Valstybinio audito ataskaita

# POLICIJOS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

2015 m. lapkričio 5 d. Nr. VA-P-90-3-15

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

# TURINYS

# SANTRUMPOS IR SĄVOKOS

ADA – automatizuoto duomenų apdorojimo informacinė sistema

ATPEĮR – Administracinių teisės pažeidimų ir eismo įvykių registras

BPC – Bendrasis pagalbos centras

BPC IS – Bendrojo pagalbos centro informacinė sistema

COBIT – ISACA[1] sukurta IT valdymo ir vadovavimo metodika

IGR – Ieškomų ginklų registras

INDR – Ieškomų numeruotų ir individualius požymius turinčių daiktų ir dokumentų registras

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

IS – informacinė sistema

IT – informacinės technologijos

ITKG – Informacinių technologijų koordinavimo grupė

ITPR – Ieškomų transporto priemonių registras

IVPK – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos

NAIS – Nusikalstamumo analizės informacinė sistema

OIS – Operatyvinės veiklos informacinė sistema

PAGD – Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

PLVIS – Policijos licencijuojamos veiklos informacinė sistema

POLIS – Policijos informacinė sistema

PPV – Policijos pajėgų vienetas

PRĮR – Policijos registruojamų įvykių registras

PVVIS – Prevencinės veiklos valdymo informacinė sistema

SPG – Strateginio planavimo grupė

VPVS – Vieninga pajėgų valdymo sistema

VRIS CDB – Vidaus reikalų ministerijos informacinės sistemos centrinis duomenų bankas

VSAT – Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos

VST – Viešojo saugumo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos

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

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

# SANTRAUKA

Lietuvos policijos misija - efektyviai naudojant turimus išteklius ginti Lietuvos žmonių teises ir laisves, saugoti visuomenę ir valstybę, padėti žmogui, šeimai ir bendruomenei. Lietuvoje yra dvi policijos dalys: kriminalinė ir viešoji. Tai vientisa policijos organizacija, jos jungiamoji ir vadovaujamoji grandis – Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.

Pagrindiniai policijos uždaviniai[2]: žmogaus teisių ir laisvių apsauga; viešosios tvarkos ir visuomenės saugumo užtikrinimas; neatidėliotinos pagalbos teikimas asmenims, kai ji būtina dėl jų fizinio ar psichinio bejėgiškumo, taip pat asmenims, nukentėjusiems nuo nusikalstamų veikų, kitų teisės pažeidimų, stichinių nelaimių ar panašių veiksnių; nusikalstamų veikų ir kitų teisės pažeidimų prevencija; nusikalstamų veikų ir kitų teisės pažeidimų atskleidimas ir tyrimas; saugaus eismo priežiūra.

Policijos uždaviniams įgyvendinti būtini duomenys tvarkomi žinybiniuose registruose, informacinėse sistemose, automatizuoto duomenų apdorojimo sistemose ir tinkluose, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija. Policijos departamentas yra visų šių informacinių išteklių valdytojas, todėl audito metu pagrindinis dėmesys buvo skirtas departamento veiklai ir veiksmams, užtikrinantiems šių išteklių planavimą ir organizavimą, stebėseną, vertinimą ir koordinavimą, ir kitiems IS ir registrų strateginio valdymo aspektams.

Audituojamas laikotarpis – 2012–2014 m., duomenų analizei buvo naudojami ankstesnių laikotarpių ir 2015 m. duomenys.

Audito tikslas – įvertinti Policijos departamento informacinių išteklių valdymą ir kūrimo kontrolę. Auditą atlikome Policijos departamente. Duomenis ir informaciją rinkome departamento specializuotose ir teritorinėse policijos įstaigose: Lietuvos kriminalinės policijos biure, Lietuvos policijos kriminalistinių tyrimų centre, Vilniaus, Kauno, Alytaus ir kitų apskričių vyriausiuosiuose policijos komisariatuose; VĮ „Regitra“, Greitosios medicinos pagalbos stotyje. Audito procedūras atlikome Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos ir Bendrajame pagalbos centre.

Policijos departamentas investuoja į IT vadovaudamasis bendrąja departamento veiklos strategija ir tikslais, tačiau šiam dokumentui trūksta detalumo aprašant pagrindines IT plėtros kryptis, IS ir registrų steigimo prioritetus, nenurodytos Policijos departamente planuojamos, vykdomos ir įgyvendinamos IT plėtros priemonės: IS, registrų kūrimas ir modernizavimas.

Policijos departamente ir policijos įstaigose sudarytos grupės ir komisijos IT klausimams svarstyti. Joms pavesta nustatyti IT vystymo kryptis, organizuoti, koordinuoti ir kontroliuoti IT plėtrą, informacinio saugumo tikslų nustatymą ir informacinėms vertybėms kylančių grėsmių stebėjimą. Jų veikla epizodiška, nustatytos funkcijos nevykdomos visa apimtimi ir persidengia, todėl neužtikrinama tinkama IT įgyvendinimo, informacinėms vertybėms kylančių grėsmių kontrolė ir stebėsena.

Policijos departamentas ir teritorinės policijos įstaigos periodiškai atlieka darbuotojų duomenų tvarkymo (asmens duomenų peržiūros) teisėtumo ir pagrįstumo patikrinimus, bendradarbiauja su

[2] Lietuvos Respublikos policijos veiklos įstatymas, 2000-10-17 Nr. VIII-2048, 5 str.

Valstybine duomenų apsaugos inspekcija. Neteisėto policijos duomenų bazių naudojimo rizika nepakankamai valdoma Lietuvos kriminalinė policijos biure.

Siekiant užtikrinti darnią Policijos departamento IT plėtrą ir indėlį įgyvendinant policijos tikslus ir uždavinius, rekomendavome parengti ir patvirtinti IT strategiją ir jos pagrindu sukurti ir nuolatos atnaujinti IT plėtros planus. Siekiant aiškios atsakomybės už strateginius sprendimus ir tinkamo požiūrio į IT valdymą, rekomendavome peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus, veiklą, atskirti jų funkcijas, užtikrinti grupių veiklos tęstinumą, pavestų funkcijų vykdymą ir atskaitomybę. Taip pat Policijos departamentas turėtų skirti daugiau dėmesio sistemų saugos ir veiklos tęstinumo užtikrinimui bei sistemingam IT projektų valdymui.

Įvertinę surinktus įrodymus, teikiame valstybinio audito išvadas ir rekomendacijas.

# IŠVADOS

1. Policijos departamente įgyvendinant policijos tikslus ir uždavinius trūksta nuoseklaus ir subalansuoto IT planavimo ir vystymo, nes strateginio planavimo dokumentuose nenurodytos pagrindinės IT plėtros kryptys, planuojamos kurti ar modernizuoti valstybės IS ir registrai, jų steigimo prioritetai (1.1 poskyris, 11 psl.).
2. Policijos departamentas neturi bendro informacijos architektūros modelio, apibrėžiančio departamento ir policijos įstaigų valdomą (sukuriamą) informaciją, jos klasifikavimo kriterijus, IS/registrų duomenų ir technologinę architektūrą, todėl neaiški Policijos departamento IS ir registrų tarpusavio sąveika, departamente ir policijos įstaigose valdomos informacijos svarba ir jautrumas tokios informacijos viešinimui, perdavimui ir atskleidimui (1.2 poskyris, 13 psl.).
3. Policijos departamentas neužtikrina teisės aktuose ir procedūrose nustatytų reikalavimų dėl informacinių išteklių saugos ir duomenų valdymo:
   3.1. Policijos departamente patvirtinta tvarka, nustatanti galimų grėsmių ir rizikos veiksnių policijos IS analizavimo, stebėjimo ir vertinimo procedūras, bet jos nesilaikoma, neatliekami saugos atitikties vertinimai teisės aktų nustatytu periodu, todėl netaikomos tinkamos kontrolės priemonės nustatytai rizikai valdyti, neįsitikinama, ar parinktos pakankamos saugos priemonės ir nevertinama, kaip jų laikomasi (1.3 poskyris, 14 psl.).
   3.2. Policijos departamente neatliekami duomenų atkūrimo bandymai iš atsarginių duomenų kopijų, duomenų kopijos saugomos toje pačioje patalpoje kaip ir tarnybinės stotys, o ši patalpa neturi automatinės gaisro gesinimo sistemos, todėl saugos incidento atveju gali būti negrįžtamai sugadinta techninė ir programinė tarnybinių stočių įranga, prarasti aktyviose IS duomenų bazėse esantys duomenys, o kartu ir šių duomenų kopijos (1.3. 1.4 poskyriai, 14,17 psl.).
   3.3. Policijos departamentas neįsitikino, ar yra pasiruošęs atkurti valdomų IS ir registrų veiklą per laikotarpį, kuris neturėtų neigiamos įtakos departamento ir susijusių institucijų funkcijų įgyvendinimui, nes departamento veiklos tęstinumo valdymo planas neatnaujintas ir neišbandytas (1.3 poskyris, 15 psl.).
   3.4. Policijos departamentas įgyvendina ne visas technines ir organizacines asmens duomenų saugumo priemones tvarkant duomenis automatizuotu būdu, neorganizuoja mokymų duomenų tvarkymo teisėtumo ir informacijos saugos klausimais, todėl tvarkant duomenis neužtikrinamas elektroninės informacijos konfidencialumas ir asmens

duomenų apsauga nuo atsitiktinio ar neteisėto sunaikinimo, atskleidimo (1.3, 1.4 poskyriai, 15, 18 psl.).

4. Išvados dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta) (1.5 poskyris, 18 psl.).
5. Policijos departamente nepatvirtinta IT pokyčių valdymo tvarka, netaikoma praktika, kad visi IT pokyčiai būtų vieningai ir standartizuotai užsakomi, pagrindžiant pokyčio reikalingumą ir naudą, nurodant pokyčio prioritetą, suskirstant juos į kategorijas pagal pokyčio tipus, todėl departamente eikvojami papildomi laiko ištekliai vertinant ir apibendrinant pateiktų IT pokyčių tikslingumą ir pagrįstumą (1.6 poskyris, 18,19 psl.).
6. Policijos departamento vidaus auditoriai nestebi ir nevertina informacinių išteklių valdymo, o tai sudaro prielaidas atsirasti galimiems informacinių sistemų valdymo vidaus kontrolės trūkumams, be to, nustatyta neatitikčių išorės reikalavimams (1.7 poskyris, 20 psl.).
7. IT valdymo organizacinė struktūra tobulintina: departamente ir policijos įstaigose sudarytos grupės ir komisijos, kad pagrindinės veiklos poreikiai būtų siejami su IT teikiamomis galimybėmis, tačiau ne visos grupės ir komisijos vykdo pavestas funkcijas visa apimtimi, grupių ir komisijų veikla nereguliari (epizodiška), todėl neužtikrinama tinkama IT įgyvendinimo kontrolė ir kylančių grėsmių stebėsena (1.8 poskyris, 20, 21 psl.).
8. Policijos departamente taikomi projektų valdymo principai neužtikrino VPVS projekto kokybės ir rizikų valdymo, nes:
   8.1. VPVS modernizuota nesilaikant teisės aktų reikalavimų: privaloma dokumentacija – VPVS nuostatai ir specifikacija – patvirtinti po projekto įgyvendinimo, baigus VPVS modernizacijos etapą nepatvirtintas VPVS perdavimo–priėmimo aktas (2.1, 2.2 poskyriai, 24, 28 psl.).
   8.2. Įgyvendinant VPVS modernizavimo projektą nesudarytas integruotas VPVS projekto valdymo planas, kuris apimtų laiko, finansinius, žmogiškuosius išteklius, sudėtinių projekto veiklų ir susijusių projektų sąlyčio taškus ar tarpusavio ryšius, todėl buvo netinkamai nustatyti IS projekto sudėtinių dalių atlikimo terminai ir iki kritinės ribos (20 kalendorinių dienų) sumažėjo VPVS funkcijų tobulinimo terminai (2.1 poskyris, 24 psl.).
   8.3. VPVS projekto įgyvendinimą koordinavusi Vidaus reikalų ministerija nesudarė sąlygų patikimam duomenų keitimuisi tarp Policijos departamento ir Bendrojo pagalbos centro, todėl buvo sukurta tik vienkryptė sąsaja tarp PRĮR, VPVS ir BPC IS (2.1 poskyris, 25 psl.).
   8.4. Nesilaikoma nustatyto vykdomų projektų kontrolės mechanizmo, VPVS programinės įrangos tobulinimo darbai buvo vykdomi skubotai, testavimo, mokymo organizavimo ir rezultatų priėmimo eiga buvo nenuosekli, neatlikta VPVS bandomoji eksploatacija ir projekto rezultatų peržiūra, todėl neįsitikinta sklandžiu sukurtų funkcijų veikimu esant realioms IS eksploatavimo sąlygoms, o baigus projektą – jo rezultatyvumu, ar sukurtos VPVS programinės įrangos funkcijos naudojamos (2.1, 2.2 poskyriai, 24, 26, 27 psl.).

   Rekomendacijų įgyvendinimo planas pateiktas 2 priede.

## REKOMENDACIJOS

1. Siekiant nuoseklaus ir kryptingo IS ir registrų tobulinimo ir atsižvelgiant į visos organizacijos veiklos poreikius, parengti ir patvirtinti IT strategiją ir jos pagrindu sukurti bei nuolatos atnaujinti IT plėtros planus (1 išvada).

2. Sudaryti informacijos architektūros modelį, apimantį Policijos departamento ir policijos įstaigų valdomos informacijos, IS/registrų duomenų bei technologinę architektūrą, nurodant kiekvienos sudedamosios dalies komponentus (naudojamos technologijas, duomenis, duomenų srautus tarp išorinių ir vidinių IS) (2 išvada).
3. Siekiant užtikrinti valdomų informacinių išteklių saugą:
   3.1. Atlikti visų Policijos departamento valdomų informacinių išteklių periodišką saugos atitikties vertinimą ir užtikrinti nustatytų trūkumų šalinimo kontrolę (3.1 išvada).
   3.2. Tobulinti rizikos valdymo procesą, laikytis departamento galimų grėsmių ir rizikų policijos IS analizavimo, stebėjimo ir vertinimo procedūrų aprašo ir užtikrinti nustatytos rizikos mažinimo priemonių įgyvendinimą (3.1 išvada).
   3.3. Suderinti atsarginių duomenų kopijų saugojimo bei duomenų atkūrimo tvarką ir planus su Vidaus reikalų ministerija, atsižvelgiant į Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašą (3.2 išvada).
   3.4. Atnaujinti departamento IS veiklos tęstinumo valdymo planą ir jį išbandyti (3.3 išvada).
   3.5. Periodiškai organizuoti darbuotojų mokymus duomenų tvarkymo teisėtumo ir informacijos saugos klausimais (3.4 išvada).
   3.6. Pranešti Valstybinei duomenų apsaugos inspekcijai apie departamento valdomuose informaciniuose ištekliuose automatiniu būdu tvarkomus asmens duomenis ir jų tvarkymo tikslus, kad būtų atnaujinta Asmens duomenų valdytojų registre esanti informacija (3.4 išvada).
   3.7. Peržiūrėti ir atnaujinti IS ir registrų duomenų tvarkymo taisykles: jose išdėstyti taikomos asmens duomenų saugos priemones taip, kaip nustato Asmens duomenų teisinės apsaugos įstatymas (3.4 išvada).
4. Rekomendacijos dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta) (4 išvada).
5. Siekiant veiksmingo ir sistemingo pokyčių valdymo, peržiūrėti taikomą pokyčių valdymo procesą ir nustatyti (patvirtinti) IT pokyčių valdymo tvarką, kurioje būtų reglamentuotas IT pokyčių valdymo planavimas ir užtikrinta šios tvarkos laikymosi (vykdymo) kontrolė (5 išvada).
6. Periodiškai stebėti ir vertinti informacinių sistemų ir registrų vidaus kontrolės būklę (6 išvada).
7. Peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus, veiklą, aiškiai atskirti jų funkcijas, užtikrinti jų veiklos tęstinumą ir pavestų funkcijų vykdymą (7 išvada).
8. Siekiant užtikrinti IT projektų kokybę ir projektų rizikos valdymą:
   8.1. Peržiūrėti ir atnaujinti Policijos departamente taikomus IT projektų valdymo principus, numatant, kad būtų sudaromas integruotas projekto įgyvendinimo planas. Pagal šį planą viso projekto gyvavimo ciklo metu organizuojamas projektų įgyvendinimas ir kontrolė, o apie nuokrypius nuo plano informuojamos už įgyvendinimo kontrolę atsakingos struktūros (8.2, 8.3, 8.4 išvados).
   8.2. Parengti ir patvirtinti valdomų informacinių išteklių nuostatus bei specifikacijas ir įteisinti naudojamas sistemas ir registrus (8.1 išvada, 4 priedas).

# ĮŽANGA

Valstybės kontrolė atliko Policijos informacinių išteklių valdymo auditą. Jis apėmė laikotarpį nuo 2012 iki 2014 m., duomenų analizei naudoti ankstesnių laikotarpių ir 2015 m. duomenys.

Policijos departamentas ir policijos įstaigos teisės aktuose nustatytoms funkcijoms atlikti naudoja aštuonis žinybinius registrus (nuo 2015-07-01 septynis), penkias valstybės informacines sistemas (nuo 2015-07-01 šešias), tris automatizuoto duomenų apdorojimo sistemas, kuriose apdorojama informacija su slaptumo žyma „Riboto naudojimo", automatizuoto duomenų apdorojimo tinklą, kuriuo perduodama informacija su slaptumo žyma „Riboto naudojimo", atskiras (lokalias) kompiuterizuotas darbo vietas, skirtas dirbti su įslaptinta informacija žymima „Riboto naudojimo" ir aukštesnėmis slaptumo žymomis. Viena valstybės informacinė sistema audito metu buvo kuriama (žr. 4 priedą).

