

Vilniaus universitetas
Tarptautinis žinių vadybos ir žinių ekonomikos centras

Viktorija Mirošničenko,
Informacijos vadybos studijų programos studentė

**IT SAVIANALIZĖS METODIKOS TAIKYMAS AUKŠČIAUSIOSE AUDITO
INSTITUCIJOSE**

MAGISTRO DARBAS

Mokslinis vadovas dr. I. Aleliūnas

Vilnius, 2007

Viktorijos Mirošničenko magistro darbas

tema

IT savianalizės metodikos taikymas Aukščiausiose audito institucijose

parengtas gynimui.

(data) (vadovo parašas)

Darbas įregistruotas Tarptautinio žinių ekonomikos ir žinių vadybos centre

(data) (administratores parašas)

Magistro darbą ginti leidžiu

_____ (centro direktoriaus parašas) _____

(data)

Recenzentu skiriu

(data) (Direktoriaus parašas)

Darba recenzavimui gavau

(data) (recenzento parašas)

Mirošničenko, Viktorija

Mi291 IT savianalizės metodikos taikymas Aukščiausiose audito institucijose: magistro darbas/ Viktorija Mirošničenko; mokslinis vadovas dr. I. Aleliūnas; Vilniaus universitetas. Tarptautinis žinių ekonomikos ir žinių vadybos centras. – Vilnius, 2007. – 75,- Mašinr.- Santr. angl.-Bibliogr.: p. 68-70 - (46 pavad.)

UDK 004:657.6

IT savianalizės metodika; IT strateginis valdymas; kontrolės procedūros; COBIT; Aukščiausioji audito institucija; auditas; IT procesai.

Magistro *darbo objektas* – EUROSAI Informacinių technologijų darbo grupės sukurta ir sėkmingai taikoma Informacinių technologijų savianalizės metodika. *Darbo tikslas* – pristatyti Informacinių technologijų savianalizės metodiką, kaip priemonę nustatyti Aukščiausių audito institucijų vykdomos veiklos santykį su informacinių technologijų teikiamomis galimybėmis, įvertinti informacinių technologijų brandą ir numatyti priemones jų brandos lygiui stiprinti ir įvertinti šią metodiką remiantis jos praktinio taikymo rezultatais. Pagrindiniai *darbo uždaviniai*:

- apibrėžti informacinių technologijų strateginio valdymo sampratą ir jo svarbą Aukščiausių audito institucijų veikloje;
- apžvelgti COBIT geros praktikos rinkinį, nes jo pagrindu EUROSAI Informacinių technologijų darbo grupė sukūrė Informacinių technologijų savianalizės metodiką.
- supažindinti su Informacinių technologijų savianalizės metodikos raida, jos tikslais ir uždaviniais, reikalavimais, keliamais šiai metodikai;
- detaliai aprašyti šios metodikos veiksmų eigą;
- išsiaiškinti Informacinių technologijų savianalizės metodikos privalumus ir trūkumus, analizuojant Informacinių technologijų savianalizės seminarų, vykusių Aukščiausiose audito institucijose, rezultatus.

Darbas yra *aktualus*, nes iki šiol valstybinėse įstaigose nėra pakankamų žinių apie informacinių technologijų valdymo procesų tobulinimo metodus. Dažnai informacinių technologijų plėtra yra atskirta nuo pagrindinių įstaigos veiklos procesų, todėl svarbu susieti IT ir veiklos procesus, nustatyti informacinių technologijų brandumo lygį, atrasti stipriausias ir silpnąsias organizacijos vietas. Čia ypač svarbu - galimybė naudoti COBIT, kuris yra įrankis informacinių technologijų valdymui. Darbas naudingas tiek mokslinė, tiek praktinė prasme visiems besidomintiems ir dirbantiems IT valdymo srityje.

Darbe iš esmės remiamasi tarptautiniu geros praktikos rinkiniu COBIT ir EUROSAI Informacinių technologijų darbo grupės sukurta IT savianalizės metodika. Taip pat atlikta įvairių su šio darbo tematiką susijusių literatūros šaltinių apžvalga ir analizė.

TURINYS

ĮVADAS	5
1. INFORMACINIŲ TECHNOLOGIJŲ STRATEGINIO VALDYMO SVARBA.....	8
1.1 IT STRATEGINIO VALDYMO SAMPRATA	8
1.2 VIDAUS KONTROLĖS POREIKIS IT STRATEGINIAME VALDYME	11
1.3 IT ĮTAKA VALSTYBINIAME SEKTORIUJE IR VALSTYBINIO AUDITO PROCESUOSE	13
1.4 IT STRATEGINIO VALDYMO SVARBA AUKŠČIAUSIOSE AUDITO INSTITUCIJOSE.....	18
1.5 SKYRIAUS APIBENDRINIMAS	18
2. COBIT SAMPRATA	19
2.1 COBIT ISTORIJA.....	19
2.2 KETVIRTOSIOS IR TREČIOSIOS COBIT VERSIJŲ PALYGINIMAS	21
2.3 COBIT PROCESAI	22
2.4 COBIT – ĮRANKIS SAVIANALIZĖS PRIEMONĖMS KURTI.....	25
2.5 SKYRIAUS APIBENDRINIMAS	31
3. AAI IT SAVIANALIZĖS METODIKA PARENGTA EUROSAI IT DARBO GRUPĖS.....	32
3.1 IT SAVIANALIZĖS METODIKOS PRIVALUMAI	34
3.2 IT SAVIANALIZĖS RAIDA	35
3.3 AAI SUKURTOS IT SAVIANALIZĖS ĮGYVENDINIMO ETAPAI	38
3.4 SKYRIAUS APIBENDRINIMAS	48
4. IT SAVIANALIZĖS METODIKOS TAIKYMAS AUKŠČIAUSIOSE AUDITO INSTITUCIJOSE	49
4.1 IT SAVIANALIZĖS SEMINARAI LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖJE	49
4.2 IT SAVIANALIZĖS SEMINARAS LATVIJOS RESPUBLIKOS VALSTYBĖS KONTROLĖJE.....	52
4.3 IT SAVIANALIZĖS SEMINARAS UKRAINOS RESPUBLIKOS ŠĄSKAITŲ RŪMUOSE	56
4.4 GAUTŲ REZULTATŲ ANALIZĖ	59
4.5 NAUJAUSIOS 4.0 IT SAVIANALIZĖS METODIKOS PRISTATYMAS.....	63
4.6 SKYRIAUS APIBENDRINIMAS	64
IŠVADOS.....	66
BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS.....	68
SUMMARY	71
PRIEDAI.....	72
1 PRIEDAS. LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖS VEIKLOS PROCESAI	72
1 PRIEDAS. KLAUSIMYNAS APIE IT SAVIANALIZĖS ĮGYVENDINIMĄ	74

IVADAS

Informacinių technologijų strateginis valdymas – tai sudėtinė bendrojo organizacijos valdymo dalis, nuo kurios priklauso, kaip efektyviai informacinės technologijos remia ir plėtoja bendruosius organizacijos tikslus. Tai nėra informacinių technologijų savitikslių plėtra, tačiau jų nuoseklus susiejimas su organizacijos veiklos procesais, padedantis užtikrinti, kad organizacijos veikla būtų geresnė.

Informacinių technologijų plėtra, kai organizacijos veiklos procesai yra atsieti nuo inicijuojamų ir vykdomų informacinių technologijų projektų, nėra optimali, todėl rizika, kad inicijuojami ir vykdomi informacinių technologijų projektai neatitiks organizacijos tikslams, o lėšos nebus išleistos efektyviai, didėja.

Informacinių technologijų strateginis valdymas – tai vadybinė, ne technologinė, disciplina, ir pakankamai nauja, nes esamos informacinių technologijų valdymo metodikos kuriamos ir tobulinamos. Realus jos perkėlimas į praktinę taikymų sritį dar tik prasideda, o profesionalus ir visa apimantis informacinių technologijų valdymo metodų naudojimas yra svarbus perspektyvinis uždavinys, apie kurį jau šiuo metu reikia galvoti.

Informacinių sistemų auditoriai ir valdymo specialistai, matydami esminius ir besikartojančius informacinių technologijų strateginio valdymo trūkumus įvairių šalių organizacijose, nusprendė sukurti paprastą metodiką, kuri, naudodama COBIT geros praktikos rinkiniu ir savianalizės principus, leistų organizacijoms pačioms įvertinti esamą informacinių technologijų brandą ir numatyti jos tobulinimo perspektyvas, susiejant organizacijos veiklos procesus su standartizuotais COBIT informacinių technologijų procesais.

EUROSAI Informacinių technologijų darbo grupės pasitarime, vykusiam 2002 m. rugsėjo 30 d. – spalio 1 d. Hagoje (Nyderlandai) buvo sudaryta projekto grupė metodikai parengti, pagal kurią Aukščiausiosios audito institucijos galėtų naudoti informacinių sistemų audito COBIT metodiką, savarankiškai atlikdamos informacinių technologijų savianalizę. Metodikos išbandymui ir supažindinimui buvo numatyti ir įgyvendinti bandomieji informacinių technologijų savianalizės seminarai Aukščiausiose audito institucijose – EUROSAI Informacinių technologijų darbo grupės narėse, o vėliau – ir kitose Aukščiausiose audito institucijose, EUROSAI narėse.

Rezultatai, gauti daugelyje Informacinių technologijų savianalizės renginių, vykusių skirtingu laiku ir skirtingų šalių Aukščiausiose audito institucijose, leidžia pakankamai objektyviai nustatyti pagrindinius aukščiausiųjų audito institucijų veiklos procesus, ir įvertinti jų ryšį su informacinių technologijų COBIT procesais.

Magistro *darbo objektas* – EUROSAI informacinių technologijų darbo grupės sukurta ir sėkmingai taikoma Informacinių technologijų savianalizės metodika. *Darbo tikslas* – pristatyti Informacinių technologijų savianalizės metodiką, kaip priemonę nustatyti Aukščiausių audito institucijų vykdomos veiklos santykį su informacinių technologijų teikiamomis galimybėmis, įvertinti informacinių technologijų brandą ir numatyti priemones jų brandos lygiui stiprinti, tai pat įvertinti šią metodiką remiantis jos praktinio taikymo rezultatais. Pagrindiniai *darbo uždaviniai*:

- apibrėžti informacinių technologijų strateginio valdymo sampratą ir jo svarbą Aukščiausių audito institucijų veikloje;
- apžvelgti COBIT geros praktikos rinkinį, nes jo pagrindu EUROSAI Informacinių technologijų darbo grupė sukūrė Informacinių technologijų savianalizės metodiką.
- supažindinti su Informacinių technologijų savianalizės metodikos raida, jos tikslais ir uždaviniais bei reikalavimais, keliamais šiai metodikai;
- detaliai aprašyti šios metodikos veiksmų eigą;
- išsiaiškinti Informacinių technologijų savianalizės metodikos privalumus ir trūkumus, analizuojant Informacinių technologijų savianalizės seminarų, vykusių Aukščiausiose audito institucijose, rezultatus.

Nepriklausomai nuo to, kad Informacinių technologijų savianalizės metodiką rengė Aukščiausiųjų audito institucijų darbuotojai, ir kad ši metodika yra taikoma daugelyje Europos Aukščiausiųjų audito institucijų, pati metodika yra universali, ir jos taikymas viešojo sektoriaus įstaigose bei organizacijose yra galimas tiek, kiek viešojo sektoriaus įstaigos ir organizacijos sugeba nustatyti bendrusios savo veiklos procesus ir susieti juos su informacinių technologijų procesais.

Darbas yra *aktualus*, nes viešojo sektoriaus įstaigose ir organizacijose kol kas nėra pakankamų žinių apie informacinių technologijų valdymo procesų tobulinimo metodus. Dažnai informacinių technologijų plėtra yra suprantama kaip technologinis, o ne vadybinis uždavinys, todėl tampa atskirta nuo pagrindinių įstaigos veiklos procesų (atsakingu skiriant Informacinių technologijų departamentą) ir vyksta nepriklausomai nuo pagrindinių įstaigos veiklos. Tai didina riziką, kad inicijuojami ir vykdomi informacinių technologijų projektai neatitiks įstaigų tikslų, o lėšos nebus išleistos efektyviai.

Svarbu skatinti viešojo sektoriaus įstaigų ir organizacijų vadovus įdiegti jų vadovaujamosiose įstaigose informacinių technologijų strateginio valdymo pagrindus, numatyti reikiamas priemones ir sprendimus šiam tikslui pasiekti. Informacinių technologijų savianalizės metodika padeda įgyvendinti informacinių technologijų strateginį valdymą: susiejamai informacinių technologijų ir veiklos procesai, nustatomas informacinių technologijų procesų brandumo lygis, atrandamos stipriosios ir silpnosios organizacijos vietos. Čia ypač svarbu - galimybė naudoti COBIT, kuris yra universalus įrankis tiek informacinių technologijų strateginiam valdymui, tiek ir auditui.

Informacinių technologijų savianalizė ne tik padeda aukščiausios auditoriaus institucijoms atskleisti ir suvokti galimas informacinių technologijų valdymo spragas, bet palaipsniui jas užpildyti bei numatyti veiksmų eigą ateičiai. Rekomenduojama informacinių technologijų savianalizę atlikti reguliariai, o paskutinės savianalizės rezultatai galėtų tarnauti kaip priemonė aukštesniam informacinių technologijų valdymo brandos lygiui pasiekti. Kartojant tokius seminarus ir pati informacinių technologijų savianalizės metodika taptų efektyvesnė, nes auditoriaus institucijos atstovai įgytų daugiau patirties ją pritaikant. Informacinių technologijų savianalizė taip pat gali būti naudojama rengiant informacinių technologijų strategijas.

Darbas naudingas tiek mokslinėje tiek praktinėje prasme visiems besidomintiems ir dirbantiems informacinių technologijų valdymo srityje.

Darbe iš esmės remiamasi tarptautiniu geros praktikos rinkiniu COBIT ir EUROSAI Informacinių technologijų darbo grupės sukurta Informacinių technologijų savianalizės metodika ir jos taikymo metu gautais rezultatais. Taip pat atlikta įvairių su šio darbo tematiką susijusių literatūros šaltinių apžvalga ir analizė.

1. INFORMACINIŲ TECHNOLOGIJŲ STRATEGINIO VALDYMO SVARBA

Pirmame šio darbo skyriuje bus pristatoma informacinių technologijų (IT) strateginio valdymo samprata, atsižvelgiant į informacijos vertės augimą šiuolaikinėse organizacijose, IT panaudojimą informacijos kūrimui, apdorojimui ir saugojimui. Aptariama situacija, kas gali nutikti, kai IT diegiamos neracionaliai, prieš tai neįvertinus organizacijos poreikių. Trumpai primenamos informacijos saugumo problemos. Palietus šias problemas, palapsniui pereinama prie IT strateginio valdymo apibrėžimų. Pristatomas COBIT(angl. *Control Objectives for Information and related Technology*), kaip IT veiklos valdymo modelis.

Šiame darbe bus analizuojama IT savianalizės metodikos veiksnių eigą remiantis praktiniu metodikos taikymu Aukščiausiose audito institucijose (AAI), todėl pirmame skyriuje pateikiamas AAI apibrėžimas, trumpai pristatomos jų pagrindinės funkcijos ir kaip jas paveikė IT atsiradimas valstybiniame sektoriuje. Pirmojo skyriaus pabaigoje pabrėžiamas IT strateginio valdymo Aukščiausiose audito institucijose būtinybė, o IT savianalizės metodikos pritaikymas – kaip pagalbinė priemonė IT strateginiam valdymui puoselėti.

1.1 IT strateginio valdymo samprata

Vienas iš svarbiausių šiuolaikinės organizacijos išteklių yra informacija. Informacijos vientisumas ir patikimumas bei sistemos, kurios tą informaciją generuoja ir apdoroja yra lemiantys veiksniai sėkmingam organizacijos gyvavimui. Tačiau dažnai nepakanka įsigyti brangią ir pačią moderniausią kompiuterinę įrangą, įdiegti specializuotas taikomąsias programas ar visus organizacijos duomenų srautus apimančias informacines sistemas. Tokios investicijos gali nepasiteisinti, jei informacinė sistema neatitiks organizacijos poreikių arba nebus tinkamas dėmesys skiriamas vartotojų apmokymui. Tokiu atveju gali gerokai smukti darbo efektyvumas, pasitikėjimas ir noras naudotis informacinėmis technologijomis, išvaistomas laikas ir patiriami finansiniai nuostoliai, kurie gali būti ir bankroto priežastimi.

Kita problema yra susijusi su yra informacijos saugumo užtikrinimu. Informacijos sugadinimo, praradimo ar neteisėto pasinaudojimo rizika didėja, todėl organizacijos nebepajėgia savarankiškai nuo jų apsisaugoti. Dėl minėtos priežasties dažniausia ieškoma konsultantų pagalbos. Dažnai tikimasi, kad patyrę specialistai gali nustatyti iškilusių arba galimų incidentų priežastis, numatyti problemų sprendimų būdus, jas pašalinti ir patarti kaip išvengti informacijos praradimo ateityje. Kita vertus, panaikinti ir atstatyti tokios nelaimės sukeltus padarinius, organizacijoje, kurioje nėra sistemingai valdomos informacinės technologijos ir nėra parengtos saugumo politikos, dažnai kainuoja didžiulius

pinigus, prarandama daug laiko, o blogiausiu atveju – gresia bankrotas. Be to, visa atsakomybė dėl incidentų padarytos žalos tenka organizacijų vadovams, o ne konsultantams.

Taigi, esama IT valdymo samprata apima esamų problemų sprendimą, tačiau ne priežastis, sukeliančias tas problemas.

Išeitis, kaip apsisaugoti nuo problemų susijusių su IT investicijomis, informacijos saugumu, IT rizikų valdymu (koordinuoti veiksmai, kuriais siekiama valdyti ir kontroliuoti organizacijos rizikas¹), vartotojų adaptacija ir apmokymu, konkurencingumo didinimu ir įvaizdžio gerinimu ir t.t., išties yra. Efektyvi IT procesų valdymo ir kontrolės sistema išsprendžia ne tik vidines problemas, bet ir pagerina organizacijos įvaizdį.

Literatūroje galima atrasti įvairių IT strateginio valdymo (angl. *IT governance*) apibrėžimų. Viename iš jų teigiama, jog IT strateginis valdymas apima tai, kaip užtikrinti, kad organizacijos IT sistemos būtų suderinamos su verslo poreikiais². Trumpiau tariant, toks valdymas turi padėti organizacijai siekti užsibrėžtų tikslų.

Detalesnį apibrėžimą pateikia Informacinių sistemų audito ir valdymo asociacija (ISACA, angl. *Information Systems Audit and Control Association*): IT strateginis valdymas – tai procesų ir jų ryšių struktūra, įgalinanti siekti savo tikslų panaudojant IT pridėtinės vertės kūrimui, tuo pačiu subalansuojant su IT susijusios rizikos lygį su IT reikmėms skiriamu finansavimu³.

Wim Van Grembergen'as knygoje „Strategijos Informacinių technologijų valdymui“ (angl. *Strategies for Information Technology Governance*) teigia, kad IT strateginis valdymas susideda iš vadovybės ir organizacinių struktūrų, procesų ir su jais susijusių mechanizmų, kurie užtikrina, kad organizacijos IT sustiprintų ir praplėstų organizacijos strateginius siekius⁴.

