Valstybinio audito ataskaita

YPATINGOS SVARBOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

2018 m. birželio 28 d. Nr. VA-2018-P-900-3-6

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

TURINYS

SANTRAUKA

Audito svarba

Valstybės informaciniai ištekliai yra informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma[1]. Ypatingos svarbos valstybės informaciniai ištekliai – ypatingos svarbos elektroninė informacija – tvarkomi pirmos kategorijos valstybės informacinėse sistemose, registruose ir kadastruose (toliau – IS). Šių sistemų pagalba įgyvendinamos svarbios valstybės funkcijos, pvz., valstybės finansų valdymas, mokesčių administravimas, sveikatos apsauga. Ypatingos svarbos informacijos praradimas ir IS, kurios tvarko šią informaciją, nepasiekiamumas gali turėti skaudžių pasekmių visuomenės saugumui ir gerovei bei ekonomikai.

Tinkamai sukurti ir efektyviai įgyvendinami informacinių technologijų procesai sudaro sąlygas veiksmingai apsaugoti informacinius išteklius nuo kylančių kibernetinių grėsmių. Pastaraisiais metais pasaulyje kibernetinių atakų taikiniu vis dažniau tampa ypatingos svarbos informaciniai ištekliai, kuriais teikiamos visuomenei svarbios paslaugos ir kuriuose saugoma ypač svarbi informacija. 2018 m. pasaulinių rizikų ataskaitoje nurodoma, kad ateityje šių atakų tikimybė augs, kartu augs pavojus sutrikdyti ypatingos svarbos informacinių išteklių darbą[2]. Nacionalinio kibernetinio saugumo centro duomenimis, kibernetinių incidentų Lietuvoje skaičius 2017 m. sudarė 54,4 tūkst. ir, palyginus su 2016 m., jų užregistruota dešimtadaliu daugiau[3]. Todėl, didėjant kibernetinių grėsmių lygiui, labai svarbu stiprinti ypatingos svarbos valstybės informacinių išteklių saugumą. Pasaulio kibernetinio saugumo indekso[4] 2017 m. rezultatais, Lietuva pasaulyje buvo 57-oje vietoje iš 165 šalių, o iš ES šalių – 23-ioje. Tai rodo, kad saugumo valdymo efektyvumas yra didintinas.

Aukščiausiosios audito institucijos 2006–2016 m. laikotarpiu atlikti informacinių technologijų bendrosios kontrolės vertinimai parodė besikartojančias IT valdymo sričių (planavimo, informacijos architektūros apibrėžimo, organizacinės struktūros, pokyčių, veiklos tęstinumo užtikrinimo, duomenų saugos, IT valdymo stebėsenos ir vertinimo) problemas. Audituotų viešojo sektoriaus subjektų IT valdymo branda per paskutinius dešimt metų vidutiniškai siekė pirmąjį brandos lygį iš 5-ių[5] ir šuo metu fiksuojame 1,7 brandos lygį. Žemas ypatingos svarbos valstybės informacinių išteklių brandos lygis rodo valstybės informacinių išteklių politikos formavimo ir įgyvendinimo trūkumus, o tai sudaro sąlygas didesniam šių išteklių pažeidžiamumui.

Aukščiausioji audito institucija nusprendė atlikti ypatingos svarbos valstybės informacinių išteklių auditą: įvertinti šių išteklių valdymo ir saugumo būklę ir numatyti priemones, kaip ją gerinti.

[1] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 2 str. 17 p.

[2] Pasaulio ekonomikos forumo pasaulinių rizikų ataskaita (angl. *Insight Report „The Global Risks Report 2018" by the World Economic Forum*). Prieiga per internetą: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[3] Prieiga per internetą: https://www.nksc.lt/.

[4] Pasaulinis kibernetinio saugumo indeksas *(angl.* Global Cyber Security Index, GCI), prieiga per internetą: https://www.itu.int/pub/D-STR-GCI.01-2017. Indeksas matuoja kibernetinio atsparumo galimybes 195 pasaulio valstybėse ir leidžia palyginti valstybių kibernetinio saugumo būklę.

[5] Pagal COBIT metodiką.

Audito tikslas ir apimtis

Tikslas – įvertinti ypatingos svarbos valstybės informacinių išteklių valdymą (bendrąją kontrolę), brandą ir nustatyti sistemines valstybės informacinių išteklių valdymo problemas.
Audito subjektai:

- Susisiekimo ministerija formuoja valstybės informacinių išteklių plėtros politiką. Audito metu Vyriausybė 2018-06-20 posėdyje priėmė sprendimą pritarti įstatymų pakeitimams, kuriais valstybės informacinių išteklių plėtros politikos, kai kurios registrų politikos ir informacinės visuomenės plėtros politikos formavimo ir koordinavimo funkcijos bus priskirtos Ūkio ministerijos kompetencijai[6];
- Vidaus reikalų ministerija iki 2018-01-01 formavo politiką valstybės informacinių išteklių saugos srityje;
- Krašto apsaugos ministerija formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą, nuo 2018-01-01 formuoja politiką valstybės informacinių išteklių saugos srityje;
- Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos atsako už valstybės informacinių išteklių funkcinį suderinamumą, kūrimą, tvarkymą ir plėtrą.

IT valdymo brandą vertinome 12-oje viešojo sektoriaus organizacijų[7], kurios tvarko 44-ias pirmos kategorijos IS, iš jų 10-yje atlikome detalią atrinktų IT valdymo procesų analizę. Dvi organizacijos nevertintos, nes vienos, atlikus pirminį vertinimą, branda siekė 0 lygį, kitoje po 2016 m. aukščiausios audito institucijos atlikto IT bendrosios kontrolės audito neįvyko pokyčių.

Atlikę visų 34-ių COBIT procesų išankstinį vertinimą, detalius vertinimus atlikome šiose rizikingiausiose srityse:

- IT strateginis planavimas;
- Informacinės architektūros nustatymas;
- IT rizikų valdymas;
- Pokyčių valdymas;
- Nepertraukiamo paslaugų teikimo užtikrinimas;
- Sistemų saugumo užtikrinimas;
- Duomenų tvarkymas;
- IT veiklos stebėsena ir vertinimas;
- IT valdymo užtikrinimas.

Procesų vertinimas apėmė ir organizacijos, ir nacionalinį IT valdymą, šių valdymo lygių abipusę sąveiką. Informacinių išteklių valdymą ir brandą vertinome pagal 2017 m. būklę. Analizuodami tam tikrų procesų nuoseklumą ir tęstinumą, naudojome 2014–2017 m. duomenis.

Auditas atliktas pagal Valstybinio audito reikalavimus ir tarptautinius aukščiausiųjų audito institucijų standartus. Vertinimas atliktas pagal COBIT[8] metodiką ir atitiktį Lietuvos Respublikos

[6] LR Vyriausybės posėdžio 2018-06-20 protokolas Nr. 27, 7 kl., Lietuvos Respublikos Vyriausybės kanceliarijos Politikos įgyvendinimo grupės 2018-06-20 pažyma Nr. NV-1585.

[7] Valstybinė mokesčių inspekcija, VĮ Registrų centras, Informatikos ir ryšių departamentas, Valstybinio socialinio draudimo fondo valdyba, VĮ Žemės ūkio informacijos ir kaimo verslo centras, Muitinės informacinių sistemų centras, Valstybinė maisto ir veterinarijos tarnyba, LR Seimo kanceliarija, Finansų ministerija, Informacinės visuomenės plėtros komitetas, Valstybinė ligonių kasa, Valstybinė miškų tarnyba.

[8] COBIT (*Control Objectives for Information and related Technologies*) – tarptautinės ISACA organizacijos standartas, aprašantis geriausią IT valdymo praktiką.

teisės aktų reikalavimams ir rekomendacijoms dėl valstybės informacinių išteklių valdymo. Ypatingos svarbos valstybės informacinių išteklių valdymo vertinimas atliktas vadovaujantis Informacinių technologijų audito vadovu[9], 5300-uoju tarptautiniu aukščiausiųjų audito institucijų standartu, Informacinių sistemų audito ir kontrolės asociacijos (ISACA) tarptautiniais audito standartais, atsižvelgta į ISACA audito gaires ir gerąją praktiką.

Audito apimtis ir taikyti metodai išsamiau aprašyti 2 priede „Audito apimtis ir metodai" (38 psl.). Atlikdami auditą darėme prielaidą, kad visi auditoriams pateikti dokumentai yra teisingi, išsamūs ir galutiniai, o jų kopijos atitinka originalus.

Išvados

Ypatingos svarbos valstybės informacinių išteklių valdymo brandos pokyčių tendencijos yra teigiamos, tačiau stebima pažanga, atsižvelgus į didėjantį kibernetinių grėsmių lygį, yra per lėta, ir šių išteklių saugumas turi būti užtikrinamas labiau. Tai lemia šie trūkumai:

1. Ypatingos svarbos valstybės informacinių išteklių nustatymo sistema yra nepakankamai veiksminga, kad būtų įgyvendinami saugumo sprendimai, atitinkantys realius poreikius:
    1.1. vertinimams, kurie pagrįstų valstybės informacinių išteklių ypatingą svarbą, trūksta objektyvumo, esant pokyčiams ne visada atliekami pakartotiniai vertinimai, šis procesas neprižiūrimas šalies mastu, o svarbos nustatymo gairės neužtikrino efektyvaus jo įgyvendinimo (1.1 poskyris, 12 psl.);
    1.2. ypatingos svarbos valstybės informacinių išteklių bei ypatingos svarbos informacinės infrastruktūros identifikavimo sistema nėra bendra, jie identifikuojami skirtingais būdais pagal informacijos ir paslaugų svarbą, o tai apsunkina šių išteklių nustatymo procesą (1.2 poskyris, 15 psl.);
    1.3. nėra sukurta nacionalinė informacinė architektūra, kuri atvaizduotų valstybės IS, jų tarpusavio ryšius, parodytų ypatingos svarbos valstybės informacinių išteklių mastą ir suteiktų galimybę priimti pagrįstus sprendimus dėl šių išteklių svarbos (1.2 poskyris, 15 psl.).
2. Valstybės informacinių išteklių valdymas turėtų labiau atitikti gerąsias IT valdymo praktikas ir standartus tam, kad vyktų kompleksinis IT srities tobulinimas, galintis prisidėti prie didesnės ypatingos svarbos valstybės informacinių išteklių valdymo pažangos:
    2.1. IT planavimas nėra darnus: planuojamos įgyvendinti IT priemonės pateikiamos skirtinguose dokumentuose, dėl strateginių dokumentų gausos trūksta sisteminio požiūrio, todėl sudėtinga nustatyti svarbiausius prioritetus ir nukreipti išteklius didžiausioms grėsmėms valdyti. Esant tokiai sistemai, IT plėtros planai ne visais atvejais parengiami, o parengtieji nėra išsamūs, nerengiami detalūs įgyvendinimo priemonių planai (2.1 poskyris, 17 psl.);
    2.2. IT stebėsena neužtikrina, kad organizacijose būtų matuojamas IT veiklos efektyvumas, o YSVII tvarkytojų atliekami auditai parodytų tikrą IT valdymo brandą. Šalies mastu nestebima faktinė IT valdymo būklė, sistemiškai neanalizuojama IT valdymo problematika. Sukurta Valstybės informacinių išteklių atitikties elektroninės informacijos saugos

[9] Patvirtintas LR valstybės kontrolieriaus 2017-06-21 įsakymu Nr. V-165.

reikalavimams stebėsenos sistema, skirta tik saugos atitikties stebėsenai palengvinti, tačiau jos funkcionalumas nėra pakankamai panaudojamas (2.2 poskyris, 19 psl.).

3. Nepakankamai veiksmingai įgyvendinamos priemonės, galinčios užtikrinti ypatingos svarbos informacinių išteklių atsparumą kibernetinių grėsmių lygiui, todėl šių išteklių pažeidžiamumo rizika išlieka:

   3.1. IT saugumo rizikų vertinimo veiksmingumas turėtų būti didinamas – identifikuojamos ne visos aktualios rizikos, o jų vertinimo metodika neatitinka naujausių IT valdymo praktikų, neužtikrinamas nepriimtinų rizikų valdymas laiku (3.1 poskyris, 23 psl.);

   3.2. sistemiškai nėra naudojamos organizacinės saugumo priemonės, galinčios sumažinti kibernetines grėsmes: IS kūrimo, modernizavimo, modifikavimo metu nepakankamai testuojamas saugumas, nepakankamai ugdomas personalas; nevaldoma programinės įrangos saugi konfigūracija ir atnaujinimai, IT veiklos tęstinumo ir atsarginių kopijų netinkamas valdymas kelia grėsmę veiklos atkūrimui, saugos veiksmingumo matavimai nėra pakankami ir neprisideda prie saugumo didinimo (3.2 poskyris, 26 psl.).

Rekomendacijos

Lietuvos Respublikos Vyriausybei

Siekiant užtikrinti geresnę valstybės informacinių išteklių valdymo kokybę ir aukštesnę YSVII tvarkytojų IT valdymo brandą, reikėtų:

1. Sukurti nacionalinę informacinę architektūrą ir jos valdymo mechanizmą, kuris leistų objektyviai nustatyti valstybės informacinių išteklių svarbą bei tinkamai kontroliuoti šį procesą ir suderinti ypatingos svarbos valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros nustatymo mechanizmus.
2. Išvystyti IT gerąsias valdymo praktikas atitinkantį valstybės informacinių išteklių valdymo mechanizmą, kuris užtikrintų bendrą ir į svarbiausius prioritetus orientuotą planavimą, numatytų siektiną IT valdymo brandos lygį ir pažangą vertinti leidžiantį stebėsenos mechanizmą, efektyviai naudojant sukurtas technines priemones.

Krašto apsaugos ministerijai

Siekiant užtikrinti ypatingos svarbos valstybės informacinių išteklių saugumą ir atsparumą didėjančioms kibernetinėms grėsmėms, reikia:

3. Gerinti kibernetinio saugumo rizikų valdymą: atnaujinti reikalavimus, metodikas, ir diegti nacionalinį IT rizikų valdymą, leidžiantį veiksmingai valdyti šalies mastu aktualias rizikas.
4. Didinti kibernetinio saugumo valdymo organizavimo ir įgyvendinimo efektyvumą: sukurti reikiamus kontrolės mechanizmus, kurie prisidėtų prie žmogiškųjų išteklių saugumo žinių ir gebėjimų didinimo, saugumo reikalavimų įgyvendinimo būklės gerėjimo ir IS pažeidžiamumų prevencijos.

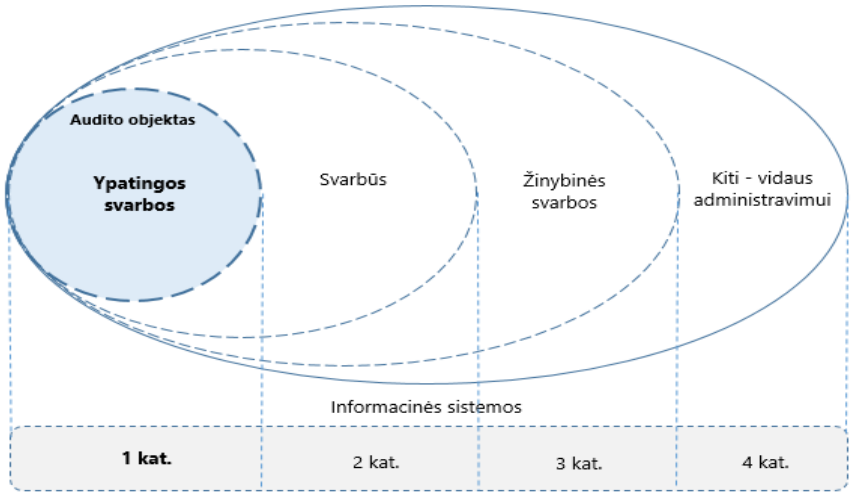
Rekomendacijų įgyvendinimo priemonės ir terminai pateikti ataskaitos dalyje „Rekomendacijų įgyvendinimo planas“ (33 psl.). Informacija apie ypatingos svarbos valstybės informacinių išteklių tvarkytojų IT brandos lygį buvo pateikta atskirais raštais.

ĮŽANGA

Kiekviena Vyriausybė turi pareigą teikti būtiniausias paslaugas savo gyventojams. Dauguma šių paslaugų yra priklausomos nuo IS, kuriose kaupiama daug jautrios informacijos, todėl jų patikimumas ir saugumas užima svarbią vietą priimant strateginius sprendimus.

Valstybės informaciniai ištekliai pagal informacijos svarbą skirstomi į ypatingos svarbos, svarbius, žinybinės svarbos ir kitus[10]. YSVII sudaro visai valstybei svarbi informacija, apdorojama 1 kategorijos valstybės IS; šios informacijos praradimas gali sukelti pasekmes visos valstybės mastu (žr. 1 pav.).

1 pav. Audito objektas



Šaltinis – AAI

2017 m. įvyko svarbus pokytis – buvo identifikuota viešojo ir privataus sektorių ypatingos svarbos informacinė infrastruktūra (angl. *critical information infrastructure*) ir sudarytas jos sąrašas[11]. Į jį pateko ypatingos svarbos infrastruktūros objektai, teikiantys ypatingos svarbos paslaugas.

Valstybės informacinių išteklių plėtros politiką formuoja Susisiekimo ministerija[12], o įgyvendina ir atsako už valstybės informacinių išteklių funkcinį suderinamumą, kūrimą, tvarkymą ir plėtrą – Informacinės visuomenės plėtros komitetas[13]. Šios politikos kontekste formuojami IT valdymo reikalavimai, kurie turi įtakos ypatingos svarbos valstybės informacinių išteklių valdymui.