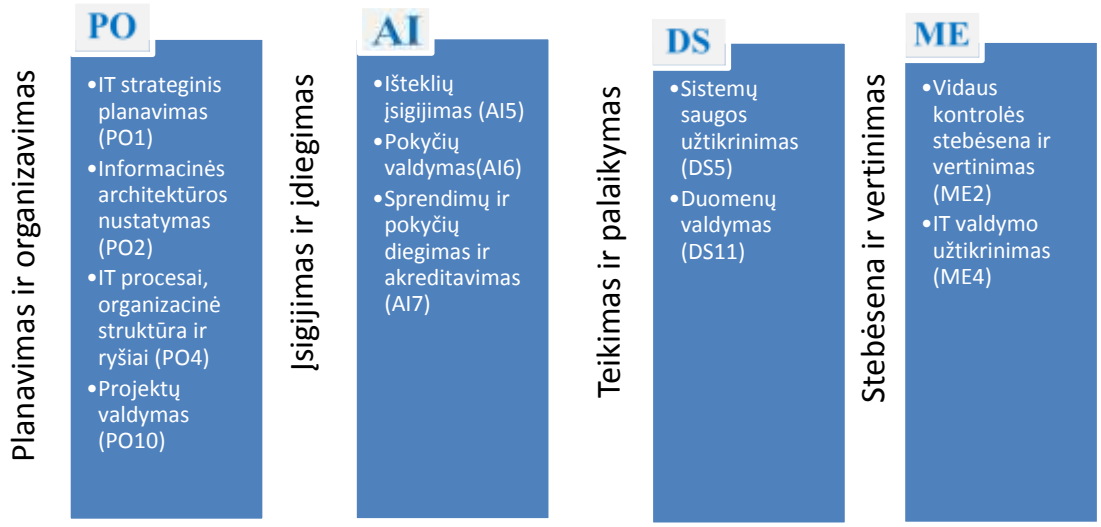
Lietuvos kriminalinės policijos biuras yra vienos valstybės informacinės sistemos valdytojas, o Policijos departamentas yra kitų valstybės informacinių valstybės sistemų ir registrų valdytojas. Kadangi departamento valdomas informacines sistemas ir registrus tvarko specializuotos ir teritorinės policijos įstaigos, todėl, siekiant įsitikinti registrų ir informacinių sistemų valdymo efektyvumu, audito procedūros buvo atliktos Lietuvos kriminalinės policijos biure, Lietuvos policijos kriminalistinių tyrimų centre, Vilniaus ir Alytaus apskrities vyriausiuose policijos komisariatuose. Departamento valdomų informacinių išteklių duomenys teikiami trečiosioms šalims, todėl siekiant nustatyti, kokią įtaką Policijos departamento IS neveikimas turi susijusioms šalims, duomenys buvo renkami VĮ „Regitra". Atsižvelgus į nustatytas rizikas, vertinta Vieningos pajėgų valdymo sistemos kūrimo kontrolė, audito procedūros atliktos Bendrajame pagalbos centre, Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos.

Policijos departamentas informacinių sistemų ir registrų plėtrai kasmet skiria vidutiniškai 434,4 tūkst. Eur valstybės kapitalo investicijų, įgyvendina projektus, finansuojamus iš Europos Sąjungos struktūrinių fondų ir kt. lėšų. Per 2012–2014 m. IT plėtrai panaudota per 8 mln. Eur.

Policijos informacinių išteklių valdymas įvertintas pagal Valstybinio audito reikalavimus ir tarptautinės Informacinių sistemų audito ir kontrolės asociacijos ISACA parengtą Informacinių technologijų valdymo metodiką COBIT[3]. Audito metu atlikus preliminarų rizikos vertinimą pasirinkta 11 iš 34 COBIT procesų (žr. 1 pav.). Ataskaitoje pateikiamas devynių COBIT procesų vertinimas, nes kituose (AI5 ir PO4) esminių IT valdymo ir kūrimo kontrolės trūkumų nenustatyta.

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

**1 pav.** Policijos informacinių išteklių valdymui ir kūrimo kontrolei vertinti pasirinkti COBIT procesai




Šaltinis – Valstybės kontrolė

Valstybiniai auditoriai, įvertinę policijos informacinių išteklių valdymą, nustatė informacinių sistemų vidaus kontrolės brandą, pateikė audito išvadas ir rekomendacijas. Išvados ir rekomendacijos dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta).

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.

# AUDITO REZULTATAI

## 1. POLICIJOS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

Policijos informacinių išteklių valdymas vertintas atsižvelgiant į teisės aktų reikalavimus ir COBIT siūlomą gerąją praktiką. Analizavome, kaip Policijos departamente vykdomas IT strateginis planavimas, valdomi IT pokyčiai, ar departamente patvirtinta ir įgyvendinama informacijos saugos politika, ar vykdoma IS vidaus kontrolės stebėsena. Įvertinus informacinių išteklių valdymą, nustatyta IS vidaus kontrolės branda (žr. 1.8 poskyrį).

### 1.1. Informacinių technologijų strateginis planavimas

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[4]. Strateginis planas leidžia pagrindinėms suinteresuotosioms šalims geriau suprasti IT teikiamas galimybes ir jų naudojimo apribojimus, įvertinti esamą veiklą, nustatyti pajėgumų ir žmogiškųjų išteklių reikalavimus, išaiškinti investicijų poreikį. Tokiu būdu užtikrinamas visų veiklos grandžių darnus darbas, įgyvendinant valdymo sričiai keliamus uždavinius ir siekiant bendrų veiklos tikslų.

Valstybės informacinių išteklių valdymo įstatymas numato, kad institucijos, valdančios ypatingos svarbos valstybės informacinius išteklius turi turėti IT plėtros planą, o institucijos valdančios valstybės informacinius išteklius IT strateginio planavimo (plėtros) kryptis, tikslus, uždavinius ir kitą įstatymo 9 straipsnio 1 dalyje nurodytą informaciją turėtų įtraukti į strateginius ir metinius veiklos planus[5].

Policijos departamentas valdo valstybės informacinius išteklius (žr. 4 priedą), todėl investuoja į IT vadovaudamasis bendrąja departamento veiklos strategija ir tikslais. Siekdamas užtikrinti, kad IT atitiktų policijos tiesioginės veiklos poreikius ir gebėtų prisitaikyti prie didėjančių ir kintančių veiklos reikalavimų, 2008 m. Policijos departamentas parengė IT strateginių planavimo dokumentų projektus, taip pat policijos įstaigos įpareigotos parengti IT vystymo ir saugos strategijas (žr. 1 pavyzdį). Šie strateginiai dokumentai taip ir nebuvo patvirtinti, o vykdant tolimesnį departamento IT strateginį planavimą jais nebuvo vadovaujamasi.

**1 pavyzdys**

2010 m. sudaryta[6] Lietuvos policijos kriminalistinių tyrimų centro informacinių technologijų vystymo ir plėtros komisija buvo įpareigota kurti informacinių technologijų diegimo, vystymo ir plėtros strategiją. Lietuvos policijos kriminalistinių tyrimų centras iki šiol tokios strategijos neturi.

Lietuvos kriminalinės policijos biuro Informacinių technologijų skyrius turėtų rengti[7] Lietuvos kriminalinės policijos biuro informacinių ir elektroninių ryšių technologijų strategiją, apimančią elektroninės informacijos saugą ir jos įgyvendinimo planus. Audito metu nustatyta, kad tokia

[4] COBIT 4.1, 2011 m., Vilnius, PO1 procesas, 29 psl.

[5] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 9 str. 1 ir 3 d.

[6] Lietuvos policijos kriminalistinių tyrimo centro viršininko 2010-01-06 įsakymas Nr. 140-V-2 (paskutinis pakeitimas – 2015-05-11 įsakymas Nr. 140-V-58).

[7] Lietuvos kriminalinės policijos biuro viršininko 2013-04-11 įsakymu Nr. 38-V-60 patvirtinti Lietuvos kriminalinės policijos biuro informacinių technologijų valdybos nuostatai, 9.1.2 p.

strategija nerengiama, o, Lietuvos kriminalinės policijos biuro duomenimis, visi informacinių ir elektroninių ryšių technologijų strateginiai klausimai įtraukiami į metinius veiklos planus.

Išanalizavę departamento ir policijos įstaigų strateginius veiklos planavimo dokumentus auditoriai nustatė, kad jų turinys neatitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatytų reikalavimų, keliamų valstybės informacinių išteklių planavimui[8], nes strateginio planavimo dokumentuose nenurodytos pagrindinės IT plėtros kryptys, planuojamos kurti ar modernizuoti valstybės IS ir registrai, jų steigimo prioritetai. Policijos departamente ir policijos įstaigose buvo planuojamos ir vykdomos IT plėtros priemonės, kurios nebuvo nurodytos strateginiuose veiklos planavimo dokumentuose (žr. 2 pavyzdį).

**2 pavyzdys**

2013 m. pradėtas vykdyti ES paramos lėšomis finansuojamas projektas „Sumanios nusikaltimų prevencijos ir kovos su nusikalstamumu vystymas, skatinantis europinį operatyvinį bendradarbiavimą ir keitimąsi informacija“ (1,095 mln. Eur) įtrauktas į 2013 m. Vilniaus apskrities vyriausiojo policijos komisariato metinį veiklos planą, bet neįtrauktas į atitinkamo laikotarpio Policijos departamento strateginį veiklos planą.

Nuo 2014 m. įgyvendinamas ES finansuojamas projektas „Keleivių duomenų įrašų sistemos sukūrimas Lietuvoje“ (1,055 mln. Eur) įtrauktas į 2014 m. Lietuvos kriminalinės policijos biuro metinį veiklos planą, bet neįtrauktas į atitinkamo laikotarpio Policijos departamento strateginį veiklos planą.

2010-2014 m. VPVS modernizavimas neįtrauktas į atitinkamo laikotarpio strateginius veiklos planus, detaliai neaptariama VPVS strateginė plėtros kryptis, trūksta ateities įžvalgų modernizuojant ir tobulinant šią IS (žr. 2.1 poskyrį).

COBIT rekomenduoja[9] IT strateginio plano pagrindu sukurti IT taktinių planų portfelį. Taktiniai planai turi apimti IT palaikomas programų investicijas, IT paslaugas ir turtą, jie turi apibrėžti reikiamas IT iniciatyvas, išteklių poreikį ir tai, kaip bus tikrinamas ir valdomas išteklių naudojimas ir naudos pasiekimas.

Audito metu nustatyta, kad Policijos departamento valdomiems IS ir registrams paskirti duomenų valdymo įgaliotiniai nesiėmė reikiamų iniciatyvų, nevykdė įpareigojimų ir neparengė IS ir registrų tobulinimo (plėtros) planų, nors, siekiant nuoseklaus ir kryptingo IS ir registrų tobulinimo, juos rengti būtina, tai buvo numatyta 2013 m. ir 2014 m., atlikus IS rizikos vertinimą.

Galiojantys Lietuvos Respublikos teisės aktų reikalavimai neįpareigoja Policijos departamento rengti atskiro IT strateginio dokumento, tačiau, atsižvelgiant į departamento valdomų informacinių išteklių skaičių, toks IT strateginis dokumentas ir jo pagrindu sukurtų IT plėtros planų įgyvendinimas padėtų susieti veiklos ir IT tikslus, užtikrinti skaidrų visų IT reikalingų išteklių planavimą, tvarkymą ir kontrolę, leistų pakylėti organizacijos IT valdymą į aukštesnį brandos lygį.

## 1.2. Informacinės architektūros nustatymas

Valdymo srities informacinė architektūra yra pagrindinis informacijos apie IT atitiktį vykdomos veiklos poreikiams šaltinis. COBIT metodikoje pažymėta[10], kad informacinės architektūros modelio parinkimas ir valdymas užtikrina sklandų programinės įrangos integravimą ir vadovybės

[8] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 9 str.

[9] COBIT 4.1, 2011 m., Vilnius, PO1 procesas, 29 psl.

[10] Ten pat, PO2 procesas, 33 psl.

sprendimams priimti reikalingos patikimos, nuoseklios ir išsamios informacijos teikimą. Institucija, nustatydama valdymo srities informacinę architektūrą, sudaro duomenų žodyną, kuriame nustatomos techninės sąlygos duomenims (kitaip – duomenų sintaksė), numato duomenų klasifikavimo schemą ir saugumo lygius. Tinkamai nustatyta informacinė architektūra sudaro galimybę racionaliai išnaudoti informacinius išteklius, juos maksimaliai lanksčiai derinti su vykdomos veiklos strategija. Taip stiprinamas atskaitingumas už duomenų vientisumą ir saugą, didinamas duomenų mainų tarp skirtingų IS efektyvumas ir kontrolė.

Policijos departamentas valdo atskirus žinybinius registrus, valstybės IS ir vidaus administravimo posistemius, kurie vidaus tvarkose[11], įsakymuose ir kt. dokumentuose įvardijami kaip informacinė sistema (POLIS), palaikanti pagrindinius Policijos departamento veiklos procesus. Toks POLIS sąvokos vartojimas dokumentuose yra klaidinantis, nes POLIS kaip IS nėra įsteigta ir įteisinta. IVPK dar 2011 m. atkreipė Policijos departamento dėmesį, kad jo valdomi registrai, IS ir posistemiai yra atskiri (savarankiški) objektai ir veikia pagal savo patvirtintus nuostatus, todėl bet koks registrų ar IS nurodymas sudedamosiomis POLIS dalimis yra netinkamas, nes Valstybės informacinių išteklių valdymo įstatymas reglamentuoja valstybės registrų, žinybinių registrų ir valstybės IS, o ne atskirų posistemių steigimą, kūrimą ir tvarkymą. Taigi departamentas turėtų peržiūrėti ir atnaujinti parengtas tvarkas ir atsisakyti POLIS sąvokos jose.

Pažymėtina, kad Policijos departamento 2015 metų veiklos plane numatyta įvertinti policijos sistemoje funkcionuojančias informacines sistemas bei galimybes jas integruoti į vieną informacinę sistemą su atskirais moduliais. Šios priemonės įtraukimas į veiklos planą nesuderintas su IT padaliniu, todėl nežinoma kokie priemonės įgyvendinimo tikslai, ar jos įgyvendinimas būtų įmanomas.

Valstybės informacinių išteklių valdymo įstatymas nustato[12], kad valstybės registras steigiamas tada, kai yra bent vienas šių pagrindų:

- registro objekto įregistravimo faktas yra reikalingas reguliuojant minėto įstatymo 17 straipsnio 1 dalyje nurodytus visuomeninius santykius valstybės mastu Lietuvos Respublikoje;
- registras yra sudedamoji Europos Sąjungos valstybėse narėse ar Europos ekonominės erdvės valstybėse tvarkomų registrų arba informacinių sistemų dalis;
- registro duomenys reikalingi kelių valdymo sričių Lietuvos Respublikos valstybės institucijoms ir valstybės įstaigoms teisės aktuose nustatytoms funkcijoms atlikti.

Policijos departamento valdomų registrų nuostatuose nustatyta, kad visi Policijos departamente įsteigti registrai yra žinybiniai, taigi registro duomenys reikalingi vienos valdymo srities Lietuvos Respublikos valstybės institucijoms ir valstybės įstaigoms teisės aktuose nustatytoms funkcijoms atlikti. Pastebėtina, kad PRĮR duomenys teikiami Lietuvos automobilių kelių direkcijai teisės aktuose numatytoms funkcijoms atlikti[13], o tai atitinka vieną iš Valstybės informacinių išteklių valdymo įstatyme numatytų pagrindų dėl valstybės registro įsteigimo. Įgyvendinant Valstybės informacinių išteklių valdymo įstatymą, Policijos departamentui reikėtų peržiūrėti visų valdomų registrų steigimo pagrindus ir esant poreikiui inicijuoti jų nuostatų pakeitimą.

Atsižvelgus į Policijos departamento valdomų valstybės informacinių išteklių įvairovę ir jų svarbą

[11] Lietuvos policijos generalinio policijos komisaro 2010-06-03 d. įsakymas Nr. 5-V-456 patvirtintas Grėsmių ir rizikų policijos informacinei sistemai analizavimo, stebėjimo ir vertinimo procedūrų aprašas.

[12] Valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 17 str. 2 d.

[13] Lietuvos Respublikos susisiekimo ministro 2006-11-30 įsakymu Nr. 3-457 patvirtinti Lietuvos automobilių kelių direkcijos prie Susisiekimo ministerijos nuostatai, 10.1.7. p.

(žr. 4 priedą), nustatyti informacinę architektūrą ypač svarbu, siekiant tinkamai juos valdyti, analizuoti ir modernizuoti. Departamentas neturi bendro savo valdomų informacinių sistemų ir registrų informacijos architektūros modelio, duomenų žodyno, o informacijos srautai tarp departamento valdomų IS ir registrų identifikuoti tik tam tikrų IS ir registrų nuostatuose ir techninėse specifikacijose. Auditoriai atkreipia dėmesį į tai, kad ne visi departamento valdomi registrai ir IS turi parengtas ir patvirtintas technines specifikacijas (žr. 3, 4 priedus). Departamentui aiškiai neaprašius turimų elektroninių duomenų srautų, duomenų struktūros, lieka neaiški informacinių išteklių tarpusavio sąveika, nesudaromos prielaidos IT ir veiklos naudotojų bendram supratimui apie duomenis ir tam, kad bus kuriami tik suderinami duomenų elementai ir nekaupiami pertekliniai duomenys.

Nustatyta, kad departamente ir policijos įstaigose trūksta valdomos informacijos klasifikavimo kriterijų / sistemos, atsižvelgiant į tokios informacijos jautrumą ir svarbą (pvz., konfidenciali, tarnybinio naudojimo ir pan.) (žr. 1.4 poskyrį). Siekiant išvengti galimų informacijos paviešinimo ir / ar perdavimo problemų, reikėtų detalizuoti departamento ir policijos įstaigų valdomos informacijos klasifikavimo kriterijus.

Pažymėtina, kad Policijos departamento Policijos informacijos valdyba 2012 m. numatė sudaryti policijoje naudojamų informacinių sistemų, registrų, posistemių ir kitos programinės įrangos sąsajų katalogą. Ši priemonė nebuvo įgyvendinta dėl žmogiškųjų išteklių stokos. Policijos departamento specialistų teigimu, toks katalogas palengvintų problemų sprendimą, ypač dėl darbuotojų kaitos, nes departamento analitikai bei IS ir registrų projektuotojai galėtų priimti sprendimus pagal dokumentaciją (detalizuotą programinės įrangos sąsajų katalogą) be sistemų administratorių pagalbos.

