



Valstybinio audito ataskaita

## VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMAS TEISINGUMO MINISTERIJOJE

2014 m. lapkričio 14 d. Nr. VA-P-90-2-13



Su valstybinio audito ataskaita galima susipažinti  
Valstybės kontrolės interneto puslapyje  
adresu [www.vkontrole.lt](http://www.vkontrole.lt)

# TURINYS

---

<u>SANTRUMPOS IR SAVOKOS</u>	<u>3</u>
<u>SANTRAUKA</u>	<u>4</u>
IŠVADOS	4
REKOMENDACIJOS	5
<u>IŽANGA</u>	<u>7</u>
<u>AUDITO REZULTATAI</u>	<u>9</u>
<u>1. Informacinių išteklių valdymas Teisingumo ministerijoje</u>	<u>9</u>
1.1. Informacinių technologijų strateginis planavimas, tikslų ir krypties komunikacija	9
1.2. Informacinės architektūros nustatymas	12
1.3. Informacinių technologijų procesų, organizacinės struktūros ir ryšių apibrėžimas	13
1.4. Informacinių technologijų investicijų valdymas	16
1.5. Projektų valdymas ir informacinių išteklių kūrimas	17
1.6. Informacinių sistemų ir registrų saugos užtikrinimas	20
1.7. Vidaus kontrolės stebėseną ir vertinimas, atitikties išoriniams reikalavimams užtikrinimas	21
<u>2. Informacinių technologijų valdymo ir informacinių sistemų vidaus kontrolės brandos įvertinimas</u>	<u>22</u>
<u>PRIEDAI</u>	<u>26</u>

## SANTRUMPOS IR SĄVOKOS

---

**COBIT** – ISACA<sup>1</sup> sukurta IT valdymo ir vadovavimo metodika

**Duomenų sintaksės taisyklės** – duomenų aprašymo ir manipuliavimo instrukcijos (taisyklės)

**Duomenų žodynas** (angl. – *Data Dictionary*) – duomenų bazė, kurią sudaro duomenų elemento pavadinimas, tipas, reikšmių diapazonas, šaltinis ir įgaliojimas prieiti prie kiekvieno duomenų bazės duomenų elemento. Ši duomenų bazė nurodo ir tai, 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<sup>2</sup>

**IS** – informacinė sistema

**IT** – informacinės technologijos

**IVPK** – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos

**KADIS** – Kalėjimų departamento informacinė sistema

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

---

<sup>1</sup> ISACA – Information Systems Audit and Control Association. Prieiga per internetą <http://www.isaca.org/about-isaca/Pages/default.aspx> [Žiūrėta 2013-11-27].

<sup>2</sup> COBIT 4.1, 2011 m., Vilnius, 189 psl.

## SANTRAUKA

---

Vienas Teisingumo ministerijos veiklos tikslų – formuoti valstybės politiką registų ir ministro valdymo sričiai priskirtų informacinių sistemų veiklos srityse, organizuoti, koordinuoti ir kontroliuoti šios valstybės politikos įgyvendinimą<sup>3</sup>. Teisingumo ministro valdymo srityje yra visai valstybei ypač didelę svarbą turintys informaciniai ištekliai – valstybės registrai ir valstybės informacinės sistemos.

Daugumą ministerijos valdomų informacinių išteklių tvarko teisingumo ministro valdymo sričiai priskirtos institucijos, todėl audito metu pagrindinis dėmesys buvo skirtas ministerijos veiklai ir veiksams, užtikrinantiems šių išteklių tvarkymo planavimą ir organizavimą, stebėseną, vertinimą ir koordinavimą, kitiems valstybės informacinių sistemų ir registų strateginio valdymo aspektams.

Ministerija ir teisingumo ministro valdymo sričiai priskirtos įstaigos valdo ir (ar) tvarko 28 informacines sistemas bei registrus ir 1 kadastrą. Teisingumo ministro valdymo sričiai priskirta 16 įstaigų.

Audito tikslas – įvertinti Teisingumo ministerijos informacinių išteklių valdymą.

Auditą atlikome Teisingumo ministerijoje. Informaciją rinkome teisingumo ministro valdymo sričiai priskirtose institucijose: Centrinėje hipotekos įstaigoje, Europos teisės departamente, Kalėjimų departamente, Valstybiniame patentų biure, Lietuvos teismo ekspertizės centre, Lietuvos teisės institute, Valstybinėje vartotojų teisių apsaugos tarnyboje, Vilniaus valstybės garantuojamos teisinės pagalbos tarnyboje, VĮ Registrų centre, Valstybinėje teismo medicinos tarnyboje ir Valstybinėje duomenų apsaugos inspekcijoje.

Audito išvados pateikiamos išanalizavus gautą ministerijos valdomų informacinių išteklių dokumentaciją, darbo grupių ir komisijų darbo reglamentus ir protokolus, informacinių išteklių kūrimo dokumentaciją, registų ir informacinių sistemų registro duomenis, atsižvelgus į pokalbius su ministerijos ir išvardytų įstaigų atstovais.

Audituojamas laikotarpis 2010–2013 m.

Įvertinę audito metu surinktus įrodymus, pateikiame valstybinio audito išvadas ir rekomendacijas.

## IŠVADOS

1. Nėra visą teisingumo ministro valdymo sritį apimančios IT valdymo sistemos, nesivadovaujama rekomenduojamais IT paslaugų valdymo standartais:
  - 1.1. ministerija į IT plėtros planavimui skirtus dokumentus įtraukdama tik dvi (iš 16) teisingumo ministro valdymo sričiai priskirtas įstaigas, koordinuoja ne visų ministro valdymo srities informacinių išteklių kūrimo ir tobulinimo kryptis (1.1 poskyris, 9 psl.);

---

<sup>3</sup> Lietuvos Respublikos Vyriausybės 1998-07-09 nutarimu Nr. 851 patvirtintų Lietuvos Respublikos teisingumo ministerijos nuostatų 7 p.

- 1.2. Teisingumo ministro valdymo srityje yra valstybės IS ir registrų, kurių valdytoja turėtų būti pati ministerija, o ne ministro valdymo sričiai priskirtos įstaigos (1.3 poskyris, 13 psl.);
- 1.3. nėra valdymo struktūros, kurioje dalyvaujantys asmenys atstovautų visų ministerijos valdomų sričių IT poreikiams ir analizuotų ministerijos valdomoms valstybės IS ir registrams kylančias rizikas, jas apibendrintų, teiktų siūlymus, priimant strateginius sprendimus dėl IT plėtros prioritetų ir investicijų į šias technologijas (1.3 poskyris, 13 psl.);
- 1.4. IT projektų vykdymo valdymas ministerijai pavaldžiose įstaigose nėra sistemiškas, ne visada įvertinamas IT sprendimų poreikis ir techninis suderinamumas valstybės mastu (1.5 poskyris, 18 psl.);
- 1.5. ministerijos vadovybė neturi duomenų apie teisingumo ministro valdymo srities IT procesų efektyvumą, atitiktį veiklos reikalavimams, todėl nenumatoma IT procesų kontrolės spragos (1.7 poskyris, 22 psl.).
2. Teisingumo ministerijoje kontrolės priemonės, padedančios užtikrinti teisės aktais nustatytą el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą, yra nepakankamos, nes:
  - 2.1. nėra teisingumo ministro valdymo srities informacinių išteklių bendros architektūros modelio, atitinkančio visoje valdymo srityje sudaromus IT plėtros planus (1.2 poskyris, 12 psl.);
  - 2.2. nenumatyta valdymo srities duomenų klasifikavimo sistema, pagrįsta duomenų svarba ir diskretiškumu (1.2 poskyris, 12 psl.);
  - 2.3. nepaskirtas asmuo, atsakingas už ministerijai pavaldžių institucijų IT saugos kuravimą, koordinavimą ir kontrolę (1.3 poskyris, 13 psl.).
3. Sukurta investicijų planavimo ir skyrimo sistema nepakankamai efektyvi sprendžiant IT investicijų klausimus, nes investicijų skyrimo atrankos kriterijai informacinėms sistemoms ir registrams taikomi netinkamai (1.4 poskyris, 16 psl.).
4. Ministerija skiria nepakankamai dėmesio teisingumo ministro valdymo sričiai priskirtų institucijų IS ir registrų kūrimui ir įteisinimui:
  - 4.1. neturi tikslios informacijos apie ministro valdymo srities informacinių išteklių skaičių, o ministerijai pavaldžios įstaigos naudoja neįteisintas IS (1.2 poskyris, 12 psl.);
  - 4.2. Kalėjų departamentas nevykdo Valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose nustatytų privalomų reikalavimų kuriant IS, todėl neužtikrina reikiamo KADIS duomenų tvarkymo, naudojimo ir saugos (1.5 poskyris, 18 psl.);
  - 4.3. nesuderinti ir nepatvirtinti vieno registro ir keturių naudojamų IS duomenų saugos nuostatai bei šešių IS saugos politiką įgyvendinantys dokumentai – Veiklos tęstinumo valdymo planas, Naudotojų administravimo taisyklės, Saugaus elektroninės informacijos tvarkymo taisyklės (1.6 poskyris, 20 psl.).

## REKOMENDACIJOS

### Lietuvos Respublikos teisingumo ministerijai

1. Parengti bendrą teisingumo ministro valdymo srities IT plėtros planą, kuris apimtų visus srities valstybės informacinius išteklius ir kuriame būtų numatytas Teisingumo ministerijos ir kitų ministerijų valdomų informacinių išteklių tvarkymo prioritetų ir krypčių suderinamumas, taip pat priemonės, užtikrinančios IT išteklių ir priemonių planavimo, skyrimo, vykdymo ir panaudojimo kontrolę (1.1 išvada).

2. Inventorizuoti valdymo srities informacinius išteklius, peržiūrėti jų valdymą reglamentuojančius aktus ir priimti sprendimus dėl šių aktų keitimo vadovaujantis Valstybės informacinių išteklių valdymo įstatymu (1.2 ir 4 išvados).
3. Sukurti organizacinę struktūrą, kuri spręstų pagrindinius IT strateginius ir IT valdymo uždavinius ir užtikrintų reikiamą visų lygių – vadovybės, visų teisingumo ministro valdymo sričių veiklos ir IT atstovavimą bei veiklų koordinavimą (1.3 išvada).
4. Siekiant užtikrinti teisingumo ministro valdymo srities įstaigų vykdomų IT projektų valdymo kokybę ir panaudoti pavaldžių įstaigų turimą IT projektų valdymo patirtį, patvirtinti bendrošius IT projektų valdymo principus (1.4 išvada).
5. Užtikrinanti IS atitiktis išoriniams reikalavimams kontrolę, mažinančią neatitikimų teisės aktams skaičių ir garantuojančią informacijos saugos reikalavimų laikymąsi (1.5, 2.3 ir 4 išvados).
6. Nustatyti teisingumo ministro valdymo srities informacinės architektūros modelį: suklasifikuoti visus srityje valdomus ir tvarkomus duomenis pagal svarbą ir apibrėžti jų vientisumo ir nuoseklumo principus (2.1–2.2 išvados).
7. Sukurti arba pritaikyti esamą IT turto ir paslaugų investicijų valdymui skirtą metodiką, kurioje būtų išsamai IT biudžeto sudarymo ir prioritetų nustatymo tvarka, IT investicijų kontrolės ir duodamos naudos analizės mechanizmas (3 išvada).
8. Pakeisti ministerijos IT investicijų planavimo ir skyrimo sistemą taip, kad visiems teisingumo ministro valdymo srities informaciniams ištekliams tenkančios investicijos būtų vertinamos taikant tinkamus kriterijus (3 išvada).

Rekomendacijų įgyvendinimo planas pateiktas 2 priede.

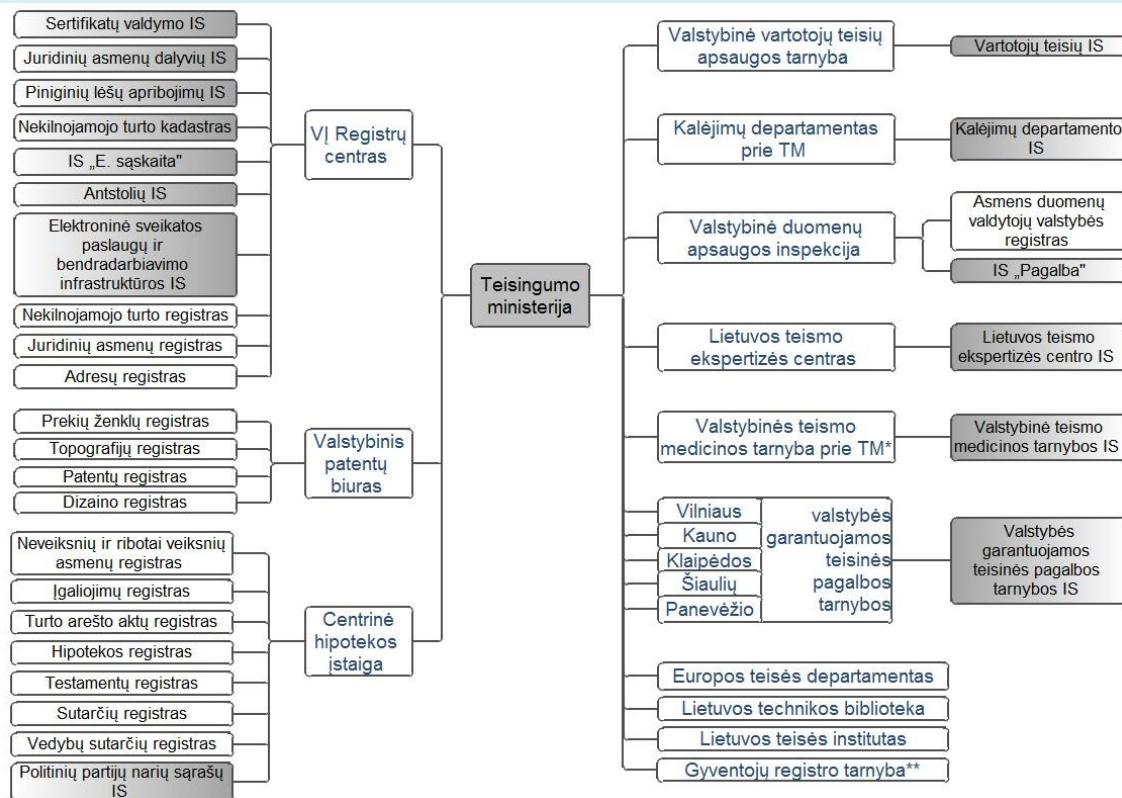
# IŽANGA

Valstybės kontrolė atliko teisingumo ministro valdymo srityje esančių informacinių išteklių valdymo ir kūrimo auditą, kuris apėmė laikotarpį nuo 2010 iki 2013 m.