Krašto apsaugos ministerija formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą[14], nuo 2018-01-01 formuoja politiką valstybės informacinių išteklių saugumo srityje[15] (iki 2018-01-01 ją formavo Vidaus reikalų ministerija). Valstybės informacinių išteklių saugumo politikos formavimo kontekste nustatomi saugumo valdymo standartai ir reikalavimai, leidžiantys įvertinti šių išteklių svarbą.

[10] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 3 str.
[11] LR Vyriausybės nutarimu patvirtintas ypatingos svarbos informacinės infrastruktūras sąrašas yra riboto naudojimo dokumentas.
[12] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 5 str. 2 d.
[13] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 6 str. 2 d.; Informacinės visuomenės plėtros komiteto nuostatai, patvirtinti susisiekimo ministro 2010-06-23 įsakymu Nr. 3-401 (2017-03-06 įsakymo Nr. 3-103 redakcija), 2 ir 9 p.
[14] LR kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 4 str. 2 d.
[15] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 5 str. 4 d.

Valstybės IS valdo valdytojas, koordinuoja IS funkcionavimą, metodiškai vadovauja ir prižiūri tvarkytoją. Už valstybės IS tinkamą veikimą ir duomenų saugą atsako tvarkytojas[16]. Kiekvienai IS turi būti skiriamas saugos įgaliotinis, kuris atsako už saugos reikalavimų vykdymą[17].

2017 m. Lietuvoje funkcionavo 44-ios pirmos kategorijos valstybės IS, kurių saugumo užtikrinimas ir tvarkymas patikėtas 12-ai viešojo sektoriaus organizacijų.

Šių IS kūrimui, modernizavimui ir palaikymui per 2014–2017 m. patirta 74,4 mln. Eur sąnaudų, kasmet vidutiniškai 18,6 mln. Eur. Iš jų palaikymo sąnaudos sudaro apie 41 proc., jos kasmet auga.

[16] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 33 ir 34 str. Institucija, paskirta valstybės informacinės sistemos valdytoja, gali būti ir valstybės informacinės sistemos tvarkytoja.

[17] Ten pat, 44 str.

AUDITO REZULTATAI

YSVII praradimas ir neveikimas gali turėti neigiamų pasekmių visuomenės ir valstybės interesams, todėl svarbu užtikrinti šių išteklių saugumą tinkamai valdant IT procesus. Valdymo procesų lygį leidžia įvertinti brandos modeliai. COBIT metodikoje nurodyta, kad kritiniams procesams ir sistemoms reikia griežtesnio saugumo valdymo nei tiems, kurie mažiau svarbūs[18], todėl siektinas brandos lygis valdymo procesams turėtų būti 3, o saugumo procesams – 4.

Brandos lygių apibūdinimas pagal COBIT metodiką

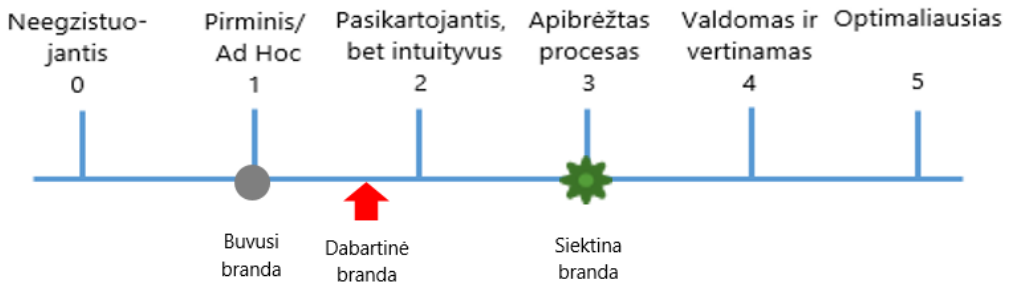
3-sis brandos lygis reikalauja procesų, politikos ir procedūrų apibrėžimo ir dokumentavimo, gerosios praktikos taikymo. Turi būti nustatyti ir procesų savininkai, atsakomybė ir atskaitomybė, apibrėžti ir dokumentuoti kompetencijos reikalavimai.

4-asis brandos lygis reikalauja išsamaus procesų dokumentavimo, standartų naudojimo procesams kurti ir valdyti, atliekami veiklos efektyvumas ir rezultatyvumas vertinamai, taikoma subalansuotų matavimo kriterijų sistema, analizuojamos pirminės priežastys, atsiranda nuolatinis tobulėjimas. Šis brandos lygis reikalauja, kad nuolat būtų atnaujinami kompetencijos reikalavimai, o ypač svarbiose srityse būtų reikalaujama aukšto lygio kompetencijų, skatinamas sertifikavimas.

AAI ankstesnių auditų rezultatai (2006–2016 m.) rodo, kad YSVII sektoriaus IT valdymo branda per paskutinius 10 metų siekė 1 lygį: procesams ir praktikai buvo taikomi *ad hoc* metodai: trūko aiškios IT valdymo politikos, darbuotojai, neturėdami aiškių tvarkų, savo iniciatyva sprendė tam tikrus klausimus, nevyko veiklos stebėsena.

Įvertinę 12-os YSVII tvarkytojų IT valdymo 2017 m. brandą, nustatėme, kad ji gerėja lėtai ir vis dar lieka žema – vidutinis IT valdymo brandos lygis yra 1,7 (žr. 2 pav.); tik vienas YSVII tvarkytojas siekia 3 brandos lygį, septyni – 2, trys – 1 ir vienas tvarkytojas – 0.

2 pav. YSVII tvarkytojų (sektoriaus) branda 2017 m.

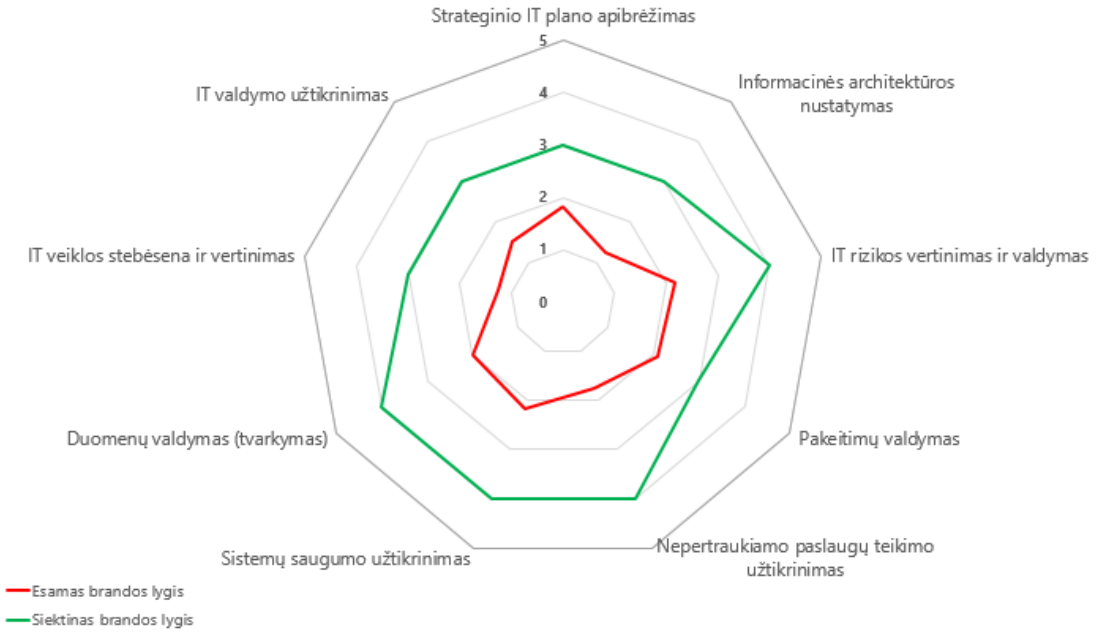


Šaltinis – AAI

Atlikti strateginio planavimo, architektūros nustatymo, rizikos, pakeitimų valdymo, nepertraukiamo paslaugų užtikrinimo, sistemų saugumo, duomenų valdymo, veiklos stebėsenos ir IT valdymo užtikrinimo procesų brandos vertinimai. Esamas ir siektinas brandos lygiai pagal kiekvieną procesą pateikiami 3 paveiksle.

[18] COBIT 4.1, 2011 m., Vilnius, 19 p.

3 pav. Vertintų procesų branda



Šaltinis – AAI

YSVII tvarkytojų bendrosios kontrolės vertinimo rezultatai rodo, kad yra sisteminių IT valdymo problemų, lemiančių nepakankamą YSVII tvarkytojų valdymo brandą. Šių problemų detalesnė analizė, atlikta 10-yje organizacijų, tvarkančių YSVII, pateikiama toliau skyriuose.

1. NEVEIKSMINGA YPATINGOS SVARBOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ NUSTATYMO SISTEMA

COBIT metodikoje nurodyta[19], kad apibrėžtas informacinės architektūros modelis padeda visus informacinius išteklius sujungti į visumą ir užtikrina, kad vadovybei ir naudotojams bus teikiama patikima, nuosekli ir išsami informacija apie turimus informacinius išteklius ir jų svarbumą. Nustatant informacinę architektūrą, turi būti sudarytas duomenų klasifikavimo planas, nustatomi saugumo lygiai. Informacinė architektūra leidžia racionaliai panaudoti informacinius išteklius, juos kiek įmanoma lanksčiau derinti su vykdomos veiklos strategija. Atsižvelgus į valdomų YSVII įvairovę, jų svarbą ir vykstantį konsolidavimo procesą[20], pagrįsti ir nustatyti tinkamą valstybės informacinę architektūrą ypač svarbu – tai suteiktų galimybę veiksmingai juos valdyti, analizuoti, modernizuoti ir apsaugoti nuo kibernetinių grėsmių.

[19] COBIT 4.1, 2011 m., Vilnius; PO2 procesas, 33 psl.

[20] LR Vyriausybės 2015-05-13 nutarimas Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“.

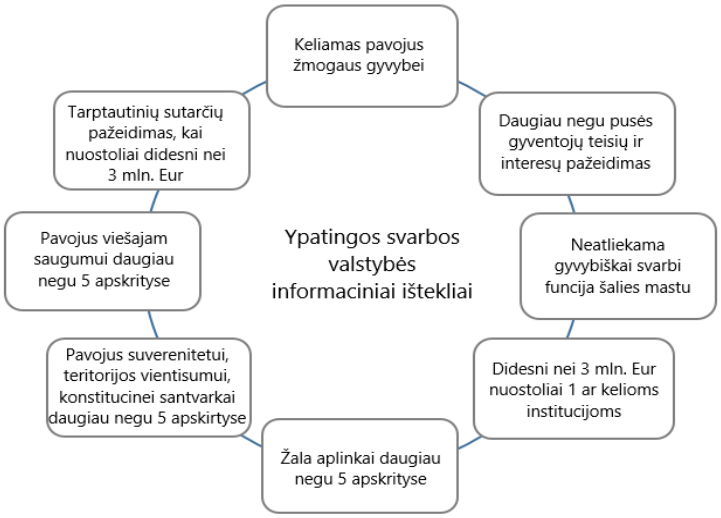
1.1. Netinkamai nustatoma ypatingos svarbos valstybės informacinių išteklių svarba

Nuo 2012 m., įsigaliojus Valstybės informacinių išteklių įstatymui[21], buvo sukurta informacijos klasifikavimo sistema, kuri pagal informaciniuose ištekliuose apdorojamos informacijos svarbą leido klasifikuoti IS kaip ypatingai svarbias ir mažiau reikšmingas. Įvertinus šį procesą nustatyta, kad:

- Neatliekami vertinimai, kurie pagrįstų valstybės informacinių išteklių ypatingą svarbą

Norint priskirti IS, registrus prie YSVII turi būti įvertintas informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo poveikis pagal nustatytus kriterijus[22] (žr. 4 pav.).

4 pav. YSVII nustatymo kriterijai



Šaltinis – AAI

Devyni valdytojai neatlieka vertinimų, kurie pagrįstų IS priskyrimą prie pirmos kategorijos[23]. Nustatant svarbą, apsiribojama darbuotojų nuomone, neatliekama detalesnių analizių ir skaičiavimų dėl galimos žalos. YSVII tvarkytojai pripažįsta, kad tam tikros IS neturi būti 1 kategorijos, toks vertinimas buvo atliktas dėl galimybės gauti finansavimą. Tai rodo, kad ypatingos svarbos valstybės informaciniai ištekliai gali būti neteisingai priskirti tiek prie aukštesnės, tiek prie žemesnės svarbos.

Vidaus reikalų ministerijos nuomonė

Vidaus reikalų ministerijos nuomone, informacinių išteklių svarbą galima nustatyti tik atsižvelgiant į darbuotojų nuomonę, priešingu atveju objektyvus vertinimas būtų galimas tik įvykus incidentui ir įvertinus realų poveikį.

[21] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807.

[22] Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto LR Vyriausybės 2013-07-24 nutarimu Nr. 716, 7 ir 13 p.

[23] Audito metu dokumentų, kurie pagrįstų IS priskyrimą prie 1 kategorijos, nepateikta.

- Įvykus pokyčiams neatliekami priskyrimo svarbai pakartotiniai vertinimai

Informacinių išteklių svarba laike gali kisti – tai priklauso nuo vykstančių teisinių pokyčių, atliekamo IS modernizavimo proceso, todėl turi būti laiku užtikrinama svarbos peržiūra. YSVII nustatymo kriterijai, tikslinant žalos ribas, keitėsi 2013 ir 2016 m., tačiau 8 organizacijos neperžiūrėjo išteklių svarbos ir neatnaujino duomenų saugos nuostatų. Svarba nėra peržiūrima ir kiekvieną kartą atliekant IS modernizavimą, pasikeitus IS sąsajoms su kitomis IS.

- Šalies mastu neveikia svarbos nustatymo kontrolės mechanizmas

VRM, derindama duomenų saugos nuostatų projektą, turi įvertinti atliktą priskyrimo konkrečiai svarbos kategorijai pagrįstumą ir prireikus pateikti savo išvadas[24]. Nustatyta, kad priežiūros funkcija buvo atliekama formaliai – derinant saugos nuostatus nebuvo reikalauta pateikti pagrindimo dokumentų, peržiūra apsiribojo šių nuostatų turinio patikrinimu. VRM neanalizavo organizacijų vertinimų, kartais prašydavo pateikti papildomos informacijos.

- Į 1 kategorijos IS sudėtį įtraukiamos kitos su IS susijusios savarankiškos IS

Vertindami 1 kategorijos IS architektūrą, nustatėme, kad dviejų IS architektūrą apėmė kitos savarankiškos sistemos, pvz., dokumentų valdymo, rizikų vertinimo ir kt. Kurdamos šią architektūrą institucijos taiko skirtingą praktiką – vienos detaliai deklaruoja visas turimas IS Registrų ir informacinių sistemų registre[25] ir rengia kiekvienos jų IS dokumentus, kitos registruoja vieną IS su daugybe posistemių, rengiamas vienas dokumentų paketas. Minėtame registre turi būti skelbiama informacija apie valstybės informacinius išteklius, tačiau nėra galimybės gauti patikimos informacijos apie valstybės informacinius išteklius pagal tvarkomos informacijos svarbą.

Minėtos problemos rodo, kad esama valstybės informacinių išteklių vertinimo ir nustatymo sistema priklauso nuo IS valdytojo ir tvarkytojo nuomonės. Tai nesudaro prielaidų tinkamai identifikuoti YSVII ir neparodo tikro šių išteklių masto. Neturint tikslių duomenų apie YSVII, gali būti diegiamos faktinio poreikio neatitinkančios saugumo priemonės[26]. Patvirtintos Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairės[27] neišsamios – nėra metodinių rekomendacijų, kaip įvertinti svarbą pagal visus kriterijus, neaišku, kokiais atvejais organizuoti pakartotinį vertinimą.

Ypatingos svarbos valstybės informacinių išteklių nustatymo procesas galėtų būti objektyvesnis ir labiau prižiūrimas turint nacionalinę informacinę architektūrą, kuri vizualizuotų visus valstybės informacinius išteklius ir tarp jų esančias sąsajas.

Saugumo srityje pirmaujančios valstybės sukūrė nacionalinę informacinę architektūrą, kuri padeda priimti strateginius informacinių išteklių plėtros ir saugumo sprendimus. Pavyzdžiui, JAV ir Estija paskyrė valstybės vyriausiąjį IT architektą, kuris atsako už minėtos architektūros tvarkymą. Estijos nacionalinė informacinė architektūra naudojama vertinant informacinių išteklių kritiškumą,

[24] Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas LR Vyriausybės 2013-07-24 nutarimu Nr. 716 (2016-08-11 redakcija Nr. 826), 15 p.

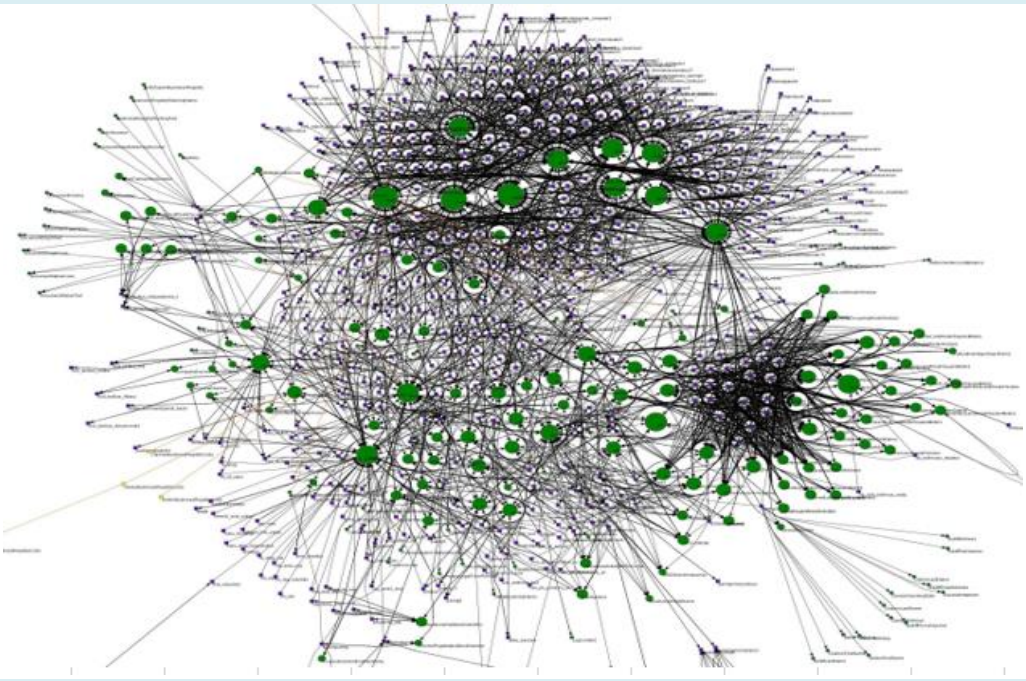
[25] Registrų ir valstybės informacinių sistemų registras, prieiga per internetą: http://registrai.lt/login.