IT strateginis valdymas yra procesas, kurio pagalba įmonės IT plėtra yra kryptinga ir kontroliuojama. Efektyvus IT strateginis valdymas užtikrina, kad IT tarnautų įmonės veiklos tikslams, maksimuotų investicijas į IT ir atitinkamai valdytų IT sukeltas rizikas. IT strateginis valdymas taip pat padeda užtikrinti rezultatyvų kritinių faktorių siekimą, priklausantį nuo informacinių ir su jomis susijusių technologijų. Vadinasi, tiek dabar, tiek ateityje turėtų būti skiriamas vis didesnis dėmesys IT strateginiam valdymui, nes IT nepaliaujamai skverbiasi į įmonių veiklos procesus. Priežastys, dėl kurių ir toliau turėtų augti IT strateginio valdymo svarba, yra šios:

- Priklausomybė nuo informacijos ir sistemų, kurios generuoja tą informaciją plėtra.

¹ Rizikos analizės vadovas. *Administracinių ir techninių gebėjimų stiprinimas užtikrinant duomenų informacinių technologijų ir jomis perduodamų duomenų apsaugą*. Lietuvos Respublikos Vidaus Reikalų Ministerija.-Vilnius: Vaga.-2005. – 161 p. ISBN 54150118271. P. 12.

² *Board Briefing on IT Governanc* [interaktyvus]. 2nd ed. USA: IT Governance Institute, 2004, [žiūrėta 2007 m. kovo 23 d.]. Prieiga per internetą: <http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf>.

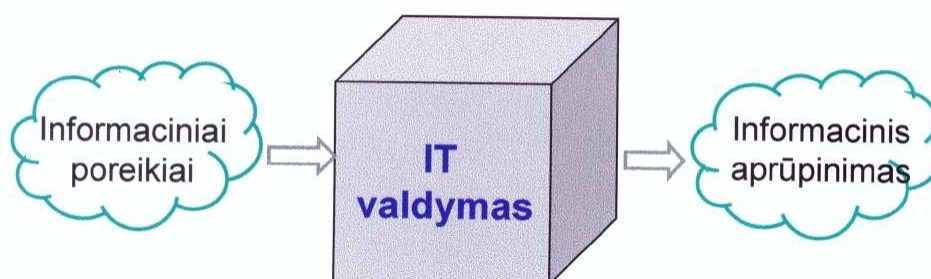
³ VAGERIS, Robertas, *ISACA pristatymas*, Vilnius, 2004.

⁴ GREMBERGEN, Wim Van, *Strategies for Information Technology Governance*, USA: Idea Group Publishing, 2004. 406 p. ISBN:1591402840. P. 2.

- Pažeidžiamumą ir plataus grėsmių spektro augimas.
- Investicijų į informaciją ir informacines technologijas didėjimas.
- Technologijos vis dar keičia organizacijas ir darbinių santykių praktiką, sukurdamos naujas galimybes ir mažindamos kaštus.

Tol kol šie faktoriai egzistuos, tol bus reikalingas efektyvus, produktyvus ir ekonomiškąs IT strateginis valdymas.

Netinkamas IT veiklos supratimas ar valdymas tenkina informacijos poreikius pagal „juodos dėžės“ principą (1 schema). Tai reiškia, kad vartotojai daugiau ar mažiau žino, kokios informacijos jiems reikia, bet kelias iki kol jie ją gauna būna visiškai neapibrėžtas. Savaime suprantama, kad pasiekti užsibrėžtą tikslą neturint plano yra žymiai sudėtingiau, nei žinant tikslas koordinatas. O tai reiškia, kad bus išsekvojama žymiai daugiau resursų ir sugaištama laiko.



1 schema. Netinkamas IT veiklos valdymo supratimas – „juodos dėžės principas“⁵.

Vienas iš *de facto* daugelyje pasaulio valstybių, finansinių, konsultacinių ir kitų organizacijų taikomų ir pasiteisinusių IT strateginio valdymo metodikų yra COBIT. COBIT IT strateginio veiklos valdymo modelis pavaizduotas 2 schemeje.



2 schema. COBIT IT veiklos valdymo modelis⁶.

⁵ VAGERIS, Robertas, *ISACA pristatymas*, Vilnius, 2004.

⁶ IT Governance Institute, *COBIT 4.0*. 4th ed. USA: ITGI, 2005. 194 p. ISBN 1-933284-37-4. P. 11.

Plačiau apie COBIT geros praktikos rinkinį bus supažindinama antrame šio darbo skyriuje.

1.2 Vidaus kontrolės poreikis IT strateginiame valdyme

Norint užtikrinti sėkmingą organizacijos veiklą, kuri siekia įgyvendinti užsibrėžtus tikslus, turi būti identifikuoti ir apibrėžti veiklos procesai. O kad užtikrintumėme nepriekaištingą procesų darbą, turi būti nustatytos, dokumentuotos ir paskelbtos kontrolės procedūros ir sukurta kontrolės aplinka. Kontrolės aplinka reiškia vadovybės požiūrį, supratimą ir veiksmus susijusius su vidaus kontrolės sistema ir jos svarba įstaigoje. Kontrolės procedūros apima įmonės politikas, nuostatus ir tvarkas, kurias vadovybė sukuria tam, kad siektume įmonės tikslų⁷. Visa tai kartu paėmus vadinama vidaus kontrolės sistema.

Yra keletas priežasčių, dėl kurių turi būti vidaus kontrolės sistema:

1. *Veiklos procesų pasikeitimas.* Informacinių ir su jomis susijusių technologijų vystymasis praėjusių 40 metų laikotarpyje padarė didžiulę įtaką vadovams, auditoriams, vyriausybės atstovams, teisininkams, vartotojams ir techniniam personalui. Dėl to atsirado poreikis atkreipti dėmesį į informacinių technologijų saugumą ir kitas kontroles IT valdymo srityje.

2. *Pasikeitimai įtakoti IT atsiradimo.* Organizacijos, ypač aptarnavimo sektorius, vis labiau priklauso nuo IT. Pirmiausiai IT buvo naudojamos tik sudėtingoms operacijoms atlikti. Vėliau jos buvo pradėtos naudoti kaip pagalbinė priemonė įvairiai įrangai valdyti. Tik tada, kaip kompiuterinė technika fiziškai tapo mažesnė ir kaina gerokai sumažėjo IT pradėta naudoti ir kaip pagalbinė priemonė versle ir valstybiniame sektoriuje. Šiandien IT yra integruotas į veiklos procesus ir dėl to IT veikla yra neatsiejama nuo veiklos procesų. Be to organizacijos kuria naujus IT produktus ir paslaugas, o technokratai prognozuoja, kad visos organizacijos gyvuos tik kibernetinėje erdvėje.

3. *Investavimas į kontrolę.* Užtikrinant sėkmingą organizacijos gyvavimą, suprantant ir valdant rizikas, susijusias su naujų technologijų diegimu, ir numatant efektyvų valdymą ir adekvačias kontrolės priemones, turi būti vadovybės pripažinimas ir IT rizikų bei kontrolių supratimo pagrindas. Vadovybė turi nuspręsti, kiek investuoti į saugumą ir IT kontrolę, kaip subalansuoti riziką ir valdyti investicijas dažnai nenuspėjamoje IT aplinkoje.

4. *Konkurencija.* Čia aptariama globali konkurencija. Daugelis įmonių restruktūrizavosi, kad supaprastinti operacijas ir įsisavinti IT teikiamus privalumus ir taip užimti geresnę konkurenciniu atžvilgiu poziciją. Veiklos reorganizavimas, tikslų užsibrėžimas, paslaugų nuoma (angl. *outsourcing*), pareigų paskirstymas, organizacijos suvienodinimas ir procesų paskirstymas tai yra pokyčiai, kuriais

⁷ ACCA *Lynchpin for International Stresam: Audit framework.* United Kingdom: AT Foulks Lynch LTD, 2000. 125 p. P. 44.

gali manipuliuoti įmonės vadovybė. Tokie pokyčiai turi ir ateityje turės didelę įtaką įmonės veiklos valdymui ir kontrolės priemonių eksploatacijai.

Konkurencinio pranašumo siekimo akcentavimas paveikia pastoviai didėjantį pasitikėjimą informacinėmis technologijomis, kaip vieną iš pagrindinių daugumos organizacijų strateginių elementų. Tokiose greitų struktūros pasikeitimų rėmuose, vadovų, IT specialistų ir auditorių įgūdžiai turi vystytis taip pat greitai kaip ir IT naujovės, tam kad jie sugebėtų efektyviai atlikti savo pareigas. Viena dalykas yra įdiegti ir įgyvendinti įprastų procesų kontrolę, bet žymiai daugiau žinių ir patirties reikia diegiant kontrolės sistemą, organizacijoje, kurioje naudojama IT.

5. *Veiklos pobūdis.* Bankų administracinė struktūra yra sukurta remiantis decentralizuotu modeliu ir tokia struktūra yra priimtina ir kitos sferos organizacijų ofisams. Administratoriai atsakingi už pagrindinių ir šalutinių veiklos tikslų įgyvendinimą, taip pat atsako ir už vidaus kontrolės sistemos sukūrimą, palaikymą ir stebėjimą. Visa tai padeda sėkmingai ir efektyviai siekti užsibrėžtų tikslų.

Kitaip tariant, gera vidaus kontrolės sistema užtikrina patikimas finansines ataskaitas, kuriomis gali remtis vadovybė, priiminėdama sprendimus dėl veiklos sąlygų, organizacijos turto apsaugos, įskaitant žmoniškuosius išteklius, taip pat atlikti sulyginimus su įstaigos parengta politika, vidinėmis ir statutinėmis taisyklėmis, nuostatais ir procedūromis.

Blogomis vidaus kontrolės pasekmėmis gali būti: biurokratijos padidėjimas, produktyvumo sumažėjimas, painiavos padidėjimas, transakcijų įgyvendinimo laiko pailgėjimas atliekant nereikšmingus darbus. Be to, prasta vidaus kontrolės sistema susiduria su organizacijos tikslų įgyvendinimu, pasireiškiančiu neteisingu arba piktavališku resursų panaudojimu, todėl juridinis asmuo gali įgauti visuomenės nepasitikėjimą⁸. Pavyzdžiui, tokia situacija buvo susiklosčiusi Jungtinėse Amerikos Valstijose (JAV), kur kilo keletas skandalų atsiradus vartotojų nepasitikėjimui kai kuriomis stambiomis organizacijomis. Viena iš tokių organizacijų buvo *Enron koncernas*⁹, kuris 2001 m. bankrutavo dėl darbuotojų ir šio koncerno bendrininkų (vienas iš jų *Arthur Andersen*¹⁰) atliktų ekonominių nusikaltimų, sukčiavimo, balansų padirbinėjimo bei netinkamos koncerno veiklos priežiūros.

Po tokių skandalų 2002 m. JAV buvo priimtas *Sarbanes-Oxley* aktas¹¹. Tai aktas, kuris apibrėžia korporacinio valdymo taisykles, jų laikymąsi ir atskaitingumą. *Sarbanes-Oxley* aktas reikalauja, kad organizacijos valdymas būtų:

⁸ BAKSHI, Sunil, Control Self-assessment for Information and related technology. *Information Systems Control Journal*, 2004, vol. 1, p. 10-18.

⁹ *Enron* [interaktyvus]. USA: Wikimedia Foundation Inc., 2002– [žiūrėta 2007-04-20]. Prieiga per internetą: <<http://en.wikipedia.org/wiki/Enron>>.

¹⁰ *Arthur Andersen* [interaktyvus]. USA: Wikimedia Foundation Inc., 2002– [žiūrėta 2007-04-20]. Prieiga per internetą: <http://en.wikipedia.org/wiki/Arthur_Andersen>.

¹¹ *Summary of the Provisions of the Sarbanes-Oxley Act of 2002* [interaktyvus]. USA: AICPA, 2004-2006– [žiūrėta 2007-04-20]. Prieiga per internetą: <<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>>.

- Pagrįstas žinojimu apie materialiąją informaciją, kuri būtų pateikiama vadovybės ir prieinama investuotojams.
- Laikymasis atsakomybės už tos informacijos teisingumą, nuodugnumą ir tikslumą¹².

Tačiau esminis *Sarbanes-Oxley* akto principas yra įmonės vadovybės atsakomybės įteisinimas už įmonės finansinių ataskaitų patikimumą.

Kuriant kontrolės susijusias su IT procesais sistemą taipogi gali pasitarnauti COBIT geros praktikos gairės. Atsižvelgdami į COBIT detaliuosius valdymo tikslus (angl. *control objectives*), vadovai gali užsitikrinti, kad yra vystoma adekvati IT aplinkos kontrolės sistema. Taip jie gali susikonsultuoti į aukštesnės rizikos sritis ir nustatyti efektyvius būdus, kaip sumažinti tą riziką.

1.3 IT įtaka valstybiniame sektoriuje ir valstybinio audito procesuose

Organizacijos jau nebegali išsiversti be kompiuterizuotų darbo vietų, duomenų bazių su moderniomis dokumentų valdymo sistemomis, kompiuterinės apskaitos, interneto ir t.t. Valstybinės įstaigos nėra išimtis. Pvz. Lietuvos valstybiniame sektoriuje, daugelyje įstaigų, jau beveik dešimt metų, kai pereinama nuo įprasto rankinio darbo ir dokumentų tvarkymo prie kompiuterizuotų informacinių sistemų. Didžiosios dalies popierinės dokumentacijos dar neatsisakyta, bet jau daugelyje Lietuvos valstybinių institucijų yra aprūpintos kompiuterine technika ir programine įranga. Kuriamos, o kai kur jau ir įdiegtos informacijos valdymo sistemos.

Situacija kitų Europos šalių valstybinėse institucijose yra nevienoda. Europos šalys senbuvėse (Didžiojoje Britanijoje, Nyderlanduose, Vokietijoje, Šveicarijoje, Norvegijoje ir kt.), kuriose ekonominė situacija yra geresnė, labiau pažengęs ir kompiuterizacijos lygis, o tuo pačiu žymiai didesnis dėmesys skiriamas IT strateginiam valdymui. Bet, pavyzdžiui, daugelyje posovietinių valstybių (Lietuva, Latvija, Ukraina ir kt.) IT lygis dar nėra aukštas, tačiau intensyviai vyksta IT kūrimo ir diegimo procesai.

IT įtaka valstybinio audito procesuose

Praktiškai visose valstybėse yra institucijos, kurios atlieka valstybinių įstaigų valstybinį auditą. Tokios institucijos vadinamos Aukščiausiomis audito institucijomis.

INTOSAI (angl. *International Organization of Supreme Audit Institutions*) pateikia tokį AAI apibrėžimą: „Aukščiausia audito institucija yra toks viešasis šalies organas arba keletą valstybių apimanti organizacija, kuri, kaip bebūtų aprašyta, įteisinta ar organizuota, atlieka pagal įstatymus ar

¹² BAKSHI, Sunil, Control Self-assessment for Information and related technology. *Information Systems Control Journal*, 2004, vol. 1, p. 10-18.

kitus šalies ar tarpvalstybinius teisės aktus pagrindinę šalies ar keletą valstybių apimančią valstybinio audito funkciją nepriklausomais metodais su arba be jurisdikcine kompetencija¹³.

Valstybinis auditas susideda iš finansinio (teisėtumo) ir veiklos auditų. Finansinis (teisėtumo) auditas – audituojamo subjekto finansinės atskaitomybės ir (ar) kitų ataskaitų duomenų, taip pat valstybės lėšų ir turto valdymo, naudojimo, disponavimo jais teisėtumo ir jų naudojimo įstatymų nustatytiems tikslams vertinimas bei nepriklausomos nuomonės pareiškimas. Veiklos auditas – audituojamo subjekto viešojo ir vidaus administravimo veiklos įvertinimas ekonomiškumo, efektyvumo ir rezultatyvumo požiūriu¹⁴. Juos atlieka Valstybės kontrolės pareigūnai.

Audito svarba ir būtinumas buvo suprasti jau senovėje, kai pirmąsyk buvo atskirtos tokių pagrindinių tų laikų ūkininkavimo subjektų kaip valstybė ir vergvaldinis dvaras turto nuosavybės ir valdymo funkcijos. Šiuolaikinio audito pradžia laikomi 1845 m., kada Didžiojoje Britanijoje buvo priimti keli įstatymai, numatantys, kad akcinės bendrovės privalo pavesti nepriklausomiems buhalteriams patikrinti tų bendrovių buhalterines knygas ir sąskaitas, o tikrinimo rezultatus pateikti akcininkams. Ilgainiui audito turinys gilėjo ir plėtėsi, audito procesas tapo daug sudėtingesnis.

Profesorius V. Lakis yra pasakęs, kad auditas yra reikalingas visais organizuotos veiklos lygiais, pradedant visos valstybės ekonomine veikla ir baigiant įmonių veikla. Jo svarba tiek viešajame, tiek privačiame versle nuolat auga, nes tai susiję su visuomenės siekimu gauti nešališką, patikimą informaciją apie dominančią organizaciją¹⁵.

Tarptautinių žodžių žodyne yra pateikiamas toks audito apibrėžimas: auditas (lot. *audio* – *girdžiu*) – oficialus firmos finansinės ir ūkinės veiklos patikrinimas¹⁶. Tačiau nuo jo atsiradimo ir per visą jo formavimosi istoriją ši sąvoka nebuvo interpretuojama vienareikšmiškai. Tai rodo ir analizuota literatūra (žr. 1 lentelę):

1 lentelė. Lietuvos ir užsienio specialioje literatūroje pateikiami audito apibrėžimai ir jų palyginimas.

Audito apibrėžimas	Pagrindiniai aspektai
Auditas – tai sisteminis įrodymų, patvirtinančių ekonominius veiksmus ir įvykius, objektyvaus gavimo ir įvertinimo procesas siekiant nustatyti patvirtinimų ir nustatytų kriterijų atitikimo laipsnį bei gautų rezultatų pateikimas suinteresuotiems asmenims ¹⁷ .	Sisteminis procesas; Ekonominiai veiksmai ir įvykiai; Rezultatų pateikimas suinteresuotiems asmenims.

¹³ INTOSAI (International Organization of Supreme Audit Institutions), *Statutes* [interaktyvus]. JAV: INTOSAI, 2004–[žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.intosai.org/blueline/upload/12estatut.pdf>>.

¹⁴ Lietuvos Respublikos valstybės kontrolės įstatymas. *Valstybės Žinios*. Vilnius: Lietuvos Respublikos Seimo leidykla, 2001-12-13, Nr. 112-4070.

¹⁵ LAKIS, V. Audito raida Lietuvoje ir sistemos kūrimo problemos. *Ekonomika*. 2002, Nr.58. P.106.

¹⁶ VAITKEVIČIŪTĖ, V. *Tarptautinių žodžių žodynas*. Vilnius: Žodynas, 2001. 1039 p. P.115.

¹⁷ Committee on Basic Auditing Concepts. *A Statement of Basic Auditing Concepts*. Sarasota: American Accounting Association, 1973. P.2.

