-01-05 įsakymas Nr. 1V-4 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos paskyrimo valstybės informacinių technologijų paslaugų teikėju“, 3.2.3 p.

Atsižvelgiant į Vidaus reikalų ministerijos valdomų informacinių išteklių svarbą ir į tai, kad Informatikos ir ryšių departamentas yra paskirtas vienu iš keturių valstybės IT paslaugų teikėju, svarbu laiku pašalinti nustatytus IT valdymo trūkumus. Aukštesnis IT valdymo procesų brandos lygis gali būti pasiektas tik įgyvendinus Lietuvos Respublikos teisės aktų reikalavimus ir mūsų rekomendacijas.

Įvertinę surinktus įrodymus, teikiame valstybinio audito išvadas ir rekomendacijas.

IŠVADOS

1. Vidaus reikalų ministerijos IT srities strateginis planavimas turi trūkumų, kurie didina riziką, kad finansiniai, technologiniai ir žmogiškieji ištekliai nebus tinkamai paskirstyti, o ypatingos svarbos informacinių išteklių plėtra nebus atlikta laiku, nes:
 - ministerija valdo aštuonis ypatingos svarbos valstybės informacinius išteklius, o vieną – Informatikos ir ryšių departamentas, tačiau nesilaiko Valstybės informacinių išteklių valdymo įstatymo: neturi IT plėtros planų ir niekas neįpareigotas juos parengti (1.1 poskyris, 11 psl.);
 - į metinius veiklos planus ne visuomet įtraukiami IT plėtros pasirengiamieji darbai: investicinio projekto, techninių ir funkcinių reikalavimų rengimas ir jų derinimas (1.2 poskyris, 11 psl.).
2. Esama ministerijos valdomų informacinių išteklių dokumentacija neparodo aktualios kompiuterizuotų funkcijų ir apdorojamos informacijos apimties; nenustačius ministerijos ir jai pavaldžių įstaigų valdomos informacijos svarbos ir jautrumo, gali būti neužtikrinami informacijos saugos reikalavimai tokią informaciją viešinant, perduodant ir atskleidžiant:
 - ne visi ministerijos valdomi registrai ir IS turi atnaujintus nuostatus (aktualūs 12 iš 16), parengtas ir patvirtintas technines specifikacijas (neturi 4 iš 16) (2.2 ir 2.3 poskyriai, atitinkamai 14 ir 15 psl.);
 - ministerija neturi išsamaus naudojamų IS, registrų ir kitos programinės įrangos sąrašo ir bendro informacijos architektūros modelio, todėl lieka neaiški informacinių išteklių tarpusavio sąveika (2 skyrius, 12 psl.).
3. Ministerijos IT valdymo organizacinė struktūra tobulintina, nes:
 - dėl IT veiklos organizavimo trūkumų, už informacinių išteklių valdymą atsakingų darbuotojų kaitos ir žmogiškųjų išteklių stokos neužtikrinama, kad būtų vykdomos Vidaus reikalų ministerijos valdomų informacinių išteklių valdytojo funkcijos, nes jų vykdymas neatitinka teisės aktų reikalavimų (3.2 poskyris, 18 psl.);
 - nėra mechanizmo, kurį taikant būtų galima kartu su vadovybe spręsti IT valdymo klausimus, kad pagrindinės veiklos poreikiai būtų siejami su IT teikiamomis galimybėmis (3.1 poskyris, 17 psl.);
 - neatskirtos politikos formavimo ir įgyvendinimo funkcijos – tas pats ministerijos padalinys atlieka ministerijos informacinių išteklių valdytojo funkcijas ir formuoja elektroninės valdžios bei elektroninės saugos politiką (koordinuoja, planuoja projektus ir vertina jų tarpusavio suderinamumą) (3.2 poskyris, 18 psl.);
 - nepaskirti 13 (iš 16) ministerijos valdomų informacinių išteklių duomenų valdymo įgaliotiniai, kurie turėtų prižiūrėti, kaip šie ištekliai kuriami, tvarkomi ir panaudojamos investicijos (3.3 poskyris, 19 psl.).
4. Nustatyta ne visų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarka (3 iš 16 nenustatyta, 7 – neatnaujinta). Praktikoje taikomas IT pokyčių valdymo procesas dažnai (14 iš

- 16 atvejų) vyksta nesilaikant esamų tvarkų nuostatų, nes neregistruojami ir neskirstomi į kategorijas visi veiklos padalinių inicijuojami pokyčiai, nenustatomi prioritetai. Todėl nėra galimybės stebėti pokyčio būseną įvairiais pokyčių valdymo etapais, nenustatytas pokyčio poveikio vertinimo procesas, o tai didina neigiamo pokyčių poveikio IS ar registro stabilumui ir vientisumui riziką (4 skyrius, 20 psl.).
5. Konsolidavus valstybės informacinius išteklius ir Informatikos ir ryšių departamentui tapus vienu iš keturių valstybės IT paslaugų teikėju, departamentas šias paslaugas teiks pagal IT paslaugų teikimo susitarimus. Kokybiškas IT paslaugų tiekimas reikiamu laiku daugeliui valstybinių įstaigų bus užtikrintas tik patvirtinus departamento teikiamų IT paslaugų katalogą ir stebint šių paslaugų teikimo lygį (5 skyrius, 22 psl.).
 6. Ministerijos kontrolės priemonės, padedančios užtikrinti el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą, yra nepakankamos, nes:
 - ministerijoje sprendžiant IS saugos klausimus nedalyvauja svarbiausių veiklos sričių: pagrindinių ministerijos veiklos sričių, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito, atstovai (6.1 poskyris, 24 psl.);
 - 2 (iš 16) ministerijos valdomiems informaciniams ištekliams nepaskirti saugos įgaliojimai, todėl neįvertinta šių išteklių rizika ir saugos atitiktis norminių teisės aktų reikalavimams (6.2 poskyris, 25 psl.);
 - nekontroliuojama, kaip įgyvendinamos IS rizikos valdymo priemonės ir šalinami saugos atitikties reikalavimams įvertinimų metu nustatyti trūkumai (6.2 poskyris, 25 psl.);
 - neparengti 3 (iš 16) ministerijos valdomų informacinių išteklių saugos politikos įgyvendinimą reglamentuojantys teisės aktai (6.3 poskyris, 26 psl.);
 - metus vėluojama įgyvendinti pasikeitusius el. saugos reikalavimus: 11 (iš 16) ministerijos valdomų informacinių išteklių saugos politiką apibrėžiantys ir jos įgyvendinimą reglamentuojantys teisės aktai iki 2016-07-01 nebuvo atnaujinti (6.3 poskyris, 26 psl.).
 7. Ypatingos svarbos informacinių išteklių auditas, kurį privalu atlikti pagal Valstybės informacinių išteklių valdymo įstatymą⁹, per 2013–2016 m. I pusmetį nebuvo atliktas, o ministerijos Vidaus audito skyrius neatliko nė vieno audito, kurio objektas būtų informacinės sistemos, jų saugos, bendrosios kontrolės ar kito IS (IT) aspekto vertinimas. Todėl ministerijos vadovybei gali trūkti informacijos apie IT procesų efektyvumą, atitiktį veiklos reikalavimams, nenustatomi IT kontrolės trūkumai ir spragos, nesilaikoma teisės aktų reikalavimų (3 priedas) (7 skyrius, 27 psl.).

REKOMENDACIJOS

1. Siekiant nuosekliai ir kryptingai tobulinti IS ir registrus ir atsižvelgiant į visos organizacijos veiklos poreikius, parengti ir patvirtinti Vidaus reikalų ministerijos valdymo srities strateginį IT planą (1 išvada).
2. Sudaryti ir nuolat atnaujinti visų ministerijoje naudojamų IS, registrų ir kitos programinės įrangos sąrašą (2 išvada).
3. Sudaryti informacijos architektūros modelį, apimantį ministerijos valdomos informacijos, IS (registrų) duomenų bei technologinę architektūrą, nurodant visus komponentus (taikomas technologijas, duomenis, duomenų šrautus tarp išorinių ir vidinių IS) (2 išvada).

⁹ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 14 str. 1 d.

4. Siekiant, kad nebūtų stabdomas saugos politiką įgyvendinančių dokumentų atnaujinimo procesas, atnaujinti N.SIS ir SVIS nuostatus. Priimti sprendimą dėl tolesnio VRIS kaip valstybės IS egzistavimo ir apibrėžti jos struktūrą, kuri būtų paprastesnė ir lankstesnė (2 ir 6 išvados).
5. Vadovaujantis subsidiarumo principu¹⁰, atskirti el. valdžios ir el. saugos politikos formavimo ir jos įgyvendinimo (t. y. IS valdytojo) funkcijas (3 išvada).
6. Skiriant ministerijos valdomų informacinių išteklių duomenų valdymo įgaliotinius, atsižvelgti į veiklos sritis, kuriose atitinkami išteklių yra dažniausiai naudojami (3 išvada).
7. Siekdama sistemingo pokyčių valdymo, peržiūrėti esamą IT pokyčių valdymo procesą ir nustatyti (patvirtinti) visų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarką. Joje turėtų būti išdėstytos IT pokyčių valdymo nuostatos, apimančios planavimą, suskirstymą į kategorijas, prioritetų nustatymą, avarines procedūras ir įtakos vertinimo procesus, be to, būtina užtikrinti šios tvarkos laikymosi (vykdymo) kontrolę (4 išvada).
8. Parengti ir patvirtinti Informatikos ir ryšių departamento teikiamų IT paslaugų katalogą ir nustatyti šių paslaugų teikimo lygį (5 išvada).
9. Sudaryti gerąją praktiką atitinkančią IS saugos klausimus sprendžiančią struktūrą, kurią sudarytų atstovai iš svarbiausių veiklos sričių: pagrindinių ministerijos veiklos sričių, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito (6 išvada).
10. Ne rečiau, kaip nustatyta teisės aktuose, stebėti ir vertinti informacinių sistemų ir registru vidaus kontrolės būklę (7 išvada).

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti 1 priede „Rekomendacijų įgyvendinimo planas“.

¹⁰ Lietuvos Respublikos viešojo administravimo įstatymas, 1999-06-17 Nr. VIII-1234, 4 str. 2 d.

IŽANGA

Audito metu analizavome ir vertinome visų Vidaus reikalų ministerijos valdomų informacinių išteklių ir jai pavaldžių įstaigų valdomų I kategorijos¹¹ informacinių išteklių valdymą (bendrąją kontrolę). Pagrindinis audito subjektas – Vidaus reikalų ministerija, kuri valdo 16 valstybės informacinių išteklių (4 priedas). Daug dėmesio skyrėme ne tik ministerijos IT valdymui, bet ir Informatikos ir ryšių departamento vykdomai veiklai. Jis yra 14 (iš 16) Vidaus reikalų ministerijos valdomų informacinių išteklių tvarkytojas ir vieno I kategorijos registro valdytojas. Departamentas atsako už šių informacinių išteklių duomenų saugą, diegia ir prižiūri techninę įrangą.

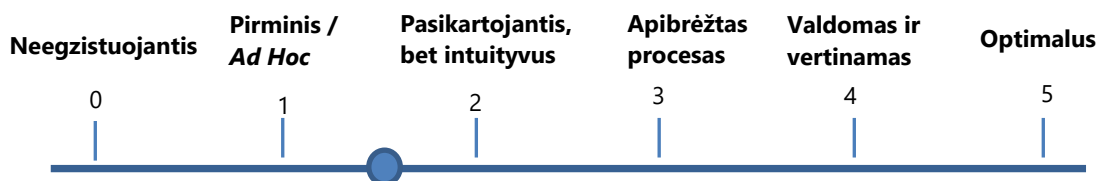
Vidaus reikalų ministerija įgyvendina projektus, finansuojamus valstybės biudžeto, Europos Sąjungos struktūrinių fondų ir kt. lėšomis. Per 2013–2015 m. informacinių sistemų ir registų plėtrai ir palaikymui laikotarpį panaudojo 12,2 mln. Eur.

Ministerijos informacinių išteklių valdymą vertinome pagal Valstybinio audito reikalavimus, Tarptautinės informacinių sistemų audito ir kontrolės asociacijos ISACA parengtą Informacinių technologijų valdymo metodiką COBIT¹² ir galiojančių Lietuvos Respublikos teisės aktų reikalavimus. Atlikę rizikos analizę pasirinkome vertinti 8 IT procesus:

- Strateginio IT plano apibrėžimas (PO1);
- Informacinės architektūros nustatymas (PO2);
- IT procesų, organizacinės struktūros ir ryšių apibrėžimas (PO4);
- Pokyčių valdymas (AI6);
- Paslaugų lygių apibrėžimas ir valdymas (DS1);
- Sistemų saugos užtikrinimas (DS5);
- Vidaus kontrolės stebėseną ir vertinimas (ME2);
- IT valdymo užtikrinimas (ME4).

IT valdymo procesų brandą vertinome remdamiesi COBIT pateikiamu brandos modeliu, kurio vertinimo skalė nuo 0 iki 5 atspindi bendruosius brandos vertinimo aspektus. Kiekviename skyriuje pagal šią skalę (1 pav.) pateikiama dabartinė ministerijos IT proceso būklė.

1 pav. IT proceso brandos vertinimo pavyzdys. Apskritimu žymėsime dabartinę IT proceso būklę



Šaltinis: Valstybės kontrolė

0 – neegzistuojantis. Visiškai nevyksta jokie atpažįstami procesai. Organizacija net nesupranta, kad reikia spręsti šį klausimą.

¹¹ Pirmai kategorijai priskiriami pagrindiniai valstybės registrai, kiti valstybės registrai (kadastrai) ir valstybės informacinės sistemos, kuriuose apdorojama ypatingos svarbos elektroninė informacija. Ypatingos svarbos valstybės informaciniai išteklius sudaro visai valstybei svarbi informacija, apdorojama valstybės informacinėse sistemose ir pagrindiniuose valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir pagrindiniai valstybės registrai.

¹² COBIT 4.1, 2011 m., Vilnius.

1 – pirminis (Ad Hoc). Yra faktų, rodančių, kad organizacija suprato, jog yra problemų, kurias reikia spręsti. Vis dėlto standartizuoti procesai nevyksta. Vietoj jų suformuoti *Ad Hoc* metodai kiekvienu individualiu atveju paprastai taikomi skirtingai. Bendras požiūris į valdymą nesistemiškas.

2 – pasikartojantis, bet intuityvus. Procesai tiek išplėtoti, kad skirtingi žmonės, atliekantys tą pačią užduotį, laikosi panašių procedūrų. Nevyksta formaliai patvirtinti standartinių procedūrų mokymai arba apie jas neinformuojama, atsakomybė paliekama individualiems darbuotojams. Didelis priklausomumas nuo individualių asmenų žinių, todėl tikėtinos klaidos.

3 – apibrėžtas procesas. Procedūros yra standartizuotos ir dokumentuotos, tai aiškinama per mokymus. Įpareigojama šių procesų laikytis. Nėra tikėtina, kad bus aptikta nuokrypių. Pačios procedūros nesudėtingos, jos tik įformina esamą praktiką.

4 – valdomas ir vertinamas. Vadovybė stebi ir vertina, kaip laikomasi procedūrų, ir imasi priemonių, kai atrodo, kad procesai vyksta neefektyviai. Procesai nuolat tobulinami, jie teikia gerą praktiką. Automatizavimas ir instrumentai taikomi tik ribotai ar fragmentiškai.

5 – optimalus. Dėl nuolatinio gerinimo ir brandos modeliavimo su kitomis organizacijomis procesai išstobulinti iki geros praktikos lygio. Kad darbo eiga būtų automatizuota, IT taikomos integruotu būdu, suteikiant priemones kokybei ir efektyvumui gerinti ir sudarant sąlygas organizacijai greitai prisitaikyti.

Atlikdami auditą darėme prielaidą, kad visi auditoriams pateikti dokumentai yra teisingi, išsamūs ir galutiniai, o jų kopijos atitinka originalus.