Daugumą ministerijos valdomų informacinių išteklių tvarko ministro valdymo sričiai priskirtos institucijos, todėl audito metu daugiausia dėmesio buvo skirta ministerijos veiklai ir veiksams, užtikrinantiems šių išteklių tvarkymo planavimą ir organizavimą, stebėseną, vertinimą ir koordinavimą, kitus valstybės informacinių sistemų ir registrų strateginio valdymo aspektus.

Ministerija ir ministro valdymo sričiai priskirtos įstaigos valdo ir (ar) tvarko 29 informacinius išteklius: 13 informacinių sistemų, 15 registrų ir 1 kadastrą. Ministro valdymo sričiai priskirta 16 įstaigų, kurios tvarko ir kitų ministerijų valdomus informacinius išteklius (žr. 1 pav.).

**1 pav.** Teisingumo ministro valdymo srities įstaigų tvarkomi informaciniai ištekliai



● - informacinė sistema, kadastras

○ - registras

\* - Valstybinė teismo medicinos tarnyba prie Teisingumo ministerijos nuo 2015-01-01, Vyriausybės 2014-06-18 nutarimu Nr. 547, priskiriama sveikatos apsaugos ministro valdymo sričiai.

\*\* - nenagrinėta, nes Gyventojų registro tarnyba teisingumo ministro valdymo sričiai priskirta nuo 2014 m. spalio 1 d.

Šaltinis – Valstybės kontrolė

Atsižvelgus į audito planavimo metu nustatytas rizikas, informacinių sistemų kūrimo kontrolės vertinimui buvo pasirinkta Kalėjimų departamento prie Teisingumo ministerijos informacinė sistema.

Teisingumo ministerijos informacinių išteklių valdymo ir kūrimo kontrolės vertinimas atliktas vadovaujantis Valstybinio audito reikalavimais ir tarptautinės Informacinių sistemų audito ir

kontrolės asociacijos ISACA parengta Informacinių technologijų valdymo metodika COBIT<sup>4</sup>. Audito metu atlikus preliminarų rizikos vertinimą, buvo pasirinkti 10 iš 34 COBIT apibrėžtų informacinių technologijų valdymo procesų, kurie audito metu buvo vertinami išsamiau.

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

Atliekant auditą buvo daroma prielaida, kad visi auditoriams pateikti dokumentai yra teisingi, išsamūs ir galutiniai, o jų kopijos atitinka originalus.

Išsami informacija apie audito duomenų rinkimo ir vertinimo metodus pateikta 1 priede.

---

<sup>4</sup> COBIT 4.1, 2011 m., Vilnius.

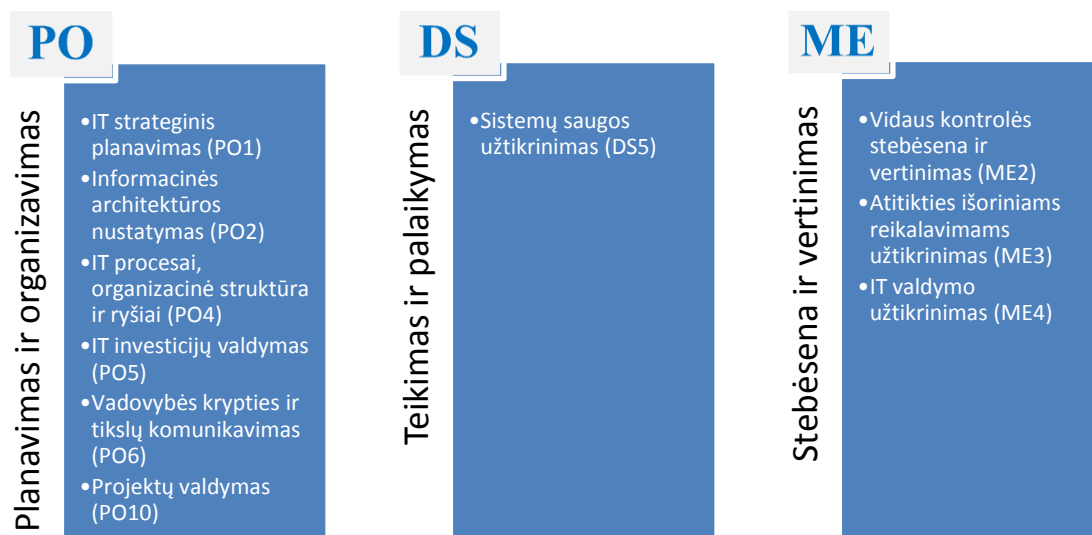


# AUDITO REZULTATAI

## 1. INFORMACINIŲ IŠTEKLIŲ VALDYMAS TEISINGUMO MINISTERIJOJE

Teisingumo ministerijos informacinių išteklių valdymas (IS bendrosios kontrolės priemonių veiksmingumas) vertintas atsižvelgiant į teisės aktų reikalavimus ir COBIT siūlomą gerąją praktiką. Atsižvelgus į audito planavimo metu pastebėtus IT valdymo trūkumus (nėra bendros IT strategijos, trūksta informacinių išteklių valdymo dokumentacijos ir kt.) ministerijos informaciniams ištekliams vertinti pasirinkta 10 COBIT procesų (žr. 2 pav.).

**2 pav.** Ministerijos informacinių išteklių valdymui vertinti pasirinkti COBIT procesai



Šaltinis – Valstybės kontrolė

Įvertinus informacinių išteklių valdymą, nustatyta IS vidaus kontrolės branda (žr. 2 skyrių).

### 1.1. Informacinių technologijų strateginis planavimas, tikslų ir krypties komunikacija

COBIT strateginio IT plano apibrėžimo procesas nurodo, kad IT strateginis planas reikalingas norint nustatyti kryptį ir valdyti IT išteklius derinant su veiklos strategija ir prioritetais<sup>5</sup>. Strateginis planas leidžia pagrindinėms suinteresuotosioms šalims geriau suprasti IT teikiamas galimybes ir jų naudojimo apribojimus, įvertinti esamą veiklą, nustatyti reikalavimus pajėgumams ir žmogiškiesiems ištekliams bei išaiškinti investicijų poreikį. Tokiu būdu užtikrinamas visų veiklos grandžių darnus darbas, įgyvendinant valdymo sričiai keliamus uždavinius ir siekiant bendrų

<sup>5</sup> COBIT 4.1, 2011 m., Vilnius, PO1 procesas, 29 psl.

veiklos tikslų.

Atsižvelgiant į strateginio planavimo svarbą ir Valstybės kontrolės 2006–2007 m. atliktų informacinių technologijų veiklos audito rekomendacijas, COBIT geroji praktika – IT strateginis planavimas – nuo 2012 m. yra perkeltas į Lietuvos informacinių išteklių valdymo teisinio reguliavimo sritį ir privalomas ypatingos svarbos valstybės informacinių išteklių valdytojams.

Ministerija valdo ypatingos svarbos valstybės informacinius išteklius<sup>6</sup>, todėl nuo 2012 m. jai taikomas įstatymu nustatytas IT strateginio planavimo reikalavimas<sup>7</sup>. Įstatymas nustato, kad tokius informacinius išteklius valdanti institucija rengia IT plėtros planą ne ilgesniam kaip 3 metų laikotarpiui. Jame turi būti nustatyti IT priemonių, skirtų informacijai, duomenims, dokumentams ir (arba) jų kopijoms tvarkyti, kūrimo ir naudojimo tikslai, uždaviniai, nurodomos planuojamos kurti ar modernizuoti valstybės informacinės sistemos ir registrai, jų steigimo, modernizavimo prioritetai, planuojamos diegti elektroninės paslaugos, reikalingi finansiniai ir žmogiškieji ištekliai, organizacinės ir teisinės priemonės, kvalifikaciniai reikalavimai darbuotojams, darbuotojų mokymų poreikis, jų veiklos organizavimas ir kontrolė.<sup>8</sup>

Atsižvelgiant į tai, kad visus ministerijos valdomus ypatingos svarbos valstybės informacinius išteklius tvarko ministro valdymo sričiai priskirtos įstaigos, šios srities IT strateginis planavimas tampa ypač svarbus. Išanalizavus ministro valdymo srityje esančių registrų ir valstybės informacinių sistemų veiklos ir IT plėtros planavimo schemą nustatyta, kad IT plėtros planavimui skirti du dokumentai<sup>9</sup>, kurie apima tik dviejų ministro valdymo sričiai priskirtų įstaigų – Centrinės hipotekos įstaigos ir VĮ Registrų centro – veiklos sričių IT plėtrą.

2010–2012 m. IT plėtros priemonės buvo nustatytos ministro valdymo sričiai priskirtų įstaigų veiklos planuose, nuo 2013 m. IT plėtra vykdyta pagal ministerijos valdomų valstybės registrų ir informacinių sistemų viešųjų paslaugų perkėlimo į elektroninę erdvę plėtros 2013–2019 metų veiksmų planą (toliau – 2013–2019 metų veiksmų planas). Plane numatyti viešųjų paslaugų perkėlimo į elektroninę erdvę tikslai, uždaviniai, modernizuojamų IS ir registrų plėtros prioritetai, planuojamos diegti paslaugos. Tačiau dokumento turinys neatitinka įstatymo reikalavimų – jame nėra informacijos apie reikalingus finansinius ir žmogiškuosius išteklius, organizacines ir teisines priemones, kvalifikacinius reikalavimus darbuotojams, darbuotojų mokymų poreikį, jų veiklos organizavimą ir kontrolę. Jis apima septynių, o ne įstatymo nustatytą trejų metų laikotarpį. Pažymėtina, kad planas nuo patvirtinimo dienos nebuvo peržiūrimas ir koreguojamas. Dalies priemonių terminai nenustatyti, tad nėra galimybės įvertinti, kada jos buvo ar bus įgyvendintos. Teisingumo ministerijoje iki 2014 m. vidurio nebuvo teisingumo ministro valdymo srities IT plėtros plano.

Valstybės informacinių išteklių valdymo įstatyme nustatyti reikalavimai iš dalies įgyvendinti tik audito metu – 2014-06-18 patvirtintas Teisingumo ministerijos valdomų registrų ir valstybės informacinių sistemų IT plėtros 2014–2016 m. planas (toliau – 2014–2016 m. IT plėtros planas), tačiau jis apima tik tų pačių dviejų įstaigų – Centrinės hipotekos įstaigos ir VĮ Registrų centro – veiklos sričių IT plėtrą.

Išanalizavus teisingumo ministro valdymo sričiai priskirtų įstaigų 2012–2014 m. veiklos

<sup>6</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 3 str. 1 p.

<sup>7</sup> Ten pat, 9 str. 1 d.

<sup>8</sup> Ten pat, 9 str. 1 d.

<sup>9</sup> Lietuvos Respublikos teisingumo ministro 2012-11-28 įsakymu Nr. 1R-297 patvirtintas Lietuvos Respublikos teisingumo ministerijos valdomų valstybės registrų ir informacinių sistemų viešųjų paslaugų perkėlimo į elektroninę erdvę plėtros 2013–2019 metų veiksmų planas ir 2014-06-18 įsakymu Nr. 1R-191 patvirtinti Lietuvos Respublikos teisingumo ministerijos valdomų registrų ir valstybės informacinių sistemų informacinių technologijų plėtros 2014–2016 metų planai.

planavimo dokumentus ir metines veiklos ataskaitas nustatyta, kad beveik visose įstaigose buvo planuojamos, vykdomos ir įgyvendinamos IT plėtros priemonės, kurios nebuvo nurodytos ministro valdymo srities IT plėtros strateginio planavimo dokumentuose (žr. 1 pavyzdį).

### 1 pavyzdys

Ministerijos valdomų valstybės registų ir informacinių sistemų viešųjų paslaugų perkėlimo į elektroninę erdvę plėtros 2013–2019 metų veiksmų plane nėra informacijos apie Valstybinio patentų biuro viešųjų paslaugų perkėlimą į elektroninę erdvę (2013 m. – 213 tūkst. Lt; 2014 m. – 265 tūkst. Lt), Valstybinės duomenų apsaugos inspekcijos IS pritaikymą aptarnauti duomenų valdytojus ir duomenų subjektus elektroniniu būdu bei jos elektroninių paslaugų sistemos tobulinimą (2008–2013 m. 2 376 tūkst. Lt).