Audito apibrėžimas	Pagrindiniai aspektai
Auditas – tai procesas, kurio metu kompetentingi ir nepriklausomi asmenys renka įrodymus tam, kad įvertinti informaciją apie ūkio subjekto ūkinę ar kitą ekonominę veiklą ir tuo pagrindu pareikšti nuomonę apie šios informacijos teisingumą ir atitikimą nustatytiems standartams ¹⁸	Nepriklausomas įrodymų rinkimas ir vertinimas; Ūkinė ir kita ekonominė veikla; Nuomonės pateikimas.
Auditas – tai oficiali nepriklausoma kliento informacijos apie finansinę atskaitomybę ar kitą ekonominę veiklą realumo ir patikimumo analizė ir įvertinimas lyginant su bendraisiais apskaitos principais, standartais ir kitais norminiais dokumentais bei auditoriaus raštiškos nuomonės apie tai pateikimas ¹⁹ .	Nepriklausoma informacijos analizė; Finansinė atskaitomybė ar kita ekonominė veikla; Nuomonės pateikimas.
Auditas – nepriklausomas finansinių ataskaitų ir informacijos patikrinimas tam, kad gauti išvadas apie ūkinio subjekto finansinę padėtį. Auditas – tai procesas, kurio metu ataskaitų vartotojams informacinė rizika sumažinama iki priimtino laipsnio (rizikos) ²⁰ .	Nepriklausomas patikrinimas; Finansinės ataskaitos ir kita informacija; Išvadų gavimas; Informacinės rizikos vartotojams sumažinimas.
Auditas - tai įmonės finansinės atskaitomybės ir su ja susijusios finansinės informacijos rinkimas, kaupimas, tyrimas, analizė ir vertinimas, kurį kompetentingai vykdo nepriklausomas auditorius (ar auditorių įmonė), ir kuris, remdamasis atitinkamais kriterijais, daro išvadą arba pareiškia savo nuomonę apie tiriamojo objekto funkcionavimo būklę ir finansinės atskaitomybės kokybę ²¹ .	Nepriklausomas vertinimas Finansinės ataskaitos ir veikla; Nuomonės pateikimas.

Lietuvoje AAI funkcijas atlieka Lietuvos Respublikos valstybės kontrolė. Valstybės kontrolė yra Seimui atskaitinga aukščiausioji valstybinio audito institucija, kuri atlieka valstybinį auditą. Valstybės kontrolės misija yra padėti valstybei išmintingai valdyti ir naudoti turtą, lėšas ir kitus išteklius, prisidedant prie Seimo vykdomos parlamentinės kontrolės, skatinant viešojo sektoriaus pažangą ir prižiūrėti ar teisėtai valdomas ir naudojamas valstybės turtas ir kaip vykdomas valstybės biudžetas²². Pagrindiniai Valstybės kontrolės uždaviniai:

- prižiūrėti, ar teisėtai ir efektyviai valdomas ir naudojamas valstybės turtas ir kaip vykdomas valstybės biudžetas;

¹⁸ СКОБАРА, В. В. *Аудит: методология и организация*. Москва: Дело и Сервис, 1998. С.3.

¹⁹ МАТІСКИЕНĖ, I. *Audito planavimas ir organizavimas*. Kaunas: Technologija, 1997. 140 p. P. 15.

²⁰ ШОХИН, С.О., ВОРОНИНА, Л. И. *Бюджетно-финансовый контроль и аудит: Теория и практика применения в России*. Москва: Финансы и статистика, 1997. С. 18.

²¹ КАТКУС, А. *Valstybinė ekonominė kontrolė*. Vilnius: Mintis, 1997. 301 p. P.202.

²² *Misija ir strateginis tikslas*. [Interaktyvus]. Vilnius: Lietuvos Respublikos valstybės kontrolė– [žiūrėta 2007 m. kovo 26 d.]. Prieiga per internetą: <http://www.vkontrole.lt/apie_misija.shtml>.

- skatinti teigiamą ir veiksmingą valstybinio audito poveikį valstybės finansų valdymo ir kontrolės sistemai bei į rezultatus ir visuomenės poreikius orientuotam viešajam valdymui²³.

Audito procesai dažniausiai išskiriami į šešis pagrindinius etapus:

1. Pasirengimas auditui: strategija;
2. Susipažinimas su audituojamos įmonės veikla;
3. audito planų ir programų sudarymas;
4. audito medžiagos rinkimas; tikrinimas;
5. auditoriaus ataskaitos ir išvados parengimas;
6. atlikto audito kontrolė.

Pradėjus diegti kompiuterines technologijas ir sistemas valstybiniame sektoriuje iškilo klausimas, kaip tai įtakos Aukščiausiųjų audito institucijų veiklą ir kaip pasikeis audito pobūdis taikant naujas technologijas. AAI, kaip ir kitose institucijose, ne išimtis, kad, įrengus kompiuterizuotas auditorių darbo vietas, atsirado elektroninė dokumentacija ir elektroninės informacijos srautai. Šie pokyčiai paveikė praktiškai visus audito proceso etapus. Pavyzdžiui, vienas iš svarbiausių audito procesų yra audito ataskaitos ir išvados parengimas, o kad išvados turi būti grindžiamos audito įrodymais (Audito įrodymai – tai audito metu parengta ar gauta informacija, reikalinga patvirtinti arba paneigti tam tikras išvadas. Tai gali būti konkretūs dokumentai, apskaičiavimai ir įrašai, taip pat kita informacija, kuria remiantis sudarytos finansinės ataskaitos²⁴). Išsamiau gilinantis į šį pavyzdį toliau aprašoma, kaip informacinės technologijos įtakoja audito įrodymų surinkimą ir jų vertinimą.

Įrodymų rinkimo pasikeitimai. Surinkdami kompiuterinės sistemos patikimumo įrodymus, auditoriai susiduria su duomenimis saugomais ir apdorojamais kompiuterinėmis informacijos sistemomis. Daugeliu aspektu tai yra žymiai patogiau, nei rinkti įrodymus popierinėje dokumentacijoje. Galima pasidaryti duomenų kopijas ir jas išsisaugoti mobiliose informacijos laikmenose, elektroniniame formate, o vėliau jas apdoroti naudojant įvairias taikomas programas pradant nuo Microsoft Office paketo programų²⁵ *Word*, *Excel* ar *Access* ir baigiant specializuotomis audito programoms, tokiomis, kaip *IDEA*²⁶ ir *ACL*²⁷. Tai yra gerai auditoriams žinomos, išbandytos ir pasiteisinusios taikomosios programos, kurios naudojamos duomenų analizei, duomenų bandinių

²³ Lietuvos Respublikos valstybės kontrolės įstatymas. *Valstybės Žinios*. Vilnius: Lietuvos Respublikos Seimo leidykla, 2001-12-13, Nr. 112-4070.

²⁴ MACKEVIČIUS, J. *Auditas: teorija, praktika, perspektyvos*. Vilnius: Lietuvos mokslas, 2001. 837 p. ISBN 9986-795-05-3. P. 228.

²⁵ *Sistemos „Microsoft Office“ produkto informacija* [interaktyvus]. United State: Microsoft Corporation, 2007– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://office.microsoft.com/lt-lt/default.aspx>>.

²⁶ *IDEA – Data Analysis Software* [interaktyvus]. Canada: CaseWare IDEA Inc., 2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.caseware-idea.com/fsh.asp>>.

²⁷ *ACL – Data You Can Trust. Results You Can See* [interaktyvus]. Canada: ACL Services Ltd., 2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.acl.com>>.

nagrinėjimui ir statistikai. *PricewaterhouseCoopers* sukurtą *TeamMate*²⁸ sistema, naudojama auditoriaus darbo proceso dokumentavimui, sisteminimui ir valdymui.

Audito įrodymus dažnai tenka rinkti iš popierinių dokumentų, tačiau juos apdorojant galima pasitelkti informacines technologijas. Dokumentus galima nuskanuoti, o duomenis atpažinti pritaikius teksto atpažinimo programinę įrangą. Pavyzdžiui, Lietuvoje Respublikos valstybės kontrolėje naudojama *ABBYY* sukurtą teksto atpažinimo programinę įrangą *Fine Reader*²⁹. Taip išgautus elektroninius duomenis toliau galima analizuoti anksčiau išvardintomis programomis.

Įrodymų vertinimo pasikeitimai. Nagrinėjant tiek paprastas, tiek ir sudėtingas kompiuterines sistemas ir su jomis susijusias vidaus kontrolės procedūras, yra dar sunkiau nustatyti kontrolės stiprių ir silpnų pusių poveikį bendram sistemos patikimumui, nei atliekant įprastinį auditą. Pirmiausia auditoriai turi suprasti, kada kontrolė yra patikima, o kada ji veikia blogai. Toliau auditoriai turi sekti stiprios ir silpnos vidaus kontrolės poveikį informacinėje sistemoje.

Klaidų padarinys kompiuterinėje sistemoje yra rimtesnis nei fizinėje. Fizinėje sistemoje klaidos atsiranda atsitiktinai, pavyzdžiui, pardavėjas gali vieną kartą parduoti prekę už neteisingą kainą, bet vėliau tokia klaida gali ir nepasikartoti. Kompiuterinėje sistemoje klaidos gali būti pastovios (sisteminės), pvz., jeigu neteisinga programa, tai ji visada bus įvykdyta su klaida. Be to, sisteminės klaidos generuojamos didele sparta, todėl jų ištaisymo ir programos patobulinimo kaina gali būti labai didelė. Blogiausiu atveju tai gali pareikalauti iš naujo suprojektuoti ir suprogramuoti sistemą. Todėl vidaus kontrolė, kuri užtikrina sistemos aukštos kokybės projektavimą, diegimą, veikimą ir priežiūrą, yra kritinė. Auditoriaus pareiga – užtikrinti, jog tokia kontrolė yra pakankama turtui, duomenų vientisumui, sistemos tinkamumui ir efektyvumui apsaugoti, be to, kad vidaus kontrolė veikia patikimai.

Išvardinti įrodymų vertinimo pasikeitimai įtakoja IS audito atsiradimą. IS auditorius turi ne tik puikiai išmanyti auditą, bet ir turėti pakankamai žinių apie informacines technologijas ir jų valdymą. Vadinasi IS auditoriams turi būti sudarytos tinkamos sąlygos pastoviai tobulėti ir gauti reikiamas konsultacijas iš specialistų, todėl, pavyzdžiui, Lietuvos Respublikos valstybės kontrolėje IS audito funkcija struktūriškai apjungta kartu su IT valdymo funkcija ir sudaro vieną Informacinių technologijų valdymo ir audito departamentą.

²⁸ *What is TeamMate?* [interaktyvus]. New York: PricewaterhouseCoopers, 2006-2007– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.pwc.com/Extweb/service.nsf/docid/443881F8A1DA32D0852568B6001A514E>>.

²⁹ *ABBYY Product Overview* [interaktyvus]. Moscow: ABBYY Software, 1996-2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.abbyy.com/products/>>.

1.4 IT strateginio valdymo svarba Aukščiausiose audito institucijose

Ankstesniame poskyryje „IT įtaka valstybinio audito procesuose“ buvo pateikta pakankamai faktų, kad galima būtų padaryti išvadas, jog IT išties įtakoja audito procesus. Maža to, IT tampa arba turi tapti integralia AAI veiklos dalimi, leidžiančia siekti AAI numatytų tikslų. Tuo pačiu AAI turi sugebėti operatyviai prisitaikyti prie IT naujovių, kurios dar labiau automatizuotų auditorių vykdomą veiklą. Sudėlioti prioritetus tenkinant AAI vartotojų poreikius susijusius su IT. Kita vertus AAI atliekamos funkcijos įpareigoja palaikyti gerą įvaizdį ir teikti pasitikėjimą audituojamiems subjektams ir kitoms įstaigoms. Todėl AAI IT strateginis valdymas yra labai svarbus ir turi būti vykdomas.

Pavyzdžiui, Lietuvos Respublikos valstybės kontrolėje remiasi nuostata, kad informacinių technologijų valdymas yra svarbi veiklos sritis, leidžianti nustatyti racionalų veiklos procesų poreikių ir informacinių technologijų teikiamų galimybių santykį. Vienas iš pagrindinių požymių, rodančių tą supratimą, yra nuo 2002 m. kas penkis metus rengiamas ir valstybės kontrolieriaus įsakymu patvirtinamas Valstybės kontrolės informacinių technologijų strateginis plėtros planas.

1.5 Skyriaus apibendrinimas

IT strateginis valdymas yra procesas, kurio pagalba įmonės IT plėtra yra kryptinga ir kontroliuojama. Efektyvus IT strateginis valdymas užtikrina, kad IT tarnautų įmonės veiklos tikslams, maksimizuotų investicijas į IT ir atitinkamai valdytų IT sukeltas rizikas. Tiek dabar, tiek ateityje turėtų būti skiriamas vis didesnis dėmesys IT strateginiam valdymui.

Esminis procesų valdymo dalykas yra aprašyti procedūras arba kitaip vadinamas vidaus kontrolės procedūras. Paragrafe „Vidaus kontrolės poreikis IT strateginiame valdyme“ pateikti vidaus kontrolės aplinkos, procedūrų ir sistemos apibrėžimai. Išvardinamos pagrindinės priežastys, dėl kurių organizacijos, kuriose daugiau ar mažiau veikia IT procesai, reikalinga kontrolės sistema.

Pristatytas COBIT, kaip IT veiklos valdymo modelis.

IT tampa arba turi tapti integralia AAI veiklos dalimi, leidžiančia siekti AAI numatytų tikslų. Tuo pačiu AAI turi sugebėti operatyviai prisitaikyti prie IT naujovių, kurios dar labiau automatizuotų auditorių vykdomą veiklą. Sudėlioti prioritetus tenkinant AAI vartotojų poreikius susijusius su IT. Kita vertus AAI atliekamos funkcijos įpareigoja palaikyti gerą įvaizdį ir teikti pasitikėjimą audituojamiems subjektams ir kitoms įstaigoms. Todėl AAI IT strateginis valdymas yra labai svarbus ir turi būti vykdomas.

2. COBIT SAMPRATA

Sėkmingai gyvuojančios organizacijos puikiai supranta informacinių technologijų naudą ir ją pritaiko savo veikloje. Jos atranda kritiškiausias sąsajas tarp veiklos procesų ir informacinių technologijų bei įvertina būtinybę kuo efektyviau valdyti riziką. Į pagalbą tokioms organizacijoms kovojant su verslo iššūkiais suskubo IT valdymo institutas išleisdamas COBIT. COBIT yra IT strateginio valdymo gairės ir palaikantis praktinių įrankių rinkinys, kuris suteikia vadovams galimybę užpildyti spragas atsižvelgiant į kontrolės sistemos reikalavimus, technines galimybes ir veiklos rizikas. COBIT organizacijose įgalina aiškių IT politikų kūrimą ir gerą IT kontrolės praktiką.

Kita vertus, COBIT taip pat gali būti sėkmingai naudojamas Informacinių technologijų savianalizei atlikti. Per pagrindinius 34 procesus ir 318 detaliųjų valdymo tikslų COBIT susieja informacinių technologijų valdymą ir informacinių technologijų savianalizę, todėl informacinių technologijų valdymo uždavinys gali būti sprendžiamas informacinių technologijų savianalizės pagrindu. Kadangi IT savianalizės metodika yra sukurta, kaip pagrindą naudojant COBIT, todėl ją taikant, darbo grupės nariai privalo išmanyti COBIT pagrindus.

Šiame skyriuje bus supažindinama su pagrindiniais COBIT raidos etapais, bei jo struktūra. Apžvelgiama ketvirtoji COBIT versija įvardinant pagrindinius pasikeitimus ir atliekant palyginimą su trečiąja versija. Paskutiniajame poskyryje bus pristatomos keturi savianalizės metodai, kuriuose daugiau ar mažiau remiamasi COBIT geros praktikos rinkiniu.

2.1 COBIT istorija

COBIT yra visame pasaulyje žinomas ISACA geros praktikos rinkinys. COBIT aprašo geriausią praktiką informacinių sistemų strateginio valdymo srityje. COBIT koncepcija buvo suformuluota pirmame leidime, kuris pasirodė 1994 metais. Nuo tada remiantis tarptautiniais standartais ir įsisavinant pirminę patirtį, buvo sukurti kontrolės tikslai (angl. *control objectives*). O vėliau buvo sukurtos ir audito gairės, kurios padeda nustatyti kokiam lygyje yra įgyvendinti kontrolės tikslai.

Vėliau susikūrusios europiečių, amerikiečių ir australų darbo grupės, besiruošdamos antrosios COBIT versijos išleidimui, atlikinėjo tyrimus į kuriuos įtraukė iš tarptautinių šaltinių atrinktos informacijos rinkinius ir analizę. Darbo grupės atliko analizę ir įvertinimą ir apjungė viską į vientisą, vieną iš geriausių, tarptautinį geros praktikos rinkinį, kuris susideda iš geros praktikos sąvadų, kokybės

valdymo standartų, profesionalių audito veiklos standartų, o taip pat iš praktinių uždavinių ir patirties. Trumpiau tariant, iš viso to kas visiškai ar iš dalies susiję su valdymo koncepcija³⁰.

Pritaikant praktiškai pirmąsias COBIT versijas buvo atidžiai analizuojami IT procesai ir jų sąsaja su veiklos procesais. Buvo nustatinėjamas jų įgyvendinimo eiliškumas, įvertinama jų svarba. Atliekant įvairiapusiškas analizes specialistai pasiūlė naujus arba patobulintus kontrolės tikslus, atitinkančius būtent konkretų IT procesą. Už rezultatų apibendrinimą buvo atsakingas Koordinuojantis COBIT komitetas.

Trečiojo COBIT leidimo projektas prasidėjo nuo vadybos gairių (angl. *Management guidelines*) kūrimo ir antrosios versijos tobulinimo atsižvelgiant į naujoves tarptautiniuose informacijos šaltiniuose. Be viso to buvo peržiūrėta ir išplėsta visa COBIT koncepcija su tikslu dar labiau sustiprinti administracinę kontrolę, apibrėžti visos veiklos valdymą ir toliau plėtoti IT strateginį valdymą. Atlikus šiuos žingsnius 2002 metais pasauli išvydo trečioji COBIT versija. COBIT trečiąją versiją sudaro septynios dokumentų grupės:

- Principai (angl. *Framework*)
- Santrumpa vadovui (angl. *Executive summary*)
- Vadybos gairės (angl. *Management guidelines*)
- Kontroliniai uždaviniai (angl. *Control Objectives*)
- Audito gairės (angl. *Audit guide*)
- Diegimo gairės (angl. *Implementation tool set*)
- Praktikų aprašymai (angl. *IT Control practice statement*)³¹

Ketvirtoji COBIT versija, kuri pasirodė 2005 metais. Ji detaliau aprašoma sekančiame paragrafe.

Ketvirtosios COBIT versijos apžvalga

COBIT kūrėjai nesustojo ties trečiąją versija, priešingai – toliau intensyviai atliko įvairius tyrimus ir analizes. Kaupė įvairių organizacijų patirtį ir atsiliepimus apie COBIT pritaikymą, atliko įvairius palyginimus su įvairiais tarptautiniais standartais norėdami dar labiau išvystyti COBIT. Tuo tikslu netgi buvo sudaromos „savanorių“ grupės į kurių sudėtį įėjo ISACA nariai, ekspertai iš mokslininkų tarpo ir kas be ko – COBIT naudotojai.