[26] LR Vyriausybės 2016-04-20 nutarimas Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“.

[27] Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas LR Vyriausybės 2013-07-24 nutarimu Nr. 716.

nustatant poveikį paslaugų veikimui ir mažinant įvairias rizikas. Ši architektūra yra nuolatos atnaujinama pagal vykstančius pokyčius (žr. 5 pav.).

5 pav. Estijos nacionalinė informacinė architektūra



Šaltinis – https://cio.event.idg.se/wp-content/uploads/sites/13/2017/09/ciogovernance2017-kotka.pdf

Šiuo metu Lietuvoje formuojamas naujas požiūris į bendrą informacinių ir ryšių technologijų valdymą ir planuojami nauji strateginiai sprendimai – kuriamas Informacinių išteklių vadovo biuras [28], kuris turėtų koordinuoti IT valdymo klausimus, užtikrinti architektūros standartų adaptavimą, sudaryti ir nuolatos atnaujinti duomenų žemėlapį šalies mastu[29].

Valstybės informacinių išteklių infrastruktūros konsolidavimo proceso rėmuose parengta paraiška projektui, kurio metu planuojama sudaryti valstybės informacinių išteklių sąsajų žemėlapį. IVPK atstovai teigia, kad duomenų žemėlapis turėtų atskleisti, kaip sąveikauja IS atliekant viešojo administravimo veiksmus, parodytų duomenų srautus.

Mūsų nuomone, minėtų pokyčių kryptis atitinka pažangių šalių gerąsias valdymo praktikas, tačiau šiame etape duomenų žemėlapio panaudojimo būdai nėra pakankamai aiškūs. Reikėtų atskirti informacinę architektūrą, kuri yra informacijos elementų, jų tarpusavio ryšių sistema ir šios sistemos valdymo metodas, apimantis atsakomybes, nuo paprasto duomenų ryšių atvaizdavimo brėžinio. Esant skirtingam suvokimui apie informacinę architektūrą (ir organizacijos veiklos architektūrą), yra rizika, kad jos modelio parinkimas, tinkamų organizacinių struktūrų ir kompetencijų panaudojimas bus pakeistas tik statine duomenų ryšių „nuotrauka", nesprendžiant informacinei architektūrai keliamų uždavinių.

Siekiant tobulinti ypatingos svarbos valstybės informacinių išteklių nustatymo sistemą, turi būti sukurta nacionalinė informacinė architektūra [30], kuri apimtų viešojo sektoriaus valdomos informacijos, IS (registrų) duomenų ir technologinę architektūrą, būtų nurodyti visi komponentai (taikomos technologijos, duomenys, duomenų srautai tarp IS), taip pat atsakomybes ir procesą šiai architektūrai valdyti, kuris būtų pritaikomas ypatingos svarbos valstybės informacinių išteklių

[28] LR Vyriausybės 2017-03-13 nutarimas Nr. 167 „Dėl Lietuvos Respublikos Vyriausybės programos įgyvendinimo plano patvirtinimo".

[29] 2017-05-30 Ekspertų tarybos rekomendacijos dėl valstybės IT infrastruktūros išteklių konsolidavimo. 2017 m. lapkričio mėn. pristatymo medžiaga apie planuojamus pokyčius LR Seimo Audito komitetui.

[30] Informacinė architektūra – tai informacijos ir jos valdymo visuma.

vertinimui ir nustatymui. Taip pat turi būti sukurtas stebėsenos mechanizmas, kuris užtikrintų valstybės informacinių išteklių svarbos vertinimo pagrįstumo ir pervertinimo priežiūrą.

Suinteresuotų šalių nuomonės dėl nacionalinės valstybės informacinių išteklių architektūros

- KAM ir NKSC atstovų nuomone, nacionaliniu lygiu IT architektūra iki šiol nėra aiški, o tai užtikrinti gali tik tam paskirtas nacionalinio lygmens proceso šeimininkas.
- NRD CS nuomone[31], Lietuvoje nėra bendro viešojo sektoriaus IS architektūros matymo, IS architektūra galėtų parodyti priklausomybę tarp IS ir poveikį.

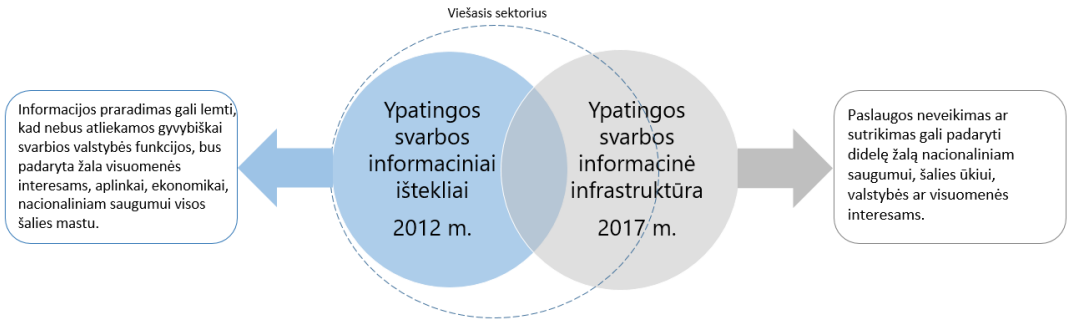
1.2. Ypatingos svarbos valstybės informacinių išteklių bei ypatingos svarbos informacinės infrastruktūros identifikavimo sistema nėra bendra

2014 m. įsigaliojus LR kibernetinio saugumo įstatymui buvo įtvirtinta nauja sąvoka – ypatingos svarbos informacinė infrastruktūra. Parengus jos identifikavimo metodiką[32], 2017 m. sudarytas šalies ypatingos svarbos informacinės infrastruktūros sąrašas. Tokia praktika taikoma daugelyje ES valstybių (Austrija, Kipras, Čekija, Estija, Suomija, Prancūzija, Vengrija, Latvija, Nyderlandai, Lenkija, Slovėnija, Šveicarija, Didžioji Britanija kt.)[33] ir atitinka Tinklų ir informacinių sistemų saugumo direktyvą[34].

Skirtingai nei ypatingos svarbos valstybės informacinių išteklių nustatymo atveju, ypatingos svarbos informacinė infrastruktūra identifikuojama atsižvelgiant ne į valdomos informacijos, o į teikiamų paslaugų svarbą. Ji apima ne tik viešojo, bet ir privataus sektoriaus informacinę infrastruktūrą – elektroninių ryšių tinklus, IS, tame tarpe pramoninių procesų valdymo, šių sistemų dalis ar jų grupes.

Įdiegus ypatingos svarbos informacinės infrastruktūros nustatymo sistemą, viešojo sektoriaus atveju, ypatingos svarbos informacinių išteklių ir informacinės infrastruktūros vertinimo ir nustatymo procesas tapo dvilypis. Abiem atvejais siekiama identifikuoti svarbiausius valstybės informacinius išteklius, kurių praradimas ir (ar) neveikimas gali sukelti žalą visai valstybei, tik tai atliekama skirtingais būdais (žr. 6 pav.).

6 pav. Ypatingos svarbos valstybės informaciniai ištekliai ir informacinė infrastruktūra



Šaltinis – AAI

[31] Technologinių kibernetinės gynybos konsultacijų, reagavimo į saugos incidentus bei taikomųjų mokslinių tyrimų įmonės UAB „NRD CS“ ekspertai rengė ypatingos svarbos valstybės informacinės infrastruktūros nustatymo metodiką ir savo iniciatyva prisidėjo rengiant duomenų žemėlapį teisėsaugos ir kontrolės institucijoms.

[32] LR Vyriausybės 2016-07-20 nutarimas Nr. 742 „Dėl Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“.

[33] ENISA dokumentas „Critical Information Infrastructures Protection approaches in EU“ (2015 m.), prieiga per internetą: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf.

[34] Europos Parlamento ir Tarybos 2016-07-06 direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, 5 ir 6 str.

Kuriant ypatingos svarbos informacinės infrastruktūros nustatymo sistemą nebuvo peržiūrėta egzistuojanti valstybės informacinių išteklių klasifikavimo sistema, jos suderinamumas su naujai diegiamu procesu[35]. Kai kurie YSVII tvarkytojai pripažįsta, kad minėti procesai kelia papildomą administracinę naštą, nes jie vienas kitą dubliuoja – abiem atvejais reikia vertinti neigiamą poveikį tai pačiai informacinei infrastruktūrai.

Ypatingos svarbos valstybės informacinių išteklių bei informacinės infrastruktūros identifikavimo mechanizmas neigiamai veikia visą šių išteklių identifikavimo procesą. Netinkamai nustatyti ypatingos svarbos valstybės informaciniai ištekliai gali būti neidentifikuojami kaip ypatingos svarbos informacinė infrastruktūra. Yra parengta ypatingos svarbos informacinės infrastruktūros nustatymo metodika, tačiau 1.1 poskyryje nurodytos problemos (subjektyvus vertinimas, nepakankama kontrolė, ne laiku atliekamas pakartotinis vertinimas) gali kartotis ir šiuo atveju.

Siekiant aiškiai identifikuoti ypatingos svarbos valstybės informacinius išteklius ir nekartoti vertinimo klaidų, turi būti vieningas požiūris dėl jų nustatymo, suderinant abu mechanizmus – kartu vertinant informacijos ir paslaugų svarbumą bei galimą žalą visuomenės ir valstybės interesams, naudojant sukurtą nacionalinę informacinę architektūrą.

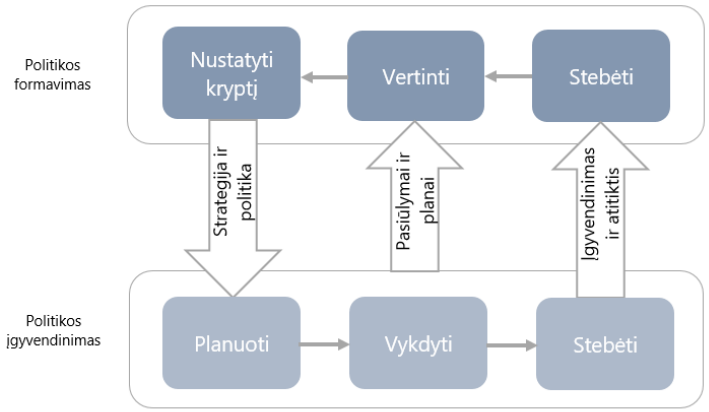
2. VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO SISTEMA NEPRISIDEDA PRIE YPATINGOS SVARBOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO GERINIMO

Ypatingos svarbos valstybės informacinių išteklių valdymo brandą lemia šalies valstybės informacinių išteklių valdymo efektyvumas. Pastarųjų išteklių valdymas užtikrina kryptingą IT valdymą, derinant IT išteklius su veiklos strategija ir prioritetais, kurie atitinka esamą aplinką, vykstančius pokyčius, yra paremti rizikų vertinimo rezultatais ir skirti mažinti pagrindines grėsmes. IT valdymo stebėsena suteikia galimybę aukščiausio lygio vadovams gauti patikimą informaciją apie nustatytos krypties ir tikslų įgyvendinimą, nuokrypius, silpnąsias valdymo vietas ir imtis veiksmų tobulinant sukurtą valdymo sistemą, siekiant didžiausios naudos[36] (žr. 7 pav.).

[35] 2017-12-21 pokalbis su NRD CS atstovu, kuris dalyvavo kuriant ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką.

[36] COBIT 4.1, 2011 m., Vilnius; PO1, ME1, ME4 procesai, 29-32, 153-156, 165-168 psl.

7 pav. Valstybės informacinių išteklių valdymo ciklas



Šaltinis – AAI pagal ISO 38500 standartą[37] ir COBIT metodiką

2.1. IT strateginis planavimas nėra darnus

Vadovaujantis Valstybės informacinių išteklių valdymo įstatymu, institucija, valdanti ypatingos svarbos valstybės informacinius išteklius, rengia trejų metų IT plėtros planą. Jame nurodo IRT tobulinimo ir plėtros kryptis, IT priemonių naudojimo tikslus, uždavinius, planuojamų kurti ar modernizuoti technologinių sprendimų prioritetus, reikalingus finansinius, žmogiškuosius išteklius, organizacines, teisines priemones, kvalifikacinius reikalavimus darbuotojams, jų mokymų poreikis, veiklos organizavimo kontrolę[38]. Šis planas turi būti suderintas su šalies strateginio planavimo dokumentais[39].

Įvertinus IT strateginio planavimo procesą ir peržiūrėjus YSVII IT plėtros planus, nustatyta, kad šis procesas yra formalus, nes:

- 4 YSVII valdytojai nėra parengę IT plėtros planų, kai kurie iš jų nemato poreikio rengti.
- Tais atvejais, kai IT plėtros planai yra parengti, jie nėra išsamūs: aiškiai nedetalizuojami visi turimi IT ištekliai, ir žmogiškieji, IT tikslai, uždaviniai ir prioritetai, nenurodomi kriterijai, skirti plano tikslams ir uždaviniams siekti ir stebėti[40].
- Nėra aiškių sąsajų su Vyriausybės ar Seimo patvirtintais planavimo dokumentais, Vyriausybės numatytomis taikomų IRT tobulinimo ir plėtros kryptimis.
- Organizacijų metiniuose veiklos planuose nedetalizuojami darbai numatyti IT plėtros planuose.
- IT plėtros planai kiekvienais metais neatnaujinami pagal vykstančius pokyčius.

[37] LST ISO/IEC 38500, Organizacijos informacinių technologijų valdymas (tapatus ISO/IEC 38500:2008), © ISO/IEC 2008.

[38] Valstybės informacinių išteklių valdymo įstatymo, 2011-12-15 Nr. XI-1807, 9 str.

[39] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013-03-14 įsakymo Nr. T-29 „Dėl Informacinių technologijų plėtros planų derinimo tvarkos aprašo patvirtinimo“, 9 p.

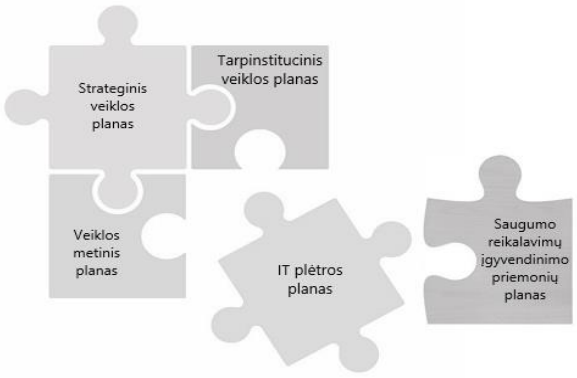
[40] Pvz., viename iš planų nurodytas planuojamas sukurti naujų IT paslaugų skaičius, tačiau nedetalizuojama, kokios naujos IS kuriamos / modernizuojamos; numatyti tik priemonių įgyvendinimo rezultato rodikliai (pvz., sukurtų naujų el. paslaugų skaičius, integruotų IS skaičius), tačiau nėra nurodyta, kokį poveikį (įtaką institucijos veiklai) šie veiksmai lems, nėra numatyti kokybiniai bei kiekybiniai šio poveikio kriterijai; nėra nurodyta informacija apie visų plane nurodytų IT tikslų ir uždavinių finansavimą prioriteto tvarka; nėra pateikiama informacija apie kvalifikacinius reikalavimus IT personalui, nėra identifikuotas konkrečių mokymų poreikis.

YSVII tvarkytojų nuomonė dėl IT planavimo sistemos

YSVII tvarkytojai pripažįsta, kad esama IT planavimo sistema jų netenkina, nes yra daug strateginio planavimo dokumentų, IT plėtros planas padidina administracinę naštą, manoma, kad IT planavimo dokumentai turėtų būti labiau integruoti į bendrą planavimo sistemą.

Dėl planavimo dokumentų gausos IT strateginis planavimas yra fragmentiškas, trūksta bendro požiūrio į IT srities strateginį planavimą – IT plėtros planuose planuojamos investicijos, siekiant modernizuoti IS pagal veiklos poreikius, tačiau priemonės, susijusios su saugumo užtikrinimu, planuojamos atskirai (žr. 8 pav.).

8 pav. Trumpos trukmės (iki 3 m.) strateginiai planavimo dokumentai



Šaltinis – AAI

YSVII saugumo užtikrinimas turi būti aukščiausio lygio prioritetas tiek valstybei, tiek organizacijoms valdančioms, tvarkančioms YSVII. Esamas planavimas nesuteikia galimybių įvertinti svarbiausius prioritetus atsižvelgiant į esamas grėsmes, todėl finansiniai ištekliai ne visada gali būti nukreipiami aktualioms saugumo problemoms spręsti.

