Valstybinio audito ataskaita

BIOMETRINIŲ ASMENS DOKUMENTŲ GAMYBA

2015 m. kovo 27 d. Nr. VA-P-90-2-6

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

TURINYS

SANTRUMPOS IR SĄVOKOS 4

SANTRAUKA 5

IŠVADOS 6

REKOMENDACIJOS 7

ĮŽANGA 8

AUDITO REZULTATAI 11

1. Asmens tapatybės dokumentų gamybos vertinimas 11

1.1. Asmens tapatybės dokumentų užsakymas / keitimas 11

1.2. Asmens ir biometrinių duomenų surinkimas 13

1.3. Asmens tapatybės dokumentų gamyba 17

1.4. Asmens tapatybės dokumentų pristatymas 21

1.5. Asmens tapatybės dokumentų naikinimas 22

2. Kitų su biometrinių asmens tapatybės dokumentų išdavimu susijusių procesų vertinimas 26

2.1. IS/ IT infrastruktūros ir informacijos valdymas 26

2.2. Atitiktis teisės aktų ir kitiems reikalavimams 35

2.3. Kaštų ir naudos analizė 36

2.4. Žmogiškųjų išteklių valdymas 38

PRIEDAI 40

SANTRUMPOS IR SĄVOKOS

ADIC –Asmens dokumentų išrašymo centras prie Vidaus reikalų ministerijos.

ADIS – Asmens dokumentų išrašymo informacinė sistema.

ADGIS – Asmens dokumentų gamybos informacinė sistema.

Autorizacija (angl. *authorisation*) – šioje ataskaitoje apima ne tik teisių asmeniui ar programai suteikimą atlikti kai kuriuos veiksmus duomenų apdorojimo sistemoje, bet ir asmens tapatybės nustatymą ir pripažinimą, duomenų patikrinimą ir patvirtinimą, lyginant įrašus arba įrašą ir jo etaloną.

ICAO – Tarptautinė civilinės aviacijos organizacija (TCAO; angl. *International Civil Aviation Organization*) – Jungtinių Tautų Organizacijos sukurta organizacija, nustatanti tarptautines normas, kordinuojanti aviacijos vystymą, reguliuojanti saugių ir efektyvių skrydžių sritis.

IS – informacinė sistema.

IT – informacinės technologijos.

PKI – viešojo rakto infrastruktūra (VRI, angl. *Public Key Infrastructure PKI*) yra techninės, programinės įrangos, žmonių ir procedurų visuma, kuri naudojama saugoti, kurti, valdyti, suteikti, atnaujinti sertifikatus viešojo rakto kriptografijos metodais.

VPN – virtualus privatus tinklas (angl. *Virtual Private Network* VPN), atskirų, nutolusių vienas nuo kito kompiuterinių tinklų sujungimas į vieną tinklą internetu.

SANTRAUKA

Biometriniai duomenys naudojami nustatyti asmens tapatybę, vykdant keleivių patikrą oro uostuose, teisėsaugos institucijų veikloje, Europos Sąjungos išorinę sieną kertančių trečiųjų šalių piliečių patikrai, įeigos kontrolės ir kt. informacinėse sistemose. Siekiant palengvinti asmens tapatybės nustatymą skaitmeniniu būdu tarptautiniai standartai rekomenduoja į asmens dokumentus integruoti elektroninį mikroelementą, kuriame būtų įrašyta papildoma asmens biometrinė informacija (pvz., veido geometrijos, pirštų atspaudų arba akies rainelės parametrai, skaitmeninė nuotrauka). Jame gali būti ir papildoma informacija, pvz., elektroninis parašas. Lietuvoje išduodami aštuonių rūšių asmens tapatybės dokumentai su biometriniais duomenimis.

Valstybės politiką asmens dokumentų išrašymo srityje formuoja Vidaus reikalų ministerija[1], įgyvendina Asmens dokumentų išrašymo centras[2]. Iki 2015 m. vasario 1 d. centras jau išrašė 7 047 019 naujos kartos Lietuvos Respublikos asmens tapatybės dokumentų. Įgyvendinant politiką dalyvauja ir Gyventojų registro tarnyba prie Teisingumo ministerijos[3], Policijos departamentas, Migracijos departamentas ir Užsienio reikalų ministerija.

Asmens tapatybės dokumentų išdavimo procese dalyvaujančios įstaigos naudoja bendrą Asmens dokumentų išrašymo informacinę sistemą ADIS, kuri veikia Gyventojų registro pagrindu, todėl leidžia užtikrinti duomenų patikimumą ir veiksmų atsekamumą. Centro užsakymu 2013 ir 2014 m. privati įmonė atliko atitikties ISO/IEC 27001:2005 priežiūros auditus. Nenustatyta neatitikčių standarto reikalavimams ir pateikta išvada, kad informacijos saugumo valdymo sistema įdiegta tinkamai ir saugos lygis geras. Informacijos saugumo valdymo sistemos sertifikavimą pagal ISO/IEC 27001:2005 reikalavimus nustatytai sričiai rekomenduota pratęsti. Įvertinus biometrinių asmens tapatybės dokumentų išdavimo procesą esminių trūkumų nenustatyta, išskyrus pateiktus pastebėjimus.

Biometrinių asmens dokumentų gamybos auditas – tarptautinio audito dalis, kuriame dalyvavo Belgijos, Latvijos, Lietuvos, Norvegijos, Portugalijos ir Šveicarijos aukščiausiosios audito institucijos. Tarptautinio audito tikslas – įvertinti biometrinių asmens tapatybės dokumentų gamybos valdymą ir kontrolę. Pagal Šveicarijos aukščiausiosios audito institucijos parengtą programą vertinome, ar Lietuvoje tinkamai įgyvendinamas dokumentų gamybos procesas, ar užtikrinama, kad šie dokumentai būtų patikimi ir saugūs.

Pagrindiniu audito subjektu pasirinkta Vidaus reikalų ministerija, kuri rengia asmens dokumentų išrašymo sričių įstatymų projektus, prižiūri, kaip įgyvendinama valstybės politika pagrindinių asmens dokumentų išrašymo srityje. Audito procedūros atliktos Asmens dokumentų išrašymo centre prie Vidaus reikalų ministerijos, kuris įgyvendina valstybės politiką asmens dokumentų išrašymo srityje, užtikrina teisės aktų ir tarptautinių standartų reikalavimus atitinkančių asmens dokumentų projektavimą, gamybą ir išrašymą; užtikrina funkcionavimą ir plėtrą viešojo rakto infrastruktūros, būtinos biometrinių asmens duomenų į asmens dokumento elektroninę

[1] Lietuvos Respublikos Vyriausybės 2001-03-14 nutarimu Nr. 291 (2010-10-13 Nr. 1465 redakcija) patvirtintų Lietuvos Respublikos vidaus reikalų ministerijos nuostatų 9.1. ir 9.8 p.

[2] Lietuvos Respublikos vidaus reikalų ministro 2011-02-07 įsakymu patvirtintų Asmens dokumentų išrašymo centro prie Vidaus reikalų ministerijos nuostatų II skyrius.

[3] Lietuvos Respublikos teisingumo ministro 2014-07-02 įsakymu Nr. 1R-205 patvirtinti Gyventojų registro tarnybos nuostatai, II skyrius. Iki 2014-10-01 galiojo Lietuvos Respublikos vidaus reikalų ministro 2011-02-07 įsakymu Nr. 1V-100 patvirtinti nuostatai.

laikmeną įrašymui bei patikrai. Audituojamas laikotarpis – 2013–2014 m. I pusmetis. Informaciją surinkome iš Užsienio reikalų ministerijos, Migracijos departamento prie Vidaus reikalų ministerijos ir Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdybos.

Audito metu nebuvo atliktas detalusis biometrinių duomenų šifravimo, apsikeitimo sertifikatais ir taikomų kriptografinių priemonių efektyvumo įvertinimas, nevertinta jautrių duomenų apdorojimo atitiktis įslaptintos informacijos apdorojimo reikalavimams.

Įvertinę surinktus įrodymus, pateikiame valstybinio audito išvadas ir rekomendacijas.

IŠVADOS

1. Biometriniai asmens tapatybės dokumentai išrašomi ir išduodami naudojant neįteisintą Asmens dokumentų išrašymo informacinę sistemą ADIS, neaprašytos saugos procedūros, nepaskirtas sistemos valdytojas, todėl nėra bendro įrangos priežiūros ir sistemos plėtros valdymo. Valstybės mastu biometrinių asmens tapatybės dokumentų išrašymo ir išdavimo procese dalyvaujančios įstaigos nevertina ar šių dokumentų išdavimo procesas (operacijų, saugumo, IS / IT valdymas) efektyvus, neturi duomenų apie kitų dalyvaujančių įstaigų patiriamus kaštus (2.1 ir 2.3 poskyriai).
2. Asmens dokumentų išrašymo centras nesilaiko kai kurių IS/IT valdymo teisės aktų reikalavimų (IS kūrimo, saugos užtikrinimo ar atsakingų asmenų paskyrimo procedūrų). Iki šiol tai neturėjo neigiamų pasekmių: nenustatyta finansinių nuostolių ar duomenų praradimo atvejų (2.1 ir 2.2 poskyriai).
3. Sutarčių su asmens dokumentų išrašymo ir programinės įrangos priežiūros paslaugų teikėjais trūkumai gali turėti įtakos asmens dokumentų išrašymui, nes sutartyse nenumatyta sutrikimų šalinimo ir maksimalaus įrangos dalinio funkcionavimo atstatymo laiko, taip pat nenumatytas laikas, per kurį paslaugų teikėjas įsipareigotų reaguoti įrangos gedimo atveju, o kritinio IT gedimo atveju nebūtų vykdomas asmens dokumentų išdavimas (2.1 ir 2.2 poskyriai).
4. Šalyje sukurtos priemonės padedančios užtikrinti sklandų biometrinių asmens tapatybės dokumentų išdavimą, duomenų patikrą ir prarastų dokumentų naikinimą, tačiau:
   4.1. asmenys nepakankamai informuojami apie biometrinių duomenų patikros galimybę atsiimant pagamintus asmens tapatybės dokumentus;
   4.2. sukurta pranešimo apie prarastą asmens tapatybės dokumentą el. paslauga leidžia asmenims bet kuriuo paros metu informuoti apie dokumento praradimą. Prarastų dokumentų skelbimo negaliojančiais procedūros vykdomos tik darbo dienomis, todėl asmens tapatybės dokumentu gali būti pasinaudota neteisėtai (1.5 poskyris).

REKOMENDACIJOS

Vidaus reikalų ministerijai

1. Paskirti asmens tapatybės dokumentų išrašymo ir išdavimo procesų valdytoją, kuris užtikrintų šių procesų išteklių ir kaštų valdymą. Užtikrinti, kad įstaigų dalyvaujančių asmens tapatybės dokumentų išrašymo ir išdavimo procesuose, naudojama įranga būtų tinkamai prižiūrima, centralizuotai planuojamas jos atnaujinimas siekiant išvengti nesuderinamumo (1 išvada).
2. Siekiant užtikrinti vientisą Asmens dokumentų išrašymo informacinės sistemos plėtrą, nustatyti IT valdymo atsakomybę – paskirti sistemos valdytoją, tvarkytojus ir duomenų valdymo įgaliotinį. Įteisinti naudojamą sistemą, parengiant teisės aktų reikalaujamus dokumentus, kuriuose būtų fiksuota sistemos tvarkomų duomenų apimtis, ryšiai su kitomis sistemomis / registrais ir numatytos taikytinos saugos užtikrinimo procedūros (1, 2 išvada).
3. Siekiant geriau išnaudoti sukurtų paslaugų galimybes, informuoti asmenis apie galimybę el. būdu pranešti apie dingusį asmens tapatybės dokumentą ir vietas, kur galima patikrinti biometrinius duomenis, atsiimant pagamintus dokumentus (4 išvada).

Asmens dokumentų išrašymo centrui prie Vidaus reikalų ministerijos

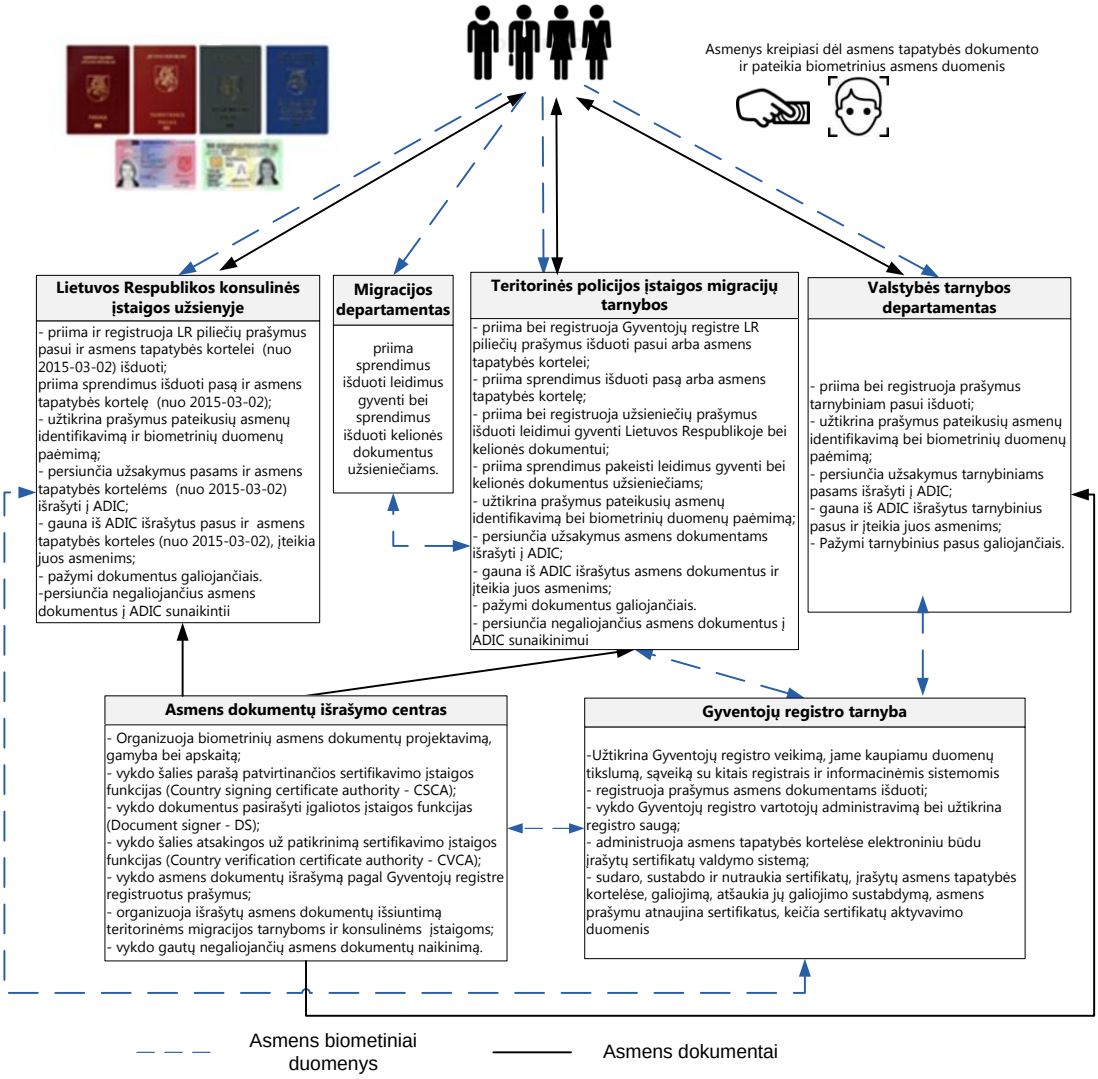
4. Siekiant užtikrinti reikiamą saugos reikalavimų įgyvendinimą, įgyvendinti trūkstamas IT saugos priemones ir peržiūrėti Asmens dokumentų išrašymo centro IT veiklos tęstinumo reikalavimus (2 išvada).
5. Siekiant užtikrinti, kad trečiųjų šalių paslaugos atitiktų veiklos poreikius: sutartyse su trečiosiomis šalimis dėl IT paslaugų nustatyti teisės aktų reikalavimus atitinkančias sąlygas, įtraukti nuostatas dėl paslaugų teikėjų veiklos kontrolės ir atsakomybės (3 išvada).

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti 2 priede.

ĮŽANGA

Biometrinių asmens tapatybės dokumentų gamybos procesą (žr. 1 pav.) Lietuvoje reglamentuoja teisės aktai, kurie nustato reikalavimus dokumentams, asmenų, norinčių gauti asmens tapatybės dokumentus pareigas ir teises, taip pat dokumentų išdavimo procese dalyvaujančių įstaigų procedūras[4].