Ministerijoje nėra IT strateginio planavimo dokumento, kuriame būtų numatyti ministro valdymo sričiai priskirtose įstaigose suplanuoti IT plėtros darbai: Valstybinio patentų biuro IS diegimas ir modernizavimas, dalyvavimas Europos patentų tarnybos IT plėtros projektuose; Kalėjų departamento KADIS pertvarkymas (2010–2013 m. 2 244 tūkst. Lt); Lietuvos teismo ekspertizės centro IT ir Valstybinės teismo medicinos tarnybos IS kūrimas ir modernizavimas.

Teisingumo ministro valdymo srities veiklos tikslų perkėlimas į IT plėtros planus ir susiejimas su IT tikslais nėra sklandus, nes planai nėra suderinti tarpusavyje ir apima ne visas vykdomas veiklas. 2014–2016 IT plėtros plane numatytos VĮ Registų centras veiklos, kurių nėra 2013–2019 veiksmų plane, pvz., kuriamos el. paslaugos vykdant Antstolių IS plėtrą, Licencijų IS kūrimą ir kt.

COBIT rekomenduoja<sup>10</sup> nustatyti IT politiką ir sukurti IT kontrolės sistemą, kurioje būtų įtvirtintos aiškios šios politikos įgyvendinimo ir atnaujinimo procedūros bei aiškiai apibūdintas institucijos požiūris į IT rizikas. Komunikacijos sistema turėtų sudaryti sąlygas bendradarbiauti visoms valdymo srities institucijoms ir reguliuoti šio proceso nukrypimus (įskaitant IT sutrikimus).

Ministerija neturi nuoseklios ir išsamios visą valdymo sritį apimančios IT valdymo strategijos, kurioje ministerijos ir ministro valdymo srities veiklos prioritetai bei strateginiai tikslai būtų susieti su visų valdymo sričiai priskirtų įstaigų IT/IS plėtra ir modernizavimu. Ministerija neturi informacijos apie ministro valdymo sričiai priskirtų institucijų IT plėtrą, nekoordinuoja ministro valdymo srities informacinių išteklių kūrimo ir tobulinimo kryptį, todėl jo valdymo sričiai priskirtos įstaigos sprendimus dėl IT plėtros prioritetų priima savarankiškai, o įstaigų IT būklė ne visada atitinka ministerijos nustatytą plėtros kryptį ir veiklos prioritetus (žr. 2 pavyzdį).

### 2 pavyzdys

Valstybinė teismo medicinos tarnyba savo funkcijoms atlikti kuria IS, kuriose tvarkomi ypatingi asmens duomenys, tačiau nesivadovauja teisės aktais patvirtinta IS kūrimo metodika, sistema kuriama be IS specifikacijos, neparengtos IS pokyčių ir testavimo tvarkos.

Vilniaus valstybės garantuojamos teisinės pagalbos tarnyboje, kaip ir kitose mažesnėse ministerijai pavaldžiose įstaigose pastebima, kad ministerija skiria nepakankamai dėmesio efektyviam IT ūkio valdymui: neužtikrinama fizinė sauga, naudojama IS, kurios tikslai, struktūra ir procesai neaprašyti – IS neįteisinta ir neturi privalomų IS dokumentų (žr. 4 priedą).

Valstybiniame patentų biure neatnaujinti registų duomenų saugos nuostatai ir veiklos tęstinumo planas, topografijų registras neturi nuostatų, specifikacijos ir priėmimo akto; dizaino ir patentų registrai neturi specifikacijų ir priėmimo aktų. Nustatyta, kad biure neužtikrinamas išorės auditų rekomendacijų įgyvendinimas (rekomenduota panaikinti tarnybinių stočių patalpų įrengimo trūkumus, tačiau apžiūrėjus šias patalpas nustatyta, kad rekomendacijos nebuvo įgyvendintos).

<sup>10</sup> COBIT 4.1, 2011 m., Vilnius, PO6 procesas.

Optimizuojant teisingumo ministro valdymo srities IT išteklius, būtų tikslinga panaudoti VĮ Registrų centro ir Centrinės hipotekos įstaigos IT kompetenciją ir informacinių išteklių valdymo patirtį, suteikiant galimybę kitoms įstaigoms geriau naudoti šiuos išteklius ir taip užtikrinti visos ministro valdymo srities vientisą IT plėtrą ir teikiamų paslaugų kokybę.

VĮ Registrų centras tvarko ir kitų ministerijų valdomus informacinius išteklius<sup>11</sup>, todėl, nesant ministro valdymo srities bendro IT plėtros plano, kuris būtų suderintas su visų tvarkomų informacinių išteklių valdytojais, nebus tinkamai nustatyti Teisingumo ir kitų ministerijų valdomų informacinių išteklių tvarkymo prioritetai ir kryptys. Parengus bendrą strateginį dokumentą, apimantį visos ministro valdymo srities valstybės informacinių išteklių IT plėtros kryptis, būtų užtikrintas skaidrus visų IT reikalingų išteklių planavimas, tvarkymas ir kontrolė.

## 1.2. Informacinės architektūros nustatymas

Valdymo srities informacinė architektūra yra pagrindinis informacijos apie visos srities IT atitiktį vykdomos veiklos poreikiams šaltinis. COBIT metodikoje pažymėta<sup>12</sup>, kad informacinės architektūros žinojimas ir tinkamas valdymas užtikrina sklandų programinės įrangos integravimą ir vadovybės sprendimams priimti reikalingos patikimos, nuoseklios ir išsamios informacijos teikimą. Institucija, nustatydamą savo valdymo srities informacinę architektūrą, sudaro duomenų žodyną, kuriame taip pat nustatomos techninės sąlygos duomenims (kitais – duomenų sintaksė), numato duomenų klasifikavimo schemą ir saugumo lygius. Tinkamas informacinės architektūros nustatymas sudaro galimybę racionaliai išnaudoti informacinius išteklius, juos maksimaliai lanksčiai derinant su vykdomos veiklos strategija. Taip pat stiprinamas atskaitingumas už duomenų vientisumą ir saugą, didinamas duomenų mainų tarp skirtingų IS efektyvumas ir kontrolė.

Teisės aktai nustato šiuos elektroninės informacijos srautų valdymo reikalavimus:

- IS ir registrai klasifikuojami pagal el. informacijos<sup>13</sup> svarbą, o pastaroji nustatoma pagal konfidencialumo, vientisumo ir (ar) prieinamumo praradimo neigiamą įtaką valstybės, valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos, steigiančios, kuriančios ir (arba) tvarkančios valstybės registrus, žinybinius registrus, valstybės informacines sistemas ir kitas informacines sistemas, veiklai ir elektroninės informacijos svarbą valstybei, kelioms institucijoms ar institucijai<sup>14</sup>.
- IS ar registrų kategorija nustatoma pagal apdorojamos informacijos svarbos kategoriją ir nurodoma duomenų saugos nuostatuose<sup>15</sup>. Techninės apsaugos priemonės parenkamos pagal informacinių išteklių kategoriją<sup>16</sup>.

Atsižvelgus į teisingumo ministro valdymo srityje esančių valstybės informacinių išteklių įvairovę ir sudėtingą valdymo bei tvarkymo struktūrą, nustatyti ministro valdymo srities informacinę

<sup>11</sup> Finansų ministerijos valdoma IS „E. sąskaita“, Sveikatos apsaugos ministerijos valdoma Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros IS, Nacionalinė žemės tarnybos prie Žemės ūkio ministerijos valdomas Nekilnojamojo turto kadastras.

<sup>12</sup> COBIT 4.1, 2011 m., Vilnius, PO2 procesas, 33 psl.

<sup>13</sup> Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, 4 ir 5 p.

<sup>14</sup> Ten pat, 3 p.

<sup>15</sup> Ten pat, 5, 6 p.

<sup>16</sup> Lietuvos Respublikos vidaus reikalų ministro 2013-10-04 įsakymu Nr. 1V-832 patvirtinti Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, II skirsnis.

architektūrą yra ypač svarbu, siekiant tinkamai valdyti, analizuoti ir modernizuoti valdymo srityje esančias informacines technologijas ir valstybės informacinius išteklius. Išnagrinėjus ministro valdymo sričiai priskirtų įstaigų veiklos planus ir dokumentus, apibūdinančius tose įstaigose esančias IS, technologijas ir kaupiamus bei saugomus duomenis, nustatyta, kad ministerija neturi parengusi ir nesivadovauja ministro valdymo sričiai sudarytu bendroju informacinių išteklių architektūros modeliu, atitinkančiu valdymo srities sudaromiems IT plėtros planams.

Teisingumo ministerija, valdanti daug valstybės IS ir registrų ir turinti metodiškai vadovauti jų tvarkytojams bei koordinuoti šių registrų ir IS funkcionavimą<sup>17</sup>, neturi valdymo srities duomenų klasifikavimo sistemos, pagrįstos duomenų svarba ir diskretiškumu (pvz.: vieša, slapta ir pan.) ir tikslios informacijos apie ministro valdymo srityje esančių informacinių išteklių skaičių. Dėl šių priežasčių ministerijoje nėra kontrolės priemonių, padedančių užtikrinti teisės aktais nustatytą el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą.

Teisingumo ministro valdymo sričiai priskirtose įstaigose planuojamos kurti, kuriamos arba jau sukurtos IS, kuriose kaupiami svarbūs duomenys (žr. 3 pavyzdį). Apie šių informacinių išteklių vietą bei tarpusavio ir išorinius ryšius ministro valdymo srities bendroje IT architektūroje ministerija neturi informacijos: nė viena šių IS nepatenka į ministro valdymo srities IS/IT plėtros dokumentus. Teisingumo ministro valdymo sričiai priskirtos įstaigos kaupia ir tvarko automatizuotu būdu asmens ir kitus veiklai svarbius duomenis neįteisintose IS, kurių tvarkymo priežiūrą turėtų atlikti ir teisingumo ministro valdymo sričiai priklausanti Valstybinė duomenų apsaugos inspekcija.

### 3 pavyzdys

Lietuvos teismo ekspertizės centre ir Valstybinėje teismo medicinos tarnyboje nėra el. informacijos klasifikatorių, nors šiose institucijose tvarkomi kitoms institucijoms ir gyventojams svarbūs duomenys apie nukentėjusius, mirusius asmenis, saugomi serologinių, DNR, toksikologinių ir kt. tyrimų duomenys bei atliktų ekspertizių rezultatai.

Siekiant išvengti galimų informacijos viešinimo ir perdavimo problemų, su kuriomis ministerija susidūrė 2011 m., kai Baltarusijos institucijoms buvo perduoti duomenys apie šios šalies piliečio banko sąskaitas, ministerijai reikėtų nustatyti visos valdymo srities el. informacijos klasifikavimo ir apsaugos kontrolės priemones. Ministerija galėtų pritaikyti IVPK rekomenduojamą Informacinių technologinių paslaugų valdymo metodiką ir inventorizuoti visas valdymo srities IT priemones, nustatyti jų santykį su konkrečiais veiklos tikslais. Tai užtikrintų pakankamą ministerijos dėmesį visiems valdymo srities IT poreikiams.

Nustačiusi teisingumo ministro valdymo srities informacinės architektūros modelį, suklasifikavusi visus srityje valdomus ir tvarkomus duomenis pagal svarbą ir apibrėžusi jų vientisumo ir nuoseklumo principus visai valdymo sričiai, Teisingumo ministerija sukurtų aplinką, kurioje visiems be išimties informaciniams ištekliams pagal jų svarbą būtų skiriamas reikiamas dėmesys, priimant tinkamus sprendimus dėl jų plėtros, kūrimo, priežiūros ir saugos užtikrinimo.

## 1.3. Informacinių technologijų procesų, organizacinės struktūros ir ryšių apibrėžimas

Tinkama IT organizacinė struktūra nustatoma pagal organizacijos vykdomą veiklą ir aprašoma įvertinus vykdomas funkcijas ir pareigų pasiskirstymą, atskaitomybę ir priežiūrą. Vadovaudamasis

<sup>17</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 2 str. 12 ir 14 d.

IT valdymo gerąją praktiką, taikoma organizacijos veiklos ir IT veiklos suderinimui, COBIT rekomenduoja sudaryti tokią organizacinę struktūrą, kuri turėtų užtikrinti tinkamą požiūrį į IT valdymą kaip sudėtinę organizacijos valdymo dalį ir veiklos poreikių realizavimą naudojant IT. Siekiant šio tikslo gali būti sukurti: IT strategijos komitetas, skirtas konsultuoti dėl strateginės krypties pasirinkimo ir dėl svarbiausių IT investicijų, ir IT valdymo komitetas, kuris atsižvelgdamas į strateginę kryptį stebėtų IT projektų vykdymą. Nustatant IT procesus, organizacinę struktūrą ir tarpusavio ryšius, ypatingas dėmesys turi būti skiriamas veiklos kontrolei, kokybės užtikrinimui, rizikos valdymui, informacijos saugai, duomenų ir sistemų valdymui bei funkcijų atskyrimui.

