LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖ

VALSTYBINIO AUDITO ATASKAITA
UŽSIENIO REIKALŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ BENDROJI IR KŪRIMO KONTROLĖ

2013 m. sausio 31 d. Nr. VA-P-90-2-2
Vilnius

Auditas atliktas, vykdant 2012-06-15 pavedimą Nr. P-90-2

Auditą atliko valstybinių auditorių grupė:
Viktorija Mirošničenko (grupės vadovė)
Jurgita Musteikienė
Donatas Vitkus

Auditas pradėtas 2012-06-15
Auditas baigtas 2013-01-31

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

TURINYS

SANTRAUKA

Lietuvos Respublikos užsienio reikalų ministerija formuoja valstybės užsienio reikalų politiką, koordinuoja veiksmus, susijusius su naryste Europos Sąjungoje, atstovauja Lietuvos Respublikai ir jos piliečių teisėtiems interesams ir juos gina tarptautinėse organizacijose ir užsienio valstybėse, įgyvendina kitus ministerijos nuostatuose nurodytus veiklos tikslus[1].

Automatizuodama veiklos funkcijas, ministerija nuo 1999 m. naudoja įvairaus sudėtingumo informacines sistemas, kuriose kaupiami ir apdorojami duomenys, įskaitant asmens duomenis ir ypatingus asmens duomenis. Be to, ministerija naudoja tinklus ir sistemas, kuriomis automatizuotai apdorojama įslaptinta informacija su žyma ne aukštesne kaip „Riboto naudojimo“. Siekiant užtikrinti ministerijos informacinėse sistemose apdorojamų duomenų konfidencialumą, tikslumą ir sistemų darbo nenutrūkstamumą, turėtų būti vykdoma tinkama informacinių sistemų valdymo kontrolė.

Audito tikslas – įvertinti Užsienio reikalų ministerijos informacinių sistemų bendrąją ir kūrimo kontrolę.

Užsienio reikalų ministerija nuo 2009 m. pradžios pasiekė nemažą informacinių sistemų valdymo pažangą. Kryptingai informacinių sistemų plėtrai buvo parengtos vystymo gairės. Patvirtintas Informacinių sistemų funkcijų pokyčių valdymo tvarkos aprašas, kurio tikslas – valdyti ministerijos informacinių sistemų pokyčius, užtikrinant kokybišką reikalingų pokyčių įvykdymą ir diegimą minimaliai sutrukdant informacinių sistemų funkcionavimą. Informacinių sistemų saugai stiprinti parengta saugos politiką apimanti dokumentacija, įgyvendintos incidentų valdymo priemonės. Tačiau audito metu nustatyta informacinių sistemų valdymo ir saugos trūkumų: nėra aiškiai aprašyti turimi el. duomenų srautai (informacijos architektūros modelis); informacinių technologijų valdymas stokoja stipresnės veiklos procesų ir informacinių technologijų sąsajos; nepaskirti duomenų įgaliotiniai; informacinių sistemų rizikos vertinimas atliekamas ne kasmet, nerengiami rizikos mažinimo įgyvendinimo priemonių planai, neatnaujinti saugos politikos dokumentai, neišbandytas veiklos tęstinumo planas; informacinės sistemos modernizuojamos neatnaujinus arba neparengus jų nuostatų, specifikacijų; nepakankama kontrolė tvarkant asmens duomenis ir ypatingus asmens duomenis bei įslaptintą informaciją.

Audito metu nustatyta, kad Užsienio reikalų ministerijos informacinių sistemų vidaus kontrolės branda apibrėžiama kaip pirminis (*Ad Hoc*) procesas[2]. Norint pasiekti aukštesnį brandos lygį, turėtų būti stiprinamos veiklos procesų ir informacinių technologijų sąsajos, atnaujintos

[1] Lietuvos Respublikos Vyriausybės 1998-09-25 nutarimu Nr. 1155 patvirtinti Lietuvos Respublikos užsienio reikalų ministerijos nuostatai, 5 p.
[2] Pagal Gebos brandos modelį (angl. *Capability Maturity Model*, CMM).

Užsienio reikalų ministerijos informacinės sistemos vystymo gairės, kad jos apimtų visas ministerijos informacines sistemas, parengti ir patvirtinti visų ministerijos informacinių sistemų nuostatai. Ministerijos informacinių sistemų valdymą ir saugą apibrėžianti dokumentacija turi būti nuolat atnaujinama ir atitikti realią situaciją. Periodiškai turi būti vertinama rizika ir informacinių sistemų saugos atitiktis, užtikrinama vykdomų procesų stebėsena. Ministerijai rekomenduota apibrėžti informacinių sistemų architektūrą, tobulinti ministerijos informacinių sistemų saugos, veiklos tęstinumo, duomenų valdymo ir trečiųjų šalių teikiamų paslaugų užtikrinimo procesus.

Užsienio reikalų ministerija parengė pateiktų rekomendacijų įgyvendinimo planą (žr. ataskaitos 2 priedą).

Išvados

1. Užsienio reikalų ministerijoje nėra bendro visas informacines sistemas apimančio informacijos architektūros modelio. Ministerijai aiškiai neaprašius turimų elektroninių duomenų srautų (duomenų struktūros), gali prireikti papildomo laiko ir išteklių juos apdorojant, taip pat gali būti parenkamos nepakankamos informacijos saugą užtikrinančios priemonės (1.1 poskyris).

2. Informacinių technologijų valdymo organizacinė struktūra tobulintina, nes:

2.1. ministerijoje nėra mechanizmo, skirto kartu su vadovybe spręsti strateginius informacinių technologijų valdymo klausimus, kad pagrindinės veiklos poreikiai būtų siejami su informacinių technologijų teikiamomis galimybėmis (1.2 poskyris);

2.2. nepaskirti duomenų valdymo įgaliotiniai (1.2 poskyris);

2.3. vyksta didelė informacinių technologijų personalo kaita, tačiau audituojamu laikotarpiu nesuplanuota rezervinė darbuotojų pakaita ir jų pareigų perėmimas (1.2 poskyris).

3. Ministerijoje nustatyta informacinių sistemų saugos valdymo trūkumų:

3.1. informacinių sistemų rizikos vertinimai nebuvo atliekami kasmet, todėl neidentifikuoti ir detaliai neįvertinti šiuo laikotarpiu egzistavę informacinių sistemų rizikos veiksniai, galintys turėti įtakos informacijos saugai, nerengiamas ir netvirtinamas informacinių sistemų rizikos mažinimo (valdymo) priemonių planas (1.3 poskyris);

3.2. vidaus dokumentuose neapibrėžta, kokios konkrečios komponentės sudaro ministerijos informacines sistemas, todėl lieka neaiškus informacinių sistemų klasifikavimas pagal kategorijas, gali būti netiksliai nustatyti ministerijos informacinėse sistemose tvarkomos elektroninės informacijos apsaugos poreikis, prioritetai ir lygis (3.3 poskyris);

3.3. informacinių technologijų saugos atitikties vertinimas buvo atliktas tik vieną kartą (2012 m.) ir ne visi duomenų saugą reglamentuojantys dokumentai atnaujinti, todėl juose

numatytos informacinių sistemų saugos valdymo priemonės gali būti neveiksmingos (3.3 poskyris);

3.4. automatizuotai apdorojamos įslaptintos informacijos su žyma „Riboto naudojimo“ valdymas nepakankamai saugus, nes ministerijoje šios informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančios tvarkos nebuvo peržiūrimos ir atnaujinamos (3.4 poskyris);

3.5. naudotojų paskyrų valdymo procesas užtikrinamas nepakankamai, nes, nutrūkus darbuotojo darbo ar tarnybos teisiniams santykiams su Užsienio reikalų ministerija, dar kurį laiką gali būti palikta prieiga prie tarnybinio elektroninio pašto. Taip pat nustatyta neatitikčių tarp ministerijos Personalo departamento pateiktų darbuotojų sąrašų ir informacinių sistemų naudotojų sąrašų paskyrų valdymo sistemoje. Naudotojų paskyros yra apsaugotos slaptažodžiais, tačiau jų kompleksiškumo reikalavimai ne visose ministerijos informacinėse sistemose užtikrinami technologinėmis priemonėmis (netikrinamas slaptažodžių ilgis, simbolių skaičius) (3.3 poskyris).

4. Ministerija nepakankamai pasirengė užtikrinti informacinių sistemų veiklos tęstinumą nenumatytų situacijų atveju, nes:

4.1. nenumatyti informacinių sistemų veiklos tęstinumo atkūrimo prioritetai, todėl pirmiausia gali būti atkurti mažiau svarbūs ministerijos veiklos procesai (3.2 poskyris);

4.2. nenurodyti už informacinių technologijų įrangos priežiūrą atsakingi administratoriai, neparengta aktuali informacinių sistemų sąrankos dokumentacija (informacinių technologijų įrangos sąrašai, šios įrangos parametrai, kompiuterių tinklo fizinio ir loginio sujungimo schemos ir kt.), nepildomas duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašas, duomenų mainų sutartys sudarytos tik su dalimi duomenų teikėjų ir gavėjų, dėl to gali būti susidurta su atsakomybės ir paslaugų teikimo problemomis (3.1 ir 3.2 poskyris);

4.3. nebuvo organizuojamas informacinių sistemų veiklos tęstinumo valdymo plano elementų testavimas ir veiksmingumo išbandymas praktinių mokymų metu, todėl, įvykus incidentui, veiklos tęstinumo valdymo planas gali būti neefektyvus ir realiai neįvykdomas (3.2 poskyris);

4.4. incidento metu aktualūs informacinių sistemų duomenys gali būti neatkurti, nes nenustatytos detalios rezervinio duomenų kopijavimo procedūros, apimančios duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą ir duomenų atstatymą iš kopijų (3.4 poskyris).

5. Ministerija neįgyvendina organizacinių asmens duomenų tvarkymo automatiniu būdu priemonių, nes:

5.1. ne visi ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslai yra registruoti Asmens duomenų valdytojų valstybės registre, todėl asmenys neturi galimybės susipažinti su išsamia informacija apie savo asmens duomenų tvarkymą (3.4 poskyris);

5.2. nenustatė tvarkomų asmens duomenų saugos lygio, neparengė ir nepatvirtino rašytinės formos dokumento, kuriame būtų išdėstytos taikomos asmens duomenų saugos priemonės, kaip numato Asmens duomenų teisinės apsaugos įstatymas (3.4 poskyris).

6. Informacinės sistemos kurtos ir modernizuotos be detaliųjų reikalavimų, priimti sprendimai nedokumentuoti:

6.1. nepatvirtinti Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos nuostatai. Užsienio reikalų ministerijos informacinės sistemos nuostatai patvirtinti, tačiau nebuvo derinami su atitinkamomis institucijomis (1.1 poskyris);

6.2. neparengtos Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos specifikacijos, Užsienio reikalų ministerijos informacinės sistemos specifikacija neatnaujinta nuo 1998 m. Taip pat nebuvo rengiami Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos modernizavimo detalieji projektai, o Užsienio reikalų ministerijos informacinės sistemos detalusis projektas buvo parengtas tik vienos posistemės modernizavimui. Minėtos sistemos modernizuojamos vadovaujantis tik pirkimo techninė užduotimi. Neatnaujinus ar neparengus informacinės sistemos specifikacijos ir detaliojo projekto prieš informacinės sistemos modernizavimą, kyla rizika, kad modernizuotų sistemų funkcijos neatitiks veiklos poreikių (2.1 poskyris);

6.3. informacinių sistemų testavimas atliekamas specialioje aplinkoje, tačiau ne visuomet sudaromi testavimo planai ir įtraukiami galutiniai vartotojai (2.2 poskyris).

7. Galiojančios Užsienio reikalų ministerijos informacinės sistemos vystymo gairės nėra detalios, jas būtina atnaujinti ir konkretizuoti, kad būtų labiau susietos su aktualiais veiklos poreikiais ir prioritetais (4.2 poskyris).

8. Informacinių sistemų valdymo stebėsenai ir vertinimui vidaus auditoriai neskiria reikiamo dėmesio, o tai sudaro prielaidas galimiems informacinių sistemų valdymo vidaus kontrolės trūkumams atsirasti, be to, nustatyta neatitikčių išorės reikalavimams (4.1 poskyris).

Rekomendacijos

Lietuvos Respublikos užsienio reikalų ministerijai:

1. Sudaryti gerosios praktikos rekomenduojamą veiklos informacijos architektūros modelį, palengvinantį optimalų veiklos informacijos kūrimą, naudojimą ir dalijimąsi ja, išlaikant jos vientisumą (1 išvada).

2. Tobulinti ministerijos informacinių sistemų valdymo organizacinę struktūrą:

2.1. užtikrinti gerosios praktikos rekomenduojamų informacinių technologijų strategijos ir informacinių technologijų valdymo komitetų funkcijų efektyvų vykdymą, parenkant optimalius struktūrinius sprendimus (2.1 išvada);

2.2. paskirti duomenų valdymo įgaliotinius (2.2 išvada);

2.3. planuoti rezervinę darbuotojų pakaitą ir svarbių informacinių technologijų darbuotojų pareigų perėmimą (2.3 išvada).

3. Siekiant užtikrinti ministerijos valdomos informacijos saugą:

3.1. atlikus informacinių sistemų rizikos vertinimą, parengti ir patvirtinti informacinių sistemų rizikos mažinimo (valdymo) priemonių planą (3.1 išvada);

3.2. Informacinių sistemų duomenų saugos nuostatuose nustatyti ministerijos informacinių sistemų kategorijas ir nurodyti, kokios komponentės jas sudaro (3.2 išvada);

3.3. peržiūrėti ir atnaujinti duomenų saugą reglamentuojančius dokumentus (Užsienio reikalų ministerijos informacinių sistemų duomenų saugos nuostatus, Naudotojų administravimo taisykles, Saugaus elektroninės informacijos tvarkymo taisykles, Informacinių sistemų veiklos tęstinumo valdymo planą, Informacinių sistemų servisų administratorių sąrašą) (3.3 išvada);

3.4. peržiūrėti ir atnaujinti ministerijoje įslaptintos informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančias vidaus tvarkas (3.4 išvada);

3.5. nustatyti paskyrų valdymo proceso procedūras ir visose ministerijos informacinėse sistemose įdiegti vartotojų prisijungimo kompleksiškumo reikalavimus užtikrinančias technologines priemones (3.5 išvada).

4. Užtikrinant nenutrūkstamą informacinių sistemų paslaugų teikimą:

4.1. nustatyti informacinių sistemų veiklos tęstinumo atkūrimo prioritetus (4.1 išvada);

4.2. testuoti informacinių sistemų veiklos tęstinumo valdymo planą ir periodiškai rengti tęstinumo plano mokymus (4.3 išvada);

4.3. užpildyti informacinių technologijų įrangos sąrašus: nurodyti įrangos parametrus ir už jos priežiūrą atsakingus administratorius, parengti minimalaus funkcionalumo informacinių technologijų įrangos specifikaciją, kiekvieno pastato aukšto patalpų brėžinius ir

patalpose esančios įrangos ir komunikacijos, kompiuterių tinklo fizinio ir loginio sujungimo schemas (4.2 išvada);

4.4. nustatyti detaliąsias rezervinio duomenų kopijavimo procedūras, apimančias duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą, duomenų atstatymą iš kopijų (4.4 išvada);

4.5. užpildyti duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašą, su visais duomenų teikėjais ir gavėjais sudaryti duomenų mainų sutartis (4.2 išvada).

5. Stiprinti asmens duomenų valdymą ir saugą:

5.1. pranešti Valstybinei asmens duomenų apsaugos inspekcijai visus ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslus (5.1 išvada);

5.2. parengti ir patvirtinti rašytinės formos dokumentą, kuriame būtų nurodytas tvarkomų asmens duomenų saugos lygis, išdėstytos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo (5.2 išvada).

6. Siekiant, kad informacinių sistemų plėtra atitiktų ministerijos veiklos poreikius:

6.1. peržiūrėti, atnaujinti, išplėsti ir detalizuoti Užsienio reikalų ministerijos informacinės sistemos vystymo gaires (7 išvada);

6.2. nustatyta tvarka patvirtinti Užsienio reikalų ministerijos informacinės sistemos, Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos nuostatus (6.1 išvada);

6.3. parengti Konsulinių procedūrų valdymo sistemos, Supaprastinto tranzito dokumentų išdavimo informacinės sistemos specifikacijas, o Užsienio reikalų ministerijos informacinės sistemos specifikaciją – atnaujinti, jas visas nustatyta tvarka suderinti ir patvirtinti. Prieš kuriant naujas ar modernizuojant esamas ministerijos informacines sistemas, atnaujinti arba parengti ir nustatyta tvarka suderinti informacinių sistemų nuostatus, specifikacijas ir detaliuosius projektus (6.2 išvada);

6.4. vidaus tvarkose nustatyti, kad, sukūrus ar modernizavus informacinę sistemą, jos testavimas turėtų būti atliekamas sudarius testavimo planą, o testavimo rezultatus vertintų ir galutiniai informacinės sistemos vartotojai (6.3 išvada).

7. Periodiškai vertinti informacinių sistemų kontrolės valdymą ir atlikti išorės reglamentavimo stebėseną (1.2 išvada).

ĮŽANGA

Valstybės kontrolė atliko Užsienio reikalų ministerijos informacinių sistemų bendrosios ir kūrimo kontrolės auditą. Jis apėmė laikotarpį nuo 2009-01-01 iki 2012-07-01, o kai kuriais atvejais palyginimui buvo naudojami ir ankstesnių metų duomenys.

Ministerija automatizuodama veiklos funkcijas[3] naudoja informacines sistemas. 1999 m. įsteigtos Užsienio reikalų ministerijos informacinės sistemos (URMIS) posistemės yra skirtos vidaus administravimo funkcijoms vykdyti ir ministerijos veiklos funkcijoms įgyvendinti. URMIS apima tinklus ir sistemas, kuriomis apdorojama įslaptinta informacija[4] su žyma, ne aukštesne kaip „Riboto naudojimo“.

Užsienio reikalų ministerijoje veikia ir konsulinių procedūrų atlikimui skirtos informacinės sistemos: Konsulinių procedūrų valdymo sistema (KPVS) ir Supaprastinto tranzito dokumentų išdavimo informacinė sistema (STDIS). Jų nuostatų projektuose nurodyta, kad:

- KPVS paskirtis yra rinkti, kaupti, apdoroti, sisteminti, saugoti, naudoti ir teikti duomenis ir informaciją apie Lietuvos Respublikos užsienio reikalų ministerijos, Lietuvos Respublikos diplomatinių atstovybių ir konsulinių įstaigų atliekamas konsulines funkcijas. Joje taip pat tvarkomi asmens duomenys[5] ir ypatingi asmens duomenys[6];
- STDIS paskirtis – rinkti, kaupti ir tvarkyti informaciją, reikalingą supaprastinto tranzito dokumentams ar supaprastinto tranzito geležinkeliu dokumentams Rusijos Federacijos piliečiams, vykstantiems į Kaliningrado sritį tranzitu per Lietuvos Respublikos teritoriją ir atgal, išduoti. Taip pat padėti keistis STDIS informacija su institucijomis, kontroliuojančiomis supaprastintą Rusijos Federacijos piliečių tranzitą per Lietuvos Respubliką.