Informacija apie audito duomenų rinkimo ir vertinimo metodus pateikta 2 priede.

AUDITO REZULTATAI

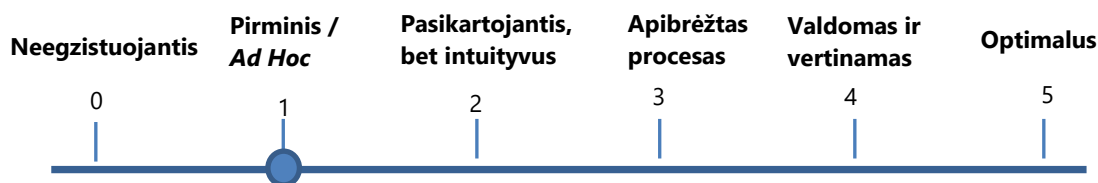
Vidaus reikalų ministerijos informacinių išteklių valdymas vertintas atsižvelgiant į teisės aktų reikalavimus ir COBIT siūlomą gerąją praktiką. Analizavome, kaip ministerijoje vykdomas IT strateginis planavimas (1 skyrius), ar pakankamai aiški informacijos architektūra (2 skyrius), kaip sudaryta ir veikia organizacinė struktūra (3 skyrius), kaip valdomi IT pokyčiai (4 skyrius), kaip apibrėžti IT paslaugų lygiai (5 skyrius), ar ministerijoje patvirtinta ir įgyvendinama informacijos saugos politika (6 skyrius), ar vykdoma IS vidaus kontrolės stebėseną (7 skyrius). Įvertinę informacinių išteklių valdymą, nustatėme, kad Vidaus reikalų ministerijoje vertintų IT valdymo procesų branda yra pirminė (*Ad Hoc*). Pastebėtina, kad 2007 m. atlikome analogišką vertinimą¹³, tačiau per devynerius metus IT valdymo branda ministerijoje nepasikeitė.

1. INFORMACINIŲ TECHNOLOGIJŲ PLANAVIMAS TURI TRŪKUMŲ

COBIT strateginio IT plano apibrėžimo procesas nurodo, kad strateginis IT planas reikalingas norint nustatyti kryptį ir valdyti IT išteklius derinant su veiklos strategija ir prioritetais¹⁴. Strateginis IT planas leidžia pagrindinėms suinteresuotosioms šalims geriau suprasti IT teikiamas galimybes ir jų naudojimo apribojimus, įvertinti esamą veiklą, nustatyti pajėgumų ir žmogiškųjų išteklių reikalavimus, išaiškinti investicijų poreikį. Tokiu būdu užtikrinamas visų veiklos grandžių darnus darbas, įgyvendinant valdymo sričiai keliamus uždavinius ir siekiant bendrų veiklos tikslų.

Vidaus reikalų ministerija ir jai pavaldžios įstaigos investuoja į IT vadovaudamosi ministerijos rengiamu strateginiu veiklos planu¹⁵. Ministerijos IT planavimo proceso būklę (žr. 2 pav.) įvertinome atsižvelgdami į nustatytus IT planavimo trūkumus, kurie įvardyti 1.1–1.2 poskyriuose, ir į dėl to kylančias rizikas.

2 pav. IT strateginio planavimo proceso (PO1)¹⁶ branda – *Ad Hoc*



Šaltinis: Valstybės kontrolė

Siekdama pagerinti IT strateginio planavimo procesą Vidaus reikalų ministerija turėtų parengti bendrą strateginį IT planą, kuris apimtų visas ministerijos sritis IS ir registrus. Parengus bendrą strateginį dokumentą, ministerijos vadovybei ir kitoms suinteresuotoms šalims būtų žinomi visų ministerijos valdomų informacinių išteklių tvarkymo prioritetai ir kryptys. Turint strateginį IT planą būtų lengviau suprasti IT teikiamas galimybes ir jų taikymo apribojimus, įvertinti esamą veiklą, nustatyti pajėgumų ir žmogiškųjų išteklių reikalavimus, pagrįsti investicijų į IT sritį poreikį.

¹³ 2007-11-10 valstybinio audito ataskaita Nr. IA-9000-2-4 „Vidaus reikalų ministerijos informacinių sistemų bendrosios kontrolės vertinimas“.

¹⁴ COBIT 4.1, 2011 m., Vilnius; PO1 procesas, 29 psl.

¹⁵ Strateginis veiklos planas – institucijos veiklos planavimo dokumentas, kuriame, atsižvelgiant į aplinkos analizę, suformuluota institucijos misija, strateginiai tikslai, aprašomos institucijos vykdomos programos ir nurodomos lėšos joms įgyvendinti.

¹⁶ COBIT 4.1, 2011 m., Vilnius; 32 psl.

1.1. Nerengiamas IT strateginis planas

Valstybės informacinių išteklių valdymo įstatymu nustatyta, kad institucijos, valdančios ypatingos svarbos valstybės informacinius išteklius, turi turėti IT plėtros planą ne ilgesniam kaip 3 metų laikotarpiui. Jame turi būti nustatyti IT priemonių, skirtų informacijai, duomenims, dokumentams ir (arba) jų kopijoms tvarkyti, kūrimo ir naudojimo tikslai, uždaviniai, nurodomos planuojamos kurti ar modernizuoti valstybės informacinės sistemos ir registrai, jų steigimo, modernizavimo prioritetai, planuojamos diegti elektroninės paslaugos, reikalingi finansiniai ir žmogiškieji išteklių, organizacinės ir teisinės priemonės, kvalifikacijos reikalavimai darbuotojams, darbuotojų mokymų poreikis, jų veiklos organizavimas ir kontrolė¹⁷.

Vidaus reikalų ministerija valdo aštuonis ypatingos svarbos (I kategorijos) valstybės informacinius išteklius, vieną – jai pavaldi įstaiga Informatikos ir ryšių departamentas. Ministerija valdo ir savo veikloje naudoja ne tik šiuos ypatingos svarbos, bet ir žemesnės svarbos informacinius išteklius (sąrašas pateiktas 4 priede) ir kitą taikomąją programinę įrangą. Ministerija 2013–2015 m. vykdė 21 IT plėtros projektą, kuriems panaudota 11,2 mln. eurų. Daugumą valdomų ypatingos svarbos valstybės informacinių išteklių (išskyrus VRIS) naudoja ministro valdymo sričiai priskirtos įstaigos, todėl šios srities IT strateginis planavimas tampa ypač svarbus. Išanalizavus ministerijos valdomų IS ir registrų plėtros planavimą nustatyta, kad bendro ar atskiriems informaciniams ištekliams patvirtinto, galiojančio ir įstatymo reikalavimus atitinkančio IT plėtros plano (planų) ir/ar gerosios praktikos rekomendacijas atitinkančio strateginio IT plano nėra.

Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos 2013 ir 2016¹⁸ m. priminė įstaigoms, valdančioms ypatingos svarbos informacinius išteklius, pareigą parengti IT plėtros planus. Vidaus reikalų ministerija atsakymo komitetui nepateikė, o Informatikos ir ryšių departamentas pateikė klaidinančią informaciją, kad nevaldo ypatingos svarbos informacinių išteklių (nuo 2012 m. departamentas yra JKNR¹⁹ valdytojas).

Vidaus reikalų ministerijai neparengus IT plėtros plano, kyla rizika, kad finansiniai, technologiniai ir žmogiškieji išteklių nebus tinkamai paskirstyti, o ypatingos svarbos informacinių išteklių steigimo (modernizavimo) darbai nebus atlikti laiku. Nenustačius kvalifikacijos reikalavimų darbuotojams, mokymų poreikio, kyla rizika, kad uždaviniams įgyvendinti reikės daugiau laiko ir nepakaks darbuotojų kompetencijos.

1.2. Į ministerijos metinius veiklos planus įtrauktos ne visos svarbiausios IT srityje vykdomos veiklos

Institucijos, valdančios valstybės informacinius išteklius, IT strateginio planavimo (plėtros) kryptis, tikslus, uždavinius ir kitą Valstybės informacinių išteklių valdymo įstatymo 9 straipsnio 1 dalyje nurodytą informaciją turėtų įtraukti į strateginius ir metinius veiklos planus²⁰.

Vidaus reikalų ministerija kasmet rengia trejų metų laikotarpio strateginius veiklos planus. Atlikę 2013–2015 m. ministerijos įgyvendinto 21 IT projekto analizę nustatėme, kad jie visi buvo įtraukti

¹⁷ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 9 str. 1 ir 2 d.

¹⁸ Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos raštai: 2013-11-08 Nr. S-1707 „Dėl informacinių technologijų planų derinimo“ ir 2016-03-10 Nr. S-267 „Dėl informacinių technologijų plėtros planų derinimo“.

¹⁹ Įtariamųjų, kaltinamųjų ir nuteistųjų registras.

²⁰ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 9 str. 3 d.

į ministerijos strateginius veiklos planus. Nustatėme, kad neretai pasirengiamieji darbai (pvz., investicinio projekto, techninių ir funkcinių reikalavimų rengimas ir jų derinimas), vykdomi iki IT projekto patvirtinimo pradžios, neįtraukiami į metinius veiklos planus.

Susiklosčius tokioms situacijoms gali nukentėti prioritetiniai darbai, o atliekant į planus neįtrauktus darbus gali būti sudėtinga įvertinti realius ministerijos ar jai pavaldžių įstaigų darbuotojų krūvius įgyvendinant IT projektus.

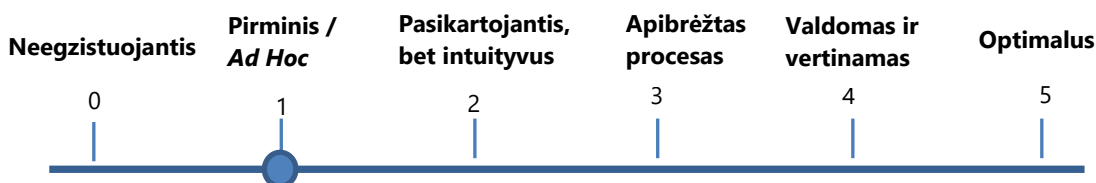
2. VIDAUS REIKALŲ MINISTERIJOS VALDYMO SRITIES INFORMACINĖ ARCHITEKTŪRA NEAPIBRĖŽTA

COBIT metodikoje pažymėta²¹, kad apibrėžtas informacinės architektūros modelis padeda visus informacinius išteklius sujungti į visumą ir užtikrina, kad vadovybei ir vartotojams bus teikiama patikima, nuosekli ir išsami informacija. Institucija, nustatydamą valdymo srities informacinę architektūrą, turėtų sudaryti duomenų žodyną, kuriame nustatomos duomenų techninės sąlygos (kitais tarimais – duomenų sintaksė), sudaryti duomenų klasifikavimo schemą ir nustatyti saugumo lygius. informacinė architektūra leidžia racionaliai panaudoti informacinius išteklius, juos kiek įmanoma lanksčiau derinti su vykdomos veiklos strategija. Taip stiprinamas atskaitingumas už duomenų vientisumą ir saugą, didinamas jų mainų tarp skirtingų IS efektyvumas ir kontrolė. Atsižvelgus į ministerijos valdomų valstybės informacinių išteklių įvairovę, jų svarbą (4 priedas) ir vykstantį konsolidavimo procesą²², nustatyti ministerijos valdomų IS ir registrų informacinę architektūrą ypač svarbu, kad būtų galima tinkamai juos valdyti, analizuoti ir modernizuoti.

Vidaus reikalų ministerija neturi išsamaus naudojamų IS ir registrų sąrašo, bendro savo valdomų informacinių sistemų ir registrų informacijos architektūros modelio, o informacijos srautai tarp ministerijos valdomų IS ir registrų nustatyti tik tam tikrų IS ir registrų nuostatuose ir techninėse specifikacijose. Be to, ne visi ministerijos valdomi registrai ir IS turi atnaujintus nuostatus (VRIS, N.VIS, N.SIS, SVIS.), parengtas ir patvirtintas technines specifikacijas (neturi VRIS, N.SIS, N.VIS, SVIS).

Ministerijai aiškiai neaprašius turimų elektroninių duomenų srautų, duomenų struktūros, lieka neiški informacinių išteklių tarpusavio sąveika, nesudaromos prielaidos IT ir veiklos naudotojams bendrai suprasti duomenis ir kurti tik suderinamus duomenų elementus bei nekaupti perteklinių duomenų. Dėl šių informacinės architektūros apibrėžties trūkumų (jie detalčiau aprašyti 2.1, 2.2, 2.3 ir 2.4 poskyriuose) proceso branda vertinama kaip pirminis (*Ad Hoc*) procesas (3 pav.).

3 pav. Informacinės architektūros nustatymo proceso (PO2)²³ branda – *Ad Hoc*



Šaltinis: Valstybės kontrolė

²¹ COBIT 4.1, 2011 m., Vilnius; PO2 procesas, 33 psl.

²² Lietuvos Respublikos Vyriausybės 2015-05-13 nutarimas Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“.

²³ COBIT 4.1, 2011 m., Vilnius; PO2 procesas, 36 psl.

Siekdama aukštesnės informacinės architektūros nustatymo proceso brandos, Vidaus reikalų ministerija turėtų ne tik įgyvendinti Lietuvos Respublikos teisės aktų reikalavimus, bet ir sudaryti informacijos architektūros modelį, apimančį ministerijos ir jai pavaldžių įstaigų valdomos informacijos, IS (registrų) duomenų bei technologinę architektūrą, nurodant visus komponentus (taikomas technologijas, duomenis, duomenų srautus tarp išorinių ir vidinių IS).

2.1. Ministerija neturi tikslių duomenų apie naudojamą programinę įrangą

Vidaus reikalų ministerija yra 16 informacinių išteklių valdytoja (4 priedas). Savo veikloje ji taip pat naudoja vidaus administravimo sistemas (Finansų apskaitos sistema, Archyvo tvarkymo posistemis, Vidaus reikalų ministerijos pensininkų apskaitos posistemis ir kt.), interneto tinklalapius, įslaptintos informacijos ryšių ir informacines sistemas²⁴, kitą sistemine²⁵ ir taikomąją programinę įrangą.

Ministerijos valdomos valstybės IS, registrai ir žinybiniai registrai įregistruoti Registrų ir valstybės informacinių sistemų registre, tačiau jos valdomų informacinių išteklių sąrašas turėtų būti papildytas įtraukiant šiuos išteklius: ADIS ir ADGIS. Dėl šių sistemų įteisinimo Vidaus reikalų ministerijai 2014 m. pateikta rekomendacija²⁶, jas įteisinti planuojama iki 2017-08-31. Kadangi rekomendacijos įgyvendinimas atidėtas, kas priima sprendimus dėl šių sistemų – neaišku.

Vidaus reikalų ministerija, įgyvendindama Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašą²⁷, pavedė²⁸ Informatikos ir ryšių departamentui iki 2016-06-30 sudaryti Vidaus reikalų ministerijos srities programinės įrangos sąrašus. Departamentas sąrašą parengė, tačiau jis apima tik Vidaus reikalų ministerijos srities įstaigų naudojamą sistemine programinę įrangą.

Ministerijos atstovai informavo²⁹, kad VRIS taikomoji programinė įrangą aprašoma VRIS CDB naudotojų administravimo posistemėje, kurioje šiems naudotojams priskiriamos teisės į tam tikrų veikloje naudojamų IS ir registrų naudojimą, todėl, jų manymu, netikslinga rengti atskirą registrų ir IS sąrašą ir jį tvirtinti. Reikėtų atsižvelgti į tai, kad sąrašas nuolat kinta, o VRIS CDB naudotojų administravimo posistemė užtikrina nuolatinį informacijos apie naudojamą taikomąją programinę įrangą atnaujinimą. Prireikus vadovybė ir kiti darbuotojai gali gauti aktualų IS ir registrų sąrašą.

Išanalizavę pateiktą programinės įrangos sąrašą nustatėme, kad jis nėra išsamus (1 pavyzdys).