Lietuvos Respublikos teisės aktai nustato šiuos valdymo reikalavimus IT organizacinei struktūrai:

- Registro ar IS valdytojas metodiškai vadovauja registro ar IS tvarkytojui ir koordinuoja jų funkcionavimą, privalo koordinuoti registro (IS) tvarkytojo ir priežiūros paslaugos teikėjo darbą, nustatyta tvarka atlikti jų veiklos priežiūrą; atlikti duomenų ir informacijos saugos reikalavimų laikymosi priežiūrą; planuoti metinį registro biudžetą, kontroliuoti jo vykdymą; nagrinėti registro (IS) tvarkytojo pasiūlymus dėl registro (IS) veiklos tobulinimo ir priimti dėl jų sprendimus; užtikrinti, kad šie išteklių būtų tvarkomi vadovaujantis teisės aktais; atlikti kitus teisės aktuose nustatytus veiksmus.<sup>18</sup>
- Registro ar valstybės IS tvarkytojas tvarko duomenis ir atsako už jų saugą.<sup>19</sup>
- Kiekvienam registrui, valstybės IS ar jos posistemiiui turi būti paskirtas duomenų valdymo įgaliotinis. Jis vadovaudamasis IT plėtros planu ir kitais institucijos planavimo dokumentais įgyvendina IS ar registro plėtrą, tiesiogiai prižiūri jų kūrimą, investicijų panaudojimą, rengia biudžeto projektus, prižiūri, kad informacija, duomenys ir jų kopijos būtų teikiami pagal teisės aktų reikalavimus, atlieka kitas teisės aktuose nustatytas funkcijas<sup>20</sup>.
- IS ar registro valdytojas teisės aktu, kuriuo tvirtinami duomenų saugos nuostatai, skiria saugos įgaliotinį, kuris koordinuoja ir prižiūri saugos politikos įgyvendinimą IS, arba paveda jį paskirti IS tvarkytojui.<sup>21</sup>
- IS ar registro valdytojas arba jo įgaliotas IS tvarkytojas turi paskirti administratorių, kuris atlieka funkcijas, susijusias su IS naudotojų teisių valdymu, IS komponentais, šių IS komponentų sąranka, IS pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėseną, reagavimu į elektroninės informacijos saugos incidentus, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su IS saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.<sup>22</sup>

Vadovaujantis Valstybės informacinių išteklių valdymo įstatymu, valstybės registro ar valstybės IS, kuria apdorojama visai valstybei arba kelioms institucijoms svarbi institucijos valdoma informacija, valdytojui pavedama strategiškai planuoti registro ar IS valdymą, žmogiškuosius ir kitus išteklius, registro metinį ir perspektyvinį biudžetus, todėl tokių išteklių valdytoju turi būti skiriamas toks juridinis asmuo, kurio vadovas yra asignavimų valdytojas.<sup>23</sup>

<sup>18</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 23, 24 ir 34 str.

<sup>19</sup> Ten pat, 24 str. 4 d ir 34 str. 4 d.

<sup>20</sup> Ten pat, 8 str.

<sup>21</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 44 str. ir Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 17 ir 22 p.

<sup>22</sup> Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 26 ir 27 p.

<sup>23</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 23 str. 2 d., 24 str. 3 d., 33 str. 2 d. ir 34 str. 4 d.

Registrų ir valstybės informacinių sistemų registro duomenimis teisingumo ministro valdymo srityje yra 13 IS ir 15 registrų, iš kurių 4 IS ir 10 registrų valdo pati ministerija (žr. 4 priedą). Kitas IS, registrus ir kadastrą valdo ministro valdymo sričiai priskirtos įstaigos, kiti asignavimų valdytojai arba jų valdymo sritims priskirtos įstaigos.

Teisingumo ministro valdymo srityje yra valstybės IS ir registrų, kurių valdytoja turėtų būti pati ministerija, kurių valdytojai yra ministerijai pavaldžios įstaigos, kurios nėra asignavimų valdytojos (žr. 4 pavyzdį). Todėl įgyvendinant Valstybės informacinių išteklių valdymo įstatymo nuostatas, ministerijai reikėtų peržiūrėti iki įstatymo įsigaliojimo priimtus teisės aktus, nustatančius ministro valdymo srities informacinių išteklių valdytojus, kad tokių informacinių išteklių valdytojai galėtų savarankiškai priimti sprendimus dėl šių išteklių biudžetų planavimo vadovaujantis Valstybės informacinių išteklių valdymo įstatymu.

#### 4 pavyzdys

Valstybinis patentų biuras, kurio vadovas nėra asignavimų valdytojas, valdo ir tvarko 2003 m. įsteigtus Patentinių patikėtinių registrą, Lietuvos Respublikos dizaino, patentų ir prekių ženklų registrus. Vartotojų teisių apsaugos tarnyba valdo ir tvarko kuriamą Vartotojų teisių informacinę sistemą. Kalėjimų departamentas valdo ir tvarko Kalėjimų departamento informacinę sistemą.

Teisingumo ministerijos valdomų valstybės registrų ir IS veiklą vadovybės lygyje kuruoja vienas iš viceministrų, o ministerijos politiką šių registrų ir IS kūrimo, veiklos ir integravimo srityje įgyvendina ministerijos Registrų departamentas. Departamentas turėtų dalyvauti, kuriant naujus ir integruojant veikiančius registrus, IS, rengti naujai steigiamų ir reorganizuojamų veikiančių registrų ir IS steigimo, reorganizavimo bei integravimo dokumentus.

Registrų departamento nuostatuose numatytos funkcijos apima dalį COBIT rekomenduojamų IT strategijos komiteto funkcijų, tačiau dėl vidinio ministerijos veiklos sričių kuravimo paskirstymo departamentas daugiausia dėmesio skiria trijų jo kuruojamų įstaigų (VĮ Registrų centro, Centrinės hipotekos įstaigos ir Valstybinės duomenų apsaugos inspekcijos) IT. Kitas teisingumo ministro valdymo sričiai priskirtas įstaigas ministerijoje kuruoja kiti departamentai, kuriems nėra pavesta rūpintis valstybės registrų ir IS kūrimo, veiklos ir integravimo politikos įgyvendinimu, todėl šių įstaigų tvarkomiems registrams skiriama nepakankamai dėmesio (žr. 5 pavyzdį).

#### 5 pavyzdys

Valstybinis patentų biuras 2013 m. birželio mėn. parengė pažymą Teisingumo ministerijai dėl šio biuro valdomų Prekių ženklų ir Dizaino registrų nuostatų pakeitimų, suderinęs juos su suinteresuotomis institucijomis, su prašymu teikti Vyriausybei. Pažymoje aptariamas registrų valdytojo ir tvarkytojo klausimas.

Diskusijoje dalyvavusių ministerijos ir Valstybinio patentų biuro darbuotojų teigimu, minėta pažyma buvo svarstyta, tačiau diskusijos rezultatas nedokumentuotas. Skirtingi ministerijos ir biuro darbuotojai šį rezultatą pristato skirtingai, todėl neaišku, kada ir kaip ministerija planuoja nuspręsti dėl valstybės registrų valdytojo ir tvarkytojo funkcijų vykdymo.

Teisingumo ministerijoje nėra valdymo struktūros, kurioje dalyvaujantys asmenys atstovautų visų ministerijos valdomų sričių IT poreikiams ir analizuotų ministerijos valdomoms valstybės IS ir registrams kylančias rizikas, jas apibendrintų, teiktų siūlymus, priimant strateginius sprendimus dėl IT plėtros prioritetų ir investicijų į šias technologijas. Nesprendžiant šių klausimų, kyla rizika, jog šiuo metu ministerijos valdomų valstybės registrų ir IS plėtra neatitiks ministerijos veiklos strateginių kryptų, liks neįteisintos ministro valdymo sričiai priskirtose institucijose kuriamos arba modernizuojamos valstybės informacinės sistemos, nebus vertinama IT teikiama nauda

ministro valdymo srityje vykdomai veiklai.

Vieną iš COBIT rekomenduojamo IT valdymo komiteto funkcijų – spręsti išteklių atitikties poreikiams klausimus – iš dalies vykdo Teisingumo ministerijos Strateginio valdymo departamento Projektų įgyvendinimo ir koordinavimo skyrius. Jis, atsižvelgęs į teisingumo ministro valdymo sričiai priskirtų įstaigų IT poreikį, organizuoja kompiuterinės technikos skirstymą. Nepaisant to, ministerijoje nėra ministro valdymo srities įstaigų IT pokyčių centralizuoto valdymo. COBIT rekomenduoja sukurti tokią IT organizacinę struktūrą, kuri turėtų įgaliojimus ir kompetenciją priimti sprendimus dėl visų valdymo srities veiklos IT poreikių.

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

Taip pat ministerijoje ir ministro valdymo srityje yra trūkumų nustatant ir įgyvendinant duomenų valdymo, IT saugos ir priežiūros atsakomybes: ji neturi struktūros, kuri būtų atsakinga už IT saugą, pavaldžių institucijų IT saugos ministerijoje taip pat niekas nekuruoja; paskirti ne visų ministerijai pavaldžių institucijų duomenų valdymo ir saugos įgaliotiniai, nepaisant to, kad įstaigos tvarko ir saugo svarbius duomenis. Dėl šių priežasčių tokių informacinių išteklių plėtos, saugos politikos įgyvendinimo nekoordinuoja ir nekontroliuoja ne tik ministerija, bet šios galimybės neturi ir įstaigų vadovai (6 pavyzdys).

#### 6 pavyzdys

Audito metu ministerija nurodė, kad IT sauga rūpinasi Strateginio valdymo departamento Projektų įgyvendinimo ir koordinavimo skyrius. Išnagrinėjus funkcijas ir vykdytas veiklas, nustatyta, kad šis skyrius neturi nieko bendra su IT saugos užtikrinimu. Kai kuriose ministerijai pavaldžiose įstaigose IT aptarnauja ne IT specialistai, o darbuotojai, kurie savanoriškai domisi IT sritimi:

Lietuvos teisės institute IT prižiūri jaunesnysis mokslo darbuotojas, kurio pagrindinė funkcija – rašyti mokslinius straipsnius. Europos teisės departamente IT prižiūri darbuotojas, kurio pagrindinės funkcijos yra viešųjų pirkimų organizavimas ir departamento ūkio priežiūros organizavimas. Atliekant darbus, reikalaujančius didesnės IT srities išmanymo, kviečiami specialistai iš kitų įstaigų.

Valstybinėje vartotojų teisių apsaugos tarnyboje už veiklos tęstinumą, IS atstatymą ir saugą atsakinga trečioji šalis, bet nėra darbuotojo, kuris būtų atsakingas už šios srities priežiūrą ar veiklų koordinavimą, nėra IS atliekamų veiksmų darbo vietose atsekamumo.

Siekdama užtikrinti sistemingą valdymo srities informacinių išteklių plėtrą ir jų saugos užtikrinimą, ministerija turėtų nustatyti už duomenų ir informacijos saugos reikalavimų laikymąsi atsakingus asmenis, koordinuoti šių veiklų vykdymą ir vykdyti jų priežiūrą.

## 1.4. Informacinių technologijų investicijų valdymas

Norint geriausiai išnaudoti IT ir gauti iš jų daugiausiai naudos vykdant numatytą veiklą, būtina skirti reikiamą dėmesį rezultatyviems ir efektyviems IT investicijų sprendimams. COBIT rekomenduoja<sup>24</sup> sudarant IT biudžetą naudoti kiekybinius ar kokybinius investavimo kriterijus, o

<sup>24</sup> COBIT 4.1, 2011 m., Vilnius, PO5 procesas.



vertinant veiklą ir lyginti gautą veiklos vertės įvertinimą su planuojama gauti verte. Šiam tikslui turėtų būti sukurta ir taikoma IT turto ir paslaugų finansinio valdymo sistema, kuri padėtų sudaryti IT biudžetą, valdyti IT sąnaudas ir stebėti IT indėlį į vykdomą veiklą.

Teisingumo ministerijoje yra patvirtinti<sup>25</sup> ministro valdymo sričių investicijų projektų atrankos bendrieji ir specialieji kriterijai ir jų reikšmės. IT plėtrai nustatytas vienas atrankos kriterijus – IS kategorija – ir jis taikomas atrenkant investicijų projektus (žr. 7 pavyzdį).

### 7 pavyzdys

Investicijų projektų atrankos kriterijui „*investicijų projektas IT, valstybės IS, valstybės ir žinybiniam registrams modernizuoti ir plėtoti*“ numatytos tokios reikšmės:

30 balų suteikiama, jei investicijų projektu siekiama kurti arba modernizuoti pirmos kategorijos IS. 20 balų, jei – antros kategorijos IS. 15 balų, jei – trečios kategorijos IS. 10 balų, jei – ketvirtos kategorijos IS. 5 balai suteikiami, jei investicijų projektas skirtas IT įrangai įsigyti ar plėtoti, arba investicijų projektas skirtas valstybės ir žinybiniam registrams modernizuoti.

Iš pavyzdžio matyti, kad atrankos kriterijai informacinėms sistemoms ir registrams taikomi netinkamai. Valstybės registrams tenkanti kriterijaus reikšmė yra mažesnė už žemiausios kategorijos IS skiriamą reikšmę, dėl to valstybės registrų plėtrai ir modernizavimui gali būti skiriamas nepakankamas dėmesys.

Investicinius projektus svarsto ir jų atitiktį kriterijams vertina ministerijos investicijų projektų atrankos ir įgyvendinimo koordinavimo komisija. Išanalizavus komisijos posėdžių protokolus ir ministro įsakymais patvirtintas investicijų projektų įgyvendinimo programas, nustatyta, kad didžiausias dėmesys skiriamas toms sritims, kurioms tenka valstybės biudžeto lėšos. IT investicijų projektai, finansuojami iš kitų šaltinių (pvz., ES finansinės paramos) sulaukia mažai komisijos dėmesio. Pažymėtina, kad Teisingumo ministerijoje sukurta investicijų planavimo ir skyrimo sistema, tačiau ji nėra pakankamai efektyvi sprendžiant IT investicijų klausimus. Nepakankamas ministerijos dėmesys IT investicijoms ministro valdymo srityje esančiose įstaigose silpnina ministerijos vykdomą IT biudžetų kontrolę.