Užsienio reikalų ministerijos informacinių sistemų bendrosios ir kūrimo kontrolės audito metu atlikus preliminarų rizikos vertinimą, detaliajam vertinimui buvo pasirinkta 13 iš 34 Informacinių technologijų valdymo metodikoje ir gerojoje praktikoje COBIT[7] apibrėžtų informacinių technologijų procesų[8].

[3] Lietuvos Respublikos Vyriausybės 1998-09-25 nutarimu Nr. 1155 patvirtinti Lietuvos Respublikos užsienio reikalų ministerijos nuostatai, 6 p.
[4] Įslaptinta informacija – paslapčių subjekto pripažinta valstybės ar tarnybos paslaptimi informacija apie dokumentų, darbų, gaminių ar kitų objektų buvimą, esmę ar turinį, taip pat tokia paslaptimi pripažinti patys dokumentai, darbai, gaminiai ar kiti objektai. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas, 1999-11-25 Nr. VIII-1443, 2 str. 1 d.
[5] Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996-06-11 Nr. I-1374), 2 str. 1 d.
[6] Ypatingi asmens duomenys – duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996-06-11 Nr. I-1374), 2 str. 8 d.
[7] COBIT 4.1, 2011 m., Vilnius.
[8] Visi 34 COBIT 4.1 procesai ir jų grupės išvardyti 1 priede „Audito apimtis ir metodai“.

Audito metu vadovaudamiesi Lietuvos Respublikos valstybės kontrolieriaus 2008-10-09 įsakymu Nr. V-217 patvirtintomis Informacinių sistemų audito metodinėmis rekomendacijos pastebėtą riziką suskirstėme į tris lygius:

Didelė rizika – vienas ar keli informacinių sistemų valdymo trūkumai, kurie gali padaryti reikšmingų finansinių nuostolių valstybei, valstybinei institucijai ir (arba) piliečiams, todėl jie nedelsiant turėtų būti pašalinti.

Vidutinė rizika – su institucijos informacinių sistemų vidaus kontrolės sistema susiję reikšmingi trūkumai, į kuriuos nedelsiant turėtų būti atkreiptas atitinkamo lygio institucijos vadovų dėmesys.

Nedidelė rizika – trūkumai, kurie gali turėti netiesioginę ir nedidelę įtaką priimant informacinių sistemų valdymo ir finansinius sprendimus, tačiau juos reikia šalinti.

Valstybiniai auditoriai, įvertinę Užsienio reikalų ministerijos informacinių sistemų valdymą, nustatė informacinių sistemų vidaus kontrolės brandą, pateikė išvadas ir rekomendacijas.

Ataskaitoje vartojamos santrumpos ir sąvokos:

COBIT (angl. – *Control Objectives for Information and related Technologies*) – ISACA[9] sukurta IT valdymo metodika ir geroji praktika;

IS – informacinė sistema;

IT – informacinės technologijos;

KIRIS – Konsulinės išankstinės registracijos sistema;

KPVS – Konsulinių procedūrų valdymo sistema;

STDIS – Supaprastinto tranzito dokumentų informacinė sistema;

URMIS – Lietuvos Respublikos užsienio reikalų ministerijos informacinė sistema.

[9] ISACA – Information Systems Audit and Control Association. [Žiūrėta 2013-01-15] Prieiga per internetą http://www.isaca.org/about-isaca/Pages/default.aspx.

AUDITO REZULTATAI

1. Planavimas ir organizavimas

COBIT[10] Planavimo ir organizavimo grupės procesai apima strategiją, taktiką ir būdus, siūlančius, kaip IT gali geriausiai padėti įgyvendinti pagrindinius organizacijos veiklos tikslus. Organizacijos strateginės vizijos turi būti planuojamos, organizuojamos ir valdomos įvairiais aspektais; tam turi būti sukurta tinkama technologinė infrastruktūra.

Nustatę, kad Užsienio reikalų ministerijoje nėra bendro ar tam tikras IS apimančio informacijos architektūros modelio ir aiškių procedūrų, užtikrinančių IT strateginę plėtrą ir veiklos poreikių suderinamumą su IT, be to, nepaskirti duomenų įgaliotiniai ir rizikos vertinimas nebuvo atliekamas periodiškai, taip pat kitas planavimo ir organizavimo sritį apimančias problemas, pasirinkome ir vertinome šiuos COBIT Planavimo ir organizavimo grupės procesus:

- PO2 Informacinės architektūros nustatymas,
- PO4 IT procesų, organizacinės struktūros ir ryšių apibrėžimas,
- PO6 Vadovybės tikslų ir krypties komunikavimas (šio proceso vertinimo rezultatai pateikiami 2.1, 3.2 ir 4.2 poskyriuose),
- PO9 IT rizikos vertinimas ir valdymas.

1.1. Informacinės architektūros nustatymas

COBIT Informacinės architektūros nustatymo procesas[11] rekomenduoja reguliariai atnaujinti veiklos informacijos modelį, apibrėžti sistemas, leidžiančias optimaliai naudoti informaciją, sukurti organizacijos duomenų žodyną[12] su organizacijos duomenų sintaksės taisyklėmis[13], duomenų klasifikavimo planą ir nustatyti saugos lygius. Užtikrindamas patikimos ir saugios informacijos teikimą, procesas pagerina vadovybės priimamų sprendimų kokybę ir leidžia racionalizuoti informacinių sistemų išteklius, kad jie atitiktų organizacijos veiklos strategijas. Procesas reikalingas norint padidinti atskaitingumą už duomenų vientisumą ir saugą ir pagerinti informacijos dalijimosi taikomosiose programose ir subjektuose rezultatyvumą ir kontrolę.

[10] COBIT 4.1, 2011 m., Vilnius, 29–69 psl.
[11] Ten pat, PO2 procesas, 33 psl.
[12] Duomenų žodynas (angl. *data dictionary*) – duomenų bazė, kurią sudaro duomenų elemento pavadinimas, tipas, reikšmių diapazonas, šaltinis bei įgaliojimas prieiti prie kiekvieno duomenų bazės duomenų elemento. Ši duomenų bazė nurodo ir kurios taikomosios programos naudoja tuos duomenis, todėl nagrinėjant duomenų struktūrą, gali būti pateiktas duomenis naudojančių programų sąrašas. Duomenų žodynas gali veikti kaip savarankiška struktūra, naudojama valdymui arba dokumentavimui, arba gali valdyti duomenų bazės darbą [COBIT 4.1, 2011 m., Vilnius, 189 psl.].
[13] Duomenų sintaksės taisyklės – duomenų aprašymo ir manipuliavimo instrukcijos (taisyklės).

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

- IS nuostatuose turi būti aptarta IS organizacinė ir informacinė struktūra[14];
- išsamūs vidiniai ir išoriniai informacijos srautai turi būti nustatomi IS specifikacijose[15];
- IS saugos dokumentuose turi būti nurodyta elektroninės informacijos priskyrimo atitinkamai kategorijai bendrieji reikalavimai, siekiant nustatyti šios informacijos apsaugos poreikį, prioritetus ir lygį[16], IS esančios elektroninės informacijos kategorijų sąrašas ir asmenys, atsakingi už šios informacijos tvarkymą[17].

Audito metu nustatyta, kad Užsienio reikalų ministerijos el. informacijos srautų valdymas neatitinka minėtų reikalavimų, nes:

- KPVS nuostatų projektas parengtas ir nuo 2008 m. derinamas su duomenų teikėjais ir Valstybine duomenų apsaugos inspekcija, tačiau iki audituojamo laikotarpio pabaigos nesuderintas ir IS nuostatai nepatvirtinti.
- STDIS nuostatų projektas parengtas 2012 m., tačiau nesuderintas su duomenų teikėjais ir kitomis atsakingomis institucijomis.
- URMIS nuostatuose (patvirtintuose užsienio reikalų ministro 2008-11-27 įsakymu Nr. V-187) nenurodyti konkretūs duomenų teikėjai ir gavėjai.
- El. informacijos kategorijų sąrašas nurodytas Užsienio reikalų ministerijos saugaus elektroninės informacijos tvarkymo taisyklėse (patvirtintose užsienio reikalų ministro 2010-02-19 įsakymu Nr. V-22). Jos taikomos viešai, tarnybinio naudojimo ir įslaptintai informacijai, kurios slaptumo žyma ne aukštesnė negu „Riboto naudojimo“. Pažymėtina, kad el. informacija nepriskirta minėtoms kategorijoms, nesudaryti el. informacijos sąrašai, nepriskirta, kokiose IS ir kokia informacija yra tvarkoma, nepaskirti asmenys, atsakingi už priskirtos informacijos tvarkymą[18]. Be to, neapibrėžta tarnybinės informacijos sąvoka.
- URMIS specifikacija neatitinka realios situacijos (žr. pavyzdį), todėl rekomenduotina ją atnaujinti ir aprašyti URMIS vidinius ir išorinius informacijos srautus. Turėtų būti parengtos ir patvirtintos KPVS ir STDIS specifikacijos.

Pavyzdys

URMIS 1998 m. specifikacija neatitinka realios situacijos, nes:

1. Specifikacijos 13 psl. pateikta schema „URM naudojama programinė įranga“ neatitinka tikrovės, nes

[14] Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės, 4.2 ir 4.3 p.
[15] Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-10-15 įsakymu Nr. T-131 patvirtinti Reikalavimai valstybės informacinių sistemų specifikacijoms, 19–24 p.
[16] Lietuvos Respublikos vidaus reikalų ministro 2007-05-08 įsakymu Nr. 1V-172 patvirtintos Saugos dokumentų turinio gairės, II sk. 3.2.1p.
[17] Ten pat, III sk., 4.1.1 ir 4.1.2 p.
[18] Ten pat, 4.1.2. p.

schemoje nurodyta programinė įranga nenaudojama, o ta, kuri naudojama, – specifikacijoje neaprašyta.

2. URMIS specifikacijoje aprašyta jungtis su Lietuvos Respublikos Vyriausybės administracine sistema, o tokios sistemos nebėra.

3. Audituojamu laikotarpiu Užsienio reikalų ministerijoje Kompiuterinių sistemų, Informacijos ir spaudos, Raštvedybos skyrių nebuvo, tačiau specifikacijoje jie nurodomi.

4. Skyrelyje „Naudojama programinė įranga“ nurodyta pasenusi ir ministerijos nenaudojama programinė įranga: „MS DOS“, „MS Windows 3.1“, „MS Windows 95“ ir kt.

Audito metu pastebėta, kad ministerijoje tos pačios IS įvairiuose dokumentuose vadinamos skirtingai (žr. pavyzdį), todėl gali būti sunku nustatyti apie kokią IS kalbama.

Pavyzdys

Specifikacijoje URMIS vadinama Užsienio reikalų ministerijos kompiuterizuotąja informacine sistema, o URMIS nuostatuose – Lietuvos Respublikos užsienio reikalų ministerijos informacine sistema.

Duomenų saugos nuostatų priede „Informacinės sistemos servisų aprašas“ STDIS vadinama Kaliningrado Tranzito IS (FRTD), Supaprastinto tranzito geležinkeliais dokumentų išdavimo sistema STD IS (minima STGD IS administratorių mokymo medžiagoje) ar Lietuvos konsulinės tarnybos informacinės sistemos dėl supaprastinto tranzito geležinkeliu dokumentų išdavimo – FRTD IS (minima Lietuvos Respublikos užsienio reikalų ministerijos ir Rusijos Federacijos susisiekimo ministerijos informacinio bendradarbiavimo, keičiantis duomenimis, reikalingais sprendimui dėl supaprastinto tranzito geležinkeliu dokumento išdavimo priimti, reglamentas[19]) ir kitaip.

Užsienio reikalų ministerijoje nėra bendro (COBIT rekomenduojamo) ar tam tikras IS apimančio (kiek nustato išvardyti teisės aktai) informacijos architektūros modelio. Ministerijai aiškiai neaprašius turimų duomenų srautų (duomenų struktūros), kyla vidutinė rizika, kad gali būti eikvojamas papildomas laikas ir ištekliai juos apdorojant, parenkamos nepakankamos informacijos saugą užtikrinančios priemonės.

Aprašius gerosios praktikos rekomenduojamą informacijos architektūros modelį, ministerijai būtų lengviau pasirinkti optimalią technologinę kryptį. Kadangi šis modelis yra lankstus, funkcionalus, saugus ir lengvai atkuriamas, sutrikus IS funkcionavimui, ministerijai būtų paprasčiau kurti, naudoti ir dalytis veiklos informacija, išlaikant ją vientisą.

1.2. Informacinių technologijų procesų, organizacinės struktūros ir ryšių apibrėžimas

COBIT IT procesų, organizacinės struktūros ir ryšių apibrėžimo procesas[20] numato, kad IT organizacinė struktūra turi būti apibrėžiama atsižvelgiant į reikalavimus darbuotojams, įgūdžiams, padaliniams, atskaitomybei, įgaliojimams, funkcijoms, atsakomybei ir priežiūrai. Ši struktūra turi būti suderinta su IT procesų modeliu, užtikrinančiu skaidrumą, kontrolę ir aukščiausio lygio vykdomųjų ir veiklos vadovų dalyvavimą. Turėtų būti užtikrintas sklandus IT strateginis planavimas ir plėtra, taip pat, dalyvaujant vadovybei, veiklos ir IT atstovams, atsižvelgiant į veiklos poreikius būtų nustatyti prioritetai IT ištekliams. Visiems padaliniams turėtų būti numatyti procesai, administracinė politika ir procedūros, ypač daug dėmesio skiriant

[19] Prieiga per internetą http://www.urm.lt/umr/m/m_files/wfiles/file2578.pdf, [Žiūrėta 2012-06-22].
[20] COBIT 4.1, 2011, Vilnius, PO4 procesas, 41 psl.

kontrolei, kokybės užtikrinimui, rizikos valdymui, informacijos saugai, duomenų ir sistemų valdymui ir funkcijų atskyrimui.

COBIT IT procesų, organizacinės struktūros ir ryšių apibrėžimo procesas[21] rekomenduoja sudaryti IT strategijos ir IT valdymo komitetus, kuriuose dalyvautų organizacijos vadovybė, veiklos padalinių atstovai ir IT darbuotojai ir kurie spręstų strateginius ir svarbiausių investicijų tikslingumo klausimus, taip pat nustatytų IT investicijų prioritetus, sektų projektų vykdymo ar teikiamų paslaugų būklę.

Užsienio reikalų ministerijoje strateginius plėtros klausimus sprendžia ministerijos kolegija, kurios darbo reglamente apibrėžtos funkcijos tik iš dalies apima COBIT rekomenduojamo IT strategijos komiteto funkcijas. Ministerijos IS pokyčių valdymą atlieka IS funkcijų pokyčių komisija, kuri atlieka tik dalį COBIT rekomenduojamų IT valdymo komiteto funkcijų (vidutinė rizika).

Pagrindinius IT strateginius ir valdymo uždavinius Užsienio reikalų ministerijoje galėtų spręsti įsteigtas vienas IT valdymo komitetas, priskiriant jam COBIT rekomenduojamų IT strategijos ir IT valdymo komitetų būdingas funkcijas ir užtikrinant reikiamą vadovybės, veiklos ir IT atstovavimą. Alternatyva galėtų būti šių funkcijų priskyrimas kitai ministerijos pasirinktai organizacinei struktūrai, tačiau šiuo atveju reikėtų įvertinti, ar papildžius funkcijas naujomis, ši struktūra būtų efektyvi spęsti jai numatytus IT strateginius ir valdymo uždavinius.

Informacinių sistemų duomenų saugos nuostatuose nurodyta išteklių savininko sąvoka[22] ir numatyta, kad kiekvienam IT ištekliui priskiriamas atsakingas IS administratorius – ištekliaus saugotojas. Nustatyta, kad ministerijoje IS išteklių savininkais paskirti struktūriniai padaliniai, tačiau nepaskirti duomenų valdymo įgaliotiniai, taigi nesivadovaujama nuo 2012-01-01 įsigaliojusio Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo[23] reikalavimais.

IT personalo ir saugos įgaliotinio atliekamos funkcijos ir atsakomybės apibrėžtos jų pareigybių aprašymuose ir ministerijos vidaus tvarkose, tačiau audituojamu laikotarpiu dalies pavestų funkcijų darbuotojai nevykdė (žr. pavyzdį). Siekiant efektyvesnio IT personalo ir saugos įgaliotinio funkcijų įgyvendinimo, turėtų būti peržiūrėtas jų funkcijų paskirstymas, sudaromi veiklos planai.

Pavyzdys

- Užsienio reikalų ministro 2010-02-19 įsakymu Nr. V-22 ministerijos kancleriui pavesta tvirtinti IS servisų administratorių sąrašą. Jis patvirtintas ministerijos kanclerio 2010-05-27 potvarkiu Nr. VP-156. Pasikeitus IS servisų administratoriams (žr. 3 priedą) arba nutraukus darbo santykius su Užsienio reikalų ministerija, sąrašas nebuvo atnaujintas, nors už atnaujinimą ir papildymą atsakingas yra IT departamento IS vystymo ir priežiūros

[21] COBIT 4.1, 2011, Vilnius, PO4 procesas, PO4.2 ir PO4.3 kontrolės tikslai, 42 psl.
[22] Lietuvos Respublikos užsienio reikalų ministro 2010-02-19 įsakymu Nr. V-22 patvirtinti Informacinių sistemų duomenų saugos nuostatai x p.: „Išteklių savininkas – darbuotojas, atsakingas už teisių, susijusių su prieiga prie išteklių, tvarkymą“.
[23] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 8 str., 1 d.

skyriaus vedėjas (šio darbuotojo pareigybės aprašyme numatyta, kad viena atliekamų funkcijų – sudaryti, papildyti ministerijos IS servisų ir juos administruojančių administratorių sąrašą ir teikti jį tvirtinti departamento vadovybei).

- 2009 ir 2012 m. IS rizikos vertinimus atliko ir rizikos vertinimo ataskaitas parengė nepriklausomi specialistai, nors pagal IS duomenų saugos nuostatus (20 p.) rizikos vertinimo ataskaitas turėtų rengti ministerijos IS saugos įgaliotinis.
- 2010-02-19 įsakymu Nr. V-22 patvirtintame IS veiklos tęstinumo valdymo plane (46 p.) numatyta, kad saugos įgaliotinis inicijuoja plano išbandymus, tačiau veiklos tęstinumo valdymo plano išbandymas nebuvo inicijuotas ir jis nebuvo išbandytas.
- užsienio reikalų ministro 2010-02-19 įsakymu Nr. V-22 patvirtintame Užsienio reikalų ministerijos IS funkcijų pokyčių valdymo tvarkos apraše nustatyta, kad turi būti aprašomas „naujas sukonstruotas funkcionalumas“, jo veikimas, naudojimas ir priežiūra. Jei sukonstruotas pokytis papildo IS programinės įrangos funkcionavimą, turi būti atitinkamai keičiami informacinės sistemos kūrimą reglamentuojantys dokumentai (specifikacija, bendrasis projektas ir kita). Už pokyčio dokumentavimą atsakingas IS administratorius. Audito metu nustatyta, kad IS specifikacija neatnaujinta nuo 1998 m., nors sistemoje buvo įdiegtos naujos funkcijos (žr. 2 skyriaus 1 pav.).