1 pav. Biometrinių asmens tapatybės dokumentų gamybos procesas



Šaltinis – Valstybės kontrolė pagal ADIC pateiktą informaciją.

Asmens tapatybės nustatymo procedūrose naudojami biometriniai identifikatoriai – skiriamosios ir išmatuojamos savybės, naudojamos žymėti ir apibūdinti asmenį. Lietuvoje išduodami aštuonių rūšių asmens tapatybės dokumentai su biometriniais duomenimis: Lietuvos Respublikos pasas, asmens tapatybės kortelė, Lietuvos Respublikos tarnybinis pasas, Lietuvos Respublikos užsieniečio pasas, asmens be pilietybės kelionės dokumentas, pabėgėlio kelionės dokumentas, leidimai gyventi Lietuvoje (leidimas laikinai gyventi Lietuvos Respublikoje ir leidimas nuolat

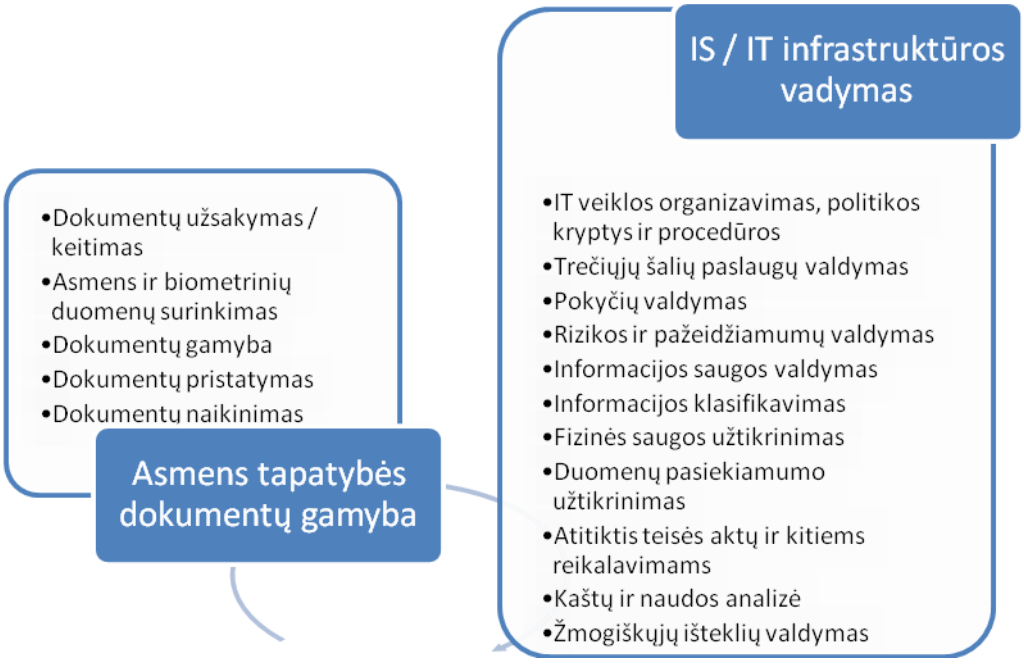
[4] Lietuvos Respublikos paso įstatymas, 2001-11-08 Nr. IX-590, Lietuvos Respublikos asmens tapatybės kortelės įstatymas, 2001-11-06 Nr. IX-577 ir Valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807.

gyventi Lietuvos Respublikoje) ir Lietuvos Respublikos diplomatinis pasas. Į jų nekontaktines elektronines laikmenas įrašomi asmens veido atvaizdas ir pirštų atspaudai. Veido atvaizdas įrašomas JPEG2000 formatu ir atitinka asmens tapatybės dokumente esantį veido atvaizdą. Informacija apie šalies sertifikavimo tarnybos (CSCA tarnyba[5]) sertifikatą publikuojama interneto tinklalapyje: www.csca.lt. Sertifikatai, skirti sertifikuoti pirštų atspaudų nuskaitymo įrangą, išduodami dvišalių sutarčių pagrindu.

Vadovaujantis 2004-12-13 Europos Tarybos reglamentu Nr. 2252/2004, nustatančiu valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartus, Asmens dokumentų išrašymo centre nuo 2006-08-28 įsteigtos šalies sertifikavimo tarnyba (CSCA tarnyba), kurios paskirtis – sertifikuoti dokumentus pasirašančias institucijas ir – Asmens dokumentų išrašymo centre išrašomiems dokumentams – Dokumento pasirašymo sertifikavimo tarnyba (DSCA tarnyba[6]), kuri sertifikuoja išrašomą biometrinį dokumentą pasirašančios institucijos parašus. Į biometrinį dokumentą įrašomas CSCA sertifikatas naudojamas dokumento patikros metu nustatyti asmens dokumentą išdavusią valstybę. Į biometrinį dokumentą įrašomas DSCA sertifikatas naudojamas dokumento patikros metu nustatyti biometrinį dokumentą išrašiusią instituciją.

Audito metu nagrinėtas biometrinių asmens tapatybės dokumentų išdavimo procesas ir su juo susijusios informacinių technologijų infrastruktūros valdymo sritys (2 pav.).

2 pav. Nagrinėtos biometrinių asmens tapatybės dokumentų išdavimo proceso sritys



Šaltinis – Valstybės kontrolė pagal Šveicarijos aukščiausiosios audito institucijos medžiagą

Kiekvienos srities įvertinimas pateikiamas pagal nustatytų trūkumų rizikos lygį, atsižvelgiant į taikomus kriterijus (žr. 1 lentelę kitame lape).

[5] CSCA tarnyba – parašą patvirtinanti Lietuvos Respublikos sertifikavimo įstaiga, kurios funkcija išduoti sertifikatus dokumentus pasirašyti įgaliotai įstaigai.

[6] DSCA tarnyba – dokumentus pasirašyti įgaliota įstaiga.

1 lentelė. Taikyti įvertinimai pagal nustatytų trūkumų rizikos lygį

Įvertinimo ženklinimas	Rizikos lygių aprašymas
●	Maža rizika, kai: ▪ kiti kontrolės trūkumai ▪ yra galimybė tobulinti ir optimizuoti procesus ir kontrolės priemones
■	Vidutinė rizika, kai: ▪ svarbiausių procesų ir kontrolės priemonių trūkumai atsirado dėl kontrolės silpnumo ▪ vidutinė įtaka siekiant veiklos ir įstaigos tikslų ▪ neatitiktis neturės neigiamų pasekmių susijusių su: □ reglamentais, potvarkiais, teisės aktais □ vidaus nuostatomis, finansais, reputacija □ duomenų privatumu ir duomenų apsauga
▲	Didelė rizika, kai: ▪ svarbiausių procesų ir kontrolės priemonių trūkumai atsirado dėl reikšmingo kontrolės silpnumo ▪ reikšminga įtaka siekiant veiklos ir įstaigos tikslų ▪ neatitiktis gali turėti neigiamų pasekmių susijusių su: □ reglamentais, potvarkiais, teisės aktais □ vidaus nuostatomis, finansais, reputacija □ duomenų privatumu ir duomenų apsauga
◆	Svarbūs aspektai, neįtraukti į biometrinių pasų audito apimtį (neaktualūs / platesni nei šio audito apimtis)
/1	Nebaigti nagrinėti klausimai / tolesnio nagrinėjimo reikalaujantys arba atviri klausimai

AUDITO REZULTATAI

1. ASMENS TAPATYBĖS DOKUMENTŲ GAMYBOS VERTINIMAS

Asmens tapatybės dokumentų gamybos procesas (3 pav.) vertintas pagal tarptautinio audito programoje numatytus kriterijus, atsižvelgiant į teisės aktų reikalavimus ir gerąją praktiką.

3 pav. Vertinti asmens tapatybės dokumentų gamybos etapai

Šaltinis – Valstybės kontrolė

1.1. Asmens tapatybės dokumentų užsakymas / keitimas

Vertintas biometrinių asmens dokumentų užsakymo / keitimo procesas (naujo dokumento gavimas, baigusio galioti dokumento keitimas, pamesto dokumento keitimas, dokumento keitimas sudarius santuoką, gimus vaikui ir kt.), įsitikinant, kad:

- užsakymai priimami tik iš asmenų, kurie turi teisę gauti minėtą dokumentą;
- dokumentų įrašų pakeitimai ar papildymai yra galiojantys ir teisingi;
- išimčių procesas ir taikomos kontrolės priemonės sukurtos atsižvelgiant į svarbiausią riziką (praradimo, netinkamo naudojimo ir kt.).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
1.1 Autorizacija	Neturintys teisės gauti asmens tapatybės dokumentą asmenys užsako ir gauna asmens tapatybės dokumentą.	Lietuvoje naudojama centralizuota biometrinių asmens dokumentų išdavimo informacinė sistema, kuri veikia Gyventojų registro pagrindu, joje pildomi ir saugomi visų asmens tapatybės dokumentų užsakymo prašymai. Asmens tapatybės dokumento užsakymo prašymas parengiamas tik pagal Gyventojų registre esančius asmens duomenis, o asmuo parašu patvirtina, kad pateikta informacija yra teisinga. Visi Lietuvos Respublikos piliečiai, gyvenamąją vietą Lietuvos Respublikoje deklaruojantys asmenys, taip pat asmenys be pilietybės ar kitos valstybės piliečiai, kurių duomenys tvarkomi Gyventojų registre ir dėl kurių priimtas sprendimas išduoti asmens tapatybės dokumentą, gali gauti naują ar pasikeisti turimą asmens tapatybės dokumentą. Migracijos tarnybų ar konsulinių įstaigų darbuotojai, priimdami prašymus išduoti / pakeisti dokumentus įvertina asmens pateiktus dokumentus, ar juose nėra klastojimo požymių, įsitikina asmens tapatybe ir sutikrina duomenis su Gyventojų registre esančiais duomenimis, kurie leidžia maksimaliai unifikuoti įrašus asmens tapatybės dokumentuose. Priimant prašymą susiduriama su subjektyviu veido panašumų / skirtumų vertinimu, todėl išlieka rizika dėl žmogiškųjų klaidų. Migracijos tarnybų ir konsulinių įstaigų taikomos priemonės veiksmingos, nes 2009–2014 m. buvo du atvejai (tai sudaro tik 0,00006 proc.), kai asmenims apgaulės būdu pavyko užsakyti ir atsiimti kito asmens vardu užsakytus asmens tapatybės dokumentus.	● Maža rizika
1.2 Kokybė (keičiant asmens tapatybės dokumentus)	Neteisėti pokyčiai arba neteisingos informacijos naudojimas asmens tapatybės dokumentuose.	Teisės aktuose yra nustatytos kontrolės procedūros užtikrinančios asmens duomenų patikslinimą, taisymą ir dokumentų pakeitimą. Asmens duomenų įrašai prašyme išduoti / pakeisti asmens tapatybės dokumentą atliekami pagal įrašus Gyventojų registre. Auditoriai įsitikino, kad nėra galimybės atspausdinti asmens tapatybės dokumentą su kitokiais asmens duomenimis, nei yra Gyventojų registre, nes įstaigos išduodančios minėtus dokumentus neturi teisių pakeisti registre esančių duomenų. Norėdamas gauti asmens tapatybės dokumentą su pasikeitusiais asmens duomenimis (asmens kodu, vardu ar pavarde, lytimi ir kt.), asmuo privalo iš anksto kreiptis į atsakingas institucijas, kurios nustatyta tvarka įrašys, papildys ar pakeis registro duomenis. Išskirtinais ir skubiais atvejais Migracijos tarnybos įstaigos priima prašymo užsakymą ir kreipiasi į Gyventojų registrą dėl duomenų patikslinimo, juos patikslintus, pildomas prašymas. Jei registre nėra duomenų apie asmenį, nėra galimybės užsakyti asmens tapatybės dokumentą.	● Maža rizika
1.3 Išimtys	Standartiniai procesai negali būti taikomi.	Kai asmuo, praradęs išduotą asmens tapatybės dokumentą, nori užsakyti kitą, taikomos papildomos kontrolės procedūros, kurios apgaulės riziką sumažina iki priimtino lygio. Priimant prašymą asmens tapatybės kortelei ar pasui gauti vietoj prarasto dokumento, Migracijos tarnybos darbuotojas siekdamas įsitikinti asmens tapatybe pateikia kontrolinius klausimus apie gimimo datą, vietą, motinos mergautinę pavardę, motinos ir / ar tėvo gimimo datą, santuokos datą, deklaruotą gyvenamąją vietą, vaikų gimimo datą, senelių vardus. Asmens atsakymai patikrinami pagal Gyventojų registro duomenis, palyginamos ankstesniuose prašymuose esančios	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		nuotraukos su besikreipiančio asmens veido atvaizdu, asmens išvaizdoje ieškoma defektų, panašumų ir skirtumų.	

Lietuvoje veikianti biometrinių asmens dokumentų užsakymo sistema užtikrina, kad asmuo turi teisę užsakyti asmens tapatybės dokumentą, veikia teisinės ir techninės kontrolės priemonės užtikrinančios, kad į asmens tapatybės dokumentus įrašomi duomenys yra tikri ir teisingi.

1.2. Asmens ir biometrinių duomenų surinkimas

Vertinti asmens tapatybės nustatymo, autorizacijos patvirtinimo, asmens ir biometrinių duomenų rinkimo, biometrinių dokumentų šablono rengimo, surinktų duomenų paruošimo ir apdorojimo procesai, įsitikinant, kad:

- asmuo užsakantis naują asmens tapatybės dokumentą yra tas, kurio duomenis jis pateikia;
- asmens tapatybės dokumentas gali būti sukurtas ir pagamintas tik pagal galiojantį užsakymą;
- asmuo gali gauti tik vieną asmens tapatybės dokumentą;
- gaminant dokumentus taikomas „keturių akių“ principas;
- gaminant ar keičiant dokumentus naudojami tik tikslūs duomenys;
- duomenys atitinka techninius (ir teisinius) reikalavimus;
- užsakovas prieš palikdamas duomenų pateikimo vietą pateikė visus reikalingus duomenis;
- išimčių procesas sukurtas atsižvelgiant į svarbiausią riziką (praradimo, netinkamo naudojimo ir kt.).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
2.1 Autorizacija	Neteisingai nustatoma asmens tapatybė ir ne tas asmuo gauna asmens tapatybės dokumentą.	Asmuo privalo asmeniškai atvykti į migracijos tarnybą ar konsulinę įstaigą dėl asmens tapatybės dokumento išdavimo ir keitimo. Asmeniškas atvykimas ir asmens tapatybės dokumentų pateikimas sumažina riziką išduoti asmens tapatybės dokumentą kitam asmeniui. Kai dokumentas išduodamas asmeniui, neturinčiam 16 metų, prašymą pateikia vienas iš nepilnamečio asmens tėvų (įtėvių) ar globėjas (rūpintojas). Nepilnametis pilietis, vyresnis nei 1 metų taip pat privalo dalyvauti pateikiant prašymą. Asmuo identifikuojamas pagal pateiktą asmens tapatybę patvirtinantį dokumentą ir jam suteiktą unikalų asmens kodą, kuris įrašytas Gyventojų registre. Audito metu įsitikinta, kad darbuotojai, priimantys asmens prašymą sutikrina jo išvaizdą ir veido atvaizdą Gyventojų	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		registre ir pateiktuose dokumentuose; taip pat įvertina, ar pateiktas dokumentas priklauso šiam asmeniui ir ar jame nėra klastojimo požymių. Migracijos tarnybos ar konsulinių įstaigų darbuotojai atvyksta į asmens buvimo vietą ir taip įsitikina asmens tapatybe, kai asmenys dėl fizinės negalios ar neveiksnumo arba arešto, terminuoto laisvės atėmimo ar laisvės atėmimo iki gyvos galvos negali patys atvykti į migracijos tarnybą ar konsulines įstaigas. Šiais atvejais asmens tapatybės dokumento prašymas registruojamas naudojant mobiliąją biometrinių duomenų registravimo įrangą, iš kurios duomenys vėliau perkeliami į ADIS į kurią perkelti Gyventojų registro duomenys apie asmenį, todėl taip pat visada atliekamos duomenų sutikrinimo procedūros.	
2.2 Autorizacija	Netinkami duomenys.	Duomenys apie visus išduotus dokumentus kaupiami Gyventojų registre (pagal kurio duomenis asmuo dokumento išdavimo metu identifikuojamas), o ADIS sukurtos funkcijos kontroliuoja ir užtikrina, kad asmuo turėtų tik vienos rūšies galiojantį pasą ar asmens tapatybės kortelę (LR piliečiams suteikta teisė vienu metu turėti du asmens tapatybės dokumentus). Prašymo išduoti/pakeisti asmens tapatybės dokumentą registravimas laikomas baigtu, kai darbuotojas apie tai pažymi sistemoje. Pagal atitinkamos rūšies dokumento išdavimo tvarką, sistemoje automatiniu būdu kontroliuojami darbuotojo veiksmai ir neleidžiama pažymėti apie proceso pabaigimą, jei darbuotojas neįvykdo visų veiksmų, kurie būtini užregistruoti atitinkamos rūšies dokumento prašymui. Migracijos tarnybų ir konsulinių įstaigų darbuotojams suteikiamos teisės, būtinos išduodant, keičiant asmens tapatybės dokumentus, o ADIC darbuotojams suteikiamos teisės išrašyti asmens tapatybės dokumentus ir perduoti migracijos tarnyboms, konsulinėms įstaigoms. Audito metu įsitikinta, kad ADIS sukurtos kontrolės priemonės, kurios fiksuoja naudotojo veiksmus ir leidžia išrašyti tik vieną tos pačios rūšies galiojantį asmens tapatybės dokumentą. Nustatyta, kad darbas ADIS vykdomas pagal nustatytas funkcijas, o tais atvejais kai darbuotojas perkeliamas į kitas pareigas, prieiga naikinama.	● Maža rizika
2.3 Kokybė	Netikslūs / neteisingi asmens duomenys.	Asmens dokumento išdavimo procese dalyvauja dvi įstaigos, kur paskirti darbuotojai peržiūrėdami įvertina asmens duomenų tikslumą ir pagaminto dokumento duomenų (įskaitant biometrinius) teisingumą. Asmens tapatybės dokumentus išduodančios įstaigos naudoja bendrą el. prašymų registravimo sistemą, o institucinių sistemų ir registrų sąsajos suteikia galimybę automatizuotai gauti aktualius duomenis (asmens kodą, vardą, pavardę, gyvenamąją vietą, pilietybę) ir užpildyti prašymą kompiuterinėmis priemonėmis. Siekiant sumažinti žmogiškąsias klaidas ir kitus nuo technologijų priklausomus dalykus atliekama dviguba asmens tapatybės dokumento kokybės užtikrinimo kontrolė. Migracijos tarnybos darbuotojai atrankos būdu	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		(prieš siųsdami užsakymą gamybai) pasirenka užregistruotus prašymus ir peržiūri: ar prašymas asmens tapatybės dokumentui gauti kokybiškai užpildytas, asmens duomenys teisingi ir sutampa su duomenimis Gyventojų registre, pagal teisės aktų reikalavimus biometriniai duomenys surinkti ir ar nufotografuotas (nuskenuotas) veido atvaizdas yra kokybiškas. Šios patikros procedūros užtikrina, kad užregistruoto prašymo duomenų klaidos būtų laiku pastebėtos ir ištaisytos, sumažintų klaidingų duomenų perdavimo riziką. Iki dokumento atspausdinimo pastebėjus, kad prašymo duomenys nekokybiški, ADIC darbuotojai grąžina prašymą migracijos tarnybai.	
2.4 Kokybė	Surinkti duomenys neatitinka reikalavimų.	Migracijos padalinių darbuotojams sukurta tinkama techninės ir programinės įrangos infrastruktūra, kuri užtikrina įrašomų duomenų (įskaitant biometrinius) kokybę. Pirštų atspaudų nuskaitymo kokybė įvertinama panaudojant įdiegtas automatines programinės kontrolės priemones, veido atvaizdo kokybė vertinama dviem etapais: ▪ migracijos padalinių ir konsulinių įstaigų darbuotojai nuskaitydami veido atvaizdą asmens tapatybės dokumentui įvertina atvaizdo kokybę; ▪ peržiūri veido atvaizdo ir parašo grafinius duomenis ir įvertina juos. Prireikus atlieka nežymias korekcijas, kad pagerintų atvaizdų kokybę. ADIC nuo 2009 m. sausio mėn. įsteigtos ir funkcionuoja CSCA ir DSCA tarnybos į asmens tapatybės korteles įrašomų pirštų atspaudų kokybės kontrolei bei asmens tapatybės kortelių patikrai migracijos tarnybose. Veido atvaizdo ir pirštų atspaudai įrašomi į asmens tapatybės dokumentą pagal standarto ISO/IES 19794−5: 2005 reikalavimus. Numatyta, kad tada, kai nėra galimybių nuskaityti asmens veido atvaizdo biometrinių duomenų registravimo įranga (jei asmuo pageidauja, kad veido atvaizdas būtų formuojamas iš nuotraukos arba, jei nuskaitant veido atvaizdą, nepavyksta išvengti šviesos atspindžių akinių stikluose, o asmuo atsisako nusiimti akinius), asmuo gali pateikti savo nuotraukas, atitinkančias nurodytus reikalavimus. Asmens tapatybės dokumentui išrašyti nuskaitomi aiškūs kairiojo ir dešiniojo smilių atspaudai. Jeigu kairysis arba dešinysis smilius sužalotas arba jo nėra, arba jo ISO/IES 19794−4 vertė yra nuo 0 iki 25, įrašomi aiškūs tos pačios rankos didžiojo ar bevardžio pirštų arba nykščio atspaudai, jeigu jų ISO/IES 19794−4 vertė aukštesnė. Jeigu visų vienos rankos pirštų atspaudų kokybė prasta (pagal kokybės vertę), daromas aiškus piršto, kurio vertė didžiausia, atspaudas. Lietuvos Respublikos asmens ir kelionės dokumentuose naudojamos ir papildomos biometrinių duomenų apsaugos priemonės. Visus asmens tapatybės dokumentus su biometriniais duomenimis projektuoja Valstybinė dokumentų technologinės apsaugos tarnyba prie Finansų ministerijos pagal ES, ICAO ir Saugiųjų dokumentų ir saugiųjų dokumentų blankų gamybos įstatymo reikalavimus.	● Maža rizika
2.5 Užbaigtumas	Surinkti ne visi duomenys.	Asmens tapatybės dokumento užsakymą galima išsiųsti tik tada, kai tinkamai ir išsamiai užpildytos privalomos prašymo išduoti (pakeisti) asmens tapatybės dokumentą eilutės. Jei darbuotojas neįvykdo visų veiksmų, kurie	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		būtini užregistruoti atitinkamos rūšies dokumento prašymą, sistemos kontrolės priemonės neleidžia baigti ir išsiųsti užsakymo (jei nėra asmens atvaizdo, parašo ir pirštų atspaudų, apmokėjimo būdo ar neįvesta dokumento keitimo priežastis). Naudojama biometrinių duomenų registravimo įrangos autonominio valdymo programa leidžia priimti prašymus asmens tapatybės dokumentams užsakyti ir tais atvejais kai nėra ryšio su Gyventojų registru. Visi asmens identifikaciniai duomenys pagal asmens pateiktus dokumentus įvedami į biometrinių duomenų registravimo įrangos lokalią saugyklą, nuskaitomi biometriniai duomenys, parašas ir jie išsaugomi užšifruotu pavidalu. Atsiradus ryšiui su Gyventojų registru, nuskaitytieji duomenys įrašomi į informacinę sistemą ir sutikrinami su registro duomenimis. Asmenys, kurių pateikti duomenys neatitinka registro duomenų, kviečiami pakartotinai pateikti prašymą ir biometrinius duomenis.	
2.6 Išimtys	Standartinis procesas negali būti taikomas.	Prašymo išduoti asmens tapatybės dokumento pateikimo / priėmimo metu nestandartinės situacijos kontroliuojamos, rečiau pasitaikančios išimtinos situacijos apibrėžtos teisės aktuose, o sprendimą dėl nustatytų išminčių pritaikymo priima dokumentų išrašymo įstaigų vadovai. Sprendimą dėl dokumento išdavimo (keitimo) priima migracijos įstaigos vadovas kai asmuo pageidauja gauti asmens tapatybės dokumentą: ▪ skubos tvarka per 1 darbo dieną (tą pačią dieną), per 5 darbo dienas vietoje prarastųjų asmens tapatybės dokumentų arba skubos ar bendra tvarka kuomet asmens gyvenamoji vieta nedeklaruota ar neapskaityta, ar kartu prarasti asmens tapatybės dokumentai. Prašymas išduoti asmens tapatybės dokumentą skubos tvarka priimamas tik tuo atveju, kai Gyventojų registre yra naujausi asmens duomenys ir nereikia laukti, kol jie bus pakeisti. ▪ nepilnamečiams vaikams, kai vaikų tėvai yra nutraukę santuoką, esant Vaikų teisių apsaugos skyriaus tarpininkavimo raštui išduoti asmens tapatybės dokumentą arba jeigu nei vienas iš tėvų, nei globėjas (rūpintojas), nei socialinės globos įstaigos atstovas piliečio iki 16 metų prašymo ir kitų dokumentų nepateikia, tai, atsižvelgus į vaiko interesus, pasas jam gali būti išduotas ar pakeistas tarpininkaujant valstybinei vaiko teisių apsaugos institucijai. ▪ kai tuo metu nagrinėjami dokumentai dėl asmens LR pilietybės netekimo. Kai asmuo atsisako pateikti biometrinius duomenis (pvz.: pirštų atspaudus), ar tai bando atlikti apgaulės būdu, jam asmens tapatybės dokumentas neišduodamas. Jei asmenys dėl medicininių priežasčių negali pateikti pirštų atspaudų ir tai yra nuolatinė asmens būsena, asmens tapatybės dokumentas išduodamas standartine tvarka. Jei asmens būsena yra laikina, asmens tapatybės dokumentas išduodamas be pirštų atspaudų duomenų ir galioja 1	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		metus, apie šias išimtis pažymima informacinėje sistemoje. Pažymėtina, kad konsulinių įstaigų darbuotojai netaiko išimčių, besikreipiančių asmenų prašymai siunčiami nagrinėti Migracijos valdybai.	

Naudojamos kontrolės priemonės leidžiančia įsitikinti besikreipiančio asmens tapatybe, sukurta tinkama techninės ir programinės įrangos infrastruktūra, kuri užtikrina įrašomų duomenų (įskaitant biometrinius) kokybę ir visų asmens tapatybės dokumentui pagaminti būtinų duomenų surinkimą.

1.3. Asmens tapatybės dokumentų gamyba

Vertintas biometrinių asmens dokumentų gamybos procesas (duomenų tikrinimo, surinkimo, kokybės užtikrinimas, dokumentų gamybos klaidos ir kt.), įsitikinant, kad:

- saugumo priemonės užkerta kelią pavogti pirminius išteklius ir blankus;
- pirminiai ištekliai saugomi viso proceso metu;
- pirminiai ištekliai negali būti prarasti ar pavogti nepastebimai;
- fizinis ir elektroninis turtas tinkamai apsaugotas transportuojant (pvz., atsargos, šifravimas);
- asmens tapatybės dokumento duomenys išsamūs (yra visi reikalingi);
- garantuojama reikalaujama duomenų kokybė ir surinktų pirminių duomenų vientisumas;
- asmens tapatybės dokumentas gali būti pagamintas tik pagal galiojantį užsakymą ir esant visiems reikalingiems duomenims;
- vienam užsakymui gali būti pagamintas tik vienas galiojantis asmens tapatybės dokumentas;
- asmens tapatybės dokumentų duomenų konfidencialumas užtikrinamas viso dokumentų paskirstymo metu;
- išimčių procesas sukurtas atsižvelgiant į svarbiausią riziką (praradimo, netinkamo naudojimo ir kt.).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
3.1 Nuostolių prevencija ir nustatymas	Laiku neaptikta, kad prarasti ar pavogti pirminiai ištekliai (rašalas, popierius, antspaudai ir t. t. arba asmens tapatybės	Asmens tapatybės dokumentų blankų gamybą prižiūri Valstybinė dokumentų technologinės apsaugos tarnyba prie Finansų ministerijos, ji tikrina įmones, turinčias saugiųjų dokumentų ir saugiųjų dokumentų blankų gamybos licencijas, ir atlieka tokių dokumentų ir blankų kokybės tikrinimus. Asmens dokumentų išrašymo centras sudarė sutartis su 2 įmonėmis dėl asmens tapatybės dokumentų (paso ir asmens tapatybės kortelės) blankų gamybos. Asmens dokumentų gamybos procese sukurtos kontrolės priemonės užtikrina tinkamą blankų apskaitymą ir išdavimą. Neteisėto asmens tapatybės dokumentų blankų panaudojimo tikimybę mažina griežta jų apskaita ir	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
	dokumentų blankai).	saugojimas uždaromis sąlygomis. Įgaliota komisija priima ir patikrina (skaičių ir kokybę) iš tiekėjų gautus blankus. Jie registruojami ADIS ir vėliau susiejami su personalizuotais asmens tapatybės dokumentais. Priimti blankai saugomi pagrindinėje saugykloje, kur veikia įeigos kontrolės priemonės (saugyklos atidarymo ir uždarymo apskaitos žurnalas, durų plombavimas, ribotas darbuotojų turinčių teisę įeiti, atidaryti / uždaryti pagrindinę asmens tapatybės dokumentų blankų saugyklą skaičius), o į tarpinę saugyklą blankai pervežami pagal vienos darbo dienos poreikius. Sunaudoti dokumentų blankai (perduoti asmens tapatybės dokumentų išdavimo įstaigoms, brokuoti) nurašomi pagal darbuotojo, atsakingo už asmens tapatybės dokumentų blankų apskaitą parengtą ataskaitą. Pagal nustatytą tvarką mėnesio paskutinę darbo dieną visi nepanaudoti dokumentų blankai perduodami į tarpinę saugyklą.	
3.2 Užbaigtumas	Duomenys naudojami sukurti asmens tapatybės dokumentus yra neišsamūs.	Įstaigose nustatytos ir informacinėje sistemoje įdiegtos kontrolės priemonės užtikrina, kad asmens tapatybės dokumentai būtų kokybiški ir juose būtų pateikti visi gamybai būtini duomenys. Priimti asmens tapatybės dokumento užsakymo prašymą, jį užregistruoti ir išsiųsti ADIS priemonėmis turi teisę tik Migracijos tarnybos ir konsulinės įstaigos. Šios įstaigos prieš siųsdamos užsakymus į gamybą, užtikrina, kad pateikti prašymai ir duomenys juose yra teisingi pagal Gyventojų registro duomenis. Jei registre būtina įvesti ar pakeisti asmens duomenis, kurie bus įrašomi į asmens tapatybės dokumentą, prašymas neįtraukiamas į užsakymą tol, kol duomenys nepakeičiami. Pagal atitinkamos rūšies dokumento išdavimo tvarką sistemoje automatiniu būdu kontroliuojami darbuotojo veiksmai ir nurodoma jei darbuotojas neįvykdo visų veiksmų, kurie būtini užregistruoti atitinkamos rūšies dokumento prašymą. Tokiu būdu sumažinamos žmogiškosios klaidos, užtikrinamas tinkamas duomenų surinkimas ir išbaigtumas. Tik įsitikinus, kad prašymo duomenys yra išbaigti ir tikslūs, siunčiamas užsakymas gaminti asmens tapatybės dokumentą. Taip pat vykdomas papildomas kontrolinis patikrinimas: Migracijos valdyboje darbuotojas atrankos būdu pasirenka el. prašymus ir patikrina duomenis su Gyventojų registro duomenimis, taip pat peržiūri popierinį prašymą ar visi duomenys pateikti, ar asmuo ir darbuotojai pasirašė.	● Maža rizika
3.3 Kokybė	Neužtikrintas duomenų, kurie naudojami gaminant asmens tapatybės dokumentus, vientisumas.	Duomenų naudojamų asmens tapatybės dokumentams gaminti kokybę ir vientisumą užtikrina tai, kad įstaigos priimančios užsakymus ir gaminančios dokumentus naudoja tą pačią duomenų bazę, tačiau jų funkcijos atskirtos. Sukurtoje dokumentų išrašymo sistemoje yra galimybė registruoti prašymus tokiu būdu, kad prašymo duomenis surenka ir į centrinę duomenų bazę įveda viena, o dokumentą spausdina kita įstaiga. Visi reikalingi duomenys, saugomi Gyventojų registro centrinėje duomenų bazėje neribotą laiką, išskyrus veido atvaizdo, pirštų atspaudų ir asmens parašo duomenis, kurių saugomi du paskutiniai. Visi užsakymai pateikiami ir saugomi vienoje sistemoje, nurodant užsakymo suformavimo datą, asmens	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		tapatybės dokumento išrašymo skubumą ir prašymų skaičių užsakyme. ADIC asmens tapatybės dokumentus išrašyti gali tik pagal prašymus gautus iš sistemoje suformuoto užsakymo. Po asmens tapatybės dokumentų pagaminimo, į Gyventojų registrą grąžinamas išrašyto dokumento numeris, sertifikatų aktyvavimo duomenys ir įrašytų sertifikatų numeriai. Pagal nustatytą tvarką patikrinami visų pagamintų (išrašytų) asmens tapatybės dokumentų duomenys ir išrašymo kokybė (vizualiai ir specializuotu skeneriu), taip pat patikrinama, ar dokumentų (paso ir asmens tapatybės kortelės) elektroninėse laikmenose pagal reikalavimus įrašyti nurodyti duomenys: asmens vardas, pavardė, lytis, gimimo data, asmens kodas, pilietybė, veido atvaizdas ir pirštų atspaudai, ar įrašyti asmens atpažinimo elektroninėje erdvėje sertifikatai ir kvalifikuoti sertifikatai.	
3.4 Autorizacija	Neteisėtai gaminami ir naudojami asmens tapatybės dokumentai.	Asmens tapatybės dokumentų blankų, prašymų ir išrašytų dokumentų saugumas ADIC užtikrinamas administracinėmis, techninėmis ir programinėmis apsaugos priemonėmis. Fizinės apsaugos priemonės užtikrina, kad į gamybines technologinės patalpas gali patekti tik leidimą turintys darbuotojai, draudžiama naudotis mobiliaisiais telefonais. Tinkamai suprojektuota ir įrengta fizinė sauga (į gamybines patalpas galima patekti nuskaitant piršto atspaudą), ribojamas kitų darbuotojų patekimas, jei darbo funkcijos nesusietos su asmens tapatybės dokumentų gamyba. ADIS priemonės apriboja galimybes manipuliuoti duomenimis, suteiktos teisės atlikti tik reikalingoms funkcijoms, todėl ADIC darbuotojai neturi galimybės paruošti prašymo asmens tapatybės dokumentui gauti, privilegijų keisti asmens duomenis ir eksportuoti duomenų. Procedūrose nuo prašymo išduoti (pakeisti) asmens tapatybės dokumentą pateikimo, gamybos ir iki išrašyto asmens tapatybės dokumento įteikimo dalyvauja skirtingos įstaigos. ADIS fiksuojami visi darbuotojo veiksmai, vykdoma blankų apskaita, kontroliuojamas gamybinis ir technologinis blankų brokas. Šios kontrolės priemonės užtikrina tinkamą apsaugą nuo neteisėtų veiksmų atlikimo gamybos procese.	● Maža rizika
3.5 Autorizacija	Pagaminti keli asmens tapatybės dokumentai ir tuo piktnaudžiaujama.	Sukurta teisinė aplinka ir ADIS sukurtos kontrolės priemonės užtikrina, kad vienam asmeniui gali būti registruotas tik vienas prašymas išduoti tam tikros rūšies dokumentus ir nėra galimybės užregistruoti vienu metu dviejų prašymų išduoti asmens tapatybės dokumentą. Asmens duomenų įrašai į prašymus išduoti (pakeisti) asmens tapatybės dokumentą įtraukiami pagal Gyventojų registro duomenis, todėl kelių tos pačios rūšies galiojančių asmens tapatybės dokumentų pagaminti nėra galimybės. Užregistravus naują prašymą, sistema automatiškai prašo nurodyti išduoto galiojančio asmens tapatybės dokumento negaliojimo priežastį. Šį dokumentą sistema automatiškai paskelbia negaliojančiu, kai pildomas naujas prašymas išduoti asmens tapatybės dokumentą.	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		Gamybos procese vykdoma griežta pirminio blanko išdavimo ir apskaitos kontrolė. Duomenys apie visus pagamintus asmens tapatybės dokumentus kaupiami Gyventojų registre, kuriame nurodomas dokumento serijos numeris, pagaminimo data ir kt.	
3.6 Privatumas	Atskleista asmeninė ir konfidenciali informacija.	Asmens dokumentų gamybos procedūros užtikrina, kad gamybos metu nebūtų atskleisti asmens duomenys ar kita konfidenciali informacija. Dokumentų gamyba vykdoma uždarojo režimo darbo sąlygomis, o prieiga prie duomenų griežtai kontroliuojama pagal naudotojui suteiktas dokumento išdavimo proceso teises. ADIC darbuotojai yra susipažinę su Informacijos saugos valdymo sistemos saugumo priemonių aprašu, kurio viena priemonių – pasižadėjimas neatskleisti neviešinamos informacijos.	● Maža rizika
3.7 Išimtys	Standartinis procesas negali būti taikomas.	Asmens dokumentų išrašymo sistemoje numatytos priemonės klaidų (duomenyse, techninių ar kitokių nesklandumų) taisymui atlikti. Pažymėtina, kad asmens tapatybės dokumento prašymas koreguojamas tiktai tais atvejais, kai asmens tapatybės dokumentas nebuvo įteiktas. ADIC savo iniciatyva taip pat gali grąžinti prašymą, iki asmens tapatybės dokumento atspausdinimo pastebėjus, kad prašymo duomenys nekokybiški. Dokumentų blankų kokybė tikrinama iki jų personalizavimo ir po jo (vizualiai patikrinama, ar atspausdinti blankai atitinka aprašyme išdėstytus reikalavimus ir pagal poreikį panaudojamos technines priemones). 2013 m. plane nustatyta maksimali 0,8 proc. gamybos broko riba neviršyta (broko lygis 2013 m. 0,26 proc.). Palyginus 2013 m. ir 2014 m. trijų ketvirčių technologinio broko rodiklius nustatyta, kad 2014 m. pasų ir leidimų gyventi Lietuvoje brokas išaugo ir jau viršija maksimalias ribas: ▪ blanko broko atvejų (neveikiantis lustas (tai galima aptikti tik išrašymo metu), duomenų lapo brokas (mechaniniai pažeidimai), nekokybiškas numeravimas, mechaniniai blanko pažeidimai) padidėjo (pasų nuo 0,06 proc. iki 0,2 proc., leidimų gyventi nuo 0,3 proc. iki 1,06 proc.). ▪ o gamybinio broko (lusto įrašymo metu atsirandantys sutrikimai, blanko mechaniniai pažeidimai išrašymo metu) padidėjo (pasų nuo 0,16 iki 0,9 proc., leidimų gyventi nuo 0,1 proc. iki 0,9 proc.).	■ Vidutinė rizika

Išrašant asmens tapatybės dokumentus naudojami dokumentų blankai, kurių kokybę ir technologines apsaugos priemones nustato ir vertina įgaliota institucija. Asmens dokumentų gamybos procedūros užtikrina, kad nebūtų atskleisti asmens duomenys ar kita konfidenciali informacija, pagal nustatytas procedūras tikrinami užsakymų duomenys ir pagamintų dokumentų kokybė. Pastebėtina, kad 2014 m. išaugo (ir viršijo maksimalias ribas) pasų ir leidimų gyventi Lietuvoje brokas.

1.4. Asmens tapatybės dokumentų pristatymas

Vertintas biometrinių asmens dokumentų pristatymo procesas (sukurto ar pakeisto dokumento pristatymas (paštu, atsiėmimas vietoje ar kt.) pareiškėjui) įsitikinant, kad:

- pareiškėjas gavo jo / jos asmens tapatybės dokumentą (pristatymas ir asmeninis įteikimas);
- laiku nustatomos asmens tapatybės dokumentų vagystės ar praradimai jų pristatymo metu;
- fizinis ir elektroninis turtas tinkamai apsaugostas transportuojant (atsargos, šifravimas);
- pareiškėjas tinkamai autorizuojamas;
- asmens tapatybės dokumentai, kurie nebuvo pristatyti / įteikti, aptinkami ir tinkamai tvarkomi;
- išimčių procesas sukurtas atsižvelgiant į svarbiausią riziką (praradimo, netinkamo naudojimo ir kt.).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
4.1 Nuostolių prevencija ir nustatymas	Laiku neaptikta, kad asmens tapatybės dokumentų pristatymo metu jie prarasti ar pavogti.	Asmens tapatybės dokumentų logistikos procedūros atliekamos taikant LST EN ISO 9001:2008 standartą, išrašyti asmens tapatybės dokumentai kartu su lydraščiu siunčiami užsakymą pateikusiai įstaigai. Taikomi papildomi reikalavimai sumažina riziką, kad dokumentų turinys perdavimo metu būtų atskleistas: išrašytų asmens tapatybės dokumentų siuntų formavimas standartizuotas, dokumentai transportuojami užplombuotuose paketuose, o migracijos tarnybų darbuotojai įsitikina, ar plombos nepažeistos. Nustačius, kad pakuotė pažeista ir / ar trūksta asmens tapatybės dokumentų, apie tai privaloma nedelsiant informuoti teritorinę policijos įstaigą arba konsulinės įstaigos vadovą ir ADIC. Prarasti dokumentai turėtų būti skelbiami kaip negaliojantys ir įtraukiami į Individualius požymius turinčių ir numeruotų daiktų registrą bei į Šengeno informacinę sistemą. Lietuvoje nuo 2003 m. nebuvo pristatomų asmens tapatybės dokumentų dingimo atvejų.	Maža rizika
4.2 Autorizacija	Ne tas asmuo gauna asmens tapatybės dokumentą.	Kontrolės priemonės sumažina riziką, kad asmens tapatybės dokumentą atsiims kitas asmuo, nes asmuo privalo asmeniškai, ar per įgaliotą atstovą, atvykti atsiimti dokumento. Įsitikinta, kad Migracijos tarnybos darbuotojai įvertina ir sutikrina asmens išvaizdą su jo veido atvaizdu Gyventojų registre bei pateiktuose dokumentuose ir įsitikina asmens tapatybe. Migracijos tarnybos ar konsulinės įstaigos darbuotojas privalo pažymėti asmens tapatybės dokumentų išrašymo sistemoje tai, kam įteiktas dokumentas, o asmuo atsiimdamas asmens tapatybės dokumentą pasirašo patvirtindamas, kad asmens tapatybės dokumentą gavo, nurodo atsiėmimo datą. Migracijos tarnybos įgaliotas valstybės tarnautojas arba konsulinis pareigūnas įvertina, ar pateiktas LR pilietybę patvirtinantis dokumentas priklauso jį pateikusiam asmeniui ir ar jame nėra klastojimo požymių (pvz., ar asmens tapatybės dokumente nepakeista asmens nuotrauka, nepakeisti įrašai, nepersiūti puslapiai ir pan.). Nustačius, kad pateiktas dokumentas suklastotas, nustatyta tvarka paskelbiama, kad jis negalioja, ir kartu su turima medžiaga dokumentas nedelsiant pateikiamas ikiteisminį tyrimą atliekančioms institucijoms.	Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		Visi asmens tapatybės dokumentai išrašyti, bet neatsiimti (galiojantys) saugomi 1 metus nuo jų išrašymo dienos. Migracijos tarnybos darbuotojai kas mėnesį patikrina neatsiimtus dokumentus ir papildomai informuoja asmenis raštu ar žodžiu. Jei asmuo neatvyksta atsiimti pagaminto dokumento migracijos tarnybos darbuotojas asmens tapatybės dokumentus paskelbia negaliojančiais ir išsiunčia naikinti į ADIC. Audito metu įsitikinta, kad pagaminti, bet neatsiimti asmens tapatybės dokumentai saugomi migracijos tarnyboje užrakintuose seifuose, o už jų apskaitą ir saugojimą atsako tarnybos darbuotojas.	
4.3 Išimtys	Standartinis procesas negali būti taikomas.	Susiklosčius nestandartinėms situacijoms, kai sistema neveikia ar nėra ryšio su Gyventojų registru, asmeniui įteikiamas neaktyvuotas asmens tapatybės dokumentas. Sukurtos priemonės leidžia dirbti autonominio valdymo priemonėmis. Atsiradus ryšiui su registru nuskaitytieji duomenys įrašomi į sistemą ir atliekamas duomenų sutikrinimas su registro duomenimis. Jeigu konsulinė įstaiga neturi techninių galimybių ADIS pažymėti apie asmens tapatybės dokumento atsiėmimą, jį įteikusi konsulinė įstaiga nedelsdama Vilniaus migracijos tarnybai išsiunčia faksu ar el. paštu nuskaitytą pranešimą ar paso įteikimą. Tokiu atveju asmuo įspėjamas, kad asmens tapatybės dokumentas pradės galioti tik tada, kai Vilniaus migracijos tarnybos darbuotojai pažymės, kad dokumentas atsiimtas. Migracijos tarnybų darbuotojams nesuteikti įgaliojimai taikyti išimtis iš teisės aktų. Pažymėtina, kad įteikiant asmens tapatybės dokumentą asmenims suteikta galimybė pasitikrinti įrašytus biometrinius duomenis, tačiau asmenys apie tai neinformuojami.	● Maža rizika

Lietuvoje nuo 2003 m. nebuvo asmens tapatybės dokumentų dingimo atvejų jų pristatymo metu, nes jie įteikiami asmeniškai užsakiusiam asmeniui arba siunčiami per konsulinę įstaigą. Logistikos procedūros užtikrina, kad asmens tapatybės dokumentų turinys perdavimo metu nebūtų atskleistas.

Siekiant skatinti sukurtų paslaugų naudojimą, siūlome pateikti informaciją apie vietas, kur asmenims atsiimant pagamintus dokumentus įrengta galimybė patikrinti išduotų asmens tapatybės dokumentų biometrinius duomenis.

1.5. Asmens tapatybės dokumentų naikinimas

Asmens tapatybės dokumentų naikinimo procesas apima naujo dokumento gavimą, baigusio galioti ar pamesto dokumento keitimą, dokumento keitimą sudarius santuoką, gimus vaikui ir kt. Audito metu vertinta, ar:

- visi sugadinti ar negaliojantys asmens tapatybės dokumentai paskelbti negaliojančiais;

- visi sugadinti ar negaliojantys asmens tapatybės dokumentai aiškiai pažymimi kaip negaliojantys ar sunaikinti;
- visi naikinti skirti asmens tapatybės dokumentai visiškai sunaikinami;
- visi naikinti skirti asmens tapatybės dokumentai sunaikinti negrįžtamai (nėra atkūrimo galimybės);
- prarasti asmens tapatybės dokumentai negali būti panaudoti, jei yra išduotas naujas asmens tapatybės dokumentas;
- naujo asmens tapatybės dokumento užsakymas nebus vykdomas jei prarastas asmens tapatybės dokumentas buvo surastas ir pakartotinai naudojamas.