Atsižvelgiant į tai, kas išdėstyta, Policijos departamentui rekomenduotina sudaryti informacijos architektūros modelį: apibrėžti organizacijos informacijos, IS, duomenų ir technologinę architektūrą, nurodyti kiekvienos sudedamosios dalies komponentus (naudojamas technologijas, duomenis, jų srautus tarp išorinių ir vidinių IS ir kt.). Nustatęs architektūros modelį, suklasifikavęs visus valdomus ir tvarkomus duomenis pagal svarbą Policijos departamentas sukurtų aplinką, kurioje visiems be išimties informaciniams ištekliams būtų skiriamas reikiamas dėmesys, priimant tinkamus sprendimus dėl jų plėtros, kūrimo, priežiūros ir saugos užtikrinimo.

## 1.3. Sistemų saugos ir veiklos tęstinumo užtikrinimas

COBIT informacinių sistemų saugos užtikrinimo procesas [14] skirtas išlaikyti informacijos vientisumą ir išsaugoti turtą. Jis apima IT saugos funkcijas ir atsakomybę, politiką, standartų ir procedūrų nustatymą ir priežiūrą. Tinkamai valdomas procesas garantuoja ne tik IT saugą, jis sumažina galimų IT saugos incidentų poveikį pagrindinei įstaigos veiklai.

Lietuvos Respublikos teisės aktai nustato, kad IS ir registro valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus[15]:

- Saugos nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;

[14] COBIT 4.1, 2011 m., Vilnius, DS5 procesas, 117 psl.

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

- Informacinės sistemos veiklos tęstinumo valdymo planą;
- Informacinės sistemos naudotojų administravimo taisykles.

Vadovaudamasis Vyriausybės nutarimu[16], Policijos departamentas atnaujino ir patvirtino Policijos informacinių sistemų ir registrų duomenų saugos nuostatus[17], kurie įsigaliojo nuo 2015-07-01. Kiti trys saugos dokumentai iki nustatyto termino nebuvo atnaujinti, todėl departamentas, užtikrindamas duomenų saugą, vadovaujasi dokumentais, kuriuose yra neaktualių / negaliojančių nuostatų, dokumentai nesuderinti tarpusavyje, juose neatsispindi įvykę organizaciniai, teisiniai ir techniniai pokyčiai.

Įvertinus Policijos departamento valdomų informacinių sistemų saugą, nustatyta saugos reikalavimų įgyvendinimo trūkumų:

- Parengtos rizikos įvertinimo ataskaitos turi būti vertinamos ITKG[18]. Apie 2013 m. ir 2014 m. atliktą rizikos vertinimą tarnybiniu pranešimu informuotas Lietuvos policijos generalinis komisaras, bet ITKG posėdžiuose rizikos vertinimo ataskaitos nesvarstytos, todėl nesiimta tinkamų veiksmų nustatytai rizikai valdyti, neapsvarstyti rizikų valdymo būdai.
- Policijos departamentas 2012–2014 m. saugos atitikties vertinimą atliko tik 2014 metais ir įvertino saugos nuostatų ir saugos politiką įgyvendinančių teisės aktų atitiktį realiai saugos situacijai, bet netikrino naudotojams suteiktų teisių ir vykdomų funkcijų atitikties. Auditoriai nustatė pavyzdžių, kai suteiktos prieigos prie IS teisės neatitinka darbuotojų vykdomų funkcijų (žr. 3 pavyzdį). Neatlikus saugos atitikties vertinimo departamento vadovybė negauna išsamios ir periodiškos informacijos apie faktinę IT saugos būklę prieš priimdama sprendimus dėl IT plėtros ar saugos priemonių įsigijimo.

**3 pavyzdys**

Klaipėdos apskrities vyriausiojo policijos komisariato Imuniteto skyrius 2014-05-19 tarnybiniu pranešimu Nr. 30-20-PR5-71 informavo Klaipėdos apskrities vyriausiojo policijos komisariato viršininką, kad, išanalizavus VPVS naudotojų sąrašą, nustatyta, kad kai kurių pareigūnų, besinaudojančių VPVS, atliekamos funkcijos neatitinka VPVS paskirties, ne visi sąraše nurodyti pareigūnai atlieka funkcijas, susijusias su pajėgų kontrole ir operatyviu pajėgų valdymo užtikrinimu. Atsižvelgiant į tai rekomenduota peržiūrėti komisariato padalinių pareigūnų, kuriems suteikta teisė naudotis VPVS, sąrašus ir įvertinti kiekvieno jų tarnybinių funkcijų atitiktį būtinumui naudotis VPVS. Taip pat suteikiant teises naudotis ja naujiems darbuotojams, griežtai vertinti tarnybinio būtinumo kriterijų.

Policijos informacijos valdybos Sistemų administravimo skyriaus viršininko pavaduotojas turėjo daugiau prieigos teisių prie Policijos departamento IS ir registrų, nei jų fiksuota šio darbuotojo prieigos prašymo formoje, kuri pildoma atsižvelgiant į pareigybės aprašyme numatytas vykdyti funkcijas prieš suteikiant teisę dirbti su IS ir registrais.

- Policijos departamento valdomų registrų ir IS (PRĮR, ATPEĮR, IGR, ITPR, INDR, PLV IS, PVVIS) duomenų kopijos saugomos toje pačioje patalpoje kaip ir tarnybinės stotys, o ši patalpa neturi automatinės gaisro gesinimo sistemos. Tokiomis aplinkybėmis yra labai didelė tikimybė, kad saugos incidento atveju (pvz., gaisras ar kt. ekstremali situacija) ne tik bus negrįžtamai sugadinta techninė ir programinė tarnybinių stočių įranga, prarasti aktyviose IS duomenų

[16] Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 2 p.

[17] Patvirtinta Lietuvos policijos generalinio komisaro 2015-02- 17 d. įsakymu Nr. 5-V-165.

[18] Lietuvos policijos generalinio komisaro 2010-04-03 įsakymu Nr. 5-V-456 patvirtintas Galimų grėsmių ir rizikų policijos IS analizavimo, stebėjimo ir vertinimo procedūrų aprašas, 14 p.

bazėse esantys duomenys, tačiau prarastos (sunaikintos) ir duomenų kopijos, todėl po IT išteklių praradimo (kurį gali nulemti gamtos nelaimės, nelaimingi atsitikimai, įrangos gedimai ir pan.) Policijos departamento veikla nebus atkurta iki priimtino lygio.

- Departamento ir policijos įstaigų IS ir registrų naudotojai administruojami naudojant ADMIN III įrankį, o prisijungimo prie IS ir registrų slaptažodžiai generuojami pagal IRD nustatytas taisykles. Slaptažodžių kompleksiškumo reikalavimai neužtikrinami technologinėmis priemonėmis (žr. 3 priedą). Audito metu nustatyti atvejai, kai policijos įstaigų darbuotojai slaptažodžius užsirašydavo ant lapelių ir laikė juos matomoje vietoje, todėl yra galimybė pasinaudojus duomenimis atlikti neteisėtus veiksmus kompiuterinėje darbo vietoje.
- 2013 m. atliekant IS rizikos vertinimą pastebėta, kad darbuotojai, tvarkydami asmens duomenis, padaro pažeidimus ne piktavališkai tikslais, o dėl kompiuterinio raštingumo arba duomenų tvarkymo reikalavimų išmanymo trūkumo, tačiau darbuotojų mokymai duomenų tvarkymo teisėtumo ir informacijos saugos klausimais neorganizuoti.
- Policijos departamento veiklos tęstinumo valdymo plano veiksmingumas nebuvo išbandytas, todėl departamentas neįsitikino, ar yra pasiruošęs atkurti valdomų IS per laikotarpį, kuris neturėtų neigiamos įtakos Policijos departamento ir kitų institucijų funkcijų įgyvendinimui (žr. 4 pavyzdį).

**4 pavyzdys**

2014 m. liepos 29 d. sutriko departamento valdomų informacinių sistemų ir registrų duomenų bazių veikla. Remiantis departamento pateiktais duomenimis (monitoringo sistemos „Zabbix“ http://www.zabbix.com/ įrašais), departamento IS ir registrai neveikė 12 val. (nuo 1 val. iki 13 val.). Saugaus elektroninės informacijos tvarkymo taisyklėse, pagal tvarkomos informacijos svarbą užtikrinant policijos įstaigoms pavestų funkcijų vykdymą, departamentas yra apsibrėžęs sąrašą kritinių IS, sudarančių problemų veiklai, kai jos nefunkcionuoja ilgiau nei 4 val. Atsižvelgiant į neveikimo laikotarpį, darytina išvada, kad departamento valdomi IS ir registrai nebuvo laiku atkurti. Pastebėtina, kad pagal sudarytas duomenų teikimo sutartis valstybės įmonė „Regitra“ automatiniu būdu gauna departamento valdomų Administracinių teisių pažeidimų ir eismo įvykių registro (nuo 2015-07-01 registro valdytojas Vidaus reikalų ministerija) ir Ieškomų transporto priemonių registrų duomenis. Valstybės įmonė „Regitra“, sutrikus minėtų registrų duomenų teikimui, negalėjo įprastine, nustatyta tvarka atlikti jai pavestų funkcijų (vairuotojo pažymėjimo užsakymo įteikimo pareiškėjui). Įmonė duomenų patikrinimą susijusiuose registruose ir procedūros pabaigą turėjo atidėti iki tol, kol bus atnaujinta registrų sąsaja. VĮ „Regitra“ pateiktais duomenimis, panašūs departamento registrų sutrikimai buvo užfiksuoti ir anksčiau.

Siekdamas užtikrinti tinkamą IT rizikų valdymą, Policijos departamentas turėtų tobulinti rizikos veiksnių nustatymo procesą, vertinant ir aptariant nustatytas rizikas – laikytis Policijos departamente dokumentuotos galimų grėsmių ir rizikų policijos IS analizavimo, stebėjimo tvarkos bei užtikrinti nustatytos rizikos mažinimo priemonių įgyvendinimą.

Policijos departamentas turėtų užtikrinti informacinių išteklių apsaugą, įgyvendindamas teisės aktų reikalavimus, šalindamas IT saugos trūkumus ir organizuodamas informacijos saugos mokymus.

## 1.4. Duomenų valdymas

COBIT Duomenų valdymo procesas[19] apibrėžia, kad, norint efektyviai valdyti duomenis, reikia nustatyti jų valdymo reikalavimus. Duomenų valdymo procesas skirtas nustatyti efektyvias laikmenų bibliotekos, duomenų atsarginių kopijų darymo, duomenų atkūrimo ir tinkamo laikmenų sunaikinimo valdymo procedūras. Efektyvus duomenų valdymas padeda užtikrinti veiklos duomenų kokybę, aktualumą ir prieinamumą.

Teisės aktai nustato šiuos elektroninės informacijos srautų valdymo reikalavimus:

- El. informacija klasifikuojama pagal svarbą[20], 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[21]. Nustatyta el. informacijos svarbos kategorija nurodoma IS ar registro duomenų saugos nuostatuose[22].
- IS ar registro kategorija nustatoma pagal juose apdorojamos el. informacijos svarbos kategoriją ir nurodoma duomenų saugos nuostatuose[23]. Techninės apsaugos priemonės parenkamos pagal informacinių išteklių kategoriją[24].

Atsižvelgiant į Policijos departamento IS ir registrų duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) įtaką policijos veiklai, departamento IS ir registruose saugoma informacija suskirstyta į kategorijas taip, kaip nustato teisės aktai[25]. Taip pat nustatyta, kad Policijos departamento IS ir registruose tvarkomi duomenys, išskyrus statistinius, priskiriami prie viešai neskelbtinos informacijos[26] ir negali būti viešai skelbiami[27]. Toks klasifikavimas apima tik el. informaciją. Jis neapima informacijos, kurią sukuria, gauna ir savo veikloje naudoja Policijos departamentas ir policijos įstaigos (pvz., planai, darbiniai dokumentai, testavimo ataskaitos, saugos projekto metu naudojama informacija, sutartys, IS projektinė dokumentacija, rizikos vertinimo ataskaitos informacija ir pan.). Pastaroji informacija nėra klasifikuota atsižvelgiant į jos jautrumą praradimui ir atskleidimui.

Klasifikavimas, atsižvelgiant į informacijos galimo atskleidimo ar praradimo pavojaus laipsnį, padėtų departamentui nustatyti, kokia informacija yra jautriausia ir būtiniausia (vertingiausia) institucijai ir užtikrinti jos konfidencialumą ir prieinamumą, kad svarbi ir konfidenciali informacija

[19] COBIT 4.1, 2011 m., Vilnius, DS11 procesas, 141 psl.

[20] 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 p.

[21] Ten pat, 3 p.

[22] Ten pat, 7 p.

[23] Ten pat, 6 p.

[24] 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.

[25] 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.

[26] Viešai neskelbtina informacija – informacija, kurios praradimas arba neteisėtas atskleidimas gali pakenkti policijos interesams ir reputacijai, sutrikdyti policijos įstaigoms vykdyti joms pavestas funkcijas arba sudaryti prielaidas neteisėtam tarnybos paslaptį sudarančios informacijos atskleidimui.

[27] Lietuvos policijos generalinio komisaro 2008-10-02 įsakymu Nr. 5-V-584 patvirtintos Saugaus policijos informacinės sistemos žinybinių registrų ir posistemių elektroninės informacijos tvarkymo taisyklės, 4 p.

nepatektų tiems, kas neturi jos gauti. Pažymėtina, kad informacijos klases įvardyti ir informaciją klasifikuoti turėtų duomenų valdymo įgaliotiniai, tiesiogiai atsakingi už duomenų valdymą.
2012 m. patvirtinta kovos su korupcija policijoje 2012–2014 metų programa ir jos įgyvendinimo priemonių planas[28], kuriame numatyta vykdyti pavaldžių policijos darbuotojų duomenų tvarkymo atvejų VRIS CDB, POLIS bei OIS teisėtumo ir pagrįstumo patikrinimus. Šios priemonės vykdytojais paskirta Policijos informacijos valdyba ir visos policijos įstaigos, kurios per metus pasirinktinai turi patikrinti 15 proc. kiekvieno padalinio policijos darbuotojų, tikrinant jų prisijungimo teisėtumą.

Nustatėme, kad Policijos departamentas ir teritorinės policijos įstaigos periodiškai atlieka darbuotojų duomenų tvarkymo VRIS CDB, POLIS teisėtumo ir pagrįstumo patikrinimus, bendradarbiauja su Valstybine duomenų apsaugos inspekcija. Esant neteisėto duomenų tvarkymo atvejams, pradedamas tarnybinis patikrinimas, administracinė teisena ar ikiteisminis tyrimas. Neteisėto policijos duomenų bazių naudojimo rizika nepakankamai valdoma Lietuvos kriminalinės policijos biure (žr. 5 pavyzdį).

**5 pavyzdys**

Policijos departamento Štabas per tikslinį patikrinimą nustatė, kad 2012–2014 m. Lietuvos kriminalinės policijos biuras VRIS CDB, POLIS, OIS teisėtumo ir pagrįstumo patikrinimų neatliko. Atsižvelgiant į Štabo ataskaitoje pateiktus pastebėjimus, Lietuvos kriminalinės policijos biuras 2014 m. pabaigoje atliko VRIS CDB, POLIS teisėtumo ir pagrįstumo patikrinimus, bet OIS patikrinimų pagal kovos su korupcija policijoje 2012-2014 metų programos įgyvendinimo priemonių planą neatliko.

Lietuvos kriminalinės policijos biuras atkreipė auditorių dėmesį, kad Lietuvos policijos generalinio komisaro 2015-07-07 patvirtintas planas[29] pagal kurį bus atliekama OIS naudotojų kontrolė ir patikrinta ne mažiau kaip 15 proc. kiekvieno padalinio darbuotojų, t. y. ar darbuotojai naudojo OIS teisės aktų nustatyta tvarka.

Policijos departamento IS ir registrų duomenų kopijos daromos periodiškai, kas tris dienas kopijuojami visi duomenų bazės įrašai, todėl duomenų kopija užima daugiau nei 2 TB. Policijos departamento duomenų saugos nuostatuose numatyta, kad periodiškai (ne rečiau kaip kartą į metus) turi būti bandoma atkurti duomenis iš atsarginių duomenų kopijų, bet Policijos departamentas neturi techninių sąlygų ir reikiamos infrastruktūros tokiems bandymams atlikti, todėl neįsitikina, kad, esant incidentui, IS ir registrų duomenys bus sėkmingai atstatyti, o IS ir registrų veikla atkurta per teisės aktuose numatytą laiką.

Siekdamas užtikrinti tinkamą valdomų registrų ir IS duomenų apsaugą, departamentas turėtų suderinti atsarginių duomenų kopijų atkūrimo tvarką ir planuojamus darbus su Vidaus reikalų ministerija, atsižvelgdamas į Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašą[30].

Lietuvos Respublikos teisės aktai nustato asmens duomenų tvarkymo ir valdymo reikalavimus:

- asmens duomenys gali būti tvarkomi automatiniu būdu tik tuo atveju, kai duomenų valdytojas arba jo atstovas Vyriausybės nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai[31].

[28] Lietuvos policijos generalinio komisaro 2012-06-07 įsakymu Nr. 5-V-447 patvirtinta Kovos su korupcija policijoje 2012–2014 metų programa ir kovos su korupcija policijoje 2012–2014 metų programos įgyvendinimo priemonių planas.
[29] Lietuvos policijos generalinio komisaro 2015-07-07 įsakymas Nr. 5-V-634 „Dėl kovos su korupcija policijoje 2015–2017 metų programos ir jos įgyvendinimo priemonių plano patvirtinimo".
[30] Lietuvos Respublikos Vyriausybės 2015-05-13 nutarimu Nr. 498 patvirtintas Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašas.
[31] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374, 31 str.

- asmens duomenų valdytojas privalo įgyvendinti tinkamas organizacines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo[32].
- asmens duomenų valdytojas turi turėti patvirtintą rašytinės formos dokumentą, kuris atitiktų teisės norminiame akte numatytus turinio reikalavimus[33].

Policijos departamento IS ir registruose tvarkomi ypatingi asmens duomenys, o atsižvelgiant į asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, Policijos departamento IS ir registruose tvarkomi asmens duomenys priskiriami antrajam ir trečiajam saugumo lygiui. Vertinant asmens duomenų valdymo procedūras buvo nustatyta, kad departamentas neįgyvendina techninių ir organizacinių asmens duomenų saugumo priemonių tvarkant duomenis automatizuotu būdu (žr. 3 priedą), todėl neužtikrinama asmens duomenų apsauga nuo atsitiktinio ar neteisėto sunaikinimo, atskleidimo.