Regioninės darbo grupės po 6-10 specialistų susibūrusios Briuselyje (Belgija), Londone (Didžioji Britanija), Čikagoje ir Vašingtone (Jungtinės Amerikos valstijos), Kanberoje (Australija),

³⁰ ХРАМЦОВСКОЙ, Н.А. *Выходит новая версия стандарта CobiT* [interaktyvus]. Москва: Электронные Офисные Системы, 2005– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.eos.ru/eos/163336>>.

³¹ *Kas yra CobIT?*[interaktyvus]. Lietuva: Asociacija ISACA Lietuva, 2003– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.isaca.lt/lt/cobit/>>.

Keiptaune (Pietų Afrika) ir Kopenhagoje (Danija) susirinkdavo 2-3 kartus per metus ir kartu sprendavo Koordinuojančio COBIT komiteto užsibrėžtus uždavinius. Be to, tokios verslo mokyklos, kaip Danijoje esančio Antverpeno universiteto verslo mokyklos³² (angl. *University of Antwerp Management School*) ir Havajų universiteto³³ (Jungtinės Amerikos valstijos) taipogi atliko keletą projektų susijusių su COBIT. Rezultatai buvo pristatyti keliuose dideliuose seminaruose, kuriuose buvo sukviesta apie 50 ekspertų iš įvairių pasaulio šalių. Tuose seminaruose pagrindinis dėmesys buvo skiriamas valdymo tikslams ir principams ir brandos modeliams. Koordinuojantis komitetas, apjungęs gautus rezultatus, parengė ir išplatino naują COBIT projektą devyniasdešimčiai specialistų. Gavus jų atsakymus buvo užbaigtas ketvirtosios COBIT versijos kūrimo procesas.

IT valdymo instituto COBIT 4.0 versija padeda organizacijoms didinti vertybes pasiekiamas panaudojus IT, sudaro galimybę palyginimams ir supaprastina COBIT gairių pritaikymą. Be to naujoji COBIT versija neanuliuoja darbų atliktų su ankstesniąja versija, o priešingai – palengvina anksčiau pradėtų darbų vystymą. Kai didžioji dalis veiklos yra suplanuota IT valdymo iniciatyva arba kai yra numatytas įmonės auditas, rekomenduojama viską iš naujo pradėti naudojant COBIT 4.0. Ketvirtosios versijos pritaikymas yra paprastesnis ir praktiškesnis, todėl ir IT strateginio valdymo įgyvendinimas tampa paprastesnis.

2007 m. gegužės mėnesį išleistas dar vienas COBIT atnaujinimas – 4.1 versija.

2.2 Ketvirtosios ir trečiosios COBIT versijų palyginimas

Pagrindiniai pasikeitimai pereinant nuo trečios prie ketvirtos COBIT versijos pagrindinėje dalyje yra šie:

- „M“ (Monitoring) domenas pasikeitė į „ME“ ir apima monitoringą ir vystymą (angl. Monitor and Evaluate).
- „M3“ ir „M4“ buvo audito, o ne IT procesai, todėl jie buvo pakeisti.
- „ME3“ yra susijęs su norminių aktų neatitikimais, kuris anksčiau buvo apibrėžtas „PO8“.
- „ME4“ apima IT valdymo procesų neatitikimus laikantis COBIT tikslų IT valdymo pagrinduose.
- Perkėlus „PO8“ į „ME3“ ir laikantis numeracijos, kad „PO9“ ir „PO10“ atitiktų trečiosios versijos numeraciją, „PO8“ buvo pervadintas į „kokybės valdymas“ (angl. manage quality). Atlikus šiuos pakeitimus sritis „planavimas ir organizavimas“ (angl. Plan & Organise) sutrumpėjo nuo 11 iki 10 procesų.

³² *University of Antwerp Management School* [interaktyvus], [žiūrėta 2007-04-17]. Prieiga per internetą: <<http://www.uams.be>>.

³³ *University of Hawaii* [interaktyvus], [žiūrėta 2007-04-17]. Prieiga per internetą: <<http://www.hawaii.edu>>.

- „AI“ srityje įvesti du pakeitimai: įsigijimo proceso papildymas ir būtinybė papildyti „AI5“ realizavimo kontrolės aspektais. Galiausiai, darant paskutinį pakeitimą buvo nuspręsta, kad tai turėtų būti paskutinis „AI“ srityje ir pavadintas „AI7“. Todėl naujojoje COBIT versijoje „AI“ sritis susideda iš septynių procesų³⁴.

Kaip matysime paskutiniame šio darbo skyriuje, kaip tik šie pasikeitimai ir buvo vienas iš pagrindinių priežasčių IT savianalizės metodikai atnaujinti.

Kitas pasikeitimas pereinant nuo trečiosios prie ketvirtosios COBIT versijų yra tai, kad buvo sumažintas detaliųjų valdymo tikslų skaičius nuo 318 iki 214. Tačiau daugeliu atveju detalieji valdymo tikslai buvo tiesiog apjungti.

2.3 COBIT procesai

COBIT – tarpusavyje susietų veiklos ar užduočių seka, turinti kontrolės taškus. COBIT išskiria 34 procesus 4-se pagrindinėse srityse:

1. Planavimas ir organizavimas:

- PO1 Apibrėžti strateginį IT planą
- PO2 Apibrėžti informacinę architektūrą
- PO3 Pasirinkti technologinę kryptį
- PO4 Apibrėžti IT procesus, organizacinę struktūrą ir veiksmus
- PO5 Valdyti IT investicijas
- PO6 Pateikti vadovybės tikslus ir kryptį
- PO7 Valdyti IT žmogiškuosius resursus
- PO8 Valdyti kokybę
- PO9 Įvertinti ir valdyti IT riziką
- PO10 Valdyti IT projektus

2. Įsigijimas ir įdiegimas:

- AI1 Automatizavimo sprendimų paieška
- AI2 Įsigyti ir palaikyti taikomąją programinę įrangą
- AI3 Įsigyti ir prižiūrėti technologinę infrastruktūrą
- AI4 Supažindinti su operacijomis ir panaudojamumu
- AI5 Įsigyti IT resursus
- AI6 Valdyti pokyčius
- AI7 Įdiegti ir akredituoti sprendimus ir pakeitimus

3. Naudojimas ir aptarnavimas:

³⁴ IT Governance Institute, *COBIT 4.0*. 4th ed. USA: ITGI, 2005. 194 p. ISBN 1-933284-37-4. P. 190.

- DS1 Apibrėžti ir užtikrinti IT paslaugų lygį
- DS2 Kontroliuoti trečiųjų šalių teikiamas paslaugas
- DS3 Kontroliuoti sistemų pajėgumus ir apkrovą
- DS4 Užtikrinti nuolatinį sistemų funkcionavimą
- DS5 Užtikrinti sistemų saugumą
- DS6 Identifikuoti ir paskirstyti IT kaštus
- DS7 Apmokyti vartotojus
- DS8 Valdyti pagalbos tarnybą ir incidentus
- DS9 Kontroliuoti konfigūraciją
- DS10 Sekti, spręsti problemas
- DS11 Valdyti duomenis
- DS12 Prižiūrėti fizinę terpę (patalpas)
- DS13 Kontroliuoti operacija (kasdienį sistemų naudojimą)

4. Monitoringas ir vystymas:

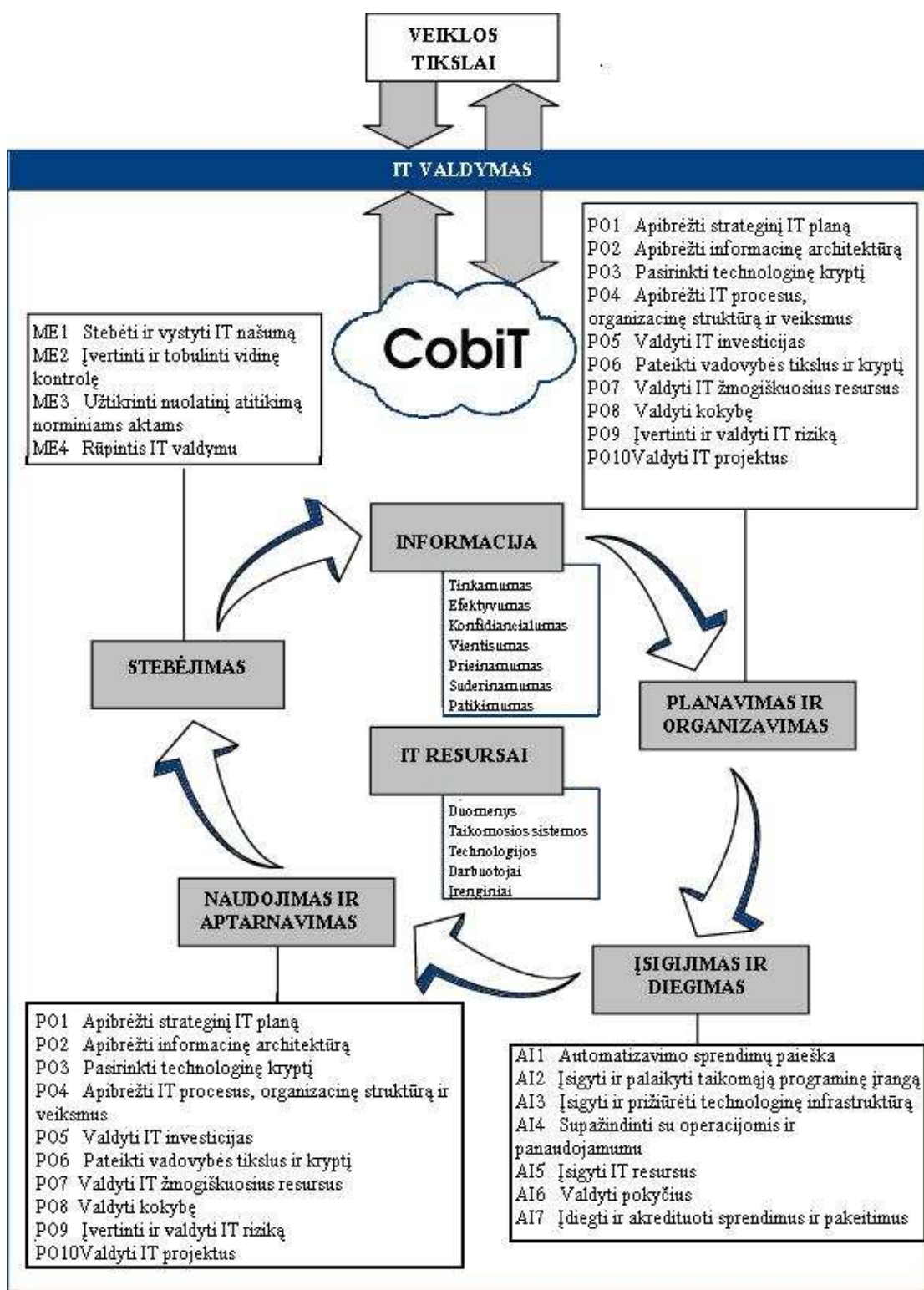
- ME1 Stebėti ir vystyti IT našumą
- ME2 Įvertinti ir tobulinti vidinę kontrolę
- ME3 Užtikrinti nuolatinį atitikimą norminiams aktams (compliance)
- ME4 Rūpintis IT valdymu³⁵

COBIT geros praktikos rinkinyje išskiriami šie informacinių technologijų ištekliai:

- Aplikacijos
- Informacija
- Infrastruktūra
- Darbuotojai

Dažniausiai COBIT procesų išsidėstymas atvaizduojamas jau, galima sakyti, klasikine tapusioje 3 schemoje. Joje vaizdžiai išreikšti pagrindiniai COBIT sluoksniai, kurie apima įmonės veiklos procesus, informacijos srautus ir IT resursus.

³⁵ IT Governance Institute, *COBIT 4.0*. 4th ed. USA: ITGI, 2005. 194 p. ISBN 1-933284-37-4. P. 33, 78, 109, 162.



3 schema. COBIT procesų išsidėstymas³⁶.

COBIT tarnauja IT strateginiam valdymui sukurdamas jam rėmus užtikrinant, kad:

- IT yra susietas su veiklos procesais.
- IT suaktyvina veiklą ir maksimizuoja pelną.
- IT resursai yra tinkamai naudojami.

³⁶ IT Governance Institute, *COBIT 3rd Executive Summary*. 3rd ed. USA: ITGI, 2000. 122 p. ISBN 1-893209-15-6. P 5.

- Atitinkamai valdoma IT rizika³⁷.

Visi dokumentai, išskyrus audito gairės, yra viešai prieinami internete, tarptautinės asociacijos ISACA internetinėje svetainėje www.isaca.org. Pagrindinis COBIT principas – norint užtikrinti tinkamą informacijos valdymą organizacijoje, informacinėms technologijoms skiriami resursai turi būti valdomi tam tikrų tarpusavyje susietų procesų pagalba.

2.4 COBIT – įrankis savianalizės priemonėms kurti

Savianalizė gali būti apibrėžiama kaip metodika, kuri naudojama apžvelgti pagrindiniams veiklos tikslams, rizikoms atsirandančiomis siekiant šių veiklos tikslų ir tų rizikų valdymui naudojant formalius, dokumentuotus procesus. Savianalizės metu yra įtraukiama ne tik darbo grupė, bet taip pat ir vadovybė, kad būtų galima aptarti bei apžvelgti egzistuojantį kontrolės sistemos efektyvumą. Moderatoriai arba auditoriai savianalizės metu atlieka profesionalų vaidmenį ir padeda atlikti savianalizę³⁸.

Praktikoje savianalizė yra vientisas tam tikros srities įrankių rinkinys, pradedant nuo paprastų klausimynų ir baigiant pagalbinėmis metodikomis, sukurtomis rinkti informacijai apie organizaciją apklausiant tuos, kurie kiekvieną dieną susiduria su tam tikra darbo sritimi, o taip pat ir jų vadovus. Pagrindiniai įrankiai naudojami savianalizės metu nepriklauso nuo to ar projektas yra techninis ar finansinis ar dar kitos srities. Savianalizės įrankiai apima vadovybės susitikimus, klientų darbo grupes, darbinius dokumentus, apklausos anketas ir savianalizės taisykles. Yra ir įvairiapusiai metodai žemesniems nei vadovybė darbuotojų lygiams apklausti; pasitaiko, kad organizacijos savianalizės metu įtraukia netgi išorės atstovus (pvz. klientus arba verslo partnerius).

Yra keletas tikslų susijusių su savianalizės programos įsisavinimu. Pirminiai tikslai yra įtakoti vidinio audito funkcijas kaitaliojant kai kurias pagrindines valdymo stebėjimo priemones (angl. *control monitoring responsibilities*) su funkcinėmis sritimis. Tai nėra ketinimas pakeisti audito atsakomybes, bet sustiprinti (papildyti) jas. Tiesioginiai vadovai, yra atsakingi už kontrolę savo aplinkoje, bet taip pat jie turi būti atsakingi ir už tos kontrolės stebėjimą. Savianalizės metu vadovybė gali išsiaiškinti, kokią kontrolę ir jos stebėjimą sudaryti atsižvelgiant į aukštos rizikos sritis.

Atlikus savianalizę, kiekvienos fazės (planavimo, įgyvendinimo ir stebėjimo) sėkmingumo matas turi būti vystomas iki kol bus pasiekiamas tikslas užsibrėžtas savianalizės metu. Kritinis sėkmės faktorius yra surengti susitikimą su verslo vieneto atstovais, įskaitant tiesiogiai susijusius darbuotojus

³⁷ *COBIT 4th edition brochure* [interaktyvus], USA: Information Systems Audit and Control Association (ISACA), 2007- [žiūrėta 2007-04-17]. Prieiga per internetą: <http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Obtain_COBIT.htm>.

³⁸ Informatikon Systems Audit and Control Association. *2004 CISA Review Manual*, USA: 2004. P. 51.

bei vadovybę, kad supažindinti juos su savianalizės rezultatais. Be to, turi būti aprašomas veiksmų planas, kaip sėkmingai pasiekti pagrindinius tikslus.

Kalbant apie IT, COBIT yra vienas iš įrankių, padedančių sukurti savianalizės priemones. Deja, tokios priemonės dažniausiai būna sukuriamos organizacijų viduje, todėl informacijos šaltiniuose galima atrasti tik keletą pavyzdžių. Toliau trumpai pristatoma IT valdymo savianalizės kontrolinis sąrašas (angl. *IT Governance Self-Assessment checklist*), kontrolės ir rizikų savianalizė (angl. *Control risk self-assessment* (CRSA)) ir kontrolės priemonių savianalizė (angl. *control selfassessment* (CSA)).

IT valdymo savianalizės kontrolinis sąrašas

Pačiame COBIT geros praktikos rinkinyje yra papildoma priemonė, kuri gali padėti organizacijoms vystyti jų IT valdymą. Ta priemonė yra IT valdymo savianalizės kontrolinis sąrašas (2 lentelė). Naudodamasi šia lentele savianalizės metu vadovybė privalo nustatyti kiekvienam iš COBIT procesų:

- Kiek svarbus yra atitinkamas procesas organizacijos veiklos tikslams?
- Ar atitinkamas COBIT procesas yra pakankamai įgyvendintas (svarbumo ir įgyvendinimo kombinacija gali būti, kaip stiprus rizikos indikatorius)?
- Kas vykdo procesą ir kas už jį atsako (ir ar atsakomybė yra nesidubliuojanti ir priimtina)?
- Ar procesai ir jų kontrolės yra formalizuotos, tai yra, ar organizacijoje yra sutartys su trečiosiomis šalimis ir aiškus procedūrų rinkinys vidiniams procesams kontroliuoti?
- Ar procesai yra audituojami³⁹?

³⁹ LAINHART IV John W., *International Standards provide Guidance for IT Governance* [interaktyvus]. USA: International Federation of Accountants, 2001- [žiūrėta 2007-04-21]. Prieiga per internetą: <<http://www.ifac.org/Library/Article.tpl?NID=99097368215895>>.

2 lentelė. IT valdymo savianalizė⁴⁰.