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
5.1 Autorizacija	Netinkami ar negaliojantys asmens tapatybės dokumentai netinkamai paskelbti negaliojančiais ir tuo piktnaudžiaujama.	Migracijos ir konsulinės įstaigos užtikrina, kad visi negaliojantys asmens tapatybės dokumentai sistemos funkcinėmis priemonėmis būtų pažymėti negaliojančiais. Visais atvejais, kai negaliojantys (įteikti naujo prašymo pildymo metu ar grąžinti) dokumentai grąžinami asmeniui, jie pažymimi specialiu prietaisu, kad nebūtų galimybės dokumentu pasinaudoti. ADIS prašymo registravimo metu pažymėtas keičiamu ir su juo susijęs asmens tapatybės dokumentas tampa negaliojančiu, kai į sistemą įvedama žyma apie naujai išrašyto asmens tapatybės dokumento įteikimą. Įsitikinta, kad asmens tapatybės dokumentus išduodančių įstaigų darbuotojai senąjį asmens tapatybės dokumentą paskelbia negaliojančiu ir fiziškai pažymi taip, kad asmuo negalėtų juo pasinaudoti.	Maža rizika
5.2 Užbaigtumas	Pamesti arba pavogti sunaikinimui skirti asmens tapatybės dokumentai.	Negaliojantys asmens tapatybės dokumentai teisės aktų numatytais atvejais ne rečiau kaip kartą per mėnesį siunčiami naikinti ADIC. Tai vienintelis įgaliotas centras, kuriam suteikta teisė naikinti iš asmens tapatybės dokumentus išduodančių institucijų gautus negaliojančius asmens tapatybės dokumentus, taip pat iš gamintojo gautus nekokybiškus ir dokumentų išrašymo proceso metu sugadintus minėtų dokumentų blankus. Įstaigos, parengia lydraščius ir kartu su naikinti skirtais negaliojančiais dokumentais perduoda ADIC. Migracijos tarnybos gavusios mirusių piliečių asmens tapatybės dokumentus, Gyventojų registro duomenų centrinėje bazėje patikrina duomenis apie mirusį asmenį ir asmens tapatybės dokumentus pažymimi kaip negaliojančius, o dokumentų originalus išsiunčia naikinti. Visi dėl asmens mirties neįteikti asmens tapatybės dokumentai siunčiami sunaikinti ir naikinami bendra tvarka. ADIC darbuotojai gautus sunaikinti asmens tapatybės dokumentus, sutikrina pagal lydraštį, supakuoja į laikinus paketus, užrašo institucijos, iš kurios jie gauti kodą, pavadinimą, lydraščio numerį, gavimo datą ir padeda juos į laikiną saugyklą. Negaliojantys dokumentai saugomi ne mažiau nei 6 mėnesius, nuo jų gavimo datos ir praėjus šiam terminui sunaikinami. Patikros metu įsitikinta, kad saugykloje saugomi asmens tapatybės dokumentai, buvo pažymėti fiziškai ir nebuvo tinkami naudoti. Sunaikinti skirti dokumentai apskaitomi ir užregistruojami negaliojančių asmens tapatybės dokumentų lydraščių registre nurodomas sunaikinimo akto numeris ir data. Negaliojantys asmens tapatybės dokumentai naikinami specialiu įrenginiu (supjaustomi), parengiamas	Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		sunaikinimo aktas, o naikinimo metu patalpoje dirba ne mažiau kaip du darbuotojai.	
5.3 Autorizacija	Asmens tapatybės dokumentai apie kurių praradimą buvo pranešta naudojami juos suradus.	Migracijos tarnybos neturi teisinių ir techninių galimybių paskelbtus negaliojančiais asmens tapatybės dokumentus iš naujo paskelbti galiojančiais, tačiau nėra pakankamų apsaugos priemonių užtikrinančių, kad pamestu ar prarastu asmens tapatybės dokumentu nebus galimybės pasinaudoti, nes tik atsiradę dokumentai siunčiami sunaikinti. Keičiamas dokumentas paskelbiamas negaliojančiu Gyventojų registre, sistemoje nurodoma negaliojimo priežastis, jis fiziškai pažymimas taip, kad asmuo negalėtų juo pasinaudoti. Sukurtos technologinės priemonės užtikrina, kad, įvedus į sistemą informaciją apie dokumento įteikimą, sistema senojo dokumento negaliojimą pažymi automatiniu būdu. Minėtus dokumentus išduodančios įstaigos pažymi ar negaliojantį dokumentą asmuo paimti atsisakė (tokie dokumentai sunaikinami), ar jis grąžinamas asmeniui, prieš tai fiziškai pažymėtas. Atliekant patikrą nustatyta, kad tais atvejais kai asmens tapatybės dokumentas skelbiamas negaliojančiu dėl praradimo, asmens tapatybės dokumentus išduodančios įstaigos iškart atnaujina informaciją ADIS. Kasmet užregistruojamas panašus skaičius pranešimų apie asmens tapatybės kortelės ar paso praradimą tai sudaro 1,2–2 proc. visų pagamintų dokumentų. Informacija apie prarastus asmens dokumentus, paskelbtus negaliojančiais, automatiniu būdu perduodama Individualius požymius turinčių ir numeruotų daiktų registrui, o iš jo į Šengeno informacinę sistemą. Tokių asmens tapatybės dokumentų galiojimo atstatymas iš tarnybų darbo vietų negalimas. Asmuo, praradęs asmens tapatybės dokumentą, privalo informuoti ir prašymą asmeniškai pateikti bet kuriai teritorinei policijos įstaigai, migracijos tarnybai, o užsienio valstybėje – konsulinei įstaigai. Nuo 2014 m. pranešimą apie prarastą asmens tapatybės dokumentą galima pateikti ir el. būdu (https://epis.vrm.lt/epis/) bet kuriuo paros metu, tačiau dokumentas nedelsiant bus paskelbtas negaliojančiu tik darbo dienomis. Apie užsienyje prarastus asmens tapatybės dokumentus ne visada pranešama tos šalies atsakingoms institucijoms. Tai sudaro prielaidą manyti, kad asmens tapatybės dokumentu gali būti pasinaudota neteisėtai.	Vidutinė rizika

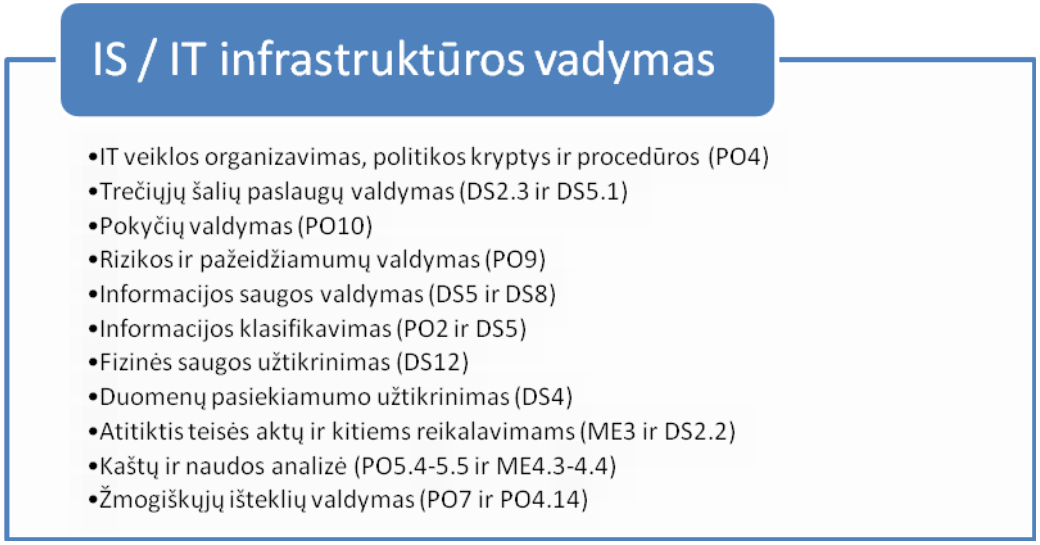
Negaliojantys asmens tapatybės dokumentai tinkamai pažymimi arba sunaikinami, kad jais nebūtų galima neteisėtai pasinaudoti. Kasmet užregistruojamas panašus skaičius pranešimų apie asmens tapatybės kortelės ar paso praradimą – tai sudaro 1,2–2 proc. visų pagamintų dokumentų. Įsitikinta, kad nėra teisinių ir techninių galimybių paskelbtus negaliojančiais asmens tapatybės dokumentus iš naujo paskelbti galiojančiais, tačiau nėra pakankamų apsaugos priemonių, užtikrinančių, kad pamestu ar prarastu dokumentu nebus galimybės pasinaudoti, nes siunčiami sunaikinti tik surasti dokumentai. Pastebėtina, kad nuo 2014 m. pranešimą apie prarastą asmens tapatybės dokumentą galima pateikti ir el. būdu (https://epis.vrm.lt/epis/) bet kuriuo paros metu, tačiau dokumentas nedelsiant bus paskelbtas negaliojančiu tik darbo dienomis, todėl asmens tapatybės dokumentu gali būti pasinaudota neteisėtai.

Asmens dokumentų išdavimo procese dalyvauja kelios įstaigos, todėl asmenims sudėtinga rasti informaciją apie tokią el. paslaugą. Siekiant skatinti sukurtų paslaugų gyventojams naudojimą, siūlome aktyviau informuoti asmenis apie galimybę el. būdu pranešti apie dingusį asmens tapatybės dokumentą.

2. KITŲ SU BIOMETRINIŲ ASMENS TAPATYBĖS DOKUMENTŲ IŠDAVIMU SUSIJUSIŲ PROCESŲ VERTINIMAS

Analizavome IS / IT infrastruktūros valdymo procesus (žr. 4 pav.) ir jų kontrolę, siekdami įsitikinti, ar duomenų saugojimo, atsarginių kopijų darymo, prieigos prie duomenų ir duomenų perdavimo procedūros tinkamai vykdomos viso biometrinių asmens dokumentų išdavimo metu.

2 lentelė. Nagrinėti IS /IT infrastruktūros valdymo procesai



Šaltinis – Valstybės kontrolė pagal Šveicarijos aukščiausiosios audito institucijos informaciją

2.1. IS/ IT infrastruktūros ir informacijos valdymas

IS/IT infrastruktūros valdymas ir kontrolės priemonių veiksmingumas vertintas atsižvelgiant į teisės aktų reikalavimus ir COBIT gerąją praktiką:

- IS/IT ir saugos procesai turi būti valdomi aukščiausiu vadovybės lygmeniu, kad saugos veiksmų valdymas atitiktų įstaigos reikalavimus. Nustatyta ir vadovybės patvirtinta politikos kryptis, standartai ir procedūros suteikia pagrįstą patikinimą, kad IS / IT naudojimas atitinka įstaigos tikslus, atitinkamus teisės aktų, standartų ir kitus reikalavimus, ir yra tinkamai išplatintos visoje įstaigoje (įsk. biometrinius reikalavimus).
- turi būti užtikrinta, kad trečiųjų šalių teikiamos paslaugos atitinka saugos reikalavimus ir vykdoma jų veiklos stebėsena. Įstaigoje turėtų būti nustatytas formalus procesas, siekiant nustatyti neatitikimus ir į juos reaguoti.
- pokyčių valdymo sistema užtikrina teisingą prioritetų suteikimą visiems pokyčiams ir jų koordinavimą, apima išteklių paskirstymą, rezultatų apibrėžimą, naudotojų patvirtinimą, etapus iki rezultato pasiekimo, kokybės užtikrinimą, testavimo planą, testavimą ir peržiūrą po įdiegimo, kad būtų pasiekta planuota nauda.
- rizikos vertinimas turi būti atliekamas reguliariai, siekiant nustatyti informacijos saugos priemonių prioritetus ir užtikrinti suderinamumą su veiklos rizika.
- nustatytos IS / IT politikos ir stebėsenos procedūros skirtos užsakyti, nustatyti, skirti, sustabdyti, keisti ir uždaryti naudotojų paskyras ir susijusias naudotojo privilegijas, naudojant naudotojo paskyrų valdymo procedūrų rinkinį.
- incidentų valdymo politika sukurta siekiant nustatyti informacijos saugos incidentų klasifikavimą, veiksmus, kurie turi būti atlikti nustačius informacijos saugos incidentą ir procesą, kaip pranešama tiems kurie pirmiausiai turi imtis priemonių. Apie visus incidentus, susijusius su apsikeitimu jautriais duomenimis, pranešama per bendrą incidentų pranešimo sistemą.
- įgyvendinta politika, kuria siekiama užkirsti kelią, aptikti ir pašalinti kenkėjiškas programas.
- įgyvendinamos apsikeitimo jautrias duomenimis kontrolės priemonės užtikrina turinio autentiškumą, įrodymų pateikimą, gavimą ir turinio nepakeičiamumą.
- įnformacijos saugos valdymas įtrauktas į saugumo technologijų atranką, įgyvendinimą ir patvirtinimą ir susijusias valdymo procedūras (pvz., ugniasienės, apsaugos įranga, tinklo segmentavimas, įsilaužimo aptikimas), leidžiančias naudoti ir kontroliuoti gaunamos ir į tinklais perduodamos informacijos srautus.
- įnformacijos tinklų ir palaikančios infrastruktūros apsauga, tinklo saugos valdymas apima įstaigos veiklos ribas, duomenų srautus, teisines pasekmes, stebėseną ir apsaugą. Taip pat numatytos papildomos kontrolės priemonės, skirtos apsaugoti jautrią / slaptą informaciją perduodamą per viešuosius tinklus. Įstaiga turi užtikrinti, kad taikomos tinkamos priemonės, siekiant užkirsti kelią, stebėti, aptikti ir pranešti apie duomenų praradimą procesuose ar sistemose.
- įnformacija turi būti klasifikuojama nurodant poreikį, prioritetus ir laukiamą tvarkomos informacijos apsaugos lygį. Informacijos klasifikavimo schema turi būti naudojama nustatant atitinkamą informacijos apsaugos lygį ir specialiųjų tvarkymo priemonių poreikį priklausomai nuo jos jautrumo ir kritiškumo.
- įranga turi būti apsaugota nuo fizinių ir aplinkos grėsmių, siekiant sumažinti neteisėtos prieigos prie informacijos riziką ir apsaugoti informaciją nuo praradimo ar sugadinimo. Kritinės arba neskelbtinos (jautrios) informacijos apdorojimo įrenginiai turi būti laikomi saugiose vietose, apsaugoti nustatytu perimetru su atitinkamais fizinės saugos barjerais ir įeigos kontrole. Jie turi būti fiziškai apsaugoti nuo neteisėto priėjimo, žalos ir poveikio. Teikiama apsauga turi būti proporcinga nustatytai rizikai.
- įstaigoje turėtų būti įgyvendintas veiklos tęstinumo valdymo procesas, siekiant kiek įmanoma sumažinti poveikį įstaigai ir atstatyti informacinį turtą po praradimo iki priimtino lygio, taikant prevencines ir veiklos atkūrimo kontrolės priemones. Šis procesas turėtų nustatyti kritinius procesus ir integruoti informacijos saugumo

valdymo reikalavimus. Poveikio veiklai analizė turėtų apimti nelaimių, saugumo sutrikimų, paslaugų praradimo ir paslaugų prieinamumo pasekmes. Veiklos tęstinumo planai turėtų būti sukurti, įgyvendinti ir išbandyti siekiant užtikrinti savalaikį operacijų atnaujinimą laiku.

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
1.1 Veiklos organizavimas	Netinkamas IS/IT valdymas ir sauga.	Nuo 2002 m. pasai ir kiti kelionės bei asmens tapatybės dokumentai (iki 10 rūšių) išrašomi centralizuotai Asmens dokumentų išrašymo centre ADIS priemonėmis, sistemą naudoja visos procese dalyvaujančios įstaigos, tačiau jai nepriskirtas valdytojas ir IS duomenų valdymo įgaliotinis, kaip numato teisės aktai. ADIC IS/ IT sauga valdoma aukščiausiu organizacijos lygmeniu: informacijos saugumą (duomenų saugą) koordinuoja, saugos politiką formuoja, tvirtina susijusius dokumentus įstaigos vadovybė, tačiau nepaskirtas gamybos IS duomenų valdymo įgaliotinis. Paskirtas saugos įgaliotinis koordinuoja elektroninės informacijos saugos incidentų tyrimą ir turi kasmet organizuoti visų informacinių sistemų rizikos vertinimą. ADIC kokybės vadybos sistema sertifikuota pagal LST EN ISO 9001:2008 Kokybės vadybos sistemos standarto reikalavimus, patvirtintas Kokybės vadybos vadovas ir kokybės valdymo procedūros. Taip pat įgyvendinta ir tobulinama informacijos saugumo valdymo sistema, atitinkanti LST ISO/IEC 27001:2006 standarto reikalavimus (sertifikavimo sritis – asmens dokumentų išrašymas) ir gerosios praktikos rekomendacijas. ADIC įsipareigoja užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą, siekia išvengti veiklos sutrikdymo dėl konfidencialios informacijos atskleidimo, informacijos vientisumo pažeidimo ir informacijos neprieinamumo dėl jos praradimo ar sistemų neveikimo.	■ Vidutinė rizika
1.2 Politikos kryptys, standartai ir procedūros	Netinkamai valdomi ir stebimi procesai, sistemos ir gamybinė aplinka.	ADIS[7] sukurta išduoti asmens tapatybės dokumentus Gyventojų registro duomenų pagrindu, bet nenustatyta kas turi užtikrinti sistemos duomenų saugą, kol vyksta asmens tapatybės dokumentų gaminimas, kokiomis priemonėmis turi būti saugomi duomenys gamybos metu, kas atsako už duomenų saugojimą ir kokį terminą turi būti saugomi duomenys siekiant užtikrinti jų konfidencialumą, vientisumą ir prieinamumą. Audito metu nebuvo patvirtinti sistemos nuostatai, neparengti saugos politiką įgyvendinantys dokumentai, tačiau sistemos tvarkytojų ir jų teisių administravimo sistema užtikrina, kad kiekvienas tvarkytojas gali vykdyti tik tas funkcijas, į kurias teises	▲ Didelė rizika

[7] Asmens dokumentų išrašymo informacinė sistema (ADIS), kuri veikia Gyventojų registro pagrindu, skirta priimti prašymus asmens tapatybės dokumentui, diplomatiniam pasui, tarnybiniam pasui, užsieniečių asmens tapatybės dokumentams su biometrinius duomenis išduoti ir paskelbti juos negaliojančiais.