Siekdamas užtikrinti tvarkomų asmens duomenų apsaugą, departamentas turėtų įgyvendinti technines ir organizacines asmens duomenų saugumo priemones.

## 1.5. Įslaptintos elektroninės informacijos valdymas

Išvados ir rekomendacijos dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta).

## 1.6. Pokyčių valdymas

COBIT Pokyčių valdymo procesas[34] rekomenduoja, kad visi pokyčiai, įskaitant ir avarinę priežiūrą ir pataisas, susijusias su infrastruktūra ir taikomosiomis programomis darbinėje aplinkoje, būtų standartizuotai valdomi ir kontroliuojami. Pokyčių (procedūrų, procesų, sistemų ir paslaugų parametrų) valdymas ir kontrolė įgyvendinama juos registruojant, vertinant, prieš vykdant jiems išduodami leidimai, o po įgyvendinimo jie peržiūrimi ir lyginami su planuotais rezultatais. Tai užtikrina pokyčių neigiamo poveikio informacinių sistemų stabilumui ar vientisumui rizikos mažinimą.

Lietuvos Respublikos teisės aktai nustato šiuos informacinių sistemų funkcijų pokyčių reikalavimus:

- IS valdytojas turi užtikrinti efektyvų ir spartų informacinės sistemos funkcijų pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas, įtakos vertinimą ir pokyčių prioritetų nustatymo procesus[35].
- Visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su IS valdytojo vadovu ar duomenų valdymo įgaliotiniu ir vykdomi tik gavus jų raštišką pritarimą[36].
- Atlikdami informacinės sistemos funkcijų pakeitimus, administratoriai turi laikytis

[32] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374, 30 str. 1 d.

[33] Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008-11-12 įsakymu Nr. 1T-71(1.12) patvirtinti Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, 8–8.15 p.

[34] COBIT 4.1, 2011, Vilnius, AI6 procesas, 93 psl.

[35] Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 39 p. ir 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemos reikalavimai (neteko galios 2013-08-08), 33 p.

[36] Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 40 p. ir 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemos reikalavimai (neteko galios 2013-08-08), 34 p.

informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos, nustatytos Saugaus elektroninės informacijos tvarkymo taisyklėse[37].

Išanalizavus Policijos departamento įgyvendinamas pokyčių valdymo procedūras nustatyta, kad departamento praktikoje yra nusistovėjęs pokyčių valdymo procesas, bet jis tobulintinas dėl nustatytų IT pokyčių valdymo trūkumų:

- departamentas neturi patvirtintos IT pokyčių valdymo tvarkos ar kito dokumento, kuriame būtų detaliai išdėstytos pokyčių planavimo ir valdymo nuostatos. Patvirtintose Saugaus elektroninės informacijos tvarkymo taisyklėse neišdėstytos teisės aktuose reikalaujamos nuostatos, susijusios su IS pokyčių planavimu, apimant pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą ir pokyčių prioritetų nustatymo procesus;
- nėra priimtas sprendimas dėl standartizuoto IT pokyčių užsakymo, pagrindžiant pokyčio reikalingumą ir naudą, nurodant pokyčio prioritetą. Vieni policijos veiklos padaliniai inicijuodami pokytį išsamiai pagrindžia IT pokyčio reikalingumą ir naudą, kiti – ne, todėl eikvojami papildomi laiko ištekliai vertinant ir apibendrinant pateikto pokyčio tikslingumą ir pagrįstumą (žr. 6 pavyzdį). Ne visi IT pokyčiai yra sistemingai užregistruojami, suskirstant juos į kategorijas pagal pokyčio tipus, todėl lieka neįvertinta pokyčio įtaka IS ir registrų funkcionavimo stabilumui, jų eksploatavimui ir departamento veiklai (žr. 2.1 poskyrį).

**6 pavyzdys**

Policijos departamentas 2014-04-02 raštu Nr. 5-S-1163 „Dėl duomenų valdymo įgaliotinio“ atkreipė policijos įstaigų dėmesį į susidariusias programinės įrangos pakeitimų problemas, kurios turi įtakos operatyvių sprendimų priėmimui ir paprašė nurodyti atsakingus darbuotojus, kurie siūlytų programinės įrangos pakeitimus, analizuotų informaciją apie kitų įstaigų naudotojų pateiktą pakeitimų poreikį, nustatytų jų prioritetus, konsultuotų Policijos informacijos valdybos darbuotojus, analizuotų naudotojų pranešimus apie programinės įrangos klaidas ar nekorektiškus duomenis.

Išanalizavę policijos įstaigų pateiktus raštus ir kitus duomenis nustatėme, kad asmenys, atsakingi už programinės įrangos pakeitimų siūlymus, kitų naudotojų pateiktų poreikių analizę, prioritetų nustatymą, buvo paskirti ne visoms Policijos departamento valdomoms IS ir registrams, daliai IS ir registrų tokie asmenys paskirti tik audito metu po auditorių užklausimo.

Siekdamas sistemingo pokyčių valdymo, Policijos departamentas turėtų peržiūrėti taikomą pokyčių valdymo procesą ir nustatyti (patvirtinti) IT pokyčių valdymo tvarką, kurioje būtų išdėstytos IT pokyčių valdymo planavimo nuostatos dėl jų identifikavimo, suskirstymo į kategorijas pagal tipą, prioritetų nustatymo ir įtakos vertinimo procesų, be to, būtina užtikrinti šios tvarkos laikymosi (vykdymo) kontrolę.

## 1.7. Vidaus kontrolės stebėsena ir vertinimas

COBIT vidaus kontrolės stebėsenos ir vertinimo procesas[38] nurodo, jog efektyviam IT veiklos valdymui reikalinga nustatyti tinkamus veiklos rodiklius, sistemingai ir laiku atlikti veiklos stebėseną ir operatyviai reaguoti, esant nuokrypių. Stebėsena reikalinga siekiant užtikrinti, kad būtų taikomos tinkamos ir nustatytas kryptis ir politiką atitinkančios priemonės. Rekomenduojama nuolat vertinti

[37] Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 28 p. ir 1997-09-04 nutarimu Nr. 952 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemos reikalavimai (neteko galios 2013-08-08), 21 p.

[38] COBIT 4.1, 2011 m., Vilnius, ME2 procesas, 157 psl.

visus IS procesus ir jų atitiktį vidaus kontrolės reikalavimams. Vertinimas turėtų apimti efektyvumo valdymą, vidaus kontrolės sistemos stebėjimą, atitiktį teisinio reguliavimo ir valdymo reikalavimams.

Lietuvos Respublikos teisės aktai nustato, kad:

- vienas vidaus audito uždavinių – ne rečiau kaip vieną kartą per trejus metus įvertinti, kaip vidaus kontrolė veikia viešajame juridiniame asmenyje; [39]
- Pavyzdinėje vidaus audito metodikoje[40] rekomenduota, kad vidaus auditorius, atlikdamas vidaus auditą, turi tikrinti ir vertinti ir taikomosios IS kontrolės priemones, atlikti jų testavimą pagal vidaus auditoriaus parengtus šių kontrolės priemonių tikrinimo klausimynus.

Policijos departamento Centralizuoto vidaus audito skyriaus nuostatuose[41] nurodyta, kad skyrius turi tikrinti ir vertinti informacinių sistemų valdymą ir naudojimą. Per 2012–2014 metus skyrius neatliko nė vieno audito, kurio objektas būtų informacinės sistemos, jų saugos, bendrosios kontrolės ar kito IS / IT aspekto vertinimas, todėl departamento vadovybė neturi duomenų apie IT procesų efektyvumą, atitiktį veiklos reikalavimams, nenustatomos IT kontrolės trūkumai ir spragos, nesilaikoma teisės aktų reikalavimų (žr. 7 pavyzdį, 3 priedą).

**7 pavyzdys**

2014-07-18 „Microsoft Ireland Operations Limited“ pagal programinės įrangos nuomos sutartyje numatytas sąlygas pradėjo auditą (atliko nepriklausomi auditoriai), siekdamas nustatyti, kokias „Microsoft“ licencijas naudoja Policijos departamentas. Nustatyta, kad departamento infrastruktūroje 62 proc. programinės įrangos nelicencijuota. Konkretūs programinės įrangos produktai, kurie buvo rasti, įdiegti ir naudojami be atitinkamos licencijos, pateikti departamentui 2014-12-16 raštu. Nurodyta, kad departamentas turi įsigyti trūkstamas licencijas ir padengti 40 tūkst. Eur audito mokestį, nes pagal „Microsoft“ verslo paslaugų sutartį („Microsoft Business and Service Agreement“) tikrinimo išlaidos turi būti atlyginamos, jei licencijų trūkumai viršija 5 proc.

2015-05-13 ITKG svarstė klausimą dėl „Microsoft“ programinės įrangos licencijavimo ir kompiuterinių darbo vietų optimizavimo. Nutarta pavesti Policijos informacijos valdybai iki 2015 m. spalio mėn. parengti policijos kompiuterizuotų darbo vietų, kurioms yra reikalingos „Microsoft“ licencijos, optimizavimo pasiūlymą, siekiant mažinti licencijų nuomai skiriamus asignavimus, ir pateikti šio tikslo įgyvendinimo priemonių planą.

Policijos departamente 2013 m. buvo atliekami išoriniai IT saugos ir pažeidžiamumo auditai, rasta trūkumų ir pateikta rekomendacijų. Audito metu rekomendacijos buvo įgyvendinamos.

Siekiant užtikrinti IS veiklos rezultatyvumą ir efektyvumą bei atitiktį teisės aktų reikalavimams, turėtų būti vykdoma vidaus kontrolės stebėsena: vidaus auditoriai turi tikrinti ir vertinti bendrosios IS kontrolės priemones, IS ir registrų valdymą ir naudojimą.

## 1.8. IT valdymo užtikrinimas ir brandos vertinimas

COBIT IT valdymo užtikrinimo procesas nurodo[42], kad rezultatyviai valdymo sistemai sukurti reikia tinkamai apibrėžti organizacijos struktūras, procesus, vadovavimą, funkcijas ir pareigas, užtikrinti, kad organizacija investuotų į IT suderintai su organizacijos strategija ir tikslais. COBIT strateginio IT plano apibrėžimo procesas nurodo, kad planas reikalingas norint valdyti ir

[39] 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.

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

[41] Lietuvos policijos generalinio komisaro 2013-02-26 įsakymu Nr. 5-V-167 patvirtinti Centralizuoto vidaus audito skyriaus nuostatai.

[42] COBIT 4.1, 2011 m., Vilnius, ME4 procesas, 165 psl.

nukreipti visus IT išteklius pagal veiklos strategiją ir prioritetus.

Policijos departamente ir policijos įstaigose sudarytos grupės ir komisijos[43], kurioms pavesta nustatyti IT vystymo kryptis, organizuoti, koordinuoti ir kontroliuoti IT plėtros darbus. Į grupių / komisijų sudėtį įeina departamento ir policijos įstaigų veiklos ir IT padalinių atstovai, todėl sudaromos sąlygos susitarti dėl galimybės geriau panaudoti IT veiklos procesams automatizuoti. Nustatyta, kad ne visos grupės ir komisijos vykdo veiklą ir pavestas funkcijas visa apimtimi, pvz., nerengiama IT strategija (žr. 1.1 poskyrį), nustatytu periodiškumu neaptariami ir nesvarstomi IT saugos klausimai ir informacinėms vertybėms kylančios grėsmės (žr. 1.5 poskyrį), neaptariama IS ir registrų programinės įrangos projektų vykdymo būklė ir eiga (žr. 2.1 poskyrį), nuo 2012 m. nebuvo išspręsti aktualūs IT klausimai (žr. 8 pavyzdį), todėl neužtikrinama tinkama IT įgyvendinimo kontrolė.

**8 pavyzdys**

Atsižvelgiant į 2009-04-06 Tarybos sprendimą 2009/371/TVR, numatyta tvarka[44], kokie duomenys kompetentingų institucijų perduodami į Europolo IS ir tai, kad duomenys į Europolo IS iš Operatyvinės IS (pertvarkoma į KŽIS) teikiami automatiniu būdu per Europolo Lietuvos nacionalinį skyrių.

2012-12-04 pasitarimo pas Lietuvos kriminalinės policijos biuro viršininką dėl duomenų teikimo Europolo IS protokole atkreiptas dėmesys į nepakankamą Lietuvos policijos generalinio komisaro 2011 m. sausio 3 d. įsakymo Nr. 5-V(S)-1(RN) „Dėl operatyvinės informacinės sistemos duomenų perdavimo Europolui ir jų įslaptinimo“ vykdymą. Nuspręsta iki 2013-01-15 išspręsti technines problemas, trukdančias automatiniu būdu teikti duomenis į Europolo IS. Iki numatytos datos problemos neišspręstos, o į Lietuvos kriminalinės policijos biuro metinį veiklos planą minėta priemonė įtraukta tik 2014 m., tačiau ji nebuvo įgyvendinta, jos vykdymas perkeltas į 2015 m.

2014 m. lapkričio mėn. ir pakartotinai 2015 m. liepos mėn. Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdybos viršininkas tarnybiniu pranešimu informavo Lietuvos kriminalinės policijos biuro viršininką apie susidariusią padėtį. Nepaisant to, kad tarnybiniuose pranešimuose pasiūlyta įpareigoti Lietuvos kriminalinės policijos biuro Informacinių technologijų valdybą padaryti reikiamus pakeitimus KŽIS, įdiegti ir prižiūrėti programinį mechanizmą, kad būtų užtikrintas automatinis duomenų teikimas į Europolo IS, reikiamų veiksmų nesiimta. Duomenys Europolui teikiami rankiniu būdu. Taigi Lietuva patenka tarp šalių, kurių teikiamų duomenų kiekis yra labai mažas ir tai nuolat nurodoma Europolo pateikiamose ataskaitose ir susitikimuose.

Nerengiamos ir Lietuvos policijos generaliniam komisarui neteikiamos metinės ITKG atlikto darbo ataskaitos, taigi nesilaikoma ITKG nuostatų, todėl departamento vadovybė neturi bendros susistemintos informacijos apie posėdžiuose priimtus sprendimus, IT būklės pasikeitimus departamente ir policijos įstaigose.

COBIT metodika, siekiant užtikrinti aiškų veiklos vertinimą, rekomenduoja[45] sukurti aiškias funkcijas ir nustatyti atsakomybes.

Auditoriai nustatė, kad departamente sudarytų SPG[46] ir ITKG 2012-2014 m. laikotarpiu vykdytos

[43] Lietuvos policijos kriminalistinių tyrimo centro viršininko 2010-01-06 įsakymas Nr. 140-V-2 „Dėl informacinių technologijų vystymo ir plėtros komisijos sudarymo“, Lietuvos policijos generalinio komisaro 2007-11-26 įsakymas Nr. 5-V-781 „Dėl policijos informacinių technologijų koordinavimo grupės sudarymo ir jos nuostatų patvirtinimo“, Lietuvos kriminalinės policijos biuro viršininko 2011-12-27 įsakymas Nr. 38-V-216 „Dėl Lietuvos kriminalinės policijos biuro informacinių technologijų koordinavimo darbo grupės sudarymo“.

[44] Lietuvos policijos generalinio komisaro 2009-12-29 įsakymu Nr. 5-V-984 patvirtinta Lietuvos teisėsaugos institucijų ir Europos policijos biuro (Europolo) bendradarbiavimo aprašas, VIII skirsnis.

[45] COBIT 5, 2013 m., Vilnius, Organizacijos IT valdymo ir vadovavimo metodika,70 psl.

funkcijos persidengė ir nebuvo aiškiai atskirtos. Abi grupės sprendžia klausimus dėl investicinių lėšų paskirstymo IT plėtrai, IT priemonių įsigijimo ar jų tobulinimo.

Nustatyta Policijos departamento IT ir veiklos padalinių glaudaus bendradarbiavimo stoka, todėl susijusios institucijos neturi tikslios informacijos apie valstybės informacinių išteklių funkcinį suderinamumą, kūrimą, tvarkymą ir plėtrą, o VPVS projektą koordinuojanti institucija – tikslių projekto įgyvendinimo rezultatų (žr. 9 pavyzdį). 2014 m. atlikusios policijos strateginio ir pokyčių valdymo analizę tą patį patvirtino trečiosios šalys ir nustatė, kad IT ir funkcinių (veiklos) padalinių bendradarbiavimo lygis žemas, bendradarbiavimas formalizuotas ir numatytas tik tam tikrose veiklos srityse (pvz., konkrečių projektų ar sistemų veiklos apimtyje).

**9 pavyzdys**

Vykdant LR finansų ministro 2009-02-13 įsakymą Nr. 1K-037 ir atsiskaitant už informacinės visuomenės plėtros investicijų projektų lėšų panaudojimo rezultatus, 2014 m. ir 2015 m. IVPK buvo pateikta klaidinanti ar netiksli informacija: nurodyta, kad planuotos IT plėtros priemonės buvo įgyvendintos, o jos įgyvendintos nebuvo arba Policijos departamente buvo priimtas sprendimas įgyvendinimo atsisakyti, o lėšas panaudoti kitiems IT plėtros poreikiams. Ataskaitas dėl informacinės visuomenės plėtros investicijų projektų įgyvendinimo rengia Investicijų planavimo ir techninės plėtros valdybos skyrius, o investicijų projekte numatytas priemones įgyvendina Policijos departamento ar policijos įstaigų IT padaliniai.

Galutinėje VPVS projekto įgyvendinimo ataskaitoje, kurią parengė Policijos departamento Investicijų planavimo ir techninės plėtros valdybos skyrius, nurodyta, kad sukurtas ir dokumentuotas standartizuotos VPVS sąsajos su įvairių gamintojų telemetrine įranga modulis, tačiau šio projekto įgyvendinimo metu buvo sukurta tik sąsajos dokumentacija.

Atsižvelgiant į COBIT rekomenduojamas IT strategijos komiteto ir IT valdymo komiteto funkcijas, reikėtų peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių veiklą, atskirti jų funkcijas ir užtikrinti grupių veiklos tęstinumą, pavestų funkcijų vykdymą, siekiant aiškios atsakomybės už strateginius sprendimus ir tinkamo požiūrio į IT valdymą.