Užsienio reikalų ministerijoje vyksta didelė IT personalo kaita (žr. pavyzdį), tačiau nesuplanuojama rezervinė darbuotojų pakaita ir tokių darbuotojų pareigų perėmimas, dėl to gali kilti problemų, susijusių su funkcijų perleidimu, sukauptų žinių, darbo rezultatų ir darbo metu įgytos patirties perdavimu. Dėl žmogiškųjų išteklių kaitos IT departamente kyla vidutinė rizika ministerijos IS valdymą ir duomenų saugą reglamentuojančiuose dokumentuose numatytų reikalavimų, priemonių ir procedūrų vykdymui bei IS veiklos tęstinumui.

Pavyzdys

IT departamento direktorius per 2012 m. keitėsi 3 kartus – dėl rotacijos į diplomatines atstovybes ir konsulines įstaigas užsienyje.
Audituojamu laikotarpiu IT departamento IS vystymo ir priežiūros skyriuje vyko didelė IT darbuotojų, einančių IS administratorių pareigas, kaita (žr. 3 priedą).

Atsižvelgiant į nustatytą riziką, ministerijoje turėtų būti planuojama rezervinė IT personalo pakaita, dubliuojamos pagrindinio IT personalo funkcijos, kad būtų sudaryta galimybė užtikrinti IT veiklų nuoseklumą, perduoti sukauptas žinias ir patirtį.

1.3. Informacinių technologijų rizikos vertinimas ir valdymas

COBIT IT rizikos vertinimo ir valdymo procesas[24] rekomenduoja, kad organizacijoje būtų susitarta dėl bendrų rizikos valdymo principų, kurie apimtų priimtino IT rizikos lygio nustatymą, rizikos ir likutinės rizikos sumažinimo strategiją. Organizacija turėtų nustatyti, analizuoti ir įvertinti bet kokį galimą poveikį įstaigos tikslams, kurį galėtų sukelti neplanuotas įvykis. Rizikos įvertinimo rezultatas turi būti suprantamas įstaigos vadovybei ir pateikiamas finansine išraiška, kad būtų galima nustatyti priimtiną toleravimo lygį ir parinkti optimalias rizikos mažinimo priemones.

Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose nustatyta[25], kad IS rizikos vertinimą kasmet turi

[24] COBIT 4.1, 2011, Vilnius, PO9 procesas, 63 psl.
[25] Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, 30 ir 31 p.

organizuoti saugos įgaliotinis. Prireikus jis gali organizuoti neeilinį IS rizikos įvertinimą.IS rizikos 5vertinimas išdėstomas rizikos įvertinimo ataskaitoje.

Audituojamu laikotarpiu ministerijoje IS rizikos vertinimai atlikti 2009 ir 2012 metais. 2010 ir 2011 m. vertinimai nebuvo atlikti, todėl nebuvo identifikuoti ir detaliai įvertinti šiuo laikotarpiu buvę IS rizikos veiksniai, galintys turėti įtakos el. informacijos saugai, nebuvo analizuota, kiek per šį laikotarpį kito rizikos ir koks buvo tikrasis rizikos mažinimo priemonių poveikis. Siekdama užtikrinti rizikos vertinimo periodiškumą, ministerija 2011 m. yra numačiusi IS rizikos vertinimą atlikti 2013 ir 2014 metais.

Nustatyta, kad nei 2009 nei 2012 m. parengtos IS rizikos įvertinimo ataskaitos nebuvo patvirtintos IS valdytojo vadovo (ministerijos kanclerio), nors pagal Užsienio reikalų ministerijos galiojusią vidaus tvarką (2008-10-07 įsakymu Nr. V-172 patvirtinti Informacinių sistemų bendrieji duomenų saugos nuostatai) ir pagal dabar galiojančius IS duomenų saugos nuostatus, pagrindinės ministerijos IS rizikos veiksnių vertinimo nuostatos ir rizikos mažinimo priemonės turi būti išdėstytos IS valdytojo vadovo (ministerijos kanclerio) tvirtinamoje rizikos įvertinimo ataskaitoje. Taip pat nustatyta, kad ministerijoje nerengiamas ir netvirtinamas IS rizikos mažinimo (valdymo) priemonių planas, todėl nepakankamas dėmesys skiriamas IS rizikos vertinimo metu pateiktų rekomendacijų įgyvendinimui (žr. pavyzdį). Nepatvirtinus IS rizikos įvertinimo ataskaitos ir neparengus IS rizikos mažinimo (valdymo) priemonių plano kyla vidutinė rizika, kad tiek 2012 m. atlikto, tiek ateityje atlikus IS rizikos vertinimus, nustatytos rizikos mažinimo priemonės gali būti neįgyvendintos.

Pavyzdys

2009 m. IS rizikos vertinimo ataskaitoje pateikti pasiūlymai (rekomendacijos) iki audituojamo laikotarpio pabaigos nebuvo įgyvendinti: nepasiruošta galimam sistemos IS atstatymui, nes reguliariai (pvz.: kartą per 3 mėnesius) nevykdomas bandomasis IS atstatymas testinėje aplinkoje; IS darbuotojų kvalifikacija nesekama taikant kvalifikacijos matricą; nesuderinta ir neparengta duomenų atsarginių kopijų darymo tvarka, nedokumentuota operacinių sistemų saugumo atnaujinimų stebėjimo, vertinimo ir diegimo proceso tvarka, rizikos analizė nebuvo atliekama periodiškai.

Siekiant užtikrinti rizikos mažinimo (valdymo) priemonių įgyvendinimo kontrolę, atlikus IS rizikos vertinimus, ministerijoje turėtų būti parengti ir patvirtinti IS rizikos mažinimo priemonių planai, juose numatant rizikos mažinimo priemonių įgyvendinimo terminus ir už rizikos mažinimo priemonių įgyvendinimą atsakingus asmenis.

2. Įsigijimas ir įdiegimas

COBIT Įsigijimo ir įdiegimo grupės[26] procesų aprašyme įvardyta, kokie IT sprendimai turės būti nustatyti, sukurti ar įsigyti, įgyvendinant organizacijos strategiją. Sprendimai vėliau turės būti įdiegti ir integruoti į organizacijos veiklos procesus.

Audituojamu laikotarpiu buvo modernizuojamos trys Užsienio reikalų ministerijos IS:

- STDIS sukurta ir pradėta eksploatuoti 2003 m., projektas buvo finansuojamas Europos Sąjungos lėšomis, įgyvendinant Finansinį memorandumą dėl specialiosios Kaliningrado tranzito programos[27]. Audituojamu laikotarpiu nuo 2010-02-25 STDIS buvo modernizuojama.
- KPVS kūrimas pradėtas 2003 m. įgyvendinant PHARE projektą[28], o sistema pradėta eksploatuoti 2005 m. viduryje. KPVS buvo modernizuojama nuo 2007-04-24 iki 2010-04-24.
- URMIS modernizuojama nuo 2008 m. vykdant Užsienio reikalų ministerijos ir Lietuvos Respublikos diplomatinių atstovybių užsienyje informacinės sistemos plėtros ir modernizavimo investicinį projektą. Projektas apima naujų paslaugų kūrimo ir diegimo darbus, esamo ministerijos ir Lietuvos Respublikos diplomatinių atstovybių saugaus duomenų perdavimo tinklo modernizavimą ir plėtrą (žr. 1 pav.).

1 pav. URMIS vystymo grafikas

Šaltinis – Valstybės kontrolė

Audito metu pastebėta, kad dalis įsigijimo ir įdiegimo srities procesų (pvz.: Pasirengimas naudojimui, IT išteklių įsigijimas ir Pokyčių valdymas) ministerijoje vykdomi be

[26] COBIT 4.1, 2011 m., Vilnius, 73–100 psl.
[27] Pasirašytas 2003-02-28, Nr. 2003/004-315.
[28] PHARE projektas. [Žiūrėta 2012-10-25] Prieiga per internetą http://ec.europa.eu/enlargement/fiche_projet/document/2002-000.601.04.02%20Consular%20procedures.pdf.

didelių rizikų. Įvertinus preliminarią riziką nustatyta, kad IS modernizuojama neatnaujinus ar neparengus IS specifikacijų ir kitos dokumentacijos, sistemos ir tinklai eksploatuojami jų neįteisinus, taigi nesivadovaujama teisės aktų reikalavimais, todėl detaliau vertinti du procesai:

- AI2 Taikomosios programinės įrangos įsigijimas ir priežiūra,
- AI7 Sprendimų ir pokyčių diegimas ir akreditavimas.

2.1. Taikomosios programinės įrangos įsigijimas ir priežiūra

COBIT Taikomosios programinės įrangos įsigijimo ir priežiūros procesas[29] numato, kad taikomoji programinė įranga turėtų būti įsigyjama atsižvelgiant į veiklos poreikius. Įsigijimas turėtų apimti taikomosios programinės įrangos projektavimą, kontrolės priemonių ir saugos reikalavimų tinkamą įtraukimą bei standartus atitinkantį kūrimą ir konfigūravimą. Tai organizacijoms padeda naudojant tinkamą taikomąją programinę įrangą atlikti veiklos operacijas.

Užsienio reikalų ministerijos IS funkcijų pokyčių valdymo tvarkos aprašo tikslas – valdyti ministerijos IS pokyčius, užtikrinant kokybišką reikalingų pokyčių įvykdymą ir diegimą minimaliai sutrukdant IS funkcionavimą. Tvarkos apraše nustatyta, kad bet koks IS pokytis turi būti užsakomas raštu, o už IS funkcijų pokyčių valdymo tvarkos aprašo laikymosi kontrolę atsakingas IS saugos įgaliotinis. Nustatyta, kad aprašo laikymosi kontrolė nepakankama, nes neužtikrinamas jo nuostatų įgyvendinimas (žr. pavyzdį).

Pavyzdys

2010-12-21 sudaryta korporatyvinė sutartis su „Microsoft“ dėl programinės įrangos licencijų nuomos, kurios pagrindu buvo iš esmės atnaujintos URM IS posistemės, skirtos vidaus administravimo funkcijoms, 2010-12-30 pasirašyta sutartis dėl įsilaužimų ir pažeidžiamumų aptikimo ir išvengimo įrangos įsigijimo ir įdiegimo,
2011-09-19 pasirašyta sutartis dėl el. pašto skenavimą dubliuojančio įrenginio įsigijimo, 2011-09-19 pasirašyta sutartis dėl virtualių tarnybinių stočių rezervinio duomenų kopijavimo programinės įrangos įsigijimo, tačiau šie IS pokyčiai nebuvo užsakomi raštu (užregistruoti), kaip nustatyta IS funkcijų pokyčių valdymo tvarkos apraše (Užsienio reikalų ministerijos administracijos padalinių vadovai IT departamento direktoriui turi pateikti bendra tvarka registruotą raštą – teikimą dėl IS funkcijų pokyčio (11p.))

Kadangi ne visi ministerijos inicijuoti IS funkcijų pokyčiai yra registruojami ir įvertinami IS funkcijų pokyčių komisijoje, lieka neįvertinta pokyčio įtaka IS funkcionavimui, eksploatavimui ir ministerijos veiklai, o diegiant pokytį nenustatomos galimos grėsmės ir rizika IS funkcionavimui ir prieinamumui. Dėl to galimi nepagrįstai dideli ištekliai IS pokyčiui įgyvendinti (finansiniai, laiko, žmogiškieji) bei atsakomybės už pokyčio įgyvendinimą stoka (nedidelė rizika).

IS funkcijų pokyčių valdymo tvarkos apraše numatyta, kad pokyčių įvykdymą koordinuoja ir prižiūri paskirtas atsakingas IS administratorius arba specialiai sukurta darbo

[29] COBIT 4.1, 2011 m., Vilnius, AI2 procesas, 75 psl.

grupė. Už pokyčių įvykdymo planavimą ir organizavimą atsakingas IT departamento direktorius, jei nėra paskirtas kitas atsakingas asmuo. Nustatyta, kad IS pokyčių įgyvendinimo kontrolė ne visada veiksminga (žr. pavyzdį). Stiprinant IS pokyčių įgyvendinimo kontrolės užtikrinimą ir sekant pokyčio vykdymo būklę, turėtų būti atsiskaitoma ne tik IT departamento direktoriui, bet ir ministerijos vadovybei.

Pavyzdys

Informacinių sistemų funkcijų pokyčių valdymo komisijos 2011-01-07 protokole Nr. 32 buvo užfiksuota, kad iki 2011-04-29 serveriuose ir vartotojų kompiuteriuose bus įdiegta nauja antivirusinė programa, kuri panaikins esančius virusus ir ateityje apsaugos nuo naujų virusų atsiradimo. Įgyvendinus pokytį turėjo būti parengta ir komisijai pateikta sistemos diegimo dokumentacija. Tokia dokumentacija nebuvo parengta.

Informacinių sistemų funkcijų pokyčių valdymo komisijos 2012-02-22 protokole Nr. 64 buvo užfiksuota, kad norint įrašyti telefoninius pokalbius Lietuvos Respublikos diplomatinėse atstovybėse ir konsulinėse įstaigose turi būti priimti visi reikalingi teisės aktai, tokie kaip asmens duomenų tvarkymo taisyklės. Iki planuojamos pokyčio įvykdymo dienos (2012-09-03) taisyklės ministerijoje nebuvo parengtos ir patvirtintos.

COBIT metodika rekomenduoja veiklos poreikius paversti bendrojo projektavimo specifikacijomis programinei įrangai įsigyti ir parengti detalųjį IS plėtros projektą ir techninius reikalavimus, taip būtų pasiekiamos mažesnės kūrimo ar modernizavimo sąnaudos. Analogiški reikalavimai IS modernizavimui nustatyti ir Valstybės informacinių sistemų steigimo ir įteisinimo taisyklėse[30]: parengti ir patvirtinti IS nuostatų pakeitimą, parengti specifikacijos pakeitimus. Valstybės IS kūrimo metodikoje[31] nustatoma, kad IS specifikavimo stadijos IS projekto valdymo etapo metu turi būti sukurtas IS projekto planas, kaip projektas bus vykdomas ir tvarkomas.

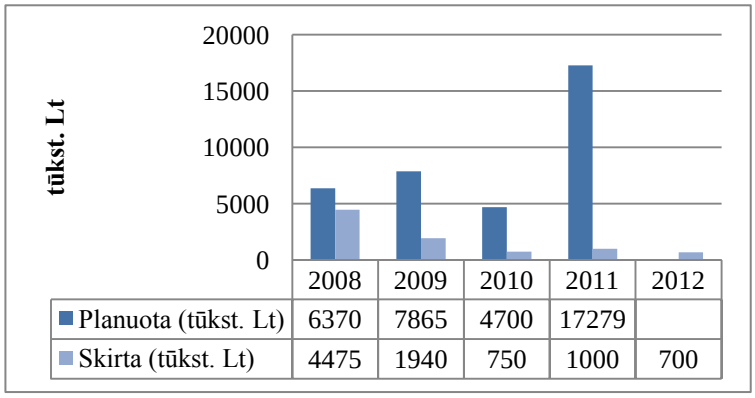
URMIS tobulinama nuo 2008 m., dalis pokyčių iki 2012-07-01 buvo įdiegta (žr. 1 pav.), tačiau IS specifikacija nuo 1998 m. nebuvo atnaujinta. Be to, ministerija nėra parengusi detalaus URMIS modernizavimo projekto. URMIS plėtra vykdoma vadovaujantis URMIS vystymo gairėmis bei URMIS plėtros ir modernizavimo investiciniu projektu. Gairės yra bendrojo pobūdžio dokumentas, kuriame išdėstyta bendra plėtros vizija, o investiciniame projekte pagrindžiamas lėšų poreikis, planuojamas finansavimas išdėstomas laike. Ministerija nenumatė, kokiais etapais projektas bus vykdomas, kokie uždaviniai numatyti kiekviename projekto etape, uždavinių įgyvendinimo išdėstymo laiko skalėje ir techninių projekto detalių. Nustatyta, kad nei kuriant, nei modernizuojant KPVS ir STDIS specifikacijos nebuvo parengtos ir suderintos. Modernizuojant šias dvi IS nebuvo rengiami detalieji projektai. Sistemos modernizuojamos vadovaujantis tik pirkimo technine užduotimi. Neatnaujinus ar neparengus

[30] Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimas Nr. 451 „Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo“, $17^{(1)}$–$17^{(5)}$ p.
[31] Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-11-15 įsakymas Nr. T-131 „Dėl Valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“, 22 p.

informacinės sistemos specifikacijos, neparengus detaliojo projekto prieš informacinės sistemos modernizavimą kyla didelė rizika, kad modernizuotų sistemų funkcijos neatitiks veiklos poreikių. Atsižvelgiant į tai, ministerija turi parengti KPVS ir STDIS specifikacijas, o URMIS specifikaciją – atnaujinti, jas visas nustatyta tvarka suderinti ir patvirtinti. Prieš kuriant naujas ar modernizuojant esamas ministerijos IS atnaujinti arba parengti ir nustatyta tvarka suderinti IS specifikacijas ir detaliuosius projektus.

URMIS investicinio projekto tikslus buvo planuota įgyvendinti iki 2012 m., tačiau dėl sumažinto finansavimo projekto įgyvendinimo pabaiga nukelta iki 2019 m. (1 pav.). 2008–2012 m. iš planuotų 36 214 tūkst. Lt skirta 8 865 tūkst. Lt, t. y. 24,5 proc. visų planuotų lėšų. Planuotas projekto finansavimas sumažintas jau pirmaisiais projekto vykdymo metais (žr. 2 pav.).

2 pav. URMIS projekto finansavimas



	2008	2009	2010	2011	2012
Planuota (tūkst. Lt)	6370	7865	4700	17279	
Skirta (tūkst. Lt)	4475	1940	750	1000	700

Šaltinis – Valstybės kontrolė pagal URMIS plėtros ir modernizavimo investicinis projekto duomenis

Apskaičiavimai atlikti remiantis 2007 metų kainomis ir ministerijos 2002–2007 metais vykdytų viešųjų pirkimų rezultatais. Planuojama projekto pabaiga 2019 m. Atsižvelgiant į projekto vykdymo laikotarpį (2008 – 2019 m.) suplanuotos investicijos gali neduoti laukiamo poveikio, nes 2007 m. numatyti sprendimai bus pasenę ir neatitiks keliamų reikalavimų.

Kintant kainoms, numatytas investicijų poreikis gali reikšmingai pakisti, todėl tikslinga iš naujo įvertinti uždaviniams atlikti reikalingų lėšų poreikį.

URMIS investiciniame projekte nenurodyti konkrečių uždavinių įgyvendinimo etapai (tik bendra projekto pradžia ir pabaiga), neišdėstytas projekto uždavinių įgyvendinimas laike, todėl kyla vidutinė rizika, kad projekto tikslai nebus pasiekti. Keičiantis projekto finansavimui, būtų tikslingiau koreguoti numatytų uždavinių kiekį, o ne atidėti projekto įgyvendinimo terminą.