Laiku neįgyvendinti techniniai saugumo reikalavimai

Metus[41] vėluojama įgyvendinti techninius kibernetinio saugumo reikalavimus:

- 4 YSVII tvarkytojai visa apimtimi neįgyvendinę iki 30 proc. minėtų reikalavimų,
- 4 YSVII tvarkytojai neįgyvendinę 40–50 proc. reikalavimų,
- 2 YSVII tvarkytojai neįgyvendinę 60–70 proc.

2012 m. įsigaliojęs Valstybės informacinių išteklių įstatymas prisidėjo prie IT strateginio planavimo gerinimo, tačiau esama planavimo sistema neteikia realios naudos. Minėtame įstatyme numatyta IT plėtros plano rengimo ir derinimo tvarka neatitinka gerųjų IT valdymo praktikų ir nesudaro sąlygų tinkamai planuoti išteklius ir nustatyti svarbiausius prioritetus atsižvelgiant į esamas rizikas. IT strateginio planavimo proceso reguliavimas labiau orientuotas į IT plėtros plano formos nustatymą ir jo techninį derinimą, tačiau neatskleidžia IT strateginio planavimo proceso turinio. Gerosios praktikos skiria daug dėmesio IT naudos valdymui, kuris turi būti nuolatos stebimas ir vertinamas strateginio valdymo struktūrų. IT planavimas ir prioritetai turi būti nuolatos atnaujinami pagal rizikų vertinimo rezultatus, IT strategija ir organizacijos strategija turi būti kuo daugiau tarpusavyje suderintos ir integruotos.

[41] LR Vyriausybės 2016-04-20 nutarimo Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 2.3 p.

Todėl siekiant užtikrinti efektyvų IT planavimą, reikia tobulinti valstybės informacinių išteklių strateginio planavimo procesą, kad jis būtų labiau integruotas į bendrą veiklos planavimą, nuoseklus, paremtas IT gerąsias valdymo praktikas atitinkančiomis metodikomis.

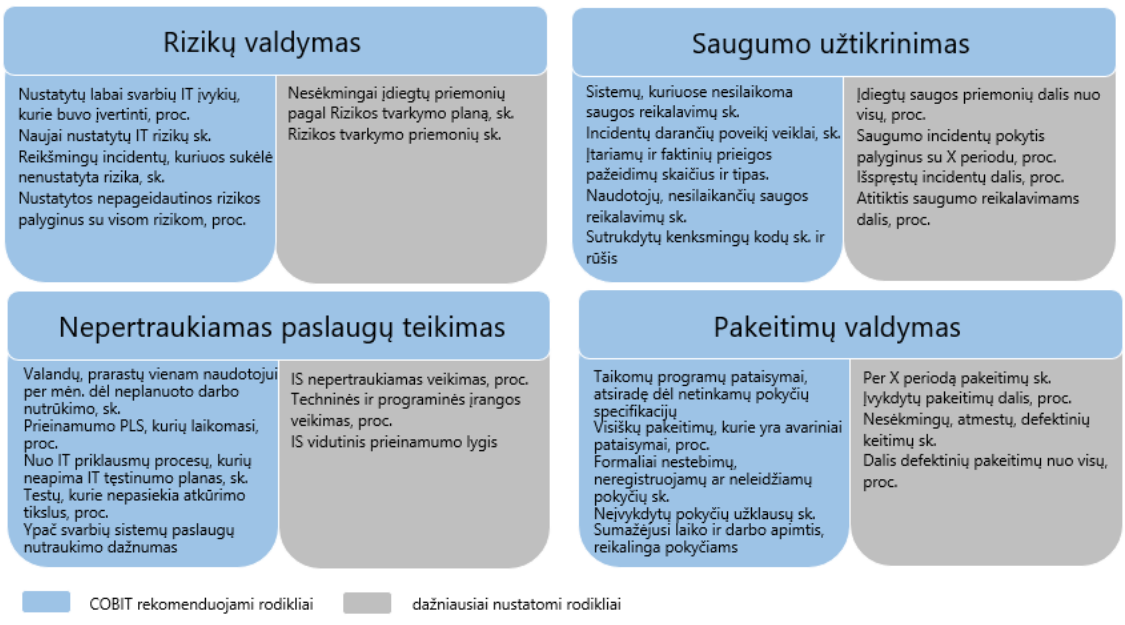
2.2. IT stebėsena neparodo ypatingos svarbos valstybės informacinių išteklių valdymo būklės

Kiekviena organizacija (institucijos ar valstybės lygmenyje), siekiant strateginių tikslų, turi žinoti savo IT valdymo būklę, nustatyti siektiną brandos lygį, numatyti ir įgyvendinti veiklas, padedančias jį pasiekti ir užtikrinti nuolatinę IT valdymo stebėseną. Efektyviai organizuota IT valdymo stebėsena parodo pažangos pokytį, kuris įvyko per atitinkamą laikotarpį, kokias strategines problemas reiktų spręsti, užtikrinti nuolatinį IT valdymo tobulėjimą. COBIT numato, kad atliekant IT stebėseną ir vertinimą reikia nustatyti tinkamus veiklos matavimo kriterijus (KPI, angl. *Key Performance Indicator*), kurie leidžia vertinti veiklos efektyvumą, sistemingai atlikti IT valdymo būklės vertinimus, remiantis vertinimo rezultatais atlikti IT valdymo tobulinimo veiksmus[42]. Įvertinus IT stebėsenos procesą, nustatyta, kad:

- Nepatikima IT veiklos efektyvumo matavimo kriterijų sistema

Didžioji dalis vertintų organizacijų (9) strateginiuose planavimo dokumentuose arba atskirose tvarkose nustatė IT veiklos matavimo kriterijus. YSVII tvarkytojai svarbių IT valdymo procesų, tokių kaip IT strateginis planavimas, pakeitimų valdymas, IT rizikos valdymas, informacinės architektūros nustatymas, veiklos efektyvumo nestebimi. Organizacijos taiko skirtingą IT veiklos matavimo praktiką – vieni nustato daug detalių rodiklių, kiti – apsiriboja keliais. Pasirenkami matavimo kriterijai ne visada subalansuoti ir nesudaro galimybės įvertinti IT veiklos efektyvumo (žr. 9 pav.).

9 pav. Naudojamų IT veiklos matavimo kriterijų pavyzdžiai



Šaltinis – AAI pagal YSVII tvarkytojų pateiktą informaciją

AAI, 2013 m. atlikusi auditą „Valstybės informacinių išteklių valdymas“, konstatavo, kad nėra IT veiklos matavimo kriterijų, kurie atitiktų IT gerąsias valdymo praktikas ir leistų sistemiškai matuoti

[42] COBIT 4.1, 2011 m., Vilnius; ME1 procesas, 153 psl.

IT veiklos efektyvumą, tačiau standartizuota IT valdymo efektyvumo matavimo rodiklių sistema sukurta nebuvo.

- Neatliekamas išsamus IT valdymo būklės vertinimas

YSVII tvarkytojai ne rečiau kaip kartą per trejus metus turi atlikti IT auditus, kurių metu turi būti vertinamas IT valdymas ir sauga[43]. Didžioji dalis YSVII tvarkytojų (8) per trejus pastaruosius metus atliko IT auditus, tačiau 4 auditai neapėmė didžiosios dalies IT valdymo procesų, o buvo orientuoti tik į paslaugų valdymo ir saugumo užtikrinimo kontrolės būklės patikrinimus, todėl faktiškai atliekami vidiniai vertinimai neparodo bendros IT valdymo būklės.

Tik du YSVII tvarkytojai 2014–2017 m. atliko išsamius IT valdymo būklės (brandos) vertinimus, bet taikoma skirtinga brandos vertinimo metodika, o tai nesuteikia galimybės informaciją palyginti ir bendrai vertinti pažangą.

IT valdymo brandos (būklės) vertinimo praktika

Vienoje organizacijoje 2017 m. vidaus auditas pagal COBIT metodiką atliko IT valdymo vertinimą ir nustatė brandą, tobulinimo kryptis. Kitoje – vidinė darbuotojų grupė kiekvienais metais atlieka IT valdymo vertinimą pagal individualiai sukurtą metodiką.

Siekiant užtikrinti įdiegtų IT paslaugų valdymo procesų nuolatinį gerinimą, IVPK rekomendavo[44] periodiškai atlikti IT paslaugų valdymo procesų brandos įvertinimą, pagal SEI (angl. *Software Engineering Institute*) sukurtą Integruotąjį brandos modelį CMMI arba kitus pasaulyje žinomus brandos modelius. Tokie vertinimai neatliekami ir orientuoti tik į paslaugų valdymą, o ne į IT strateginį planavimą ir stebėseną, siekiant įvertinti IT valdymo būklę ir brandą.

- Šalies mastu nežinoma kokia yra IT valdymo būklė

Geroji praktika nustato, kad, siekiant operatyviai spręsti išskylusias problemas ir imtis reikiamų strateginių veiksmų, reikia valdyti informaciją apie viešojo sektoriaus IT valdymą, pokyčius, problemas. Stebėsena reikalinga, kad būtų taikomos tinkamos priemonės, atitinkančios nustatytas kryptis ir politiką[45].

IVPK, įgyvendindamas valstybės informacinių išteklių valdymą, turi atlikti valstybės IS steigimo, kūrimo ir funkcionavimo stebėseną, analizuoti, kaip įgyvendinami IT plėtros planai, kaip valstybės informaciniai ištekliai panaudojami valstybės valdymui, teikti SM pasiūlymus dėl valstybės informacinių išteklių valdymo tobulinimo[46]. IVPK, atlikdamas stebėseną, nerenka informacijos apie YSVII išteklių valdymo ir tvarkymo būklę, neanalizuoja valdymo problematikos, apsiriboja tik informacijos rinkimu apie įsteigtas IS ir įgyvendinamus investicinius projektus (žr. IVPK paaiškinimą).

[43] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 14 str. 1 d.

[44] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013-06-19 įsakymas Nr. T-83 „Dėl Informacinių technologijų paslaugų valdymo metodikos patvirtinimo“, 17 p.

[45] COBIT 4.1, 2011 m., Vilnius; PO1 ir ME1 procesas, 29-32, 153-156 psl.

[46] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos nuostatai, patvirtinti LR susisiekimo ministro 2010-06-23 įsakymu Nr. 3-401 (2017-03-06 įsakymo Nr. 3-103 redakcija).

IVPK paaiškinimas dėl IT plėtros planų derinimo ir būklės analizės

IVPK tik derina IT plėtros planų projektus. Derinimą atlieka metodiškai įvertindami, ar pateikti IT plėtros planai atitinka turinio reikalavimus[47]. Turėdami suderintus ir IS valdytojų patvirtintus IT plėtros planus, planuoja lėšų paskirstymą valstybės informacinių išteklių plėtrai, vertina valstybės investicinių projektų atitiktį suplanuotoms lėšoms. Informacijos apie IT plėtros planų įgyvendinimą nerenka ir neanalizuoja. IVPK nuomone, IT plėtros planų įgyvendinimo stebėsenos procedūra tik padidintų administracinę naštą ir nesukurtų pridėtinės vertės.

Nežinant ypatingos svarbos valstybės informacinių išteklių tvarkytojų IT valdymo būklės, nėra galimybių numatyti reikalingas priemones esamai būklei pagerinti iki siektino brandos lygio. Tik tam tikrų IT valdymo elementų stebėsena neužtikrina, kad valstybės skiriamos lėšos būtų tinkamai panaudojamos siekiant ilgojo ir vidutinio laikotarpio Vyriausybės programose numatytų tikslų.

- Saugos atitikties stebėsenai sukurta informacinė sistema nėra pakankamai panaudojama

Viena iš IT valdymo sričių yra saugumas, kurio stebėsenai nuo 2016 m. sukurta ARSIS. Jos paskirtis: informacinių technologijų priemonėmis vykdyti valstybės informacinių išteklių atitikties Lietuvos Respublikos Vyriausybės nustatytiems elektroninės informacijos saugos reikalavimams stebėseną; automatizuoti duomenų apie saugos reikalavimų įgyvendinimą informaciniuose ištekliuose tvarkymo, valstybės ir kitų informacinių sistemų, valstybės ir žinybinių registrų rizikos vertinimo, atitikties saugos reikalavimams priežiūros, informacinių sistemų ir registrų valdytojų informavimo apie jų valdomiems informaciniams ištekliams taikomus saugos reikalavimus bei elektroninės informacijos saugos rizikas procesus[48]. Šios IS kūrimui buvo skirta apie 520 tūkst. Eur valstybės biudžeto lėšų.

Kartą per metus, atlikus atitikties nustatytiems saugos reikalavimams bei rizikos vertinimus, YSVII tvarkytojai privalo pateikti duomenis ARSIS, tačiau pusė jų šios informacijos į ARSIS neteikia. VRM siuntė YSVII tvarkytojams priminimus apie pareigą teikti informaciją, tačiau reaguojama nepakankamai. VRM nuomone, tokia situacija susidaro, nes valstybės mastu trūksta kompetentingų saugos analitikų ir saugos įgaliotinių, mokančių profesionaliai vykdyti informacinių sistemų saugos atitikties ir rizikos vertinimo procesus. VRM faktiškai neatliko sisteminės saugumo būklės analizės ir saugos valdymo tobulinimui buvo skiriamas nepakankamas dėmesys.

YSVII tvarkytojų nuomonė

- Buvo skiriamas mažas dėmesys IT valdymo tobulinimui.
- ARSIS duomenų apie saugumo atitiktį įkėlimas ir vertinimas gali užtrukti net iki 2 dienų.

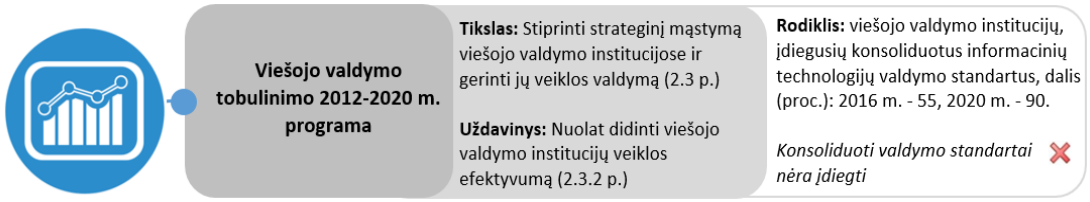
Minėtos problemos rodo, kad nėra sukurta visos IT valdymo būklės stebėsenos sistema, kuri atitiktų gerąsias valdymo praktikas ir sudarytų sąlygas valstybės informacinių išteklių valdymo nuolatiniam tobulėjimui, o tai galėtų prisidėti prie didesnės YSVII tvarkytojų valdymo brandos. Taip pat IT valdymo teisinis reguliavimas neatitinka geruų valdymo praktikų, numato minimalius reikalavimus arba rekomendacinio pobūdžio gaires, kurių valstybės informacinių išteklių tvarkytojai neprivalo įgyvendinti (žr. 3 priedą).

[47] Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013-03-14 įsakymas Nr. T-29 „Dėl Informacinių technologijų plėtros planų derinimo tvarkos aprašo patvirtinimo".

[48] Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, patvirtinti LR vidaus reikalų ministro 2012-10-16 įsakymu Nr. 1V-740 (2016-11-02 įsakymo Nr. 1V-778 redakcija).

Viešojo tobulinimo 2012-2020 m. programoje[49] buvo numatyta didinti viešojo valdymo institucijų veiklos efektyvumą diegiant konsoliduotus IT valdymo standartus (ISO 38500, TOGAF, COBIT, ITIL, kt.), tačiau planuotų rezultatų nepasiekta – konsoliduoti valdymo standartai nebuvo įdiegti (žr. 10 pav.).

10 pav. Siekis tobulinti IT valdymą



Šaltinis – AAI

YSVII tvarkytojai ISO standartus ir gerąsias praktikas savo veikloje naudoja pagal galimybes, maža dalis turi sertifikuotas sistemas[50]. Esant tokiai situacijai, tarp organizacijų didėja IT valdymo brandos skirtumai – vienos siekia trečią lygį, o kitos pasiekusios tik pirmą.

Gerosios valdymo praktikos diegiamos pagal galimybes

Gerąsias valdymo praktikas įsidiegė 4 YSVII tvarkytojai: du akredituoti pagal LST ISO/IEC 27001:2013 ir 3 pagal EN ISO 9001:2015 standartą. Kitos organizacijos nurodo, kad nėra įsidiegusios, bet pagal galimybes vadovaujasi jomis. Gerąsias praktikas įsidiegusių organizacijų brandos lygis aukštesnis, tačiau sertifikavimasis kainuoja ir ne visos organizacijos turi tokias galimybes.

Manome, kad tokia padėtis nesudaro sąlygų subalansuotai ir bendrai siekti tam tikros IT valdymo pažangos – nevyksta kompleksinis IT srities tobulinimas, kuris darniai veiktų visą IT valdymą. Siekiant aukštesnės YSVII valdymo brandos, reikėtų tobulinti valstybės informacinių išteklių valdymą, kad jis labiau atitiktų IT valdymo gerąją praktiką (pvz., ISO/IEC 38500 standarto [51], COBIT metodikos[52] rekomendacijas), sukuriant bendrą IT srities stebėsenos mechanizmą, kuris nustatytų siektiną IT valdymo brandos lygį, jo matavimo metodiką, atsiskaitymo už pasiektus rezultatus ir tobulinimo veiksmų įgyvendinimo tvarką, efektyviai panaudojant technologinius įrankius.

[49] LR Vyriausybės 2012-02-07 nutarimas Nr. 171 „Dėl viešojo valdymo tobulinimo 2012–2020 metų programos patvirtinimo".
[50] Objektyvus nepriklausomos organizacijos atliekamas įvertinimas ir patvirtinimas, kad organizacijoje įdiegta ir veikia vadybos sistema, atitinkanti pasirinkto standarto reikalavimus.
[51] ISO/IEC 38500:2015 „Information technology – Governance of IT for the organization".
[52] COBIT 5, A Business Framework for the Governance and management of Enterprise IT, USA, 2012 ISACA.