1 pavyzdys

Ministerijos pateiktame sąrašė iš VRIS CDB naudotojų administravimo posistemės neįtraukti šie ištekliai: ARSIS, SVIS, NETAIS, Vidaus reikalų pareigūnų registras, ARSIS – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams

²⁴ Įslaptintos informacijos ryšių ir informacinė sistema – iš vieno ar daugiau kompiuterių, išorinių įrenginių ir programinės įrangos sudaryta ir informacinių technologijų pagrindu veikianti infrastruktūra įslaptintai informacijai apdoroti ir elektroninių ryšių tinklai, kuriais perduodama įslaptinta informacija (išskyrus viešuosius ryšių tinklus).

²⁵ Sistemine programinė įrangą atsakinga už techninės įrangos komponentų kontrolę, integravimą ir valdymą, kad taikomoji programinė įrangą galėtų naudoti šią įrangą nežinodama žemo lygio detalių. Galima išskirti kelias sisteminės įrangos kategorijas: operacinės sistemos, tvarkyklės, vartotojų identifikavimo sistemos.

²⁶ 2015-03-27 valstybinio audito ataskaita Nr. VA-P-90-2-6 „Biometrinių asmens dokumentų gamyba“.

²⁷ Lietuvos Respublikos Vyriausybės 2015-05-13 nutarimas Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“, 11 p.

²⁸ Lietuvos Respublikos vidaus reikalų ministro 2016-01-05 įsakymas Nr. 1V-4 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos paskyrimo valstybės informacinių technologijų paslaugų teikėju“, 3.2.3 p.

²⁹ Lietuvos Respublikos vidaus reikalų ministerijos 2016-09-14 raštas „Dėl valstybinio audito ataskaitos „Vidaus reikalų ministerijos informacinių išteklių valdymo“ audito ataskaitos derinimo“.

stebėsenos sistema, Lietuvos Respublikos kelių transporto priemonių registras, Lietuvos Respublikos kelių transporto priemonių vairuotojų registras.

Taigi, nei departamentas, nei ministerija išsamaus visų savo veikloje naudojamų ir (ar) tvarkomų IS ir registrų sąrašo iki 2016 m. liepos mėn. nebuvo parengę. Nesant aktualaus naudojamų IS ir registrų sąrašo, tikėtina, kad ministerijos vadovybė ir kiti darbuotojai, atsakingi už duomenų saugą, administravimą ir IT valdymą, nežino, kokias IS naudoja (išskyrus įregistruotas Registrų ir valstybės informacinių sistemų registre).

2.2. Ne visų ministerijos valdomų informacinių išteklių nuostatai atnaujinti, parengtos ne visos specifikacijos

Lietuvos Respublikos teisės aktai nustato šiuos elektroninės informacijos srautų valdymo reikalavimus:

- IS nuostatuose turi būti aptarta IS organizacinė ir informacinė struktūra³⁰;
- išsamūs vidiniai ir išoriniai informacijos srautai turi būti nustatomi IS specifikacijose³¹.

Visos ministerijos valdomos IS (išskyrus ADGIS ir ADIS, kurios nėra įteisintos ir kurių valdytojas nepaskirtas) ir registrai turi patvirtintus nuostatus, tačiau nustatytas atvejis, kai nuostatai parengti ir patvirtinti sukūrus IS. Pastebėta tendencija, kad, IS ir registrų naudojimo laikotarpiu įvykus esminių pokyčių, nuostatai ne visada atnaujinami. Dar blogesnė situacija rengiant specifikacijas, nes 4 (iš 16) ministerijos valdomos IS yra sukurtos ir eksploatuojamos neturint patvirtintų specifikacijų (2 pav. ir 3, 4 priedai). 3 (iš 16) informaciniai išteklių neturi priėmimo ir tinkamumo eksploatuoti aktų, t. y. neįteisinti (3 priedas).

2 pavyzdys

N.SIS, N.VIS, SVIS buvo modernizuotos 2013–2015 m., tačiau jų nuostatai neatnaujinti.

Ministerija daugiau kaip 14 m. naudoja ir atnaujina VRIS, tačiau nėra parengusi šios IS specifikacijos, neatnaujina nuostatų (neįgyvendintos prieš šešerius metus teiktos³² rekomendacijos).

Eksploatuojamos N.SIS (nuo 2007 m), N.VIS (nuo 2009 m.), SVIS (nuo 2011 m.) neturi patvirtintų specifikacijų ir tinkamumo eksploatuoti aktų (neįteisintos).

PASIS nuostatai patvirtinti 2016-04-08, nors šios IS kūrimo procesas prasidėjo 2013 m., o eksploatuoti ji pradėta 2014 m. pirmąjį pusmetį.

Nesant atnaujintų IS nuostatų, stabdomi kiti procesai, eikvojami Informatikos ir ryšių departamento išteklių. Išsamiau apie tai rašome 1.6.1 skirsnyje. Be to, kuriant, modernizuojant IS (registrus), neparengus ir nustatyta tvarka nepatvirtinus techninių specifikacijų, sukurtų (modernizuotų) IS (registrų) funkcijos gali neatitikti veiklos poreikių, o esant darbuotojų kaitai gali būti sunku užtikrinti IS (registrų) vientisumą ir suderinamumą bei funkcionavimo tęstinumą.

³⁰ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 30 str.; Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr.180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, 15 p.

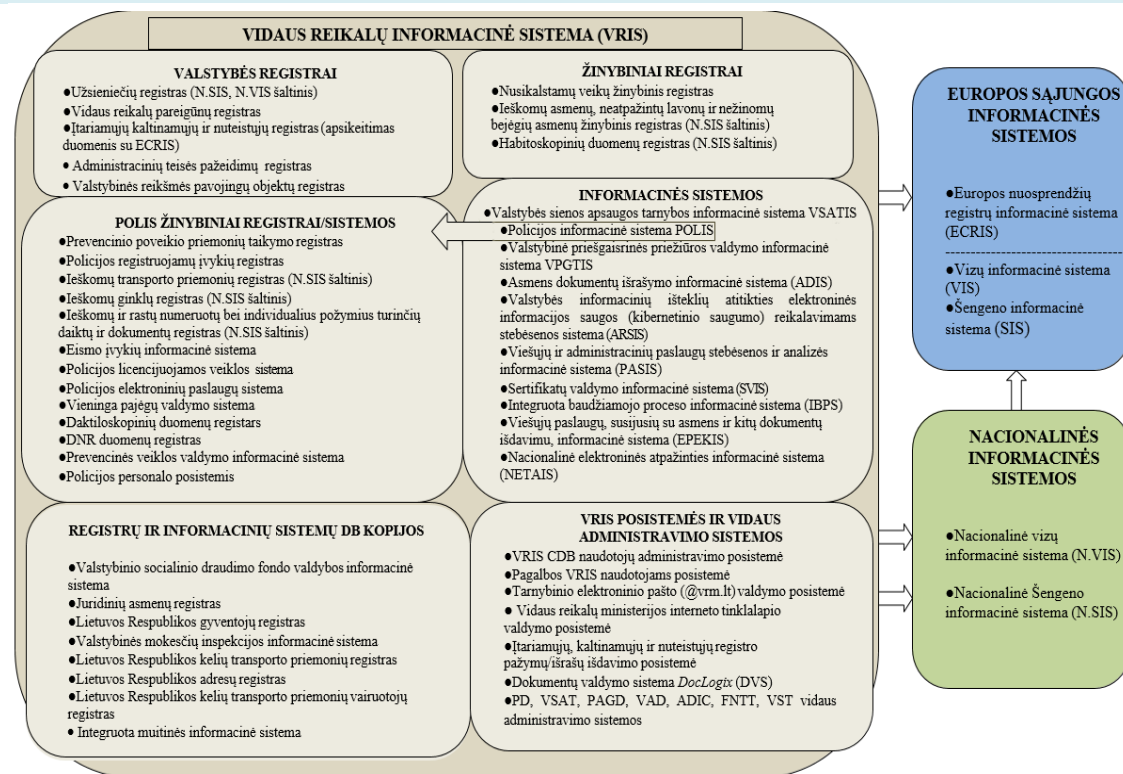
³¹ Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29 patvirtinti Valstybės informacinės sistemos techninio aprašymo (specifikacijos) rengimo reikalavimai, 11.2–11.6 p.

³² 2010-12-31 valstybinio audito ataskaita Nr. VA-P-900-1-27 „Valstybės tarnautojų pažymėjimų panaudojimas elektroninėje erdvėje“.

2.3. VRIS architektūra sudėtinga ir nelanksti

Audito metu detaliau analizavome VRIS. Jos architektūra yra sudėtinga, nes ji susideda ne tik iš posistemų, bet ir kitų IS bei registrų, kaupiamos kitų IS ir registrų duomenų kopijos, vyksta įvairių IS ir registrų duomenų mainai (4 pav.).

4 pav. VRIS struktūros sudedamosios dalys ir ryšiai



Šaltinis: Informatikos ir ryšių departamentas

VRIS struktūra yra sudėtinga, tačiau tik vienas jos posistemis yra skirtas veiklos funkcijoms įgyvendinti. Kitos VRIS nuostatuose įvardytos sudedamosios dalys – Vidaus reikalų ministerijos ir jai pavaldžių įstaigų valdomos IS ir registrai – įsteigtos (turi atskirus nuostatus), veikia ir įteisintos kaip atskiri objektai.

Informacinės visuomenės plėtros komitetas analogišku atveju yra pateikęs išaiškinimą³³: jei registrai, informacinės sistemos ir posistemiai yra atskiri (savarankiški) objektai ir veikia pagal savo patvirtintus nuostatus, bet koks nurodymas sudedamosiomis IS dalimis yra netinkamas.

VRIS posistemiai³⁴ naudojami ministerijos ir jai pavaldžių įstaigų IS ir registrams administruoti ir valdyti. Tokiu būdu efektyviau naudojami ištekliai, nes atskiroms IS ar registrams nereikia kurti posistemų minėtoms funkcijoms atlikti. Kita vertus, tokios VRIS architektūros didžiausias trūkumas – nelankstumas (tiek iš organizacinės, tiek ir iš technologinės pusės).

Taigi, siekiant, kad VRIS struktūra būtų paprastesnė ir lankstesnė, tikslinga, atnaujinant jos nuostatus, neįtraukti kitų Vidaus reikalų ministerijos ir jai pavaldžių įstaigų valdomų IS ir registrų, veikiančių pagal savo patvirtintus nuostatus, kaip sudedamųjų dalių.

³³ 2011-12-30 raštas Nr. (13)S-1425 „Dėl Policijos informacinės sistemos nuostatų projekto derinimo“.

³⁴ VRIS CDB naudotojų administravimo posistemis, Pagalbos VRIS naudotojams posistemis, Tarybinio elektroninio pašto (@vrm.lt) valdymo posistemis, Vidaus reikalų ministerijos tinklalapio valdymo posistemis.

2.4. Duomenų klasifikavimas neatitinka reikalavimų

COBIT³⁵ rekomenduoja nustatyti visoje organizacijoje taikomą informacijos klasifikavimo sistemą, grįstą organizacijos duomenų svarba ir diskretiškumu (pvz.: vieša, slapta, visiškai slapta). Šioje sistemoje reikia aprašyti duomenų valdytojus, apibrėžti tinkamus saugos lygius ir apsaugos kontrolės priemones, trumpai aprašyti duomenų išsaugojimo ir naikinimo reikalavimus, svarbą ir diskretiškumą.

Teisės aktai nustato šiuos elektroninės informacijos srautų valdymo reikalavimus:

- Elektroninė informacija turi būti klasifikuojama, jos svarba nustatoma pagal konfidencialumo, vientisumo ir (ar) prieinamumo praradimo neigiamą įtaką valstybės, valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos, steigiančios, kuriančios ir (arba) tvarkančios valstybės registrus, žinybinius registrus, valstybės informacines sistemas ir kitas informacines sistemas, veiklai ir elektroninės informacijos svarbą valstybei, kelioms institucijoms ar institucijai³⁶.
- IS ar registrų kategorija nustatoma pagal juose apdorojamos elektroninės informacijos svarbos kategoriją ir nurodoma IS (registro) duomenų saugos nuostatuose³⁷.

Vidaus reikalų ministerija, valdanti 16 valstybės IS ir registrų ir turinti metodiškai vadovauti jų tvarkytojams bei koordinuoti šių registrų ir IS funkcionavimą, neturi valdymo srities duomenų klasifikavimo sistemos, pagrįstos duomenų svarba ir diskretiškumu (pvz.: konfidenciali, tarnybinio naudojimo, neviešintina ir pan.). Dėl šių priežasčių ministerijoje nėra kontrolės priemonių, padedančių užtikrinti teisės aktais nustatytą el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą. Valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų valdytojai iki 2015-07-01 turėjo peržiūrėti ir patobulinti savo valdomų registrų ir IS saugos dokumentus³⁸. Tačiau 12 (iš 16) Vidaus reikalų ministerijos valdomiems IS ir registrams naujos redakcijos saugos dokumentai yra nebaigti rengti ir (arba) nepatvirtinti (1, 3 priedai). be to, nustatėme, kad 2 (iš 16) ministerijos valdomiems informaciniams ištekliams yra suteikta koreguotina kategorija (3 pav.), o NETAIS nepriskirta jokiai kategorijai.

3 pavyzdys

IAŽR ir NVŽR priskirti I kategorijai. Šiuose registruose netvarkoma ypatingos svarbos informacija³⁹, todėl jiems turėtų būti nustatomos žemesnės kategorijos. Diegiant I kategorijos registro duomenų saugumo lygį, reikia taikyti ir palaikyti daugiau organizacinių ir techninių priemonių nei žemesnio lygio kategorijai. Pasirinkus žemesnę kategoriją, būtų užtikrinama pakankama duomenų sauga, taupomos lėšos ir kiti ištekliai.

Netinkamas IS apdorojamos informacijos svarbos nustatymas gali lemti tai, kad bus netinkamai nustatytas IS tvarkomos elektroninės informacijos apsaugos poreikis, prioritetai ir lygis, nebus parinktos tinkamos techninės saugos priemonės⁴⁰.

³⁵ COBIT 4.1, 2011 m., Vilnius; PO2 procesas, 33 psl.

³⁶ Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 (galiojo nuo 2013-08-08 iki 2016-08-19) patvirtintas Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, 3, 4, 4.1–4.4 p.; Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (patvirtinta Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716, 2016-08-11 nutarimo Nr. 826 redakcija galiojanti nuo 2016 08 19), 4, 6, 6.1–6.4 p.

³⁷ Ten pat, 3–4, 4.1–4.4, 5, 5.1–5.4 ir 6–7 p.

³⁸ Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas Nr. 716 (akto redakcija galiojanti nuo 2013-08-08 iki 2016-08-18), 2 p.

³⁹ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 3 str.

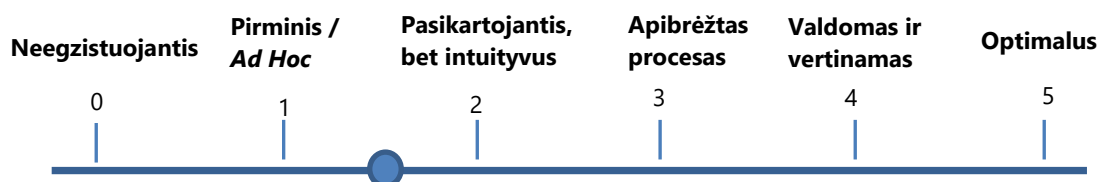
⁴⁰ Lietuvos Respublikos vidaus reikalų ministro 2013-10-04 įsakymu Nr. 1V-832 (galioja nuo 2013-10-11) patvirtinti Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, 9 p.