Sąlygas nuosekliam ir skaidriam IT investicijų valdymui ministro valdymo srityje galėtų sudaryti IT turto bei paslaugų investicijų valdymui skirta metodika, kuri apimtų IT išlaidas, naudą, biudžeto prioritetus, patvirtintą biudžeto sudarymo procesą, IT sąnaudų ir naudos kontrolę ir korekcinį veiksmų inicijavimą.

## 1.5. Projektų valdymas ir informacinių išteklių kūrimas

COBIT projektų valdymo procesas<sup>26</sup> nurodo, jog organizacijoje turėtų būti įdiegta programų ir projektų valdymo sistema, užtikrinanti tinkamą projektų prioritetų nustatymą ir koordinavimą ir apimanti visus IT projektus. Siekiant užtikrinti, kad IT projektai kurtų vertę veiklai, o jų rizikos būtų valdomos, sistema turi apimti bendrąjį planą, išteklių paskirstymą, laukiamų rezultatų apibrėžimą, naudotojų pritarimą, įgyvendinimo etapais metodą, kokybės užtikrinimą, formaliai patvirtintą testavimo planą ir testavimo ir įdiegtos sistemos analizę. Toks metodas sumažina nenumatytų sąnaudų ir projektų nutraukimo riziką, gerina ryšius su veiklos atstovais ir galutiniais

<sup>25</sup> Lietuvos Respublikos teisingumo ministro 2012-11-20 įsakymas Nr.1R-289.

<sup>26</sup> COBIT 4.1, 2011 m., Vilnius, PO10 procesas, 67 psl.

naudotojais ir jų įsitraukimą, užtikrina projekto rezultatų sukuriama vertę ir kokybę ir labai padidina jų indėlį į IT investicijų programas.

Kuriant IS, projekto rengimo stadijoje turi būti sudarytas IS projektinis modelis, išanalizuoti IS realizavimo variantai ir pasirinktas vienas, ekonomiškai, techniškai ir socialiai pagrįstas, parengtos IS komponentų specifikacijos, parengtas ir kompiuterizuojamo objekto vadovybės patvirtintas IS projekto aprašas<sup>27</sup>.

Už projektų valdymą Teisingumo ministerijoje atsakingas Projektų įgyvendinimo ir koordinavimo skyrius, kurio viena iš funkcijų – koordinuoti teisingumo ministro valdymo srities įstaigų vykdomus investicijų projektus, ministerija skiria nepakankamą dėmesį valdymo srityje vykdomiems IT/IS projektams ir neužtikrina visų projektų vykdymo stebėsenos. Pastebėtina, kad ministerija ir jai pavaldžios įstaigos neturi patvirtintos bendros projektų valdymo metodikos, todėl IT projektų valdymas įstaigose vykdomas nesistemiškai.

Plėtojant nuoseklius projektų valdymo ir įgyvendinimo procesus ministerijai būtų tikslinga naudoti integruotas projektų valdymo priemones, panaudoti pavaldžių įstaigų turimą patirtį ir sprendimus.

Vykdamas informacinių išteklių kūrimo projektus, teisės aktai numato šias kontrolės priemones:

- IS valdytojas, steigdamas IS, parengtą jos nuostatų projektą derina su IVPK, Vidaus reikalų ministerija ir institucijomis, kurios nuostatų projekte nurodytos kaip duomenų teikėjos.<sup>28</sup> IS laikoma įsteigta nuo jos nuostatų patvirtinimo<sup>29</sup>.
- Patvirtinus nuostatus, rengiama IS specifikacija<sup>30</sup>, o IS kuriama ir diegiama pagal patvirtintą specifikaciją<sup>31</sup>.
- Baigus diegti IS arba jos dalį (komponentę, posistemę), sistemos valdytojo vadovas tvirtina IS priėmimo ir tinkamumo eksploatuoti aktą<sup>32</sup>. Naudojama tik įteisinta valstybės IS ar jos posistemis<sup>33</sup>.

Audito metu nagrinėtas Kalėjų departamento IS kūrimas. Kalėjų departamento IS (KADIS) skirta užtikrinti departamento, jam pavaldžių įstaigų ir valstybės įmonių prie pataisos įstaigų vykdomos veiklos duomenų surinkimą, kaupimą, apdorojimą ir rezultatų pateikimą bei

<sup>27</sup> Valstybės informacinių sistemų kūrimo metodikos, patvirtintos Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-10-15 įsakymu Nr. T-131 „Dėl valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“, 24.2-24.5 ir 29 p. Nuo 2014-02-25 Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29, 19, 26 ir 27 p.

<sup>28</sup> Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (neteko galios 2013-02-27 nutarimu Nr. 180), 5 p., Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, 8 p.

<sup>29</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas 2011-12-15, Nr. XI-1807, 30 str. 4 d., Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (neteko galios 2013-02-27 nutarimu Nr. 180), 9 p., Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, 12 p.

<sup>30</sup> Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (neteko galios 2013-02-27 nutarimu Nr. 180), 10 p., Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, 23 p.

<sup>31</sup> Ten pat, 14 ir 29 p.

<sup>32</sup> Ten pat, 16 ir 30 p.

<sup>33</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas 2011-12-15, Nr. XI-1807, 31 str. 6 d. Iki įstatymo įsigaliojimo (2012-01-01) buvo reikalavimas, kad „duomenys kitoms institucijoms kompiuteriniu būdu gali būti teikiami tik iš įteisintų IS.“ (Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (neteko galios 2013-02-27 nutarimu Nr. 180), 22 p.).

perdavimą laiku, išsamiai ir kokybiškai. Ši IS pradėta kurti 2006 m., joje kaupiami ir tvarkomi duomenys apie suimtąjį (nuteistąjį) ir jo sveikatos priežiūrą, duomenys apie pataisos inspekcijų įskaitoje esančius nuteistuosius, departamentui pavaldžių įstaigų nuteistųjų darbinės veiklos rodiklius, departamentui pavaldžių įstaigų etatus, valstybės tarnautojų ir darbuotojų skaičių ir darbo užmokestį, departamentui pavaldžių įstaigų metinę ir ketvirtinę finansinę atskaitomybę, vidaus tyrimų tarnybų ir apsaugos ir priežiūros tarnybų duomenys apie vykdytas veiklas ir patikrinimų rezultatus ir kt. KADIS valdytojas ir tvarkytojas yra Kalėjimų departamentas.

Nustatyta, kad departamentas kurdamas IS nesivadovauja IS kūrimo tvarka – nepatvirtino privalomos dokumentacijos, kaupia jautrius duomenis apie asmenis ir teikia duomenis kitoms institucijoms iš neįteisintos ir nebaigtos kurti IS. Departamentas IS kuria panaudodamas finansavimo šaltinius, kurių kontrolės nevykdo IVPK, todėl prieš skiriant lėšas nebuvo įvertintas tokių IT sprendimų poreikis ir techninis suderinamumas valstybės mastu (8 pavyzdys).

### 8 pavyzdys

Kalėjimų departamento IS (KADIS) nėra įteisinta (nėra priėmimo ir tinkamumo eksploatuoti akto), neparengta IS specifikacija ir duomenų saugos nuostatai, nors atskiri KADIS moduliai veikia ir ši sistema yra naudojama įstaigos veikloje. KADIS nuostatai neatnaujinti nuo jų sukūrimo 2006 m., nors 2010–2013 m. vykdytas šios IS tobulinimo projektas įdiegiant KADIS-1 IS. Projektas finansuotas pagal 2007–2013 m. Žmogiškųjų išteklių plėtros veiksmų programos 4 prioriteto „Administracinių gebėjimų stiprinimas ir viešojo administravimo efektyvumo didinimas“ įgyvendinimo priemonę „Viešojo administravimo subjektų sistemos tobulinimas“, biudžetas 2 244 tūkst. Lt.

Europos ekonominės erdvės ir Norvegijos paramos 2004–2009 m. lėšomis (5 784 tūkst. Lt) 2008–2010 m. vykdytas projektas, kurio metu sukurta IS PRISONIS. Ši IS skirta keisti duomenimis tarp Kalėjimų departamentui pavaldžių įstaigų ir teikti el. informaciją kitoms institucijoms, bet ji nebuvo įsteigta, įteisinta ir neparengti IS dokumentai. Joje naudojami asmens duomenys, bet departamentas nėra įsiregistravęs Asmens duomenų valdytojų registre, todėl neužtikrinamos tinkamos techninės ir organizacinės priemonės, apsaugančios nuo bet kokio neteisėto asmens duomenų tvarkymo.

Departamente saugos, strategijų ir kitų dokumentų parengimas siejasi su KADIS įteisinimu, tačiau iki šio audito pradžios nebuvo jokio postūmio – neatliekama informacinių sistemų vidaus kontrolės stebėseną ir vertinimą, neparengti saugos politiką įgyvendinantys dokumentai, duomenų archyvavimo / atsarginių kopijų darymo tvarka ir veiklos tęstinumo planai. Audito metu departamente buvo atlikta informacinių technologijų esamos būklės analizė.

Rengiant IS dokumentaciją po IS sukūrimo, nėra galimybės užtikrinti, kad sukonstruota IS tenkins veiklos poreikius ir bus suderinama su kitomis IS valstybės mastu, o šios dokumentacijos rengimas tampa tik formalumu. Kalėjimų departamentas nevykdo Valstybės informacinių išteklių valdymo įstatyme<sup>34</sup> ir kituose teisės aktuose nustatytų privalomų reikalavimų kuriant IS, todėl neužtikrina reikiamo KADIS duomenų tvarkymo, naudojimo ir saugos.

Ministerijai vertėtų atlikti ministro valdymo srities informacinių išteklių atitikties teisės aktams auditą, inventorizuoti visus informacinius išteklius ir, siekiant užtikrinti vykdomų IT projektų valdymo kokybę, patvirtinti bendrusius ministerijos IT projektų valdymo principus.

<sup>34</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 11 str. 2 d.

## 1.6. Informacinių sistemų ir registų saugos užtikrinimas

COBIT informacinių sistemų saugos užtikrinimo procesas<sup>35</sup> skirtas išlaikyti informacijos vientisumą ir išsaugoti turtą. Jis apima IT saugos funkcijas ir atsakomybę, politiką, standartų ir procedūrų nustatymą ir priežiūrą. Tinkamai valdomas IS saugos užtikrinimo procesas garantuoja ne tik IT saugą, jis sumažina galimų IT saugos incidentų poveikį pagrindinei įstaigos veiklai.

Norint įvertinti saugos poreikį ir skirti IS tinkamas saugos priemones, reikia taikyti teisės aktų nustatytą valstybės IS klasifikavimą pagal kategorijas<sup>36</sup> nuo pirmos (aukščiausiosios) iki ketvirtos (žemiausiosios). Kategorija nustatoma IS duomenų saugos nuostatuose<sup>37</sup>.

Lietuvos Respublikos teisės aktai nustato šiuos sistemų saugos užtikrinimo reikalavimus:

- IS ir registro valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus<sup>38</sup>:
  - Saugos nuostatus;
  - Saugaus elektroninės informacijos tvarkymo taisykles;
  - Informacinės sistemos veiklos tęstinumo valdymo planą;
  - Informacinės sistemos naudotojų administravimo taisykles.
- Saugos įgaliotinis turi kasmet organizuoti visų informacinių sistemų rizikos vertinimą<sup>39</sup> ir periodiškai organizuoti IS naudotojų mokymą elektroninės informacijos saugos klausimais<sup>40</sup>;
- Administratorius atlikdamas informacinės sistemos sąrankos pakeitimus, turi laikytis informacinės sistemos valdytojo nustatytos IS pokyčių valdymo tvarkos, nustatytos Saugaus elektroninės informacijos tvarkymo taisyklėse<sup>41</sup>.

Įvertinus Teisingumo ministerijos valdomų registų ir IS saugą, nustatyta saugos reikalavimų trūkumų:

- nesuderinti su Vidaus reikalų ministerija ir nepatvirtinti vieno registro ir keturių naudojamų IS duomenų saugos nuostatai (žr. 4 priedą);
- nėra nustatyta tvarka suderintų su atsakingomis institucijomis ir patvirtintų kadastro ir šešių IS saugos politiką įgyvendinančių dokumentų – Veiklos tęstinumo valdymo plano, Naudotojų administravimo taisyklių, Saugaus elektroninės informacijos tvarkymo taisyklių (žr. 4 priedą);
- rizikos vertinimas buvo atliekamas VĮ Registų centre, Centrinėje hipotekos įstaigoje ir Valstybiniame patentų biure, o Teisingumo ministerijoje ir kitose pavaldžiose įstaigose toks vertinimas kasmet neatliktas, ministerijoje neorganizuojami mokymai el. informacijos saugos klausimais.

Taip pat nustatyta, kad ministerijoje nėra IT saugos klausimus sprendžiančios struktūros, kurią sudarytų svarbiausių veiklos sričių atstovai: pagrindinių ministerijos veiklų, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito. Nustatyta ir kitų saugos procedūrų trūkumų – ministerijoje ir kai kuriose jai pavaldžiose įstaigose<sup>42</sup> neužtikrinamas IS ir kompiuterizuotose darbo vietose atliktų

<sup>35</sup> COBIT 4.1, 2011, Vilnius, DS5 procesas, 117 psl.

<sup>36</sup> Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Valstybės informacinių sistemų, registų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, 5 p.

<sup>37</sup> Ten pat, 6 p.

<sup>38</sup> Ten pat, 7 p.

<sup>39</sup> Ten pat, 35 p.

<sup>40</sup> Ten pat, 25 p.

<sup>41</sup> Ten pat, 28 p.