STDIS tvarkomi Rusijos Federacijos piliečių asmens duomenys reikalingi tranzito dokumentams per Lietuvos Respublikos teritoriją gauti. Ministerijos Specialioji ekspertų komisija nutarė įslaptinti informaciją susijusią su STDIS pirkimais. Pastebėta, kad STDIS programinės įrangos modernizavimo pirkimas ir 2010-02-25 sudaryta sutartis buvo įslaptinti

(su slaptumo žyma „Riboto naudojimo“), tačiau pagal ją sukurti produktai (STDIS programinė įranga, vartotojų vadovai) – be slaptumo žymos. Todėl ateityje vykdant STDIS modernizavimo pirkimus rekomenduotina pakartotinai įvertinti, ar yra būtinybė STDIS pirkimus vykdyti įslaptintu būdu.

2.2. Sprendimų ir pokyčių diegimas

COBIT procesas Sprendimų ir pokyčių diegimas ir akreditavimas[32] rekomenduoja, kad kiekvieno IS kūrimo, diegimo ar keitimo projekto metu pagal nustatytą mokymo ir diegimo planą bei susijusią medžiagą dirbti su sistema turėtų būti išmokyti susijusių naudotojų padalinių darbuotojai ir IT padalinio techniniai darbuotojai. Ministerijai planuojant URMIS plėtrą ir modernizavimą, IS naudotojų ir administratorių mokymai nebuvo planuojami, todėl kyla maža rizika, kad nebus nuosekliai įgyjami nauji įgūdžiai, nesusipažinta su naujomis IS, laiku nenustatomos naudojimo problemos, o pareigas ir darbus atlikti reikalingos žinios bus fragmentiškos.

COBIT metodikoje apibrėžta[33], kad turi būti nustatytas ir vadovybės patvirtintas IS testavimo planas. Užsienio reikalų ministerijoje veikia testavimo aplinka, kurioje yra penkios tarnybinės stotys ir dvi darbo vietos. Kaip ir rekomenduoja geroji praktika, testavimo aplinka nesąveikauja su darbine aplinka, jos atskirtos. Ministerijoje vykdant IS plėtrą ir modernizavimą, sistemų testavimas atliekamas specialioje aplinkoje, tačiau ne visuomet sudaromi testavimo planai (pvz., vykdant URMIS plėtros ir modernizavimo projektą nebuvo sudaromi testavimo planai, išskyrus finansų valdymo posistemei. Testavimo planai nebuvo parengti ir modernizuojant KPVS ir STDIS). Vykdant nesuplanuotus testavimus, kyla nedidelė rizika, kad nebus nustatomos IS veikimo problemos, nekontroliuojamos testavimo darbų išlaidos, neapibrėžtos jo funkcijos ir atsakomybė, nebus iki minimumo sumažinti veiklos trikdžiai, kylantys dėl sistemos sutrikimų.

Nustatyta, kad IS testavimo rezultatus įvertina tik testavimus atlikęs administratorius, nedalyvaujant galutiniams IS naudotojams, o IS pokyčių komisijai pateikiami pokyčio testavimo ir įgyvendinimo rezultatai, todėl kyla nedidelė rizika, kad bus nepastebėtos IS veikimo problemos. COBIT metodika rekomenduoja, kad galutinius testavimus peržiūrėtų procesų savininkai (vartotojai): taip būtų iki minimumo sumažinti gamybos sutrikimai, apsaugoti svarbiausi duomenų srautai, nustatomi nukrypimai nuo lauktos paslaugų kokybės, taikomoji programinė įranga atitiktų naudotojų reikalavimus.

[32] COBIT 4.1, 2011 m., Vilnius, AI7 procesas, AI7.1 kontrolės tikslas, 98 psl.
[33] Ten pat, AI7.6 kontrolės tikslas, 98 psl.

3. Teikimas ir palaikymas

COBIT Teikimo ir palaikymo grupės procesai[34] aprašo, kaip turi būti teikiamos IT paslaugos. Tai apima organizacijos IT padalinio paslaugų teikimą kitiems padaliniams, informacijos saugos ir organizacijos veiklos tęstinumo užtikrinimą, vidaus vartotojų aptarnavimą ir duomenų valdymą.

Audito planavimo etape buvo pastebėta, kad Užsienio reikalų ministerijoje ne su visais duomenų teikėjais ir gavėjais sudarytos sutartys, IS veiklos tęstinumo valdymo planas nėra išsamus, neišbandomas ir neatnaujinamas, IS saugos procesas nėra tinkamai įgyvendinamas, nepakankamai užtikrinama asmens duomenų apsauga ir t. t, todėl audito metu buvo įvertinti šie COBIT procesai:

- DS2 Trečiųjų šalių paslaugų valdymas,
- DS4 Nepertraukiamo paslaugų teikimo užtikrinimas,
- DS5 Sistemų saugos užtikrinimas,
- DS11 Duomenų valdymas.

3.1. Trečiųjų šalių paslaugų valdymas

Trečiųjų šalių paslaugų valdymas[35] rekomenduoja nustatyti visus ryšius su teikėjais (paslaugų, duomenų ir kt.), nustatyti visas teikėjų paslaugas ir suskirstyti jas į kategorijas pagal teikėjo tipą, reikšmingumą ir lemiamą svarbą.

Saugaus elektroninės informacijos tvarkymo taisyklėse turi būti nurodyta duomenų perkėlimo ir teikimo kitoms IS, duomenų gavimo iš jų tvarka[36]. Ministerijos Saugaus elektroninės informacijos tvarkymo taisyklėse nustatyta, kad duomenų kėlimą, perdavimą ir gavimą turi reglamentuoti sutartys, sudarytos su kitos IS valdytoju arba tvarkytoju. Nustatyta, kad ministerijoje ne su visais duomenų teikėjais ir gavėjais sudarytos duomenų mainų sutartys, dėl to nustatyta vidutinė rizika, kad vykdant duomenų mainus tarp IS gali būti susidurta su atsakomybės problemomis užtikrinant teikiamų duomenų teisingumą bei gaunamų duomenų (el. informacijos) apsaugą.

Pavyzdys

KPVS duomenų teikėja yra Vidaus reikalų ministerija. Ji teikia Įtariamų, kaltinamų ir teistų asmenų žinybinio registro ir ieškomų asmenų, neatpažintų lavonų ir nežinomų bejėgių asmenų žinybinio registro duomenis apie įtariamus, kaltinamus, teistus ir ieškomus asmenis. STDIS duomenų teikėja yra Vidaus reikalų ministerija. Ji teikia duomenis apie nepageidaujamus asmenis iš Užsieniečių registro nepageidaujamų asmenų posistemės. Sutartinių įsipareigojimų dėl šių duomenų teikimo tarp Vidaus

[34] COBIT 4.1, 2011, Vilnius, 101–152 psl.
[35] Ten pat, DS2 procesas, DS2.1 kontrolės tikslas, 106 psl.
[36] Lietuvos Respublikos vidaus reikalų ministro 2007-05-08 įsakymas Nr. 1V-172 „Dėl saugos dokumentų turinio gairių patvirtinimo“, 4.3.4. p.

reikalų ir Užsienio reikalų ministerijos nėra.

KPVS duomenų teikėja yra Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. Ji teikia Lietuvos Respublikos gyventojų registro duomenis. Sutartinių įsipareigojimų dėl šių duomenų teikimo tarp šios institucijos ir Užsienio reikalų ministerijos nėra.

KPVS duomenų gavėjas yra Policijos departamentas prie Vidaus reikalų ministerijos. Jis gauna duomenis apie užsienio valstybėse sulaikytus, suimtus ar nuteistus už padarytas nusikalstamas veikas Lietuvos Respublikos piliečius, bei užsienyje nukentėjusius Lietuvos Respublikos piliečius, taip pat apie ieškomus Lietuvos Respublikos piliečius, kurie kreipiasi į konsulinę įstaigą dėl asmens grįžimo pažymėjimo gavimo. Sutartinių įsipareigojimų dėl šių duomenų teikimo tarp šios institucijos ir Užsienio reikalų ministerijos nėra.

IS veiklos tęstinumo valdymo plano turinyje turi būti nurodyti duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai[37]. Užsienio reikalų ministerijos IS veiklos tęstinumo valdymo plane numatyta duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašo forma. Ji sudaryta iš teiktinos paslaugos aprašymo, paslaugos teikėjo, kontaktinio asmens, telefono ir parašo, tačiau ši forma nepildoma, o kontaktinių asmenų duomenys nenurodomi ir pačiose sutartyse. Ministerijoje nesudarius administruojamų sutarčių, susijusių su IS sritimi, sąrašo ir nesuskirsčius teikiamų IS paslaugų į kategorijas pagal tiekėjo pobūdį, reikšmingumą ir svarbą, gali kilti sunkumų jas prižiūrint, vertinant paslaugų teikimo kokybę (žr. pavyzdį).

Pavyzdys

Ministerijoje tiekėjų sutarčių ir įsipareigojimų nesilaikymas buvo nustatytas 2009 m. rizikos vertinimo metu (2009-11-02 parengta IS laikomos ir apdorojamos elektroninės informacijos rizikos analizės ataskaita), todėl ministerijai buvo pasiūlyta vykdyti tiekėjų vertinimus (auditus) prieš pasirašant sutartis ir periodiškai vertinti IS paslaugų teikimo kokybę, sutartyse nustatyti paslaugų teikimo kokybinius parametrus.

Ministerijos IS sritį apimančiose sutartyse su trečiosiomis šalimis (tiekėjais, gamintojais ir partneriais) numatomi susitarimai dėl paslaugų lygio, apimantys garantinius ir sutartinius įsipareigojimus, kokybės užtikrinimą, garantinius įsipareigojimus, tiekėjo sutartinių įsipareigojimų įvykdymo terminą, garantinės techninės priežiūros reakcijos laiką. Ministerijoje nedokumentuotos trečiųjų šalių teikiamų IS paslaugų stebėjimo ir kontrolės procedūros, todėl kyla vidutinė rizika, kad IS paslaugų teikimo lygiai, numatyti su trečiosiomis šalimis sudarytose sutartyse dėl paslaugų teikimo, nebus įgyvendinti, vykdomi ir išlaikomi. Norint užtikrinti, kad trečiųjų šalių teikiamos IS paslaugos atitiktų Užsienio reikalų ministerijos veiklos poreikius, rekomenduotinas rezultatyvus trečiųjų šalių valdymo procesas. Jis apima aiškų funkcijų, atsakomybės ir lūkesčių apibrėžimą susitarimuose su trečiosiomis šalimis bei tokių susitarimų rezultatyvumo ir atitikties peržiūrą ir tikrinimą. Rezultatyvus trečiųjų šalių paslaugų valdymas sumažina veiklos riziką, kurią kelia sutarčių nevykdantys tiekėjai, todėl ministerijoje turėtų būti įgyvendinamos trečiųjų šalių teikiamų IS paslaugų stebėjimo ir kontrolės procedūros ir sudarytos sutartys su visais paslaugų (duomenų) teikėjais.

[37] Ten pat, „Dėl saugos dokumentų turinio gairių patvirtinimo“, 5.3.6. p.

3.2. Nepertraukiamo paslaugų teikimo užtikrinimas

Nepertraukiamo paslaugų teikimo ir užtikrinimo procesas[38] rekomenduoja, kad, norint teikti nenutrūkstamas IT paslaugas, reikia sukurti, prižiūrėti ir testuoti IT tęstinumo planus, naudoti nuotolinę atsarginių kopijų saugyklą ir periodiškai rengti tęstinumo plano mokymus. Rezultatyvus nenutrūkstamų paslaugų procesas sumažina IT paslaugų nutrūkimo tikimybę ir poveikį pagrindinėms veiklos funkcijoms ir procesams. Be to, IS veiklos tęstinumo valdymo plano nuostatos turi būti pagrįstos tam tikrais principais – vienas iš jų – IS veiklos atkūrimas (IS veikla atkuriama pagal plane numatytą IS funkcijų prioritetą)[39].

Užsienio reikalų ministerijoje yra patvirtintas veiklos tęstinumo valdymo planas, tačiau jame nenumatyti IS veiklos tęstinumo atkūrimo prioritetai (IS funkcijų prioritetai), todėl kyla vidutinė rizika, kad nenumatytų situacijų atveju pirmiausia gali būti atkurti mažiau svarbūs ministerijos veiklos procesai.

IS veiklos tęstinumo valdymo plano analizė parodė, kad jis nebuvo peržiūrimas ir atnaujinamas įvykus reikšmingiems pasikeitimams (plačiau 1.3 poskyryje), jame nepateikti užpildyti IT įrangos sąrašai, parametrai ir už šios įrangos priežiūrą atsakingi administratoriai, minimalaus funkcionalumo IT įrangos specifikacija, kiekvieno pastato aukšto patalpų brėžiniai ir šiose patalpose esanti įranga bei komunikacijos, kompiuterių tinklo fizinio ir loginio sujungimo schemos ir kita, kaip reikalaujama teisės akte[40].

Užsienio reikalų ministerija numatė, kad IS veiklos tęstinumo valdymo plano veiksmingumas turi būti reguliariai išbandomas praktiniuose mokymuose, tačiau mokymai nebuvo organizuojami, todėl nustatyta nedidelė rizika, kad darbuotojai gali nežinoti ir nesuprasti apie veiklos tęstinumo ir informacijos saugumo svarbą, savo atsakomybę ir funkcijas taikant šį planą ir atkuriant IS veiklą. Kita vertus, neišbandžius, ar planas veiksmingas, nenumatytų situacijų atveju IS veiklos gali nepavykti atkurti taip, kaip numatyta IS veiklos tęstinumo valdymo plane.

Veiklos tęstinumo valdymo plano elementai (organizacinės, aprašomosios, plano veiksmingumo išbandymo nuostatos, veiklos tęstinumo valdymo plane numatyta techninė dokumentacija: sąrašai, schemos, būtinos ministerijos IS veiklos tęstinumui užtikrinti) nebuvo testuojami ir išbandyti, todėl kyla vidutinė rizika, kad įvykus incidentui Užsienio reikalų ministerijos patvirtintas veiklos tęstinumo valdymo planas bus efektyvus ir realiai įvykdomas.

[38] COBIT 4.1, 2011, Vilnius, DS4 procesas, 113 psl.
[39] Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, 11.2 ir 11.2.2 p.
[40] Lietuvos Respublikos vidaus reikalų ministro 2007-05-08 įsakymu Nr. 1V-172 patvirtintos Saugos dokumentų turinio gairės, 5.3.1–5.3.4 ir 5.3.6 p.

Užsienio reikalų ministerija, siekdama teikti nenutrūkstamas IT paslaugas, turėtų prižiūrėti ir testuoti IS veiklos tęstinumo valdymo planą ir periodiškai rengti tęstinumo plano mokymus. Rezultatyvus nenutrūkstamų paslaugų procesas sumažina didelio IT paslaugų nutrūkimo tikimybę ir poveikį pagrindinėms veiklos funkcijoms ir procesams.

3.3. Informacinių sistemų saugos užtikrinimas

Informacinių sistemų saugos užtikrinimo procesas[41] nurodo, kad informacijos vientisumą ir IT saugą nustato IS saugos užtikrinimo procesas, kuris apibrėžia IS naudotojų vaidmenis ir priskiria atsakomybę už IT saugą, IT saugos politikos nustatymą ir saugos procedūrų vykdymą. Tinkamai valdomas IS saugos užtikrinimo procesas garantuoja ne tik IT saugą – jis sumažina galimų IT saugos incidentų poveikį pagrindinei įstaigos veiklai.

Norint įvertinti, koks saugos užtikrinimas turi būti taikomas vienai ar kitai IS, teisės aktai nustato, kad IS klasifikuojamos pagal kategorijas nuo pirmos (aukščiausiosios) iki ketvirtos (žemiausiosios)[42]. Kategorija nustatoma IS duomenų saugos nuostatuose[43].

Ministerijos IS duomenų saugos nuostatuose numatyta, kad atsižvelgiant į duomenų savybes (vientisumo, konfidencialumo ir prieinamumo įtaką sistemų darbui), ministerijos IS priskiriamos antrajai, trečiajai arba ketvirtajai kategorijai. Antrajai priskiriamos konsulinėms funkcijoms atlikti naudojamos IS, trečiai – organizacijos vidinei administracinei veiklai vykdyti skirtos IS, ketvirtai – visos kitos ministerijos vidiniams poreikiams sukurtos ir naudojamos IS. Tikslų IS priskyrimą kategorijoms turėtų nusakyti IS sąrašas (IS duomenų saugos nuostatų priedas „IS servisų aprašas“), tačiau minėtame sąraše kategorijos priskiriamos ne konkrečioms ministerijoje naudojamoms IS, bet IS komponentėms (pvz.: failų serveriai, išoriniai pašto serveriai, tinklas, antivirusinių programų valdymas, KPVS ir kt.).

Ministerijos vidaus dokumentuose neapibrėžta, kokios konkrečios IS komponentės sudaro ministerijos IS (IS komponentės nepriskirtos konkrečioms sistemoms URMIS, KPVS, STDIS), todėl neaiškus IS klasifikavimas pagal kategorijas, taigi gali būti netiksliai nustatyti ministerijos IS tvarkomos elektroninės informacijos apsaugos poreikis, prioritetai ir lygis (vidutinė rizika).

Siekiant aiškesnio ministerijoje naudojamų IS klasifikavimo, ministerija turėtų sukonkretinti ir įvardyti IS, kurios priskiriamos IS duomenų saugos nuostatuose nurodytoms kategorijoms.

[41] COBIT 4.1, 2011, Vilnius, DS5 procesas, 117 psl.
[42] Lietuvos Respublikos vidaus reikalų ministro 2007-07-11 įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės, 3 p.
[43] Ten pat, 4 p.

Saugos politika

IS valdytojas privalo turėti pagal Vidaus reikalų ministerijos tvirtinamas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus IS saugos dokumentus[44]:

- Duomenų saugos nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;
- IS veiklos tęstinumo valdymo planą;
- IS naudotojų administravimo taisykles.

Užsienio reikalų ministerija, užtikrindama IS saugą, vadovaujasi 2010-02-19 užsienio reikalų ministro įsakymu Nr. V-22 patvirtintais IS duomenų saugos nuostatais, IS naudotojų administravimo taisyklėmis, IS veiklos tęstinumo valdymo planu, Saugaus elektroninės informacijos tvarkymo taisyklėmis, tačiau nustatyta, kad ne visi duomenų saugą reglamentuojantys dokumentai atnaujinti (žr. lentelę.