Rizika	Svarbumas – kaip svarbu organizacijai įvertinti skalėje nuo 1 (visiškai nesvarbu) iki 5 (labai svarbu)		Kas tai atlieka?				Kas atsakingas?
	Svarbumas	Atlikimas	IT	Kiti	Nuomos sutartys	Nežinau	
		Atlikimas – kaip gerai yra atliekama, nuo 1 (nėra žinoma arba blogai) iki 5 (labai gerai)					
		Audituojama – Taip, ne arba ?					
		Formalizuota – ar yra sutartys, SLA ar aiškiai aprašytos procedūros? (Taip, ne arba ?)					
		Atsakingas asmuo – vardas arba „nežinau“					
		COBIT domenai ir procesai					
		PLANAVIMAS IR ORGANIZAVIMAS					
		PO1 Apibrėžti strateginį IT planą					
		PO2 Apibrėžti informacinę architektūrą					
		PO3 Pasirinkti technologinę kryptį					
		PO4 Apibrėžti IT procesus, organizacinę struktūrą ir veiksmus					
		PO5 Valdyti IT investicijas					
		PO6 Pateikti vadovybės tikslus ir kryptį					
		PO7 Valdyti IT žmogiškuosius resursus					
		PO8 Valdyti kokybę					
		PO9 Įvertinti ir valdyti IT riziką					
		PO10 Valdyti IT projektus					
		ĮSIGIMAS IR ĮDIEGIMAS					
		AI1 Automatizavimo sprendimų paieška					
		AI2 Įsigyti ir palaikyti taikomąją programinę įrangą					
		AI3 Įsigyti ir prižiūrėti technologinę infrastruktūrą					
		AI4 Supažindinti su operacijomis ir panaudojimu					
		AI5 Įsigyti IT resursus					
		AI6 Valdyti pokyčius					
		AI7 Įdiegti ir akredituoti sprendimus ir pakeitimus					
		NAUDOJIMAS IR APTARNAVIMAS					
		DS1 Apibrėžti ir užtikrinti IT paslaugų lygį					
		DS2 Kontroliuoti trečiųjų šalių teikiamas paslaugas					
		DS3 Kontroliuoti sistemų pajėgumus ir apkrovą					
		DS4 Užtikrinti nuolatinių sistemų funkcionavimą					
		DS5 Užtikrinti sistemų saugumą					
		DS6 Identifikuoti ir paskirstyti IT kaštus					
		DS7 Apmokyti vartotojus					
		DS8 Valdyti pagalbos tarnybą ir incidentus					
		DS9 Kontroliuoti konfigūraciją					
		DS10 Sekti, spręsti problemas					
		DS11 Valdyti duomenis					
		DS12 Prižiūrėti fizinę terpę (patalpas)					
		DS13 Kontroliuoti operacija (kasdienį sistemų naudojimą)					
		STEBĖJIMAS IR VYSTYMAS					
		ME1 Stebėti ir vystyti IT našumą					
		ME2 Įvertinti ir tobulinti vidinę kontrolę					
		ME3 Užtikrinti nuolatinių atitikimą norminiams aktams					
		ME4 rūpintis IT valdymu					

⁴⁰ IT Governance Institute, *COBIT 3rd Implementation Tool Set*. 3rd ed. USA: ITGI, 2000. 92 p. ISBN 0-893209-16-14. P 50.

Užpildžius tokią kontrolinę lentelę ir išanalizavus rezultatus, turėtų sustiprėti vadovybės supratimas apie rizikas bei pareigybių ir atsakomybių formalizavimo lygį. Aukštos rizikos identifikatorių ir atsakymo „nežinau“ sutapimas turėtų vadovybei sukelti ypatingą susirūpinimą.

Ten kur nustatoma aukšta rizika, vadovybė turi susikcentruoti, pasinaudoti COBIT aukštojo lygio ir detalizuotus valdymo tikslais ir į pagalbą pasitelkti IS auditorius, kad nustatyti kainos ir efektyvumo reikšmes siekiant sušvelninti rizikas. Atlikus šiuos žingsnius akivaizdžiai išaugs IT valdymo lygis ir tuo pačiu bus nauda visai organizacijai.

Kontrolės ir rizikų savianalizė - CRSA

Viena iš pirmiausiai pasirodžiusių savianalizių yra ISACA 2002 metais sukurta kontrolės ir rizikų savianalizė (angl. *Control risk self-assessment (CRSA)*)⁴¹. Ši metodika yra apibūdinta kaip priemonė leidžianti vadovybei ir visų sričių darbuotojams drauge identifikuoti ir įvertinti su informacinėmis sistemomis susijusias rizikas ir kontroles.

Kontrolės rizikų savianalizė padeda vadovybei ir darbuotojams:

- Identifikuoti veiklos procesus ir suteikti jiems prioritetus.
- Įvertinti ir valdyti veiklos procesų aukštos rizikos sritis.
- Patiems įsivertinti kontrolių adekvatumą.
- Sudaryti rizikų valdymo veiksmų planą.
- Užtikrinti, kad identifikuoti, atpažinti ir įvertinti veiklos tikslai ir rizikos atitinka visus organizacijos lygmenis.

CRSA įgyvendinimas susideda iš šių etapų:

- CRSA seminaro planavimas.
- Darbo grupės surinkimas.
- Metodikos pristatymas darbo grupei.
- Darbo įrankių paruošimas.
- Darbas grupėje naudojant metodikos priemones.
- Rezultatų patikrinimas.
- Ataskaitos parengimas ir jos pristatymas.
- Monitoringas.

CRSA gali būti pritaikoma įvairiose srityse susijusiose su sistemų kūrimo projektais, projektų vystymo grupėmis, duomenų centrų operacijomis, kompiuteriniais tinklais, sistemų saugumu,

⁴¹ *IS auditing procedure: Control Risk self-assessment (CRSA)* [interaktyvus]. USA: Information Systems Audit and Control Association [žiūrėta 2007-04-21]. Prieiga per internetą: <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31605>.

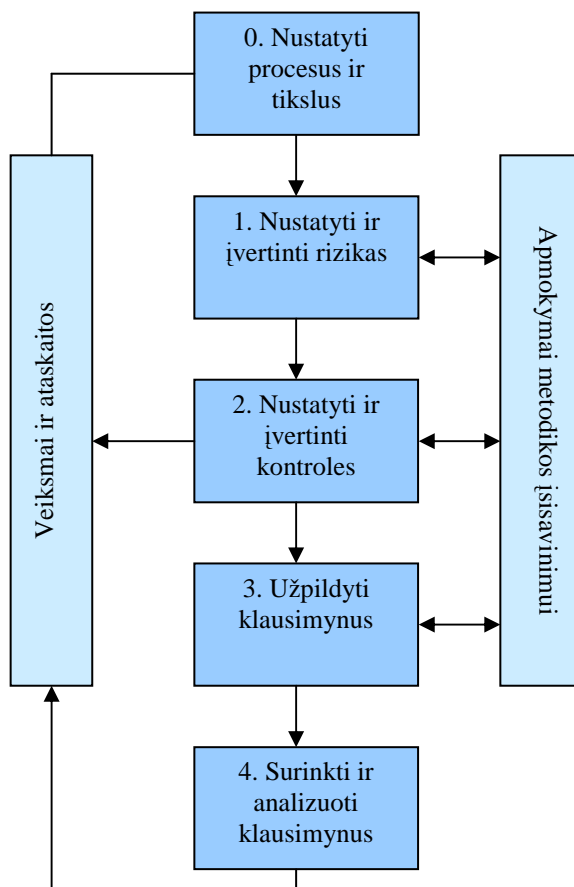
duomenų bazių ir taikomųjų programų sistemomis, pagalbos tarnyba (angl. *Help desk*), telekomunikacine sistema, veiklos tęstinumo pasirengimu, informacinių sistemų dokumentacija, elektroninių duomenų transakcijomis, elektroninio pašto sistema ir IT valdymu.

Esminė priežastis, dėl ko šioje metodikoje naudojamas COBIT yra tai, jog vienoje iš COBIT dalių „Planavimas ir organizavimas“ (angl. *Planning & Organisation*) yra įtrauktas aukšto lygio valdymo tikslas – „rizikos valdymas“ (angl. *Assess Risks (PO9)*), kuris susideda ir detaliųjų valdymo tikslų, tokių kaip rizikos indentifikavimas (angl. *Risk Identification*), rizikos vertinimas (angl. *Risk Measurement*) ir rizikos veiksmų planas (angl. *Risk Action Plan*). Tai reiškia, kad kontrolės rizikų savianalizė padeda siekti minėtų detaliųjų valdymo tikslų. CRSA gali būti naudojama norint nustatyti ir analizuoti su informacinėmis sistemomis susijusias rizikas, o gautus rezultatus panaudoti sudarant rizikų valdymo veikslų planą.

Kontrolės savianalizė – CSA

Kontrolės procedūros turi būti ne tik dokumentuotos, bet ir jų laikomasi. Dažniausiai tai, kaip laikomasi vidaus kontrolės procedūrų prižiūri vidaus auditoriai, bet kas liečia IT kontrolės procedūrų auditą, ši sritis gerokai sudėtingesnė ir reikalauja daug žinių susijusių su IT. Samdyti specialistus tokiam auditui atlikti yra brangu, todėl kaip pagalbiniė priemonė gali būti reguliariai atliekama kontrolės procedūrų savianalizė,

Yra ir kitų būdų kaip garantuoti, kad kontrolės sistema būtų tinkama ir efektyvi. Tokią garantiją galima gauti atliekant kontrolės priemonių savianalizę (ang. *control selfassessment (CSA)*). Šios savianalizės etapai pavaizduoti 4 schemeje.



4 schema. CSA įgyvendinimo etapai⁴².

Sistemos ir jų kontrolės procedūros organizacijoje diegiamos nuosekliai, bet tam reikia nemažai laiko. Pavyzdžiui, bankai – pats seniausias aptarnavimo sektorius ir juose kontrolės procedūros svarbios ne tik vidaus procesams, bet ir visuomenei. Kontrolės procedūros bankininkystėje taip pat vystėsi ilgą laiką. Vis dėl to bankuose pradėjus diegti kompiuterines technologijas, tuo pačiu reikėjo patobulinti ir kontrolės procedūras. Tai kas įgyvendinta bankinėje sferoje, galima įdiegti ir kituose tiek verslo tiek valstybinėse vidutinio dydžio ar didelėse organizacijose.

IT kontrolės procedūrų savianalizė tokiose organizacijose užtikrintų vadovybę, akcininkus ir klientus, kad kontrolės priemonės yra tinkamos ir efektyvios.

Vidaus ir išorės auditoriai padeda vadovybei vystyti procedūras ir vidinę kontrolę, tačiau jie nepajėgūs iš pagrindų patikrinti visų veiklos procesų. Norint pagelbėti vadovybei įvertinti vidines kontrolės priemones ir padidinti darbuotojų supratingumą apie tas priemones, turėtų būti atliekama kontrolės savianalizė. Dauguma organizacijų galėtų atlikti ir pripažinti savianalizės teikiamą naudą, nes taip galima atsisakyti atskiro vidaus IS auditoriaus etato ir sumažinti biudžeto išlaidas. Savianalizė padeda vadovybei nustatant tikslus, įvertinant kontroles ir rizikas, sudarant veiksmų planą.

⁴² BAKSHI, Sunil, Control Self-assessment for Information and related technology. *Information Systems Control Journal*, 2004, vol. 1, p. 10-18.

Pabrėžtina, kad kontrolių savianalizė yra vidaus kontrolės mechanizmo praplėtimas, tačiau, kol nėra įdiegta kontrolės sistema – kontrolių savianalizės atlikimas yra beprasmiškas reikalas. Vadinasi, reikalingas bent supratimas apie tai kas yra ir kam reikalingos vidaus kontrolės procedūros.

2.5 Skyriaus apibendrinimas

Darbe ypatingas dėmesys skiriamas COBIT pristatymui, nes jis yra pagrindas ant kurios sukurta IT savianalizės metodika. Apžvelgus istorinius COBIT faktus, galima pastebėti, kad šis produktas buvo kuriamas ir toliau tobulinamas labai atsakingai. Į jo kūrimo darbą įtraukti specialistai ir jų grupės. COBIT yra IT strateginio valdymo gairės ir palaikantis įrankių rinkinys, kuris suteikia vadovams galimybę užpildyti spragas atsižvelgiant į kontrolės sistemos reikalavimus, technines galimybes ir veiklos rizikas.

Pagrindiniai COBIT elementai, kaip matysime tolimesniuose darbo skyriuose, naudojami AAI sukurtoje IT savianalizės metodikoje, tai yra COBIT IT procesai:

- Planavimas ir organizavimas (10 procesų)
- Įsigijimas ir įdiegimas (7 procesai)
- Tiekimas ir palaikymas (13 procesų)
- Stebėjimas (monitoringas) (4 procesai)

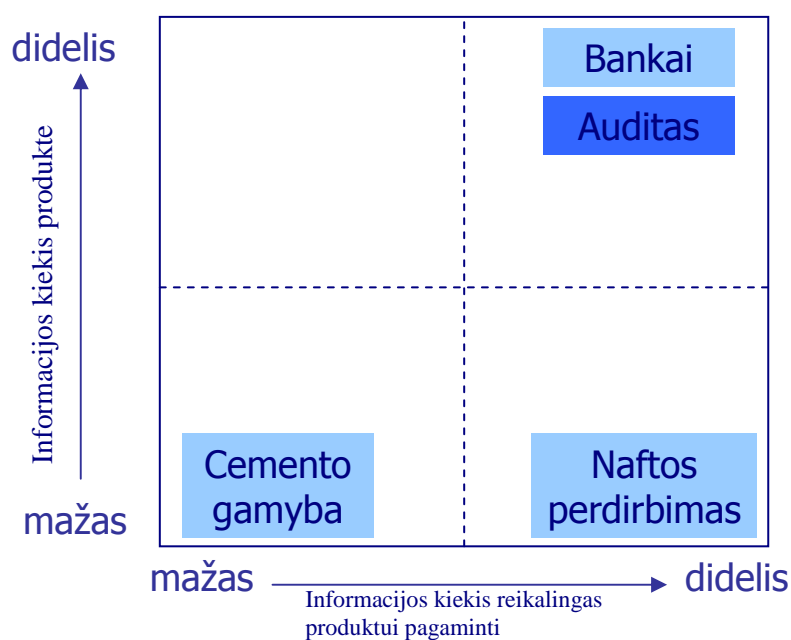
Antrajame skyriuje taip pat buvo paminimas faktas, kad COBIT yra puikus įrankis savianalizės priemonėms sudaryti. Įrodant šį faktą buvo pristatyti keli savianalizės metodai/metodikos, kurie daugiau ar mažiau remiasi COBIT geros praktikos rinkiniu: IT valdymo savianalizės kontrolinis sąrašas (angl. *IT Governance Self-Assessment checklist*), kontrolės ir rizikų savianalizė (angl. *Control risk self-assessment (CRSA)*) ir kontrolės priemonių savianalizė (angl. *control selfassessment (CSA)*).

3. AAI IT SAVIANALIZĖS METODIKA PARENGTA EUROSAI IT DARBO GRUPĖS

Ankstesniuose skyriuose jau buvo trumpai užsiminta apie savianalizių egzistavimą ir jų pritaikymo naudą. Nepriklausomai nuo savianalizės formos, tikslas išlieka tas pats: padėti organizacijai įvertinti tikimybę pasiekti jos užsibrėžtų tikslų, remiantis darbuotojų, kurie atsako už šių organizacijai keliamų tikslų pasiekimą, žiniomis.

AAI IT savianalizės metodika parengta EUROSAI IT darbo grupės (toliau vadinsime – IT savianalizė) yra išskirtinė tuo, kad ji apima visą organizacijos IT strateginį valdymą, nes yra parengta COBIT pagrindu. Todėl dažnai ši metodika vadinama – IT valdymo savianalizės metodika. IT savianalizė yra patogus būdas informacijai rinkti ir seminaro dalyvių žinioms ugdyti, bet jos nereikėtų tapatinti su IS auditu. Tai yra ribotas laikas, per kurį patys organizacijos darbuotojai, tiksliau surinkta grupė, padedant moderatoriui iš išorės išsiaiškina pagrindines organizacijos su IT susijusias problemas ir jų keliamas rizikas, bei parengia veiksmų planą kaip elgtis toliau.

Neabejotinai kyla klausimas, kodėl būtent AAI susikūrė ir sėkmingai naudoja IT savianalizės metodiką? Į šį klausimą atsakymą galima rasti 5 schemeje.



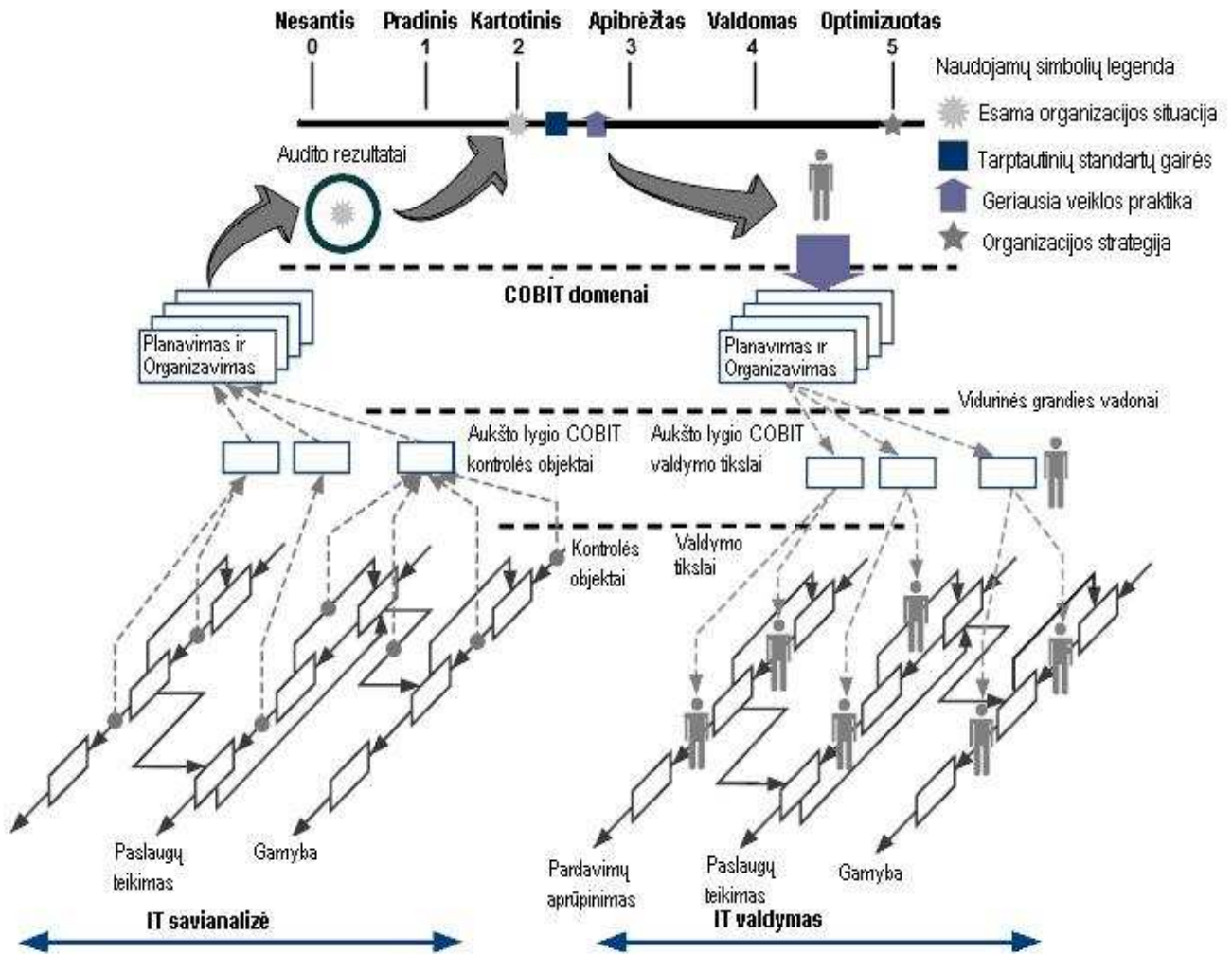
5 schema. Informacinių technologijų valdymo strateginė svarba⁴³.