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		suteikė administratorius. Nors ADIC įdiegta Informacijos saugumo valdymo sistema pagal ISO 27000 standarto reikalavimus, centro veikla neatitinka teisės aktų reikalavimų, t. y. ADIS ir ADGIS[8] neįteisintos teisės aktų nustatyta tvarka. Auditoriai pažymi, kad ADGIS saugos politikos dokumentai nesuderinti su Vidaus reikalų ministerija, sistemos nuostatai neatnaujinti ir neperžiūrėti vadovybės analizės metu nuo 2011 m., o saugos politiką įgyvendinantys dokumentai – nuo 2012 m. Įvertinus IS saugą ADIC, nustatyta saugos reikalavimų trūkumų: rizikos vertinimas buvo atliekamas ne kasmet (atlikta 2012, 2014 metais); neparengta rizikos vertinimo ataskaita, kurioje nurodomi įvertinti rizikos veiksniai, galintys turėti įtakos elektroninės informacijos saugai.	
1.3 Trečiųjų šalių paslaugų valdymas	Paslaugų perdavimas ir išorės paslaugų teikėjai neatitinka saugos ir stebėsenos reikalavimų.	Asmens dokumentų išrašymo procese dalyvauja asmens tapatybės dokumentų blankų tiekimo, įrangos priežiūros, saugaus tinklo, kurjerių ir kitas paslaugas teikiančios įstaigos. Šiose sutartyse nustatyti informacijos naudojimo, saugojimo ar platinimo reikalavimai, su asmens tapatybės dokumentų blankų tiekėjais ir ADGIS techninės priežiūros paslaugų teikėjais pasirašyti pasižadėjimai dėl neviešinamos informacijos neatskleidimo. Sutartyse numatyti įsipareigojimai tiekėjams saugoti įslaptintą informaciją, komercines paslaptis ir užtikrinti duomenų saugą. Jei tiekėjas pažeidžia sutartinius įsipareigojimus, ar jų nevykdo, ADIC gali pareikalauti atlyginti nuostolius (sumokėti delspinigius, baudą, vienašališkai nutraukti sutartį ir kt.). Nustatyta, kad reikalavimai įsigyjamos ADGIS priežiūros paslaugoms neatitiko teisės aktų reikalavimų IS veiklos tęstinumui užtikrinti, todėl kritinio IT gedimo atveju nebūtų buvęs užtikrintas asmens dokumentų išdavimo veiklos proceso vykdymas. Audituojamu laikotarpiu ADIC sudarė 3 metų sutartį Asmens dokumentų išrašymo ir programinės įrangos priežiūros paslaugoms atlikti, tačiau joje nenumatyti sutrikimų šalinimo ir maksimalūs įrangos dalinio funkcionavimo atstatymo laikai, nenumatytas laikas, per kurį paslaugų teikėjas įsipareigotų reaguoti įvykus įrangos gedimui. Šie sutarčių trūkumai gali turėti įtakos asmens tapatybės dokumentų išrašymui.	Vidutinė rizika
1.4 Pokyčių valdymas	Konfidencialios ir saugai kritiškos aplinkos pokyčiai atliekami be pakankamos kontrolės.	Vykdant informacinių sistemų kūrimo projektus, teisės aktai numato IS kūrimo etapų ir pokyčių kontrolės priemones. ADIS pradėta kurti 2001 m., iki dabar modifikuojama, tačiau neaiški jos struktūra, nes nėra vientisos ir išbaigtos specifikacijos. Sistemos kūrimo pradžia, eiga ir pabaiga neatitinka IS kūrimo reikalavimų, nors sistemos priemonėmis centralizuotai išrašomi asmens tapatybės dokumentai, tvarkomi jų duomenys. Programinė įranga testuojama tam tikra testavimo aplinka, tačiau ji neatitinka realios IS aplinkos, todėl, perkėlus	Vidutinė rizika

[8] Asmens dokumentų gamybos informacinė sistema (ADGIS) yra Asmens dokumentų išrašymo informacinės sistemos (ADIS) sudedamoji dalis, ją naudojant išrašomi asmens tapatybės dokumentai, užsieniečių asmens dokumentai, tarnybiniai pasai, diplomatiniai pasai pagal pateiktus prašymo duomenis iš Asmens dokumentų išrašymo informacinės sistemos.

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		sistemos patobulinimus į realią sistemą, galimi asmens tapatybės dokumentų gamybos ar išdavimo procesų trikdžiai. Rizikos valdymo plane numatyta iki 2014-12-31 tobulinti testinę aplinką ir priartinti tikrajai, tačiau audito metu nebuvo taikomos priemonės šiai rizikai suvaldyti. ADIC atsižvelgė į teisės aktų pokyčius (pase įrašomi duomenys apie asmens tautybę (IS pakeitimai atlikti 2014-12-30) ir centrui pavesta išrašyti ir diplomatinius pasus (pakeitimai atlikti 2014-11-01): laiku išplėtė ADIS funkciją. Keitimų valdymo planavimas, bandymas ir diegimas vykdomas pagal keitimų valdymo proceso aprašą.	
1.5 Rizikos valdymas	Nenustatyta reikšminga rizika ir netinkamai mažinama.	Rizikos valdymo kontrolės priemones nustato teisės aktai. ADIC direktoriaus patvirtinta tvarka, numatyta IS rizikos vertinimą atlikti kasmet. Rizikos valdymo procese nustatyta trūkumų: 2013 m. neatliktas IS rizikos įvertinimas, o saugos įgaliotinis neparengė rizikos įvertinimo ataskaitos, kurioje išdėstomi įvertinimo rezultatai, atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. 2013 m. patvirtinti[9] asmens dokumentų blankų atsargų (rezervo) normatyvai, tačiau ADIC nevertino paslaugų praradimo tikimybės jei abu blankų tiekėjai (Lietuvoje yra tik du) pažeistų sutartinius įsipareigojimus ar vienašališkai nutrauktų sutartis, ir nevertino galimybės blankus gamintis kitose ES šalyse. 2014 m. atliktas veiklos rizikos vertinimas: atlikta tik poveikio ADIC vykdomai veiklai analizė. 2014-02-20 sudarytas rizikos valdymo planas, kuriame nustatyti valdymo veiksmai, ištekliai, atsakomybės ir informacijos saugumo rizikos valdymo prioritetai, tačiau nenustatytos aiškios saugumo priemonės. Siekdamas užtikrinti nenutrūkstamą asmens tapatybės dokumentų išrašymo procesą, ADIC turi įvertinti galimas rizikas dėl informacijos praradimo ir užtikrinti, kad veiklos proceso savininkai ir IT darbuotojai nustatytų atsarginių kopijų saugyklos turinį, paskirtų atsakingus asmenis prižiūrėti, testuoti ir tobulinti IT tęstinumo planus ir su juo susijusius dokumentus.	Vidutinė rizika
1.6 Pažeidžiamumų valdymas	IS/ IT aplinkos pažeidžiamumai sistemiškai nevertinami, dėl to gali būti įgyvendinamos neefektyvios priemonės ir rizika nėra mažinama.	ADIC atliekant pažeidžiamumų analizę įvertinta ir biometrinių duomenų apdorojimo įranga, kuri atlieka personalizavimo funkcijas asmens tapatybės dokumentų gamybos, biometrinių identifikavimo kortelių gamybos ir biometrinių pasų gamybos posistemėse. Pastebėtina, kad 2012 m. ADGIS grėsmių analizės apraše, įvertinta aukštos grėsmės tikimybė dėl saugumo reikalavimų nesilaikymo ar nesupratimo, kai darbuotojui trūkta kompetencijos, tačiau audituojamu laikotarpiu šios sistemos naudotojams nebuvo rengiami informacijos saugos mokymai.	Maža rizika

[9] Lietuvos Respublikos vidaus reikalų ministro 2013-01-09 įsakymas Nr. 1V-7 „Dėl asmens dokumentų blankų atsargų normatyvų".

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
1.7 Tapatybės ir prieigos valdymas	Netinkamos naudotojų paskyros ir prieigos teisės.	Auditoriai įsitikino, kad ADIS naudotojų prieiga, naudotojų prisijungimo ir teisių suteikimo procesas tinkamai valdomas. Gyventojų registro atsakingi darbuotojai kas šešis mėnesius peržiūri prisijungimo teises, jei nustatoma, kad naudotojai nebesinaudoja prieiga, o apie tai buvo pamiršta pranešti, prieiga panaikinama. Migracijos valdyboje nepaskirtas asmuo, kuris nuolat peržiūrėtų prašymus suteikti prieigą, stebėtų darbuotojų kaitą ir laiku praneštų apie prieigos panaikinimą. Migracijos valdyboje už prieigos teisių suteikimą ir panaikinimą atsako tiesioginis vadovas, ADIC darbuotojų prieigą prie Gyventojų registro koordinuoja saugos įgaliotinis. ADIS naudotojai jungdamiesi prie posistemių pagal suteiktas teises gali įrašyti informaciją arba ją tik tikrinti pagal atliekamas roles. Šios sistemos administratorius suteikia teises ir jas panaikina, jeigu naudotojas atleidžiamas iš valstybės tarnybos ar darbo, keičia darbo vietą ar jo tiesioginis vadovas pateikia prašymą dėl prieigos parametrų pakeitimo / panaikinimo, taip pat kai nustatomas neteisėtas IS duomenų naudojimas ar IS administratoriui kyla įtarimų, kad IS naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti IS arba joje apdorojamų duomenų saugą (audituojamu laikotarpiu tokių atvejų nebuvo).	● Maža rizika
1.8 Saugos incidentų stebėsena	Saugos incidentai neaptinkami laiku, kas neleidžia imtis atitinkamų priemonių, kad būtų išspręsti saugos pažeidimai.	Saugumo incidentų valdymo procesas apibrėžtas tvarkose, proceso aprašas parengtas vadovaujantis LST ISO/IEC 27001:2006 standartu. ADIC incidentų registracijos žurnale neužfiksuota nė vieno saugumo incidento, nes nė vieno neįvyko, kaip teigia saugos įgaliotinis. ADIC incidentų valdymo proceso tvarka neapima IT paslaugų tarnybos veiklos aprašymo, todėl jos darbai vyksta pagal nerašytinas taisykles. Nuo 2011 m. centre naudojamas elektroninis sutrikimų registravimo žurnalas, šie incidentai klasifikuojami pagal veiklas. IT paslaugų tarnyba konsultuoja ir teikia informaciją asmens tapatybės dokumentų prašymo priėmimo įstaigų darbuotojams, asmens tapatybės dokumentų gamybos darbuotojams, tačiau ne visi paklausimai registruojami, todėl IT pagalbos tarnyba negali atlikti tendencijų ir esminių priežasčių analizės. Nustatyta, kad ADIC IT priežiūros skyriaus specialistų ir priežiūros paslaugų tiekėjų atlikti profilaktiniai darbai neregistruojami el. sutrikimų registravimo žurnale, jie fiksuojami popieriniame dokumente.	● Maža rizika
1.9 Virusų ir kenkėjiškų programų aptikimas	Dėl virusų ir kenkėjiškų programų prarasti, pakeisti ar sunaikinti duomenys.	Saugaus elektroninės informacijos tvarkymo taisyklėse nustatytos techninės ir kitos saugos priemonės, kurios faktiškai įgyvendintos: siekiant užkirsti kelią, aptikti ir pašalinti kenkėjiškas programas naudojamos vidinio ir išorinio tinklo ugniasienės, asmens tapatybės dokumentų gamybos proceso saugumui užtikrinti naudojama centralizuotai valdoma antivirusinė programinė įranga ir nepageidaujamo turinio valdymo įranga. Naudojamos programinės ir techninės tinklo užkardos priemonės, kurios atpažįsta ir blokuoja paplitusių virusų ar „kirminų“ siunčiamus paketus, kenkėjiškus kodus, vykdomas reguliarus programinės įrangos atnaujinimas, gamintojo siūlomi atnaujinimai diegiami laiku. Naudotojams suteiktos ribotos teisės, kompiuterinę įrangą priežiūri IT priežiūros skyriaus darbuotojai, nustatytos procedūros kaip turi elgtis sistemos naudotojas jei įtaria kad jo	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		kompiuteris paveiktas (užkrėstas) kenksmingo kodo (virusų).	
1.10 Ryšių sauga	Duomenų perdavimo metu prarasti, pakeisti ar sunaikinti duomenys, konfidencialumo praradimas.	Viešaisiais telekomunikaciniais tinklais perduodamos ADIS elektroninės informacijos konfidencialumas užtikrinimas naudojant šifravimą, VPN, skirtines linijas, Saugų valstybinį duomenų perdavimo tinklą ir kt. priemones. Siekiant užtikrinti autentiškumą ir duomenų apsaugą, naudojami saugūs duomenų perdavimo protokolai, kriptografiniai algoritmai ir tinklo kodavimas (PKI). Duomenų formavimas vykdomas naudojant naršyklę ir saugų duomenų siuntimo protokolą (S–HTTP) užtikrinantį privatų ir saugų ryšį tarp kliento ir serverio. Kokybė tikrinama naudojant kliento–serverio principu veikiančią patikros taikomąją programą, jungiantis saugiu ryšiu (TLS/SSL), išrašymo įrenginiai valdomi naudojant naršyklę ir saugų ryšį (TLS/SSL ir terminalas). Proceso metu jautri informacija neperduodama viešaisiais tinklais, tarp valstybės institucijų naudojamas uždaras telekomunikacinis tinklas, veikiantis TCP/IP duomenų perdavimo protokolu ir atskirtas nuo bendro naudojimo tinklų. Visais atvejais „jautriausi duomenys“ (pvz.: pirštų antspaudai) šifruojami, o konkrečias funkcijas, kai vykdomi duomenų mainai, gali atlikti tik įgaliojimus turintys asmenys. Sertifikatais keičiamasi tik iš sertifikuotų darbo vietų, informacija koduojama PGP programa. ADIC koduota informacija keičiasi su Valstybinės sienos apsaugos tarnyba, kuri atlieka kelionės dokumentų ir pirštų atspaudų nuskaitymo patikrą. Jautri informacija neperduodama paslaugos teikėjams, išskyrus įstatymų numatytus atvejus.	Maža rizika
1.11 Informacijos klasifikavimas	Nesuklasifikavimus informacijos – prarasta informacija ar pažeistas konfidencialumas.	ADIC neklasifikuoja valdomos el. informacijos, nenustatyti svarbos kriterijai, todėl tai gali padaryti žalą vieno ar kelių asmenų teisėtiems interesams, ir asmens tapatybės dokumentų apsaugai, o tai gali turėti neigiamų padarinių institucijos veiklai, gali būti taikomos perteklinės saugos priemonės. ADGIS duomenų saugos nuostatuose priskirta II kategorijai, bet taikomos nepakankamos saugos užtikrinimo priemonės: nenumatytos atsarginės patalpos, kasmet neatliekamas saugos atitikties vertinimas. Auditoriai pažymi, kad ADIC vykdydamas asmens tapatybės dokumentų išrašymą, apdoroja gautus asmens tapatybės dokumentų gamybai prašymus su asmens duomenimis, įskaitant biometrinius, tvarkant duomenis nesilaikoma asmens duomenų apsaugos reikalavimų. Įgyvendinant patvirtintų saugos reikalavimų nuostatas, ADIC iki 2015-07-01 turi peržiūrėti IS klasifikavimą ir atnaujinti IS priskirtas saugos kategorijas, nurodyti kriterijus, pagal kuriuos priskirtina atitinkama kategorija. ADIC kai kurie duomenys klasifikuojami pagal įslaptintos informacijos teisės aktų reikalavimus. Audito metu įsitikinta, kad įslaptinta informacija darbuotojams prieinama tik pagal tiesiogiai susijusias funkcijas, centre įrengtos patalpos apdoroti tokią informaciją. Blankų gamintojai ir įrangą aptarnaujantys tiekėjai turi leidimus dirbti ar susipažinti su informacija, turinčią slaptumo žymą.	Vidutinė rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
1.12 Fizinė ir aplinkos sauga	Dėl neefektyvių ar nesamų fizinės apsaugos priemonių prarasti, pakeisti ar sunaikinti duomenys.	Taikomos fizinės ir aplinkos saugos priemonės apsaugo nuo asmens dokumentų proceso duomenų pakeitimo ar praradimo. ADIC fizinė sauga gerai suprojektuota ir įgyvendinta, patekimas į teritoriją apribotas, aplinka stebima, patekti į patalpas neautorizuotiems asmenims neįmanomas. Visose patalpose įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų. Patekti į tarnybinę stočių patalpą įmanoma, sistemai patvirtinus autorizuotų darbuotojų biometrinius piršto duomenis. Tarnybinių stočių patalpoje įrengtos įsibrovimo ir priešgaisrinės signalizacijos bei, automatinė gesinimo sistemos, apribota fizinė prieiga prie tarnybinių stočių, įdiegta įrangos, aplinkos, elektros tinklų ir kitų kritinių pokyčių stebėjimo sistema, dubliuota oro kondicionavimo sistema, drėgmės kontrolės įranga, dujinė automatinė gaisro gesinimo sistema ir įrengtas elektros tiekimas techninei įrangai per nenutrūkstamo maitinimo šaltinį su įtampos filtru. Nustatyta, kad pagal techninius parametrus nepertraukiamos srovės šaltiniai užtikrina 15 min. trumpesnį veikimą nei nustatyta tvarkose, bet naudojamas dyzelinis generatorius, kuris užtikrina nepertraukiamą tarnybinių stočių veikimą sutrikus elektros tiekimui. Naudojamos tinkamos fizinės kontrolės priemonės, kurios apsaugo nuo nepageidaujamų grėsmių, stebima svarbiausia techninė įranga (asmens tapatybės dokumentų gamybos įranga, tarnybinės stotys, vidaus duomenų perdavimo tinklo mazgai, dubliuotos ryšio linijos). Taikomos apsaugos priemonės mažina įrangos vagystės, informacijos atskleidimo iš išmestų ar pakartotinam naudojimui skirtų laikmenų, nesankcionuotą informacijos atskleidimo riziką: nustatytos nešiojamų kompiuterių naudojimo ne institucijos patalpose taisyklės, nenaudojamos įrangos kietieji diskai nenaikinami, juos saugo saugos įgaliotinis specialiose patalpose.	● Maža rizika
1.13 Duomenų pasiekiamumas (įskaitant atsargines kopijas)	Nuolatinis duomenų praradimas arba nepasiekiami duomenys kai jų reikia.	Audituojamu laikotarpiu duomenų praradimo / nepasiekiamumo atvejų nenustatyta, bet įvertinę ADIC pasirengimą tęsti veiklą jei įvyktų incidentas ar kritinis sistemos gedimas, auditoriai įsitikino, kad tinkamai nepasiruošta užtikrinti veiklos tęstinumą. Centras vadovaujasi 2012 m. patvirtintu IS veiklos tęstinumo valdymo planu, kuris atitinka jam keliamus turinio reikalavimus, tačiau jis nesuderintas teisės aktų nustatyta tvarka, peržiūrimas rečiau negu kartą per metus ir tik vieną kartą buvo išbandytas. Veiklos valdymo ir atkūrimo principų plane numatyta atkurti pagrindinę infrastruktūrą, reikalingą ADGIS veikti, tačiau nedetalizuotos kritiškiausios IS funkcijos, nenumatytas toleruotinas veiklos atkūrimo laikas, nėra sąryšio tarp veiklos tęstinumo ir veiklų atstatymo planų. IS veiklos tęstinumo valdymo plane deklaruojama, kad atsarginės patalpos, skirtos IS veiklai atkurti numatytos, tačiau faktiškai ADIC neturi tokių patalpų. Pagal tvarkomų duomenų svarbą valstybės mastu ADGIS taikoma antroji informacinių sistemų klasifikavimo kategorija, todėl pagal teisės aktų reikalavimus IS neveikimo laikotarpis negali būti ilgesnis negu 12 val. Asmens dokumentų išrašymo centras nusistatė 4 val. toleruotiną neveikimo laiko trukmę (angl. Acceptable Interruption	▲ Didelė rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
		Window), tačiau šis parametras nedokumentuotas. Auditorių nuomone, atlikus tik vieną veiklos atkūrimo bandymą, centras neįsitikino koks būtų realus veiklos atkūrimo laikas. Nedetalizuota kokios informacijos atsarginės kopijos turi būti daromos, todėl kiekvieną dieną kopijuojama duomenų bazės struktūra su duomenimis. Pagal patvirtintą tvarką saugos įgaliotinis ne rečiau negu kartą per metus turi organizuoti duomenų atkūrimo bandymą iš atsarginių IS elektroninių informacijos kopijų, tačiau toks bandymas audituojamu laikotarpiu nebuvo atliekamas. Nustatyta, kad dalies atsarginių kopijų laikymas atitinka reikalavimus, tačiau pagrindinės biometrinių dokumentų personalizavimo sistemų kopijos saugomos tarnybinių stočių patalpose, todėl įvykus incidentui šiose patalpose, taip pat būtų prarastos. 2012 ir 2014 metų rizikų planuose numatyta aukštos tikimybės grėsmė dėl aparatinės įrangos gedimo, nes iki šiol neįvertinta biometrinių duomenų registravimo įrangos reali būklė ir neaišku kas ir kada priims sprendimą dėl tolesnio įrangos naudojimo ar keitimo.	
1.14 Duomenų konfidencialumo pažeidimų prevencija ir aptikimas	Neatpažintas konfidencialios informacijos praradimas.	ADIC įsipareigojęs atitikti teisės aktų reikalavimus, peržiūrėti ir įvertinti esamus veiklos procesus ir nuolat gerinti teikiamų paslaugų kokybę. Siekiant išsiaiškinti ir reaguoti į pažeidimus ar neatitikimus centre pagal Informacijos saugos valdymo sistemos procedūras vykdomas atitikčių valdymas ir vidaus auditai. Duomenys apie naudotojo veiksmus IS saugomi 1 mėnesį, auditoriai įsitikino, kad atsekamumas užtikrinamas. Pagal nustatytas prieigos prie IS teises duomenis įrašyti, keisti ir atnaujinti gali tik autorizuoti IS naudotojai. Registruojamas duomenų pakeitimą atlikęs naudotojas, fiksuojamas duomenų keitimo laikas. Visi naudotojai ir sistemos procesai unikaliai identifikuojami. Prieigai suteikti naudojamos iš anksto nustatytos ir iš anksto apibrėžtos taisyklės, funkcijos apibrėžtos pagal mažiausiai privilegijų suteikimo principą.	● Maža rizika