Lentelė. Užsienio reikalų ministerijos IS duomenų saugos politikos dokumentų neatnaujinimo pavyzdžiai

Eil. Nr.	Dokumento pavadinimas	Užsienio reikalų ministerijos veiklos pokyčiai, turėję įtakos elektroninės informacijos saugos užtikrinimui ir valdymui
1.	Lietuvos Respublikos užsienio reikalų ministerijos IS duomenų saugos nuostatai	2011-02-04 keitėsi IT departamento organizacinė struktūra – panaikintas IT ir apsaugos departamentas (ITAD) ir įsteigtas IT departamentas su trimis skyriais, todėl saugos dokumentuose atsakingi asmenys nurodomi neteisingai (*pvz.; ITAD direktorius, ITAD administratoriai*). Šis pokytis turi įtakos visiems išvardytiems duomenų saugos dokumentams ir Naudojimosi internetu ir elektroniniu Užsienio reikalų ministerijos paštu, Užsienio reikalų ministerijos IS funkcijų pokyčių valdymo tvarkos aprašams, Užsienio reikalų ministerijos IS naudotojų administravimo taisyklėms.
2.	Lietuvos Respublikos užsienio reikalų ministerijos saugaus elektroninės informacijos tvarkymo taisyklės	Saugaus elektroninės informacijos tvarkymo taisyklių priede pateiktas asmenų, turinčių įėjimo į tarnybinių stočių patalpas leidimus, sąrašas nebuvo atnaujintas. Jame yra įrašyta asmenų, kurie jau nebedirba Užsienio reikalų ministerijos IT departamente (pvz., nuo 2010-12-01, 2011-07-05).
3.	Lietuvos Respublikos užsienio reikalų ministerijos IS veiklos tęstinumo valdymo planas	Neaktualus IS veiklos tęstinumo valdymo ir veiklos atkūrimo grupių dalyvių sąrašas (kai kurie darbuotojai jau nebedirba ministerijoje arba perkelti dirbti į diplomatines atstovybes, pvz., nuo 2011-08-16, 2012-05-14).
4.	IS servisų aprašas	Apraše įrašyti ne visi ministerijoje naudojami IS komponentai, pvz., nėra ESIDIS, skirtos koordinuoti Lietuvos pozicijas ES išorinės politikos klausimais, kolaboravimo sistemų PANDA ir PANDA II ir kt. Kadangi sąraše įrašyti ne visi naudojami IS servisai, todėl ne visiems servisams priskirti administratoriai.
5.	IS servisų administratorių sąrašas	IS servisus valdo nepriskirti administratoriai, nes pasikeitus administratoriams sąrašas neatnaujintas – sąraše yra asmenų, kurie nebedirba Užsienio reikalų ministerijos IT departamente (pvz. nuo 2010-12-01, 2011-07-05, 2012-01-16).
6.	Prieigos prie URMIS išteklių anketa	Dokumentų valdymo sistema „Avilys“ priskirta prie padidinto saugumo tinklo išteklių, nors realiai ji veikia bendrame ministerijos tinkle.

Šaltinis – Valstybės kontrolė

[44] Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai, 6 p.

Atsižvelgiant į didelę IT darbuotojų kaitą Užsienio reikalų ministerijoje, esamų dokumentų aktualumas turėtų pagerinti IT veiklų tęstinumą, todėl rekomenduotina nustatyti, kad IS tvarkų peržiūros būtų vykdomos periodiškai.

Saugos atitikties vertinimas

Užsienio reikalų ministerijoje, vadovaujantis teisės aktų reikalavimais, antros kategorijos sistemų IT saugos atitikties vertinimą turi atlikti ne rečiau kaip kartą per metus[45]. Ministerijos IS duomenų saugos nuostatuose numatyta, kad siekiant užtikrinti saugos politikos ir kitų saugos politiką reglamentuojančių dokumentų įgyvendinimo kontrolę, saugos įgaliotinis kasmet organizuoja IT saugos atitikties vertinimus. Audituojamu laikotarpiu ministerijos IT saugos atitikties vertinimas buvo atliktas tik vieną kartą – 2012 m. Kyla vidutinė rizika, kad periodiškai neperžiūrint ministerijos IT saugos (neįvertinant saugos dokumentų ir kitų saugumo politiką įgyvendinančių teisės aktų atitiktį realiai duomenų saugos situacijai, neįvertinant pasirengimo atkurti ir užtikrinti IS veiklos tęstinumą saugos incidentų atveju ir kt.), dokumentais įformintos IS saugumo valdymo priemonės gali būti neveiksmingos, didinti veiklos pertrūkių tikimybę.

Naudotojų paskyrų valdymas ir vartotojų identifikavimas

COBIT rekomenduoja[46] sukurti naudotojo paskyros valdymo procedūras, skirtas prašyti, nustatyti, išduoti, pristabdyti, keisti ir uždaryti naudotojo paskyras ir kitas susijusias naudotojo privilegijas, įvesti patvirtinimo procedūrą, nustatančią duomenų ar sistemos valdytoją, suteikiantį prieigos privilegijas.

Užsienio reikalų ministerijoje prieiga prie IS išteklių suteikiama užpildžius Prieigos prie Užsienio reikalų ministerijos informacijos išteklių anketą. Ministerijoje yra įdiegta naudotojų paskyrų valdymo sistema (angl. *Active Directory*), kurioje visi naudotojai suskirstyti į grupes, atitinkančias skyriaus ar departamento pavadinimus. Atitinkamai pagal užimamas pareigas ir veiklą suteikiama prieiga prie informacinių išteklių. Į naudotojų paskyrų valdymo procesą įtrauktas ir personalo departamentas – jis informuoja IT departamentą apie personalo pasikeitimus el. paštu.

IS naudotojų paskyrų valdymo procesas ministerijoje nėra pakankamai užtikrinamas, nes, nutrūkus darbuotojo darbo ar tarnybos teisiniams santykiams su Užsienio reikalų ministerija, dar kurį laiką jam gali būti palikta prieiga prie tarnybinio el. pašto. Todėl yra maža rizika, kad el. laiškus išsiuntus ministerijos vardu informacija gali būti neteisėtai atskleista. Taip pat nustatyta neatitikimų tarp Užsienio reikalų ministerijos Personalo departamento pateiktų darbuotojų sąrašų ir

[45] Lietuvos Respublikos vidaus reikalų ministro 2008-10-27 įsakymu Nr. 1V-384 patvirtinti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, 5.2 p.
[46] COBIT 4.1, 2011, Vilnius, DS5 procesas, DS5.4 kontrolės tikslas, 118 psl.

IS naudotojų sąrašų paskyrų valdymo sistemoje (žr. pavyzdį). Darbuotojų sąrašai IS nėra periodiškai atnaujinami, todėl kyla nedidelė rizika, kad vartotojams suteikiamos teisės, kurios nėra reikalingos jų tiesioginėms pareigoms – informacija gali būti atskleista, pakeista, sunaikinta ar kitaip disponuojama, neturint tam teisės.

Pavyzdys

- Naudotojų paskyrų valdymo sistemoje (*angl. Active Directory*) Konsulinio departamento Piliečių reikalų ir konsulinės pagalbos skyriaus sąrašuose įrašyti du naudotojai, kurių nėra Personalo departamento pateiktuose sąrašuose.
- Du atleisti darbuotojai (2012-07-31 ir 2012-09-03) 2012-10-25 dieną dar galėjo naudotis ministerijos elektroniniu paštu (buvo naudotojų paskyrų valdymo sąrašuose, tačiau su ribota prieiga).
- IT departamento IS vystymo ir priežiūros skyriaus naudotojų paskyrų valdymo sąraše nebuvo darbuotojo, kuris grįžo dirbti į ministeriją iš ambasados Maskvoje. Pagal Personalo departamento pateiktą sąrašą jis priskiriamas IT departamento IS vystymo ir priežiūros skyriui.

COBIT rekomenduoja[47], kad visi IS naudotojai (vidaus, išorės ir laikini) ir jų veiksmai sistemose (veiklos taikomojoje programoje, IT aplinkoje, sistemos operacijose, kuriant ir prižiūrint) būtų unikaliai identifikuojami. Autentiškumo patvirtinimo mechanizmais turėtų nustatyti naudotojų tapatybes. Įdiegtos ir nuolat atnaujintos rentabilios techninės ir procedūrinės priemonės, leidžiančios identifikuoti naudotojus, patvirtinti autentiškumą ir administruoti prieigos teises.

IS naudotojų identifikavimo reikalavimus ministerija yra nustačiusi IS duomenų saugos nuostatuose. IS naudotojų paskyros apsaugotos slaptažodžiais, tačiau ne visuose ministerijos IS (pvz.: KPVS, STDIS) slaptažodžių kompleksiškumo reikalavimai užtikrinami technologinėmis priemonėmis (netikrinamas slaptažodžių ilgis, simbolių skaičius), todėl kyla nedidelė rizika, kad naudotojai gali pasirinkti per silpną ar neatitinkantį reikalavimų slaptažodį.

3.4. Duomenų valdymas

COBIT Duomenų valdymo procesas[48] apibrėžia, kad, norint efektyviai valdyti duomenis, reikia nustatyti reikalavimus duomenims. Duomenų valdymo procesas taip pat skirtas nustatyti efektyvioms laikmenų bibliotekos, duomenų atsarginių kopijų darymo, duomenų atkūrimo ir tinkamo laikmenų sunaikinimo valdymo procedūroms. Efektyvus duomenų valdymas padeda užtikrinti veiklos duomenų kokybę, aktualumą ir prieinamumą.

Asmens duomenys gali būti tvarkomi automatiniu būdu tik tuo atveju, kai duomenų valdytojas arba jo atstovas Vyriausybės nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai[49]. Ministerija yra registruota Asmens duomenų valdytojų valstybės registre 2003-03-28, tačiau ministerijoje automatiniu būdu tvarkomi asmens duomenys ir

[47] COBIT 4.1, 2011, Vilnius, DS5 procesas, DS5.3 kontrolės tikslas,118 psl.
[48] COBIT 4.1, 2011, Vilnius, DS11 procesas, 141 psl.
[49] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 31 str.

kitiems tikslams (žr. pavyzdį), apie kuriuos nebuvo pranešta Valstybinei duomenų apsaugos inspekcijai.

Pavyzdys

Užsienio reikalų ministerijos IS automatiniu būdu tvarkomi, tačiau Asmens duomenų valdytojo registre neįregistruoti asmens duomenys, kurių tvarkymo tikslai yra:

- tvarkyti sulaikytų, suimtų ar nuteistų už padarytas nusikalstamas veikas Lietuvos Respublikos piliečių, bei užsienyje nukentėjusių Lietuvos Respublikos piliečių apskaitą;
- sprendimams dėl konsulinių pažymų dėl pradėto ikiteisminio tyrimo ar teistumo išdavimo priimti;
- sprendimams dėl konsulinių pažymų vietoje prarastų vairuotojo pažymėjimų išdavimo ar atsisakymo išduoti priimti;
- sprendimams dėl konsulinių pažymų vietoje prarastų transporto priemonių registracijos liudijimų išdavimo ar atsisakymo išduoti priimti;
- sprendimams dėl asmens grįžimo pažymėjimo ar jam prilyginto dokumento išdavimo ar atsisakymo išduoti asmens grįžimo pažymėjimui priimti;
- supaprastinto tranzito dokumentams ar supaprastinto tranzito geležinkeliu dokumentams Rusijos Federacijos piliečiams, vykstantiems į Kaliningrado sritį tranzitu per Lietuvos Respublikos teritoriją ir atgal, išduoti.

Asmens duomenų valdytojas privalo įgyvendinti tinkamas organizacines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo. Priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente[50].

Ministerijoje automatiniu būdu asmens duomenys tvarkomi KPVS, STDIS. Atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ministerijos IS automatiniu būdu tvarkomi asmens duomenys turėtų būti priskirti antrajam (STDIS) ir pirmajam (KPVS) saugumo lygiams (žr. pavyzdį).

Pavyzdys

- KPVS turėtų būti priskirtas antrasis asmens duomenų saugumo lygis[51], nes šioje IS tvarkomi ir kaupiami šie ypatingi asmens duomenys[52]: informacija apie asmens teistumą (žyma apie tai, kad asmuo nėra įregistruotas įtariamų, kaltinamų ir teistų asmenų žinybiniame registre, įtariamų, kaltinamų ir teistų asmenų žinybinio registro pažymos duomenys, žyma, ar Lietuvos Respublikos pilietis sulaikytas, suimtas, nuteistas ar nukentėjęs, užsienio valstybės policijos pažymos santrauka, įvykio fabula, sulaikymo, suėmimo ar nuteisimo priežastys bei trukmė, Lietuvos Respublikos piliečio laikymo vieta).
- STDIS turėtų būti priskirtas pirmasis asmens duomenų saugumo lygis[53], nes šioje IS tvarkomi ir apdorojami šie Rusijos Federacijos piliečių, vykstančių į Kaliningrado sritį tranzitu per Lietuvos Respublikos teritoriją ir atgal, asmens duomenys: vardas, pavardė, ankstesnės pavardė, gimimo data, dabartinės pilietybės, pilietybė gimimo metu, ankstesnės pilietybės, asmens tapatybę patvirtinančio dokumento numeris, lytis, šeiminė padėtis, tėvo vardas, tėvo pavardė, motinos vardas, motinos pavardė, adresas, miestas, šalis, gatvė, namo Nr., pašto kodas, telefonas.

Ministerijoje darbuotojai pasirašytinai supažindinami su asmens duomenų apsaugą reglamentuojančiais teisės aktais pagal ministerijos kanclerio 2012-03-08 potvarkiu Nr. VP-93 patvirtintą Supažindinimo su asmens duomenų apsaugą reglamentuojančiais teisės aktais formą. Ministerija neturi parengusi ir patvirtinusi rašytinės formos dokumento, kuriame būtų

[50] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996-06-11 Nr. I-1374), 30 str. 1 d.
[51] Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008-11-12 įsakymu Nr. 1T-71(1.12) patvirtinti Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, 7.3 p.
[52] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996-06-11 Nr. I-1374), 2 str. 8 d.
[53] Ten pat, 7.2 p.

išdėstytos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Kadangi ministerijoje įgyvendintos ne visos teisės aktuose reikalaujamos organizacinės asmens duomenų saugumo priemonės, skirtos apsaugoti asmens duomenims, jie gali būti atsitiktinai sunaikinti, pakeisti arba atskleisti.

COBIT rekomenduoja nustatyti ir vykdyti veiklos poreikius ir tęstinumo planą atitinkančias sistemų, taikomųjų programų, duomenų ir dokumentų atsarginių kopijų darymo ir atkūrimo procedūras.

Ministerijos vidaus Saugaus elektroninės informacijos tvarkymo taisyklėse numatyta, kad atsarginių duomenų kopijų darymo metodika ir technologijos užtikrina galimybę atkurti aktualius duomenis, tačiau ministerija šios metodikos neturi. Atsarginių kopijų tvarkymas vykdomas vadovaujantis IS duomenų saugos nuostatais ir Saugaus elektroninės informacijos tvarkymo taisyklėmis, tačiau šiuose dokumentuose nenustatyti atsarginių duomenų kopijų darymo metodai, detalios rezervinio kopijavimo procedūros, apimančios duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą, duomenų atstatymą iš kopijų. Yra vidutinė rizika, kad, nesant duomenų tvarkymo metodikos, nebus patikrintas kopijose esančios informacijos teisingumas, nebus išbandytas el. informacijos atstatymas iš rezervinės kopijos, todėl incidento metu prarasti aktualūs IS duomenys gali būti neatkurti.

COBIT rekomenduoja nustatyti ir vykdyti procedūras, užtikrinančias, kad būtų laikomasi veiklos poreikių diskretiškų duomenų ir programinės įrangos apsaugos, kai naikinami ar perkeliami duomenys ir techninė įranga.

Ministerijoje įslaptintos informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuoja ministerijos vidaus tvarkos, tačiau nustatyta vidutinė rizika, kad dauguma dokumentų keičiantis organizaciniams, sisteminiams ar kitiems veiklos pokyčiams nebuvo peržiūrimi ir atnaujinami (žr. 6 priedą), todėl kyla rizika, kad tvarkos yra neišsamios ir pasenusios.

4. Stebėsena ir vertinimas

COBIT stebėsenos ir vertinimo grupė[54] pabrėžia, kad nuolat turi būti vertinami visi IS procesai ir jų atitiktis vidaus kontrolės reikalavimams. Vertinimas turėtų apimti efektyvumo valdymą, vidaus kontrolės sistemos stebėjimą, atitiktį teisinio reguliavimo ir valdymo reikalavimams.

Audito metu analizuota, kaip Užsienio reikalų ministerija vertina savo valdomus IS procesus, įvertinti COBIT procesai:

- ME2 Vidaus kontrolės stebėsena ir vertinimas,
- ME3 Atitikties išoriniams reikalavimams užtikrinimas,
- ME4 IT valdymo užtikrinimas.

Įvertinus Užsienio reikalų ministerijos IS valdymą, nustatyta IS vidaus kontrolės branda.

4.1. Vidaus kontrolės stebėsena ir vertinimas, atitikties išoriniams reikalavimams užtikrinimas

COBIT Vidaus kontrolės stebėsenos ir vertinimo procesas[55] rekomenduoja, kad, kuriant efektyvią IT vidaus kontrolės sistemą, reikėtų gerai apibrėžti stebėsenos procesą, apimantį kontrolės išimčių, savianalizės rezultatų, trečiųjų šalių peržiūrų rezultatų stebėseną ir ataskaitas. Pagrindinė vidaus kontrolės stebėsenos nauda yra rezultatyvios ir efektyvios veiklos užtikrinimas bei atitiktis įstatymų ir reglamentuojančių dokumentų reikalavimams.

Lietuvos Respublikos vidaus kontrolės ir vidaus audito įstatymas[56] numato, kad vienas iš vidaus audito uždavinių yra ne rečiau kaip vieną kartą per trejus metus įvertinti, kaip vidaus kontrolė veikia viešajame juridiniame asmenyje. Pavyzdinėje vidaus audito metodikoje[57] rekomenduota, kad vidaus auditorius, atlikdamas vidaus auditą, turi tikrinti ir vertinti bendrosios IS kontrolės priemones ir taikomosios IS kontrolės priemones, atlikti jų testavimą pagal vidaus auditoriaus parengtus šių kontrolės priemonių tikrinimo klausimynus. Užsienio reikalų ministerijos vidaus audito metodikoje, patvirtintoje Lietuvos Respublikos užsienio reikalų ministro 2003-07-02 įsakymu Nr. 122 (2011-01-18 įsakymo Nr. V-12 redakcija) numatyta, kad Vidaus audito skyriaus vidaus auditorius tikrina ir vertina bendrosios IS

[54] COBIT 4.1, 2011, Vilnius, 153–168 psl.
[55] Ten pat, ME2 procesas, 157 psl.
[56] Lietuvos Respublikos vidaus kontrolės ir vidaus audito įstatymas, 2002-12-10 Nr. IX-12535 (nuo 2010-07-01 galiojanti redakcija), 5 str. 2 d. 6 p.
[57] Lietuvos Respublikos finansų ministro 2003-05-02 įsakymas Nr. 1K-117 „Dėl Pavyzdinės vidaus audito metodikos, Vidaus auditorių profesinės etikos taisyklių patvirtinimo“ (nuo 2010-06-04 galiojanti redakcija), 12.5 p.

kontrolės priemones ir taikomosios IS kontrolės priemones, jas testuoja pagal vidaus auditoriaus parengtus kontrolės priemonių tikrinimo klausimynus.

Užsienio reikalų ministerijos vidaus auditoriai nesilaiko šio reikalavimo ir neatlieka IS bendrosios kontrolės vertinimo, todėl kyla vidutinė rizika, kad gali būti nenustatomi vidaus kontrolės trūkumai ir vadovybė apie juos neinformuojama.

Efektyvi atitikties priežiūra reikalauja proceso, užtikrinančio atitiktį įstatymams, taisyklėms ir sutarčių reikalavimams.