5 schemeje parodoma, kad pagrindiniai ir antriniai aukščiausiųjų audito institucijų veiklos procesai yra priklausomi nuo informacijos. Informacijos kūrimą ir apdorojimą tiesiogiai įtakoja informacinių technologijų būklė. Maža to, tendencijos yra tokios, kad IT įtaka audito veiklai ateityje

⁴³ MANTELAERS, Paul, *The Strategic Importance of IT for SAIs*. Seminaro pateiktis. Vilnius, 2005. P. 20.

neišvengiamai didės. Visiškai priešinga situacija yra pavyzdžiui, su cemento gamyba. Į šį produktą informacija beveik neįeina.

Norėdami kuo efektyviau pradėti įgyvendinti IT strateginį valdymą organizacijoje, pirmiausiai turėtume įsivertinti esamą situaciją. Kitaip tariant - įvertinti IT procesų brandos lygį. Žemiau pateikiamoje 6 schemoje vaizdžiai matyti IT strateginio valdymo IT savianalizės santykis.



6 schema. Informacinių technologijų strateginio valdymo ir informacinių technologijų audito santykis⁴⁴.

Savianalizės rezultatas yra suminė kontroliuojamų savianalizės objektų įvertinimo išraiška ir nustato esamą organizacijos informacinių technologijų brandos lygį. Pageidaujamas (siektinąs) organizacijos informacinių technologijų brandos lygis yra nustatomas ir vėliau detalizuojamas į konkrečius COBIT detaliuosius valdymo tikslus, sudaromas veiksmų planas šių detaliųjų valdymo

⁴⁴ ГУЗИК, Сергей, *Стандарт СoBIT Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ* ISACA.ru, 2002, p. 21.

tikslų brandos lygiui pakelti. Tokiu būdu, COBIT metodas leidžia valdyti informacinių technologijų pokyčius valdant atskirus detaliuosius valdymo tikslus.

3.1 IT savianalizės metodikos privalumai

Dar tik pradėjus kurti IT savianalizės metodiką, pagrindinis uždavinys buvo sukurti savianalizės instrumentą, kuris būtų naudojamas AAI. Be to naudodamos COBIT AAI galėtų palyginti savo IT aplinką su kitų AAI IT aplinkomis, o taip pat su geriausios praktikos standartais ir numatyti būdus savo IT aplinkai pagerinti.

IT savianalizės metodikoje iškeliam šie tikslai:

- Įtakoti AAI darbą užtikrinant veiklos kokybę ir darbų atlikimą AAI IT aplinkoje ir didinant supratimą apie IT strateginį valdymą.
- Stiprinti Aukščiausiųjų audito institucijų gebėjimus siekti jų strateginių tikslų panaudojant informacines technologijas.

IT Savianalizė taip pat gali būti naudinga:

- Gerinant supratimą, kaip Aukščiausiose audito institucijose valdomas informacines technologijos, kokie yra jų valdymo rizikos faktoriai, kaip apsaugoti IT infrastruktūrą.
- Suteikti auditoriams ir AAI galimybę išbandyti IT savianalizės metodiką ir COBIT, kaip IT analizės ir valdymo instrumentas.
- Įgyti žinių apie COBIT.
- Atlikti IT aplinkos analizę Aukščiausių audito institucijų viduje.

IT savianalizė yra svarbi, nes:

- IT yra integrali įstaigos/organizacijos veiklos dalis.
- IT strateginis valdymas yra integrali bendrojo įstaigos valdymo dalis.
- IT yra kritinės ir strateginės įstaigos veiklai.
- Planuojami ir realūs rezultatai dažnai nesutampa.
- IT nėra kreipiamas reikalingas dėmesys.
- IT reikia didelių investicijų ir jos yra rizikinga sritis⁴⁵.

Sėkmingas IT savianalizės įgyvendinimas gali atnešti štai tokios naudos:

- skatina tiesioginę IT darbuotojų įtaką veiklos procesų valdymui.
- IT savianalizę atlieka patys organizacijos darbuotojai, todėl nereikia samdyti išorės ekspertų. Taip sutaupoma lėšų.
- Skatina geresnį organizacijos suvokimą apie IT veiklą ir jos valdymą.
- Suderina atskirų padalinių siekius su bendrais organizacijos tikslais.

⁴⁵ JAKIMAVIČIUS, Dainius, *Įvadas į Informacinių technologijų valdymo savianalizę*. Seminaro medžiaga, 2005.

- Skatina veiklos rizikų valdymą ir kontrolės procedūrų taikymą;
- Paskirstomos atsakomybės už veiklos valdymo rizikas;
- Pagerina komunikavimą tarp organizacijos padalinių ir pačioje organizacijoje apskritai;
- Gerina supratimą apie tai, kokia yra silpno valdymo įtaka visai organizacijai⁴⁶.

Dar viena labai svarbi IT savianalizės charakteristika yra ta, kad jos metu dalyviai esantys iš įvairių AAI veiklos sričių gali diskutuoti su IT funkcijas atliekančiais atstovais. Tokių diskusijų metu pagalbininko vaidmenį atlieka moderatorius/ekspertas iš išorės.

3.2 IT savianalizės raida

Kiekvienas darbas yra žymiai greičiau ir efektyviau atliekamas, kai remiamasi jau įgyta patirtimi, sukurtomis metodikomis ir ekspertų patarimais. Todėl daugelyje sričių pavieniai asmenys buriasi į grupes, o juridiniai vienetai – į organizacijas. Ne išimtis ir valstybinį auditą atliekančios institucijos.

Viso pasaulio audito institucijas vienija INTOSAI (angl. *International Organisation of Supreme Audit Institutions*), o EUROSAI (angl. *European Organisation of Supreme Audit Institutions*) yra jos padalinys Europoje. EUROSAI yra nepriklausoma ir nepolitinė organizacija įkurta siekiant glaustesnio bendradarbiavimo ir skatinti idėjų, patirties ir metodikų apsikeitimą tarp Aukščiausių audito institucijų, atliekant valstybinius auditus. Ši organizacija vienija 46 Europos AAI. O vienas svarbiausių EUROSAI parengtų dokumentų yra Deklaracija dėl aukščiausiosios audito institucijos nepriklausomumo⁴⁷.

EUROSAI šiuo metu egzistuoja šios darbo grupės: Aplinkos audito, Informacinių technologijų ir Mokesčių lengvatų audito. Lietuvos Respublikos valstybės kontrolė EUROSAI veikloje dalyvauja nuo 1993 m. ir yra įsitraukusi į darbą Aplinkos audito, Informacinių technologijų ir Mokesčių lengvatų audito darbo grupėse bei Kvalifikacijos tobulinimo komitete.

EUROSAI Informacinių technologijų darbo grupės tikslas yra dalintis kompetencija ir patirtimi tarp Europos regione esančių AAI ir skatinti IT naudojimą pagrindinėje organizacijos veikloje. Taip pat šios darbo grupės tikslas yra stimuliuoti Europos AAI bendrai išbandyti strateginius IT pagrindu sukurtus produktus naudojamus tiek audito, tiek ir administracinio pobūdžio informacijai valdyti. Be to siūloma programa Europos AAI kaip kooperuotis perduodant vieni kitiems įgytą patirtį.

EUROSAI IT darbo grupės siekiai yra tokie:

- Skatinti vizijų įgyvendinimą.
- Palengvinti patirties ir kompetencijos sklaidą tarp AAI.

⁴⁶ EUROSAI IT Working Group, *A methodology for IT self-assessment by SAI's*, 2004 59 p. P. 7.

⁴⁷ EUROSAI [interaktyvus]. Ispanija - [žiūrėta 2006 m. sausio 12 d.]. Prieiga per internetą: <<http://www.eurosai.org>>.

- Skatinti bendradarbiavimą kuriant IT technologijomis paremtus auditus.
- Skatinti paralelinius, jungtinius ar koordinuotus auditus⁴⁸.

Pirmasis EUROSAI Informacinių technologijų darbo grupės pasitarimas įvyko 2002 metų rugsėjo 30 ir spalio 1 dienomis Hagoje, kur buvo parengtas veiksmų planas. Vienas iš veiklos tikslų buvo pradėti projektą, kurio metu būtų parengta IT savianalizės metodika Aukščiausioms audito institucijoms naudojantis COBIT'u. Šis darbas buvo priskirtas pogrupiui sudarytam iš šešių šalių AAI:

- Šveicarijos federalinė audito įstaiga – Michel Huissound(projekto vadovas)⁴⁹
- Ispanijos audito rūmai – Alberto Rubio⁵⁰
- Lietuvos Respublikos valstybės kontrolė – Dainius Jakimavičius⁵¹
- Nyderlandų audito rūmai – Henk van der Geest ir Paul Mantelaers⁵²
- Norvegijos generalinio auditoriaus įstaiga – Rune Juhannessen⁵³
- Slovėnijos audito rūmai – Marjan Podgorsek⁵⁴

IT savianalizės projekto grupė darbą pradėjo apibrėždama, kas yra savianalizė ir kokie jos privalumai ir trūkumai, jos taikymo galimybės. Taip pat apsvarstytas klausimas, kokią vietą audito aplinkoje užima COBIT. Ar juo galima grįsti savianalizės metodiką, ar savianalizės metodika turėtų būti grindžiama kitais standartais? COBIT yra parengtas 36 nacionalinių ir tarptautinių standartų pagrindu, o trys pagrindiniai COBIT šaltiniai yra IT valdymo standartai (ISO17799, SPICE, ITIL ir t.t.), IT saugumo standartai (ITSEC, BS7799 ir t.t.), IT audito standartai (IFAC, IIA, COSO, GAO ir t.t.). Taigi, COBIT yra jungtinė metodika įstaigų vadovams, IT profesionalams ir auditoriams, o šioms vartotojų grupėms yra taikomos COBIT „Valdymo gairės“ (angl. *Management Guidelines*), „Detalūs kontroliniai uždaviniai“ (angl. *Detailed Control Objectives*) bei „Audito gairės“ (angl. *Audit Guidelines*). Jei pavyzdžiui, standartas ISO17799⁵⁵ reglamentuoja tik IT saugumo aspektus, tai COBIT skirtas IT strateginiam valdymui.

COBIT remiasi dviem skirtingomis procesų grupėmis – bendrieji įstaigos veiklos procesai ir specifiniai IT procesai ir šių procesų tarpusavio įtaka. 1-ąją (veiklos procesų) grupę nustato vadinamoji BVC-forma (angl. *Business Value Chain*). BVC skirta šiems procesams išdėstyti ir jų reikšmingumo lygiui įvertinti. Jei veiklos procesuose kažkas negerai – ieškoma priežastiniai IT procesai (COBIT

⁴⁸ *EUROSAI-IT Working Group, Objectives* [interaktyvus]. Netherlands: EUROSAI IT Working Group Secretariat - [žiūrėta 2006 m. sausio 12 d.]. Prieiga per internetą: <<http://www.eurosai-it.org/9282201/v/index.htm>>.

⁴⁹ *Swiss Federal Audit Office* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.efk.admin.ch/english/index.htm>>.

⁵⁰ *Spanish Court of Audit* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.tcu.es>>.

⁵¹ *Lietuvos Respublikos valstybės kontrolė* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.vkontrole.lt>>.

⁵² *Netherlands Court of Audit* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.rekenkamer.nl>>.

⁵³ *Office of the Auditor General of Norway* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.riksrevisjonen.no>>.

⁵⁴ *Court of Audit of the Republic of Slovenia* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.rs-rs.si>>.

⁵⁵ Informacijos technologija. *Informacijos saugumo valdymo praktikos kodeksas* (tapatus ISO/IEC 1799:2000). Lietuvos standartizacijos departamentas. 2004, LST ISO/IEC 17799:2004 lt

išskirti 34 reikšmingesni IT procesai, sudarantys 4 didesnes grupes), nustatoma šių procesų įtaka bendriesiems įstaigos veiklos procesams. Tokiu būdu yra sudaroma 2-oji (IT procesų grupė), turinti didelę įtaką įstaigos veiklai (t.y, 1-osios grupės procesams).

Remiantis COBIT nustatytais IT procesų įvertinimo kriterijais, galima išrinkti tuos bendruosius įstaigos veiklos (1-osios grupės) procesus, kurie yra esminiai siekiant IT efektyvumo. Tokiu būdu, COBIT leidžia (per IT prizmę, t.y., remiantis IT kriterijais) siekti bendrųjų įstaigos veiklos procesų brandos⁵⁶.

Pirmojo IT savianalizės projekto etapo metu buvo suformuluoti šie tikslai:

- Sukurti metodiką, kuri būtų pritaikyta naudoti Aukščiausiose audito institucijose atliekant informacinių technologijų savianalizę.
- Savianalizės metodika turi leisti nustatyti IT strateginio valdymo brandą, analizuoti ir sudaryti veiklos planus.
- Savianalizės metodika turi būti tobulinama analizuojant pilotinių seminarų metu gautą informaciją.
- Pasiiekti, kad EUROSAI aukščiausiosiose audito institucijose būtų atliekama IT savianalizė⁵⁷.

Be užsibrėžtų tikslų kuriama IT Savianalizės priemonė turėjo atitikti šiuos reikalavimus:

- Paprasta naudoti.
- Apimti visus svarbius AAI informacinių technologijų procesus.
- Gali būti naudojama kitose įstaigose ar organizacijose.
- Išsamiai dokumentuota.
- Nepriklausoma nuo programinės įrangos.
- Skatinanti diskusijas ir dialogus.
- Skatintų išgauti rezultatus, kuriuos būtų galima sulyginti.
- Įtakotų kokybės pagerinimą.

Kito IT savianalizės projekto grupės pasitarimo Berne metu (2003 metų kovo mėn.) buvo nuspręsta IT savianalizės pagrindu naudoti COBIT, nes jis plačiai naudojamas pasaulinėje informacinių sistemų valdymo ir audito praktikoje.

2003 m. rugsėjį išleista pirmoji IT savianalizės versija. Buvo aprašyta IT savianalizės metodika, paruoštos formos ir parengta prezentacija. Be to buvo nuspręsta keturių šalių AAI atlikti savianalizę, kad pratestuoti naujai sukurtą IT savianalizės metodiką. Tos šalys buvo Lietuva, Ispanija, Prancūzija ir Danija.

⁵⁶ JAKIMAVIČIUS, Dainius, *ATASKAITA apie EUROSAI Informacinių technologijų darbo grupės 2-ąjį pasitarimą, vykusį 2004 m. kovo 29 - 30 d. Berne (Šveicarija)*, 2004, p. 2-4.

⁵⁷ EUROSAI IT Working Group, *A methodology for IT self-assessment by SAI's. Version 2.0*, Bern: 2004, P. 6.

2003 metų pabaigoje buvo atliktos pirmosios savianalizės, apibendrinti rezultatai. Remiantis gautomis išvadomis buvo patobulinta IT savianalizės metodika, pataisytos formos bei prezentacija. 2004 m. vasario mėnesį buvo Aukščiausiųjų audito institucijų išleista 2.0 IT savianalizės versija ir patvirtinta EUROSAI IT darbo grupės.

2.0 IT savianalizės metodika atitiko šiuos kriterijus:

- Nuosekli, sudaryta iš 7 žingsnių.
- Rezultatų pateikimui naudojami grafikai.
- Rezultatų analizei naudojamos Excel formos.
- Medžiagos pateikimas – PowerPoint pateiktys.
- Pasirengimas seminarui – instrukcijos dėstytojui.
- Metodikos paskirtis – padėti pasirengti savianalizei kitų aukščiausiųjų audito institucijų darbuotojams⁵⁸.

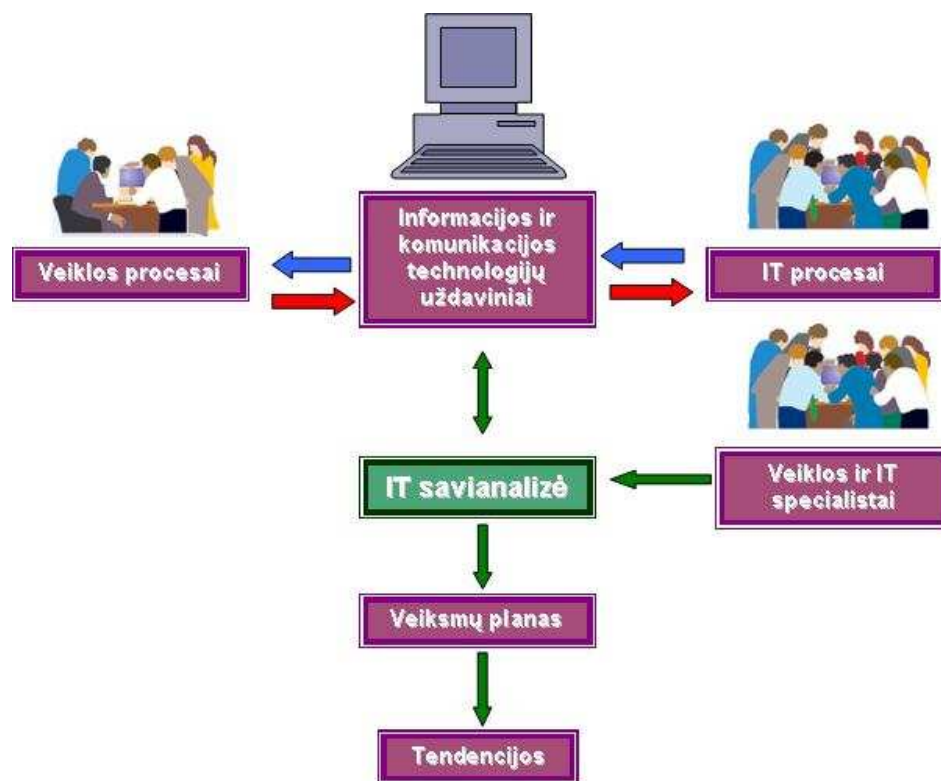
Trečiasis IT savianalizės etapas prasidėjo nuo 2.0 versijos išleidimo ir tęsiasi iki 2006 m. Darbo grupės siekis buvo, kad kuo daugiau Europos AAI išbandytų IT savianalizės metodiką ir pateiktų savo rezultatus, bei pačios savianalizės metodikos įvertinimą. Tokia informacija IT savianalizės projekto grupei labai svarbi tobulinant IT savianalizės metodiką.

Šiuo metu jau yra patvirtinta 4.0 IT savianalizės metodikos versija, bet apie tai plačiau bus aprašoma 4.5 paragrafe.

3.3 AAI sukurtos IT savianalizės įgyvendinimo etapai

Pagrindiniai savianalizės etapai pavaizduoti 7 schemeje.

⁵⁸ JAKIMAVIČIUS, Dainius, *ATASKAITA apie EUROSAI Informacinių technologijų darbo grupės 2-ąjį pasitarimą, vykusį 2004 m. kovo 29 - 30 d. Berne (Šveicarija), 2004, p. 2-4..*



7 schema. IT savianalizės metodas parengtas EUROSAI IT darbo grupės⁵⁹.

Pagal IT savianalizės 2.0 versijos metodiką IT savianalizės įgyvendinimas susideda iš pasiruošimo IT savianalizės seminarui ir 7 IT savianalizės įgyvendinimo etapų:

- 1 dalis: Įvadas
- 2 dalis: Pagrindiniai veiklos procesai ir informacinės technologijos
- 3 dalis: Informacinių technologijų procesų parinkimas ir įvertinimas
- 4 dalis: Pagrindinių atrinktų informacinių technologijų procesų brandos lygio įvertinimas
- 5 dalis: Priemonių plano parengimas
- 6 dalis: Įvertinimas
- 7 dalis: Baigiamasis pranešimas

Detaliau kiekvienas žingsnis aprašomas sekančiuose poskyriuose.