<sup>42</sup> Lietuvos teismo ekspertizės centre, Centrinėje hipotekos įstaigoje, Valstybės garantuojamos teisinės pagalbos tarnyboje (Vilniaus skyriuje), Valstybėje teismo medicinos tarnyboje ir Valstybiniame patentų biure.

veiksmų atsekamumas, nenustatyti svarbiausi (kritiniai) IT procesai ir išteklių, todėl neužtikrinamas tvarkomų duomenų patikimumas ir jų apsauga.

Vertinant saugos priemones valstybės registrus tvarkančiuose VĮ Registrų centre, Centrinėje hipotekos įstaigoje ir Valstybiniame patentų biure, esminių rizikų dėl netinkamo saugos planavimo ir valdymo nenustatyta. Audito metu nustatyta geroji praktika teisingumo ministro valdymo sričiai priskirtoje institucijoje: Centrinė hipotekos įstaiga 2013 m. įdiegė kolektyvinės apsaugos nuo grėsmių iš viešųjų tinklų sistemą „Kolektyvinis kibernetinis skėtis“ ir dalyvavo kibernetinėse pratybose „X1306“, kurias organizavo Lietuvos Respublikos ryšių reguliavimo tarnybos Incidentų tyrimo padalinys CERT-LT. Pratybų ataskaitoje konstatuota, kad beveik visas užduotis įstaiga vykdė greičiausiai.

Ministerija turėtų užtikrinti valdymo srities informacinių išteklių apsaugą, įgyvendindama teisės aktų reikalavimus ir pašalindama kitus IT saugos trūkumus (žr. 3 priedą).

## 1.7. Vidaus kontrolės stebėseną ir vertinimą, atitiktį išoriniams reikalavimams užtikrinimas

COBIT vidaus kontrolės stebėsenos ir vertinimo procesas<sup>43</sup> nurodo, jog efektyviam IT veiklos valdymui reikalinga nustatyti tinkamus veiklos rodiklius, sistemingai ir laiku atlikti veiklos stebėseną ir operatyviai reaguoti, esant nuokrypių. Stebėseną reikalinga siekiant užtikrinti, kad būtų taikomos tinkamos ir nustatytas kryptis ir politiką atitinkančios priemonės. Rekomenduojama vertinti nuolat visus IS procesus ir jų atitiktį vidaus kontrolės reikalavimams. Vertinimas turėtų apimti efektyvumo valdymą, vidaus kontrolės sistemos stebėsimą, atitiktį teisinio reguliavimo ir valdymo reikalavimams.

Lietuvos Respublikos teisės aktai nustato, kad:

- vienas vidaus audito uždavinių – ne rečiau kaip vieną kartą per trejus metus įvertinti, kaip vidaus kontrolė veikia viešajame juridiniame asmenyje;<sup>44</sup>
- vertinant valstybės IS, kuriomis apdorojama visai valstybei svarbi institucijos valdoma informacija, ir pagrindinių valstybės registrų, taip pat valstybės IS ir registrų, kuriems kurti ar modernizuoti viršytas 1 mln. Lt<sup>45</sup>, valdymą ir saugą, ne rečiau kaip kartą per 3 metus turi būti atliekamas IT auditas;<sup>46</sup>
- kartą per dvejus metus turi būti atliekamas informacinių sistemų saugos atitiktį vertinimas, antros kategorijos IS – ne rečiau kaip kartą per metus, pirmos kategorijos IS – ne rečiau kaip kartą per 3 metus atitiktį vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti IS auditoriai<sup>47</sup>.

Per 2010–2013 m. laikotarpį Teisingumo ministerijos Centralizuotas vidaus audito skyrius neatliko nė vieno audito, kurio objektas būtų informacinės sistemos, jų saugos, bendrosios kontrolės ar kito IS/IT aspekto vertinimas, todėl ministerijos vadovybė neturi duomenų apie IT procesų efektyvumą, atitiktį veiklos reikalavimams, nenustatomos IT kontrolės spragos. Teisingumo ministro valdymo srityje buvo atliekami išoriniai IT valdymo ir saugos auditai, tačiau

<sup>43</sup> COBIT 4.1, 2011 m., Vilnius, ME2 procesas, 157 psl.

<sup>44</sup> 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.

<sup>45</sup> Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimas Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 1,2 p.

<sup>46</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 14 str. 1 d.

<sup>47</sup> Lietuvos Respublikos vidaus reikalų ministro 2008-10-27 įsakymas Nr. 1V-384, 4.1 p., neteko galios 2013-10-11. Vidaus reikalų ministro 2013-10-04 įsakymas Nr. 1V-832, 5.1, 7.2 ir 8.2 p.

ne visos įstaigos įgyvendina pateiktas rekomendacijas (žr. 2 pavyzdį, 10 psl.).

IS saugos atitikties vertinimas ministerijai pavaldžiose įstaigose atliekamas pagal teisės aktų reikalavimus, išskyrus Kalėjų departamentą ir Valstybinę teismo medicinos tarnybą, kurie valdo ir tvarko valstybės IS, jas neįteisinę ir neparengę saugos politikos dokumentų.

Teisingumo ministerijoje (ir nė vienoje pavaldžioje įstaigoje) nėra procedūros, užtikrinančios atitiktį išoriniams reikalavimams, kuri padėtų sumažinti neatitikimus su teisės aktais, padidintų personalo supratimą apie IS valdymo reikalavimus, didintų įstaigos veiklos efektyvumą.

## 2. INFORMACINIŲ TECHNOLOGIJŲ VALDYMO IR INFORMACINIŲ SISTEMŲ VIDAUS KONTROLĖS BRANDOS ĮVERTINIMAS

COBIT IT valdymo užtikrinimo procesas<sup>48</sup> nurodo, kad, siekiant sukurti rezultatyvią IT valdymo sistemą, kad organizacija investuotų į IT pagal organizacijos strategiją ir tikslus, reikia tinkamai apibrėžti organizacijos struktūras, procesus, vadovavimą, funkcijas ir pareigas.

Lietuvos Respublikos teisės aktai nustato šiuos IT valdymo užtikrinimo proceso reikalavimus:

- valdant informacines technologijas (jų sąranką, jų pakeitimus, veiklos tęstinumą, veiklos sutrikimus ir kitus procesus) rekomenduojama<sup>49</sup> atsižvelgti į IT paslaugų valdymo metodinius dokumentus<sup>50</sup>, parengtus atsižvelgiant į visuotinai pripažintus nacionalinius ir tarptautinius IT standartus ar kitus jiems prilygintus dokumentus;
- perduodant techninės ir programinės įrangos priežiūros ir duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymo funkcijas, rekomenduojama vadovautis visuotinai pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais<sup>51</sup>;
- organizuojant visų valstybės informacinių išteklių saugą, rekomenduojama vadovautis pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais.<sup>52</sup> Institucija valdanti pirmos kategorijos IS, turi įgyvendinti Lietuvos standarte LST ISO/IEC 27002:2009 nurodytas saugos priemones, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, IS ar naudojamos IS techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2006 nurodytus reikalavimus informacijos saugumo valdymo sistemai<sup>53</sup>.

<sup>48</sup> COBIT 4.1, 2011 m., Vilnius, ME4 procesas, 165 psl.

<sup>49</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 13 str.

<sup>50</sup> Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos 2013-06-19 įsakymu Nr. T-83 patvirtinta Informacinių technologijų paslaugų valdymo metodika. Metodika parengta remiantis tarptautiniu standartu ISO/IEC 20000 keliama reikalavimais bei ITIL (angl. *Information Technology Infrastructure Library*) metodikomis, paremtomis geriausia pasauline patirtimi, kaip efektyviai valdyti ir teikti IT paslaugas.

<sup>51</sup> Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 41 str. 3 d.

<sup>52</sup> Lietuvos standartais LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 43 str. 2 d. ir Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtinto Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 6 p.

<sup>53</sup> Lietuvos Respublikos vidaus reikalų ministro 2008-10-27 įsakymu Nr. 1V-384 patvirtinti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimai, 6.2 p. Nuo 2013-10-11 2013-10-04 vidaus reikalų ministro įsakymu Nr. 1V-832 patvirtinti Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, 8.3 p.

Ministerija ir kai kurios jai pavaldžios įstaigos įsidiegė ir sertifikavo veiklos valdymo standartus atitinkančias vadybos sistemas, tačiau jos neintegruotos su IT procesais (neapima visų IT veiklų). Ministerija ir jai pavaldžios įstaigos pagrindinius veiklos tikslus įgyvendina naudodamos IT sprendimus, todėl, vertinant vykdomų IT procesų kokybę, būtų galimybė nustatyti tobulintinas IT sritis ir sukurti efektyvesnę sistemą (žr. 9 pavyzdį).

## 9 pavyzdys

Ministerijoje 2011 m. įdiegta ir sertifikuota LST EN ISO 9001:2008 standarto<sup>54</sup> reikalavimus atitinkanti kokybės vadybos sistema (sertifikatas galioja iki 2014-12-11), patvirtintas kokybės vadovas, kuriuo vadovaujantis organizuojamas kasmetinis ministerijos vidinės IT infrastruktūros funkcionalumo įvertinimas – vykdoma vidinė ministerijos darbuotojų apklausa dėl pasitenkinimo IT infrastruktūra.

Valstybinėje vartotojų teisių apsaugos tarnyboje įdiegtas LST EN ISO 9001:2008 9001 standartas (sertifikatas galioja iki 2017-07-06) apimantis valstybės politikos įgyvendinimą vartotojų teisių apsaugos srityje ir vartotojų teisių apsaugą. Standartas netaikomas tarnybos IT ir IS procesams.

Valstybinėje teismo ekspertizės tarnyboje įdiegtas LST EN ISO/IEC 17025:2005 standartas<sup>55</sup>. Pagal šį tarptautinį standartą įdiegta ir akredituota vadybos sistema, kuri taip pat atitinka ISO 9001 standarto principus. Standartas apima techninės kompetencijos reikalavimus, taikomus darant tyrimus ir bandymus ir nėra susietas su tarnybos IT/IS procesais.

Kalėjų departamente diegiama projektų (ir IT) valdymo sistema, atitinkanti tarptautinio standarto LST ISO 21500:2012 reikalavimus projektų valdymui / vadybai.

Teisingumo ministro valdymo srityje nėra bendros IT valdymo sistemos, nesivadovaujama rekomenduojamais IT paslaugų valdymo standartais. Kiekviena ministerijai pavaldi įstaiga savarankiškai nusistato IT valdymo principus, kryptis ir parenka saugos priemones. IT valdymo struktūra ministerijoje nustatyta (1.3 skyrius), tačiau pavaldžių įstaigų IT kūrimas ir plėtra nekoordinuojami, pvz., IS plėtra ir kūrimas Kalėjų departamente ir Valstybinėje teismo medicinos tarnyboje vykdomi savarankiškai.

Teisingumo ministerijai pavaldžios įstaigos, tvarkančios pirmos kategorijos IS (registrus), įgyvendina teisės aktais nurodytų standartų reikalavimus informacijos saugumo valdymo sistemoms. Įvertinus Centrinės hipotekos įstaigos tvarkomų IS būklę, buvo nustatyta, kad įdiegtos visos standarto LST ISO/IEC 27002:2009 reikalaujamos ir pagal IS veiklos pobūdį būtinos informacijos saugos valdymo priemonės.

Ministerijos IS vidaus kontrolės branda įvertinta taikant Gebos brandos modelį (angl. *Capability Maturity Model, CMM*). Siekiant atspindėti realią teisingumo ministro valdymo srities IT valdymo brandą ministerijos IT valdymo procesai palyginti, su juos atitinkančių teisės aktų reikalavimų, standartų ir IT valdymo praktikų visuma, nustatytas bendras ministerijos IS vidaus kontrolės brandos lygis (IS brandos vertinimo kriterijai pateikti 5 priede). Atsižvelgiant į ataskaitoje pateiktus faktus, įvardytas IT valdymo spragas, nustatyta, kad Teisingumo ministerijos IS vidaus kontrolės branda apibrėžiama kaip Pirminis / *Ad Hoc* procesas (žr. 3 pav.).

<sup>54</sup> Lietuvos standartas LST EN ISO 9001:2008 (LST EN ISO 9001:2008) Kokybės vadybos sistemos. Reikalavimai (ISO 9001:2008).

<sup>55</sup> Lietuvos standartas LST EN ISO/IEC 17025:2005 Tyrimų, bandymų ir kalibravimo laboratorijų kompetencijai keliami bendrieji reikalavimai.

**3 pav.** Teisingumo ministerijos IS vidaus kontrolės brandos lygis

	(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
- ⚠ – ne visiškai atitinka kriterijų
- ✓ – atitinka kriterijų
- ◆ – nepasiektas tam tikras gebėjimų brandos lygis
- ▲ – nevisiškai pasiektas tam tikras gebėjimų brandos lygis
- – pasiektas tam tikras gebėjimų 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

**Teisingumo ministerijos nuomonė**

Nediferencijuotas visų teisingumo ministro valdymo srityje esančių valstybės IT (registrų, valstybės informacinių sistemų, kurių valdytoja yra Teisingumo ministerija, ir tų registrų bei valstybės informacinių sistemų, kurių Teisingumo ministerija nėra valdytoja) vidaus kontrolės brandos vertinimas nėra tikslus ir valstybinio audito rezultatai neatspindi realios situacijos šios ministerijos valstybės IT valdymo srityje. Teisingumo ministerija, nebūdama valdytoja, pagal Valstybės informacinių išteklių valdymo įstatymą neturi atitinkamo teisinio pagrindo ir teisinių valdymo bei vidaus kontrolės instrumentų jos valdymo srityje esančių registrų ir valstybės informacinių sistemų valdytojų atžvilgiu. Pažymėtina, kad tais atvejais, kai registrų arba valstybės informacinių sistemų valdytoja yra Teisingumo ministerija, valstybės IT valdymo trūkumai yra neesminiai, visi reikalingi teisės aktai yra priimti ir vidaus kontrolės branda, manytina, jog yra aukštesnė nei 2 lygio.