3. IT ORGANIZACINĖ STRUKTŪRA NEUŽTIKRINA EFEKTYVAUS INFORMACINIŲ IŠTEKLIŲ VALDYMO

Vadovaudamasis IT valdymo gerąją praktiką, taikoma organizacijos ir IT veiklai suderinti, COBIT rekomenduoja⁴¹ sudaryti tokią organizacinę struktūrą, kuri užtikrintų tinkamą požiūrį į IT valdymą kaip sudedamąją organizacijos valdymo dalį ir turėtų įgaliojimus ir kompetenciją priimti sprendimus dėl visų valdymo srities veiklos IT poreikių. Siekiant šio tikslo, gali būti sukurtas IT strategijos komitetas, kurio paskirtis – konsultuoti strateginės krypties pasirinkimo ir svarbiausių IT investicijų klausimais, ir IT valdymo komitetas, kuris, atsižvelgdamas į strateginę kryptį, stebėtų, kaip vykdomi IT projektai. Nustatant IT procesus, organizacinę struktūrą ir tarpusavio ryšius, ypač daug dėmesio turi būti skiriama veiklos kontrolei, kokybės užtikrinimui, rizikos valdymui, informacijos saugai, duomenų ir sistemų valdymui ir funkcijų atskyrimui.

Atsižvelgiant į nustatytus IT procesų, organizacinės struktūros trūkumus (žr. 3.1, 3.2 ir 3.3 poskyrius) ir dėl to kylančias rizikas, IT procesų, organizacinės struktūros ir ryšių apibrėžties proceso branda vertinama kaip pirminis (*Ad Hoc*) procesas (5 pav.).

5 pav. IT procesų, organizacinės struktūros ir ryšių apibrėžties proceso (PO4)⁴² branda – *Ad Hoc*



Šaltinis: Valstybės kontrolė

Kad IS ir registrų valdytojo funkcijos būtų vykdomos nuosekliai ir sistemiškai, turi būti skiriama daugiau dėmesio ir darbo laiko išteklių.

3.1. Aukščiausiu ministerijos valdymo lygmeniu nepakankamai dėmesio skiriama IT valdymo koordinavimui ir kontrolei

COBIT rekomenduoja⁴³ įkurti IT valdymo komitetą (ar jo atitikmenį), susidedantį iš vykdomųjų, veiklos ir IT vadovų, kuris:

- pagal organizacijos veiklos strategiją ir prioritetus nustatytų IT palaikomų investicijų programų prioritetus;
- stebėtų projektų vykdymo būklę ir spręstų išteklių neatitikties problemas;
- stebėtų paslaugų lygius ir jų gerėjimą.

Vidaus reikalų ministerijoje veikia strateginio planavimo darbo grupė, kurią sudaro ministerijos padalinių vadovai, vadovybės ir vidaus audito atstovai. Ši darbo grupė yra lėšų paskirstymo (perskirstymo) struktūrinis vienetas. Grupėje aptariami ir IT (IS) kūrimo bei finansavimo klausimai, tačiau

⁴¹ COBIT 4.1, 2011 m., Vilnius; PO4 procesas, 41psl.

⁴² Ten pat, PO4 procesas, 46 psl.

⁴³ Ten pat, PO4.3 procesas, 42 psl.

joje neaptariai ilgalaikiai IT plėtros planai, siekiant įvertinti IT (IS) plėtros naudą, planuojamos kurti ar modernizuoti valstybės IS ir registrai, jų steigimo ir (ar) modernizavimo prioritetai.

Ministerijoje 2009 m. sudarytas⁴⁴ Informacinės visuomenės plėtros vidaus reikalų sistemoje koordinavimo komitetas, tačiau 2013–2016 m. I pusmetį nebuvo organizuotas nė vienas posėdis, taigi jam priskirtos informacinės visuomenės plėtros vidaus reikalų sistemoje koordinavimo funkcijos nebuvo atliekamos.

Sudaromos IT projektų valdymo ir (ar) plėtros koordinavimo grupės, projektų priežiūros komitetai ir atliktų darbų vertinimo komisijos, kuriems pavedama organizuoti ir koordinuoti IS tobulinimo darbus, vertinti jų atitiktį funkciniais reikalavimams, projektų tarpinius ir galutinius rezultatus, priimti sprendimus dėl rezultatų priėmimo.

Be to, 2016 m. vidaus reikalų ministro įsakymu⁴⁵ inicijuotas gerąją praktiką atitinkančios IT veiklos valdymo struktūros sukūrimas – Viešojo valdymo politikos departamentui pavesta iki 2016-02-29 pateikti ministrui įsakymo projektą. Pagal jį būtų sudaroma Vidaus reikalų ministerijos srities įstaigų informacinių išteklių valdymo taryba, kurios sudėtyje būtų ministerijos, jos srities įstaigų ir Informatikos ir ryšių departamento atstovai. Jos pagrindinės funkcijos būtų IT plėtros ir palaikymo strateginių kryptų nustatymas, Vidaus reikalų ministerijos srities įstaigų IT projektų tvirtinimas, strateginių klausimų, susijusių su IT paslaugų teikimu, koordinavimas, IT paslaugų teikimo kokybės valdymas. Iki 2016-07-01 minėta taryba nesukurta.

Taigi IT veiklos valdymo struktūros, į kurią įeity svarbiausių Vidaus reikalų ministerijos veiklos procesų valdytojai, IT ir vadovybės atstovai, nėra. Tai rodo, kad IT valdymo koordinavimui ir kontrolei skiriama nepakankamai dėmesio aukščiausiu valdymo lygmeniu.

Pagrindinius IT strateginius ir valdymo uždavinius Vidaus reikalų ministerijoje galėtų spręsti sudaryta organizacinė struktūra, kuriai turėtų būti priskirtos krypties nustatymo, strateginio planavimo, rizikos kontrolės ir ministerijos koordinuojamų IT investicinių programų poveikio vertinimo funkcijos ir užtikrintas reikiamas visų lygių (vadovybės, visų ministro valdymo sričių veiklos ir IT) atstovavimas ir veiklų koordinavimas.

3.2. Neužtikrinamas ministerijai priskirtų valstybės informacinių išteklių valdytojo funkcijų įgyvendinimas

Valstybės informacinių išteklių valdymo įstatyme nustatyta, kad: IS ar registro valdytojas metodiškai vadovauja registro ar IS tvarkytojui ir koordinuoja jų funkcionavimą; privalo koordinuoti registro (IS) tvarkytojo ir priežiūros paslaugos teikėjo darbą; nustatyta tvarka atlikti jų veiklos priežiūrą; vykdyti duomenų ir informacijos saugos reikalavimų laikymosi kontrolę; planuoti metinį registro biudžetą, kontroliuoti jo vykdymą; nagrinėti registro (IS) tvarkytojo pasiūlymus dėl registro (IS) veiklos tobulinimo ir priimti sprendimus; užtikrinti, kad šie ištekliai būtų tvarkomi vadovaujantis teisės aktais; atlikti kitus teisės aktuose nustatytus veiksmus⁴⁶.

Už ministerijai priskirtų valstybės ir žinybinių registrų, valstybės informacinių sistemų ir kitų

⁴⁴ Lietuvos Respublikos vidaus reikalų ministro 2009-05-21 įsakymas Nr. 1V-213 „Dėl Informacinės visuomenės plėtros vidaus reikalų sistemoje koordinavimo komiteto sudarymo ir informacinės visuomenės plėtros vidaus reikalų sistemoje prioritetų nustatymo“ (2009-05-28 įsakymo Nr. 1V-231, 2009-07-24 įsakymo Nr. 1V-408 ir 2009-11-26 įsakymo Nr. 1V-639 redakcijos).

⁴⁵ Lietuvos Respublikos vidaus reikalų ministro 2016-01-05 įsakymas Nr. 1V-4 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos paskyrimo valstybės informacinių technologijų paslaugų teikėju“, 3.5 p.

⁴⁶ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 23, 24 ir 34 str.

informacinių sistemų valdytojo funkcijų vykdymą nuo 2011-05-17 iki 2015-09-10 buvo atsakingas Vidaus reikalų ministerijos Elektroninės valdžios politikos skyrius (toliau – EVPS). Vidaus reikalų ministro 2015-06-30 įsakymu Nr. 1V-535 „Dėl Vidaus reikalų ministerijos administracijos padalinių ir pareigybių“ EVPS buvo panaikintas 2015-09-10, jo funkcijos perduotos ministerijos Viešojo valdymo politikos departamento Viešojo administravimo politikos skyriui.

Tiek EVPS, tiek Viešojo administravimo politikos skyrius ne tik atliko (atlieka) valdytojo funkcijas, bet ir formuoja elektroninės valdžios ir elektroninės saugos politiką, planuoja projektus, užtikrina jų tarpusavio suderinamumą ir koordinuoja įgyvendinimą. Tai reiškia, kad tas pats ministerijos padalinys formuoja politiką ir ją įgyvendina. Vadovaujantis subsidiarumo principu – reikalavimu, kad aukštesnėms institucijoms nebūtų priskiriamos funkcijos, kurias gali atlikti žemesniosios institucijos ar kiti asmenys⁴⁷, ministerijoje turėtų būti atskirtos politikos formavimo ir jos įgyvendinimo funkcijos.

Nuo 2010 m. ministerijoje vykdomi įvairūs jos veiklos sričių optimizavimo procesai, tačiau dėl IT veiklos organizavimo trūkumų, už informacinių išteklių valdymą atsakingų darbuotojų kaitos ir žmogiškųjų išteklių stokos (4 pavyzdys) neužtikrinama, kad būtų vykdomos ministerijos valdomų informacinių išteklių valdytojo funkcijos. Tai neatitinka teisės aktų reikalavimų (3 priedas).

4 pavyzdys

Ministerijos IS ir registrų valdytojo funkcijoms vykdyti tiek EVPS, tiek Viešojo administravimo skyriuje buvo ir yra skirta viena pareigybė. Iki 2014-03-16 jos niekas nėjo, todėl funkcijos buvo neatliekamos ar jas minimaliai atliko kiti darbuotojai. Nuo 2016 m. kovo mėn. ši pareigybė vėl neužimta.

Darbuotojui, atliekančiam Vidaus reikalų ministerijos IS ir registrų valdytojo funkcijas, pagal pareigybės aprašymą, be kita ko, yra nurodyta analizuoti ir teikti pastabas, derinti kitų institucijų steigiamų ar modernizuojamų registrų ar IS įteisinimo dokumentus, rengti išvadas dėl gautų derinti teisės aktų projektų, susijusių su valstybės informacinių išteklių sauga, ir kt. Remiantis pateikta informacija, tokių dokumentų paketų (apie 100 puslapių apimties) pateikiama po kelis per savaitę, tad vien šios derinimo veiklos vykdymas yra nemažas krūvis vienam darbuotojui. Neatmestina tai, jog dalis valdytojo funkcijų (žr. 1.2.2 poskyrį) neįgyvendinama būtent dėl žmogiškųjų išteklių stokos.

Reikia pažymėti ir tai, kad dalį funkcijų, kurias atlieka Viešojo administravimo politikos skyrius, atlieka ir Informatikos ir ryšių departamentas, pvz., rengia IS nuostatų ir duomenų saugos nuostatų projektus. Departamento Duomenų saugos skyrius taip pat analizuoja ir teikia pastabas, derina kitų institucijų steigiamų ar modernizuojamų registrų ar IS įteisinimo dokumentus, rengia išvadas dėl gautų derinti teisės aktų projektų, susijusių su valstybės informacinių išteklių sauga.

Vadovaujantis subsidiarumo principu, būtina atskirti el. valdžios ir el. saugos politikos formavimo ir jos įgyvendinimo (t. y. IS valdytojo) funkcijas. Kad ministerijos valdomų informacinių išteklių valdytojo funkcijos būtų vykdomos nuosekliai ir sistemiškai, ministerija turėtų skirti pakankamai žmogiškųjų išteklių šioms funkcijoms įgyvendinti.

3.3. Daugeliui ministerijos valdomų IS ir registrų nėra paskirti duomenų valdymo įgaliotiniai

Valstybės informacinių išteklių valdymo įstatyme⁴⁸ nurodyta, kad įstaigoje kiekvienam registriui, valstybės informacinei sistemai ar jos posistemiiui turi būti paskirtas duomenų valdymo įgaliotinis. Jį skiria valstybės informacinės sistemos ar registro valdytojas arba tvarkytojas.

⁴⁷ Lietuvos Respublikos viešojo administravimo įstatymas, 1999-06-17 Nr. VIII-1234, 4 str. 2 d.

⁴⁸ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 8 str. 3 d.

Informatikos ir ryšių departamento direktoriaus įsakymais yra paskirti dviejų registru (IKNR ir NVŽR) duomenų valdymo įgaliotiniai, o vidaus reikalų ministro įsakymu – PISIS ir NETAIS įgaliotiniai.

Nesant paskirto duomenų valdymo įgaliotinio, atsakingo už teisės aktais institucijai nustatytų funkcijų vykdymą, nebus įgyvendinamos jam teisės aktais nustatytos funkcijos⁴⁹, susijusios su IS ar registro kūrimu, priežiūra, plėtra, investicijomis bei duomenų ir informacijos valdymu.

Atsižvelgiant į tai, kad daugumos ministerijos valdomų informacinių išteklių naudotojai yra Vidaus reikalų ministerijos pavaldžios įstaigos, skiriant ministerijos valdomų informacinių išteklių duomenų valdymo įgaliotinius, tikslinga atsižvelgti į veiklos sritis, kuriose atitinkami ištekliai yra dažniausiai naudojami (1 lentelė).

1 lentelė. Vidaus reikalų ministerijos ir Informatikos ir ryšių departamento valdomų informacinių išteklių naudojimas pagal veiklos sritis

Veiklos sritis	Viešasis saugumas ⁵⁰	Migracija	Viešasis administravimas ir informacinių technologijų taikymas viešojo administravimo (elektroninės valdžios) srityje	Regionų plėtra	Valstybės informacinių išteklių sauga tiek, kiek tai neapima kibernetinio saugumo	Vietos savivalda	Valstybės tarnyba	Kūno kultūra ir sportas
IS ar registras naudojamas veiklos srities funkcijoms įgyvendinti	VRIS, N.SIS, IBPS, ATPR, NVŽR, IAŽR, HDR, VRPR, IKNR, VRIS	VRIS, N.VIS, UR, EPEKIS, ADIS, ADGIS	VRIS, SVIS, PISIS, NETAIS, ADIS, ADGIS	-	ARSIS	-	-	-

Šaltinis: Informatikos ir ryšių departamentas

4. NUSTATYTA NE VISŲ MINISTERIJOS VALDOMŲ INFORMACINIŲ IŠTEKLIŲ IT POKYČIŲ VALDYMO TVARKA

COBIT pokyčių valdymo procesas⁵¹ rekomenduoja, kad visi IT pokyčiai, įskaitant ir avarinę priežiūrą bei pataisas, susijusias su infrastruktūra ir taikomosiomis programomis darbinėje aplinkoje, būtų standartizuotai valdomi ir kontroliuojami. Pokyčių (procedūrų, procesų, sistemų ir paslaugų parametrų) valdymas ir kontrolė įgyvendinama juos registruojant, vertinant, prieš vykdant jiems išduodami leidimai, o įgyvendinus jie peržiūrimi ir lyginami su planuotais rezultatais. Tai užtikrina pokyčių neigiamo poveikio informacinių sistemų stabilumui ar vientisumui rizikos mažinimą.

Norminiuose teisės aktuose nustatyta, kad, atlikdami informacinės sistemos funkcijų pakeitimus, administratoriai turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos

⁴⁹ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 8 str. 2 d.

⁵⁰ Viešojo tvarka, vidaus tarnyba, priešgaisrinė bei civilinė sauga ir gelbėjimo darbai, valstybės sienos apsauga, ginklų, šaudmenų, sprogmenų ir specialiųjų priemonių apyvarta, saugomo asmens statusą turinčių asmenų apsauga.

⁵¹ COBIT 4.1, 2011, Vilnius; AI6 procesas, 93 psl.

pokyčių valdymo tvarkos, nustatytos Saugaus elektroninės informacijos tvarkymo taisyklėse⁵².

Nustatėme (4 priedas), kad neparengtos 3 (iš 16) ministerijos valdomų informacinių išteklių pokyčių valdymo tvarkos (3 priedas), o septynių – neatnaujintos (5 pavyzdys).