COBIT procesas Atitikties išoriniams reikalavimams užtikrinimas[58] apima atitikties reikalavimų nustatymą, reagavimo optimizavimą ir vertinimą, reikalavimų laikymosi užtikrinimą ir, galiausiai, IT atitikties ataskaitų integravimą į visos veiklos atitikties procesus.

Nustatyta, kad ministerijoje nėra procedūrų dėl atitikties išoriniams reikalavimams, susijusiems su IS užtikrinimu. Be to, įvertinus ministerijos IS valdymo atitiktį Lietuvos Respublikos teisės aktų reikalavimams, nustatytos elektroninės informacijos saugos valdymo, asmens duomenų tvarkymo, IS steigimo ir įteisinimo neatitiktys, kurios pateiktos 4 priede. Taip pat pastebėtina, kad 2009 m. ministerija įsigijo (kaina su PVM – 13 209,00 Lt) saugos politikos ir ją įgyvendinančių dokumentų atitikties vertinimo ir valdymo sistemą ir šios sistemos mokymus IS naudotojams bei administratoriams. Į sistemą buvo įkelti ministerijos IS saugos dokumentai, sukurta galimybė atvaizduoti IT veiklos ir saugos procesus, IT paslaugų ar IS bei atitinkamų išorinių reguliuojančių ir vidinių URM dokumentų valdymą ir atitiktis, IT veiklos procesų ir informacijos saugos valdymo efektyvumą ir kt. Šios sistemos sukūrimo ir įdiegimo paslaugos buvo suteiktos 2009 m., tačiau sistema audituojamuoju laikotarpiu nebuvo naudojama.

Užsienio reikalų ministerijoje, siekiant užtikrinti IS veiklos rezultatyvumą ir efektyvumą bei atitiktį įstatymų ir reglamentuojančių dokumentų reikalavimams, turėtų būti vykdoma vidaus kontrolės stebėsena: vidaus auditoriai turi tikrinti ir vertinti bendrosios IS kontrolės priemones ir taikomosios IS kontrolės priemones.

4.2. Informacinių technologijų valdymas ir informacinių sistemų vidaus kontrolės brandos įvertinimas

COBIT IT valdymo užtikrinimo procesas[59] rekomenduoja sukurti rezultatyvią valdymo sistemą, apimančią organizacijos struktūrų, procesų, vadovavimo, funkcijų ir pareigų apibrėžimą, užtikrinantį, kad organizacija investuoja į IT suderintai ir pagal bendrą organizacijos strategiją ir tikslus. Rekomenduojama visus IS procesus ir jų atitiktį vidaus kontrolės reikalavimams vertinti

[58] COBIT 4.1, 2011, Vilnius, ME3 procesas, 161 psl.
[59] Ten pat, ME4 procesas, 165 psl.

nuolat. Vertinimas turėtų apimti efektyvumo valdymą, vidaus kontrolės sistemos stebėjimą, atitiktį teisinio reguliavimo ir valdymo reikalavimams.

Užsienio reikalų ministerijos veikla organizuojama vadovaujantis užsienio reikalų ministro patvirtintais strateginiais veiklos planais, kurie apima ir IT veiklos planavimą. COBIT gerojoje praktikoje rekomenduojamo IT strateginio plano ministerija neturi, bet, vykdant Užsienio reikalų ministerijos kolegijos 2009-03-03 nutarimą, buvo sudaryta darbo grupė, kuri parengė URMIS vystymo gaires artimajam (iki 2 metų) ir vidutinės trukmės (iki 5 metų) laikotarpiui. Gairėse numatyta, kad IT departamentas turėtų atsiskaityti ministerijos kolegijai kartą per metus, tačiau audituojamu laikotarpiu buvo tik vienas atsiskaitymas, kuriame pritarta tarpinei URMIS vystymo gairių įgyvendinimo ataskaitai. IT departamentui reguliariai neatsiskaitant ministerijos kolegijai už URMIS plėtrą, numatytą vystymo gairėse, kyla vidutinė rizika, kad URMIS vystymo gairėse numatyti tikslai nebus įgyvendinti. Artimasis (iki 2 metų) laikotarpis jau yra pasibaigęs, bet gairės nebuvo nė karto atnaujintos, todėl IT planai gali būti nesuderinti su veiklos poreikiais, neskiriamas dėmesys reikiamiems prioritetams.

URMIS vystymo gairės parengtos vienai IS, nors ministerija eksploatuoja ir kitas IS (pvz.: KPVS, STDIS), gairėse neaptartas jų vystymas ir plėtra. Nenustačius vystymo gairių visoms ministerijoje valdomoms IS, gali būti neįvertinti veiklos procesai susiję su tomis IS (vidutinė rizika), todėl būtų tikslinga atnaujinant esamas vystymo gaires išplėsti ir įtraukti minėtas IS.

Ministerijos IS vidaus kontrolė ir branda įvertinta taikant Gebos brandos modelį (angl. *Capability Maturity Model*, CMM). IS brandos vertinimo kriterijai pateikti 5 priede. Atsižvelgiant į ataskaitoje pateiktus faktus nustatyta, kad Užsienio reikalų ministerijos IS vidaus kontrolės branda apibrėžiama kaip Pirminis / *Ad Hoc* (1) procesas (žr. 3 pav.).

3 pav. Užsienio reikalų ministerijos IS vidaus kontrolės brandos lygis

GEBOS BRANDOS MODELIS (angl. - *CMM*)

	(a)	(b)	(c)	(d)	CMM
Optimalus procesas (5)	✗	✗	✗	✗	◆
Lengvai valdomas ir vertinamas procesas (4)	✗	✗	✗	✗	◆
Apibrėžtas procesas (3)	!	✗	✗	✗	△
Pasikartojantis, bet intuityvus procesas (2)	✓	!	!	!	△
Pirminis / Ad Hoc procesas (1)	✓	✓	✓	✓	●
Neegzistuojantis procesas (0)	✓	✓	✓	✓	●

✗	- neatitinka kriterijų
!	- nevisiškai atitinka kriterijų
✓	- atitinka kriterijų
◆	- nepasiektas tam tikras Gebos brandos lygis
△	- nevisiškai pasiektas tam tikras Gebos brandos lygis
●	- pasiektas tam tikras Gebos brandos lygis

(a) - problemos pripažinimas ir informavimas apie ją;
(b) - politika;
(c) - susiję procesai ir mokymas, skirti politikai įgyvendinti;
(d) - politikos efektyvumo ir susijusių procesų vertinimas ir tobulinimas, remiantis šiuo pagrindu.

Šaltinis – Valstybės kontrolė

Norint pasiekti aukštesnį brandos lygį ministerijoje turėtų būti sudarytas IT valdymo komitetas, ar jo funkcijoms atlikti pasirinkta kita ministerijos organizacinė struktūra, tačiau turi būti užtikrintas vadovybės ir pagrindinės veiklos atstovų dalyvavimas, ir tinkamas IT srities klausimų sprendimo detalumas. Be to, URMIS vystymo gairės turi būti atnaujinamos ir apimti visas ministerijos IS, o esama IS valdymą ir saugą apibrėžianti dokumentacija turi būti nuolat atnaujinama ir atitikti realią situaciją. Periodiškai turi būti vertinama rizika ir IS saugos atitiktis, užtikrinama vykdomų procesų stebėsena.

Informacinių sistemų ir infrastruktūros audito
departamento direktorius Dainius Jakimavičius

Informacinių sistemų ir infrastruktūros audito departamento
Informacinių sistemų audito skyriaus
vyriausioji valstybinė auditorė Viktorija Mirošničenko

Valstybinio audito ataskaita pateikta:
Lietuvos Respublikos Seimo Audito komitetui;
Informacinės visuomenės plėtros komitetui;
Lietuvos Respublikos užsienio reikalų ministerijai.

PRIEDAI

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos informacinių sistemų bendroji ir kūrimo kontrolė“
1 priedas

Audito apimtis ir metodai

Audito objektas – Užsienio reikalų ministerijos informacinės sistemos.

Audito subjektas – Lietuvos Respublikos užsienio reikalų ministerija.

Audito tikslas – įvertinti Užsienio reikalų ministerijos IS bendrąją ir kūrimo kontrolę.

Vertinimo kriterijai: Užsienio reikalų ministerijos IS bendroji kontrolė įvertinta taikant Gebos brandos modelį (4 priedas). IS valdymo ir saugos užtikrinimo organizavimą vertinome naudodami IT valdymo metodiką COBIT[60], kuri apibrėžia 34 procesus, kurie suskirstomi į 4 grupes:

Planavimas ir organizavimas:

PO1 Strateginio IT plano apibrėžimas

PO2 Informacinės architektūros nustatymas

PO3 Technologinės krypties nustatymas

PO4 IT procesų, organizacinės struktūros ir ryšių apibrėžimas

PO5 IT investicijų valdymas

PO6 Vadovybės tikslų ir krypties komunikavimas

PO7 IT žmogiškųjų išteklių valdymas

PO8 Kokybės valdymas

PO9 IT rizikos vertinimas ir valdymas

PO10 Projektų valdymas

Įsigijimas ir Įdiegimas:

AI1 Automatizuotų sprendimų nustatymas

AI2 Taikomosios programinės įrangos įsigijimas ir priežiūra

AI3 Technologinės infrastruktūros įsigijimas ir priežiūra

AI4 Pasirengimas naudojimui

AI5 IT išteklių įsigijimas

AI6 Pokyčių valdymas

AI7 Sprendimų ir pokyčių diegimas ir akreditavimas

Teikimas ir palaikymas:

DS1 Paslaugų lygių apibrėžimas ir valdymas

DS2 Trečiųjų šalių paslaugų valdymas

DS3 Veiklos efektyvumo ir pajėgumo valdymas

DS4 Nepertraukiamo paslaugų teikimo užtikrinimas

[60] COBIT 4.1, 2011 m., Vilnius.

DS5 Sistemų saugos užtikrinimas

DS6 Sąnaudų nustatymas ir paskirstymas

DS7 Naudotojų švietimas ir mokymas

DS8 Pagalbos tarnybos ir incidentų valdymas

DS9 Konfigūracijos valdymas

DS10 Problemų valdymas

DS11 Duomenų valdymas

DS12 Fizinės aplinkos valdymas

DS13 Procesų valdymas

Stebėsena ir vertinimas:

ME1 IT veiklos stebėsena ir vertinimas

ME2 Vidaus kontrolės stebėsena ir vertinimas

ME3 Atitikties išoriniams reikalavimams užtikrinimas

ME4 IT valdymo užtikrinimas

Užsienio reikalų ministerijos informacinių sistemų bendrosios ir kūrimo kontrolės audito metu, atrinkus svarbiausius ministerijos veiklos procesus ir atlikus preliminarų rizikos vertinimą, detaliam vertinimui buvo pasirinkta 13 su jais susijusių COBIT[61] apibrėžtų informacinių technologijų procesų, kuriuos analizavome detaliau. Tai Planavimo ir organizavimo grupės (PO) procesai (PO2, PO4, PO6, PO9), Įsigijimo ir įdiegimo grupės (AI) procesai (AI2 (nagrinėtas Užsienio reikalų ministerijos IS modernizavimas) ir AI7), Teikimo ir palaikymo grupės (DS) procesai (DS2, DS4, DS5 ir DS11) ir Stebėsenos ir vertinimo (ME) grupės procesai (ME2, ME3 ir ME4). Audito metu vertinome atitiktį Lietuvos Respublikos teisės aktų reikalavimams ir rekomendacijoms valstybės IS valdymui ir saugai.

Valstybinis auditas atliktas vadovaujantis Valstybinio audito reikalavimais[62], ISACA Tarptautiniais audito standartais, audito gairėmis ir gerąja praktika.

Audito metodai: duomenys Užsienio reikalų ministerijoje rinkti taikant dokumentų peržiūros, apklausos, pokalbio ir anketavimo metodus. Gauti duomenys vertinti taikant skaičiavimo, palyginamosios ir situacijos analizių metodus.

Audituojamas laikotarpis: nuo 2009-01-01 iki 2012-07-01 Ankstesni veiklos laikotarpiai nagrinėti tiek, kiek jie susiję su iki audituojamo laikotarpio pradžios Užsienio reikalų ministerijos priimtais IS plėtros, valdymo ir saugos sprendimais ir jų įgyvendinimu.

Atlikdami auditą laikėmės prielaidos, kad visi mums pateikti dokumentai yra išsamūs ir galutiniai, o jų kopijos atitinka originalus.

[61] COBIT 4.1, 2011 m., Vilnius.

[62] Lietuvos Respublikos valstybės kontrolieriaus 2002-02-21 įsakymas Nr. V-26 (20-01-2012-06-28 įsakymo Nr. V-171 redakcija) „Dėl valstybinio audito reikalavimų patvirtinimo“.

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos
informacinių sistemų bendroji
ir kūrimo kontrolė“
2 priedas

Rekomendacijų, pateiktų valstybinio audito ataskaitoje „Užsienio reikalų ministerijos informacinių sistemų bendroji ir kūrimo kontrolė“, įgyvendinimo planas

Eil. Nr. ataskaitoje	Rekomendacija		Užsienio reikalų ministerijos numatytos rekomendacijų įgyvendinimo priemonės	Rekomendacijos įgyvendinimo terminas (data)
1.	Sudaryti gerosios praktikos rekomenduojamą veiklos informacijos architektūros modelį, palengvinantį optimalų veiklos informacijos kūrimą, naudojimą ir dalijimąsi ja, išlaikant jos vientisumą (1 išvada).		1.1. Sudaryti Užsienio reikalų ministerijos informacinės architektūros modelį. 1.2. Nustatyti informacinės architektūros modelio atnaujinimo procedūras.	2014-12-31
2.	Tobulinti ministerijos IS valdymo organizacinę struktūrą:	2.1.užtikrinti gerosios praktikos rekomenduojamų IT strategijos ir IT valdymo komitetų funkcijų efektyvų vykdymą, parenkant optimalius struktūrinius sprendimus (2.1 išvada);	2.1.1. Priimti/atnaujinti vidaus teisės aktus, įtvirtinant IT strategijos ir IT valdymo funkcijų aiškų priskyrimą esamiems arba naujai įsteigtiems organams.	2013-12-31
		2.2. paskirti duomenų valdymo įgaliotinius (2.2 išvada);	2.2.1. Paskirti duomenų valdymo įgaliotinius.	2013-12-31
		2.3. planuoti rezervinę darbuotojų pakaitą ir svarbių IT darbuotojų pareigų perėmimą (2.3 išvada).	2.3.1. Sudaryti planus, nustatančius IT darbuotojų rezervinę pakaitą bei numatančius svarbių IT darbuotojų pareigų tolygų perėmimą.	2014-12-31
3.	Siekiant užtikrinti ministerijos valdomos informacijos saugą:	3.1. atlikus IS rizikos vertinimą, parengti ir patvirtinti IS rizikos mažinimo (valdymo) priemonių planą (3.1 išvada);	3.1.1. Parengti ir atitinkama tvarka patvirtinti IS rizikos mažinimo (valdymo) priemonių 2012, 2013 ir 2014 m. planus po kiekvieno IS rizikos vertinimo atlikimo.	2014-12-31
		3.2. IS duomenų saugos nuostatuose nustatyti ministerijos IS kategorijas ir nurodyti, kokios komponentės jas sudaro (3.2 išvada);	3.2.1. Priimti atitinkamus URM IS duomenų saugos nuostatų pakeitimus, nurodant komponentes, sudarančias ministerijos IS pagal nustatytas kategorijas.	2014-12-31
		3.3. peržiūrėti ir atnaujinti duomenų saugą reglamentuojančius dokumentus (Užsienio reikalų ministerijos IS duomenų saugos nuostatus, Naudotojų administravimo taisykles, Saugaus elektroninės informacijos tvarkymo taisykles, IS veiklos tęstinumo valdymo planą, IS servisų administratorių sąrašą) (3.3 išvada);	3.3.1. Atnaujinti duomenų saugą reglamentuojančius dokumentus (IS duomenų saugos nuostatus, Naudotojų administravimo taisykles, Saugaus elektroninės informacijos tvarkymo taisykles, IS veiklos tęstinumo valdymo planą, IS servisų administratorių sąrašą).	2013-12-31
		3.4. peržiūrėti ir atnaujinti ministerijoje įslaptintos informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančias ministerijos vidaus tvarkas (3.4 išvada);	3.4.1. Atnaujinti ministerijoje įslaptintos informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančias ministerijos vidaus tvarkas.	2013-12-31

Eil. Nr. ataskaitoje	Rekomendacija		Užsienio reikalų ministerijos numatytos rekomendacijų įgyvendinimo priemonės	Rekomendacijos įgyvendinimo terminas (data)
		3.5. nustatyti paskyrų valdymo proceso procedūras ir visose ministerijos IS įdiegti vartotojų prisijungimo kompleksiškumo reikalavimus užtikrinančias technologines priemones (3.5 išvada).	3.5.1. Nustatyti paskyrų valdymo proceso procedūras. 3.5.2. Visose ministerijos IS įdiegti vartotojų prisijungimo kompleksiškumo reikalavimus užtikrinančias technologines priemones.	2014-12-31
4.	Užtikrinant nenutrūkstamą IS paslaugų teikimą:	4.1. nustatyti IS veiklos tęstinumo atkūrimo prioritetus (4.1 išvada);	4.1.1. Veiklos tęstinumo valdymo plane nustatyti IS veiklos tęstinumo atkūrimo prioritetus.	2013-12-31
		4.2. prižiūrėti ir testuoti IS veiklos tęstinumo valdymo planą ir periodiškai rengti tęstinumo plano mokymus (4.3 išvada);	4.2.1. Nustatyti IS veiklos tęstinumo valdymo plano testavimo ir tęstinumo plano mokymų periodiškumą. 4.2.2.Atlikti IS veiklos tęstinumo valdymo plano testavimą. 4.2.3. Surengti tęstinumo plano mokymus.	2014-12-31
		4.3. užpildyti IT įrangos sąrašus: nurodyti įrangos parametrus ir už jos priežiūrą atsakingus administratorius, parengti minimalaus funkcionalumo IT įrangos specifikaciją, kiekvieno pastato aukšto patalpų brėžinius ir patalpose esančios įrangos ir komunikacijos, kompiuterių tinklo fizinio ir loginio sujungimo schemas (4.2 išvada);	4.3.1. Užpildyti IT įrangos sąrašus: nurodyti įrangos parametrus ir paskirti už jos priežiūrą atsakingus administratorius. 4.3.2. Parengti minimalaus funkcionalumo IT įrangos specifikaciją. 4.3.3 Parengti kiekvieno pastato aukšto patalpų brėžinius ir patalpose esančios įrangos ir komunikacijos, kompiuterių tinklo fizinio ir loginio sujungimo schemas.	2013-12-31
		4.4. nustatyti detaliąsias rezervinio duomenų kopijavimo procedūras, apimančias duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą, duomenų atstatymą iš kopijų (4.4 išvada);	4.4.1. Nustatyti detaliąsias rezervinio duomenų kopijavimo procedūras, apimančias duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą, duomenų atstatymą iš kopijų.	2014-12-31
		4.5. užpildyti duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašą, su visais duomenų teikėjais ir gavėjais sudaryti duomenų mainų sutartis (4.2 išvada).	4.5.1. Sudaryti duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių registrą, 4.5.2. Su visais duomenų teikėjais ir gavėjais sudaryti duomenų mainų sutartis.	2014-12-31
5.	Stiprinti asmens duomenų valdymą ir saugą:	5.1. pranešti Valstybinei asmens duomenų apsaugos inspekcijai visus ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslus (5.1 išvada);	5.1.1. Pranešti Valstybinei asmens duomenų apsaugos inspekcijai visus ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslus.	2014-12-31
		5.2. parengti ir patvirtinti rašytinės formos dokumentą, kuriame būtų nurodytas tvarkomų asmens duomenų saugos lygis, išdėstytos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo	5.2.1. Parengti ir patvirtinti rašytinės formos dokumentą, kuriame būtų nurodytas tvarkomų asmens duomenų saugos lygis, išdėstytos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio	2014-12-31