3. NEPAKANKAMAI VEIKSMINGAI ĮGYVENDINAMOS PRIEMONĖS, GALINČIOS UŽTIKRINTI YPATINGOS SVARBOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ ATSPARUMĄ KIBERNETINIŲ GRĖSMIŲ LYGIUI

Vis dažniau ypatingos svarbos informaciniai ištekliai sulaukia kibernetinių atakų. Prognozuojama, kad ateinančiais metais šių atakų lygis labai išaugs[53]. 2017 m. nustatyta beveik 21 tūkst. programinės įrangos pažeidžiamumų – tai 31 proc. daugiau negu 2016 m.[54]. Dėl IS defektų ir programavimo klaidų kibernetinės atakos gali greitai plisti tinkle ir neigiamai paveikti ypač daug informacinių išteklių.

Pakankamas organizacijų atsparumas gali padėti sumažinti kibernetinių atakų efektą[55]. Ekspertai pripažįsta, kad aukštas techninis pasirengimo lygis ne visada reiškia žemą grėsmių lygį, todėl atsparumas gali būti didinamas sistemiškai taikant ne tik technines bet ir kitas priemones:

- rizikų valdymas padeda suvokti, kokios yra kibernetinės grėsmės, jų mastas, galimas poveikis organizacijos tikslams; efektyviai valdomas procesas leidžia laiku identifikuoti kritines rizikas ir jas sumažinti iki priimtino lygio[56];
- kompleksiškai įgyvendinant prevencines priemones, gali būti mažinamas IS pažeidžiamumo lygis, socialinės inžinerijos pavojai, užtikrinamas greitas IS veikimo atstatymas[57].

3.1. IT saugumo rizikų vertinimas nėra pakankamai veiksmingas

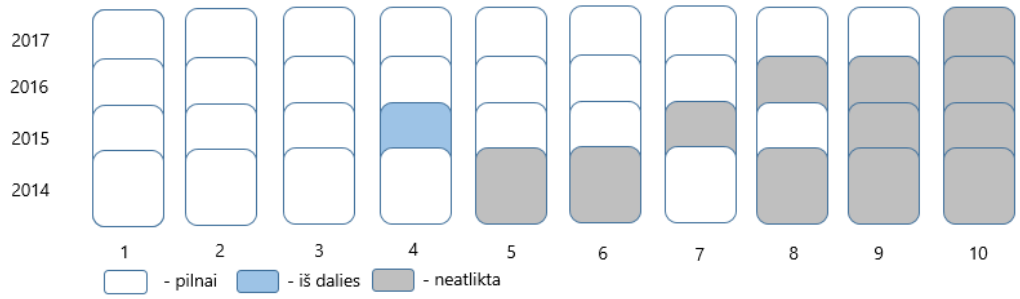
IT rizikų vertinimo sistema apima rizikos konteksto nustatymą, rizikų identifikavimą, analizę, vertinimą, rizikų tvarkymą[58].
2017 m. pusė YSVII tvarkytojų rizikų vertinimą atliko savarankiškai, kitiems vertinimus atliko pasamdytos išorės organizacijos. Įvertinus rizikų vertinimo procesą, nustatyta, kad:

- Informacinių sistemų rizikų vertinimas atliekamas ne kasmet

Teisės aktai numato, kad visų IS rizikos įvertinimas turi būti organizuojamas kasmet[59]. Nuosekliai atliekamas vertinimas leidžia laiku reaguoti į grėsmių pokyčius. 2017 m. beveik visi YSVII tvarkytojai atliko rizikų vertinimą, tačiau jis ne visada atliekamas kasmet ir ne visų IS atžvilgiu (žr. 11 pav.).

[53] Pasaulio ekonomikos forumo pasaulinių rizikų ataskaita (angl. *Insight Report „The Global Risks Report 2018" by the World Economic Forum*). Prieiga per internetą: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.
[54] *Vulnerability QuickView – 2017 Vulnerability Trend, Risk Based Security*. Prieiga per internetą: https://pages.riskbasedsecurity.com/hubfs/Reports/2017/2017%20Year%20End%20Vulnerability%20QuickView%20Report.pdf
[55] Pasaulio bendruomenė ruošiasi atremti kibernetines atakas. Pasaulio tendencijų tyrimas 2018 m., PwC.
[56] COBIT 4.1, 2011 m., Vilnius; PO9 procesas, 63-66 psl.
[57] COBIT 4.1, 2011 m., Vilnius; DS4, DS5 procesai, 113–120 psl.
[58] COBIT 4.1, 2011 m., Vilnius; PO9 procesas, 64 psl.
[59] LR 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", 35 p.

11 pav. YSVII tvarkytojų atlikti rizikų vertinimai 2014–2017 m.



Šaltinis – AAI pagal YSVII tvarkytojų pateiktas rizikų vertinimo ataskaitas

Yra atvejų, kai rizikų vertinimas per keturis paskutinius metus nebuvo atliktas arba pirmą kartą rizikas pradėta vertinti 2017 metais.

- Identifikuojamos ne visos aktualios rizikos

YSVII tvarkytojai rizikas identifikuoja pagal ARSIS pateiktą standartinių rizikų sąrašą[60]: jame yra 46 unikalios rizikos, jų aprašai, vertinimo ir tvarkymo aspektai. Palyginus šį sąrašą su COBIT rizikų vertinimo gairėse nurodytomis IT rizikomis[61] nustatyta, kad jis yra neišsamus – neapima visų galimų rizikų, pavyzdžiui, trūksta rizikų dėl IT investicinio portfelio sukūrimo ir priežiūros, IT architektūros, programinės įrangos valdymo, išorės paslaugų tiekėjų valdymu, inovacijomis ir kt.

Beveik visais atvejais identifikuojamos tik standartinės rizikos ir per mažai dėmesio skiriama rizikoms, kurios iš tiesų gali būti aktualios organizacijai ir turi būti tvarkomos (žr. pavyzdį).

Pavyzdys

2017 m. lapkričio mėn. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos serverių ištekliai buvo išnaudoti, todėl ilgiau nei 8 val. sistema neveikė. Nors, 2016 m. vertinant rizikas, buvo vertinta bendra ARSIS numatyta rizika dėl išteklių trūkumo, tačiau ji nebuvo konkreti: susieta tik su dubliuoto duomenų centro, žmogiškųjų išteklių trūkumais, o ne tarnybinių stočių išteklių visišku išnaudojimu, todėl, aiškiai neidentifikavus rizikos bei nenumačius tinkamų jos valdymo priemonių, ši rizika faktiškai nebuvo valdoma. Tik įvykus 2017 m. lapkričio mėn. incidentui rizika dėl tarnybinių stočių išteklių išnaudojimo buvo nustatyta 2017 m. rizikų vertinimo ataskaitoje.

- Rizikų vertinimo metodika neatitinka naujausių IT valdymo praktikų

Rizikų vertinimo procesas sudėtingas ir reikalauja specifinių žinių, todėl reikia turėti rizikų vertinimo metodiką[62]. Bendras standartas užtikrina, kad organizacijos dėl analogiškų grėsmių taikys panašią analizės, vertinimo ir reagavimo praktiką. VRM 2005 m. parengė Rizikos analizės vadovą[63], kurį rekomendavo naudoti viešojo sektoriaus organizacijoms vertinant IS rizikas. Jame aprašomos rizikų vertinimo taisyklės, bet nenurodoma išsami viso proceso įgyvendinimo tvarka. Didžioji dalis YSVII tvarkytojų (7), vertindami rizikas, nenaudoja šio vadovo, keli yra parengę savo metodikas. Pripažįstama,

[60] Pagal LR vidaus reikalų ministerijos informaciją ARSIS rizikų sąrašas parengtas pagal Vokietijos federalinės informacinių technologijų saugumo tarnybos (BSI) informacijos saugos rizikoms vertinti taikomą 46 rizikų sąrašą. ARSIS rizikų sąrašas nėra privalomas.

[61] Risk Scenarios Using COBIT® 5 for Risk, ISACA.

[62] COBIT 4.1, 2011 m., Vilnius; PO9 procesas, 64-65 psl.

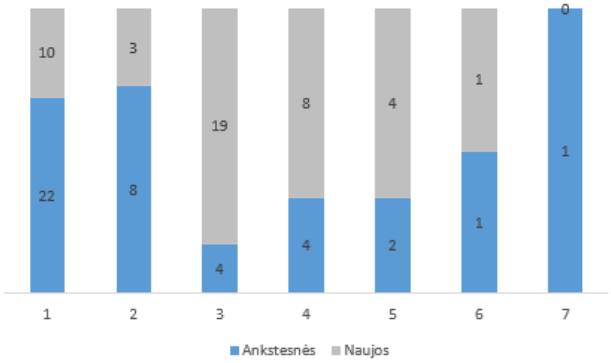
[63] Prieigą per internetą: https://vrm.lrv.lt/uploads/vrm/documents/files/Rizikos_analize.pdf.

kad metodika neaktuali – dauguma šaltinių, kuriais remtasi ją rengiant, šiuo metu negalioja (LST ISO/IEC 13335-1:2000, LST ISO/IEC 17799:2004, BS 7799 ir kt.), nurodytos senos IT valdymo metodikos.

- Neužtikrinamas nepriimtinų rizikų tvarkymas laiku.

Nustačius nepriimtinas rizikas turi būti rengiamas jų valdymo (tvarkymo) priemonių planas, kuriame numatomi techniniai, administraciniai ir kiti ištekliai, reikalingi rizikai suvaldyti[64]. Visi YSVII tvarkytojai, kurie atliko vertinimus, parengė minėtus planus, bet nustatyta, kad skirtingų metų planuose dažnai nurodomos tos pačios rizikos, jos perkeliamos į naujai sudaromus rizikų valdymo planus (žr. 12 pav.).

12 pav. Ankstesniais metais nepriimtinų ir naujų rizikų pasiskirstymas 2017 m.[65]



Šaltinis – AAI pagal YSVII tvarkytojų pateiktas rizikų vertinimo ataskaitas

Tai rodo, jog nesiimama pakankamų veiksmų valdant šias rizikas, o jų potencialas kasmet didėja. YSVII tvarkytojai nurodo, kad pagrindinės priežastys, kurios sąlygojo nepakankamą rizikų tvarkymą, yra išorinės: IT personalo, finansavimo trūkumas, šalyje nevykstantis IT išteklių konsolidavimo procesas.

Sukurtos metodinės priemonės neužtikrina efektyvaus rizikų valdymo ir YSVII didesnio atsparumo kibernetinėms grėsmėms. Siekiant gerinti rizikų valdymą, tarptautinės organizacijos – EBPO, ENISA – ES valstybėms rekomenduoja sukurti ir nuolatos prižiūrėti nacionalinio lygmens rizikų valdymo procesą (žr. pavyzdį).

Tarptautinių organizacijų rekomendacijos dėl nacionalinio lygmens rizikų valdymo, siekiant apsaugoti kritinę informacinę infrastruktūrą

EBPO rekomenduoja atsižvelgiant į atliktą rizikų vertinimą sukurti ir nuolat peržiūrėti nacionalinio lygmens rizikų valdymo procesą, apimanti organizacines, technines ir stebėsenos priemones, skirtas įgyvendinti rizikų valdymo strategiją visuose lygmenyse[66].

ENISA rekomenduoja vykdyti nacionalinių rizikų vertinimą. Šiam tikslui pasiekti turi būti sukurta nacionalinio lygmens rizikų vertinimo metodika ir nacionalinių rizikų registras, kuris būtų atnaujinamas ir peržiūrimas, atsižvelgiant į naujai nustatomus pavojus ir pažeidžiamumus[67].

[64] COBIT 4.1, 2011 m., Vilnius; PO9 procesas, 64-65 psl.; LR 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“, 37 p.

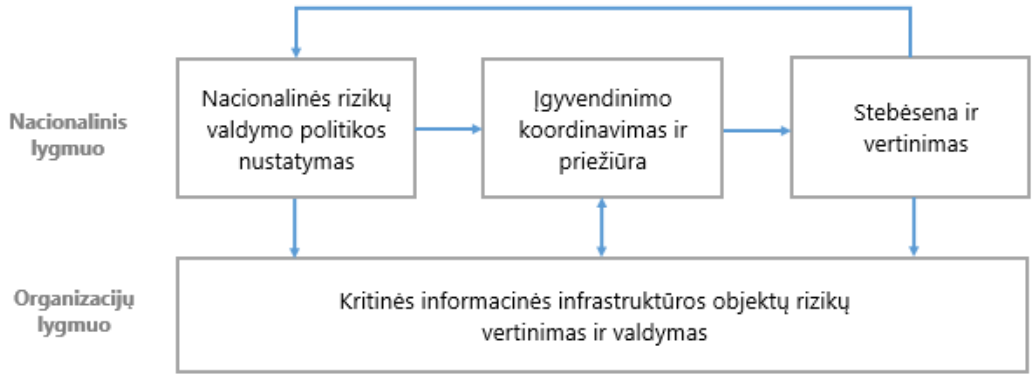
[65] Nurodytos 7 institucijos, nes 2017 m. vienu atveju vertinimas nebuvo atliktas, kitu – pradėta vertinti tik 2017 m., vienu atveju 2017 m. ataskaita buvo rengiama.

[66] EBPO dokumentas „Recommendation of the Council on the Protection of Critical Information Infrastructures“ (2008), prieiga per internetą: https://www.oecd.org/sti/40825404.pdf.

[67] ENISA ataskaitos: „ad hoc Working Group on National Risk Management Preparedness“ (2011), prieiga per internetą: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/WG%202010%20NRMP; „National Cyber Security Strategies Practical Guide on Development and Execution“ (2012), prieiga per internetą: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

Nacionalinis rizikų valdymas leidžia atitinkamoms institucijoms politikos formavimo lygmenyje gauti aktualią informaciją apie YSVII tvarkytojų identifikuojamas grėsmes ir nacionaliniu lygiu koordinuoti rizikų valdymo procesą, tokiu būdu užtikrinant reikiamus apsaugos, prevencijos, aptikimo ir atsako pajėgumus. Tyrimų duomenimis, vis daugiau valstybių, kurios decentralizuotai valdė rizikas, diegia nacionalinį rizikų valdymo modelį[68] (žr. 13 pav.).

13 pav. Nacionalinis rizikų valdymo modelis



Šaltinis – ENISA[69]

Informacinių išteklių saugumo srityje pastaraisiais metais vyksta pokyčiai – konsoliduojama elektroninės informacijos ir kibernetinio saugumo politika, stiprinami kibernetinio saugumo pajėgumai, šios srities stebėsena, rengiama kibernetinio saugumo strategija. Atliekama svarbiausių kibernetinių grėsmių apžvalga [70] teigiamai prisideda prie nacionalinių rizikų identifikavimo, tačiau pilnavertis nacionalinių rizikų valdymo procesas, galintis YSVII lygmenyje koordinuoti veiksmus ir įtakoti rizikų tvarkymą YSVII valdymo lygmenyje, nėra sukurtas. Nacionalinio rizikų valdymo metu gauta informacija turi būti naudojama priimant kibernetinio saugumo strateginius sprendimus, todėl minėtų pokyčių kontekste reikėtų gerinti kibernetinio saugumo rizikų valdymo procesą organizacijų lygmenyje ir diegti nacionalinį rizikų valdymą.

3.2. Sistemiškai nenaudojamos kibernetines grėsmes mažinančios saugumo priemonės

Saugumo ekspertai pripažįsta, kad pagrindinių saugumo higienos principų laikymasis didina atsparumą kibernetinėms grėsmėms. Pavienės priemonės nėra veiksmingos ir tik jų kompleksiškas naudojimas gali užtikrinti didesnį YSVII saugumą. Įvertinus YSVII tvarkytojų taikomas saugumo priemones, nustatyta, kad:

- IS kūrimo, modernizavimo, modifikavimo metu nepakankamai testuojamas saugumas

COBIT metodikoje nurodyta, kad į gamybinę aplinką perkeliami pokyčiai pirmiausia turi būti testuojami dėl saugos ir veiklos. Tarptautinė bendruomenė OWASP (angl. *The Open Web*

[68] ENISA dokumentas „Stocktaking, Analysis and Recomendations on the Protection of CIIS", (2016), prieiga per internetą: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis, 23–24 psl.
[69] Prieiga per internetą: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/WG%202010%20NRMP, 14 psl.
[70] 2016 ir 2017 m. nacionalinės kibernetinio saugumo būklės ataskaitos. Prieiga per internetą: https://kam.lt/download/57062/nksc_metine_ataskaita_uz_2016.pdf; https://www.nksc.lt/doc/NKSC_ataskaita_2017_[lt].pdf.

Application Security Project), kuri siekia gerinti programinės įrangos saugumą[71], rekomenduoja kiekviename IS kūrimo (modernizavimo) etape atlikti tam tikrus saugumo tikrinimus, pvz., atlikti grėsmių modeliavimą, peržiūrėti išeities kodą [72]. Efektyvus kuriamų sprendimų saugumo testavimas gali sumažinti IS pažeidžiamumo riziką.

YSVII tvarkytojai priimdami pakeitimus daugiau dėmesio skiria funkcijų testavimui, bet nėra atliekamas visapusis kuriamų sprendimų saugumo patikrinimas (neatliekamas grėsmių modeliavimas, išeities kodo peržiūra ir įvairūs saugumo vertinimai). 3 YSVII tvarkytojai neatlieka atsparumo įsilaužimui testavimo.

IVPK 2017 m. rekomendavo kuriant ir modernizuojant IS atlikti atsparumo įsilaužimui testavimą[73], tačiau YSVII tvarkytojai neprivalo laikytis rekomendacijų, taigi ir testavimo gali neatlikti. Rekomendacijose nėra išsamiai aprašyti visi reikiami atlikti saugumo testavimo veiksmai. Pažymėtina, kad Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikoje[74], kuri privaloma, ir aprašo visą IS kūrimo eigą, reikalavimų atlikti šį testavimą nėra.