Pasiruošimas IT savianalizės seminarui

AAI nusprendusi atlikti IT savianalizę ir gavusi aukščiausios vadovybės sutikimą, pirmiausiai turi susitarti ir pasikviesti moderatorių. Šiuo metu yra 6 moderatoriai, galintys praveisti IT savianalizės seminarą. Labai didelis plusas, jei moderatorius gali kalbėti gimtąja AAI, kuri ruošiasi atlikti savianalizę, kalba. Jei tokios galimybės nėra, tada reikėtų rinktis tokią užsienio kalbą, kuri yra

⁵⁹IT Self-assessment [interaktyvus], Nyderlandai: 2005- [žiūrėta 2006 m. sausio 12 d.]. Prieiga per internetą: <<http://www.eurosai-it.org/9282201/v/index.htm>>.

priimtinausia AAI. Su moderatoriumi betarpiškam kontaktavimui turi būti paskirtas atstovas iš AAI. dažniausiai tokiu žmogumi būna paskiriamas IT skyriaus darbuotojas.

Tariantis su moderatorium tuo pačiu reikia suderinti IT savianalizės seminaro datą. Ją nustatant galima orientuotis į tai, kad pati IT savianalizė užtrunka apie 2 dienas. Nors kaip parodė praktika, tiek laiko kokybiškai atlikti savianalizę – mažoka.

Sekantis ir labai atsakingas veiksmas yra surinkti AAI darbuotojų grupę, kuri atstovautų skirtingas veiklos sritis. IT metodikoje rekomenduojama, kad grupė būtų sudaryta iš 8-12 žmonių. Dalyviai ne būtinai turi būti aukščiausio lygmens vadovai. Geriausiai kai parenkami AAI darbuotojai, kurie intensyviausiai naudojami informacinėmis technologijomis. Be abejonės į grupę turi būti įtraukti ir IT specialistai. Dalyvių sąrašas turi būti iš anksto persiunčiamas moderatoriui, kad jis galėtų patikrinti ar grupė tinkamai suformuota IT savianalizei atlikti.

Metodikoje rekomenduojama, kad ir pats moderatorius prieš kiekvieną savianalizę perskaitytų IT savianalizės metodiką, pasiruoštų prezentacijos skaitymui ir pasiruoštų darbines lenteles. Moderatorius iš anksto prieš IT savianalizės seminarą turi persiųsti reikiamą medžiagą kontaktiniam AAI asmeniui.

IT savianalizės dalyvių grupės nariai prieš savianalizę irgi turi savarankiškai, kiek įmanoma daugiau, pasiruošti. Reikiamą medžiagą turi padalinti AAI atstovas atsakingas už IT savianalizės įgyvendinimą:

- IT savianalizės metodika (su visomis formomis, kurios bus naudojamos savianalizės metu).
- Reikiamas COBIT dalis.

Atsakingas asmuo turi pasirūpinti ir tokiais organizaciniais dalykais, kaip patalpomis tinkamomis seminarui vesti, paruošti 2 nešiojamus kompiuterius, projektorių, rašymo lentą, atspausdinti padalinamąją įvadinės prezentacijos medžiagą, tuščių formų kopijas ir apklausos anketas.

1 dalis – įvadas

Įvadas dažniausiai rengiamas pirmąją savianalizės dieną, bet jei yra galimybė, tai geriau savianalizės dalyviams įvadinės žiniais suteikti bent vieną savaitę prieš IT savianalizės įgyvendinimą. Įvadas užtrunka apie 1 val.

Moderatorius įvadinės dalies metu supažindina dalyvius su IT savianalizės raida, ankstesnių IT savianalizėjų rezultatais ir patirtimi. Ypatingai moderatorius turi pabrėžti, kodėl AAI turi atlikti IT savianalizę ir kodėl kaip pagrindas naudojamas COBIT. Įvadinėje dalyje dalyviai supažindinami su tolimesne IT savianalizės eiga. AAI atstovai taip pat pasidalina savo IT patirtimi, išsako turimas problemas ir esamą situaciją.

2 dalis – pagrindiniai veiklos procesai ir informacinės technologijos

IT savianalizės etapas „Pagrindiniai veiklos procesai ir informacinės technologijos“ susideda iš šių žingsnių:

1. Įvadas. Moderatorius supažindina seminaro dalyvius su etapo „Pagrindiniai veiklos procesai ir informacinės technologijos“ veiksmų eiga. Pristato BVC (angl. *Business Value Chain*) formą ir apmoko, kaip ją užpildyti. BVC forma susideda iš penkių stulpelių (2 pav.). Trečiame stulpelyje reikia surašyti pirminius ir antrinius AAI veiklos procesus ir juos įvertinti pagal BVC formoje nurodytus kriterijus.

BVC forma – išeginiai duomenys Informacinių technologijų procesų atrankai.

Kokia yra dabartinis IT sistemų svarbos lygis atitinkamam veiklos procesui?					Kokia bus ateities IT sistemų svarbos lygis atitinkamam veiklos procesui?					Forma 1. Veiklos procesų grandinė (angl. <i>Business added-value chain (BVC)</i>). Ar IT padeda AAI siekti strateginių tikslų? <small>versija 2.1</small>					Kokia yra dabartinių IT sistemų kokybė?					Kuris IT-procesas (žiūrėti Formoje 2) sukelia problemas (ypač jei kokybės lygis = 0 arba 1)?			
nėra taikomųjų programų (0) Zemas (1) Svarbos lygis (2) Svarbos lygis (3) Svarbos lygis (4) aukštas (5)					nėra taikomųjų programų (0) Zemas (1) Svarbos lygis (2) Svarbos lygis (3) Svarbos lygis (4) aukštas (5)										labai žema (0) Kokybės lygis (1) Kokybės lygis (2) Kokybės lygis (3) Kokybės lygis (4) labai aukšta (5)								
										V1	Audito rizikos valdymas												
										V2	Audito planavimas												
										V3	Duomenų analizavimas												
										V4	IS auditas												
										V5	Audito ataskaitos rengimas												
										V6	Rekomendacijų įgyvendinimas												
										V7	Informacijos ir žinių valdymas												
										V8	Finansų ir personalo valdymas												
										V9	Teisinė pagalba												
										V10	Audito rezultatų publikavimas												
										V11	Komunikavimas												
										V12	Kita ...												
										V13	Kita ...												

1 pav. BVC forma⁶⁰.

2. Veiklos procesų sąrašo sudarymas. Diskutuodami IT savianalizės dalyviai sudaro AAI veiklos procesų sąrašą ir suskirsto juos į pirminius ir antrinius. Palengvinimui metodikoje yra pateikiamas tokio sąrašo pavyzdys. Sudarytas veiklos procesų sąrašas surašomas į BVC formą, kuri atspausdinama ir išdalinama seminaro dalyviams.

⁶⁰ EUROSAT IT Working Group, *A methodology for IT self-assessment by SAI's*. Version 2.0, Bern: 2004, P. 45.

3. *Supažindinimas su informacinių technologijų procesais.* Šio žingsnio tikslas – supažindinti IT savianalizės dalyvius su COBIT išskiriamais 34 IT procesais. Šiame darbe jie buvo pristatyti skyriuje „COBIT samprata“.

4. *Informacinių technologijų procesų įtakos veiklos procesams lygio įvertinimas.* IT savianalizės dalyviai individualiai užpildo visą BVC formą ir tada pereinama prie šių žingsnių:

- Suskaičiuoti kiekvieno proceso vidutinės reikšmės.
- Darbas grupėje:
- Pasiiekti bendrą sutarimą dėl IT įtakos veiklos procesams.
- Dokumentuoti tai įrodančius faktus.
- Nustatyti kritinius susietus IT procesus.

IT savianalizės etapui „Pagrindiniai veiklos procesai ir informacinės technologijos“ atlikti metodikoje numatytas laikas – 75 min.

3 dalis – informacinių technologijų procesų atrinkimas ir įvertinimas

Informacinių technologijų procesų parinkimo ir įvertinimo etape pagrindinis tikslas – labiausiai kritinių IT procesų atranka. Atrinkamų procesų skaičius turi būti ribotas. Nors dalyviai prieš savianalizės seminarą savarankiškai turi išstudijuoti IT procesus, bet prieš pradėdant IT procesų vertinimą, būtina, kad moderatorius dar kartą IT savianalizės dalyviams detaliai pristatytų COBIT 34 IT procesus. Metodikoje rekomenduojama, kad atrinktų IT procesų skaičius neturi būti daugiau kaip 15. Šis etapas susideda iš trijų žingsnių:

- Kiekvieno IT proceso svarbos individualus vertinimas. IT procesų įvertinimui naudojama COBIT forma (2 pav.). Vertinimai (nuo 0 iki 2) surašomi pirmajame COBIT formos stulpelyje.
- Statistika : vidutinės reikšmės.
- Darbas grupėje : susitarti dėl 15 pačių svarbiausių IT procesų.

Atrinkti kritiškiausi IT procesai naudojami dviejuose sekančiuose IT savianalizės įgyvendinimo etapuose.

IT savianalizės etapui „Informacinių technologijų procesų atrinkimas ir įvertinimas“ atlikti metodikoje numatytas laikas – 90 min.

IT procesų svarbos lygis					COBIT forma 2: Koks yra IT procesų brandos lygis? versija 2.1					Dabartinis IT proceso brandos lygis					Siekiamas IT proceso brandos lygis						
Nežinau	Visškai nesvarbus (1)	Svarbumo lygis (2)	Svarbumo lygis (3)	Labai svarbus (5)	COBIT domenai ir procesai					nesantis (0)	pradinis (1)	kartotinis (2)	apibrėžtas (3)	valdomas (4)	optimizuotas (5)	nesantis (0)	pradinis (1)	kartotinis (2)	apibrėžtas (3)	valdomas (4)	optimizuotas (5)
COBIT domenai ir procesai																					
Planavimas ir Organizavimas																					
					P01	Apibrėžti strateginį IT planą															
					P02	Apibrėžti informacinę architektūrą															
					P03	Pasirinkti technologinę kryptį															
					P04	Apibrėžti IT organizacinę struktūrą ir veiksmus															
					P05	Kontroliuoti IT investicijas															
					P06	Komunikuoti vadovybės tikslus ir kryptį															
					P07	Valdyti žmogiškuosius resursus															
					P08	Užtikrinti išorinių reikalavimų vykdymą															
					P09	Įvertinti riziką															
					P010	Valdyti IT projektus															
					P011	Kontroliuoti kokybę															
Pirkimai ir įdiegimas																					
					A11	Automatizavimo sprendimų paieška															
					A12	Įsigyti ir prižiūrėti taikomąją programinę įrangą															
					A13	Įsigyti ir prižiūrėti technologinę infrastruktūrą															
					A14	Sukurti ir atnaujinti IT naudojimo procedūras															
					A15	Įdiegti ir akredituoti sistemas															
					A16	Kontroliuoti IT sistemų pokyčius															
Naudojimas ir aptarnavimas																					
					DS1	Apibrėžti ir užtikrinti IT paslaugų lygį															
					DS2	Kontroliuoti trečiųjų šalių teikiamas paslaugas															
					DS3	Kontroliuoti sistemų pajėgumus ir apkrovą															
					DS4	Užtikrinti nuolatinį sistemų funkcionavimą															
					DS5	Užtikrinti sistemų saugumą															
					DS6	Identifikuoti ir paskirstyti IT kaštus															
					DS7	Apmokėti vartotojus															
					DS8	Teikti pagalbą vartotojams															
					DS9	Kontroliuoti sistemų konfigūraciją															
					DS10	Sėkti, spręsti problemas ir skundus															
					DS11	Prižiūrėti duomenis															
					DS12	Prižiūrėti patalpas kuriose yra įranga															
					DS13	Kontroliuoti kasdien sistemų naudojimą															
Monitoringas																					
					M1	Stebėti procesus															
					M2	Įvertinti vidinės kontrolės adekvatumą															
					M3	Užtikrinti trečiųjų šalių audito garantą															
					M4	Organizaciškai remti audito procesą															

2 pav. COBIT forma⁶¹.

4 dalis – pagrindinių atrinktų informacinių technologijų procesų brandos lygių įvertinimas

Pagrindinių atrinktų informacinių technologijų procesų brandos lygių įvertinimo tikslas – nustatyti atrinktų svarbiausių IT procesų brandos lygius. Tai bus pagrindas IT strateginio valdymo gerinimui. Šiame etape turi būti atlikta:

- Supažindinimas su brandos lygiais.
- Brandos lygių nustatymas:
- Individualus kiekvieno IT proceso brandos lygio nustatymas

⁶¹ EUROSAT IT Working Group, *A methodology for IT self-assessment by SAI's*. Version 2.0, Bern: 2004, P. 46.

- Rezultatų statistika
- Darbas grupėje: bendras sutarimas ir įrodymai

Brandos lygių vertinimas atliekamas naudojantis COBIT, kuriame išskiriami šeši brandos lygiai (3 pav.): 0 – nesantis; 1 – pradinis; 2 – kartotinis; 3 – apibrėžtas; 4 – valdomas; 5 – optimizuotas.



3 pav. Brandos lygiai⁶².

COBIT brandos lygiai aprašomi atskirai, kiekvienam iš 34 procesų, bet galima remtis ir bendru IT brandos lygių aprašymu⁶³:

0. Nesantis:

- (a) Organizacija nepripažįsta spęstinios problemos egzistavimo ir dėl to apie tai nepateikia jokios informacijos.
- (b) Šiuo klausimu nėra jokios politikos.
- (c) Nėra jokio atpažįstamo proceso, susijusio su šia problema.
- (d) Neatliekamas joks vertinimas, susijęs su šia problema.

1. Pradinis:

- (a) Yra faktų, patvirtinančių, kad organizacija pripažįsta problemos egzistavimą ir būtinumą ją spręsti, tačiau apie tai per mažai informuojama.

⁶² IT Governance Institute, COBIT 3rd edition, USA, 2000.

⁶³ Europos Komisijos 1995-07-07 reglamento Nr. 1663/95, nustatančio išsamias Tarybos reglamento (EEB) Nr. 729/70 dėl EŽŪOGF Garantijų skyriaus sąskaitų apmokėjimo tvarkos taikymo taisykles, priedas – Informacinių sistemų saugumo gairėmis.

(b) Egzistuoja neišsami politika. Ji netinkamai dokumentuojama, skelbiama arba įgyvendinama.

(c) Individualiu arba kiekvienu konkrečiu atveju taikomi *ad hoc* metodai. Problema nenagrinėjama valdybos lygiu.

(d) Stebėseną vykdoma reaguojant į incidentą, dėl kurio organizacija patiria tam tikrą nuostolį.

2. Kartotinis:

(a) Apie problemą (prireikus) atitinkamai informuojama visa organizacija.

(b) Egzistuoja aiški politika.

(c) Su problema susiję procesai formaliai yra nustatyti, aktyviai dalyvaujant ir prižiūrint vadovybei, tačiau taikomi ne visoje organizacijoje. Mokymas neorganizuojamas, o informavimas apie standartus ir pareigas paliktas individualių darbuotojų nuožiūrai.

(d) Vadovybė yra nustačiusi pagrindinius vertinimus ir vertinimo metodus bei būdus, tačiau pastarieji parengti nepakankamai.

3. Apibrėžtas:

(a) Visa organizacija supranta, kad reikia reaguoti į problemą, ir tam pritaria.

(b) Organizacijoje vykdoma tvirta ir aiški politika, suderinta su kai kuriomis kitomis susijusiomis politikos kryptimis. Iš dalies atsižvelgiama į rizikos valdymą.

(c) Procedūros standartizuotos, dokumentuotos ir dauguma jų įgyvendinamos visoje organizacijoje. Vadovybė yra informavusi apie standartizuotas procedūras ir vykdo neformalų mokymą. Nors procedūras galima įvertinti, tačiau jos nėra sudėtingos ir formaliai atspindi esamą patirtį.

(d) Susijusių veiklos sričių rodiklių registravimas ir stebėseną padeda tobulinti veiklą. Beveik visų susijusių procesų stebėseną vykdoma pagal tam tikrus (pirminius) dokumentus, tačiau mažai tikėtina, kad vadovybė galėtų pastebėti bet koki nukrypimą, kadangi tokios priemonės paprastai taikomos individualiai. Priežasčių analizė atliekama retai.

4. Valdomas:

(a) Visais atitinkamais organizacijos lygiais problema suprantama tinkamai ir reikalaujama imtis priemonių.

(b) Vykdoma tvirta ir aiški politika, integruota su kitomis susijusiomis politikos kryptimis. Atsižvelgiama į rizikos valdymą.

(c) Organizacija gerai pažįsta savo klientą ir turi aiškiai apibrėžtas pareigas. Procesai yra aiškiai suformuluoti, integruoti ir taikomi visoje organizacijoje. Procesai yra gerai įsisavinami ir palaikomi organizuojant atitinkamą mokymą. Visi susijusių procesų dalyviai žino apie riziką ir galimybes.

(d) Susijusių procesų tobulinimas visų pirma yra pagrįstas kiekybiniu supratimu, užtikrinant galimybę stebėti ir vertinti, kaip laikomasi procedūrų bei susijusių procesų dokumentų reikalavimų. Vadovybė yra nustatiusi leistinus nukrypimus, į kuriuos būtina atsižvelgti, vykdant susijusius procesus. Paaiškėjus, kad procesai yra neveiksmingi arba neefektyvūs, dažniausiai, tačiau ne visada, imamasi priemonių. Kartais susiję procesai tobulinami, įgyvendinant geriausią vidaus praktiką. Vykdomas priešasčių analizės standartizavimas. Pradedamas nuolatinis veiklos gerinimo procesas.

5. Optimizuotas:

(a) Problemos ir jos sprendimo būdų vertinimas yra pažangus bei perspektyvus.

(b) Organizacija vykdo tvirtą ir aiškią politiką, integruotą su visomis kitomis susijusiomis politikos kryptimis, visapusiškai atsižvelgiant į rizikos valdymą.

(c) Susiję procesai atnaujinti, atsižvelgiant į geriausią išorinę praktiką ir nuolatinio veiklos tobulinimo bei brandos modeliavimo rezultatus kitose organizacijose. Susijusių procesų rizika ir rezultatai yra apibrėžti, suderinti, ir apie juos informuojama visa organizacija. Organizuojamas modernus mokymas ir informavimas. Įgyvendinama politika užtikrino organizacijos, darbuotojų ir procesų sugebėjimą greitai prisitaikyti ir visapusiškai palaikyti rizikos struktūros pokyčius.

(d) Stebėseną, savęs vertinimą ir informavimą apie problemą (prireikus) vykdomi visos organizacijos lygiu, optimaliai išnaudojant procesus ir technologijas, naudojamus vertinimo, analizės, informavimo ir mokymo tikslais. Analizuojamos visų problemų ir nukrypimų priežastys, laiku numatant ir inicijuojant veiksmingas priemones. Naudojamasi nepriklausomų ekspertų konsultavimo paslaugomis ir lyginamąja analize.