Su biometrinių asmens tapatybės dokumentų išdavimu susijusios IS/IT infrastruktūros valdymas turi trūkumų ir ne visos kontrolės priemonės veiksmingos:

- Nuo 2002 metų Lietuvoje pasai, kiti kelionės ir asmens tapatybės dokumentai išrašomi centralizuotai Asmens dokumentų išrašymo centre ADIS priemonėmis, šią sistemą naudoja visos procese dalyvaujančios įstaigos, tačiau nepriskirtas sistemos valdytojas ir duomenų valdymo įgaliotinis, kaip nustato teisės aktai.
- Nenustatyta kas turi užtikrinti ADIS duomenų saugą, kol vyksta asmens tapatybės dokumentų gaminimas, kokiomis priemonėmis turi būti saugomi duomenys gamybos metu, kas atsako už duomenų saugojimą ir kokį terminą turi būti saugomi, siekiant užtikrinti jų konfidencialumą, vientisumą ir prieinamumą. Audito metu nebuvo patvirtinti sistemos nuostatai, neparengti saugos politiką įgyvendinantys dokumentai, bet sistemos tvarkytojų ir jų teisių administravimo sistema užtikrina, kad kiekvienas tvarkytojas gali vykdyti tik tas funkcijas, į kurias teises suteikė administratorius. ADIC įdiegta Informacijos saugumo valdymo sistema pagal ISO 27000 standarto reikalavimus, bet centro veikla neatitinka teisės aktų reikalavimų – ADIS ir ADGIS neįteisintos teisės aktų nustatyta tvarka.

- Nustatytas atvejis kai reikalavimai įsigyjamoms ADGIS priežiūros paslaugoms neatitiko teisės aktų reikalavimų IS veiklos tęstinumui užtikrinti, todėl kritinio IT gedimo atveju nebūtų vykdomas asmens tapatybės dokumentų išdavimas. Įsigydamas ADIS ir ADGIS priežiūros paslaugas ADIC neįvertino, kad pagal teisės aktų reikalavimus antros kategorijos informacinės sistemos valdytojas turi nusistatyti ne mažesnį nei 12 val. neveikimo laikotarpį. ADIC sudarė 3 metų sutartį asmens dokumentų išrašymo ir programinės įrangos priežiūros paslaugoms atlikti, tačiau joje nenumatyti sutrikimų šalinimo ir maksimalūs įrangos dalies funkcijų atstatymo laikai, taip pat nenumatytas laikas, per kurį tiekėjas įsipareigotų reaguoti įvykus įrangos gedimui. Šie sutarčių trūkumai gali turėti įtakos asmens dokumentų išrašymui.
- ADIS kurti pradėta 2001 m. ir iki dabar modifikuojama, tačiau neaiški jos struktūra, nes nėra vientisos ir išbaigtos specifikacijos. Kūrimo pradžia, eiga ir pabaiga neatitinka IS kūrimo reikalavimų, nors jos priemonėmis centralizuotai išrašomi asmens tapatybės dokumentai, tvarkomi jų duomenys.
- ADIC 2013 m. neatliktas IS rizikos įvertinimas, o 2014 m. vertinta tik dalis dokumentų išrašymo proceso, atlikta tik ADIC vykdomos veiklos poveikio analizė.
- ADIC neklasifikuoja valdomos el. informacijos, nenustatyti jos svarbos kriterijai, todėl tai gali turėti neigiamų padarinių institucijos veiklai, gali būti taikomos perteklinės saugos priemonės. Pagal nustatytą kategoriją ADGIS taikomos nepakankamos saugos užtikrinimo priemonės: nenumatytos atsarginės patalpos, ne kasmet vertinama saugos atitiktis.
- ADIC tinkamai nepasiruošta užtikrinti veiklos tęstinumą, nes centras vadovaujasi nuo 2012 m. neatnaujintu IS veiklos tęstinumo valdymo planu, nedetalizuotos kritiškiausios IS funkcijos, nenumatytas toleruotinas veiklos atkūrimo laikas, nėra sąryšio tarp veiklos tęstinumo ir veiklų atstatymo planų. ADIC neturi atsarginių patalpų skirtų atkurti IS veiklą, ne visų atsarginių kopijų laikymas atitinka reikalavimus, todėl įvykus incidentui tarnybinių stočių patalpose, kopijos taip pat būtų prarastos.

Siekiant užtikrinti tinkamą naudojamos ADIS valdymą ir vientisą jos plėtrą, turėtų būti paskirtas šio proceso ir informacinės sistemos valdytojas. Taip būtų užtikrinta, kad visose asmens dokumentų išdavimo procese dalyvaujančiose įstaigose būtų įdiegtos tinkamos saugos priemonės, užtikrintas techninės ir programinės įrangos suderinamumas, valstybės mastu būtų žinomos proceso sąnaudos ir įvertintas efektyvumas.

Įgyvendinant Vyriausybės patvirtintų saugos reikalavimų nuostatas Asmens dokumentų išrašymo centras iki 2015-07-01 turi peržiūrėti IS klasifikavimą ir taikomas saugos priemones. Atsižvelgiant į pastebėtus IT valdymo trūkumus, tikslinga tobulinti IT veiklos tęstinumo užtikrinimo procedūras ir numatyti efektyvias paslaugų teikėjų veiklos kontrolės priemones.

2.2. Atitiktis teisės aktų ir kitiems reikalavimams

Vertinta ar biometrinių asmens dokumentų išdavimo procedūros, IS / IT valdymas ir išorės paslaugų teikėjai atitinka teisės aktuose nustatytus reikalavimus:

- turi būti įdiegtas procesas užtikrinantis nuolatinę atitiktį teisės aktams ir kitiems reikalavimams, jis turi apimti taikytinų teisinių ir kitų reikalavimų nustatymą.
- turėtų būti užtikrinta, kad perduodant IS/ IT tvarkymo funkcijas procedūros ir paslaugų teikėjų veikla atitiktų teisės aktų reikalavimus. Turėtų būti užtikrinta atitiktis teisiniams reikalavimams, kai paslaugas teikia išorės paslaugų teikėjai (įstaigoje ar nuotoliniu būdu).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
2.1 Atitiktis	Neatitiktis teisės aktų ir reguliavimo reikalavimams.	Asmens tapatybės dokumentų išdavimo procesas atitinka teisinius ir kitus reikalavimus, ADIC kokybės vadybos sistema sertifikuota pagal LST EN ISO 9001:2008 Kokybės vadybos sistemos standarto reikalavimus, asmens tapatybės dokumentų išrašymo (gamybos proceso) veikla planuojama užtikrinant įstatymų ir kitų teisės aktų reikalavimų vykdymą. Nustatyta, kad ADIC nesilaiko kai kurių IS/IT valdymo teisės aktų reikalavimų (IS kūrimo, saugos užtikrinimo ar atsakingų asmenų paskyrimo procedūrų), tačiau tai kol kas neturėjo neigiamų pasekmių – nenustatyta finansinių nuostolių ar duomenų praradimo atvejų.	Vidutinė rizika
2.2 Trečiosios šalys	IS/ IT tvarkymo perdavimas ir paslaugų teikėjų veikla neatitinka teisės aktų ir kitų reikalavimų.	Asmens tapatybės dokumentų blankų ir IT paslaugos perkamos pagal Viešųjų pirkimų įstatymo reikalavimus, tiekėjams keliami kvalifikaciniai ir ekonominiai–finansiniai reikalavimai, yra numatomi sutartyse. Kiekvienai sutarčiai priskiriamas atsakingas asmuo, kuris stebi, kaip vykdoma sutartis ir laikomasi sutartinių įsipareigojimų. Audito metu įvyko teisės aktų pokyčių dėl kurių ADIC 2015 m. turės peržiūrėti veiklos procesus ir sutartis su trečiosiomis šalimis – planuojami techniniai infrastruktūros pokyčiai, dėl kurių reiks pakeisti duomenų gavimo/ teikimo sąlygas.	Maža rizika

Asmens tapatybės dokumentų išdavimo procesas atitinka teisinius ir kitus reikalavimus, tačiau ADIC nesilaiko kai kurių IS/IT valdymo teisės aktų reikalavimų (IS kūrimo, saugos užtikrinimo ar atsakingų asmenų paskyrimo procedūrų, detaliau 2.1 poskyryje), tačiau tai kol kas neturėjo neigiamų pasekmių – nenustatyta finansinių nuostolių ar duomenų praradimo atvejų.

2.3. Kaštų ir naudos analizė

Vertinta ar biometrinių asmens dokumentų išdavimo procesas (operacijų, saugumo, IS / IT valdymas) efektyvus:

- nustatytos procedūros, siekiant užtikrinti, kad IS/IT naudojimas atitinka įstaigos tikslus ir nuolat teikia laukiamą naudą išduodant biometrinius asmens tapatybės dokumentus;
- žinomi gamybos proceso vidiniai ir išoriniai, tiesioginiai ir netiesioginiai kaštai, analizuojami planuotų ir faktinių išlaidų pokyčiai. Proceso kaštai apskaičiuojami pagal patiriamas dokumentų išdavimo išlaidas;
- prižiūrimas IS/IT turtas ir investicijos, jų naudojimas ir paskirstymas per visą ekonominį gyvavimo ciklą. IT/IS lėšos derinamos su esamais ir būsimais strateginiais tikslais ir veiklos iniciatyvomis, reguliariai vertinamos IS/IT iniciatyvos (pvz.: naujų paslaugų kūrimas, efektyvumo didinimas, gebėjimų reaguoti į klientų poreikius tobulinimas).