- Personalas nepakankamai ugdomas kibernetinio saugumo klausimais

Kibernetiniai nusikaltėliai, vis dažniau pasinaudodami darbuotojais, įsilaužia į organizacijos infrastruktūrą, t. y. naudoja socialinės inžinerijos atakas. 2017 m. laiškų, sukurtų naudojantis socialinės inžinerijos principais, skaičius išaugo pusantro karto[75]. Tyrimai rodo, kad daugiau negu pusė (63 proc.) IT saugumo incidentų įvyksta dėl darbuotojų klaidos[76]. Todėl turi būti nuolatos vykdomi saugumo mokymai, atliekami socialinės inžinerijos testai. Didžioji dalis YSVII tvarkytojų (7) neskiria pakankamo dėmesio darbuotojų ugdymui – 2 atvejais mokymai per 2014– 2017 m. nebuvo organizuoti, 5 atvejais tai atliekama fragmentiškai, apsiribojama informacinių pranešimų apie informacijos saugumą platinimu elektroniniu paštu, mokymuose dalyvauja maža dalis darbuotojų – vidutiniškai 18 proc. organizacijos darbuotojų. 3 YSVII tvarkytojai labiau prisideda prie darbuotojų ugdymo, tačiau mokymų turinys priklauso nuo saugos įgaliotinio gebėjimų ir žinių, dažnai nėra naudojami socialinės inžinerijos testai, kurie galėtų atskleisti ugdomosios veiklos veiksmingumą, parodytų darbuotojų sąmoningumo lygį.

- Nevaldoma programinės įrangos saugi konfigūracija ir atnaujinimai

Kiekvienais metais nustatoma vis daugiau operacinės sistemos ir programinės įrangos spragų, kurios gali būti išnaudojamos kibernetinių atakų metu. Programinės įrangos gamintojai, siekdami ištaisyti nustatytas klaidas ir silpnas vietas, paruošia įvairius šios įrangos atnaujinimus. Todėl šiais atvejais reikia operatyviai reaguoti į siūlomus technologinius naujinimo sprendimus, užtikrinti saugią įrangos konfigūraciją. Nustatyta, jog per audituojamąjį laikotarpį pusė YSVII tvarkytojų (5) patyrė didelės ar vidutinės reikšmės kibernetinius incidentus, kurių metu nustatyti 34 programinės įrangos užkrėtimo atvejai. 8 YSVII tvarkytojai vis dar eksploatuoja *Windows XP* gamintojo nebepalaikomą programinę įrangą, kuri įdiegta 1,2 tūkst. kompiuteriuose.

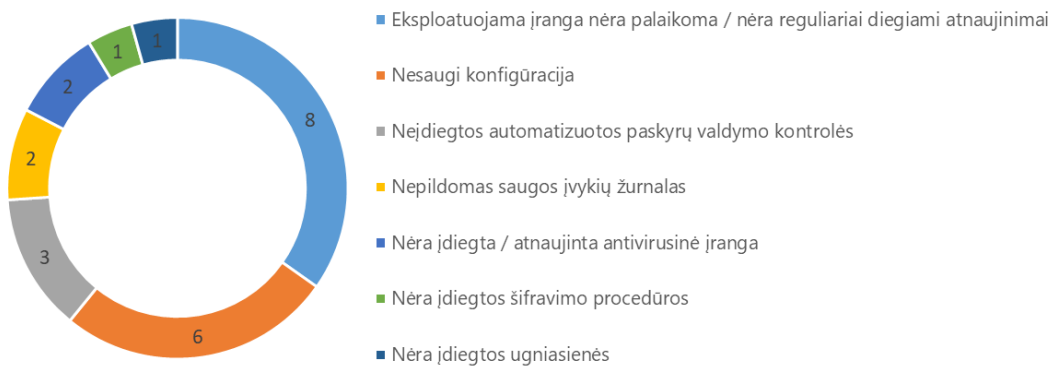
[71] Atviros bendruomenės, skleidžiančios su programinės įrangos saugumu susijusią informaciją, interneto svetainė, prieiga per internetą: https://www.owasp.org/index.php/Main_Page.
[72] Prieiga per internetą: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents.
[73] Projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos 2017-11-22 įsakymu Nr. T-126, 33.9 p.
[74] Patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014-02-25 įsakymu Nr. T-29.
[75] Nacionalinio kibernetinio saugumo būklės ataskaita, 2017 m., prieiga per internetą: https://kam.lt/download/61258/nksc%20ataskaita_final.pdf. Psl. 22
[76] Deloitte 2018 m. tyrimo „Enjeux Cyber 2018. L'évolution de la menace Cyber" pristatymo medžiaga. Prieiga per internetą: http://efl.fr.s3.amazonaws.com/pdf/20180118_Etude_Cyber2018_VDEF.pdf.

Windows XP programinės įrangos naudojimo galimos pasekmės

2017-05-12 pasklidusia „WannaCry“ kenkėjiška išpirkos reikalaujančia programa (angl. *Ransomware*) buvo apkrėsta 200 000 kompiuterių per 150-yje pasaulio šalių. Šis virusas turėjo ypač neigiamą poveikį Jungtinės Karalystės sveikatos apsaugos sistemai: dalyje sveikatos įstaigų buvo užblokuota kompiuterinė įranga, todėl buvo apribotas sveikatos paslaugų teikimas. Jungtinės Karalystės AAI 2017 m. atlikto audito metu paaiškėjo, jog pagrindinė tokio didelio masto apkrėtimo priežastis – pažeistos organizacijos eksploatavo nepalaikomą programinę įrangą (*Windows XP*) arba nebuvo laiku įdiegusios reikiamų programinės įrangos atnaujinimų.

Pažeidžiamumų vertinimo rezultatai rodo, kad YSVII tvarkytojai dažnai reguliariai nediegia reikiamų atnaujinimų, naudoja nesaugią konfigūraciją (žr. 14 pav.).

14 pav. YSVII tvarkytojų skaičius, kuriuose nustatyta pažeidžiamumų



Šaltinis – AAI pagal pažeidžiamumų vertinimo ataskaitas

Nėra metodikų, kaip saugiai valdyti konfigūracijas, ir programinės įrangos atnaujinimo valdymo gairių, kurios padėtų personalui efektyviai atlikti šią veiklą.

- IT veiklos tęstinumo ir atsarginių kopijų valdymas kelia grėsmę veiklos atkūrimui

Vykstančio kibernetinio išpuolio poveikį galima sumažinti greitai ir veiksmingai reaguojant. Toks reagavimas parodytų, kad viešosios institucijos nėra bejėgės ir gali atremti šiuos išpuolius, ir padėtų didinti pasitikėjimą[77]. Efektyvus IT veiklos tęstinumo ir atsarginių kopijų valdymas užtikrina greitą reagavimą į kritines situacijas. Turi būti sukurtas, prižiūrimas, kartą per metus išbandomas IT veiklos tęstinumo valdymo planas, kuriame turi būti aprašyti išsamūs veiksmų scenarijai atkuriant veiklą, taip pat nuolatos prižiūrima atsarginių kopijų saugykla, reguliariai organizuojami veiklos tęstinumo valdymo plano mokymai[78]. IS veiklos tęstinumo valdymo planą patvirtinto beveik visi YSVII tvarkytojai (9), tačiau jų turinys galėtų būti kokybiškesnis ir išsamesnis (žr. pavyzdį).

[77] Europos Komisijos bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, 2017 m. Prieiga per internetą: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/LT/JOIN-2017-450-F1-LT-MAIN-PART-1.PDF.

[78] COBIT 4.1, 2011, Vilnius, DS4 procesas, 113 psl.; LR 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“.

IT veiklos tęstinumo valdymo planas galėtų būti kokybiškesnis ir išsamesnis

IT veiklos tęstinumo valdymo plano turiniui reikalavimai yra nustatyti, formaliai planai juos atitinka, tačiau:

- 6 planai nėra pakankamai detalūs ir, įvykus kritiniam incidentui, nebus aišku, kokius veiksmus, kokiu eiliškumu reikia atlikti, su kuo komunikuoti, norint greitai reaguoti į vykstančius įvykius;
- 4 planuose nėra aiškios veiklos atkūrimo strategijos: nėra išskiriami veiklos atkūrimo eiliškumo prioritetai arba jie neracionalūs, pvz., numatyta, kad 2 kategorijos IS turi būti atkurtos pirmiau negu 1 kategorijos IS;
- planuose nurodomi scenarijai yra susiję su tipinėmis rizikomis (pvz.: gaisras, elektros sutrikimai, užpylimai), bet trūksta aktualių kibernetinių grėsmių scenarijų (konkretus kibernetinės atakos (angl. *Denial of Service* (DoS) scenarijus yra tik vienoje organizacijoje;
- 5 planuose nėra nurodyta konkreti IT tęstinumo dokumentacijos saugojimo vieta arba nurodyta tokia, kuri neužtikrina, jog dokumentacija bus skubiai prieinama ekstremalių situacijų (pvz., gaisro) atveju.

Didžioji dalis YSVII tvarkytojų (7) reguliariai minėtų planų neperžiūri ir laiku neatnaujina, atsižvelgiant į atliktų rizikų bei saugos atitikties, pažeidžiamumo vertinimo rezultatus ar įvykus organizacinės struktūros pasikeitimų. Pažymėtina, kad praktiškai neatliekami IT veiklos tęstinumo valdymo planų veiksmingumo išbandymai.

IT veiklos tęstinumo valdymo planų veiksmingumo bandymai neefektyvūs

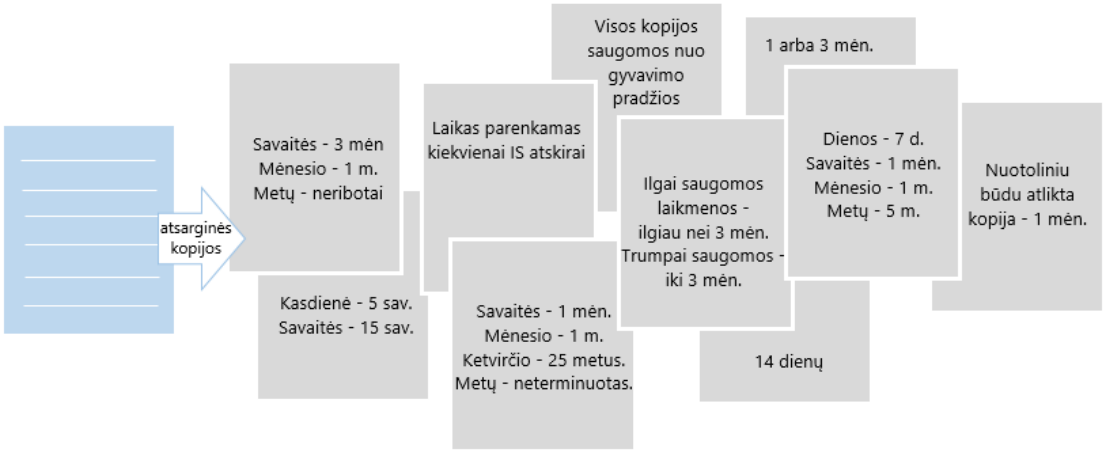
Neišbandomi IT veiklos tęstinumo valdymo planai neteikia naudos, nes nejsitikinama, ar jie bus veiksmingi ir padės skubiai atstatyti veiklą ekstremaliųjų situacijų atveju. IT veiklos tęstinumo testavimas turi apimti daugumą pagrindinių veiklos atkūrimo scenarijų, įtraukiant veiklos atstovus, kurie testuodami turėtų įvertinti alternatyvius paslaugų teikimo būdus, laikinai sutrikus IS veiklai. Nustatyta, kad:

- 1 atveju šio plano testavimai vyko nuosekliai – kasmet 2014–2017 m., bet buvo testuojama tik viena 1 kategorijos IS.
- 3 atvejais toks testavimas atliktas bent kartą per audituojamąjį laikotarpį, tačiau šis testavimas iš esmės apėmė tik 1-2 IS atkuriant atsargines kopijas, kas nėra pilnavertis minėto plano veikimo patikrinimas.
- 6 atvejais IT veiklos tęstinumo valdymo planas visiškai nebuvo testuojamas.

Atlikus patikras vietoje, nustatyta, kad visi YSVII tvarkytojai atlieka atsargines kopijas, tačiau tam skiriamas nepakankamas dėmesys. Teisės aktai [79] numato pačioms organizacijoms saugos nuostatuose ir saugaus elektroninės informacijos tvarkymo taisyklėse aprašyti atsarginių kopijų įgyvendinimo politiką. Tačiau trimis atvejais tokia politika nėra nustatyta, kitais atvejais nurodomi tik pagrindiniai atsarginių kopijų saugojimo principai (saugojimo vieta, kopijų įrašymo periodiškumas), tačiau nedetalizuota atsarginių kopijų organizavimo ir saugojimo tvarka, naudojami šių kopijų metodai, šifravimo politika, prieigos prie kopijų teisių valdymas, kt. Todėl taikoma skirtinga atsarginių kopijų tvarkyto praktika, o kai kurie saugojimo terminai nėra racionalūs atsižvelgiant į IS svarbą (žr. 15 pav.).

[79] LR 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“, 3.3.6. p., 4.3.3. p., 5.2.6. p.

15 pav. YSVII tvarkytojų atsarginių kopijų saugojimo laikas



Šaltinis – AAI pagal YSVII tvarkytojų pateiktą informaciją

Kaip ir IT veiklos tęstinumo plano atveju, nėra atliekami atsarginių kopijų testavimai, parenkama netinkama jų saugojimo vieta (žr. pavyzdį).

Atsarginės kopijos tvarkomos neturint aiškios jų valdymo politikos (strategijos)

Vienas YSVII tvarkytojas neatlieka atsarginių kopijų atkūrimo bandymų, trys neatlieka kiekvienais metais, o atliekantieji (9) atsargines kopijas testuoja ne visų IS. Tokiu atveju neįsitikinama, ar pavyktų atkurti ir jei pavyktų, kiek laiko užtruktų duomenų atkūrimas iš atsarginės kopijos.

Atsarginės kopijos saugomos neatsižvelgiant į įvairias rizikas, kurioms atsitikus kopijos būtų prarastos, pavyzdžiui, kopijos saugomos cokolinio aukšto patalpose, kurios gali būti užpiltos, 4 atvejais saugomos tose pačiose patalpose ar pastate, kur įvykus gaisrui, gali būti viskas sunaikinta.

- Saugos veiksmingumo matavimų rezultatai nesudaro prielaidų stiprinti saugumą

COBIT rekomenduoja reguliariai vertinti IT saugumo valdymo silpnąsias vietas. Teisės aktai įpareigoja kasmet atlikti visų IS saugos atitikties, pažeidžiamumų (angl. *penetraton test, pen-test*)[80] vertinimus, o nustatytus trūkumus šalinti parengiant tobulinimo planus[81]. Šie vertinimai leidžia iš anksto nustatyti neįprastus ir (ar) netaisyklingus veiksmus, kuriuos reikia koreguoti.

Vienas YSVII tvarkytojas per 2014–2017 m. saugos atitikties vertinimo neatliko. Didžioji dalis YSVII tvarkytojų (9) šį vertinimą atlieka, bet ne kasmet, o rezultatai ne visais atvejais patikimi ir rodo tikrą atitikties būklę (žr. pvz.) Pažymėtina, kad beveik visi YSVII tvarkytojai šias vertinimo paslaugas perka, todėl valstybės biudžeto lėšos tokiais atvejais gali būti naudojamos nepakankamai efektyviai.

Saugos atitikties 2017 m. vertinimo pavyzdžiai

Remiantis Informacinių technologijų saugos atitikties vertinimo metodika[82], vertintojas įvertina, kaip IS valdytojas ir (ar) IS tvarkytojas įgyvendina saugos reikalavimus. Vertinimas turi apimti faktinį saugos politikos nuostatų įgyvendinimą. Nustatytas atvejis, kai, tikrinant atitiktį, buvo užfiksuota, jog ne visose tarnybinėse stotyse reguliariai atnaujinama programinė įranga, bet reikalavimas dėl laiku įdiegiamų programinės įrangos atnaujinimų įvertintas 4 balais (iš 5), o tai reiškia, kad saugos

[80] Pažeidžiamumo vertinimas yra autorizuota imituota IS ataka, atliekama siekiant įvertinti šios sistemos saugumą.

[81] LR Vyriausybės 2016-04-20 nutarimas Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 12 p.; LR vidaus reikalų ministro 2013-10-04 įsakymas Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, 7.2 p.

[82] Patvirtinta LR vidaus reikalų ministro 2004-06-06 įsakymu Nr. 1V-156.

reikalavimai įgyvendinti, tačiau nustatyta neesminių trūkumų. Kitu atveju reikalavimas dėl atsarginių kopijų šifravimo įvertintas 5 balais kaip visiškai įgyvendintas, bet, audito metu tikrinant atsarginių kopijų tvarkymą, nustatyta, kad atitinkama organizacija šių kopijų nešifruoja, o reikalavimas yra tik nurodytas saugos politikoje, t. y. faktiškai nėra įgyvendintas.

Pažeidžiamumų vertinimų neatliko 3 YSVII tvarkytojai. Audituojamu laikotarpiu buvo įvertintas 24 proc. 1 kategorijos IS pažeidžiamumas. Neatliekant visų IS vertinimų, nėra aiškus faktinis jų pažeidžiamumų lygis.

Organizacijos nesiima pakankamų veiksmų mažinti neatitiktis – trečdalis YSVII tvarkytojų, atliekančių saugos atitikties ir pažeidžiamumų vertinimus, nesudaro tobulinimo planų. Nustatyta atvejų, kai ankstesniais metais nustatyti neatitikimai nėra panaikinami arba nekontroliuojama planuose pateiktų priemonių įgyvendinimo būklė.