Eil. Nr. ataskaitoje	Rekomendacija		Užsienio reikalų ministerijos numatytos rekomendacijų įgyvendinimo priemonės	Rekomendacijos įgyvendinimo terminas (data)
		(5.2 išvada).	kito neteisėto tvarkymo.	
6.	Siekiant, kad IS plėtra atitiktų ministerijos veiklos poreikius:	6.1. peržiūrėti, atnaujinti, išplėsti ir detalizuoti URMIS vystymo gaires (7 išvada);	6.1.1. URMIS vystymo gaires peržiūrėti, atnaujinti ir konkretizuoti, kad būtų labiau susietos su aktualiais veiklos poreikiais ir prioritetais ir apimtų visas ministerijos IS.	2013-12-31
		6.2. nustatyta tvarka patvirtinti URMIS, KPVS ir STDIS nuostatus (6.1 išvada);	6.2.2. Patvirtinti URMIS, KPVS ir STDIS nuostatus.	2013-12-31
		6.3. parengti KPVS, STDIS specifikacijas, o URMIS specifikaciją – atnaujinti, jas visas nustatyta tvarka suderinti ir patvirtinti. Prieš kuriant naujas ar modernizuojant esamas ministerijos IS, atnaujinti arba parengti ir nustatyta tvarka suderinti IS nuostatus, specifikacijas ir detaliuosius projektus (6.2 išvada);	6.3.1. Parengti, suderinti ir patvirtinti KPVS ir STDIS specifikacijas. 6.3.2. Atnaujinti, suderinti ir patvirtinti URMIS specifikaciją. 6.3.3. Numatyti kontrolės priemones, kad prieš kuriant naujas ar modernizuojant esamas ministerijos IS, būtų atnaujinti arba parengti ir nustatyta tvarka suderinti IS nuostatai, specifikacijos ir detalieji projektai.	2014-12-31
		6.4. vidaus tvarkose nustatyti, kad, sukūrus ar modernizavus IS, jos testavimas turėtų būti atliekamas sudarius testavimo planą, o testavimo rezultatus vertintų ir galutiniai IS vartotojai (6.3 išvada).	6.4.1. Patvirtinti tvarką, kad sukūrus ar modernizavus IS, jų testavimas būtų atliekamas tik sudarius testavimo planą, o testavimo rezultatus vertintų ir galutiniai IS vartotojai.	2014-12-31
7.	Periodiškai vertinti informacinių sistemų valdymo kontrolę ir atlikti išorės reglamentavimo stebėseną (1.2 išvada).		7.1. Vidaus audito skyriaus planuose numatyti tikrinti ir vertinti bendrosios informacinių sistemų kontrolės priemones ir taikomosios informacinių sistemų kontrolės priemones, atlikti jų testavimą, taip pat atlikti išorės reglamentavimo stebėseną.	2014-12-31
Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytu laiku: Užsienio reikalų ministerijos Informacinių technologijų departamento direktorius Vaclovas Šalkauskas, tel.: (8-5) 236 2475, el. paštas: vaclovas.salkauskas@urm.lt.				

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos
informacinių sistemų bendroji
ir kūrimo kontrolė“
3 priedas

IT personalo kaita 2009–2012 m.

	Darbuotojas	Einamos pareigos	Nuo kada pradėjo dirbti IS administravimo skyriuje (po 2011 m. restruktūrizacijos IS vystymo ir priežiūros skyrius)	Iki kada dirbo IS aptarnavimo skyriuje (po 2011 m. restruktūrizacijos IS vystymo ir priežiūros skyrius)	Pastabos
1.	Darbuotojas A	Vyriausiasis specialistas	2009-07-07	2010-01-11	Esant tarnybinei būtinybei paskirtas IS administravimo skyriaus vedėju
2.		IS administravimo skyriaus vedėjas	2010-01-12	2012-05-14	Esant tarnybinei būtinybei paskirtas IT departamento direktoriumi
3.		IS vystymo ir priežiūros skyriaus vedėjas	2012-11-05	-	Ėjo šias pareigas iki 2012-12-01
4.	Darbuotojas B	Vyriausiasis specialistas	Iki audituojamojo laikotarpio pradžios	2009-07-07	Rotacijos būdu perkeltas dirbti į diplomatinę atstovybę
5.		Vyriausiasis specialistas	2012-10-22	-	Ėjo šias pareigas iki 2012-12-01
6.	Darbuotojas C	Vyriausiasis specialistas	2009-12-28	-	Ėjo šias pareigas iki 2012-12-01
7.	Darbuotojas D	Vyriausiasis specialistas	Iki audituojamojo laikotarpio pradžios	2009-11-30	Perkeltas į kitą departamentą
8.	Darbuotojas E	Vyriausias specialistas	Iki audituojamojo laikotarpio pradžios	2010-08-09	Rotacijos būdu perkeltas dirbti į diplomatinę atstovybę
9.	Darbuotojas F	Vyriausiasis specialistas	Iki audituojamojo laikotarpio pradžios	2010-12-01	Rotacijos būdu perkeltas dirbti į diplomatinę atstovybę
10.	Darbuotojas G	Vyriausiasis specialistas	2010-12-01	2012-07-31	Darbo santykių pabaiga
11.	Darbuotojas H	Vyriausiasis specialistas	2011-07-01	2012-05-14	Esant tarnybinei būtinybei paskirtas IS vystymo ir priežiūros skyriaus vedėju
12.		IS vystymo ir priežiūros skyriaus vedėjas	2012-05-14	2012-11-05	
13.		Vyriausiasis specialistas	2012-11-05	-	Ėjo šias pareigas iki 2012-12-01
14.	Darbuotojas I	Vyriausiasis specialistas	Iki audituojamojo laikotarpio pradžios	2011-07-04	Atleistas
15.	Darbuotojas Y	Vyriausiasis specialistas	2011-08-16	2012-03-05	Perkeltas į kitą departamentą
16.	Darbuotojas J	Vyriausiasis specialistas	2012-02-06	-	Ėjo šias pareigas iki 2012-12-01
17.	Darbuotojas K	Vyriausiasis specialistas	2012-11-13	-	Ėjo šias pareigas iki 2012-12-01
18.	Darbuotojas L	Vyriausiasis specialistas	2012-08-28	2012-10-15	Rotacijos būdu perkeltas dirbti į diplomatinę atstovybę
19.	Darbuotojas M	Vyriausiasis specialistas	2012-11-23	-	Ėjo šias pareigas iki 2012-12-01

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos
informacinių sistemų bendroji
ir kūrimo kontrolė“
4 priedas

Neatitiktis privalomiems vykdyti teisės aktų reikalavimams

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai		
1.	*10 punktas:* Saugaus elektroninės informacijos tvarkymo taisyklėse pateikiama: 10.1. informacinėje sistemoje esančios informacijos kategorijų sąrašas ir kiekvienai kategorijai priskirtini duomenys; [...]	Užsienio reikalų ministerijos IS saugaus elektroninės informacijos tvarkymo taisyklėse nepateikiama kiekvienai informacijos kategorijai priskirti duomenys.
2.	*11 punktas:* Informacinės sistemos veiklos tęstinumo valdymo planui keliami šie reikalavimai: […] 11.2 Informacinės sistemos veiklos tęstinumo valdymo plano nuostatos turi būti pagrįstos tam tikrais principais. Privalomi šie pagrindiniai principai: [...] 11.2.2. informacinės sistemos veiklos atkūrimas (informacinių sistemų veikla atkuriama pagal šiame plane numatytą informacinių sistemų funkcijų prioritetą).	Užsienio reikalų ministerijos IS veiklos tęstinumo valdymo plane nenumatyti IS funkcijų prioritetai.
3.	*26 punktas:* Saugos dokumentai valstybės institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Vidaus reikalų ministerija.	Saugos dokumentai ministerijoje nebuvo persvarstomi (peržiūrimi) 2011 ir 2012 m. Ministerijos IS duomenų saugos nuostatai, IS saugaus elektroninės informacijos tvarkymo taisyklės ir IS naudotojų administravimo taisyklės neatnaujintos nuo 2010-02-19, nors buvo pokyčių, turinčių įtakos elektroninės informacijos saugos užtikrinimui ir valdymui (žr. 3.3 poskyrio 1 lentelė).
4.	*30 punktas:* Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika” grupės standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis.	Audituojamu laikotarpiu ministerijoje IS rizikos įvertinimas buvo organizuojamas ne kasmet. IS rizikos vertinimas neatliktas 2010 ir 2011 m.
5.	*36 punktas:* Informacinės sistemos sąrankos dokumentacija turi būti nuolat atnaujinama ir rodyti esamą informacinės sistemos sąrankos būklę.	IS sąrankos dokumentacija ministerijoje neatnaujinama nuolat, todėl ji nerodo esamos IS sąrankos būklės (pvz.: URMIS specifikacija neatnaujinta nuo 1998 m., nors buvo IS pakeitimų, turinčių įtakos IS programinei ir techninei įrangai).
Lietuvos Respublikos vidaus reikalų ministro 2007-05-08 įsakymu Nr. 1V-172 patvirtintos Saugaus dokumentų turinio gairės		
6.	*3 punktas:* Informacinės sistemos duomenų	URMIS duomenų saugos nuostatuose nenurodyti

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	saugos nuostatus (toliau – nuostatai) sudaro šie skyriai: 3.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta: [...] 3.1.3. informacinės sistemos valdytojo ir tvarkytojo (tvarkytojų) bei kitų subjektų, kuriems taikomi nuostatų reikalavimai, pavadinimai ir adresai; [...] 3.3. „Organizaciniai ir techniniai reikalavimai“, kuriame turi būti nurodyta: [...] 3.3.2. įrangos, skirtos apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai, nurodant ilgiausią leistiną neatnaujinimo laiką; [...] 3.4. „Reikalavimai personalui“, kuriame turi būti nurodyta: [...] 3.4.2. informacinės sistemos naudotojų mokymo, mokymų dažnumo reikalavimai ir asmuo, atsakingas už šių mokymų organizavimą.	subjektų, kuriems taikomi nuostatų reikalavimai, pavadinimai ir adresai (3.1.3. p.). Taip pat nenurodytas įrangos, skirtos apsaugoti IS nuo kenksmingos programinės įrangos, ilgiausias leistinas neatnaujinimo laikas (3.3.2. p.) bei IS naudotojų mokymų dažnumo reikalavimai ir asmuo, atsakingas už šių mokymų organizavimą (3.4.2. p.).
7.	*4 punktas:* Saugaus elektroninės informacijos tvarkymo taisykles sudaro šie skyriai: 4.1. „Bendrosios nuostatos“, kuriame turi būti nurodyta: [...] 4.1.2. elektroninės informacijos, priskirtos tam tikrai kategorijai, sąrašas ir asmenys, atsakingi už šios informacijos tvarkymą. [...] 4.3. „Saugaus elektroninės informacijos tvarkymas“, kuriame turi būti nurodyta: 4.3.3. atsarginių duomenų kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarka, nurodant kopijuojamų duomenų imtį, atsarginių duomenų kopijų darymo metodus ir dažnumą, visiško ir dalinio duomenų atkūrimo bandymų metodus ir dažnumą bei atsakingus už atsarginių duomenų kopijų darymą, duomenų atkūrimą ir atsarginių duomenų kopijų apsaugą asmenis ir atsarginių duomenų kopijų saugojimo kontrolę; [...]	URMIS saugaus elektroninės informacijos tvarkymo taisyklėse nenurodytas elektroninės informacijos, priskirtos tam tikrai kategorijai, sąrašas ir asmenys, atsakingi už šios informacijos tvarkymą (4.1.2 p.) ir kopijuojamų duomenų imtis bei atsarginių duomenų kopijų darymo metodai (4.3.3. p.).
8.	*5 punktas:* Informacinės sistemos veiklos tęstinumo planą sudaro šie skyriai: [...] 5.2. „Organizacinės nuostatos“, kuriame turi būti nurodyta: [...] 5.2.9. reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti elektroninės informacijos saugos incidento atveju. 5.3. „Aprašomosios nuostatos“, kuriame turi būti nurodyta: [...] 5.3.1. informacinių technologijų įrangos sąrašai, šios įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai bei minimalus informacinės sistemos veiklos atkūrimui, nesant administratoriaus, reikalingos kompetencijos ar žinių lygis; 5.3.2. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos užtikrinti institucijos poreikius atitinkančią informacinės	Užsienio reikalų ministerijos IS veiklos tęstinumo valdymo plane nenurodomi reikalavimai, keliami atsarginėms patalpoms, naudojamoms IS veiklai atkurti elektroninės informacijos saugos incidento atveju (5.2.9. p.). IS veiklos tęstinumo valdymo plano turinys neatitinka nustatytų reikalavimų IS veiklos tęstinumo valdymo plano turiniui, nes nenurodyta: – IT įrangos sąrašai, šios įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai bei minimalus IS veiklos atkūrimui, nesant administratoriaus, reikalingos kompetencijos ar žinių lygis (5.3.1. p.); – minimalaus funkcionalumo IT įrangos, tinkamos užtikrinti institucijos poreikius atitinkančią IS veiklą elektroninės informacijos saugos incidento metu, specifikacija (5.3.2. p.);

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	sistemos veiklą elektroninės informacijos saugos incidento metu, specifikacija; 5.3.3. kiekvieno pastato aukšto patalpų brėžiniai ir šiose patalpose esanti įranga bei komunikacijos: [...] 5.3.4. kompiuterių tinklo fizinio ir loginio sujungimo schemos; […] 5.3.6. duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai; [...] 5.3.8. institucijos darbuotojų sąrašas, kuriame nurodyti darbuotojų darbo telefonai, o veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių – mobiliojo ir namų telefono numeriai ir gyvenamosios vietos adresai. 5.4. „Plano veiksmingumo išbandymo nuostatos“, kuriame turi būti nurodyta: 5.4.1. plano veiksmingumo paskutinio ir kito planuojamo išbandymo būdas ir data.	– kiekvieno pastato aukšto patalpų brėžiniai ir šiose patalpose esanti įranga bei komunikacijos (5.3.3.p.); – kompiuterių tinklo fizinio ir loginio sujungimo schemos (5.3.4. p.); – duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai (5.3.6. p.) – institucijos darbuotojų sąrašas, kuriame nurodyti darbuotojų darbo telefonai (5.3.8. p.). Užsienio reikalų ministerijos veiklos tęstinumo valdymo plane nenurodyta plano veiksmingumo paskutinio ir kito planuojamo išbandymo data (5.4.1. p.).
Lietuvos Respublikos vidaus reikalų ministro 2008-09-27 įsakymu Nr. 1V-384 patvirtinti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai		
9.	*3 punktas:* Bendrieji informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai:[...] 3.8. institucija turi išsiaiškinti, kiek ji ilgiausiai gali tęsti savo funkcijų įgyvendinimą neveikiant informacinei sistemai ar jos daliai; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atkūrimą per šį laikotarpį; turi būti parengtas veiksmų planas, užtikrinantis informacinės sistemos veiklos atnaujinimą ketvirtosios kategorijos informacinėms sistemoms per 16 val., trečiosios kategorijos informacinėms sistemoms – per 8 val., antrosios kategorijos informacinėms sistemoms – per 1 val., pirmosios kategorijos informacinėms sistemoms – per 15 min.;	URMIS priskiriama antros kategorijos valstybės IS. Numatytas veiklos atkūrimo laikotarpis (Priklausomai nuo posistemės numatyta neveikimo trukmė svyruoja nuo 4 val. iki 7 dienų.) neatitinka antrai IS kategorijai keliamų reikalavimų.
10.	*5 punktas:* Antrosios kategorijos informacinių sistemų elektroninės informacijos papildomi techniniai saugos reikalavimai:[...] 5.2. Atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;[…] 5.3. turi būti reglamentuota nešiojamųjų kompiuterių, skirtų informacinės sistemos elektroninės informacijos tvarkymui, naudojimo ne institucijos patalpose tvarka; [...] 5.12. Patekimas į tarnybinių stočių patalpas turi būti registruojamas.[…] 5.19. patekimas į patalpas, kuriose laikomos kopijos, turi būti registruojamas žurnale;[…] 5.21. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai; 5.22. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 6 paskutinių slaptažodžių; 5.23. administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu naudotojų	Užsienio reikalų ministerijos antrosios kategorijos IS atitikties vertinimas atliekamas rečiau kaip kartą per metus. Atitikties vertinimas neatliktas 2009, 2010 ir 2011 m. (5.2. p.). Ministerijoje nereglamentuota nešiojamųjų kompiuterių, skirtų IS elektroninės informacijos tvarkymui, naudojimo ne institucijos patalpose tvarka. Patekimas į tarnybinių stočių patalpas neregistruojamas. Patekimas į patalpas, kuriose laikomos kopijos, neregistruojamas žurnale. URMIS naudotojų administravimo taisyklių 30 p. nurodoma, kad slaptažodį turi sudaryti ne mažiau kaip 7 simboliai. URMIS nėra kontrolės priemonių, kurios neleistų naudotojui įvesti trumpesnį nei 8 simbolių slaptažodį. IS nėra kontrolės priemonių, kurios neleistų naudotojui nustatyti slaptažodį iš buvusių 6 paskutinių slaptažodžių. Nėra specialių reikalavimų administratorių slaptažodžiams.