Policijos departamento IS vidaus kontrolės branda įvertinta taikant Gebos brandos modelį (*angl. Capability Maturity Model, CMM*). IS brandos vertinimo kriterijai pateikti 5 priede. Atsižvelgiant į ataskaitoje pateiktus faktus nustatyta, kad Policijos departamento IS vidaus kontrolės branda apibrėžiama kaip Pirminis/Ad Hoc procesas (žr. 2 pav.).

**2 pav.** Policijos departamento IS vidaus kontrolės brandos lygis

| | (a) | (b) | c) | (d) | *CM* |
|---|---|---|---|---|---|
| Optimalus procesas (5) | ✗ | ✗ | ✗ | ✗ | ◆ |
| Lengvai valdomas ir vertinamas procesas (4) | ✗ | ✗ | ✗ | ✗ | ◆ |
| Apibrėžtas procesas (3) | ✗ | ✗ | ✗ | ✗ | ◆ |
| Pasikartojantis, bet intuityvus procesas (2) | ! | ! | ✓ | ! | ▲ |
| Pirminis/Ad Hoc procesas (1) | ✓ | ✓ | ✓ | ✓ | ● |
| Negzistuojantis procesa 0) | ✓ | ✓ | ✓ | ✓ | ● |

✗ – neatitinka kriterijų
! – ne visiškai atitinka kriterijų
✓ – atitinka kriterijų
◆ – nepasiektas tam tikras gebos bandos lygis
▲ – nevisiškai pasiektas gebos brandos lygis
● – pasiektas tam tikras gebos brandos lygis

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

Šaltinis – Valstybės kontrolė

[46] Lietuvos policijos generalinio komisaro 2010-08-20 įsakymu Nr. 5-V-655 patvirtintas Strateginio planavimo darbo grupės sudėtis ir darbo reglamentas.

Norėdamas pasiekti aukštesnį brandos lygį Policijos departamentas turėtų peržiūrėti sudarytų IT komisijų, grupių ir kitų su IT susijusių struktūrų (pvz., strateginio planavimo grupės) veiklą, aiškiai atskirti šių grupių funkcijas ir užtikrinti jų veiklos tęstinumą, atskaitomybę Lietuvos policijos generaliniam komisarui ir pavestų funkcijų vykdymą. Turi būti parengta IT strategija, jos pagrindu sukurti, nuolatos peržiūrimi ir atnaujinami IT plėtros planai. Esama IS saugą apibrėžianti dokumentacija turi būti nuolatos atnaujinama ir atitikti realią situaciją, užtikrintas efektyvus IS rizikos nustatymo ir jos mažinimo, pokyčių valdymo procesas, užtikrinama vykdomų procesų stebėsena ir IT vidaus kontrolės vertinimas.

## 2. VIENINGOS PAJĖGŲ VALDYMO SISTEMOS KŪRIMO KONTROLĖ

Siekiant automatizuoti policijos įstaigų ir VSAT, PAGD, VST ir joms pavaldžių įstaigų pajėgų valdymo procesus ir užtikrinti jų greitą reagavimą į įvykį, 2009 metais Policijos pajėgų valdymo sistemos pagrindu buvo sukurta Vieninga pajėgų valdymo sistema. Jos kūrimo pagrindas – Europos Komisijos 2008 m. gruodžio 19 d. sprendimas Nr. K(2008)8460, kuriuo Lietuvai patvirtinama Išorės sienų fondo daugiametė programa 2007–2013 m. laikotarpiu[47]. Programos lėšomis Policijos departamentas įgyvendino projektą „Sukurti vieningą pajėgų valdymo sistemą". Sukurta sistema leidžia valdyti ir kontroliuoti operacijoje dalyvaujančių institucijų pajėgų vienetus, operatyviai teikti įvykio duomenis. Pažymėtina, kad siekiant užtikrinti tinkamą policijos pajėgų valdymą ir pagerinti darbo kokybę, sukurta VPVS naudojama ir kitoms policijos reikmėms: administracinio teisės pažeidimo protokolams spausdinti, kriminalinės policijos pajėgoms valdyti.

Pagal Išorės sienų fondo 2010 m. ir 2012 m. metines programas (Specialioji tranzito schema) VPVS plėtrai panaudota 2,978 mln. Eur (10,282 mln. Lt). Pirkti ir sumontuoti telemetriniai įrenginiai policijos, VSAT PAGD, VST pajėgų automobiliuose, pirkti ir parengti darbui automobiliniai kompiuteriai, spausdintuvai, atnaujinta VPVS infrastruktūros techninė įranga, išplėstos VPVS programinės įrangos funkcijos.

Išorės sienų fondo daugiametės 2007–2013 m. programos dalyje „Specialioji tranzito schema" numatyta, kad sudėtingoje ekstremalioje situacijoje gali dalyvauti iki penkių institucijų (VSAT, Lietuvos policija, VST, PAGD ir greitosios medicinos pagalbos tarnyba) (toliau – pajėgų vienetai), kurios valdo pajėgas, reaguoja į įvykius ir kiekviena atskirai, ir bendradarbiaudamos tarpusavyje, įgyvendindamos teisės aktais nustatytus uždavinius. Tačiau VšĮ Greitosios medicinos pagalbos stotis į VPVS kūrimo procesą nebuvo įtraukta, nėra gavusi informacijos apie vykdomą projektą, nebuvo vykdomas projekto derinimas ir svarstymas su šia įstaiga, todėl VPVS skaitmeniniame žemėlapyje nėra greitosios pagalbos automobilių buvimo vietos koordinačių, o ekstremalių situacijų atveju priimant sprendimus bus reikalingi papildomi koordinavimo veiksmai tarp pajėgų vienetų.

Auditoriai, atlikę VPVS kūrimo (modernizavimo) kontrolės procedūras, nustatė esminių trūkumų: projekto valdymo kokybės užtikrinimo stoka, nesilaikoma VPVS kūrimo gyvavimo ciklo etapų eiliškumo, nustatyta tarpinstitucinio bendradarbiavimo ir projekto koordinavimo stoka.

[47] Lietuvos policijos generalinio komisaro, Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos vado, Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus ir Viešojo saugumo tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos vado 2014-05-15 įsakymu Nr. 5-V-442/4-164/1-199/47V-346 patvirtinti Vieningos pajėgų valdymo sistemos nuostatai, 4.1 p.

## 2.1. Projektų valdymas

COBIT projektų valdymo procesas[48] nurodo, jog organizacijoje įdiegta programų ir projektų valdymo sistema visiems IT projektams valdyti turėtų užtikrinti tinkamą visų projektų prioritetų nustatymą ir koordinavimą. Siekiant užtikrinti projektų rizikos valdymą ir vertės kūrimą veiklai, 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 mažina nenumatytų sąnaudų ir projektų nutraukimo riziką, gerina ryšius su veiklos atstovais ir galutiniais naudotojais ir jų įsitraukimą, užtikrina projekto rezultatų sukuriamą vertę ir kokybę ir maksimaliai padidina jų indėlį į IT palaikomas investicijų programas.

Policijos departamentas neturi parengęs atskiros IT projektų valdymo metodikos, o kurdamas, tobulindamas IS ir registrus vadovaujasi LR norminių teisės aktų reikalavimais ir programinės įrangos kūrimo taisyklėmis[49], kurios reglamentuoja bendruosius programinės įrangos kūrimo principus policijos sistemoje, tačiau neapima visų projekto valdymo principų: sprendimo kelių parinkimo (alternatyvų), projekto planavimo, plano vykdymo, projekto kontrolės ir užbaigimo.

COBIT rekomenduoja[50] nustatyti nuokrypius nuo projekto plano, įvertinti jų poveikį projektui, apie projekto rezultatus informuoti suinteresuotas šalis.

Audito metu nustatyta, kad Policijos departamente neužtikrinama efektyvi vykdomo projekto kontrolė (žr. 10 pavyzdį), todėl nesuvaldomos projekto rizikos ir nuokrypiai nuo plano.

**10 pavyzdys**

Vadovaujantis Europos Sąjungos ir kitos tarptautinės finansinės paramos administravimo policijos įstaigose tvarkos aprašu[51], projektams, kurie finansuojami iš Europos Sąjungos ir kitos tarptautinės paramos, nustatytas projektų koordinavimo ir kontrolės mechanizmas. Departamento projektų įgyvendinimo kontrolę užtikrina Investicijų planavimo ir techninės plėtros valdybos Paramos administravimo skyrius, kuriam kas ketvirtį buvo teikiamos VPVS projekto pažangos ataskaitos. Išanalizavus šias ataskaitas nustatyta, kad jos parengtos tik formaliai, nepateikiant informacijos, kodėl nebuvo įvykdytos suplanuotos projekto veiklos, kada jas numatoma įvykdyti.

Pagal Lietuvos policijos programinės įrangos kūrimo taisykles, programinės įrangos kūrimo projektą kontroliuoja Policijos informacinių technologijų koordinavimo grupė. Išanalizavus ITKG protokolus, nustatyta, kad VPVS programinės įrangos funkcijų tobulinimo klausimai ir eiga šioje grupėje nenagrinėti.

Audituotu laikotarpiu galioję teisės aktai numatė[52], kad IS projekto valdymo etapo metu turi būti patvirtinta IS specifikacija, kurioje aprašytas IS projekto planas, nustatantis, kaip IS projektas bus vykdomas ir tvarkomas. Lietuvos policijos programinės įrangos kūrimo taisyklėse nustatyta, kad turi būti patvirtinamas bendras programinės įrangos kūrimo projekto įgyvendinimo planas[53].

[48] COBIT 4.1, 2011 m., Vilnius, PO10 procesas, 67 psl.

[49] Lietuvos policijos generalinio komisaro 2005-05-30 įsakymu Nr. 5-V-336 patvirtintos Lietuvos policijos programinės įrangos kūrimo taisyklės.

[50] COBIT 4.1, 2011 m., Vilnius, PO10 procesas, 69 psl.

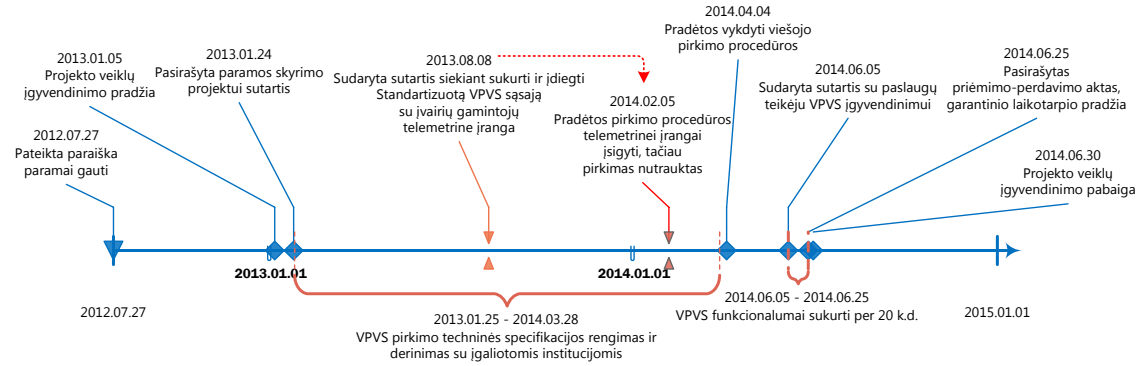
[51] Lietuvos policijos generalinio komisaro 2013-07-25 įsakymu Nr. 5-V-634 patvirtintas Europos Sąjungos ir kitos tarptautinės finansinės paramos administravimo policijos įstaigose tvarkos aprašas.

[52] Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-10-15 įsakymu Nr. T-131 (neteko galios 2014-02-06) patvirtinta Valstybės informacinių sistemų kūrimo metodika, 22 p.

[53] Lietuvos policijos generalinio komisaro 2005-05-30 įsakymu Nr. 5-V-336 patvirtintos Lietuvos policijos programinės įrangos kūrimo taisyklės, 11 p.

ISF 2012 m. metinės programos lėšomis Policijos departamentas atliko VPVS programinės įrangos funkcijų tobulinimus, pirko techninės ir kompiuterinės įrangos, tačiau nepatvirtino IS specifikacijos, kurioje būtų aprašytas IS projekto planas (žr. 3 priedą). Integruotas IS projekto valdymo planas, kuris apimtų laiko, finansinius, žmogiškuosius išteklius, sudėtinių projekto veiklų ir susijusių projektų sąlyčio taškus ar tarpusavio ryšius, taip pat nebuvo sudarytas. Nesant integruoto projekto įgyvendinimo plano ir efektyvaus kontrolės bei projekto rizikų valdymo mechanizmo, buvo netinkamai nustatyti IS projekto sudėtinių dalių atlikimo terminai – ilgiau nei planuota užsitęsė pirkimo sąlygų rengimas, pirkimo dokumentai ilgai buvo derinami su Vidaus reikalų ministerija ir Centrine projektų valdymo agentūra, todėl iki kritinės ribos sutrumpėjo faktinių projekto veiklų (VPVS programinės įrangos tobulinimo ir pakeitimų dokumentavimo) įgyvendinimo terminas (20 kalendorinių dienų, žr. 3 paveikslėlį). Dėl to VPVS programinės įrangos tobulinimo darbai buvo vykdomi skubotai, nenuosekliai, nesilaikant gyvavimo ciklo etapų eiliškumo (žr. 2.2 poskyrį).

**3 pav.** VPVS programinės įrangos funkcijų tobulinimo eiga




Šaltinis – Valstybės kontrolė

*Pokyčiai audito metu: Policijos departamentas VPVS nuostatus patvirtino 2014-05-15, IS specifikaciją patvirtino ir įregistravo Registrų ir informacinių sistemų registre 2015-06-09.*

Pastebėtina, kad tuo pat metu iš valstybės biudžeto lėšų buvo įgyvendinami ir kiti VPVS modernizavimo darbai – siekta sukurti ir įdiegti standartizuotą VPVS sąsają su įvairių gamintojų telemetrine įranga.

Policijos departamente įgyvendintas sprendimas riboja galimybę kitiems telemetrinės įrangos gamintojams dalyvauti viešuose pirkimo konkursuose, nes duomenų perdavimo protokolas neuniversalus ir pritaikytas tik vieno paslaugų teikėjo sukurtam sprendimui. Standartizuotos sąsajos sukūrimo projektas nebuvo sėkmingai įgyvendintas (žr. 3 paveikslėlį), nes Policijos departamento pateiktais duomenimis paslaugos teikėjas nekvalifikuotai teikė paslaugas ir neįvykdė sutartinių įsipareigojimų. Nesukūrus sąsajos su įvairių gamintojų telemetrine įranga, neįvyko ir ISF 2012 m. metinės programos lėšomis finansuojamas pirkimas, todėl Policijos departamentas neįsigijo 250 vnt. telemetrinių įrenginių ir 150 vnt. telemetrinių įrenginių su tikslios kuro apskaitos įrenginiais.

*Siekdamas išspręsti susidariusią problemą, departamentas minėtą sąsają sukūrė savo jėgomis pagal VPVS projekto metu pirktą dokumentaciją.*

VPVS projekto metu Policijos departamentas realizavo tinklines paslaugas (*angl.* web service) perduoti informaciją iš PRĮR į BPC IS apie pagalbos prašymo tikrinimo eigą (būsenas) ir pagalbos suteikimo rezultatus, kaip tai numatyta Bendrojo pagalbos centro įstatymo 11 str. 6 d. Sukūrė tinklines paslaugas, skirtas perduoti policijos bei priešgaisrinių ir gelbėjimo pajėgų vienetų statusą (poilsis, laisvas, vyksta į įvykio vietą, įvykio vietoje arba užimtas) ir koordinates iš VPVS į

BPC IS. Sukurtos VPVS funkcijos daugiau negu metus nepradedamos naudoti, nes PAGD neatliko BPC IS tobulinimo darbų ir tik 2015-05-27 pateikė Vidaus reikalų ministerijai derinti investicinį projektą BPC IS modernizavimo darbams atlikti.

Vidaus reikalų ministerija nepakankamai koordinavo pavaldžių institucijų veiklą ir nesiėmė tinkamų veiksmų, kad departamentas ir BPC patikimai keistųsi duomenimis apie pagalbos prašymo tikrinimo eigą (būsenas), pagalbos suteikimo rezultatus, PRĮR registruotų įvykių baigtį, nėra pagreitinta komunikacija tarp BPC ir policijos operatyvaus valdymo padalinių, siekiant sutrumpinti BPC reagavimo laiką.

COBIT nurodo[54], kad kiekvieno projekto pabaigoje reikėtų nustatyti, ar projektas davė planuotų rezultatų ir naudą, informuoti apie neatliktus veiksmus, įvertinti projekto vykdymo metu gautą patirtį, kurią būtų galima panaudoti būsimiems projektams.

Baigęs VPVS modernizavimo projektą, Policijos departamentas neatliko projekto rezultatų peržiūros, todėl neįsitikino projekto rezultatyvumu, neįvertino, ar sukurtos funkcijos atitinka VPVS naudotojų lūkesčius, ar pirkta ir policijos įstaigoms perduota kompiuterine įranga patogu naudotis, ar sukurtos VPVS programinės įrangos funkcijos naudojamos mobiliose darbo vietose (žr. 11 pavyzdį).

**11 pavyzdys**

Nepradėta naudoti 2014-06-25 sukurta PPV darbo vietos funkcija, skirta policijos pareigūnui vykdančiam funkcijas nustatytoje teritorijoje ir reaguojančiam į PRĮR registruotus įvykius, gauti pranešimus ar kitą informaciją; priskirti sau apdorojimui iš PRĮR gautą įvykį; fiksuoti PPV vykimo, atvykimo į įvykio vietą ir darbo įvykyje baigimo, poilsio laikus ir PPV statusus, matyti perspėjimus apie naujus įvykius.

Policijos departamentas nepriėmė sprendimų, kokie ir kiek PPV bus priskirti reaguoti į įvykius naudojant PPV darbo vietai sukurtą funkciją, o kurie padaliniai naudos tik manipuliatorius, skirtus perduoti įvykio statuso būseną. Tai, kad neįvertintos šios aplinkybės ir 2015 m. nupirkta 48 vnt. telemetrinės įrangos su manipuliatoriais (2014 m. planuota pirkti 400 vnt. telemetrinės įrangos su manipuliatoriais), suponuoja netikslingą lėšų panaudojimą manipuliatorių pirkimui.