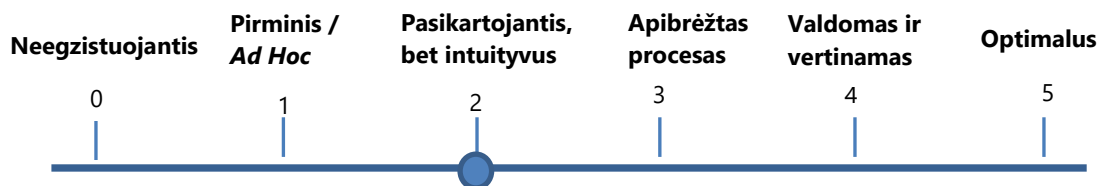
5 pavyzdys

Vadovaudamasi iki 2013-08-08 galiojusiais teisės aktais⁵³, Vidaus reikalų ministerija IS pokyčiams valdyti parengė ir patvirtino VRIS (ministro 2007-12-29 įsakymas Nr. 1V-453), kurios dalys yra dar penki informaciniai ištekliai ir N.SIS (ministro 2008-02-22 įsakymas Nr. 1V-68), pokyčių valdymo tvarkos aprašus. Reikia pažymėti, kad šie dokumentai nėra atnaujinti nuo 2007 m. Juose apibrėžiamas IS pokyčių valdymas neatitinka aktualių teisės aktų normų (nuostatos, susijusios su IS pokyčių suskirstymu į kategorijas pagal pokyčio tipą, įtakos vertinimu ir pokyčių prioritetų nustatymo procesais, ir kt.) ir gerosios praktikos šiam procesui keliamų reikalavimų: užtikrinti, kad IT paslaugose arba IT infrastruktūroje atliekamiems pakeitimams būtų taikomi standartizuoti metodai ir procedūros, tam, kad jei vyktų greitai, efektyviai ir tuo pačiu sumažintas su keitimais susijusių sutrikimų neigiamas poveikis.

Nepaisant to, kad 13 ministerijos valdomų informacinių išteklių pokyčių valdymo procesas yra apibrėžtas, praktikoje daugumos jų (11 iš 13) pokyčiai vykdomi nesilaikant reikalavimų: neatliekamas nuoseklus ir išsamus veiklos padalinių inicijuotų pokyčių dokumentavimas, apimantis visų pokyčių registravimą, skirstymą į kategorijas, prioritetų nustatymą, avarines procedūras, nėra galimybės stebėti pokyčio būseną įvairiais pokyčių valdymo etapais, nenustatytas pokyčio poveikio vertinimo procesas, o tai lemia (didina) neigiamo pokyčių poveikio IS stabilumui ir vientisumui riziką.

Atsižvelgiant į šiame skyriuje įvardytus IT pokyčių valdymo proceso trūkumus ir dėl jų kylančias rizikas, šio proceso branda vertinama kaip pasikartojantis, bet intuityvus procesas (6 pav.).

6 pav. Pokyčių valdymo proceso (AI6)⁵⁴ branda – pasikartojanti, bet intuityvi



Šaltinis: Valstybės kontrolė

Siekdama sistemiškai valdyti pokyčius, Vidaus reikalų ministerija turėtų peržiūrėti esamą IT pokyčių valdymo procesą ir nustatyti jų valdymo tvarką visiems ministerijos valdomiems informaciniams ištekliams. Tvarkoje turėtų būti išdėstytos IT pokyčių valdymo nuostatos, apimančios planavimą, suskirstymą į kategorijas, prioritetų nustatymą, avarines procedūras ir įtakos vertinimo procesus, be to, būtina užtikrinti šios tvarkos laikymosi (vykdymo) kontrolę.

Informatikos ir ryšių departamentas pateikė informaciją, kad 2017 m. planuojama reglamentuoti IT pokyčių valdymo proceso įgyvendinimą vidaus reikalų sistemoje ir įdiegti priemones IT pokyčių

⁵² Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 28 p. (akto redakcijoje galiojusioje nuo 2013-08-08 iki 2016-08-19) ir 21 p. (naujoje akto redakcijoje galiojančioje nuo 2016-08-19); Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 (neteko galios 2013-08-08) patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemos reikalavimai, 21 p.

⁵³ Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 (neteko galios 2013-08-08) patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, 33 p.

⁵⁴ COBIT 4.1, 2011 m., Vilnius; AI6 procesas, 96 psl.

procesams valdyti (darbai įtraukti į vidaus reikalų ministrui pavestų valdymo sričių 2017–2019 m. strateginio veiklos plano projektą).

5. INFORMATIKOS IR RYŠIŲ DEPARTAMENTO TEIKIAMŲ IT PASLAUGŲ LYGIAI NEAPIBRĖŽTI

IT paslaugų ir jų lygių apibrėžimas ir dokumentavimas sudaro sąlygas IT vadovams ir veiklos klientams rezultatyviai komunikuoti dėl reikalingų paslaugų. Į šį procesą įeina stebėseną ir pranešimas reikiamu laiku suinteresuotosioms šalims apie pasiektus paslaugų lygius. Be to, šis procesas leidžia suderinti IT paslaugas su susijusiais veiklos poreikiais⁵⁵.

Informacinių technologijų paslaugų valdymo metodika⁵⁶ nurodo, jog planavimo etape valstybės informacinių išteklių veikimui tinkamai stebėti, prižiūrėti ir plėtoti sudaromas IT paslaugų katalogas: nurodomas IT paslaugos užsakovas, kiekvienai IT paslaugai paskiriamas institucijos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, atsakingas už IT paslaugos teikimo organizavimą bei priežiūrą (toliau – atsakingas už IT paslaugos teikimą asmuo).

Informatikos ir ryšių departamentas ne tik administruoja (užtikrina saugą, integralumą, suderinamumą, naudotojų centralizuotą valdymą ir kt.) Vidaus reikalų ministerijos valdomus informacinius išteklius – 2016-01-05 jis paskirtas⁵⁷ vienu iš keturių valstybės IT paslaugų teikėju. Atsižvelgiant į tai, IT paslaugų ir jų lygių apibrėžtis įgauna dar didesnę svarbą.

Vidaus reikalų ministras įpareigojo⁵⁸ Informatikos ir ryšių departamentą iki 2016-03-31 parengti ir patvirtinti detalų Vidaus reikalų ministerijos srities įstaigoms teikiamų IT paslaugų katalogą, tačiau iki 2016-03-31 jis nebuvo patvirtintas.

Be to, iki 2016-04-31 Informatikos ir ryšių departamentas turėjo inventorizuoti Vidaus reikalų ministerijos srities įstaigų tuo metu galiojančias, su perduodamomis funkcijomis susijusias sutartis⁵⁹, sudaryti tarpusavio IT paslaugų teikimo susitarimus (angl. *Service Level Agreement*)⁶⁰ tarp Informatikos ir ryšių departamento ir Vidaus reikalų ministerijos bei jos srities įstaigų. Šie pavedimai iki nustatyto termino taip pat nebuvo įgyvendinti.

Nustatėme, kad Informatikos ir ryšių departamento teikiamų IT paslaugų analizė neatliekama.

Nepatvirtinus Informatikos ir ryšių departamento teikiamų IT paslaugų katalogo ir neatliekant paslaugų lygio stebėsenos, kyla rizika, kad IT paslaugos nebus teikiamos pagal visus IT paslaugų teikimo susitarimus. Konsolidavus informacinius išteklius ir departamentui tapus vienu iš keturių IT paslaugų teikėju, galimai nebus užtikrintas kokybiškas IT paslaugų tiekimas daugeliui valstybinių įstaigų reikiamu laiku.

⁵⁵ COBIT 4.1, 2011 m., Vilnius; DS1 procesas, 101 psl.

⁵⁶ Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013-06-19 įsakymu Nr. T-83 patvirtinta Informacinių technologijų paslaugų valdymo metodika.

⁵⁷ Lietuvos Respublikos vidaus reikalų ministro 2016-01-05 įsakymas Nr. 1V-4 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos paskyrimo valstybės informacinių technologijų paslaugų teikėju“, 1 p.

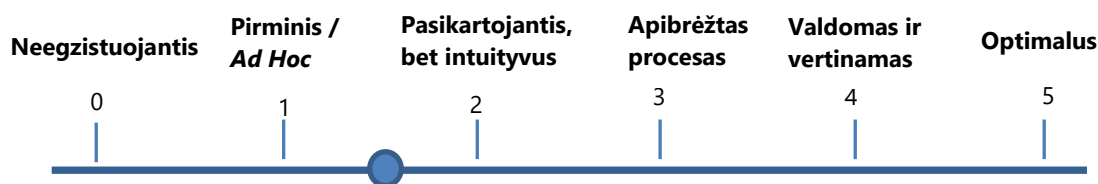
⁵⁸ Lietuvos Respublikos vidaus reikalų ministro 2016-01-05 įsakymas Nr. 1V-4 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos paskyrimo valstybės informacinių technologijų paslaugų teikėju“, 3.2.4 p.

⁵⁹ Ten pat, 3.1.3 p.

⁶⁰ Ten pat, 3.1.6 p.

Atsižvelgiant į šiame skyriuje nustatytus IT paslaugų apibrėžimo trūkumus ir dėl to kylančias rizikas, IT paslaugų lygių apibrėžimo ir valdymo proceso branda vertinama kaip pirminis (*Ad Hoc*) procesas (7 pav.).

7 pav. IT paslaugų lygių apibrėžimo ir valdymo proceso⁶¹ branda – *Ad hoc*



Šaltinis: Valstybės kontrolė

Kokybiškas IT paslaugų tiekimas daugeliui valstybinių įstaigų reikiamu laiku bus užtikrintas tik patvirtinus departamento teikiamų IT paslaugų katalogą ir stebint šių paslaugų teikimo lygį.

Pažanga audito metu: 2016-10-07 Informatikos ir ryšių departamento direktoriaus įsakymu Nr. 5V-68 patvirtintas Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos teikiamų informacinių technologijų ir telekomunikacijų paslaugų katalogas.

6. MINISTERIJA NEPAKANKAMAI PASIRENGUSI UŽTIKRINTI IS SAUGĄ IR VEIKLOS TĘSTINUMĄ

Norint išlaikyti informacijos vientisumą ir apsaugoti IT turtą, reikalingas saugos valdymo procesas, apimantis IT saugos funkcijas ir atsakomybę, politiką, standartų ir procedūrų nustatymą ir priežiūrą. Saugos valdymas apima ir saugos tikrinimą, periodišką testavimą ir nustatytų saugos trūkumų ar incidentų korekcinis veiksmus. Rezultatyvus saugos valdymas apsaugo visą IT turtą ir sumažina saugos silpnųjų vietų ir incidentų poveikį veiklai⁶².

Vidaus reikalų ministerijoje nuo 2013 iki 2016 m. vidurio nebuvo užfiksuota saugos incidentų, kurie būtų pažeidę ministerijos valdomuose IS ar registruose saugomų duomenų konfidencialumą, prieinamumą ar vientisumą, tačiau audito metu nustatėme IS saugos valdymo trūkumų:

- ministerijoje nėra IS saugos klausimus sprendžiančios struktūros, kurią sudarytų svarbiausių veiklos sričių: pagrindinių ministerijos veiklos sričių, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito, atstovai;
- 2 (iš 16) ministerijos valdomiems informaciniams ištekliams nepaskirti saugos įgaliotiniai, todėl neatlikti šių išteklių rizikos ir saugos atitikties vertinimai;
- ministerija skiria nepakankamai dėmesio IS rizikos ir saugos atitikties vertinimų metu nustatytų rizikos valdymo priemonių įgyvendinimo kontrolei;
- neparengti ir nepatvirtinti ministerijos valdomos 1 (iš 16) IS duomenų saugos nuostatai ir trys saugos politiką įgyvendinantys dokumentai⁶³.
- 11 (iš 16) ministerijos valdomų informacinių išteklių saugos politiką apibrėžiantys ir jos

⁶¹ COBIT 4.1, 2011 m., Vilnius; DS1 procesas, 104 psl.

⁶² Ten pat, 117 psl.

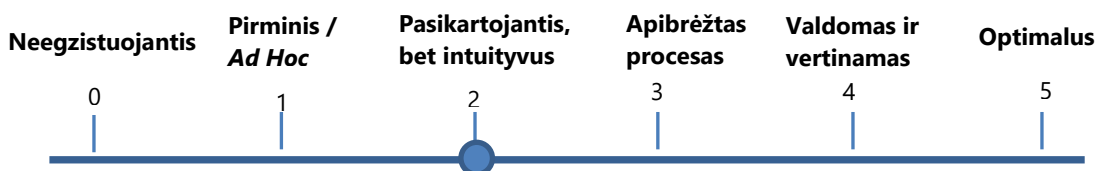
⁶³ Saugos politiką įgyvendinantys dokumentai: Saugaus elektroninės informacijos tvarkymo taisyklės; Informacinės sistemos veiklos tęstinumo valdymo planas; Informacinės sistemos naudotojų administravimo taisyklės.

įgyvendinimą reglamentuojantys teisės aktai iki 2016-07-01 neatnaujinti.

Išsamiau apie tai rašome 6.1, 6.2 ir 6.3 poskyriuose.

Taigi, IT sistemų saugos užtikrinimo proceso branda vertinama kaip pasikartojantis, bet intuityvus procesas (8 pav.).

8 pav. Informacinių sistemų saugos užtikrinimo proceso (DS5)⁶⁴ branda – pasikartojanti, bet intuityvi



Šaltinis: Valstybės kontrolė

Siekiant aukštesnio brandos lygio, turėtų būti įgyvendinti teisės aktų reikalavimai ir:

- sudaryta gerąją praktiką atitinkanti IT saugos valdymo struktūra, kurios pagrindinis uždavinys būtų koordinuoti Vidaus reikalų ministerijos valdomų informacinių sistemų ir registrų saugos politikos įgyvendinimą;
- užtikrintas saugos įgaliojimo funkcijų įgyvendinimas ir IS rizikos ir saugos atitikties vertinimų metu nustatytų rizikos valdymo priemonių įgyvendinimo kontrolė.

6.1. Skiriama nepakankamai dėmesio organizuojant, koordinuojant ir kontroliuojant sistemų saugos užtikrinimo procesą

COBIT rekomenduoja IT saugą valdyti aukščiausiu tinkamu organizacijos lygmeniu, kad saugos veiksmų valdymas atitiktų veiklos poreikius⁶⁵.

Vidaus reikalų ministro nuo 2008 m. sudaryta⁶⁶ Vidaus reikalų informacinės sistemos, Lietuvos nacionalinės Šengeno informacinės sistemos ir Lietuvos nacionalinės vizų informacinės sistemos saugos darbo grupė (toliau – SDG) turėjo:

- koordinuoti informacijos saugos priemonių ir metodų taikymą VRIS, NSIS ir NVIS;
- koordinuoti VRIS, NSIS, NVIS duomenų saugos incidentų tyrimą;
- teikti siūlymus VRIS, NSIS ir NVIS saugos įgaliojiniui įgyvendinant saugos politiką;
- teikti VRIS, NSIS ir NVIS valdytojui rekomendacijas, susijusias su šių informacinių sistemų saugos politikos tobulinimu ir jos įgyvendinimu;
- svarstyti VRIS, NSIS ir NVIS saugos įgaliojimo pateiktus siūlymus dėl VRIS, NSIS ir NVIS saugos dokumentų nuostatų keitimo ar pripažinimo netekusiomis galios būtinumo, teikti dėl jų savo rekomendacijas;
- prižiūrėti vykdomą VRIS, NSIS ir NVIS saugos politiką, kaupti informaciją, reikalingą saugos politikos tobulinimui.

⁶⁴ COBIT 4.1, 2011 m., Vilnius; DS5 procesas, 120 psl.

⁶⁵ Ten pat, 118 psl.