Nors Teisingumo ministerija turėtų formuoti valstybės politiką registrų ir ministro valdymo sričiai priskirtų informacinių sistemų veiklos srityse, organizuoti, koordinuoti ir kontroliuoti šios valstybės politikos įgyvendinimą, audituojamu laikotarpiu ministerija nesiėmė priemonių, kurios užtikrintų rezultatyvią teisingumo ministro valdymo srities IT valdymo sistemą ir pašalintų neatitiktis teisės aktams (3 priedas).

Teisingumo ministro valdymo srityje IT kontrolės aplinka neužtikrina IT tikslų ir krypties komunikacijos, ministerija investuoja į IT vadovaudamasi bendrąja organizacijos strategija ir tikslais. Siekiant investicijų efektyvumo, veiklos poreikių ir IT teikiamų galimybių, derinimą vertėtų stiprinti: sukurti organizacinę struktūrą (komitetą, komisiją ar darbo grupę), sudarytą iš veiklos procesų vadovų ir IT atstovų, kuri išskirtinai svarstyti galimybes geriau panaudoti IT, siekiant automatizuoti veiklos procesus.

Norint pasiekti aukštesnį negu Pirminį / Ad Hoc brandos lygį, ministerijoje turėtų būti sudaryta IT strategijos ir IT valdymo komitetų funkcijoms atlikti pasirinkta ministerijos organizacinė struktūra, turi būti užtikrinta, kad dalyvaus vadovybės ir pagrindinės veiklos atstovai ir bus tinkamai sprendžiami IT srities klausimai. Informacinių išteklių 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 stebėseną.

Informacinių sistemų ir infrastruktūros audito departamento  
direktorius

Dainius Jakimavičius

Audito plėtros departamento  
Strateginio planavimo ir analizės skyriaus  
vyriausiasis valstybinis auditorius

Darius Žalalis

Valstybinio audito ataskaitos kopijos pateiktos:

Lietuvos Respublikos Seimo Audito komitetui, 1 egz.

Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komitetui, 1 egz.

---

Auditas atliktas, vykdant 2013-09-16 pavedimą Nr. P-90-2

Auditą atliko valstybinių auditorių grupė:

Darius Žalalis (grupės vadovas)

Algirdas Šakys (iki 2014-03-17)

## PRIEDAI

Valstybinio audito ataskaitos  
„Valstybės informacinių išteklių  
valdymas Teisingumo ministerijoje“  
1 priedas

### Audito apimtis ir metodai

Audito objektas – Teisingumo ministerijos informaciniai ištekliai.

Audito subjektas – Lietuvos Respublikos teisingumo ministerija.

Audito tikslas – įvertinti Teisingumo ministerijos informacinių išteklių valdymą.

Vertinimo kriterijai: Teisingumo ministerijos informacinių išteklių valdymas įvertintas taikant Gebos brandos modelį (5 priedas). IS valdymo ir saugos užtikrinimo organizavimą vertinome naudodami IT valdymo metodiką COBIT<sup>56</sup>, kuri apibrėžia 34 procesus, kurie suskirstomi į 4 grupes. Atrinkus svarbiausius Teisingumo ministerijos veiklos procesus ir atlikus preliminarų rizikos vertinimą, detaliai bendrosios kontrolės vertinimui buvo pasirinkta 10 su jais susijusių COBIT apibrėžtų IT procesų, kuriuos analizavome detaliau. Tai Planavimo ir organizavimo grupės (PO) procesai (PO1, PO2, PO4, PO5, PO6), Teikimo ir palaikymo grupės (DS) procesas (DS5) ir Stebėsenos ir vertinimo (ME) grupės procesai (ME2 ir ME4). IS kūrimo kontrolei buvo pasirinkta Kalėjimų departamento informacinė sistema (KADIS) atsižvelgus į šias nustatytas rizikas: patvirtintos KADIS projektinės dokumentacijos trūkumas, nenustatyta tvarkomų duomenų svarba. Kūrimo kontrolė buvo vertinama pagal šiuos COBIT procesus: PO10 ir ME3.

Audituojamas laikotarpis: nuo 2010 iki 2013 m.

### Pagrindiniai duomenų rinkimo ir vertinimo metodai

Eil. Nr.	Metodas	Tikslai
1.	Dokumentų analizė: Nagrinėjome Teisingumo ministerijos ir jai pavaldžių įstaigų <sup>57</sup> dokumentus, susijusius su informacinių išteklių kūrimu, priežiūra, valdymu ir finansavimu.	Nustatyti – ministerijos IT valdymo struktūrą; – valdomus informacinius išteklius, jų techninę infrastruktūrą, kūrimo ir palaikymo trūkumus ir privalumus.
2.	Pokalbiai su: <ul style="list-style-type: none"> <li>▪ Teisingumo ministerijos Registrų departamento, Strateginio valdymo departamento ir Centralizuoto vidaus audito skyriaus darbuotojais;</li> <li>▪ VĮ Registrų centro administracijos, taip pat už IS saugą atsakingais darbuotojais;</li> <li>▪ Centrinės hipotekos įstaigos vadovybės atstovais, Registrų plėtros departamento bei už IS saugą</li> </ul>	Nustatyti: – ministerijos informacinių išteklių valdymo struktūrą, privalumus ir problemas; – ministerijos valdomus informacinius išteklius; – informacinių išteklių kūrimo ir palaikymo problemas.

<sup>56</sup> COBIT 4.1, 2011 m., Vilnius.

<sup>57</sup> Centrinė hipotekos įstaiga, Europos teisės departamentas, Kalėjimų departamentas prie Lietuvos Respublikos teisingumo ministerijos, Valstybinis patentų biuras, Lietuvos teismo ekspertizės centras, Lietuvos teisės institutas, Valstybinė vartotojų teisių apsaugos tarnyba, Vilniaus valstybės garantuojamos teisinės pagalbos tarnyba, Valstybės įmonė Registrų centras, Valstybinės teismo medicinos tarnyba prie Lietuvos Respublikos teisingumo ministerijos, Valstybinė duomenų apsaugos inspekcija.

Eil. Nr.	Metodas	Tikslai
	atsakingais darbuotojais; <ul style="list-style-type: none"> <li>▪ Valstybinio patentų biuro vadovybės atstovais, Informacinių technologijų skyriaus ir už IS saugą atsakingais darbuotojais;</li> <li>▪ Lietuvos Teismo ekspertizės centro administracijos ir Informacinių sistemų poskyrio darbuotojais;</li> <li>▪ Valstybės vartotojų teisių apsaugos tarnybos vadovybe, Duomenų analizės ir prevencijos skyriaus, Turto valdymo ir viešųjų pirkimų skyriaus darbuotojais;</li> <li>▪ Kalėjimų departamento Projektų valdymo skyriaus darbuotojais</li> <li>▪ Vilniaus valstybės garantuojamos teisinės pagalbos tarnybos vadovu ir už IT atsakingais darbuotojais;</li> <li>▪ Europos teisės departamento vadovu ir už IT atsakingais darbuotojais;</li> <li>▪ Valstybinės teismo medicinos tarnybos Informacinių technologijų skyriaus darbuotojais;</li> <li>▪ Lietuvos teisės instituto administracijos, Leidybos ir bendrųjų reikalų skyriaus ir Tarptautinių ryšių skyriaus darbuotojais.</li> </ul>	
3.	Stebėseną: Valstybiniame patentų biure, Lietuvos teismo ekspertizės centre, Vilniaus valstybės garantuojamos teisinės pagalbos tarnyboje, stebėjome, kaip tvarkomos ir saugomos ministerijos valdomų informacinių išteklių tarnybinės stotys.	Nustatyti ministerijos valdomus informacinius išteklius aptarnaujančios techninės kompiuterinės įrangos priežiūros atitiktį teisės aktų reikalavimams.

Šaltinis – Valstybės kontrolė

Valstybinio audito ataskaitos  
 „Valstybės informacinių išteklių  
 valdymas Teisingumo ministerijoje“  
 2 priedas

## Rekomendacijų įgyvendinimo planas

Nr.	Rekomendacija	Subjektas	Rekomendacijų įgyvendinimo priemonės	Rekomendacijos įgyvendinimo terminas (data)
1.	Parengti bendrą teisingumo ministro valdymo srities IT plėtros planą, kuris apimtų visus srities valstybės informacinius išteklius ir kuriame būtų numatytas Teisingumo ministerijos ir kitų ministerijų valdomų informacinių išteklių tvarkymo prioritetų ir kryptių suderinamumas, taip pat priemonės, užtikrinančios IT išteklių ir priemonių planavimo, skyrimo, vykdymo ir panaudojimo kontrolę.	Teisingumo ministerija	Papildyti teisingumo ministro 2014-06-18 įsakymu Nr. 1R-191 patvirtintus Teisingumo ministerijos valdomų registų ir valstybės informacinių sistemų informacinių technologijų plėtros 2014–2016 metų planus, kad jie apimtų visų Teisingumo ministerijos valdymo srityje esančių registų ir valstybės informacinių sistemų plėtrą.	2016-04-01
2.	Inventorizuoti valdymo srities informacinius išteklius, peržiūrėti jų valdymą reglamentuojančius aktus ir priimti sprendimus dėl šių aktų keitimo vadovaujantis Valstybės informacinių išteklių valdymo įstatymu.		Peržiūrėti teisingumo ministro valdymo srityje esančių informacinių išteklių valdymą, reglamentuojančius aktus ir priimti sprendimus dėl šių aktų keitimo.	2016-01-01
3.	Sukurti organizacinę struktūrą, kuri spręstų pagrindinius IT strateginius ir IT valdymo uždavinius ir užtikrintų reikiamą visų lygių – vadovybės, visų ministro valdymo sričių veiklos ir IT atstovavimą bei veiklų koordinavimą.		Sukurti organizacinę struktūrą, kuri spręstų pagrindinius IT strateginius ir IT valdymo uždavinius ir užtikrintų reikiamą visų lygių – vadovybės, visų ministro valdymo sričių veiklos ir IT atstovavimą bei veiklų koordinavimą.	2015-01-01
4.	Siekiant užtikrinti teisingumo ministro valdymo srities įstaigų vykdomų IT projektų valdymo kokybę ir panaudoti pavaldžių įstaigų turimą IT projektų valdymo patirtį, patvirtinti bendruosius IT projektų valdymo principus.		Įgyvendinant 1 rekomendacijos priemonę, Teisingumo ministerijos valdymo srityje esančių registų ir valstybės informacinių sistemų plėtros plane numatyti bendruosius ministerijos IT projektų valdymo principus.	2016-04-01
5.	Užtikrinti atitikties išoriniams reikalavimams kontrolę, mažinančią neatitikimų teisės aktams skaičių ir garantuojančią informacijos saugos reikalavimų laikymąsi.		Atliekant Teisingumo ministerijos centralizuotą vidaus auditą: -numatyti priemones, kurios padėtų užtikrinti atitikties išoriniams reikalavimams kontrolę, mažinančią neatitikimų teisės aktams skaičių; -įvertinti valdymo srities įstaigų informacijos saugos	Ne rečiau kaip kartą per 3 metus.  Ne rečiau kaip kartą į metus

Nr.	Rekomendacija	Subjektas	Rekomendacijų įgyvendinimo priemonės	Rekomendacijos įgyvendinimo terminas (data)
			reikalavimų įgyvendinimo būklę ir planuojamas priemones.	
6.	Nustatyti teisingumo ministro valdymo srities informacinės architektūros modelį: suklasifikuoti visus srityje valdomus ir tvarkomus duomenis pagal svarbą ir apibrėžti jų vientisumo ir nuoseklumo principus.		Teisingumo ministro įsakymu patvirtinti teisingumo ministro valdymo srityje esančių registrų ir valstybės informacinių sistemų informacijos architektūros modelį, kuriame visa informacija pagal svarbą būtų suskirstyta į kategorijas.	2015-07-01
7.	Sukurti arba pritaikyti esamą IT turto ir paslaugų investicijų valdymui skirtą metodiką, kurioje būtų išsamai IT biudžeto sudarymo ir prioritetų nustatymo tvarka, IT investicijų kontrolės ir duodamos naudos analizės mechanizmas.		Patvirtinti teisingumo ministro valdymo sričių investicijų projektų rengimo, vertinimo ir įgyvendinimo kontrolės tvarkos aprašą, kuriame būtų nustatytas ir IT investicijų projektų vertinimo ir kontrolės mechanizmas.	2015-04-01
8.	Pakeisti ministerijos IT investicijų planavimo ir skyrimo sistemą taip, kad visiems teisingumo ministro valdymo srities informaciniams ištekliams tenkančios investicijos būtų vertinamos taikant tinkamus kriterijus.		Patikslinti patvirtintus teisingumo ministro valdymo sričių investicijų projektų atrankos bendruosius ir specialiuosius kriterijus bei jų reikšmes.	2015-04-01
<p>Atstovai ryšiams, atsakingi už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais:</p> <p>Strateginio valdymo departamento Veiklos planavimo skyriaus vedėja Asta Malinauskienė, el. paštas: <a href="mailto:asta.malinauskiene@tm.lt">asta.malinauskiene@tm.lt</a>, tel. (8 5) 266 2958;</p> <p>Registrų departamento Registrų teisinio reguliavimo skyriaus vyriausioji specialistė Sigita Panovienė, el. paštas: <a href="mailto:sigita.panoviene@tm.lt">sigita.panoviene@tm.lt</a>, tel. (8 5) 2662955.</p>				