2014 m. VPVS techninėje pirkimo specifikacijoje buvo numatyti reikalavimai VPVS programinės įrangos modernizavimui – PPV darbo vietos naudotojo sąsaja turi būti pritaikyta kompiuteriams su liečiamaisiais ekranais. ISF 2010 m. ir 2012 m. metinės programos lėšomis departamente pirkti 1 072 kompiuteriai neturi liečiamo ekrano funkcijos ir nesudaromos prielaidos patogiam policijos pareigūnų darbui reaguojant į įvykį.

Departamentas, baigęs projektą, ne tik neįsitikino jo nauda ir rezultatyvumu, bet galutinėje projekto įgyvendinimo ataskaitoje nepateikė tikslios informacijos, kaip buvo pamatuoti projekto rezultatyvumo (kokybiniai) rodikliai. Auditoriams šią informaciją departamentas pateikė tik po papildomo užklausimo, nurodydamas, kad galutinėje projekto ataskaitoje įsivėlė klaida (žr. 12 pavyzdį).

**12 pavyzdys**

ISF 2012 m. programos lėšomis finansuojamo VPVS projekto įgyvendinimo galutinėje ataskaitoje nurodyta, kad kokybinis rodiklis – atnaujinus įrangą, sumažės technikos gedimų – įgyvendintas iš esmės, o jo įgyvendinimui daugiausia įtakos turėjo sukurta PPV darbo vieta, kurią naudodamas ekipažas pats gali priimti ir apdoroti naują pranešimą, o ne telemetriniai kuro apskaitos įrenginiai, kurių nebuvo pirkta. Auditoriai atkreipia dėmesį, kad PPV darbo vietos funkcija, skirta policijos pareigūnui, vykdančiam funkcijas nustatytoje teritorijoje ir reaguojančiam į PRĮR registruotus buvo sukurta 2014-06-25, tačiau nebuvo naudojama. Pagal Policijos departamento

[54] COBIT 4.1, 2011 m., Vilnius, PO10 procesas, 69 psl.

pateiktą informaciją, PPV darbo vietą planuojama pradėti eksploatuoti 2015 m. rugsėjo pradžioje.

Siekdamas užtikrinti departamento vykdomų projektų valdymo kokybę, departamentas turėtų peržiūrėti ir atnaujinti IT projektų valdymo principus. Prieš įgyvendinant projektą derėtų sudaryti integralų projekto įgyvendinimo planą, pagal kurį viso projekto gyvavimo ciklo metu bus organizuojami projekto įgyvendinimas ir kontrolė, o apie nuokrypius nuo plano būtina informuoti už projekto įgyvendinimo kontrolę atsakingas struktūras. Siekdamas įsitikinti projekto rezultatyvumu ir planuota nauda, departamentas turėtų atlikti jo rezultatų peržiūrą, įvertinti vykdymo trukdžius ir gerąją patirtį, kuriuos būtų galima pritaikyti valdant būsimų IT projektų rizikas.

## 2.2. Sprendimų ir pokyčių diegimas ir akreditavimas

COBIT nurodo[55], kad, baigus kūrimo procesą, reikia pradėti naudoti naujas sistemas. Tam jas reikia tinkamai testuoti specialioje aplinkoje su aktualiais testavimo duomenimis, apibrėžti išleidimo ir perkėlimo instrukcijas, planuoti paleidimą, pradėti faktinę eksploataciją.

Lietuvos Respublikos teisės aktai nustato, kad:

- Valstybės IS valdytojo vadovas, raštu pritaręs siūlymui pradėti bandomąją eksploataciją, prireikus sprendžia dėl valstybės IS bandomosios eksploatacijos vykdymo organizavimo, atsakingų asmenų paskyrimo, vykdomų veiklos funkcijų ir bandomosios eksploatacijos pabaigos termino[56];
- valstybės IS tvarkytojas arba valstybės IS valdytojo paskirtas tvarkytojas, jeigu sistemos nuostatuose nurodyti keli tvarkytojai, rengia ir tvirtina detalųjį bandomosios eksploatacijos planą, kuriame numatomas techninių ir programinių priemonių diegimo, pirminių duomenų, reikalingų eksploatacijos pradžiai, ir normatyvinės informacijos parengimo grafikai, trūkumų fiksavimo ir šalinimo terminai[57];
- bandomosios eksploatacijos metu nustatytu periodiškumu projekto priežiūros komisijos posėdžiuose svarstoma bandomosios eksploatacijos eiga, aptariamos valstybės informacinės sistemos kūrėjų parengtos užfiksuotų trūkumų ir jų šalinimo rezultatų ataskaitos[58];
- pasibaigus valstybės IS, jos modulio arba prieaugio bandomajai eksploatacijai, po trūkumų šalinimo patikslinus programinį kodą ir techninę dokumentaciją, projekto priežiūros komisija posėdžio protokolu patvirtina valstybės IS, jos modulio arba prieaugio tinkamumą eksploatuoti[59].

VPVS programinės įrangos modernizavimo 2012 ir 2014 m. projekto vykdymo reglamentuose buvo apibrėžta VPVS naujai sukurtų funkcijų testavimo strategija, apimanti programinės įrangos testavimą prieš pateikiant bandomajai eksploatacijai (testavimo planavimas, projektavimas, įgyvendinimas), buvo sudarytos testų rezultatų ataskaitos, pirkimo specifikacijoje buvo numatyta po įdiegimo organizuoti mokymus VPVS naudotojams.

Nustatėme, kad, 2014 m. modernizuojant VPVS programinę įrangą, testavimo, mokymų organizavimo ir rezultatų priėmimo eiga buvo nenuosekli, neatlikta bandomoji eksploatacija

[55] COBIT 4.1, 2011 m., Vilnius, AI7 procesas, 97 psl.

[56] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 d įsakymu Nr. T-29 patvirtinta Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, 46 p.

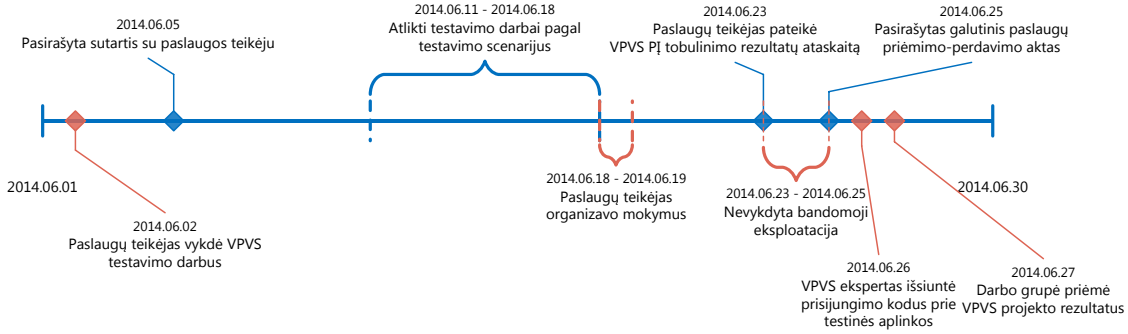
[57] Ten pat, 47 p.

[58] Ten pat, 48 p.

[59] Ten pat, 49 p.

(žr. 4 paveikslėlį).

**4 pav.** VPVS programinės įrangos funkcijų įdiegimo eiga




Šaltinis – Valstybės kontrolė

Kadangi sukurtos VPVS funkcijos nebuvo išbandytos tokiomis sąlygomis, kurios atitiktų realias IS eksploatavimo sąlygas, todėl Policijos departamentas neįsitikino sklandžiu sukurtų funkcijų (pvz., PPV darbo vieta) veikimu, naudotojai neįvertino, ar darbo vietos su įdiegta programine įranga yra parengtos ir pritaikytos optimalioms darbo sąlygoms, ar jos patogios.

Atkreiptinas dėmesys, kad 2014 m. testavimo ataskaitose ir VPVS projekto valdymo darbo grupės protokoluose pateikiama prieštaringa informacija, susijusi su sukurtų funkcijų testavimu, nurodomos skirtingos testavimo datos ir skirtingas aptiktų klaidų skaičius, tai rodo, kad testavimo darbai buvo vykdomi skubotai, o testavimo ataskaitos rengiamos tik formaliai (žr. 13 pavyzdį).

**13 pavyzdys**

Pagal tiekėjo klaidų registravimo sistemoje JIRA užregistruotas klaidas ir jų registracijos datas nustatyta, kad viešojo pirkimo konkursą laimėjęs tiekėjas VPVS naujos funkcijos testavimo darbus pradėjo 2014-06-02, t. y. 3 dienomis anksčiau, nei pasirašyta 2014-06-05 paslaugų teikimo sutartis.

2014 m. paslaugų tiekėjo parengtoje galutinėje testų rezultatų ataskaitoje fiksuota, kad testavimo darbai buvo vykdomi nuo 2014-06-09 iki 2014-06-23.

Testavimo scenarijuose nurodyta, kad testavimas vyko 2014-06-11 ir 2014-06-18 dienomis; kritinių klaidų neaptikta, vidutinių klaidų procentas (20%) neviršija numatytų priėmimo kriterijų (<35%), o priėmimo testavimo rezultatai tenkina priėmimo kriterijus. Projekto valdymo darbo grupė 2014-06-20 buvo susirinkusi apsvarstyti dalinių VPVS programinės įrangos tobulinimo rezultatų ir suderino, kad iki kito susitikimo darbo grupės nariams bus atsiųsti prisijungimo prie policijos techninėje architektūroje įdiegtos VPVS testinės aplinkos vardai. Policijos departamento pateiktais duomenimis, projekto valdymo darbo grupės nariams 2014-06-26 buvo išsiųsti prisijungimo vardai (žr. 4 paveikslėlį).

Atkreiptinas dėmesys, kad tuo metu (2014-06-25) paslaugų perdavimo–priėmimo aktas jau buvo pasirašytas. o projekto valdymo darbo grupė tik po 2 dienų posėdžio protokolu fiksavo galutinių projekto rezultatų priėmimą ir nurodė, kad 50-yje testavimo scenarijų neaptikta kritinių ir vidutinių klaidų.

Policijos departamentas kurdamas ar modernizuodamas IS turėtų laikytis IS gyvavimo ciklo, o sukurtų funkcijų rezultatus priimti tik visiškai įsitikinęs, kad visi techninėje užduotyje numatyti darbai atlikti pagal techninės užduoties reikalavimus, sistema yra patogi naudotojui, veikia be nesklandumų ir trikdžių realiomis IS eksploatavimo sąlygomis.

Teisės aktais[60] nustatyta, kad Valstybės IS realizavimo etapas laikomas baigtu, kai duomenys apie patvirtintą valstybės IS priėmimo ir tinkamumo eksploatuoti aktą įrašomi Registrų ir valstybės informacinių sistemų registre. Akte turi būti nurodyta, kad visa valstybės IS nuostatuose ir specifikacijoje aprašyta valstybės IS yra sukurta ir tinkama eksploatuoti.

Nustatyta, kad audituotu laikotarpiu modernizuota VPVS nebuvo įteisinta teisės aktų nustatyta tvarka, nes departamentas nepatvirtino VPVS priėmimo ir tinkamumo eksploatuoti akto, kuris turi būti pateiktas Registrų ir valstybės informacinių sistemų registro tvarkytojui – Informacinės visuomenės plėtros komitetui prie Susisiekimo ministerijos[61].

Taigi Policijos departamentas, neįsitikinęs sukurtų IS funkcijų tinkamumu ir duomenų patikimumu, elektroninę informaciją tvarko neįteisintoje VPVS, nors gali būti naudojami tik įteisintų valstybės informacinių sistemų duomenys.

Informacinių sistemų ir infrastruktūros audito departamento
direktorius Dainius Jakimavičius

Informacinių sistemų ir infrastruktūros audito departamento
Informacinių sistemų audito skyriaus
vyresnioji valstybinė auditorė Jurgita Musteikienė

Valstybinio audito ataskaitos kopijos pateiktos:

Lietuvos Respublikos Seimo Audito komitetui, 1 egz.

Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komitetui, 1 egz.

Lietuvos Respublikos vidaus reikalų ministerijai, 1 egz.

---

Auditas atliktas, vykdant 2014-11-12 pavedimą Nr. P-90-3

Auditą atliko valstybinių auditorių grupė:

Jurgita Musteikienė (grupės vadovė),

Loreta Tomickytė-Šajaukienė,

Kęstutis Valeika (nuo 2015-02-27)

[60] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29 (galioja nuo 2014-02-26) patvirtinta Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, 54 ir 55 p.

[61] Lietuvos Respublikos Vyriausybės 2013-02-27 d. nutarimu Nr. 180 patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, 30 ir 31 p.

# PRIEDAI

Valstybinio audito ataskaitos
„Policijos informacinių išteklių valdymas“
1 priedas

## Audito apimtis ir metodai

Audito objektas – Policijos informaciniai ištekliai.

Audito subjektas – Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.

Audito tikslas – įvertinti policijos informacinių išteklių valdymą ir kūrimo kontrolę.

Vertinimo kriterijai: Policijos departamento informacinių išteklių valdymas įvertintas taikant Gebos brandos modelį (5 priedas). IS valdymo, saugos užtikrinimo organizavimą, IS kūrimo kontrolę vertinome naudodami IT valdymo metodiką COBIT, kuri apibrėžia 34 procesus, kurie suskirstomi į 4 grupes. Atrinkus svarbiausius Policijos departamento veiklos procesus ir atlikus preliminarų rizikos vertinimą, detaliam bendrosios kontrolės vertinimui buvo pasirinkta 11 su jais susijusių COBIT apibrėžtų IT procesų, kuriuos analizavome detaliau. Tai Planavimo ir organizavimo grupės (PO) procesai (PO1, PO2, PO4), Teikimo ir palaikymo grupės (DS) procesas (DS5, DS11) ir Stebėsenos ir vertinimo (ME) grupės procesai (ME2 ir ME4). IS kūrimo kontrolei buvo pasirinkta Vieninga pajėgų valdymo sistema (VPVS). Kūrimo kontrolė buvo vertinama pagal šiuos COBIT procesus: PO10, AI5, AI6, AI7.
Audituojamas laikotarpis: nuo 2012 iki 2014 m.

## Pagrindiniai duomenų rinkimo ir vertinimo metodai

| Eil. Nr. | Metodas | Tikslai |
|---|---|---|
| 1. | Dokumentų analizė:<br>Nagrinėjome Policijos departamento prie Vidaus reikalų ministerijos ir policijos įstaigų dokumentus, susijusius su informacinių išteklių kūrimu, priežiūra, valdymu, finansavimu, strateginiu planavimu. | Nustatyti<br>▪ Policijos departamento IT valdymo struktūrą;<br>▪ valdomus informacinius išteklius,<br>▪ informacinių išteklių techninę infrastruktūrą,<br>▪ taikomas duomenų valdymo ir IS/registrų saugos užtikrinimo priemones,<br>▪ IT pokyčių valdymo tvarką,<br>▪ kūrimo ir palaikymo trūkumus ir privalumus. |
| 2. | Pokalbiai su Policijos departamento prie Vidaus reikalų ministerijos:<br>▪ Policijos informacijos valdybos darbuotojais,<br>▪ Įslaptintos informacijos apsaugos (kontrolės) grupės darbuotojais;<br>▪ Investicijų planavimo ir techninės plėtros valdybos darbuotojais; | |

| Eil. Nr. | Metodas | Tikslai |
|---|---|---|
| | ▪ Štabo darbuotojais;<br>▪ Viešosios policijos valdybos darbuotojais.<br>Pokalbiai su Lietuvos kriminalinės policijos biuro:<br>▪ Informacinių technologijų valdybos darbuotojais;<br>▪ Veiklos koordinavimo ir kontrolės valdybos darbuotojais;<br>▪ Organizuoto nusikalstamumo 1-osios valdybos darbuotojais;<br>▪ Specialiųjų užduočių 1-osios valdybos darbuotojais;<br>▪ Tarptautinių ryšių valdybos darbuotojais.<br>Pokalbiai su:<br>▪ Vilniaus apskrities vyriausiojo policijos komisariato Informatikos ir ryšių skyriaus darbuotojais;<br>▪ Vilniaus apskrities vyriausiojo policijos komisariato Operatyvaus valdymo skyriaus darbuotojais;<br>▪ Alytaus apskrities vyriausiojo policijos komisariato Informatikos ir ryšių poskyrio darbuotojais;<br>▪ Alytaus apskrities vyriausiojo policijos komisariato Kriminalinės policijos nusikaltimų skyriaus darbuotojais;<br>▪ Bendrojo pagalbos centro Informacinių technologijų skyriaus darbuotojais;<br>Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos darbuotojais. | |
| 3. | Apklausti devynių apskričių vyriausieji policijos komisariatai | |
| 4. | Raštai:<br>▪ Policijos departamentui prie Vidaus reikalų ministerijos;<br>▪ VĮ „Regitrai“;<br>▪ Lietuvos Respublikos vidaus reikalų ministerijai;<br>▪ Vilniaus miesto savivaldybės Socialinių reikalų ir sveikatos departamentui;<br>▪ VšĮ Greitosios medicinos pagalbos stočiai;<br>▪ Vilniaus apskrities vyriausiajam policijos komisariatui;<br>▪ Bendrajam pagalbos centrui;<br>▪ Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Vidaus reikalų ministerijos;<br>Lietuvos Respublikos valstybės saugumo departamentui. | Įvertinti VPVS projekto kūrimo eigą ir rezultatus.<br><br>Nustatyti:<br>▪ Policijos departamento IS/registrų neveikimo poveikį susijusių institucijų veiklai,<br>▪ Įslaptintos informacijos tvarkymui taikomas saugos užtikrinimo priemones. |
| 5. | Stebėsena:<br>Policijos departamente prie Vidaus reikalų ministerijos, Lietuvos kriminalinės policijos | Nustatyti Policijos departamento valdomus informacinius išteklius aptarnaujančios techninės kompiuterinės įrangos priežiūros atitiktį teisės |

| Eil. Nr. | Metodas | Tikslai |
|---|---|---|
| | biure, Vilniaus apskrities vyriausiajame policijos komisariate, Alytaus apskrities vyriausiajame policijos komisariate, Bendrajame pagalbos centre, Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos. | aktų reikalavimams.<br>Įvertinti VPVS projekto metu įdiegtą techninę įrangą ir sukurtas programinės įrangos funkcijas. |