YSVII tvarkytojų nuomonė dėl saugumo priemonių neįgyvendinimo

YSVII tvarkytojų nuomone, visos reikiamos saugumo priemonės nėra įgyvendinamos, nes trūksta žmogiškųjų išteklių, metodinių rekomendacijų, kaip teisingai atlikti tam tikrus veiksmus.

Taikomų saugumo priemonių efektyvumas daugeliu atvejų priklauso nuo organizacijos vadovybės požiūrio, organizacinės struktūros, personalo žinių ir gebėjimų. Nustatytos problemos rodo, kad esamos struktūros neužtikrina pakankamo saugumo lygio. Visais atvejais saugos įgaliotiniai yra paskirti, tačiau pusėje tvarkytojų jie pavaldūs IT padalinio vadovybei, o tai sudaro sąlygas šališkumui. Organizacijose retai veikia saugos priežiūros komitetai, kurie aktyvai aukščiausiu lygmeniu stebi saugumo būklę ir prisideda prie jos gerinimo.

Nuo 2015 m. įsigaliojus Kibernetinio saugumo įstatymui[83] Nacionalinis kibernetinio saugumo centras pradėjo analizuoti saugumo situaciją, stebėti organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą, teikti konsultacijas ir rekomendacijas kibernetinio saugumo klausimais. Kasmet rengiamos kibernetinio saugumo pratybos. Ši veikla prisideda prie kibernetinio saugumo situacijos gerėjimo, tačiau esama saugumo būklė rodo, kad to nepakanka. Reikėtų aktyviau ugdyti kompetencijas, teikti organizacijoms metodinę pagalbą, organizuoti mokomąją veiklą, skleisti gerąją kibernetinio saugumo praktiką, ypač organizaciniais klausimais, kurie prevenciškai prisideda prie atsparumo kibernetinėms grėsmėms didinimo. Tokias priemones taiko kitų valstybių institucijos, atsakingos už kibernetinį saugumą (žr. pavyzdį).

Kitų šalių metodinio vadovavimo, informacijos sklaidos ir švietėjiškos veiklos pavyzdžiai

Jungtinės Karalystės Nacionalinis kibernetinio saugumo centras[84] kas savaitę leidžia ataskaitas, kuriomis informuoja suinteresuotas šalis (visuomenę, valdžios institucijas (ir vietos savivaldos) apie naujus pavojus internete, pateikia nuorodas į parengtas gaires, gerosios praktikos rekomendacijas, kaip nuo šių pavojų apsisaugoti. Dėmesys ypač skiriamas kritinei infrastruktūrai – skelbiami įvairūs išaiškinimai, gairės dėl tinklų ir debesų kompiuterijos saugumo, rizikų valdymo, kriptografijos, saugios architektūros ir konfigūracijos, žmogiškųjų įgūdžių ir kt. Be to, pateikiama informacija apie darbuotojų švietimą, švietimo programų sertifikavimą, būtinus formuoti įgūdžius.

JAV CERT [85] įstaiga taip pat kas savaitę leidžia suvestines apie nustatytus naujus pažeidžiamumus, siunčia skubius pranešimus apie naujus saugumo įvykius. Valdžios

[83] LR kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428.

[84] Prieiga per internetą: https://www.ncsc.gov.uk/index/guidance?f%5B0%5D=field_topics%253Aname%3ARisk%20management.

[85] JAV Nacionalinio kibernetinio saugumo ir ryšių integracijos centro (NCCIC) interneto svetainė, prieiga per internetą: https://www.us-cert.gov/security-publications.

institucijoms pateikiami patarimai apie geriausias saugumo praktikas, pvz.: daiktų interneto apsauga, rinkėjų duomenų apsauga, būdus, kaip išvengti socialinės inžinerijos pavojų ir pan. Pateikiamos nuorodos į pažeidžiamumų duomenų bazes, saugios konfigūracijos standartus, informacijos apie saugumą dalijimosi platformas.

Estijos informacinių sistemų valdžios įstaiga savo tinklalapyje kas mėnesį skelbia pranešimus apie kibernetinio saugumo būklę, aptinkamą naują kenkėjiška programinę įrangą, organizuoja informacijos saugumo seminarus. Įstaiga skleidžia informaciją apie saugumo standartus, gaires, teikia rekomendacijas dėl saugumo didinimo, organizuoja ir koordinuoja kibernetinio saugumo mokslinių tyrimų ir plėtros veiklą, o tyrimų rezultatus skelbia interneto svetainėje[86].

Siekiant užkirsti kelią valstybės IS kūrimo spragų apraiškoms, turi būti numatyti privalomi reikalavimai atlikti grėsmių analizę, išeities (programinio) kodo peržiūrą ir kitus reikiamus saugumo testavimus, priklausomai nuo IS svarbos.

[86] Estijos informacinių sistemų valdžios įstaigos interneto svetainė, prieiga per internetą: https://www.ria.ee/ee/kuberturvalisuse-arendus-ja-uurimistegevus.html.

REKOMENDACIJŲ ĮGYVENDINIMO PLANAS

Rekomendacijos eilės numeris ataskaitoje	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Veiksmas / Priemonės / Komentarai*	Rekomendacijos įgyvendinimo ir informavimo apie įgyvendinimą data*
Siekiant užtikrinti geresnę valstybės informacinių išteklių valdymo kokybę ir aukštesnę YSVII tvarkytojų IT valdymo brandą, reikėtų:				
1.	Sukurti nacionalinę informacinę architektūrą ir jos valdymo mechanizmą, kuris leistų objektyviai nustatyti valstybės informacinių išteklių svarbą bei tinkamai kontroliuoti šį procesą ir suderinti ypatingos svarbos valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros nustatymo mechanizmus.	LR Vyriausybės įgaliota institucija	Remiantis tarptautinėje praktikoje pripažintais organizacijos architektūros principais, apibrėžti siekiamą nacionalinę informacinę architektūrą, kuri apimtų veiklos architektūrą, duomenų architektūrą, aplikacijų / informacinių sistemų architektūrą ir technologijų architektūrą bei jos brandos stebėsenos ir pokyčių valdymo procesus.	2019-12-01
		KAM	Parengti elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašą, be kita ko, įvertinant poveikį nacionalinei informacinei architektūrai ir ypatingos svarbos informacinės infrastruktūros objektams.	2019-03-01
		IVPK prie SM	Sukurti valstybės informacinių išteklių informacijos sąsajų žemėlapį bei jo tvarkymo metodines ir automatines priemones.	2018-12-31
2.	Išvystyti IT gerąsias valdymo praktikas atitinkantį valstybės informacinių išteklių valdymo mechanizmą, kuris užtikrintų bendrą ir į svarbiausius prioritetus orientuotą planavimą, numatytų siektiną IT valdymo brandos lygį ir pažangą vertinti leidžiantį stebėsenos mechanizmą, efektyviai naudojant sukurtas technines priemones.	LR Vyriausybės įgaliota institucija	Parengti Valstybės informacinių išteklių valdymo įstatymo pakeitimo projektą, kuriame būtų patikslinta valstybės informacinių išteklių planavimo ir IT valdymo kokybės reikalavimų nustatymo tvarka, atsižvelgiant į nacionalinės informacinės architektūros prioritetus.	2019-07-01
		LR Vyriausybės įgaliota institucija	Parengti valstybės IT projektų portfelio valdymo gaires, apimančias IT projektų portfelio valdymo procedūras,	2018-12-31

Rekomendacijos eilės numeris ataskaitoje	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Veiksmas / Priemonės / Komentarai*	Rekomendacijos įgyvendinimo ir informavimo apie įgyvendinimą data*
			dalyvaujančius subjektus, jų roles ir atsakomybes bei IT projektų stebėsenos technines priemones.	
		LR Vyriausybės įgaliota institucija	Peržiūrėti su ARSIS susijusius teisės aktus ir priimti sprendimus dėl ARSIS funkcionalumo tobulinimo.	2019-06-01
		IVPK prie SM	Parengti institucijos valstybės informacinių išteklių rekomenduojamo IT valdymo brandos lygio nustatymo ir vertinimo taisykles.	2019-12-01
Siekiant užtikrinti ypatingos svarbos valstybės informacinių išteklių saugumą ir atsparumą didėjančioms kibernetinėms grėsmėms, reikia:				
3.	Gerinti kibernetinio saugumo rizikų valdymą: atnaujinti reikalavimus, metodikas ir diegti nacionalinį IT rizikų valdymą, leidžiantį veiksmingai valdyti šalies mastu aktualias rizikas.	KAM	Patvirtinus Nacionalinę kibernetinio saugumo strategiją, parengti jos įgyvendinimo priemonių plano projektą, kuriame būtų numatyti veiksmai susiję su kibernetinio saugumo rizikų valdymu.	2019-12-31
		LR Vyriausybės įgaliotos institucijos	Įgyvendinti patvirtintame Nacionalinės kibernetinio saugumo strategijos priemonių plane numatytus veiksmus, susijusius su kibernetinio saugumo rizikų valdymu.	2023-06-01
4.	Didinti kibernetinio saugumo valdymo organizavimo ir įgyvendinimo efektyvumą: sukurti reikiamus kontrolės mechanizmus, kurie prisidėtų prie žmogiškųjų išteklių saugumo žinių ir gebėjimų didinimo, saugumo reikalavimų įgyvendinimo būklės gerėjimo ir IS pažeidžiamumų prevencijos.	KAM	Patvirtinus Nacionalinę kibernetinio saugumo strategiją, parengti jos įgyvendinimo priemonių plano projektą, kuriame būtų numatyti veiksmai susiję su žmogiškųjų išteklių saugumo žinių ir gebėjimų didinimu.	2019-12-31
		LR Vyriausybės įgaliotos institucijos	Įgyvendinti patvirtintame Nacionalinės kibernetinio saugumo strategijos priemonių plane numatytus veiksmus, susijusius su žmogiškųjų išteklių saugumo žinių ir gebėjimų didinimu.	2023-06-01
		KAM	Parengti Administracinių nusižengimų kodekso pakeitimus, kurie nustatytų įstaigų vadovams arba kitiems	2018-12-31

Rekomendacijos eilės numeris ataskaitoje	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Veiksmas / Priemonės / Komentarai*	Rekomendacijos įgyvendinimo ir informavimo apie įgyvendinimą data*
			atsakingiems asmenims administracinę atsakomybę už organizacinių ir techninių kibernetinio saugumo reikalavimų nevykdymą ir teisėtų Nacionalinio kibernetinio saugumo centro nurodymų, susijusių su kibernetinio saugumo užtikrinimu, neįvykdymą laiku.	

* Priemones ir terminus rekomendacijoms įgyvendinti pateikė Vyriausybė, Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos ir Krašto apsaugos ministerija.

Atstovai ryšiams, atsakingi už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais:
Vyriausybės Kanceliarijos Strateginių kompetencijų grupės patarėjas
Martynas Jokūbauskas, tel. (8 706) 63 969, martynas.jokubauskas@lrv.lt.

Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos l. e. direktoriaus pareigas
Kęstutis Andrijauskas, tel. (8 693) 63 852, kestutis.andrijauskas@ivpk.lt.

Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento direktorius
Jonas Skardinskas, tel. (8 706) 80 800, jonas.skardinskas@kam.lt.

L. e. p. Valdymo audito departamento direktorė Jurgita Grebenkovienė

Valdymo audito departamento direktoriaus pavaduotoja Živilė Uždavinytė-Kerbelė

Auditą atliko:

Venera Michalovska (grupės vadovė), Aidana Karbauskienė, Dainoras Bagavičius, Gytis Tamulevičius, Linas Balčiūnas, Olga Gricajenko.

Valstybinio audito ataskaita pateikta: Vyriausybei, Seimo Audito komitetui, Susisiekimo ministerijai, Ūkio ministerijai, Krašto apsaugos ministerijai, Vidaus reikalų ministerijai, Informacinės visuomenės plėtros komitetui prie Susisiekimo ministerijos.

PRIEDAI

Valstybinio audito ataskaitos
„Ypatingos svarbos valstybės
informacinių išteklių valdymas“
1 priedas

Santrumpos

AAI – aukščiausioji audito institucija.
ARSIS – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema.
COBIT (angl. *Control Objectives for Information and related Technologies*) – ISACA[87] sukurta IT valdymo ir vadovavimo metodika.
EBPO (angl. *Organisation for Economic Co-operation and Development*, OECD) – Tarptautinė ekonominio bendradarbiavimo ir plėtros organizacija.
ENISA (angl. *European Union Agency for Network and Information Security*) – Europos Sąjungos tinklų ir informacijos apsaugos agentūra (Europos kibernetinio saugumo kompetencijos centras).
IRT – Informacinės ir ryšių technologijos.
IS – informacinė sistema, registras, kadastras;
IT – informacinės technologijos;
IVPK – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos.
KAM – Krašto apsaugos ministerija.
NKSC – Nacionalinis kibernetinio saugumo centras.
PLS (angl. *Service Level Agreement*) – paslaugų lygio susitarimas.
YSVII – ypatingos svarbos valstybės informaciniai ištekliai.
VRM – Vidaus reikalų ministerija.

Sąvokos

Informacija – tai duomenys, kurių turinys ir forma tinka tam tikram naudojimui. Informacija gaunama apdorojus duomenis, tai galėtų būti formatavimas, filtravimas, sumavimas analizė ar kitos sudėtingesnės operacijos[88].
Informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, apdorojanti neįslaptintą informaciją[89].
Informacinė sistema – registras ar valstybės informacinė sistema, kaip tai apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, taip pat visuma privačių subjektų valdomų teisinių, organizacinių, techninių ir programinių priemonių, skirtų naudojant informacines technologijas apdoroti informaciją[90].

[87] ISACA – ne pelno siekianti pasaulinė asociacija, teikianti praktines gaires, standartus ir kitas efektyvias priemones informacinių sistemų naudojimui. Prieiga per internetą http://www.isaca.org/about-isaca/Pages/default.aspx.
[88] Saulis A., Vasilecas O., Informacinių sistemų projektavimo metodai. Vilnius: VGTU, 2008.
[89] Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos, patvirtintos LR Vyriausybės 2016-07-20 nutarimu Nr. 742, 2.1 p.
[90] Ten pat, 2.2 p.

Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams[91].

Ypatingos svarbos paslauga – ypatingos svarbos sektoriuje ypatingos svarbos infrastruktūros objekto teikiama paslauga, būtina valstybės funkcionavimui, valstybės valdymui, ekonomikai, sveikatos apsaugai, gynybai ar saugumui užtikrinti, kurios neveikimas ar sutrikimas padarytų didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams[92].

IT valdymo branda – COBIT taikomas metodas, kuris organizacijos brandos lygį leidžia įvertinti nuo neegzistuojančio (0) iki optimalaus (5):

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

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

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

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

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

5 – optimalus. Dėl nuolatinio gerinimo ir brandos modeliavimo su kitomis organizacijomis procesai ištobulinti iki geros praktikos lygio. Kad darbo eiga būtų automatizuota, IT taikomos integruotu būdu, suteikiant priemones kokybei ir efektyvumui gerinti ir sudarant sąlygas organizacijai greitai prisitaikyti[93].

Rizika – pagrįstai nustatoma aplinkybė ar įvykis, galintys turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui[94].

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.[95]

Valstybės informacinių išteklių valdymas – valstybės informacinių išteklių kūrimo, tvarkymo, plėtros tikslų nustatymas, jų tvarkymo ir priežiūros organizavimas ir kontrolė, valstybės tarnautojų ir (arba) darbuotojų, dirbančių pagal darbo ar karo tarnybos sutartis, informacinių technologijų priemonėmis apdorojančių informaciją, dokumentus ir (arba) jų kopijas, veiklos organizavimas ir priežiūra.[96]

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

[91] LR kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 2 str. 2 d.

[92] Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos, patvirtintos LR Vyriausybės 2016-07-20 nutarimu Nr. 742, 2.4 p.

[93] COBIT 4.1, 2011 m., Vilnius, 17-20 psl.

[94] 2016 m. liepos 6 d. Europos parlamento ir Tarybos direktyva (ES) Nr. 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

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

[96] Ten pat, 2 str., 18 d.

Valstybinio audito ataskaitos
„Ypatingos svarbos valstybės informacinių išteklių valdymas“
2 priedas

Audito apimtis ir metodai

Audito apimtis

Audito tikslas – įvertinti ypatingos svarbos valstybės informacinių išteklių valdymą (bendrąją kontrolę), brandą ir nustatyti sistemines valstybės informacinių išteklių valdymo problemas.

Pagrindiniai audito klausimai – svarbiausios audito sritys – IT strateginis planavimas (PO1), Informacinės architektūros nustatymas (PO2), IT rizikų valdymas (PO9), Pokyčių valdymas (AI6), Nepertraukiamo paslaugų teikimo užtikrinimas (DS4), Sistemų saugumo užtikrinimas (DS5), Duomenų tvarkymas (DS11), IT veiklos stebėsena ir vertinimas (ME1), IT valdymo užtikrinimas (ME4) – vertintos pagal COBIT metodiką ir atitiktį LR teisės aktų reikalavimams.

Audituojami subjektai – Susisiekimo ministerija, Vidaus reikalų ministerija (iki 2018-01-01), Krašto apsaugos ministerija, Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos.

Audituojamas laikotarpis – 2014–2017 m.