⁶⁶ Lietuvos Respublikos vidaus reikalų ministro 2008-11-06 įsakymas Nr. 1V-400 „Dėl Vidaus reikalų informacinės sistemos ir Lietuvos nacionalinės Šengeno informacinės sistemos saugos darbo grupės sudarymo ir jos darbo reglamento patvirtinimo“ (neteko galios 2012-06-18); 2012-06-18 įsakymu Nr. 1V-462 „Dėl Vidaus reikalų informacinės sistemos ir Lietuvos nacionalinės Šengeno informacinės sistemos saugos darbo grupės sudarymo ir jos darbo reglamento patvirtinimo“ sudaryta naujos sudėties analogiška darbo grupė, atnaujintas jos reglamentas; 2013-04-30 įsakymu Nr. 1V-384 pakeista darbo grupės sudėtis.

Nustatėme, kad 2013–2016 m. I ketvirtį ši grupė veiklos nevykdė, nors reglamente nustatyta, kad grupė renkasi į savo posėdžius ne rečiau kaip kartą per pusę metų. Tai rodo nepakankamą Vidaus reikalų ministerijos vadovybės dėmesį (palaikymą) organizuojant, koordinuojant ir kontroliuojant informacinės saugos užtikrinimo procesus.

Pokyčiai audito metu: ministerija parengė įsakymo projektą, kuriame numatoma sudaryti gerąją praktiką atitinkančią IT saugos valdymo struktūrą – Vidaus reikalų ministerijos valdomų informacinių sistemų ir registrų saugos darbo grupę, vadovaujamą viceministro. Darbo grupės pagrindinis uždavinys – koordinuoti ministerijos valdomų informacinių sistemų ir registrų saugos politikos įgyvendinimą.

6.2. Atliekami ne visų IS rizikos ir saugos atitikties vertinimai, o atliktų vertinimų metu nustatyti trūkumai šalinami vangiai

COBIT rekomenduoja aktyviai testuoti ir stebėti IT saugos būklę. IT sauga turi būti laiku akredituojama iš naujo, kad būtų išlaikomi patvirtinti organizacijos informacijos saugos baziniai rodikliai⁶⁷.

Teisės aktai nustato, kad:

- IS ar registro valdytojas teisės aktu, kuriuo tvirtinami duomenų saugos nuostatai, skiria saugos įgaliotinį, kuris koordinuoja ir prižiūri saugos politikos įgyvendinimą IS, arba paveda jį paskirti IS tvarkytojui⁶⁸.
- Saugos įgaliotinis kasmet turi organizuoti IS rizikos vertinimą. IS rizikos įvertinimas turi būti išdėstomas rizikos įvertinimo ataskaitoje⁶⁹.
- Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui, taip pat pastebėtų trūkumų šalinimo planas; jį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas⁷⁰.

Nustatėme, kad iš 16 ministerijos valdomų informacinių išteklių 14 yra priskirti saugos įgaliotiniai (4 priedas), todėl kitų dviejų IS rizikos ir saugos atitikties vertinimai 2013–2015 m. nebuvo atlikti. Informatikos ir ryšių departamento valdomo registro saugos įgaliotinis paskirtas, tačiau nuo 2012 m. pradžios iki 2016-07-01 rizikos vertinimų neatlikta. Saugos atitikties vertinimas atliktas tik 2015 m. (ankstesniais laikotarpiais nebuvo atliekamas).

Įvertinę 2013–2015 m. parengtas IS rizikos ir saugos atitikties ataskaitas ir nustatytų trūkumų šalinimo planavimo ir rekomendacijų įgyvendinimo procesą nustatėme, kad IS valdytojų vadovai nepakankamai užtikrina pastebėtų trūkumų šalinimo kontrolę, nes:

- trūkumų šalinimo planuose nenumatomi kontrolės priemonių įgyvendinimo terminai ir atsakingi vykdytojai;
- vertinimo ataskaitos ir planai nėra suderinti ir patvirtinti IS ar registrų valdytojų vadovų.

⁶⁷ COBIT 4.1, 2011 m., Vilnius; DS5 procesas, 118 psl.

⁶⁸ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 44 str.; Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 19 ir 22 p.

⁶⁹ Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, 30 ir 31 p.; Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 35 ir 36 p.

⁷⁰ Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 44 p.

Išanalizavę 2013 ir 2014 m. VRIS, N.SIS, ir N.VIS saugos atitikties vertinimo ataskaitas, pastebėjome, kad jose įvardyti tie patys atitikties nustatytiems saugos reikalavimams trūkumai ir pateiktos tokios pačios rekomendacijos.

Neįgyvendinant trūkstamų saugos priemonių, padidėja įsilaužimų į sistemas, duomenų nutekėjimo, praradimo ir informacinių išteklių sutrikdymo tikimybė.

6.3. IS ir registų saugos politikos dokumentai laiku neatnaujinami

COBIT rekomenduoja⁷¹: norint išlaikyti informacijos vientisumą ir apsaugoti IT turtą, reikalingas saugos valdymo procesas, apimantis IT saugos funkcijų ir atsakomybės, politikos, standartų ir procedūrų nustatymą ir priežiūrą. Saugos valdymas apima ir saugos tikrinimą, periodišką testavimą ir nustatytų saugos trūkumų ar incidentų koregavimo veiksmus. Rezultatyvus saugos valdymas apsaugo visą IT turtą ir sumažina saugos silpnųjų vietų ir incidentų poveikį veiklai.

Lietuvos Respublikos teisės aktai nustato, kad IS ir registro valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus⁷²:

- Saugos nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;
- Informacinės sistemos veiklos tęstinumo valdymo planą;
- Informacinės sistemos naudotojų administravimo taisykles.

Nustatėme, kad ministerija iki 2016-07-01 neparengė ir nepatvirtino visų saugos dokumentų Nacionalinei elektroninės atpažinties informacinei sistemai (NETAIS). PASIS ir SVIS neturi parengtų ir patvirtintų saugos politiką įgyvendinančių dokumentų.

Be to, kaip rašyta 2.4 poskyryje, Vidaus reikalų ministerijos valdomų informacinių sistemų ir registų (12 iš 16) naujos redakcijos saugos dokumentų atnaujinimas vėluoja daugiau kaip metus, nes nuostata nebuvo įgyvendinta iki 2016-07-01 (3 priedas). Tokia situacija susiklosto dėl laiku neatnaujinamų IS nuostatų – stabdomas ir saugos politiką įgyvendinančių dokumentų atnaujinimo procesas (6 pavyzdys).

6 pavyzdys

2015 m. Informatikos ir ryšių departamentas, atsižvelgdamas į teisės aktų reikalavimus, parengė VRIS duomenų saugos nuostatus bei saugos politiką įgyvendinančių dokumentų projektus ir, suderinęs su ministerijos Elektroninės valdžios politikos skyriumi, pateikė derinti Vidaus reikalų ministerijos Teisės departamentui. Vidaus reikalų ministerijos Teisės departamentas 2015-06-19 raštu Nr. 3D-598 „Dėl Vidaus reikalų informacinės sistemos“ pateikė pastabas ir nurodė, kad nėra tikslinga VRIS duomenų saugos nuostatus keisti, nekeičiant VRIS nuostatų. Pažymėtina, kad VRIS nuostatuose turi būti aiškiai apibrėžiamas objektas, kurio elektroninės informacijos sauga reguliuojama duomenų saugos nuostatuose. Aiškiai neapibrėžus elektroninės informacijos saugos objekto, nėra galimybės tinkamai sureguliuoti ir elektroninės informacijos saugos.

2016 m. VRIS duomenų saugos nuostatus bei saugos politiką įgyvendinančių dokumentų projektus Informatikos ir ryšių departamentas dar kartą atnaujino, tačiau derinti nebeteikė, nes Vidaus reikalų ministerija VRIS nuostatų iki 2016-06-01 neatnaujino.

⁷¹ COBIT 4.1, 2011 m., Vilnius; DS5 procesas, 117 psl.

⁷² Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 7 p.

Taip pat nustatėme trūkumų įgyvendinant techninius IS ir registrų elektroninės informacijos saugos reikalavimus (3 priedas).

Ministerijoje naudojama techninė ir programinė įranga bus tinkamai paruošta laiku ir veiksmingai reaguoti į informacijos saugos incidentus tik nustačius ir įdiegus teisės aktų reikalaujamas IS saugos užtikrinimo priemones.

7. VIDAUS KONTROLĖS STEBĖSENOS IR VERTINIMO PROCESAS APIBRĖŽTAS, BET NEĮGYVENDINAMAS

COBIT vidaus kontrolės stebėsenos ir vertinimo procesas⁷³ nurodo, jog siekiant efektyviai valdyti IT veiklą reikia nustatyti tinkamus veiklos rodiklius, sistemingai ir laiku atlikti veiklos stebėseną ir operatyviai reaguoti, esant nuokrypių. Stebėseną reikalinga siekiant užtikrinti, kad būtų taikomos tinkamos ir nustatytas kryptis bei politiką atitinkančios priemonės. Rekomenduojama nuolat vertinti visus IT procesus ir jų atitiktį vidaus kontrolės reikalavimams. Vertinimas turėtų apimti efektyvumo valdymą, vidaus kontrolės sistemos stebėjimą, atitiktį teisinio reguliavimo ir valdymo reikalavimams.

Lietuvos Respublikos teisės aktai nustato, kad:

- Vertinant valstybės informacinių sistemų, kuriomis apdorojama visai valstybei svarbi institucijos valdoma informacija, ir pagrindinių valstybės registrų, taip pat valstybės informacinių sistemų ir registrų, kuriems kurti ar modernizuoti viršytas Vyriausybės ar jos įgaliotos institucijos nustatytas lėšų dydis, valdymą ir saugą, ne rečiau kaip kartą per trejus metus atliekamas informacinių technologijų auditas⁷⁴.
- Vienas vidaus audito uždavinių – ne rečiau kaip vieną kartą per trejus metus įvertinti, kaip vidaus kontrolė veikia viešajame juridiniame asmenyje⁷⁵.
- Pavyzdinėje vidaus audito metodikoje⁷⁶ rekomenduota, kad vidaus auditorius, atlikdamas vidaus auditą, turi tikrinti ir vertinti ir taikomosios IS kontrolės priemones, atlikti jų testavimą pagal vidaus auditoriaus parengtus šių kontrolės priemonių tikrinimo klausimynus.

Vidaus reikalų ministerija valdo aštuonis ypatingos svarbos informacinius išteklius, tačiau nuo Informacinių išteklių valdymo įstatymo įsigaliojimo datos (2012-01-01) informacinių technologijų auditas nebuvo atliktas.

Vidaus reikalų ministerijos Vidaus audito skyriaus nuostatuose⁷⁷ nurodyta, kad skyrius turi tikrinti ir vertinti informacinių sistemų valdymą ir naudojimą. Per 2013–2015 metus skyrius neatliko nė vieno audito, kurio objektas būtų informacinės sistemos, jų saugos, bendrosios kontrolės ar kito IS (IT) aspekto vertinimas, todėl ministerijos vadovybė neturi duomenų apie IT procesų efektyvumą, atitiktį veiklos reikalavimams, nenustatomos IT kontrolės trūkumai ir spragos, nesilaikoma teisės aktų reikalavimų (3 priedas).

⁷³ COBIT 4.1, 2011 m., Vilnius; ME2 procesas, 157 psl.

⁷⁴ Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 14 str. 1 d.

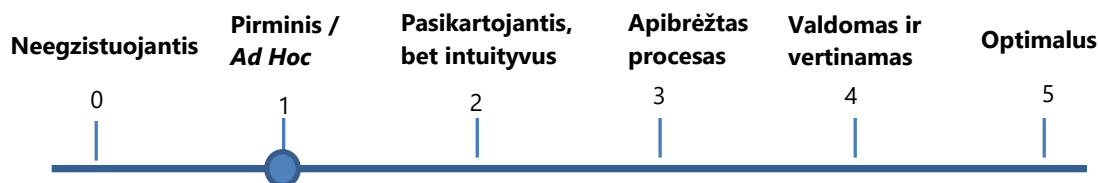
⁷⁵ Lietuvos Respublikos vidaus kontrolės ir vidaus audito įstatymas, 2002-12-10 Nr. IX-12535 (nuo 2010-07-01 galiojanti redakcija), 5 str. 2 d. 6 p.

⁷⁶ Lietuvos Respublikos finansų ministro 2003-05-02 įsakymas Nr. 1K-117 „Dėl Pavyzdinės vidaus audito metodikos, Vidaus auditorių profesinės etikos taisyklių patvirtinimo“ (nuo 2010-06-04 galiojanti redakcija), 12.5 p.

⁷⁷ Lietuvos Respublikos vidaus reikalų ministro 2003-07-18 įsakymu Nr. 1V-280 (2009-11-19 įsakymo Nr. 1V-614 redakcija) patvirtinti Vidaus reikalų ministerijos Vidaus audito skyriaus nuostatai, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.7 p.

Ministerijos IT vidaus kontrolės stebėsenos ir vertinimo proceso branda pateikiama 9 paveiksle.

9 pav. IT vidaus kontrolės stebėsenos ir vertinimo proceso (ME2)⁷⁸ branda – *Ad Hoc*



Šaltinis: Valstybės kontrolė

Siekiant užtikrinti IS veiklos rezultatyvumą ir efektyvumą bei atitikti teisės aktų reikalavimus, turėtų būti vykdoma vidaus kontrolės stebėseną: būtina ne rečiau, kaip nustatyta teisės aktuose, stebėti ir vertinti informacinių sistemų ir registų vidaus kontrolės būklę.

L. e. p. Informacinių technologijų audito departamento
direktorė

Živilė Simonaitytė

Informacinių technologijų audito departamento
vyriausioji valstybinė auditorė

Viktorija Mirošničenko

Valstybinio audito ataskaitos kopijos (po 1 egz.) pateiktos:

Lietuvos Respublikos Seimo Audito komitetui,

Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komitetui.

Auditas atliktas, vykdant 2016-01-18 pavedimą Nr. P-90-2

Auditą atliko valstybinių auditorių grupė:

Viktorija Mirošničenko (grupės vadovė),

Kęstutis Kumetaitis (iki 2016-04-01),

Kęstutis Valeika.

⁷⁸ COBIT 4.1, 2011 m., Vilnius; ME2 procesas, 160 psl.

PRIEDAI

Valstybinio audito ataskaitos
„Vidaus reikalų ministerijos
informacinių išteklių valdymas“
1 priedas

Rekomendacijų įgyvendinimo planas

Eil. Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės	Rekomendacijos įgyvendinimo terminas (data)
1.	Siekiant nuosekliai ir kryptingai tobulinti IS ir registrus ir atsižvelgiant į visos organizacijos veiklos poreikius, parengti ir patvirtinti Vidaus reikalų ministerijos valdymo srities strateginį IT planą.	Vidaus reikalų ministerija	Parengti ir patvirtinti Vidaus reikalų ministerijos strateginį IT planą.	2017-12-31
2.	Sudaryti ir nuolat atnaujinti visų ministerijoje naudojamų IS, registrų ir kitos programinės įrangos sąrašą.	Vidaus reikalų ministerija	Aktualizuoti Vidaus reikalų ministerijoje naudojamų IS, registrų ir kitos programinės įrangos sąrašą.	2017-06-01
3.	Sudaryti informacijos architektūros modelį, apimantį ministerijos valdomos informacijos, IS (registrų) duomenų bei technologinę architektūrą, nurodant visus komponentus (taikomas technologijas, duomenis, duomenų srautus tarp išorinių ir vidinių IS).	Vidaus reikalų ministerija	Sudaryti Vidaus reikalų informacinių išteklių informacijos architektūros modelį, nurodant taikomas technologines platformas, duomenų grupes ir duomenų srautus).	2018-05-31
4.	Siekiant, kad nebūtų stabdomas saugos politiką įgyvendinančių dokumentų atnaujinimo procesas, atnaujinti N.SIS ir SVIS nuostatus. Priimti sprendimą dėl tolesnio VRIS kaip valstybės IS egzistavimo ir apibrėžti jos struktūrą, kuri būtų paprastesnė ir lankstesnė.	Vidaus reikalų ministerija	- Atnaujinti N.SIS nuostatus - Atnaujinti SVIS nuostatus. - Reorganizuoti VRIS. Parengti ir patvirtinti valstybės informacinės sistemos – Vidaus reikalų integracinės platformos nuostatus. - Parengti ir patvirtinti Vidaus reikalų informacinių išteklių aprašą, jo priede nurodyti ministerijos ir jai pavaldžių įstaigų valdomas IS ir registrus, jų sąveikumui užtikrinti skirtą Vidaus reikalų integracinę platformą, telekomunikacijų tinklus.	2017-10-01 2016-10-01 2017-10-30 2017-12-30
5.	Vadovaujantis subsidarumo principu ⁷⁹ , atskirti el. valdžios ir el. saugos politikos formavimo ir jos įgyvendinimo (t. y. IS valdytojo) funkcijas.	Vidaus reikalų ministerija	Atskirti e. valdžios ir e. saugos politikos formavimo ir jos įgyvendinimo (t. y. IS valdytojo) funkcijas pareigybių lygiu – atitinkamai patikslinti	2016-12-31

⁷⁹ Lietuvos Respublikos viešojo administravimo įstatymas, 1999-06-17 Nr. VIII-1234, 4 str. 2 d.