Šaltinis – Valstybės kontrolė

Valstybinio audito ataskaitos
„Policijos informacinių išteklių valdymas“
2 priedas

## Rekomendacijų įgyvendinimo planas

| Eil. Nr. | Rekomendacija | Subjektas, kuriam pateikta rekomendacija | Priemonės | Rekomendacijos įgyvendinimo terminas (data) |
|---|---|---|---|---|
| 1. | Siekiant nuoseklaus ir kryptingo IS ir registrų tobulinimo ir atsižvelgiant į visos organizacijos veiklos poreikius, parengti ir patvirtinti IT strategiją ir jos pagrindu sukurti bei nuolatos atnaujinti IT plėtros planus. | Policijos departamentas | 1.1. Parengti ir patvirtinti policijos IT strategiją.<br>1.2. Parengti ir patvirtinti policijos IT plėtros planus kartu su jų nuolatinės peržiūros ir atnaujinimo procedūromis. | 2016-07-01 |
| 2. | Sudaryti informacijos architektūros modelį, apimantį Policijos departamento ir policijos įstaigų valdomos informacijos, IS/registrų duomenų bei technologinę architektūrą, nurodant kiekvienos sudedamosios dalies komponentus (naudojamos technologijas, duomenis, duomenų srautus tarp išorinių ir vidinių IS). | Policijos departamentas | 2.1. Sudaryti policijos informacijos architektūros modelį.<br>2.2. Numatyti ir patvirtinti policijos informacijos architektūros pokyčių valdymo procedūras. | 2016-12-21 |
| 3. | Siekiant užtikrinti valdomų informacinių išteklių saugą: | - | | |
| 3.1. | atlikti visų Policijos departamento valdomų informacinių išteklių periodišką saugos atitikties vertinimą ir užtikrinti nustatytų trūkumų šalinimo kontrolę; | Policijos departamentas | 3.1.1. Kiekvienais metais atlikti Policijos departamento valdomų informacinių išteklių saugos atitikties vertinimą.<br>3.1.2. Sudaryti ir patvirtinti saugos atitikties vertinimo nustatytų trūkumų šalinimo priemonių planus po kiekvieno saugos atitikties vertinimo. | 2016-12-21 |
| 3.2. | tobulinti rizikos valdymo procesą, laikytis departamento galimų grėsmių ir rizikų policijos IS analizavimo, stebėjimo ir vertinimo procedūrų aprašo ir užtikrinti nustatytos rizikos mažinimo priemonių įgyvendinimą; | Policijos departamentas | 3.2.1. Kiekvienais metais teikti rizikų vertinimo ataskaitas Informacinių technologijų koordinavimo grupei.<br>3.2.2. Sudaryti rizikų ir grėsmių šalinimo (mažinimo) planus ir užtikrinti jų kontrolę bei įgyvendinimą. | 2015-12-18<br>2016-04-01 |

| Eil. Nr. | Rekomendacija | Subjektas, kuriam pateikta rekomendacija | Priemonės | Rekomendacijos įgyvendinimo terminas (data) |
|---|---|---|---|---|
| 3.3. | suderinti atsarginių duomenų kopijų saugojimo bei duomenų atkūrimo tvarką ir planus su Vidaus reikalų ministerija, atsižvelgiant į Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašą; | Policijos departamentas | 3.3.1. Suderinti atsarginių duomenų kopijų saugojimo bei duomenų atkūrimo tvarką ir planus su VRM. | 2016-03-01 |
| 3.4. | atnaujinti departamento IS veiklos tęstinumo valdymo planą ir jį išbandyti; | Policijos departamentas | 3.4.1. Atnaujinti Policijos departamento IS veiklos tęstinumo planą.<br>3.4.2. Išbandyti Policijos departamento IS veiklos tęstinumo planą. | 2016-02-01<br>2016-06-30 |
| 3.5 | periodiškai organizuoti darbuotojų mokymus duomenų tvarkymo teisėtumo ir informacijos saugos klausimais; | | 3.5.1. Parengti darbuotojų mokymų duomenų tvarkymo teisėtumo ir informacijos saugos klausimais programą.<br>3.5.2. Mokymus įtraukti į atitinkamus mokymų planus. | 2015-12-18 |
| 3.6. | pranešti Valstybinei duomenų apsaugos inspekcijai apie departamento valdomuose informaciniuose ištekliuose automatiniu būdu tvarkomus asmens duomenis ir jų tvarkymo tikslus, kad būtų atnaujinta Asmens duomenų valdytojų registre esanti informacija; | Policijos departamentas | 3.6.1. Pranešti Valstybinei duomenų apsaugos inspekcijai apie departamento valdomuose informaciniuose ištekliuose automatiniu būdu tvarkomus asmens duomenis ir jų tvarkymo tikslus. | 2016-04-01 |
| 3.7. | peržiūrėti ir atnaujinti IS ir registrų duomenų tvarkymo taisykles: jose išdėstyti taikomos asmens duomenų saugos priemones taip, kaip nustato Asmens duomenų teisinės apsaugos įstatymas; | Policijos departamentas | 3.7.1. Patvirtinti saugaus elektroninės informacijos tvarkymo taisykles.<br>3.7.2. Patvirtinti asmens duomenų tvarkymo policijos įstaigose taisykles.<br>3.7.3. Suderinti IS ir registrų duomenų tvarkymo taisykles. | 2016-04-01<br>2016-09-01 |
| 4. | Rekomendacijos dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta) | | | |
| 5. | Siekiant veiksmingo ir sistemingo pokyčių valdymo, peržiūrėti taikomą pokyčių valdymo procesą ir nustatyti (patvirtinti) IT pokyčių valdymo tvarką, kurioje būtų reglamentuotas IT pokyčių valdymo planavimas ir užtikrinta šios tvarkos laikymosi (vykdymo) kontrolė. | Policijos departamentas | 5.1. Parengti ir patvirtinti policijos IT pokyčių valdymo tvarką ir užtikrinti jos laikymosi kontrolę. | 2016-12-21 |

| Eil. Nr. | Rekomendacija | Subjektas, kuriam pateikta rekomendacija | Priemonės | Rekomendacijos įgyvendinimo terminas (data) |
|---|---|---|---|---|
| 6. | Periodiškai stebėti ir vertinti informacinių sistemų ir registrų vidaus kontrolės būklę. | Policijos departamentas | 6.1. Informacinių sistemų ir registrų vidaus kontrolės veikimo vertinimą įtraukti į atitinkamus veiklos planus Centralizuoto vidaus audito skyriaus metinius veiklos planus.<br>6.2. Atlikti metiniame Centralizuoto vidaus audito skyriaus veiklos plane numatytus vidaus auditus, kurių tikslas tikrinti ir vertinti bendrosios IS kontrolės priemones, IS ir registrų valdymą ir naudojimą bei pateikti vidaus audito ataskaitą vadovybei. | 2016-02-15<br>2016-12-21 |
| 7. | Peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus, veiklą, aiškiai atskirti jų funkcijas, užtikrinti jų veiklos tęstinumą ir pavestų funkcijų vykdymą. | Policijos departamentas, Lietuvos kriminalinės policijos biuras, Lietuvos policijos kriminalistinių tyrimų centras | 7.1. Pakeisti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus darbo reglamentus, aiškiai atskiriant jų funkcijas.<br>7.2. Užtikrinti darbo grupių veiklos tęstinumą. | 2016-01-30<br>2016-12-21 |
| 8. | Siekiant užtikrinti IT projektų kokybę ir projektų rizikos valdymą: | - | | |
| 8.1. | peržiūrėti ir atnaujinti Policijos departamente taikomus IT projektų valdymo principus, numatant, kad būtų sudaromas integruotas projekto įgyvendinimo planas. Pagal šį planą viso projekto gyvavimo ciklo metu organizuojamas projektų įgyvendinimas ir kontrolė, o apie nuokrypius nuo plano informuojamos už įgyvendinimo kontrolę atsakingos struktūros. | Policijos departamentas | 8.1.1. Parengti ir patvirtinti IT projektų valdymo metodiką. | 2016-12-21 |
| 8.2. | parengti ir patvirtinti valdomų informacinių išteklių nuostatus bei specifikacijas ir įteisinti naudojamas sistemas ir registrus. | Policijos departamentas | 8.2.1. Parengti ir patvirtinti valdomų informacinių išteklių nuostatus bei specifikacijas.<br>8.2.2. Įteisinti naudojamas sistemas ir registrus. | 2016-12-21 |

Šaltinis – Valstybės kontrolė

Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais: Policijos departamento prie Vidaus reikalų ministerijos Policijos informacijos valdybos viršininkas Artūras Kavolis.

Valstybinio audito ataskaitos „Policijos informacinių išteklių valdymas“
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.<br>1 d. Valstybės informacinė sistema pradedama kurti patvirtinus valstybės informacinės sistemos nuostatus.<br>2 d. Valstybės informacinė sistema kuriama pagal valstybės informacinės sistemos techniniame aprašyme (specifikacijoje) nurodytą kūrimo būdą. [...]<br>6 d. Naudojama tik įteisinta valstybės informacinė sistema ar jos posistemis. | PVVIS, Keleivių duomenų įrašų IS, PLVIS pradėtos kurti nepatvirtinus IS nuostatų.<br>*Audito metu padaryta pažanga: PLVIS nuostatai patvirtinti Lietuvos policijos generalinio komisaro 2015-03-03 įsakymu Nr. 5-V-262, PVVIS nuostatai patvirtinti Lietuvos policijos generalinio komisaro 2014-12-08 įsakymu Nr. 5-V-1066.*<br>PVVIS, Keleivių duomenų įrašų IS, PLVIS, VPVS buvo kuriamos nepatvirtintus IS techninio aprašymo (specifikacijos).<br>*Audito metu padaryta pažanga: VPVS specifikacija Lietuvos policijos generalinio komisaro patvirtinta 2015-06-09.*<br>Policijos departamentas, specializuotos ir teritorinės policijos įstaigos naudoja neįregistruotas ir neįteisintas 6 IS ir registrus (PRĮR, INDR, ITPR, VPVS, PLVIS, PVVIS). |
| 2. | 9 straipsnis. Planavimas [...]<br>3 d. Institucijos, valdančios valstybės informacinius išteklius, šio straipsnio 1 dalyje nurodytą informaciją įtraukia į Vyriausybės nustatyta tvarka rengiamus strateginio veiklos plano ir metinio veiklos plano projektus. | Policijos departamento strateginiuose veiklos planuose ir policijos įstaigų metiniuose veiklos planuose nenustatyti informacinių technologijų priemonių, skirtų informacijai, duomenims, dokumentams ir (arba) jų kopijoms tvarkyti, kūrimo ir naudojimo tikslai, uždaviniai, valstybės informacinių sistemų ir registrų steigimo, modernizavimo prioritetai, reikalingi finansiniai ir žmogiškieji ištekliai, organizacinės ir teisinės priemonės, kvalifikaciniai reikalavimai darbuotojams, darbuotojų mokymų poreikis, jų veiklos organizavimas ir kontrolė. |
| 3. | 8 straipsnis. Duomenų valdymo įgaliotinis. [...]<br>3 d. Duomenų valdymo įgaliotinį skiria valstybės informacinės sistemos ar registro valdytojas arba tvarkytojas. Duomenų valdymo įgaliotinis turi būti paskirtas kiekvienam registrui, valstybės informacinei sistemai ar jos posistemiui. | Duomenų valdymo įgaliotiniai nebuvo paskirti NAIS, OIS.<br>*Audito metu padaryta pažanga: Lietuvos kriminalinės policijos biuro viršininko 2014-12-30 įsakymu paskirti šių IS duomenų valdymo įgaliotiniai.* |
| 4. | 19 straipsnis. Registrų kūrimas<br>3 d. vadovaujantis registro nuostatais, parengiamas registro techninis aprašymas (specifikacija). Registro techninis aprašymas (specifikacija) ir kiti projektiniai dokumentai rengiami, derinami ir tvirtinami Vyriausybės nustatyta tvarka ir institucijos, atsakingos už valstybės informacinių išteklių funkcinį suderinamumą, jų kūrimą, tvarkymą ir plėtrą, patvirtinta metodika. <...><br>4 d. registras kuriamas vadovaujantis registro techniniu aprašymu (specifikacija), kitais projektiniais ir saugos dokumentais. | PRĮR, IGR, ITPR, INDR, Prevencinių poveikio priemonių taikymo registras sukurti, tačiau neturi patvirtintų specifikacijų. |

| Eil. Nr. | Teisės akto reikalavimai | Auditorių pastebėjimai |
|---|---|---|
| Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374 | | |
| 5. | 31 straipsnis. Pranešimas apie duomenų tvarkymą.<br>Asmens duomenys gali būti tvarkomi automatiniu būdu tik tuo atveju, kai duomenų valdytojas arba jo atstovas (pagal šio įstatymo 1 straipsnio 3 dalies 3 punktą) Vyriausybės nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai [...]. | PVVIS asmens duomenų tvarkymo tikslas – identifikuoti asmenis, kurių atžvilgiu policijos įstaigos vykdo Lietuvos Respublikos policijos veiklos įstatyme ir kituose teisės aktuose nustatytas bendrosios ir individualiosios prevencijos funkcijas. Šioje sistemoje tvarkomi ir kaupiami ypatingos svarbos asmens duomenys, tačiau asmens duomenų valdytojų valstybės registre toks asmens duomenų tvarkymo tikslas ir asmens duomenys nėra registruoti. |
| Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008-11-12 įsakymu Nr. 1T-71(1.12) patvirtinti Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms | | |
| 6. | 8. Organizacinės ir techninės asmens duomenų saugumo priemonės turi būti išdėstytos rašytinės (popierinės ar elektroninės) formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.), kuriame nurodoma: [...]<br>14. Siekiant užtikrinti antrąjį saugumo lygį, turi būti įgyvendintos pirmojo saugumo lygio organizacinės ir techninės asmens duomenų saugumo priemonės, nurodytos Bendrųjų reikalavimų 13 punkte, ir šios organizacinės ir techninės asmens duomenų saugumo priemonės: [...]<br>14.2. nustatomas leistinų nepavykusių prisijungimų prie programinės įrangos skaičius; [...]<br>14.7. registruojami asmens duomenų kopijavimo, jei jis daromas, ir atkūrimo jų avarinio praradimo atveju veiksmai (kada ir kas atliko šiuos veiksmus);<br>15. Siekiant užtikrinti trečiąjį saugumo lygį, turi būti įgyvendintos pirmojo ir antrojo saugumo lygio organizacinės ir techninės asmens duomenų saugumo priemonės, nurodytos Bendrųjų reikalavimų 13 ir 14 punktuose, ir šios organizacinės ir techninės asmens duomenų saugumo priemonės: [...]<br>15.4. atsarginės asmens duomenų kopijos, jei jos daromos, saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;<br>15.5. šifruojami atsarginėse kopijose, archyvuose ir išorinėse duomenų laikmenose saugomi asmens duomenys;<br>16. Duomenų valdytojams ir duomenų tvarkytojams, tvarkantiems ypatingus asmens duomenis, atsižvelgiant į šių duomenų tvarkymo keliamą riziką, rekomenduojama įgyvendinti šias papildomas organizacines ir technines asmens duomenų saugumo priemones:<br>16.2. ne rečiau kaip kartą per 1 metus patikrinti avarinio asmens duomenų atkūrimo tvarką atliekant praktinius bandymus;<br>16.3. šifruoti aktyvioje (veikiančioje) duomenų bazėje saugomus asmens duomenis. | Policijos departamente asmens duomenų tvarkymo taisyklės nėra parengtos ir patvirtintos. Daugeliu atvejų asmens duomenų tvarkymas reglamentuotas atitinkamų registrų, sistemų, posistemių duomenų tvarkymo taisyklėse, tačiau šių dokumentų turinys neatitinka reikalavimų (pvz.: neapibrėžiama tai, kaip tvarkomi asmens duomenys, nenurodomas baigtinis tvarkomų asmens duomenų sąrašas kiekvienu asmens duomenų tvarkymo tikslu, automatiniu būdu tvarkomų asmens duomenų saugumo lygis ir kt.).<br>Nenustatytas skaičius leistinų nevykusių bandymų prisijungti prie Policijos departamento duomenų bazių, kuriose saugomi asmens duomenys.<br>Neregistruojami avarinio asmens duomenų atkūrimo veiksmai (kada ir kas vykdė asmens duomenų atkūrimo veiksmus tiek automatiniu, tiek neautomatiniu būdu).<br>Atsarginės asmens duomenų kopijos saugomos toje pačioje geografinėje vietoje kaip ir aktyvi (veikianti) duomenų bazė.<br>Nešifruojami atsarginėse kopijose ir archyvuose saugomi asmens duomenys.<br><br>Neatliekami asmens duomenų atkūrimo praktiniai bandymai.<br>Nešifruojami aktyvioje duomenų bazėje saugomi asmens duomenys. |
| Lietuvos Respublikos Vyriausybės 2004-04-19 nutarimu Nr. 451 (neteko galios 2013-03-02) patvirtintos Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės. Lietuvos Respublikos Vyriausybės 2013-02-27 nutarimu Nr. 180 (galioja nuo 2013-03-03) patvirtintas Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas. | | |
| 7. | 10. Patvirtinus informacinės sistemos nuostatus, rengiama informacinės sistemos specifikacija. Specifikacijos projektą rengia informacinės sistemos nuostatuose nurodytas informacinės sistemos valdytojas arba informacinės sistemos | Kuriant IS nebuvo parengtos specifikacijos: VPVS, PLVIS, PVVIS, Keleivių duomenų įrašų IS. |