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	slaptažodžiams, arba kitomis autentiškumo patvirtinimo priemonėmis (pvz., biometrinėmis, lustinėmis kortelėmis ir pan.).	
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374.		
11.	*30 straipsnis:* Duomenų saugumas. 1. Duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.).	Ministerija neįgyvendino tinkamų organizacinių asmens duomenų saugumo priemonių, nes nepatvirtino rašytinės formos dokumento (duomenų valdytojo patvirtintos asmens duomenų tvarkymo taisyklės, duomenų valdytojo ir duomenų tvarkytojo sudaryta sutartis ir pan.).
12.	*3 straipsnis:* Asmens duomenų tvarkymo reikalavimai 1. Duomenų valdytojas privalo užtikrinti, kad asmens duomenys būtų: 1) renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis; 31 straipsnis: Pranešimas apie duomenų tvarkymą Asmens duomenys gali būti tvarkomi automatiniu būdu tik tuo atveju, kai duomenų valdytojas arba jo atstovas (pagal šio įstatymo 1 straipsnio 3 dalies 3 punktą) Vyriausybės nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai [...] 33 straipsnis: Išankstinė patikra 1. Valstybinė duomenų apsaugos inspekcija atlieka išankstinę patikrą šiais atvejais: 1) kai duomenų valdytojas automatiniu būdu ketina tvarkyti ypatingus asmens duomenis, išskyrus šių duomenų tvarkymą vidaus administravimo tikslais arba šio įstatymo 5 straipsnio 2 dalies 6 ir 7 punktuose nustatytais atvejais;	STDIS tvarkomi asmens duomenys, reikalingi supaprastinto tranzito dokumentams ar supaprastinto tranzito geležinkeliu dokumentams Rusijos Federacijos piliečiams, vykstantiems į Kaliningrado sritį tranzitu per Lietuvos Respublikos teritoriją ir atgal, išduoti. Toks duomenų tvarkymo tikslas nėra registruotas asmens duomenų valdytojų valstybės registre. KPVS tvarkomi ir kaupiami ypatingos svarbos asmens duomenys, tačiau asmens duomenų valdytojų valstybės registre tokie asmens duomenys nėra registruoti.
Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008-11-12 įsakymu Nr. 1T-71(1.12) patvirtinti Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms		
13.	*9 punktas:* Siekiant užtikrinti pirmąjį saugumo lygį, turi būti įgyvendintos šios organizacinės ir techninės duomenų saugumo priemonės: 9.1. patvirtintas (-i) rašytinės formos dokumentas (-ai) (duomenų valdytojo patvirtintos asmens duomenų tvarkymo taisyklės, duomenų valdytojo ir duomenų tvarkytojo sudaryta sutartis ir pan.), kuriame (-iuose) turi būti nurodyta: […]	Ministerija neįgyvendino organizacinių duomenų saugumo priemonių, nes nepatvirtino rašytinės formos dokumento, nors tvarko asmens duomenis STDIS, KPVS.
14.	*10 punktas:* Siekiant užtikrinti antrąjį saugumo lygį, turi būti įgyvendintos Bendrųjų reikalavimų 9 punkte numatytos organizacinės ir techninės duomenų saugumo priemonės bei šios organizacinės ir techninės duomenų saugumo	Nenustatytas skaičius leistinų nevykusių bandymų prisijungti prie STDIS ir KPVS duomenų bazių, kuriuose saugomi asmens duomenys.

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	priemonės: […] 10.3. nustatytas leistinų nevykusių bandymų prisijungti prie duomenų bazės (-ių) skaičius; [...] 10.9. registruojami avarinio asmens duomenų atkūrimo veiksmai (kada ir kas vykdė asmens duomenų atkūrimo veiksmus tiek automatiniu, tiek neautomatiniu būdu.	Ministerijoje neregistruojami avarinio asmens duomenų atkūrimo veiksmai (10.9. p).
Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės		
15.	*4 punktas:* Informacinės sistemos steigėjas rengia informacinės sistemos nuostatų projektą, kuriame turi būti aptarti šie informacinės sistemos klausimai: 4.1. Steigimo pagrindas: teisės aktai, kuriems įgyvendinti steigiama informacinė sistema, įstatymai ir kiti teisės aktai, kuriais reglamentuojama numatoma kompiuterizuoti veiklos sritis, steigiamos informacinės sistemos tikslai, pagrindinės funkcijos, laukiamas rezultatas. 4.2. Organizacinė struktūra: informacinės sistemos valdytojas, tvarkytojas (-ai) ir institucijos, nuolat teikiančios ir gaunančios informacinės sistemos duomenis (t. y. duomenų teikėjai ir duomenų gavėjai). Informacinės sistemos valdytojas ir tvarkytojas gali būti ta pati valstybės institucija.	2008 m. patvirtintuose URMIS nuostatuose nėra nurodytas steigimo pagrindas, teisės aktai, kuriems įgyvendinti steigiama IS, duomenų teikėjai ir duomenų gavėjai. Informacinės visuomenės komiteto prie Lietuvos Respublikos Vyriausybės 2008-12-11 rašte Nr. (13)S-1755 nurodoma, kad URMIS nuostatai neatitinka Taisyklių 4 p. nurodytų struktūros ir turinio reikalavimų. KVPS ir STDIS nuostatų projektai nepatvirtinti.
16.	*14 punktas:* Informacinė sistema kuriama ir diegiama pagal patvirtintą informacinės sistemos specifikaciją. Kūrimą ir diegimą atlieka informacinės sistemos valdytojas, informacinės sistemos tvarkytojas arba teisės aktų nustatyta tvarka išrinktas kitas asmuo. Jeigu informacinę sistemą kuria kitas juridinis asmuo, jam informacinės sistemos valdytojas gali suteikti teisę tvarkyti informacinės sistemos duomenis sistemos kūrimo ir diegimo laikotarpiu. Tokiu atveju informacinės sistemos kūrėjas privalo užtikrinti tvarkomų duomenų apsaugą Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.	KVPS ir STDIS specifikacijos neparengtos ir nepatvirtintos.
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807		
17.	*8 straipsnis:* Duomenų valdymo įgaliotinis [...] 3. Duomenų valdymo įgaliotinį skiria valstybės informacinės sistemos ar registro valdytojas arba tvarkytojas. Duomenų valdymo įgaliotinis turi būti paskirtas kiekvienam registrui, valstybės informacinei sistemai ar jos posistemiui. Valstybės informacinės sistemos ar registro valdytojo arba tvarkytojo sprendimu tas pats asmuo gali būti paskirtas kelių registrų, valstybės informacinių sistemų ar posistemių duomenų valdymo įgaliotiniu.	Ministerijoje nuo 2012-01-01 duomenų valdymo įgaliotinis nepaskirtas.
Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas, 1999-11-25 Nr. VII-1443		
18.	*40 straipsnis:* ADA sistemų ir tinklų steigimas ir įteisinimas [...]	Užsienio reikalų ministerija neturi leidimo automatizuotai apdoroti įslaptintą informaciją su slaptumo žyma „Riboto naudojimo“, nors

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	3. Automatizuotai apdoroti ir perduoti įslaptintą informaciją galima tik įteisintomis ADA sistemomis ir tinklais. ADA sistemos ir tinklai laikomi įteisintais, kai paslapčių subjektui, jo rangovui (subrangovui) yra išduodamas leidimas automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais. Leidimą automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais išduoda Saugumo priežiūros tarnybos funkcijas atliekanti institucija ar žinybinė saugumo priežiūros tarnyba Saugumo priežiūros tarnybos funkcijas atliekančios institucijos nustatyta tvarka.	apdoroja ir perduoda šią informaciją (Padidinto saugumo tinkle veikia saugus el. paštas tarp ministerijos ir diplomatinių atstovybių).
Lietuvos Respublikos vidaus reikalų ministerijos 2010-07-07 nutarimu Nr. 1014 patvirtintas Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas		
19.	*31 punktas:* Laikmenų, pažymėtų žymėjimo ženklu su nuoroda, kad laikmenoje galima saugoti įslaptintą informaciją, žymimą slaptumo žymomis „Visiškai slaptai“ arba „Slaptai“, patikrinimas atliekamas kartą per metus.	Ministerijoje laikmenų, pažymėtų žymėjimo ženklu su nuoroda, kad laikmenoje galima saugoti įslaptintą informaciją, žymimą slaptumo žymomis „Visiškai slaptai“ arba „Slaptai“, patikrinimas nebuvo atliktas.
20.	*32 punktas:* Laikmenų, pažymėtų žymėjimo ženklu su nuoroda, kad laikmenoje galima saugoti įslaptintą informaciją, žymimą slaptumo žyma „Konfidencialiai“, patikrinimas atliekamas kartą per trejus metus.	Ministerijoje laikmenų, pažymėtų žymėjimo ženklu su nuoroda, kad laikmenoje galima saugoti įslaptintą informaciją, žymimą slaptumo žyma „Konfidencialiai“, patikrinimas nebuvo atliktas.
Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės 2004-10-15 įsakymas Nr. T-131 „Dėl Valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“		
21.	*50.4 punktas:* parengto IS projekto patvirtinimas.[...] Pakeitimai IS specifikacijoje ir parengtame IS projekte tvirtinami tuo pačiu metu. Konkrečią IS specifikacijos ir IS projekto pakeitimų tvirtinimo tvarką ir procedūras nustato kompiuterizuojamo objekto vadovybė. IS specifikacijos pakeitimai taip pat derinami su Informacinės visuomenės plėtros komitetu prie Susisiekimo ministerijos ir institucijomis, kurios yra nurodytos IS nuostatuose ir teiks duomenis IS.	URMIS specifikacija nebuvo atnaujinta nuo 1998 m. nors buvo IS pakeitimų, turinčių įtakos IS programinei ir techninei įrangai.

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos informacinių sistemų bendroji ir kūrimo kontrolė“
5 priedas

Gebos brandos modelis

Šiame priede apibūdinamas Gebos brandos modelis, taikomas IS kontrolės tikslų brandos lygiui įvertinti. IS valdymo brandos vertinimo kriterijai pateikiami lentelėje. Pateiktas kiekvieno tikslo įvertinimas yra žemiausias atitinkamo tikslo įvertinimas pagal bet kurį iš toliau išvardytų keturių punktų (a–d). Vertinimo vidurkis neišvedamas, nes sudėtinių vertinimų vidurkiai neatspindi realios situacijos.

Kiekvienoje kategorijoje analizuojami šie aspektai:			
(a) Problemos pripažinimas ir informavimas apie ją	(b) Politika	(c) Susiję procesai ir mokymas, skirti politikai įgyvendinti	(d) Politikos efektyvumo ir susijusių procesų vertinimas ir tobulinimas, remiantis šiuo pagrindu
0. Neegzistuojantis procesas			
Organizacija nepripažįsta spręstinos problemos egzistavimo ir dėl to apie tai nepateikia jokios informacijos.	Šiuo klausimu nėra jokios politikos.	Nėra jokio atpažįstamo proceso, susijusio su šia problema.	Neatliekamas joks vertinimas, susijęs su šia problema.
1. Pirminis (*Ad Hoc*) procesas			
Yra faktų, patvirtinančių, kad organizacija pripažįsta problemos egzistavimą ir būtinumą ją spręsti, tačiau apie tai per mažai informuojama.	Egzistuoja neišsami politika. Ji netinkamai dokumentuojama, skelbiama arba įgyvendinama.	Individualiu arba kiekvienu konkrečiu atveju taikomi *Ad Hoc* metodai. Problema nenagrinėjama valdybos lygiu.	Stebėsena vykdoma reaguojant į incidentą, dėl kurio organizacija patiria tam tikrą nuostolį.
2. Pasikartojantis, bet intuityvus procesas			
Apie problemą (prireikus) atitinkamai informuojama visa organizacija.	Egzistuoja aiški politika.	Su problema susiję procesai formaliai yra nustatyti, aktyviai dalyvaujant ir prižiūrint vadovybei, tačiau taikomi ne visoje organizacijoje. Mokymas neorganizuojamas, o informavimas apie standartus ir pareigas paliktas individualių darbuotojų nuožiūrai.	Vadovybė yra nustačiusi pagrindinius vertinimus ir vertinimo metodus bei būdus, tačiau pastarieji parengti nepakankamai.
3. Apibrėžtas procesas			
Visa organizacija supranta, kad reikia reaguoti į problemą, ir tam pritaria.	Organizacijoje vykdoma tvirta ir aiški politika, suderinta su kai kuriomis kitomis susijusiomis politikos kryptimis. Iš dalies atsižvelgiama į rizikos valdymą.	Procedūros standartizuotos, dokumentuotos ir dauguma jų įgyvendinamos visoje organizacijoje. Vadovybė yra informavusi apie standartizuotas procedūras ir vykdo neformalų mokymą. Nors procedūras galima įvertinti, tačiau jos nėra sudėtingos ir formaliai atspindi esamą patirtį.	Susijusių veiklos sričių rodiklių registravimas ir stebėsena padeda tobulinti veiklą. Beveik visų susijusių procesų stebėsena vykdoma pagal tam tikrus (pirminius) dokumentus, tačiau mažai tikėtina, kad vadovybė galėtų pastebėti bet kokį nukrypimą, kadangi tokios priemonės paprastai taikomos individualiai. Priežasčių analizė atliekama retai.
4. Lengvai valdomas ir vertinamas procesas			
Visais atitinkamais organizacijos lygiais	Vykdoma tvirta ir aiški politika,	Organizacija gerai pažįsta savo klientą ir turi aiškiai apibrėžtas	Susijusių procesų tobulinimas visų pirma yra pagrįstas kiekybiniu supratimu, užtikrinant

problema suprantama tinkamai ir reikalaujama imtis priemonių.	integruota su kitomis susijusiomis politikos kryptimis. Atsižvelgiama į rizikos valdymą.	pareigas. Procesai yra aiškiai suformuluoti, integruoti ir taikomi visoje organizacijoje. Procesai yra gerai įsisavinami ir palaikomi organizuojant atitinkamą mokymą. Visi susijusių procesų dalyviai žino apie riziką ir galimybes.	galimybę stebėti ir vertinti, kaip laikomasi procedūrų bei susijusių procesų dokumentų reikalavimų. Vadovybė yra nustačiusi leistinus nukrypimus, į kuriuos būtina atsižvelgti, vykdant susijusius procesus. Paaiškėjus, kad procesai yra neveiksmingi arba neefektyvūs, dažniausiai, tačiau ne visada, imamasi priemonių. Kartais susiję procesai tobulinami, įgyvendinant geriausią vidaus praktiką. Vykdomas priežasčių analizės standartizavimas. Pradedamas nuolatinis veiklos gerinimo procesas.
5. Optimalus procesas			
Problemos ir jos sprendimo būdų vertinimas yra pažangus bei perspektyvus.	Organizacija vykdo tvirtą ir aiškią politiką, integruotą su visomis kitomis susijusiomis politikos kryptimis, visapusiškai atsižvelgiant į rizikos valdymą.	Susiję procesai atnaujinti, atsižvelgiant į geriausią išorinę praktiką ir nuolatinio veiklos tobulinimo bei brandos modeliavimo rezultatus kitose organizacijose. Susijusių procesų rizika ir rezultatai yra apibrėžti, suderinti, ir apie juos informuojama visa organizacija. Organizuojamas modernus mokymas ir informavimas. Įgyvendinama politika užtikrino organizacijos, darbuotojų ir procesų sugebėjimą greitai prisitaikyti ir visapusiškai palaikyti rizikos struktūros pokyčius.	Stebėsena, savęs vertinimas ir informavimas apie problemą (prireikus) vykdomi visos organizacijos lygiu, optimaliai išnaudojant procesus ir technologijas, naudojamus vertinimo, analizės, informavimo ir mokymo tikslais. Analizuojamos visų problemų ir nukrypimų priežastys, laiku numatant ir inicijuojant veiksmingas priemones. Naudojamasi nepriklausomų ekspertų konsultavimo paslaugomis ir lyginamąja analize.

Valstybinio audito ataskaitos
„Užsienio reikalų ministerijos
informacinių sistemų bendroji
ir kūrimo kontrolė“
6 priedas

Užsienio reikalų ministerijoje įslaptintos informacijos duomenų tvarkymą reglamentuojantys dokumentai

Nr.	Tvarka	Priežastis atnaujinti tvarką
1.	Lietuvos Respublikos užsienio reikalų ministro 2010-03-03 įsakymu Nr. V-27 patvirtintas „Nacionalinių įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“ perdavimo URM ADA sistemomis tvarkos aprašas“ (aktuali redakcija 2010-05-28 Nr. V-67)	Neatnaujinta: 1.1. Šiuo įsakymu Informacinių technologijų ir apsaugos departamento Informacinių sistemų ir darbo vietų priežiūros skyriui buvo pavesta konsultuoti darbuotojus ir šalinti nesklandumus, susijusius su įslaptintų dokumentų perdavimu Užsienio reikalų ministerijos ADA sistemomis, tačiau po restruktūrizacijos departamentas buvo panaikintas, o vietoj jo įsteigtas IT departamentas ir Saugos kontrolės skyrius.
2.	Lietuvos Respublikos užsienio reikalų ministerijos valstybės sekretoriaus 2005-12-09 potvarkiu Nr. VP-32 patvirtintas „Lietuvos Respublikos užsienio reikalų ministerijos įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas“	Neatnaujinta: 2.1. Apraše numatyta, kad Apsaugos skyrius, kuris pasirašytinai supažindina atitinkamus ministerijos darbuotojus su teisės aktų, reglamentuojančių įslaptintai informacijai įrašyti skirtų kompiuterių informacijos laikmenų ir ADA sistemų ir tinklų apsaugą, reikalavimais, tačiau restruktūrizacijos šias funkcijas perėmė Saugos kontrolės skyrius. 2.2. Apraše numatyta, kad Specialiosios kanceliarijos skyrius yra atsakingas už įslaptintai informacijai įrašyti skirtų laikmenų registravimą, laikmenų perdavimą, tačiau po restruktūrizacijos šis skyrius buvo panaikintas, o už šias funkcijas atsakomybė priskirta Įslaptintos informacijos valdymo skyriui.
3.	Lietuvos Respublikos užsienio reikalų ministro 2004-09-30 įsakymu Nr. V-125 patvirtintas „Užsienio reikalų ministerijos Europos Sąjungos departamento antrinės subregistratūros įslaptintos informacijos, gaunamos saugiu elektroninio pašto tinklu, administravimo taisyklės“ (aktuali redakcija 2006-10-13 Nr. V-116)	Neatnaujinta: 3.1. Apraše likusi nuostata dėl SKS (Specialiosios kanceliarijos skyriaus), tačiau po 2011-02-04 restruktūrizacijos skyrius buvo panaikintas, o vietoj jo įsteigtas Įslaptintos informacijos valdymo skyrius.
5.	Lietuvos Respublikos užsienio reikalų ministro 2010-05-21 įsakymu Nr. V-64 patvirtintas „Įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, rengimo, paskirstymo, dauginimo, kopijų naudojimo, perdavimo ir naikinimo užsienio reikalų ministerijoje tvarkos aprašas“	Neatnaujinta: 5.1. Apraše likusi nuostata, kad Lietuvos Respublikos diplomatinėms atstovybėms, remiantis Lietuvos Respublikos įslaptintos informacijos ir dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, perdavimo ministerijos valdomomis ADA sistemomis krypčių sąrašu, patvirtintu užsienio reikalų ministro 2010-04-06 įsakymu Nr. V-43, įslaptinti dokumentai perduodami saugiu elektroniniu paštu, tačiau 2011-01-04 įsakymas Nr. V-43 pripažintas netekusiu galios.
6.	Lietuvos Respublikos užsienio reikalų ministro 2007-12-27 įsakymu Nr. V-120 patvirtintas „Nacionalinių, NATO ir Europos sąjungos įslaptintų dokumentų, žymimų slaptumo žymomis „Visiškai slaptai“, „Slaptai“ ir „Konfidencialia“, rengimo, registravimo, siuntimo, dauginimo, skirstymo, saugojimo, naikinimo ir apskaitos užsienio reikalų ministerijoje tvarkos aprašas“ (aktuali redakcija 2011-06-16 Nr. V-112)	Neatnaujinta: 6.1. Apraše likusi nuostata dėl IT ir apsaugos departamento, tačiau po 2011-02-04 restruktūrizacijos departamentas buvo panaikintas, o vietoj jo įsteigtas IT departamentas ir Saugos kontrolės skyrius.