Eil. Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės	Rekomendacijos įgyvendinimo terminas (data)
			Elektroninės valdžios ir saugos politikos skyriaus valstybės tarnautojų pareigybių aprašymus.	
6.	Skiriant ministerijos valdomų informacinių išteklių duomenų valdymo įgaliotinius, atsižvelgti į veiklos sritis, kuriose atitinkami ištekliai yra dažniausiai naudojami.	Vidaus reikalų ministerija	Paskirti N.SIS, N.VIS, UR, IAŽR, ATPR, IBPS, VRPR, KTPR, KTPVR, HDR, SVIS, ARSIS, VRIP duomenų valdymo įgaliotinius.	2016-12-31
7.	Siekdama sistemingo pokyčių valdymo, peržiūrėti esamą IT pokyčių valdymo procesą ir nustatyti (patvirtinti) visų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarką. Joje turėtų būti išdėstytos IT pokyčių valdymo nuostatos, apimančios planavimą, suskirstymą į kategorijas, prioritetų nustatymą, avarines procedūras ir įtakos vertinimo procesus, be to, būtina užtikrinti šios tvarkos laikymosi (vykdymo) kontrolę.	Vidaus reikalų ministerija	Atnaujinti Vidaus reikalų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarką.	2016-12-31
8.	Parengti ir patvirtinti Informatikos ir ryšių departamento teikiamų IT paslaugų katalogą ir nustatyti šių paslaugų teikimo lygį.	Vidaus reikalų ministerija	Parengti ir patvirtinti Informatikos ir ryšių departamento teikiamų IT paslaugų katalogą ir nustatyti jų teikimo lygį.	2016-10-10 Rekomendacija įgyvendinta ⁸⁰ .
9.	Sudaryti gerąją praktiką atitinkančią IS saugos klausimus spendžiančią struktūrą, kurią sudarytų atstovai iš svarbiausių veiklos sričių: pagrindinių ministerijos veiklos sričių, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito.	Vidaus reikalų ministerija	Atnaujinti Vidaus reikalų ministerijos srities informacinių sistemų ir registrų saugos darbo grupę.	2016-12-31
10.	Ne rečiau, kaip nustatyta teisės aktuose, stebėti ir vertinti informacinių sistemų ir registrų vidaus kontrolės būklę.	Vidaus reikalų ministerija	Įgyvendinus Valstybės kontrolės pateiktas rekomendacijas, atlikti vidaus reikalų ministro valdymo srityse taikomų informacinių technologijų auditą.	2018-12-31

Šaltinis: Valstybės kontrolė

Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais: vidaus reikalų viceministras J. Morkūnas, tel. 8 5 271 7076 el. paštas julius.morkunas@vrm.lt.

⁸⁰ 2016-10-07 Informatikos ir ryšių departamento direktoriaus įsakymu Nr. 5V-68 patvirtintas Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos teikiamų informacinių technologijų ir telekomunikacijų paslaugų katalogas.

Valstybinio audito ataskaitos
 „Vidaus reikalų ministerijos
 informacinių išteklių valdymas“
 2 priedas

Pagrindiniai duomenų rinkimo ir vertinimo metodai

Eil. Nr.	Metodas	Tikslai
1.	<p>Dokumentų analizė:</p> <ul style="list-style-type: none"> ▪ nagrinėjome Vidaus reikalų ministerijos, Informatikos ir ryšių departamento bei VĮ „Regitra“ dokumentus, susijusius su informacinių išteklių planavimu, įsigijimu, palaikymu ir priežiūra, saugos ir pokyčių valdymu. 	<p>Nustatyti:</p> <ul style="list-style-type: none"> ▪ ministerijos IT valdymo struktūrą; ▪ ministerijos valdomus informacinius išteklius, jų techninę infrastruktūrą, taikomas duomenų valdymo ir IS (registrų) saugos užtikrinimo priemones; ▪ IT pokyčių valdymo tvarką; ▪ kūrimo ir palaikymo trūkumus ir pranašumus; ▪ kaip atliekama stebėseną ir vertinimas.
2.	<p>Pokalbiai su šių Vidaus reikalų ministerijos padalinių darbuotojais:</p> <ul style="list-style-type: none"> ▪ Viešojo valdymo politikos departamento; ▪ Viešojo administravimo politikos skyriaus; ▪ Veiklos planavimo ir organizavimo skyriaus; ▪ Ekonomikos ir finansų departamento; ▪ Personalo ir Vidaus audito skyrių. <p>Pokalbiai su Informatikos ir ryšių departamento vadovybe ir šių skyrių darbuotojais:</p> <ul style="list-style-type: none"> ▪ Valdymo organizavimo skyriaus darbuotojais; ▪ Projektų valdymo skyriaus darbuotojais; ▪ Informacijos saugos skyriaus darbuotojais. <p>Pokalbiai su VĮ „Regitra“ Informacinių technologijų departamento darbuotojais.</p>	

Šaltinis: Valstybės kontrolė

Valstybinio audito ataskaitos
 „Vidaus reikalų ministerijos informacinių
 išteklių valdymas“
 3 priedas

Neatitiktys privalomiems vykdyti teisės aktų reikalavimams, numatomi jų pašalinimo priemonės ir terminai

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807				
1.	8 straipsnis. Duomenų valdymo įgaliojimas. [...] 3 d. Duomenų valdymo įgaliojimą skiria valstybės informacinės sistemos ar registro valdytojas arba tvarkytojas. Duomenų valdymo įgaliojimas turi būti paskirtas kiekvienam registru, valstybės informacinei sistemai ar jos posistemii.	Paskirti JKNR (valdytojas – Informatikos ir ryšių departamentas), NVŽR, PASIS duomenų valdymo įgaliojiminiai. Nepaskirti VRIS, N.SIS, N.VIS, UR, IAŽR, ATPR, IBPS, VRPR, KTPR, KTPVR, HDR, SVIS, ARSIS, NETAIS duomenų valdymo įgaliojiminiai.	Paskirti visų Vidaus reikalų ministerijos valdomų informacinių išteklių duomenų valdymo įgaliojimus.	2016-12-31
2.	9 straipsnis. 1 d. Institucija, valdanti ypatingos svarbos valstybės informacinius išteklius, rengia informacinių technologijų plėtros plano projektą, kuriame, atsižvelgiant į Vyriausybės ar Seimo patvirtintus planavimo dokumentus, Vyriausybės numatytas taikomų informacinių ir ryšių technologijų tobulinimo ir plėtros kryptis ir rekomenduojamus taikyti techninius reikalavimus (standartus) bei suderinus su kitais institucijos planavimo dokumentais, nustatomi informacinių technologijų priemonių, skirtų informacijai, duomenims, dokumentams ir (arba) jų kopijoms tvarkyti, kūrimo ir naudojimo tikslai, uždaviniai, nurodomos planuojamos kurti ar modernizuoti valstybės informacinės sistemos ir registrai, jų steigimo, modernizavimo prioritetai, planuojamos diegti elektroninės paslaugos, reikalingi finansiniai ir žmogiškieji ištekliai, organizacinės ir teisinės priemonės, kvalifikaciniai reikalavimai darbuotojams, darbuotojų mokymų poreikis, jų veiklos organizavimas ir kontrolė.	Lietuvos Respublikos vidaus reikalų ministerija valdo 8 ypatingos svarbos (ATPR, UR, VRIS, N.SIS, N.VIS, IAŽR, NVŽR) valstybės informacinius išteklius, vieną (JKNR) – jai pavaldi įstaiga, Informatikos ir ryšių departamentas. Audito metu nustatėme, kad nei ministerija, nei departamentas IT plėtros plano (planų) nėra parengę.	Parengti ir patvirtinti Vidaus reikalų ministerijos IT plėtros planą, apimančį visus ministerijos valdomus informacinius išteklius ir JKNR.	2017-12-31

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
3.	14 straipsnis. 1 d. Vertinant valstybės informacinių sistemų, kuriomis apdorojama visai valstybei svarbi institucijos valdoma informacija, ir pagrindinių valstybės registru, taip pat valstybės informacinių sistemų ir registru, kuriems kurti ar modernizuoti viršytas Vyriausybės ar jos įgaliotos institucijos nustatytas lėšų dydis, valdymą ir saugą, ne rečiau kaip kartą per trejus metus atliekamas informacinių technologijų auditas.	Vidaus reikalų ministerija valdo 8 ypatingos svarbos informacinius išteklius, bet nuo Informacinių išteklių valdymo įstatymo įsigaliojimo datos (2012-01-01) informacinių technologijų auditas nebuvo atliktas.	Įgyvendinus Valstybės kontrolės pateiktas rekomendacijas, atlikti vidaus reikalų ministro valdymo srityse taikomų informacinių technologijų auditą.	2018-12-31
4.	31 straipsnis. Valstybės informacinių sistemų kūrimas. 1 d. Valstybės informacinė sistema pradedama kurti patvirtinus valstybės informacinės sistemos nuostatus. 2 d. Valstybės informacinė sistema kuriama pagal valstybės informacinės sistemos techniniame aprašyme (specifikacijoje) nurodytą kūrimo būdą. [...] 6 d. Naudojama tik įteisinta valstybės informacinė sistema ar jos posistemis.	Viešųjų ir administracinių paslaugų portalo ir analitinės informacinės sistemos (PASIS) nuostatai ⁸¹ patvirtinti 2016-04-08, nors ši IS buvo pradėta kurti 2013 m., o sukurta 2014 m. kovo mėn. Eksploatuojamos VRIS, N.SIS, N.VIS, SVIS, PASIS, ADIS, ADGIS nėra įteisintos.	Įteisinti (parengti / atnaujinti nuostatus, specifikacijas, priėmimo ir tinkamumo eksploatuoti aktus) N.SIS, N.VIS, SVIS, PASIS, ADIS. Reorganizuoti VRIS ir įsteigti valstybės informacinės sistemą – Vidaus reikalų integracinę platformą.	2017-10-30
5.	44 straipsnis. 1 d. Saugos įgaliotiniu skiriamas darbuotojas, kuris atsako už saugos reikalavimų vykdymą ir atlieka kitas teisės aktuose nustatytas funkcijas. 2 d. Saugos įgaliotinis skiriamas teisės aktu, kuriuo tvirtinami registro ar valstybės informacinės sistemos saugos nuostatai, arba registro ar valstybės informacinės sistemos valdytojas paveda registro arba valstybės informacinės sistemos tvarkytojui paskirti saugos įgaliotinį. Saugos įgaliotinis gali būti paskiriamas keliems registrams, valstybės informacinėms sistemoms ar posistemiams. Saugos įgaliotinis ir šio įstatymo 8 straipsnyje nurodytas duomenų valdymo įgaliotinis gali būti tas pats asmuo. 3 d. Saugos įgaliotinis atlieka registro ar valstybės informacinės sistemos saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.	Nepaskirti šių Vidaus reikalų ministerijos valdomų ir naudojamų informacinių išteklių saugos įgaliotiniai: <ul style="list-style-type: none"> • SVIS (nuo 2015 m. pradžios); • NETAIS. 	Paskirti SVIS saugos įgaliotinį. Paskirti NETAIS saugos įgaliotinį.	2017-01-15 2017-10-15

⁸¹Lietuvos Respublikos vidaus reikalų ministro 2016-04-08 įsakymu Nr. 1V-272 patvirtinti Viešųjų ir administracinių paslaugų portalo ir analitinės informacinės sistemos nuostatai.

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas, 1999-11-25 Nr. VII-1443				
6.	40 straipsnis: ADA sistemų ir tinklų steigimas ir įteisinimas. <...> 3 d. Automatizuotai apdoroti ir perduoti įslaptintą informaciją galima tik įteisintomis ADA sistemomis ir tinklais. ADA sistemos ir tinklai laikomi įteisintais, kai paslapčių subjektui, jo rangovui (subrangovui) yra išduodamas leidimas automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais. Leidimą automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais išduoda Saugumo priežiūros tarnybos funkcijas atliekanti institucija ar žinybinė saugumo priežiūros tarnyba Saugumo priežiūros tarnybos funkcijas atliekančios institucijos nustatyta tvarka.	Informatikos ir ryšių departamentas naudoja ADA sistemas, tačiau neturi leidimo automatizuotai apdoroti įslaptintą informaciją su slaptumo žyma „Riboto naudojimo“.	Įteisinti Informatikos ir ryšių departamente naudojamą ADA darbo vietą.	2017-12-31
Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 (neteko galios 2013-03-02) patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės; Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 (galioja nuo 2013-03-03) patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas.				
7.	10. Patvirtinus informacinės sistemos nuostatus, rengiama informacinės sistemos specifikacija. Specifikacijos projektą rengia informacinės sistemos nuostatuose nurodytas informacinės sistemos valdytojas arba informacinės sistemos tvarkytojas. Specifikacijos projektas rengiamas vadovaujantis informacinės sistemos kūrimo metodiniais dokumentais. Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (23 p.).	Kuriant ar modernizuojant IS nebuvo parengtos šių IS: VRIS, N.SIS, N.VIS, SVIS, ADIS, ADGIS, specifikacijos.	Parengti / atnaujinti N.SIS, N.VIS, SVIS, ADIS, Vidaus reikalų integracinės platformos (reorganizavus VRIS). specifikacijas.	2017-10-30
8.	16. Užbaigus informacinės sistemos arba jos sudedamosios dalies (komponentės, posistemo) diegimą, informacinės sistemos valdytojo vadovas tvirtina informacinės sistemos priėmimo ir tinkamumo eksploatuoti aktą, kurio kopija per 5 darbo dienas nuo patvirtinimo pateikiama Komitetui. Informacinės sistemos valdytojas gali sudaryti komisiją atliktiems darbams įvertinti. Į komisijos sudėtį gali būti įtraukti suinteresuotų institucijų atstovai.	VRIS, N.SIS, N.VIS, SVIS, PASIS, ADIS, ADGIS sukurtos ir naudojamos, tačiau nepatvirtinti ir neįregistruoti šių IS ir registrų priėmimo ir tinkamumo eksploatuoti aktai.	Įteisinti (parengti / atnaujinti nuostatus, specifikacijas, priėmimo ir tinkamumo eksploatuoti aktus) N.SIS, N.VIS, SVIS, PASIS, ADIS. Reorganizuoti VRIS ir įsteigti valstybės informacinės sistemą – Vidaus reikalų integracinę platformą.	2017-10-30