| Eil. Nr. | Teisės akto reikalavimai | Auditorių pastebėjimai |
|---|---|---|
| | tvarkytojas. Specifikacijos projektas rengiamas vadovaujantis informacinės sistemos kūrimo metodiniais dokumentais.<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (23 p.). | |
| 8. | 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.<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (30 p.). | PRĮR, INDR, ITPR, VPVS, PLVIS, PVVIS, sukurtos ir naudojamos, tačiau nepatvirtinti ir neįregistruoti šių IS ir registrų priėmimo ir tinkamumo eksploatuoti aktai. |
| 9. | $17^2$. Sprendimą modernizuoti informacinę sistemą priima informacinės sistemos valdytojas. Priėmęs sprendimą modernizuoti informacinę sistemą, informacinės sistemos valdytojas rengia informacinės sistemos nuostatų pakeitimo projektą. Jis derinamas ir tvirtinamas šių Taisyklių $5–8^1$ p. nustatyta tvarka. [...]<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-02-27 nutarimu Nr. 180 patvirtintame apraše (33 p.). | PRĮR nuostatai nebuvo atnaujinti nuo 2011 m., nors 2013-2014 m. vykdytas šio registro tobulinimas įdiegiant policijos areštinių modulį.<br>*Audito metu padaryta pažanga: Lietuvos policijos generalinio komisaro 2015-02-06 įsakymu Nr. 5-V-124 atnaujinti PRĮR nuostatai, tačiau pakeitimas neregistruotas registrų ir informacinių sistemų registre.* |
| Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-10-15 įsakymu Nr. T-131 (neteko galios 2014-02-26) patvirtinta Valstybės Informacinių sistemų kūrimo metodika Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29 (galioja nuo 2014-02-26) patvirtinta Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika. | | |
| 10. | 22. IS projekto valdymo etapo metu turi būti sukurtas IS projekto planas, kuris nustatytų, kaip IS projektas bus vykdomas ir tvarkomas. Numatomas IS įgyvendinimo būdas (kompiuterizuojamo objekto valstybės tarnautojų ar darbuotojų, dirbančių pagal darbo sutartis, jėgomis ar sudarant sutartis su parinktais vykdytojais), nustatoma IS projekto struktūra (ar visas IS projektas bus skaidomas į smulkesnius IS projektus). [...] Aptariama IS projekto kontrolės ir jo rezultatų priėmimo tvarka. Visa tai aprašoma IS specifikacijoje. | 2012 m. pradėto vykdyti VPVS modernizavimo projekto metu nebuvo patvirtinta IS specifikacija, kurioje būtų aprašytas IS projekto planas. |
| 11. | 40. IS bandomosios eksploatacijos etapo metu, nuolat stebint, IS pradedama eksploatuoti. Pastebėti IS trūkumai protokoluojami.<br>Analogiški reikalavimai nustatyti 2014-02-25 įsakymo Nr. T-29 patvirtintoje metodikoje (45, 46, 47 p.). | VPVS bandomoji eksploatacija nebuvo vykdoma. |
| 12. | 41. IS trūkumų šalinimo etapo metu šalinami IS bandomosios eksploatacijos metu pastebėti trūkumai. Pašalinus trūkumus ir atlikus numatytus pakeitimus, IS vėl bandoma. Baigus bandymus, pasirašomas valstybės informacinės sistemos perdavimo-priėmimo aktas.<br>Analogiški reikalavimai nustatyti 2014-02-25 įsakymo Nr. T-29 patvirtintoje metodikoje (48 p.). | VPVS bandomoji eksploatacija nebuvo vykdoma, IS perdavimo-priėmimo aktas pasirašytas po testavimo darbų. |
| 13. | VIII skyrius. Eksploatuojant IS, rekomenduojama vesti IS eksploatacijos žurnalą ir fiksuoti visus IS sutrikimus bei visas vartotojų pastabas.<br>Peržiūrint IS eksploatacijos žurnalą, apibendrinamos jame sukauptos vartotojų pastabos, sprendžiama, ar reikia rengti IS tobulinimo specifikaciją. | VPVS eksploatacijos metu nebuvo vedamas IS eksploatacijos žurnalas. |
| Lietuvos Respublikos Vyriausybės 1997-09-04 nutarimu Nr. 952 (neteko galios 2013-08-08) patvirtinti Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. Lietuvos | | |

| Eil. Nr. | Teisės akto reikalavimai | Auditorių pastebėjimai |
|---|---|---|
| Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 (galioja nuo 2013-08-08) patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas. | | |
| 14. | 21. Atlikdami informacinės sistemos funkcijų pakeitimus, administratoriai turi laikytis informacinės sistemos valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos.<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame apraše (28 p.) | Policijos departamentas neturi patvirtintos pokyčių valdymo tvarkos. |
| 15. | 26. Saugos dokumentai valstybės institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Vidaus reikalų ministerija. | Saugos dokumentai Policijos departamente nebuvo persvarstomi (peržiūrimi) ne rečiau kaip kartą į metus. IS saugaus elektroninės informacijos tvarkymo taisyklės neatnaujintos nuo 2010-03-24, IS naudotojų administravimo taisyklės neatnaujintos nuo 2008-12-16, IS veiklos tęstinumo valdymo planas neatnaujintas nuo 2011-04-14. |
| 16. | 33. Informacinės sistemos valdytojas užtikrina efektyvų ir spartų informacinės sistemos funkcijų pokyčių (toliau vadinama – pokyčiai) valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas, įtakos vertinimą ir pokyčių prioritetų nustatymo procesus. Su tuo susijusios nuostatos numatomos informacinės sistemos valdytojo tvirtinamoje Informacinės sistemos pokyčių valdymo tvarkoje arba Saugaus elektroninės informacijos tvarkymo taisyklėse.<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame apraše (39 p.) | Policijos departamentas neturi patvirtintos IS pokyčių valdymo tvarkos, Saugaus elektroninės informacijos tvarkymo taisyklėse, taip pat neišdėstytos nuostatos, susijusios su pokyčių identifikavimo, suskirstymo į kategorijas, įtakos vertinimo ir pokyčių prioritetų nustatymo procesais. |
| 17. | 30. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje (http://www.vrm.lt/Rizikos_analize.pdf), Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis. | Rizikos vertinimas nebuvo atliktas 2012 m. (2012 m. II pusmetyje saugos įgaliotinio pareigybė buvo laisva). |
| 18. | 38. Teisės aktų nustatyta tvarka atliekant informacinių technologijų saugos atitikties vertinimą, rekomenduojama:<br>38.1. įvertinti saugos dokumentų ir realios informacijos saugos situacijos atitiktį;<br>38.2. inventorizuoti informacinės sistemos techninę ir programinę įrangą;<br>38.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų informacinės sistemos naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtas programas ir jų sąranką;<br>38.4. patikrinti (įvertinti) informacinės sistemos naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;<br>38.5. įvertinti pasirengimą užtikrinti informacinės sistemos veiklos tęstinumą įvykus saugos incidentui. | 2012 m. ir 2013 m. saugos įgaliotinis neatliko IT saugos atitikties vertinimo, saugos atitikties vertinimas atliktas tik 2014 m. |
| Lietuvos Respublikos vidaus reikalų ministro 2007-05-08 įsakymu Nr. 1V-172 (neteko galios 2013-08-08), patvirtintos Saugaus dokumentų turinio gairės. Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 (galioja nuo 2013-08-08) patvirtintas Saugos dokumentų turinio gairių aprašas. | | |
| 19. | 4 p. Saugaus elektroninės informacijos tvarkymo taisykles sudaro šie skyriai: [...]<br>4.3. „Saugaus elektroninės informacijos tvarkymas“, kuriame turi būti nurodyta: [...]<br>4.3.3. atsarginių duomenų kopijų darymo, saugojimo ir | Policijos departamento saugaus elektroninės informacijos tvarkymo taisyklėse nenurodyta kopijuojamų duomenų imtis bei atsarginių duomenų kopijų darymo metodai. |

| Eil. Nr. | Teisės akto reikalavimai | Auditorių pastebėjimai |
|---|---|---|
| | duomenų atkūrimo iš atsarginių duomenų kopijų tvarka, nurodant kopijuojamų duomenų imtį, atsarginių duomenų kopijų darymo metodus ir dažnumą, visiško ir dalinio duomenų atkūrimo bandymų metodus ir dažnumą bei atsakingus už atsarginių duomenų kopijų darymą, duomenų atkūrimą ir atsarginių duomenų kopijų apsaugą asmenis ir atsarginių duomenų kopijų saugojimo kontrolę; [...]<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame apraše (4.3.3. p.) | |
| 20. | 5 p. Informacinės sistemos veiklos tęstinumo planą sudaro šie skyriai: [...]<br>5.2. „Organizacinės nuostatos“, kuriame turi būti nurodyta: [...]<br>5.2.9. reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti elektroninės informacijos saugos incidento atveju.<br>5.3. „Aprašomosios nuostatos“, kuriame turi būti nurodyta:<br>5.3.1. informacinių technologijų įrangos sąrašai, šios įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai bei minimalus informacinės sistemos veiklos atkūrimui, nesant administratoriaus, reikalingos kompetencijos ar žinių lygis;<br>5.3.2. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos užtikrinti institucijos poreikius atitinkančią informacinės sistemos veiklą elektroninės informacijos saugos incidento metu, specifikacija; [...]<br>5.3.6. duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai.<br>Analogiški reikalavimai nustatyti Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame apraše (5.2.6, 5.3.1.1, 5.3.1.2, 5.3.1.5 p.). | Policijos departamento veiklos tęstinumo valdymo plane nenurodyti:<br>reikalavimai, keliami atsarginėms patalpoms, naudojamoms IS veiklai atkurti elektroninės informacijos saugos incidento atveju;<br>IT įrangos sąrašai, šios įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai bei minimalus IS veiklos atkūrimui, nesant administratoriaus, reikalingos kompetencijos ar žinių lygis;<br>minimalaus funkcionalumo IT įrangos, tinkamos užtikrinti institucijos poreikius atitinkančią IS veiklą elektroninės informacijos saugos incidento metu, specifikacija;<br>duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai. |
| Lietuvos Respublikos vidaus reikalų ministro 2008-10-27 įsakymu Nr. 1V-384 (neteko galios 2013-10-11) patvirtinti Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai. Lietuvos Respublikos vidaus reikalų ministro 2013-10-04 įsakymu Nr. 1V-832 (galioja nuo 2013-10-11) patvirtinti Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai. | | |
| 21. | 3. Bendrieji informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai:<br>3.1. turi būti periodiškai atliekamas informacinės sistemos informacinių technologijų saugos atitikties vertinimas; [...]<br>Analogiški reikalavimai nustatyti 2013-10-04 įsakymu Nr. 1V-832 patvirtintuose el. informacijos saugos reikalavimuose (5.1 p.) | Policijos departamente IS informacinių technologijų atitikties vertinimas atliktas tik 2014 m. |
| 22. | 3.9.4. informacinėje sistemoje turi būti naudojama tik legali programinė įranga;<br>Analogiški reikalavimai nustatyti 2013-10-04 įsakymu Nr. 1V-832 patvirtintuose el. informacijos saugos reikalavimuose (5.12.6 p.) | Policijos departamente 2014 m. IV ketvirtį buvo 9 401 kompiuterizuotos darbo vietos (be KŽTT), iš jų 8 401 buvo naudojama nelegali programinė įranga. |
| 23. | 3.9.10. turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti laikomos atskiroje patalpoje;<br>Analogiški reikalavimai nustatyti 2013-10-04 įsakymu Nr. 1V-832 patvirtintuose el. informacijos saugos reikalavimuose (5.12.12 p.) | IS ir registrų (PRĮR, ATPEĮR, IGR, ITPR, INDR, PLVIS, PVVIS) duomenų (elektroninės informacijos) kopijos laikomos toje pačioje patalpoje kaip ir tarnybinės stotys. |
| 24. | 4.17. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;<br>Analogiški reikalavimai nustatyti 2013-10-04 įsakymu Nr. 1V-832 patvirtintuose el. informacijos saugos reikalavimuose (5.14.1 p.) | IS ir registrų naudotojai administruojami naudojant IRD įrankį ADMIN III, tačiau slaptažodis sudaromas ne iš raidžių, skaičių ir specialiųjų simbolių. |
| 25. | 5.22. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;<br>Analogiški reikalavimai nustatyti 2013-10-04 įsakymu Nr. 1V-832 patvirtintuose el. informacijos saugos reikalavimuose (5.14.7.3 p.) | ADMIN III nėra kontrolės priemonių, kurios neleistų naudotojui nustatyti slaptažodį iš buvusių 6 paskutinių slaptažodžių. |

Valstybinio audito ataskaitos
„Policijos informacinių išteklių valdymas“
4 priedas

## Policijos departamento ir policijos įstaigų valdomi informaciniai ištekliai

| Nr. | Pavadinimas | Valdytojas | Nuostatai | Specifikacija | Svarba (kategorija) | Įteisinta | Pastabos |
|---|---|---|---|---|---|---|---|
| 1. | Policijos registruojamų įvykių registras (PRĮR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Ne | Planuojama modernizuoti į Policijos registruojamų įvykių IS |
| 2. | Administracinių teisės pažeidimų ir eismo įvykių registras (ATPEĮR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Taip | Nuo 2015-07-01 modernizuota į Administracinių teisės pažeidimų registrą (valdytojas VRM) ir Eismo įvykių registrą |
| 3. | Ieškomų ir rastų numeruotų bei individualius požymius turinčių daiktų ir dokumentų registras (INDR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Ne | |
| 4. | Ieškomų transporto priemonių registras (ITPR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Ne | |
| 5. | Ieškomų ginklų registras (IGR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Taip | |
| 6. | Prevencinio poveikio priemonių taikymo registras (PPPTR) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Taip | |
| 7. | DNR duomenų registras (DNR) | Policijos departamentas | Taip | Taip | II, svarbi elektroninė informacija | Taip | |
| 8. | Daktiloskopinių duomenų registras (DDR) | Policijos departamentas | Taip | Taip | II, svarbi elektroninė informacija | Taip | |
| 9. | Policijos elektroninių paslaugų sistema (PEPS) | Policijos departamentas | Taip | Taip | II, svarbi elektroninė informacija | Taip | |
| 10. | Vieninga pajėgų valdymo sistema (VPVS) | Policijos departamentas | Taip | Taip | III, žinybinės svarbos elektroninė informacija | Ne | |
| 11. | Policijos licencijuojamos veiklos informacinė sistema (PLVIS) | Policijos departamentas | Taip | Ne | II, svarbi elektroninė informacija | Ne | |
| 12. | Prevencinės veiklos valdymo informacinė sistema (PVVIS) | Policijos departamentas | Taip | Taip | III, žinybinės svarbos elektroninė informacija | Ne | |
| 13. | Keleivių duomenų įrašų informacinė sistema | Policijos departamentas | Ne | Ne | - | - | Kuriama |
| 14. | Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdybos informacinė sistema (TRV IS) | Lietuvos kriminalinės policijos biuras | Taip | Ne | III | Ne | Registrų ir informacinių sistemų registre neįregistruota |

Valstybinio audito ataskaitos
„Policijos informacinių išteklių valdymas“
5 priedas

## Gebos brandos modelis

Gebos brandos modelis (angl. – CMM) yra 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 neišvedamas, nes sudėtinių vertinimų vidurkiai neatspindi realios situacijos. Auditorius, vadovaudamasis modelio paaiškinamąja lentele (1 lentelė), turi užpildyti 2 paveikslėlyje pateiktą lentelę.

1 lentelė. Paaiškinamoji Gebos 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. |
|---|---|---|---|---|
| **0. Neegzistuojantis procesas** | Organizacija nepripažįsta spręstinos problemos egzistavimo ir dėl to apie tai nepateikia jokios informacijos. | Šiuo klausimu nėra jokios politikos. | Nėra jokio atpažįstamo proceso, susijusio su šia problema. | Neatliekamas joks vertinimas, susijęs su šia problema. |
| **1. Pirminis/Ad Hoc procesas** | Yra faktų, patvirtinančių, kad organizacija pripažįsta problemos egzistavimą ir būtinumą ją spręsti, tačiau apie tai per mažai informuojama. | Egzistuoja neišsami politika. Ji netinkamai dokumentuojama, skelbiama arba įgyvendinama. | Individualiu arba kiekvienu konkrečiu atveju taikomi *ad hoc* metodai. Problema nenagrinėjama vadovybės lygiu. | Stebėsena vykdoma reaguojant į incidentą, dėl kurio organizacija patiria tam tikrą nuostolį. |
| **2. Pasikartojantis, bet intuityvus procesas** | Apie problemą (prireikus) atitinkamai informuojama visa organizacija. | Egzistuoja aiški politika. | Su problema susiję procesai formaliai yra nustatyti, aktyviai dalyvaujant ir prižiūrint vadovybei, tačiau taikomi ne visoje organizacijoje. Mokymas neorganizuojamas, o informavimas apie standartus ir pareigas paliktas individualių darbuotojų nuožiūrai. | Vadovybė yra nustačiusi pagrindinius vertinimo objektus ir vertinimo metodus bei būdus, tačiau pastarieji parengti nepakankamai. |
| **3. Apibrėžtas procesas** | Visa organizacija supranta, kad reikia reaguoti į problemą, ir tam pritaria. | Organizacijoje vykdoma nuosekli ir aiški politika, suderinta su kai kuriomis kitomis susijusiomis | Procedūros standartizuotos, dokumentuotos ir dauguma jų įgyvendinamos visoje organizacijoje. Vadovybė yra informavusi apie standartizuotas procedūras ir vykdo neformalų | Susijusių veiklos sričių rodiklių registravimas ir stebėsena padeda tobulinti veiklą. Beveik visų susijusių procesų stebėsena vykdoma pagal tam tikrus |

| 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. |
|---|---|---|---|---|
| | | politikos kryptimis. Iš dalies atsižvelgiama į rizikos valdymą. | mokymą. Procedūras galima įvertinti, tačiau jos nėra sudėtingos ir formaliai atspindi esamą patirtį. | (pirminius) dokumentus, tačiau mažai tikėtina, kad vadovybė galėtų pastebėti bet kokį nukrypimą, nes tokios priemonės paprastai taikomos individualiai. Priežasčių analizė atliekama retai. |
| **4. Lengvai valdomas ir vertinamas procesas** | 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. |
| **5. Optimalus procesas** | 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, darbuotojų ir procesų sugebėjimą greitai prisitaikyti ir visapusiškai valdyti rizikos pokyčius. | Stebėsena, savianalizė ir informavimas apie problemą (prireikus) vykdomi visos organizacijos lygiu, optimaliai išnaudojant procesus ir technologijas, naudojamus vertinimo, analizės, informavimo ir mokymo tikslais. Analizuojamos visų problemų ir nukrypimų priežastys, laiku numatant ir inicijuojant veiksmingas priemones. Naudojamasi nepriklausomų ekspertų konsultavimo paslaugomis ir lyginamąja analize. |