Valstybinio audito ataskaitos  
 „Valstybės informacinių išteklių  
 valdymas Teisingumo ministerijoje“  
 3 priedas

## Neatitiktis privalomiems vykdyti teisės aktų reikalavimams

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807		
1.	31 straipsnis. Valstybės informacinių sistemų kūrimas. [...] 6. Naudojama tik įteisinta valstybės informacinė sistema ar jos posistemis.	Ministerijai pavaldžios įstaigos naudoja 4 neįregistruotas ir neįteisintas IS (žr. 4 priedą).
Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (neteko galios 2013-03-02). Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas.		
2.	10. Patvirtinus informacinės sistemos nuostatus, rengiama informacinės sistemos specifikacija. Specifikacijos projektą rengia informacinės sistemos nuostatuose nurodytas informacinės sistemos valdytojas arba informacinės sistemos tvarkytojas. Specifikacijos projektas rengiamas vadovaujantis informacinės sistemos kūrimo metodiniais dokumentais. Analogiški reikalavimai nustatyti 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (23 p.).	Kuriant IS neparengta trijų IS specifikacijos: KADIS, Vartotojų teisių ir Piniginių lėšų apribojimų (žr. 4 priedą).
3.	16. Užbaigus informacinės sistemos arba jos sudedamosios dalies (komponentės, posistemės) diegimą, informacinės sistemos valdytojo vadovas tvirtina informacinės sistemos priėmimo ir tinkamumo eksploatuoti aktą, kurio kopija per 5 darbo dienas nuo patvirtinimo pateikiama Komitetui. Informacinės sistemos valdytojas gali sudaryti komisiją atliktiems darbams įvertinti. Į komisijos sudėtį gali būti įtraukti suinteresuotų institucijų atstovai. Informacinės sistemos, kurioje yra tvarkomi asmens duomenys, priėmimo akto kopija papildomai pateikiama Valstybinei duomenų apsaugos inspekcijai. Analogiški reikalavimai nustatyti 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (30 p.).	KADIS sukurta ir naudojama, tačiau nepatvirtintas jos priėmimo ir tinkamumo eksploatuoti aktas.
4.	172. Sprendimą modernizuoti informacinę sistemą priima informacinės sistemos valdytojas. Priėmęs sprendimą modernizuoti informacinę sistemą, informacinės sistemos valdytojas rengia informacinės sistemos nuostatų pakeitimo projektą. Jis derinamas ir tvirtinamas šių Taisyklių 5–81 p. nustatyta tvarka. [...] Analogiški reikalavimai nustatyti 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (33 p.).	KADIS nuostatai neatnaujinti nuo sukūrimo 2006 m., nors 2010–2013 m. vykdytas šios IS tobulinimo projektas įdiegiant KADIS-1 IS.
Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai (neteko galios 2013-08-08), Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas.		
5.	6. Informacinės sistemos valdytojas privalo turėti pagal Vidaus reikalų ministerijos tvirtinamas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus: 6.1. nuostatus; 6.2. Saugaus elektroninės informacijos tvarkymo taisykles;	Nesuderinti su Vidaus reikalų ministerija ir nepatvirtinti vieno registro ir keturių naudojamų IS duomenų saugos nuostatai (žr. 4 priedą); nėra nustatyta tvarka suderintų su atsakingomis institucijomis ir patvirtintų 6 IS saugos

Eil. Nr.	Teisės akto reikalavimai	Auditorių pastebėjimai
	6.3. Informacinės sistemos veiklos tęstinumo valdymo planą; 6.4. Informacinės sistemos naudotojų administravimo taisykles. Analogiški reikalavimai nustatyti 2013-07-24 nutarimu Nr. 716 patvirtintame apraše (7 p.).	politiką įgyvendinančių dokumentų – Veiklos tęstinumo valdymo plano, Naudotojų administravimo taisyklių, Saugaus elektroninės informacijos tvarkymo taisyklių.
6.	25. Saugos įgaliotinis periodiškai organizuoja informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas. Mokymo ir informavimo būdai pasirenkami atsižvelgiant į informacinės sistemos specifiką. Mokymas planuojamas, organizuojamas ir vykdomas informacinės sistemos valdytojo tvirtinamuose Saugos nuostatuose nustatyta tvarka.	Ministerijoje neorganizuojami mokymai el. informacijos saugos klausimais.
7.	35. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje ( <a href="http://www.vrm.lt/Rizikos_analize.pdf">http://www.vrm.lt/Rizikos_analize.pdf</a> ), 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.	Rizikos vertinimas buvo atliekamas VĮ Registrų centre, Centrinėje hipotekos įstaigoje ir Valstybiniame patentų biure, o Teisingumo ministerijoje ir kitose ministro valdymo sričiai priskirtose įstaigose toks vertinimas kasmet neatliekamas.

## Valstybinio audito ataskaitos

## „Valstybės informacinių išteklių valdymas Teisingumo ministerijoje“

## 4 priedas

## Teisingumo ministro valdymo srities įstaigų tvarkomi informaciniai ištekliai\*

Nr.	Pavadinimas	Įregistravimo data	Valdytojas	Tvarkytojas	Nuostatai	Specifikacija	Duomenų saugos nuostatai	Saugos politiką įgyvendinantys dokumentai**	Priėmimo aktas
<b>Informacinės sistemos</b>									
1	Juridinių asmenų dalyvių informacinė sistema	2013-10-17	TM	RC	yra	yra	yra	projektas	yra
2	Piniginių lėšų apribojimų informacinė sistema	2012-05-02	TM	RC	yra	nėra	yra	yra	nėra
3	Antstolių informacinė sistema	2011-03-08	TM	RC, Antstolių rūmai	yra	yra	yra	yra	yra
4	Politinių partijų narių sąrašų informacinė sistema	2010-03-08	TM	TM, CHĮ	yra	yra	yra	yra	yra
5	Vartotojų teisių informacinė sistema	2013-01-29	VVTAT	VVTAT, RC	yra	nėra	yra	nėra	nėra
6	Informacinė sistema „E. sąskaita“	2012-11-13	FM	RC	yra	yra	yra	nėra	nėra
7	Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema	2011-10-05	SAM	RC	yra	yra	yra	yra	nėra
8	Informacinė sistema „Pagalba“	2002-10-23	VDAI	VDAI	yra	yra	yra	yra	yra
9	Kalėjimų departamento informacinė sistema	2006-12-21	KD	KD	yra	nėra	nėra	nėra	nėra
<b>Registrai</b>									
1	Neveiksnių ir ribotai veikusių asmenų registras	2010-12-21	TM	CHĮ	yra	yra	yra	yra	yra
2	Įgaliojimų registras	2010-12-21	TM	CHĮ	yra	yra	yra	yra	yra
3	Juridinių asmenų registras	2003-01-27	TM	RC	yra	yra	yra	yra	yra
4	Sutarčių registras	2003-01-23	TM	CHĮ	yra	yra	yra	yra	yra
5	Nekilnojamojo turto registras	2003-01-23	TM	RC	yra	yra	yra	yra	yra
6	Vedybų sutarčių registras	2003-01-23	TM	CHĮ	yra	yra	yra	yra	yra
7	Testamentų registras	2003-01-23	TM	CHĮ	yra	yra	yra	yra	yra



Nr.	Pavadinimas	Įregistravimo data	Valdytojas	Tvarkytojas	Nuostatai	Specifikacija	Duomenų saugos nuostatai	Saugos politiką įgyvendinantys dokumentai**	Priėmimo aktas
8	Turto arešto aktų registras	2003-01-22	TM	CHĮ	yra	yra	yra	yra	yra
9	Adresų registras	2003-01-21	TM	RC	yra	yra	yra	yra	yra
10	Hipotekos registras	2003-01-17	TM	CHĮ	yra	yra	yra	yra	yra
11	Asmens duomenų valdytojų valstybės registras	2003-01-22	VDAI	VDAI	yra	yra	yra	yra	yra
12	Dizaino registras	2003-01-28	VPB	VPB	yra	nėra	yra	yra	nėra
13	Patentų registras	2003-01-24	VPB	VPB	yra	nėra	yra	yra	nėra
14	Prekių ženklų registras	2003-01-23	VPB	VPB	yra	yra	yra	yra	yra
15	Topografijų registras		VPB	VPB	nėra	nėra	nėra	yra	nėra
	<b>Kadastrai</b>								
1	Nekilnojamojo turto kadastras	2003-01-23	Žemės tarnyba	RC	yra	nėra	nėra	nėra	nėra
	<b>Naudojamos neįregistruotos IS</b>								
1	Lietuvos teismo ekspertizės centro informacinė sistema				nėra	nėra	nėra	nėra	nėra
2	Valstybinė teismo medicinos tarnybos informacinė sistema				nėra	nėra	nėra	nėra	nėra
3	Valstybės garantuojamos teisinės pagalbos tarnybos IS				nėra	nėra	nėra	nėra	nėra
4	Sertifikatų valdymo informacinė sistema		RC	RC	yra	nėra	yra	yra	nėra

\* – pagal pateiktą atitinkamų institucijų informaciją ir Registrų ir valstybės informacinių sistemų registro duomenimis

\*\* – Veiklos tęstinumo valdymo planas, Naudotojų administravimo taisyklės ir Saugaus elektroninės informacijos tvarkymo taisyklės

TM – Lietuvos Respublikos teisingumo ministerija

RC – valstybės įmonė Registrų centras

Antstolių rūmai – asociacija Lietuvos antstolių rūmai

VPB – Lietuvos Respublikos valstybinis patentų biuras

CHĮ – Centrinė hipotekos įstaiga

VVTAT – Valstybinė vartotojų teisių apsaugos tarnyba

FM – Lietuvos Respublikos finansų ministerija

- SAM – Lietuvos Respublikos sveikatos apsaugos ministerija
- VDAI – Valstybinė duomenų apsaugos inspekcija
- KD – Kalėjų departamentas prie Lietuvos Respublikos teisingumo ministerijos
- Žemės tarnyba – Nacionalinė žemės tarnyba prie Žemės ūkio ministerijos

Valstybinio audito ataskaitos  
 „Valstybės informacinių išteklių valdymas Teisingumo ministerijoje“  
 5 priedas

## Gebėjimų brandos modelis

Šiame priede apibūdinamas Gebėjimų brandos modelis (angl. – CMM), taikomas IS kontrolės tikslų brandos lygiui įvertinti. Pateiktas kiekvieno tikslo įvertinimas yra žemiausias atitinkamo tikslo įvertinimas pagal bet kurį iš toliau išvardytų keturių punktų (a–d). Vertinimo vidurkis neišvedinėjamas, nes sudėtinių vertinimų vidurkiai neatspindi realios situacijos. Auditorius, vadovaudamasis modelio paaiškinamąja lentele (1 lentelė), turi užpildyti žemiau pateiktą 2 lentelę.

1 lentelė. Paaiškinamoji Gebėjimų brandos modelio lentelė.

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.
<b>0. Neegzistuojantis procesas</b>	Organizacija nepripažįsta spręstinios 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.
<b>1. Pirminis/Ad Hoc procesas</b>	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 kiekienu konkrečiu atveju taikomi ad hoc metodai. Problema nenagrinėjama vadovybės lygiu.	Stebėseną vykdoma reaguojant į incidentą, dėl kurio organizacija patiria tam tikrą nuostolį.
<b>2. Pasikartojantis, bet intuityvus procesas</b>	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	Vadovybė yra nustačiusi pagrindinius vertinimo objektus ir vertinimo metodus bei būdus, tačiau pastarieji parengti nepakankamai.

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.
			apie standartus ir pareigas paliktas individualių darbuotojų nuožiūrai.	
<b>3. Apibrėžtas procesas</b>	Visa organizacija supranta, kad reikia reaguoti į problemą, ir tam pritaria.	Organizacijoje vykdoma nuosekli 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. Procedūras galima įvertinti, tačiau jos nėra sudėtingos ir formaliai atspindi esamą patirtį.	Susijusių veiklos sričių rodiklių registravimas ir stebėseną padeda tobulinti veiklą. Beveik visų susijusių procesų stebėseną vykdoma pagal tam tikrus (pirminius) dokumentus, tačiau mažai tikėtina, kad vadovybė galėtų pastebėti bet kokią nukrypimą, nes tokios priemonės paprastai taikomos individualiai. Priežasčių analizė atliekama retai.
<b>4. Lengvai valdomas ir vertinamas procesas</b>	Visais atitinkamais organizacijos lygiais problema suprantama tinkamai ir reikalaujama imtis priemonių.	Vykdoma nuosekli ir aiški politika, integruota su kitomis susijusiomis politikos kryptimis. Atsižvelgiama į rizikos valdymą.	Organizacija gerai pažįsta savo klientą ir turi aiškiai apibrėžtas pareigas. Procesai yra aiškiai suformuluoti, integruoti ir taikomi visoje organizacijoje. Procesai yra gerai pritaikyti ir palaikomi organizuojant tinkamą mokymą. Visi susijusių procesų dalyviai žino apie riziką ir galimybes.	Kartais susiję procesai tobulinami, įgyvendinant geriausią vidaus praktiką. Vykdomas priežasčių analizės standartizavimas. Pradedamas nuolatinis veiklos gerinimo procesas.
<b>5. Optimalus procesas</b>	Problemos ir jos sprendimo būdų vertinimas yra pažangus bei perspektyvus.	Organizacija vykdo nuoseklią 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 užtikrina organizacijos,	Stebėseną, savianalizę ir informavimą 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

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.
			darbuotojų ir procesų sugebėjimą greitai prisitaikyti ir visapusiškai valdyti rizikos pokyčius.	analize.