Apribojimai (jeigu yra) – audito procedūros atliktos tik organizacijose, kurios audito pradžioje metu identifikuotos kaip 1 kat. IS valdytojos/tvarkytojos. Dalis informacijos yra konfidenciali, todėl ji pateikiama apibendrintai. Išankstinio tyrimo metu buvo nustatyta, kad vienos organizacijos, tvarkančios 1 kat. IS, IT valdymo branda siekia nulinį lygį, todėl detaliosios audito procedūros pagrindinio tyrimo metu nebuvo atliekamos, o informacija apie organizacijos būklę apibendrinama pagal išankstinio tyrimo metu gautus duomenis ir vertinimus. Kitos organizacijos IT bendroji kontrolė vertinta 2016 m. valstybinio audito metu, pervertinus šios organizacijos IT valdymo būklę, nustatyta, kad pokyčių po minėto audito neįvyko, todėl detaliosios audito procedūros pagrindinio tyrimo metu nebuvo atliekamos, o informacija apie organizacijos būklę vertintina pagal išankstinio tyrimo metu gautus duomenis.

Auditas atliktas pagal Valstybinio audito reikalavimus[97] ir tarptautinius aukščiausiųjų audito institucijų standartus[98].

Audito duomenų rinkimo ir vertinimo metodai

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
1. Neveiksminga svarbiausių valstybės informacinių išteklių nustatymo sistema		
1.1. Netinkamai nustatoma ypatingos svarbos valstybės informacinių išteklių svarba	Dokumentų analizė. Nagrinėjome: □ Lietuvos teisės aktus, reglamentuojančius valstybės informacinių išteklių identifikavimą; □ 44 IS dokumentacija (duomenų saugos nuostatai, specifikacijos); □ Organizacijų pateikti dokumentai (informacijos klasifikavimo planai,	*Įvertinti informacinės architektūros valdymo atitikimą COBIT ir teisės aktų reikalavimams, kokios sisteminės problemos.*
1.2. Ypatingos svarbos valstybės informacinių išteklių bei ypatingos svarbos informacinės		*Įvertinti informacinės architektūros valdymo atitikimą COBIT ir teisės aktų*

[97] LR valstybės kontrolieriaus 2002-02-21 įsakymas Nr. V-26 „Dėl Valstybinio audito reikalavimų patvirtinimo“.
[98] 3000-asis TAAIS „Veiklos audito standartas“ (http://www.vkontrole.lt/page.aspx?id=350).

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
infrastruktūros identifikavimo sistema nėra bendra	informacinės architektūros nustatymo tvarkos); □ Valstybės kontrolės valstybinių auditų ataskaitas (2006-09-12 Nr. IA-9000-4-2 „Valstybinių informacinių sistemų bendroji kontrolė. Valstybinis ir institucinis lygmenys“, 2013-01-31 Nr. VA-P-90-3-3 „Valstybės informacinių išteklių valdymas“ ir rekomendacijų įgyvendinimo stebėsenos ataskaitas; □ Užsienio šalių gerosios praktikos pavyzdžius (Jungtinės Amerikos Valstijos ir Estijos IT architektūros dokumentus; Pokalbiai su YSVII tvarkytojais, SM, IVPK, VRM, KAM, NKSC, NRD CS.	*reikalavimams, kokios sisteminės problemos.*
2. Valstybės informacinių išteklių valdymo sistema neprisideda prie ypatingos svarbos valstybės informacinių išteklių valdymo gerinimo		
2.1. IT strateginis planavimas nėra darnus	Dokumentų analizė. Nagrinėjome: □ Strateginius planavimo dokumentus (organizacijų strateginiai dokumentai, veiklos ir stebėsenos rezultatų ataskaitos, Viešojo valdymo tobulinimo programa); □ Lietuvos teisės aktus, reglamentuojančius strateginio planavimo sistemą, analizė (strateginio planavimo metodikas, IT plėtros plano rengimo, derinimo tvarką, kt.); □ EBPO ataskaitą (OECD Public Governance Reviews, Lithuania Fostering open and inclusive policy making) □ Lietuvoje atliktų tyrimų medžiagą (2015 m. tyrimas „Europos skaitmeninė darbotvarkė: Lietuvos požiūris“: galutinė tyrimo ataskaita, 2012 m. vertinimo ataskaita „Lietuvos informacinės visuomenės plėtros tendencijų ir prioritetų 2014-2020 m. vertinimas“, 2017 m. KURK LIETUVAI projektu metu atliktą tyrimą „Lietuvos strateginio planavimo dokumentų sistemos optimizavimo modelis“); □ kitus organizacijų pateiktus papildomus dokumentus (įsakymai, tvarkos, informacija apie pasirašytas paslaugų sutartis, patirtas sąnaudas, raštai, kt.); □ Valstybės kontrolės valstybinių auditų ataskaitas (2006-09-12 Nr. IA-9000-4-2 „Valstybinių informacinių sistemų bendroji kontrolė. Valstybinis ir institucinis lygmenys“, 2013-01-31 Nr. VA-P-90-3-3 „Valstybės informacinių išteklių valdymas“, 2016-10-10 Nr. VA-P-60-2-17 „Programinio biudžeto sistema: strateginių veiklos planų sudarymas ir įgyvendinimo stebėsena“) ir rekomendacijų įgyvendinimo stebėsenos ataskaitas. Pokalbiai su YSVII tvarkytojais, SM, IVPK, VRM, KAM, NKSC.	*Įvertinti IT strateginio planavimo ir stebėsenos valdymo atitikimą COBIT ir teisės aktų reikalavimams, kokios sisteminės problemos.*

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
2.2. IT stebėsena neparodo ypatingos svarbos valstybės informacinių išteklių valdymo būklės	Dokumentų analizė. Nagrinėjome: □ Finansų ministerijos ataskaitą „Vyriausybei atskaitingų institucijų ir įstaigų bendrųjų funkcijų 2016 m. efektyvumo vertinimas“ (2016); □ Viešojo valdymo tobulinimo 2012–2020 metų programos įgyvendinimą; □ kitus organizacijų pateiktus papildomus dokumentus (su vertintais procesais susijusi dokumentacija, informaciją apie įgyvendintas priemones pagal strategiją, naudojamos matavimo metodikos, vertinimo kriterijai, darbo ataskaitos, būklės vertinimo ataskaitos). Pokalbiai su YSVII tvarkytojais, SM, IVPK, VRM, KAM, NKSC.	*Įvertinti IT strateginio planavimo ir stebėsenos valdymo atitikimą COBIT ir teisės aktų reikalavimams, kokios sisteminės problemos.*
3. Nepakankamai veiksmingai įgyvendinamos priemonės, galinčios užtikrinti ypatingos svarbos valstybės informacinių išteklių atsparumą kibernetinių grėsmių lygiui		
3.1. IT saugumo rizikų vertinimas nėra pakankamai veiksmingas	Dokumentų analizė. Nagrinėjome: □ LT teisės aktus ir gerosios praktikos reikalavimus, reglamentuojančius IT rizikos vertinimą ir valdymą; □ ENISA ataskaitas („ad hoc Working Group on National Risk Management Preparedness“ (2011), „National Cyber Security Strategies Practical Guide on Development and Execution“ (2012), „Stocktaking, Analysis and Recomendations on the Protection of CIIS“ (2016). □ EBPO dokumentą (*Recommendation of the Council on the Protection of Critical Information Infrastructures*“ (2008); □ Pasaulio ekonomikos forumo pasaulinių rizikų ataskaitą (*Insight Report „The Global Risks Report 2018“*); □ 2016 m. ir 2017 m. nacionalinės kibernetinio saugumo būklės ataskaitas; □ organizacijų pateiktus papildomus dokumentus (rizikos valdymo tvarkas, rizikos vertinimo ataskaitas, rizikos mažinimo/tvarkymo planus). Pokalbiai su YSVII tvarkytojais, SM, IVPK, VRM, KAM, NKSC.	*Įvertinti saugumo, tame tarpe atsarginių kopijų ir veiklos tęstinumo užtikrinimo, valdymo atitikimą COBIT ir teisės aktų reikalavimams, kokios sisteminės problemos.*
3.2. Sistemiškai nenaudojamos kibernetines grėsmes mažinančios saugumo priemonės	Dokumentų analizė. Nagrinėjome: □ ES, LT teisės aktus ir gerosios praktikos reikalavimus, reglamentuojančius saugumo reikalavimus; □ Atliktų tyrimų medžiagą (Deloitte SAS 2018 m. tyrimo „Enjeux Cyber 2018. L'évolution de la menace Cyber“); □ OWASP *bendruomenės informaciją, susijusią* su programinės įrangos saugumu; □ Organizacijų pateiktus dokumentus (saugumo politikos dokumentai, pareigybių aprašymai, saugos atitikties vertinimo, pažeidžiamumų vertinimo ataskaitas, tobulinimo planus, veiklos	*Įvertinti saugumo, tame tarpe atsarginių kopijų ir veiklos tęstinumo užtikrinimo, valdymo atitikimą COBIT ir teisės aktų reikalavimams, kokios sisteminės problemos.*

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
	tęstinumo/atkūrimo planai, šių planų testavimo ataskaitos, atsarginių kopijų tikrinimo įrašai (žurnalai), patikrinimo ataskaitos, tęstinumo užtikrinimo metodikos); □ ARSIS pateikiama informacija; □ 2016 m. ir 2017 m. nacionalinės kibernetinio saugumo būklės ataskaitas; □ Kitų šalių (Jungtinės Karalystės, Jungtinių Amerikos Valstijų, Estijos) kibernetinio saugumo centro veiklas; □ organizacijų pateiktus dokumentus (įsakymai dėl saugos įgaliotinio paskyrimo, saugumo politikos dokumentacija, mokymų dokumentacija, atitikties vertinimo, pažeidžiamumų vertinimo ataskaitos, pakeitimų valdymo tvarkos, testavimo dokumentai, kita saugumo priemonių įgyvendinimo dokumentacija). Pokalbiai su YSVII tvarkytojais, SM, IVPK, VRM, KAM, NKSC. Tyrimo metu atlikome 12 YSVII tvarkytojų apklausą pagal sudarytus klausimynus dėl organizacinių ir techninių saugumo reikalavimų įgyvendinimo.	

Valstybinio audito ataskaitos
„Ypatingos svarbos valstybės informacinių išteklių valdymas“
3 priedas

Vertintų COBIT procesų gretinimas su Lietuvos teisės aktais

Procesas	Teisės aktas, atitinkantis COBIT reikalavimus	Teisės akto atitiktis COBIT procesui	Dabartinio teisinio reglamentavimo trūkumai
PO1. Strateginio IT plano apibrėžimas	- LR valstybės informacinių išteklių valdymo įst., 2011-12-15 Nr. XI-1807 (**P**) - LRV 2002-06-12 Nr. 825[99] (**P**) - IVPK 2013-03-14 įsakymas Nr. T-29[100] (**P**)		Nenumatytos strateginio valdymo struktūros, kurios būtų atsakingos už IT plėtros tikslų, prioritetų nustatymą; plano tvirtinimą, stebėseną ir naudos vertinimą, sukūrimą. Neapibrėžta informacija (veiklos poreikiai, nepageidaujamos organizacijos ir IT rizikos, IT saugumo, valdymo būklė, branda ir t.t.), kuri turėtų būti surenkama ir vertinama rengiant IT plėtros planą. Nenumatyta, kad detalus (metinis) organizacijos planas turi atitikti IT plėtros planą. Reguliavimas nukreiptas į dokumento turinį ir derinimą, vyrauja siauras požiūris į IT strateginį planavimą, kuris apimtų visą IT sritį.
PO2. Informacinės architektūros nustatymas	- LRV 2013-07-24 nutarimas Nr. 716[101] (**P**) - LRV 2013-02-27 nutarimas Nr. 180[102] (**P**) - IVPK 2013-03-14 įsakymas Nr. T-29 (**P**)		TA nėra nustatytų reikalavimų/bendrų standartų informacinės architektūros modeliui, organizacinei atsakomybei už informacinės architektūros modelio kūrimą ir priežiūrą. Viešojo tobulinimo 2012-2020 m. programoje buvo planuota taikyti veiklos ir technologijų sujungimo į bendrą įstaigų architektūrą metodus (TOGAF, COBIT, ITIL ir kiti), tačiau programos įgyvendinimo planuose numatytos priemonės nepadeda siekti programoje numatytų tikslų.
PO9. IT rizikos vertinimas ir valdymas	- LRV 2013-07-24 nutarimas Nr. 716 (**P**) - VRM 2004-05-06 įsakymas Nr. 1V-156[103] (**P**)		TA nenumatyta IT rizikos valdymo sistemą derinti su organizacijos rizikos valdymo sistema. Nėra išsamiai aprašytas rizikų valdymo procesas, kaip ji turi būti įgyvendinamas. Rizikų vertinimo metodika pasenusi.

[99] Strateginio planavimo metodika, patvirtinta LR Vyriausybės 2002-06-12 nutarimu Nr. 827.

[100] Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta IVPK direktoriaus 2014-02-25 įsakymu Nr. T-29.

[101] LR 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“.

[102] Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, patvirtintas LR Vyriausybės 2013-02-27 nutarimu Nr. 180.

[103] Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta LR vidaus reikalų ministro 2004-05-06 įsakymu Nr. 1V-156.

Procesas	Teisės aktas, atitinkantis COBIT reikalavimus	Teisės akto atitiktis COBIT procesui	Dabartinio teisinio reglamentavimo trūkumai
AI6. Pokyčių valdymas	- LRV 2013-07-24 nutarimas Nr. 716 (**P**) - IVPK 2013-06-19 įsakymas Nr. T-83[104] (**R**) - IVPK 2013-03-14 įsakymas Nr. T-29 (**P**) - IVPK 2017-11-22 įsakymas Nr. T-126[105] (**R**)		Rekomendacinio pobūdžio reguliavimas neužtikrina, kad procesas bus įgyvendinamas pagal siūlomą mechanizmą. Atsiranda skirtinga praktika ir valdymo branda. Nepakankamas pokyčių testavimo reglamentavimas.
DS4. Nepertraukiamo paslaugų teikimo užtikrinimas	- LRV 2013-07-24 nutarimas Nr. 716 (**P**) - LRV 2016-04-20 nutarimas Nr. 387 (**P**) - VRM 2013-10-04 įsakymas Nr. 1V-832[106] (**P**)		Reikalavimai nukreipti į dokumento turinį, tačiau nenumato šio proceso įgyvendinimo mechanizmo, nenustatytas periodinis veiklos tęstinumo plano privalomas testavimas.
DS5. Sistemų saugumo užtikrinimas	- Kibernetinio saugumo įst. 2014-12-11 Nr. XII-1428 (**P**) - LRV 2013-07-24 nutarimas Nr. 716 (**P**) - LRV 2016-04-20 nutarimas Nr. 387[107] (**P**) - VRM 2004-05-06 įsakymas Nr. 1V-156 (**P**)		Nenumatyta pakankama saugos užtikrinimo valdymo organizacinė struktūra (nėra numatyta saugos priežiūros komiteto sukūrimas, neužtikrinamas saugos įgaliotinio pakankamas funkcijų atskyrimas nuo IT administravimo veiklos). Rekomenduojama IT paslaugų valdymo procesus sertifikuoti pagal ISO/IEC 20000 standarto reikalavimus. Numatyta, kad institucijos turi įgyvendinti Lietuvos standarte LST ISO/IEC 27002:2009 nurodytas saugos priemones, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, IS ar naudojamos IS techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2006 nurodytus reikalavimus informacijos saugumo valdymo sistemai.
DS11. Duomenų valdymas (tvarkymas)	- LRV 2013-02-27 nutarimas Nr. 180 (**P**) - LRV 2013-07-24 nutarimas Nr. 716 (**P**)		Nėra numatytų reikalavimų atsarginių kopijų politikai sukurti organizaciniu lygmeniu. Nenumatytas privalomas periodinis atsarginių kopijų testavimas. Palikus laisvę organizacijoms pačios apibrėžti atsarginių kopijų politiką, tai deramai nėra atliekama, atsiranda skirtinga valdymo praktika, kuri įtakoja nepakankamą brandos lygį.

[104] Informacinių technologijų paslaugų valdymo metodika, patvirtinta IVPK direktoriaus 2013-06-19 įsakymu Nr. T-83.
[105] Projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijos, patvirtintos IVPK direktoriaus 2017-11-22 įsakymu Nr. T-126.
[106] Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti LR vidaus reikalų ministro 2013-10-04 įsakymu Nr. 1V-832.
[107] Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas LR Vyriausybės 2016-04-20 nutarimu Nr. 387.

Procesas	Teisės aktas, atitinkantis COBIT reikalavimus	Teisės akto atitiktis COBIT procesui	Dabartinio teisinio reglamentavimo trūkumai
ME1. IT veiklos stebėsena ir vertinimas	- IVPK 2013-06-19 įsakymas Nr. T-83 (**R**) - IVPK 2013-03-14 įsakymas Nr. T-29 (**P**)		Nenustatyti visoms valstybės valdymo sritims pritaikomi IT efektyvumo ir saugos matavimo kriterijai, koks viešajame sektoriuje turi būti siektinas IT valdymo brandos lygis, atsiskaitymo už pasiektus rezultatus mechanizmas nėra aiškus. Organizacijos taiko savo metodus, kurie išsiskiria ir nėra subalansuoti, todėl palyginti ir panaudoti informaciją strateginiams sprendimams sudėtinga.
ME4. IT valdymo užtikrinimas	- LR valstybės informacinių išteklių valdymo įst., 2011-12-15 Nr. XI-180 (**P**) - IVPK 2013-06-19 įsakymas Nr. T-83 (**R**)		Viešojo tobulinimo 2012-2020 m. programoje buvo planuota taikyti veiklos ir technologijų sujungimo į bendrą įstaigų architektūrą metodus (TOGAF, COBIT, ITIL ir kiti), taip pat taikyti bendrąjį IT valdymą reglamentuojantį ISO 38500. Konsoliduoti valdymo standartai nėra įdiegti, atsiranda skirtinga branda, valdymo praktika.
✔ Atitinka visiškai  Atitinka iš dalies  Neatitinka; **P** – privalomo pobūdžio, **R** – rekomendacinio pobūdžio			

Šaltinis: AAI