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
	Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (30 p.).			
9.	17. Sprendimą modernizuoti informacinę sistemą priima informacinės sistemos valdytojas. Priėmęs sprendimą modernizuoti informacinę sistemą, informacinės sistemos valdytojas rengia informacinės sistemos nuostatų pakeitimo projektą. Jis derinamas ir tvirtinamas šių Taisyklių 5–8 ¹ p. nustatyta tvarka. [...] Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (33 p.).	Priėmus sprendimą modernizuoti VRIS, N.SIS, N.VIS, SVIS, jų nuostatai nebuvo atnaujinti.	Atnaujinti N.SIS, N.VIS, SVIS nuostatus. Reorganizavus VRIS parengti ir patvirtinti valstybės informacinės sistemos, Vidaus reikalų integracinės platformos, nuostatus.	2017-10-30
10.	23. Patvirtinus IS nuostatus, rengiama IS specifikacija; 29. IS kuriama ir diegiama pagal patvirtintą specifikaciją; 30. Baigus diegti IS arba jos dalį (komponentę, posistemį), IS valdytojo vadovas tvirtina IS priėmimo ir tinkamumo eksploatuoti aktą.	Eksplatuojamos SVIS, N.SIS, N.VIS neturi patvirtintų specifikacijų, priėmimo ir tinkamumo eksploatuoti aktų, t. y. nėra įteisintos. VRIS įteisinga 2002-10-21, tačiau neturi patvirtintos specifikacijos.	Įteisinti (parengti / atnaujinti nuostatus, specifikacijas, priėmimo ir tinkamumo eksploatuoti aktus) N.SIS, N.VIS, SVIS, PASIS, ADIS. Reorganizuoti VRIS ir įsteigti valstybės informacinės sistemą – Vidaus reikalų integracinę platformą.	2017-10-30
Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas 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 (akto redakcija galiojanti nuo 2013-08-08 iki 2016-08-18)				
11.	2. Nustatyti, kad valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų valdytojai peržiūri ir su šiuo nutarimu patvirtintų teisės aktų nuostatomis suderina savo valdomų registrų ir informacinių sistemų saugos dokumentus iki 2015-07-01 dienos.	Iki 2016-07-01 nebaigti rengti ir nepatvirtinti šių Vidaus reikalų ministerijos valdomų valstybės informacinių sistemų ir registrų: VRIS, N.SIS, N.VIS, UR, VRPR, IAŽR, NVŽR, HDR, ATPR, NETAIS, ARSIS, SVIS, KTPR, KTPVR, naujos redakcijos saugos dokumentai, atitinkantys Saugos dokumentų turinio gairių aprašą.	Atnaujinti ir patvirtinti N.SIS, N.VIS, UR, VRPR, IAŽR, NVŽR, HDR, ARSIS, SVIS (jei bus patvirtinti nuostatai), KTPR, KTPVR naujos redakcijos saugos politiką įgyvendinančius dokumentus. Parengti ir patvirtinti SVIS, PASIS, NETAIS saugos politiką įgyvendinančius dokumentus	2017-09-20 2017-11-01

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas (Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas Nr. 716, akto redakcija galiojanti nuo 2013-08-08 iki 2016-08-18); Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (patvirtinta Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716, Lietuvos Respublikos Vyriausybės 2016-08-11 nutarimo Nr. 826 redakcija galiojanti nuo 2016-08-19).				
12.	<p>4. Elektroninė informacija pagal svarbą skirstoma į 4 kategorijas: ypatingos svarbos elektroninė informacija, svarbi elektroninė informacija, žinybinės svarbos elektroninė informacija ir kita elektroninė informacija (Redakcija iki 2016 08 19).</p> <p>4. Informacijos svarba nustatoma pagal jos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamą poveikį valstybės ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 1 straipsnio 3 dalyje nurodytų institucijų (toliau – institucijos) veiklai.</p> <p>6. Įvertinus informacijos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamą poveikį, informacija priskiriama vienai iš 4 kategorijų:</p> <p>6.1. ypatingos svarbos informacija;</p> <p>6.2. svarbi informacija;</p> <p>6.3. vidutinės svarbos informacija;</p> <p>6.4. mažiausios svarbos informacija. (redakcija nuo 2016 08 19)</p>	<p>VRIS, N.SIS, N.VIS, VRPR, IAŽR, NVŽR, HDR, NETAIS, ARSIS, SVIS, KTPR, KTPVR informacinėse sistemose elektroninė informacija pagal svarbą nėra skirstoma.</p> <p>Pastaba: vadovautasi vidaus reikalų ministro 2007-07-11 įsakymu Nr. 1V-247 patvirtintomis Informacinių sistemų klasifikavimo gairėmis, kur toks reikalavimas nenumatytas.</p>	Analogiškos 11 p. priemonės.	2017-09-20
Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas Nr. 716, aktuali akto redakcija, galiojanti nuo 2016-08-19)				
13.	<p>19. Informacinės sistemos valdytojas teisės aktu, kuriuo tvirtinami Saugos nuostatai, skiria saugos įgaliotinį arba paveda jį paskirti informacinės sistemos tvarkytojui.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>	<p>Nepaskirti šių Vidaus reikalų ministerijos valdomų ir eksploatuojamų informacinių išteklių saugos įgaliotiniai:</p> <ul style="list-style-type: none"> • SVIS (nuo 2015 m. I ketvirčio); • NETAIS. 	Analogiškos 5 p. priemonės.	2017-10-15
Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas Nr. 716, aktuali akto redakcija, galiojanti nuo 2016-08-19)				
14.	<p>7. Informacinės sistemos valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus:</p>	<p>Nepatvirtinti saugos dokumentai NETAIS. PASIS ir SVIS neturi parengtų ir patvirtintų saugos politiką įgyvendinančių dokumentų</p>	<p>Parengti ir patvirtinti SVIS, PASIS, NETAIS saugos politiką įgyvendinančius dokumentus.</p>	2017-09-20

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
	<p>7.1. Saugos nuostatus; 7.2. Saugaus elektroninės informacijos tvarkymo taisyklės; 7.3. Informacinės sistemos veiklos tęstinumo valdymo planą; 7.4. Informacinės sistemos naudotojų administravimo taisyklės.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>			
15.	<p>21. Atlikdami informacinės sistemos funkcijų pakeitimus, administratoriai turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos. (redakcija iki 2016-08-19);</p> <p>28. Atlikdamas (-i) informacinės sistemos sąrankos pakeitimus, administratorius (administratoriai) turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos, nustatytos informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse (redakcija nuo 2016-08-19).</p>	Neparengtos N.VIS, NETAIS, IBPS, SVIS, PASIS, JKNR, ir VRIS sistemoje esančių registų: UR, VRPR, ARSIS, JAŽR, HDR ir NVŽR, pokyčių tvarkos.	Atnaujinti Vidaus reikalų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarką.	2016-12-31
16.	<p>35. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje (http://vrm.lrv.lt/uploads/vrm/documents/files/Rizikos_analize.pdf), Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>	JKNR, SVIS ir NETAIS rizikos vertinimai 2013–2015 m. nebuvo atlikti.	Kasmet atlikti Vidaus reikalų ministerijos valdomų IS rizikos vertinimus.	2017-12-31

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
17.	<p>37. Atsižvelgdamas į rizikos įvertinimo ataskaitą, informacinės sistemos valdytojas prirėkė tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>	<p>Atlikus rizikos vertinimą, rengiami ministerijos valdomų informacinių išteklių rizikos valdymo priemonių planų projektai, tačiau jie netvirtinami valdytojo, juose nenumatomi priemonių įgyvendinimo terminai ir nenurodomi atsakingi vykdytojai.</p>	<p>Atsižvelgiant į IS rizikos vertinimo ataskaitas rengti ir tvirtinti rizikos valdymo priemonių planus.</p>	2017-12-31
18.	<p>39. Informacinės sistemos valdytojas užtikrina informacinės sistemos pokyčių (toliau – pokyčiai) valdymo planavimą, apimančią pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą ir pokyčių prioritetų nustatymo procesus. Su tuo susijusios nuostatos turi būti numatomos informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse ar kitame informacinės sistemos valdytojo patvirtintame teisės akte.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>	<p>Vidaus reikalų ministro įsakymais patvirtinti tik VRIS ir N.SIS pokyčių valdymo tvarkos aprašai. Tvarkos nebeatitinka aktualių teisės aktų normų, apibrėžiančių IS pokyčių valdymą (pvz., IS pokyčių suskirstymas į kategorijas pagal pokyčio tipą, įtakos vertinimas ir pokyčių prioritetų nustatymas).</p>	<p>Atnaujinti ir patvirtinti Vidaus reikalų ministerijos valdomų informacinių išteklių IT pokyčių valdymo tvarką.</p>	2016-12-31
19.	<p>44. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.</p> <p>Analogiškas reikalavimas buvo ir akto redakcijoje, galiojusioje nuo 2013-08-08 iki 2016-08-19.</p>	<p>Ataskaitos ir trūkumų šalinimo planų projektai rengiami, tačiau nėra tvirtinami IS valdytojo vadovo. Nebuvo atliekamas SVIS ir NETAIS atitikties vertinimas.</p>	<p>Atlikus informacinių technologijų saugos atitikties vertinimą, ministerijos vadovybei teikti tvirtinti trūkumų šalinimo planus.</p>	2017-12-31

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-10-15 įsakymu Nr. T-131 (neteko galios 2014-02-26) patvirtinta Valstybės informacinių sistemų kūrimo metodika; Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29 (galioja nuo 2014-02-26) patvirtinta Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika.				
20.	26. Saugos dokumentai valstybės institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Vidaus reikalų ministerija.	Rečiau kaip kartą per metus Vidaus reikalų ministerijoje nebuvo persvarstomi (peržiūrimi) šių informacinių išteklių: VRIS, N.SIS, N.VIS, VRPR, IAŽR, NVŽR, HDR, NETAIS, SVIS, KTPR, KTPVR, saugos politiką įgyvendinantys dokumentai.	Ne rečiau kaip kartą per metus persvarstyti (peržiūrėti) IS saugos dokumentus.	
Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai (LRV 2013-10-04 nutarimas Nr. 1V-832, aktuali akto redakcija, galiojanti nuo 2013-10-11).				
21.	5.12.12. informacinės sistemos valdytojo tvirtinamuose informacinės sistemos duomenų saugos nuostatuose nustatyta tvarka turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti saugomos kitose patalpose nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;	Atsarginių kopijų darymo įrenginys yra tarnybinių stočių patalpose. Atsarginės kopijos saugomos ir tarnybinių stočių patalpose ⁸² .	Parengti ir patvirtinti elektroninės informacijos ir informacinių sistemų programinės įrangos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašą. Užtikrinti techninę įrangą, skirtą atsarginių elektroninės informacijos ir informacinių sistemų programinės įrangos kopijų saugojimui ir patalpinti kitose patalpose nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota.	2016-12-31 2018-10-01
22.	5.12.14. atsarginės laikmenos su informacinės sistemos programinės įrangos kopijomis turi būti laikomos kitose	Atsarginės programinės įrangos kopijos saugomos ir tarnybinių stočių patalpose	Analogiškos 21 p. priemonės.	

⁸² Vidaus reikalų informacinės sistemos (VRIS), Lietuvos nacionalinės Šengeno informacinės sistemos (N.SIS), Lietuvos nacionalinės vizų informacinės sistemos (N.VIS) informacinių technologijų saugos atitikties vertinimo ataskaita, 2015-01-05 Nr. (6-7)12R-7, 23, 25 p.

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai	Vidaus reikalų ministerijos pasirinktos neatitikties pašalinimo priemonės	Numatoma neatitikties pašalinimo data
	patalpose arba kitame pastate nei yra informacinės sistemos tarnybinės stotys;			
23.	5.14. reikalavimai prisijungimo prie visų kategorijų informacinių sistemų slaptažodžiams: 5.14.1. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;	VRIS CDB naudotojų paskyrų valdymo procesas, naudojant ADMIN III administravimo posistemį, neleidžia naudoti specialiųjų simbolių.	Atlikti Naudotojų administravimo posistemės ADMIN III slaptažodžių sudarymo analizę ir užtikrinti specialiųjų simbolių naudojimą pagal baigtinį sąrašą.	2016-12-15
24.	5.14.6. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu, ar užšifruojami nepatikimais algoritmais; saugos įgaliojimo sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo.	Nešifruojami.	Patobulinti taikomąją programinę įrangą, naudojamą slaptažodžių perdavimui.	2018-12-31

Valstybinio audito ataskaitos
 „Vidaus reikalų ministerijos informacinių
 išteklių valdymas“
 4 priedas

Vidaus reikalų ministerijos ir Informatikos ryšių departamento valdomi informaciniai ištekliai

Nr.	Pavadinimas	Informacijos svarba (kategorija)	Nuostatai	Specifikacija	Įteisinta	Duomenų saugos nuostatai	Saugos politiką įgyvendinantys dokumentai	Paskirtas saugos įgaliojimas	Paskirtas duomenų valdymo įgaliojimas	Vertinama rizika	Atliekamas saugos atitikties vertinimas	Ar apibrėžtas pokyčių valdymas
1.	VRIS – Vidaus reikalų informacinė sistema	I – ypatingos svarbos	Yra (neatnaujinti)	Nėra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
2.	UR – Užsieniečių registras	I – ypatingos svarbos	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
3.	IAŽR – Ieškomų asmenų, neatpažintų lavonų ir nežinomų bejėgių asmenų žinybinis registras	I – ypatingos svarbos	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
4.	NVŽR – Nusikalstamų veikų žinybinis registras	I – ypatingos svarbos	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Taip	Taip	Taip	Taip (neatnaujinta)
5.	ATPR – Administracinių teisės pažeidimų registras	I – ypatingos svarbos	Yra	Yra	Taip	Yra	Yra	Taip	Ne	Taip	Taip	Yra
6.	N.SIS – Lietuvos nacionalinė Šengeno informacinė sistema	I – ypatingos svarbos	Yra (neatnaujinti)	Nėra	Ne	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
7.	N.VIS – Lietuvos nacionalinė vizų informacinė sistema	I – ypatingos svarbos	Yra (neatnaujinti)	Nėra	Ne	Yra	Yra	Taip	Ne	Taip	Taip	Taip
8.	IBPS – Integruota baudžiamojo proceso informacinė sistema	I – ypatingos svarbos	Yra	Yra	Taip	Yra	Yra	Taip	Ne	Taip	Taip	Taip

Nr.	Pavadinimas	Informacijos svarba (kategorija)	Nuostatai	Specifikacija	Įteisinta	Duomenų saugos nuostatai	Saugos politiką įgyvendinantys dokumentai	Paskirtas saugos įgaliotinis	Paskirtas duomenų valdymo įgaliotinis	Vertinama rizika	Atliekamas saugos atitikties vertinimas	Ar apibrėžtas pokyčių valdymas
9.	ĮKNR – Įtariamųjų, kaltinamųjų ir nuteistųjų registras ⁸³	I – ypatingos svarbos	Yra	Yra	Taip	Yra	Yra	Taip	Taip	Ne	Taip	Taip
10.	VRPR – Vidaus reikalų pareigūnų registras	II – svarbi	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
11.	HDR – Habitoskopinių duomenų registras	II – svarbi	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Ne
12.	ARSIS – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistema	II – svarbi	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip (neatnaujinta)
13.	SVIS – Sertifikatų valdymo informacinė sistema	II – svarbi	Yra (neatnaujinti)	Nėra	Ne	Yra (neatnaujinti)	Nėra	Ne	Ne	Ne	Ne	Ne
14.	Lietuvos Respublikos kelių transporto priemonių registras	II – svarbi	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip
15.	Lietuvos Respublikos kelių transporto priemonių vairuotojų registras	II – svarbi	Yra	Yra	Taip	Yra (neatnaujinti)	Yra (neatnaujinti)	Taip	Ne	Taip	Taip	Taip
16.	PASIS – Viešųjų ir administracinių paslaugų stebėsenos ir analizės informacinė sistema	III – vidutinės svarbos	Yra	Yra	Ne	Yra	Nėra	Taip	Taip	Taip	Taip	Ne
17.	NETAIS – Nacionalinės elektroninės atpažinties informacinė sistema	Nenustatyta	Yra	Yra	Taip	Nėra	Nėra	Ne	Taip	Ne	Ne	Ne

⁸³ Valdytojas – Informatikos ir ryšių departamentas.