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
3.1 Naudos sukūrimas	Neteisingai panaudotos IT investicijos, neskaidri IT pridėtinė vertė, neteisingas IT pridėtinės vertės suvokimas.	Valstybės mastu įstaigos nevertina ar biometrinių asmens tapatybės dokumentų išdavimo procesas (operacijų, saugumo, IS / IT valdymas) efektyvus ir neturi duomenų apie kitų dalyvaujančių institucijų kaštus. Nė viena institucija neturi tikslios informacijos apie valstybės mastu surinktas pajamas už asmens tapatybės dokumentų išdavimą, neatlieka IT kaštų ir naudos vertinimo. ADIS ir bendrą IT pridėtinės vertės valdymą apsunkina tai, kad IT turtas esantis sistemoje priklauso skirtingoms įstaigoms ir nėra bendro įrangos priežiūros ir vystymo valdymo. Siekiant įvertinti IT investicijų naudą, tikslinga atlikti asmens tapatybės dokumentų išdavimo kaštų ir naudos apskaičiavimą įtraukiant visų susijusių veiklos grandžių kaštus.	Vidutinė rizika
3.2 Kaštų aiškumas ir padengimas	Neteisingai panaudotos IT investicijos, neskaidri IT pridėtinė vertė, netinkama paslaugų kainodara.	Teisės aktai numato, kad dalis asmens tapatybės dokumentų (pvz.: diplomatinis ir tarnybinis pasai) išduodami nemokamai, už kitų asmens dokumentų išdavimą mokama rinkliava. Valstybės rinkliavos dydis apskaičiuojamas, vadovaujantis Lietuvos Respublikos rinkliavų įstatymu, atsižvelgiant į paslaugos suteikimo išlaidas, kurias sudaro išlaidos: darbui, susijusiam su paslaugos suteikimu, apmokėti; juridinę galią turinčio dokumento blankui pagaminti; teisės aktų nustatytų reikalavimų įvykdymui patikrinti. Biometrinių asmens dokumentų išdavimo IS/ IT įranga įsigyta ir prižiūrima panaudojant valstybės biudžeto lėšas. Kiekviena biometrinių asmens dokumentų išdavimo procese dalyvaujanti įstaiga vertina IT investicijų panaudojimą, analizuojami pokyčiai tarp prognozuotų ir faktinių kaštų, įvertinus rezultatus koreguojamas įstaigos IT biudžetas ir atliekamas lėšų poreikio perskirstymas, tačiau valstybės mastu nėra duomenų apie asmens dokumentų išdavimo procesui skirtų IT investicijų panaudojimą.	Maža rizika
3.3 Efektyvumas ir kaštų valdymas	Nepakankami pajėgumai, žinios ir ištekliai pasiekti norimus tikslus. Paskirstant išteklius naudojami netinkami prioritetai.	Kadangi nuo naudojamų IT sistemų funkcionalumo priklauso asmens tapatybės dokumentų išdavimo proceso efektyvumas, IT finansuojama tiek, kad būtų įvykdytos būtinos ES reikalavimų ir saugos standartų rekomendacijos. Biometrinių asmens tapatybės dokumentų išrašymo įranga iki šiol veikia patikimai ir atnaujinama keičiant susidėvėjusias dalis ir išnaudojus dalių išteklius. IT investicijų poreikis ir prioritetai peržiūrimi kasmet įvertinant turimos techninės įrangos būklę bei numatomus teisės aktų pakeitimus. Asmenų nuomonė ir grįžtamasis ryšys gaunamas ir analizuojamas atliekant klientų nuomonės tyrimus. Esant reikalui atliekamos galimybių studijos siekiant įvertinti planuotinų investicijų apimtis bei tinkamai pasirinkti reikalavimų įgyvendinimo priemones.	Maža rizika

Valstybės mastu įstaigos nevertina ar biometrinių asmens dokumentų išdavimo procesas (operacijų, saugumo, IS / IT valdymas) efektyvus, neturi duomenų apie

kaštus kitų institucijų, dalyvaujančių procese. ADIS ir bendrą IT pridėtinės vertės valdymą apsunkina tai, kad IT turtas esantis sistemos sudėtyje, priklauso skirtingoms įstaigoms ir nėra bendro įrangos priežiūros ir vystymo valdymo.

2.4. Žmogiškųjų išteklių valdymas

Vertinta ar darbuotojai, rangovai ir trečiųjų šalių atstovai supranta savo pareigas, yra tinkami jas atlikti, ar procedūros padeda sumažinti vagystės, sukčiavimo ar piktnaudžiavimo riziką:

- visi predentuojantys įsidarbinti asmenys, rangovai ir trečiųjų šalių atstovai turėtų būti atidžiai patikrinami (patikrinimas, atsiliepimai ir kt.). Ypač svarbių funkcijų ar gamybos vietų personalas turtų būti tikrinamas reguliariai, pvz., kas 1–2 metus. Darbuotojai, rangovai ir trečiųjų šalių atstovai turi pasirašyti konfidencialumo susitarimus dėl saugos įsipareigojimų ir atsakomybės.
- Kontrolės priemonės turi užtikrinti, kad darbuotojams, rangovams ir trečių šalių atstovams baigus darbą įstaigoje bus gražinta visa įranga ir pašalintos visos prieigos teisės. Keičiantis darbuotojo pareigoms ar darbuotojams turi būti užtikrintas prieigos teisių valdymas.

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
4.1 Žmogiškiesiams ištekliams taikomos saugos procedūros	Vagystė, sukčiavimas ir piktnaudžiavimas asmens tapatybės dokumentais, ištekliais, dokumentų blankais ir duomenimis.	Audito metu nenustatyta atvejų, kai dėl personalo ar paslaugų teikėjų kaltės būtų atskleisti, prarasti asmens tapatybės dokumentai ar jų blankai. Taikomos kontrolės priemonės užtikrina personalo kvalifikacijos atitiktį specialiesiems reikalavimams, darbuotojai, kurie atlieka asmens tapatybės dokumentų prašymų priėmimo/išdavimo funkcijas iš anksto pasirašytinai supažindinami su tvarkomis dėl informacijos apdorojimo saugumo ir atsakomybės. Visi migracijos tarnybų ir ADIC darbuotojai turi leidimą dirbti su įslaptinta informacija ir yra pasirašę pasižadėjimus ją saugoti. Kompetentingos valstybės institucijos įvertino ir patvirtino, kad blankų tiekėjas gali automatizuotai apdoroti įslaptintą informaciją, o šios įmonės darbuotojams išduoti leidimai dirbti ar susipažinti su tokia informacija. Asmens tapatybės dokumentų blankų tiekėjas įsipareigoja laikytis sutartinių reikalavimų įsigyjant prekių gamybai būtinas originaliąsias ir spausdinimo medžiagas ir priemones, neatskleisti tretiesiems asmens komercinės paslapties, kurią gavo ar sužinojo vykdydami sutartį. Su blankus gaminančiais darbuotojais, visais ADIC ir migracijos tarnybų darbuotojais, kurie vykdo prašymų priėmimo / išdavimo funkcijas, pasirašyti pasižadėjimai dėl neviešinamos informacijos neatskleidimo.	● Maža rizika
4.2 Žmogiškiesiams ištekliams taikomos saugos procedūros	Vagystė, sukčiavimas ir piktnaudžiavimas asmens tapatybės dokumentais, ištekliais, dokumentų blankais ir	Įeigos į asmens tapatybės dokumentų gamybos ir blankų saugojimo vietas ir sistemos prieigos teisių valdymo procedūros užtikrina, kad prieigą prie duomenų / dokumentų turėtų tik tie asmenys, kuriems tai būtina vykdant funkcijas. Asmens tapatybės dokumentų blankų tiekėjai įsipareigoja neatskleisti ir nenaudoti neviešintinos informacijos ir komercinės paslapties iki sutarties nutraukimo ar pabaigimo. Įvykdžius sutartį, tiekėjas įsipareigoja ir privalo grąžinti visą perduotą įslaptintą informaciją, taip pat perduoti sukurtą įslaptiną informaciją. ADIC	● Maža rizika

Audito sritis	Rizika	Srities vertinimas	Įvertinimas
	duomenimis.	darbuotojai rašytinai įsipareigoja darbo vietoje ir už organizacijos ribų su asmenimis, nesusijusiais su įstaigos veikla, neaptarinėti jokios informacijos, kurią sužinojo. Pasibaigus darbo santykiams darbuotojai rašytinai įsipareigoja toliau saugoti darbo metu sužinotą informaciją.	

Su blankų gamybą vykdančiais darbuotojais, visais ADIC ir migracijos tarnybų darbuotojais, kurie vykdo prašymų priėmimo / išdavimo funkcijas pasirašyti pasižadėjimai dėl neviešinamos informacijos neatskleidimo, procedūros užtikrina, kad prieigą prie duomenų / dokumentų turėtų tik tie asmenys, kuriems tai būtina vykdant funkcijas.

Informacinių sistemų ir infrastruktūros
audito departamento direktorius Dainius Jakimavičius

Informacinių sistemų audito skyriaus
vyriausiasis valstybinis auditorius Rimgaudas Gamulis

Valstybinio audito ataskaitos kopijos pateiktos:

Lietuvos Respublikos Seimo Audito komitetui

Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komitetui

---

Auditas atliktas, vykdant 2014-01-17 pavedimą Nr. P-90-2

Auditą atliko valstybinių auditorių grupė:

Rimgaudas Gamulis (grupės vadovas)

Loreta Tomickytė-Šajaukienė

PRIEDAI

Valstybinio audito ataskaitos
„Biometrinių asmens dokumentų gamyba“
1 priedas

Pagrindinė informacija apie auditą, duomenų rinkimo ir vertinimo metodai

3 lentelė. Pagrindinė informacija apie auditą.

Audito objektas	biometrinių asmens dokumentų gamyba.
Audito tikslas	įvertinti biometrinių asmens dokumentų išdavimo valdymą ir kontrolę.
Audito subjektai	Vidaus reikalų ministerija, Asmens dokumentų išrašymo centras prie Vidaus reikalų ministerijos.
Audituojamas laikotarpis	2013 m., 2014 m. I pusmetis, tendencijų ir pokyčių analizei naudojami ir kitų laikotarpių duomenys.

4 lentelė. Audito duomenų rinkimo ir vertinimo metodai.

Metodai	Tikslai
Dokumentų analizė – nagrinėjome Vidaus reikalų ministerijos, Užsienio reikalų ministerijos, Gyventojų registro tarnybos, Asmens dokumentų išrašymo centro prie Vidaus reikalų ministerijos ir Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdybos dokumentus susijusius su biometrinių asmens dokumentų gamyba (dokumentų užsakymo / keitimo, prašymų / duomenų surinkimo, dokumentų gamybos, pristatymo ir naikinimo procesai) ir kitų susijusių specifinių procesų valdymu (pvz.: IS/IT ir informacijos valdymas).	Išsiaiškinti ir nustatyti teisinio reglamentavimo, planavimo ir stebėsenos, funkcijų pasiskirstymo, biometrinių asmens dokumentų gamybos ir kitų susijusių specifinių procesų trūkumus ir problemas. Taip pat išsiaiškinti, kokias problemas įžvelgia audituoti subjektai.
Pokalbiai su Vidaus reikalų ministerijos, Užsienio reikalų ministerijos, Gyventojų registro tarnybos darbuotojais. Taip pat Asmens dokumentų išrašymo centro prie Vidaus reikalų ministerijos ir Vilniaus apskrities vyriausiojo policijos komisariato Migracijos valdybos darbuotojais.	
Duomenų analizė ir skaičiavimas: biometrinių asmens dokumentų užsakymo / keitimo, prašymų / duomenų surinkimo, gamybos, pristatymo ir naikinimo pokyčių analizė per audituojamą laikotarpį. Taip pat biometrinių asmens dokumentų gamybos ir šio proceso išlaidų / šiam tikslui renkamų mokesčiai skaičiavimas.	Nustatyti, biometrinių asmens dokumentų gamybos ir kitų susijusių specifinių procesų trūkumus ir pokyčius audituojamu laikotarpiu. Pateikti konkrečius pavyzdžius audito ataskaitoje.
Analizavome dokumentų užsakymo / keitimo, prašymų / duomenų surinkimo, dokumentų gamybos, pristatymo ir naikinimo procesų, taip pat IS/IT ir informacijos valdymo, procesų atitiktį šiems teisės aktų reikalavimams: LR asmens tapatybę patvirtinančių dokumentų išdavimo klausimais (https://www.dokumentai.lt/viewpage.php?page_id=11); LR pilietybės klausimais (https://www.dokumentai.lt/viewpage.php?page_id=12); Užsieniečių teisinės padėties LR klausimais (https://www.dokumentai.lt/viewpage.php?page_id=13); Valstybės tarnautojo pažymėjimų išdavimo klausimais (https://www.dokumentai.lt/viewpage.php?page_id=13); Kitais klausimais (http://www.vrm.lt/lit/Teises-aktai/258).	Įvertinti, ar biometrinių asmens dokumentų išdavimo procedūros, IS / IT valdymas (duomenų saugojimo / atsarginių kopijų darymo, prieigos prie duomenų ir duomenų perdavimo procedūros) ir išorės paslaugų teikėjai atitinka teisės aktuose nustatytus reikalavimus. Apibendrintus rezultatus / konkrečius pavyzdžius pateikti audito ataskaitoje.

Šaltinis – Valstybės kontrolė.

Valstybinio audito ataskaitos
„Biometrinių asmens dokumentų gamyba“
2 priedas

Rekomendacijų įgyvendinimo planas

Eil. Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės	Rekomendacijos įgyvendinimo terminas (data)
1.	Paskirti asmens tapatybės dokumentų išrašymo ir išdavimo procesų valdytoją, kuris užtikrintų šių procesų išteklių ir kaštų valdymą. Užtikrinti, kad įstaigų dalyvaujančių asmens tapatybės dokumentų išrašymo ir išdavimo procesuose, naudojama įranga būtų tinkamai prižiūrima, centralizuotai planuojamas jos atnaujinimas siekiant išvengti nesuderinamumo.	Vidaus reikalų ministerija	1.1 Bus parengti valstybės informacinės sistemos - Asmens dokumentų išrašymo sistemos (ADIS) nuostatai, kuriuose reglamentuojamas asmens dokumentų išrašymo ir įteikimo proceso dalyviai, jų teisės ir pareigos, paskiriamas valstybės informacinės sistemos valdytojas, tvarkytojai ir duomenų valdymo įgaliotinis. 1.2 Įteisinta Asmens dokumentų išrašymo sistema (ADIS)	2016-05-01
2.	Siekiant užtikrinti vientisą Asmens dokumentų išrašymo informacinės sistemos plėtrą, nustatyti IT valdymo atsakomybę – paskirti sistemos valdytoją, tvarkytojus ir duomenų valdymo įgaliotinį. Įteisinti naudojamą sistemą, parengiant teisės aktų reikalaujamus dokumentus, kuriuose būtų fiksuota sistemos tvarkomų duomenų apimtis, ryšiai su kitomis sistemomis / registrais ir numatytos taikytinos saugos užtikrinimo procedūros.	Vidaus reikalų ministerija		2016-08-01
3.	Siekiant geriau išnaudoti sukurtų paslaugų galimybes, informuoti asmenis apie galimybę el. būdu pranešti apie dingusį asmens tapatybės dokumentą ir vietas, kur galima patikrinti biometrinius duomenis, atsiimant pagamintus dokumentus.	Vidaus reikalų ministerija	Migracijos departamentas prie Vidaus reikalų ministerijos ir Policijos departamentas prie Vidaus reikalų ministerijos iki numatomos rekomendacijos įgyvendinimo datos parengia ir išplatina rekomendacijoje nurodytą informaciją.	2015-07-01
4.	Siekiant užtikrinti reikiamą saugos reikalavimų įgyvendinimą, įgyvendinti trūkstamas IT saugos priemones ir peržiūrėti Asmens dokumentų išrašymo centro IT veiklos tęstinumo reikalavimus.	Asmens dokumentų išrašymo centras prie VRM	4.1 Asmens dokumentų gamybos informacinė sistema (ADGIS) bus įteisinta, kaip 2 kategorijos informacinė sistema, parengiant teisės aktų reikalaujamus dokumentus, kuriuose bus fiksuota sistemos tvarkomų duomenų apimtis, ryšiai su kitomis sistemomis / registrais ir numatytos taikytinos saugos užtikrinimo procedūros. 4.2 Bus įgyvendintos trūkstamos IT saugos priemonės ir peržiūrėti Asmens dokumentų išrašymo centro IT veiklos tęstinumo reikalavimai. Bus suderintas ADGIS veiklos tęstinumo planas, atlikti plano bandymai. Bus detalizuotos kritiškiausios funkcijos	2015-12-31

Valstybinio audito ataskaitos
„Biometrinių asmens dokumentų gamyba“
2 priedo tęsinys

Eil. Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės	Rekomendacijos įgyvendinimo terminas (data)
5.	Siekiant užtikrinti, kad trečiųjų šalių paslaugos atitiktų veiklos poreikius: sutartyse su trečiosiomis šalimis dėl IT paslaugų nustatyti teisės aktų reikalavimus atitinkančias sąlygas, įtraukti nuostatas dėl paslaugų teikėjų veiklos kontrolės ir atsakomybės.	Asmens dokumentų išrašymo centras prie VRM	Sutartyse su trečiosiomis šalimis dėl IT paslaugų bus įtraukiamos nuostatos dėl paslaugų teikėjų veiklos kontrolės ir atsakomybės.	2015-09-01

Šaltinis – Valstybės kontrolė, Vidaus reikalų ministerija ir Asmens dokumentų išrašymo centras prie Vidaus reikalų ministerijos

Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais:

Lietuvos Respublikos vidaus reikalų viceministras Elvinas Jankevičius, tel. 8 5 271 7146, el. p. elvinas.jankevicius@vrm.lt