Vertinant IT procesų brandą nustatoma ne tik esama branda, bet ir norima. Jei esamos ir norimos IT procesų brandos rezultatai sutampa, tokiu atveju nieko toliau daruti nereikia. Tačiau, jei norima branda yra didesnė už esamą, tada surašomos problemos/spragos, kurios trukdo pasiekti norimos brandos. Išrašytos problemos/spragos naudojamos sudarant veiksmų planą.

IT savianalizės etapui „Pagrindinių atrinktų informacinių technologijų procesų brandos lygių įvertinimas“ atlikti metodikoje numatytas laikas – 90 min.

5 dalis – veiksmų plano parengimas

Veiksmų plano parengimas yra esminis IT savianalizės etapas, kuris susideda iš šių žingsnių:

- Įvadas. Moderatorius pristato veiksmų plano formą į kurią jau turi būti sukeltos ankstesniame etape nustatytos problemos/spragos. Veiksmų plano forma susideda iš 6 stulpelių: Gauta problema/spraga; padariniai/rizika; Rekomendacija/veiksmas; Atsakingas asmuo; Priemonės įgyvendinimo terminas; Prioritetas. Sekančių žingsnių metu užpildomi visi veiksmų plano formos stulpeliai:
- Išanalizuoti 4-oje dalyje nustatytas problemas/spragas.
- Nustatyti galimus padarinius/rizikas, t.y. kas gali nutikti AAI jei problema nebus sprendžiama.
- Kiekvienai problemai parengti galimus jos/jų sprendimus, o galimus sprendimus apjungti į projektus.
- Numatyti atsakingus asmenis kiekvienos priemonės įgyvendinimui.
- Apibrėžti priemonės įgyvendinimo terminą.
- Kiekvienam projektui/priemonei nustatyti prioritetus.

IT savianalizės etapui „Pagrindinių atrinktų informacinių technologijų procesų brandos lygių įvertinimas“ atlikti metodikoje numatytas laikas – 60 min.

6 dalis – įvertinimas

Kiekvienas dalyvis turi užpildyti klausimyną apie IT savianalizės seminaro eigą (1 priedas). Atsakymai labai svarbūs IT savianalizės metodikos autoriams tobulinant IT savianalizės metodiką. IT savianalizės įvertinimo etape dalyviai gali ir žodžiu išsakyti savo nuomonę apie įgytą patirtį IT savianalizės seminaro metu. Taip pat išrenkamas atstovas, kuris sekančiame etape pristatys gautus rezultatus AAI vadovybei.

IT savianalizės etapui „Įvertinimas“ atlikti metodikoje numatytas laikas – 30 min.

7 dalis – baigiamasis pranešimas

AAI vadovybė ir visi norintys darbuotojai pakviečiami susipažinti su IT savianalizės seminaro metu gautais rezultatais ir veiksmų planu. Taip pat supažndinama su IT savianalizės nauda ir aptariamia tolimesni žingsniai.

IT savianalizės etapui „Baigiamasis pranešimas“ atlikti metodikoje numatytas laikas – 60 min.

3.4 Skyriaus apibendrinimas

EUROSAI IT darbo grupės 1-me pasitarime, vykusiam 2002 m. rugsėjo 30 d. – spalio 1 d. Hagoje (Nyderlandai) buvo sudaryta projekto grupė parengti metodiką, pagal kurią Aukščiausiosios audito institucijos galėtų naudoti informacinių sistemų audito COBIT standartą, savarankiškai atlikdamos IT savianalizę. Metodikos išbandymui ir supažindinimui buvo numatyti ir įgyvendinti bandomieji IT savianalizės seminarai AAI - EUROSAI Informacinių technologijų darbo grupės narėse. Vėliau, 3-jame darbo grupės posėdyje, vykusiam 2005 m. vasario 14 - 15 d. Nikosijoje (Kipras), daugumai dalyvių pritarus, – ir kitose Aukščiausiose audito institucijose, EUROSAI narėse.

IT savianalizės projekto grupėje dalyvauja šešios AAI - EUROSAI IT darbo grupės narės:

- Šveicarijos federalinė audito įstaiga
- Ispanijos audito rūmai
- Lietuvos Respublikos valstybės kontrolė
- Nyderlandų audito rūmai
- Norvegijos generalinio auditoriaus įstaiga
- Slovėnijos audito rūmai

IT savianalizės įgyvendinimas susideda iš pasiruošimo IT savianalizės seminarui ir 7 IT savianalizės įgyvendinimo etapų:

1 dalis: Įvadas

2 dalis: Pagrindiniai veiklos procesai ir informacinės technologijos

3 dalis: Informacinių technologijų procesų parinkimas ir įvertinimas

4 dalis: Pagrindinių atrinktų informacinių technologijų procesų brandos lygio įvertinimas

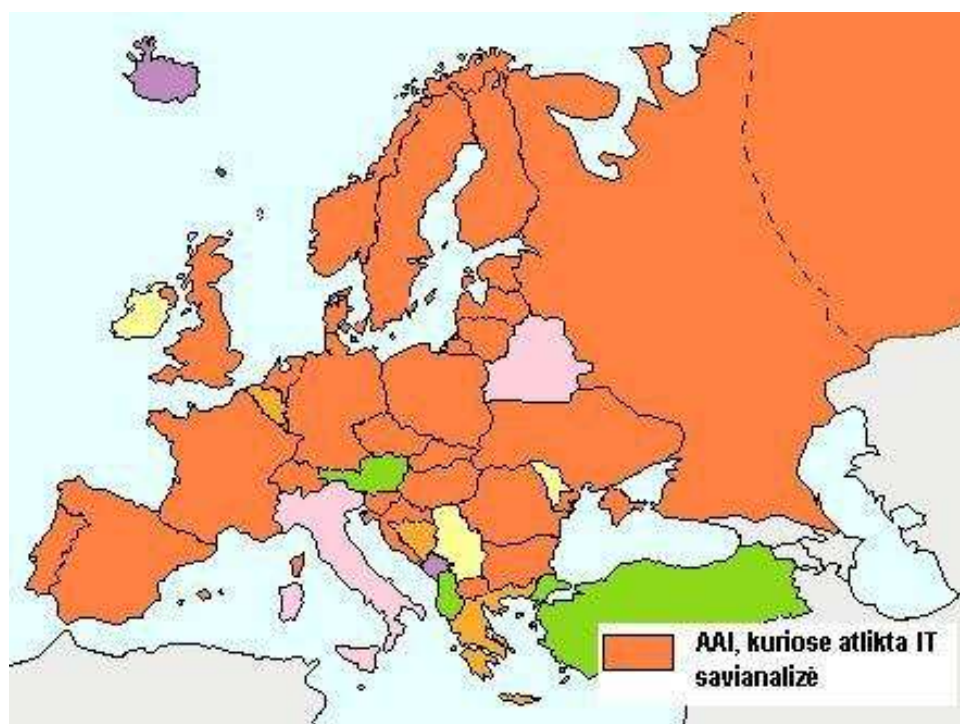
5 dalis: Priemonių plano parengimas

6 dalis: Įvertinimas

7 dalis: Baigiamasis pranešimas

4. IT SAVIANALIZĖS METODIKOS TAIKYMAS AUKŠČIAUSIOSE AUDITO INSTITUCIJOSE

Šiuo metu informacinių technologijų savianalizės seminarai jau yra įvykę 26 EUROSAI Aukščiausiose audito institucijose⁶⁴ (4 pav.). Kituose trijuose paragrafuose detaliau bus apžvelgiami IT savianalizės seminarai vykę Latvijoje, Lietuvoje ir Ukrainoje, nes juose moderatoriaus pareigą atliko pati šio darbo autorė.



4 pav. EUROSAI Aukščiausiose audito institucijos, kuriose jau įvyko IT savianalizės seminarai: Bulgarija, Kroatija, Čekija, Danija, Estija, Europos Audito rūmai, Suomija, Prancūzija, Vokietija, Vengrija, Lietuva, Latvija, Lenkija, Makedonija, Malta, Norvegija, Portugalija, Rumunija, Rusija, Slovėnija, Slovakija, Ispanija, Šveicarija, Švedija, Nyderlandai, Jungtinė Karalystė, Ukraina⁶⁵.

4.1 IT savianalizės seminarai Lietuvos Respublikos valstybės kontrolėje

2003 metų spalio mėnesį Lietuvos Respublikos valstybės kontrolėje buvo surengtas pilotinis IT savianalizės seminaras. Tai buvo pirmasis projekto grupės atliktas seminaras. Jame dalyvavo devyni Valstybės kontrolės darbuotojai iš skirtingų veiklos sričių, tame tarpe du žmonės iš IT departamento.

⁶⁴ HUISSOUD Michel, *So you like IT self assessments?*, Bratislava 2006.

⁶⁵ Sukurta darbo autoriaus.

Seminaro dalyvių žinios apie savianalizės metodiką bei COBIT buvo neaukšto lygio. Be to, seminaras truko tik nepilnas dvi dienas viena po kitos. Tiek laiko, kaip parodė Lietuvos ir kitų šalių praktika yra ištis per mažai, kad įgyti pakankamai teorinių žinių, suvokti jų esmę bei gebėti pritaikyti praktikoje.

Savianalizės seminaro metu buvo išskirti pagrindiniai IT procesai ir nustatytas jų brandos lygis. Nustačius pagrindinių IT procesų brandos lygį, išsiaiškinta, kad pagrindinės problemos kylančios iš IT procesų. Nustačius pagrindines su IT procesais susijusias problemas buvo sudarytas veikslių planas.

IT plėtra Lietuvos Respublikos valstybės kontrolėje po pirmojo IT savianalizės seminaro:

- VK Strateginio valdymo ir rizikų valdymo komisijos sudarymas, IT – viena iš 7 rizikos valdymo sričių (2003 m. lapkritis);
- VK Informacinių technologijų strateginio plėtros plano Priemonių įgyvendinimo plano patvirtinimas VK Taryboje (2004 m. sausis);
- VK Informacinių technologijų valdymo komiteto sudarymas (2004 m. vasaris);
- Pritarta naujos VK informacinės sistemos kūrimo metmenims (2004 m. kovas);
- Įsteigta darbo grupė VK Audito valdymo ir dokumentavimo sistemos vartotojų poreikiams nustatyti (2004 m. gegužė);
- Paskelbtas konkursas VK Audito valdymo ir dokumentavimo sistemai sukurti (2005 m. balandis);
- Pasirašyta sutartis dėl VK Audito valdymo ir dokumentavimo sistemos sukūrimo (2005 m. spalio), gautos TeamMate licencijos.

Vienas iš pagrindinių nustatytų spęstinų uždavinių – tai geresnis veiklos padalinių įtraukimas į informacinių technologijų strateginių tikslų formavimą. Tokiu būdu, Valstybės kontrolės informacinių technologijų strategija turėtų ne tik siūlyti pažangių technologijų galimybių diegimą Valstybės kontrolės veiklos procesuose, tačiau ir labiau remtis veiklos padalinių suformuotais poreikiais. Šiam uždaviniui spręsti 2004 m. vasario mėn. buvo įsteigtas Informacinių technologijų komitetas, kurio pagrindinės funkcijos yra šios:

- analizuoja ir peržiūri Valstybės kontrolės Informacijos valdymo departamento strateginius ir operacinius planus, kad būtų užtikrintas jų suderinamumas su Valstybės kontrolės strateginiais planais bei prioritetiniais informaciniais poreikiais;
- analizuoja Valstybės kontrolės informacinius poreikius, nustato informacinių sistemų prioritines plėtros kryptis;
- svarsto informacinių sistemų plėtros projektus ir teikia siūlymus valstybės kontrolieriui dėl jų tvirtinimo;
- nustato svarbiausius kompiuterinės ir programinės įrangos pirkimus, neviršijant šiam tikslui metinėse išlaidų sąmatose nustatytų lėšų;

- stebi ir teikia siūlymus informacinių sistemų plėtros projektų įgyvendinimo eigos⁶⁶.

Informacinių technologijų komiteto įsteigimas buvo reikšmingas žingsnis, gerinant Valstybės kontrolės IT valdymą, nustatant Valstybės kontrolės veiklos poreikius ir susiejant juos su IT teikiamomis galimybėmis.

2006 m. gegužės mėnesį LR valstybės kontrolėje buvo surengtas antrasis IT savianalizės seminaras. Pabrėžtina, kad tai pirmoji AAI, kuri antrą kartą nusprendė įsivertinti savo IT valdymą pasinaudojant IT savianalizės metodika.

Antrasis IT savianalizės seminaras vyko pagal tokį grafiką:

- Parengiamasis seminaras. Tema: „Supažindinimas su aukščiausiųjų audito institucijų informacinių technologijų savianalizės metodika ir praktika“ – 2006 m. gegužės 2 d.
- Pagrindinis seminaras. Tema: „Valstybės kontrolės veiklos procesų nustatymas“ – 2006 m. gegužės 4 d.
- Pagrindinis seminaras. Tema: „Valstybės kontrolės informacinių technologijų brandos įvertinimas ir prioritetinių informacinių technologijų plėtros kryptių nustatymas; Veiksmų plano sudarymas“ – 2006 m. gegužės 11 d. – 12 d.

Darbo grupę sudarė dvylika atstovų iš audito, audito plėtros, informacinių technologijų ir informacijos valdymo veiklos sričių. Kai kurie dalyviai jau turėjo patirties iš pirmosios IT savianalizės seminaro.

Antrojo informacinių technologijų savianalizės seminaro, vykusio 2006 m. gegužės mėn., metu, buvo analizuojami pagrindiniai įstaigos veiklos procesai (Priedas 1), nustatytas jų ryšys su informacinių technologijų COBIT procesais, įvertintas esamas ir siektinas svarbiausiųjų COBIT procesų brandos lygis. Nustatyti trūkumai, kuriuos pašalinus būtų galima siekti norimo (aukštesnio) informacinių technologijų COBIT brandos lygio. Nustačius pagrindines su IT procesais susijusias problemas buvo sudarytas veiksmų planas, kuriuo remiantis 2006 m. buvo parengtas ir patvirtintas antrasis Lietuvos Respublikos valstybės kontrolės Informacinių technologijų strateginis plėtros planas.

Išanalizavus ir apibendrinus klausimyno apie IT savianalizės įgyvendinimą dalyvių atsakymus paaiškėjo, kad 36 % IT savianalizės seminaro dalyvių anksčiau jau buvo dalyvavę panašiam renginyje, tačiau daugiau kaip 60 % dalyvių daugiau ar mažiau buvo susipažinę su COBIT metodika. Daugumos Lietuvos Respublikos valstybės kontrolės darbuotojų dalyvavusių antrajame IT savianalizės seminare nuomone, seminaro dalyvių grupė buvo tinkamai suformuota, bet buvo pasigesta atstovų iš personalo valdymo skyriaus, turto valdymo departamento ir savivaldybes audituojančių auditorių atstovų.

Iš atsakymų į klausimą „Kaip Jūs manote ar Jums pakako medžiagos ir pagalbos/paiškinimų (prieš IT savianalizės seminarą ir jo eigoje), reikalingų sėkmingam IT savianalizės įgyvendinimui?“

⁶⁶ VK įsakymas dėl IT valdymo komiteto

galima pastebėti, kad didžiajai daugumai dalyvių (daugiau kaip 70 %) pakako metodinės medžiagos ir moderatoriaus pagalbos. Tačiau keletas nusiskundimų buvo, kad pritrūko paaiškinimo apie IT procesus. BVC formoje kilo neaiškumų, kokia prasmė yra nustatinėjant IT svarbą ateityje. O bendrai paėmus tiek BVC tiek, tik COBIT formoje trūksta paaiškinimų dėl terminų paaiškinimo ir gautų rezultatų naudos.

Jei Lietuvos Respublikos valstybės kontrolėje būtų dar kartą kartojamas IT savianalizės seminaras, reikėtų daugiau laiko skirti seminaro pasiruošimui, t.y. susipažinti su IT savianalizės metodika ir detaliau išstudijuoti COBIT procesus. Kadangi daug laiko užėmė rezultatų skaičiavimas, reikėtų patobulinti Excel lenteles.

Lietuvos Respublikos valstybės kontrolės antrasis IT savianalizės seminaras patenkino daugumos dalyvių lūkesčius. Be to tai buvo gera praktika dar kartą pritaikyti IT savianalizės metodiką ir įgyti žinių apie COBIT, o diskusijų metu kitų sričių atstovai sužinojo daugiau apie IT darbuotojų veiklą. Gauti rezultatai ir sudarytas veiksnių planas ypač pasitarnavo rengiant Lietuvos Respublikos valstybės kontrolės Informacinių technologijų strateginis plėtros planą 2006-2011 metams.

Lietuvos Respublikos valstybės kontrolės antrasis IT savianalizės seminaro dalyviai išskyrė šiuos privalumus:

- Galimybė išsiaiškinti IT poreikius, kurie padėtų efektyviau įgyvendinti Lietuvos Respublikos valstybės kontrolės uždavinius.
- IT valdymas peržiūrimas visos institucijos mastu, todėl galima atrasti beveik visas IT strateginio valdymo spragas.
- Galimybė sulygtinti gautus rezultatus su kitomis AAI.
- Galimybė numatyti pasikeitimus susijusius su IT.

Trūkumai:

- Dalyviai turi turėti aukštą žinių lygį IT ir COBIT srityje.
- Seminare dalyvaujant vien saviems darbuotojams yra rizika, kad kai kurios problemos bus nutylėtos.
- Trūksta detalesnio kiekvieno IT savianalizės etapo aprašymo.

Lietuvos Respublikos valstybės kontrolės IT savianalizės seminaro dalyviai vienbalsiai patvirtino, kad IT savianalizės metodika yra efektyvus IT valdymo įrankis ir tokius seminarus būtina reikėtų kartoti ateityje.

4.2 IT savianalizės seminaras Latvijos Respublikos valstybės kontrolėje

IT savianalizės seminaras, vykęs 2005 m. rugsėjo 28d. ir 2005 m. spalio 10 - 12 d. Latvijos Respublikos valstybės kontrolėje, yra įsipareigojimo, kaip vienos iš EUROSAI IT darbo grupės narės,

įvykdymas. Dainius Jakimavičius ir šio darbo autorė buvo pakviesti vadovauti IT savianalizės seminarui kaip vienos iš šešių šalių (Šveicarija, Ispanija, Lietuva, Nyderlandai, Norvegija, Slovėnija) aukščiausiųjų audito institucijų, dirbusių IT savianalizės metodikos srityje atstovai (moderatoriai).

IT savianalizės metodika numato, kad seminaras turėtų trukti ne mažiau 2 dienų, gali būti ir 3 dienos; be to, turi būti numatytas laikas seminaro dalyviams susipažinti su metodikoje aptariama medžiaga, ypač su COBIT „Valdymo gairėmis“ (angl. *Management Guidelines*). Todėl, esant galimybei, siūloma surengti įvadinį seminarą likus 10-14 dienų iki pagrindinio seminaro. Atskyrus grynai teorinę dalį, kuri yra išdėstoma įvadinio seminaro metu, seminaro dalyviams lieka pakankamai laiko pasirengti darbui, kuris vyksta pagrindinės praktinės seminaro dalies metu. Šia galimybe buvo pasinaudota seminaro Latvijos Respublikos valstybės kontrolėje metu, įvadinį (teorinį) seminarą surengiant 2005 m. rugsėjo 28 d. (trečiadienį), pagrindinį (praktinį) – 2005 m. spalio 10-12 d.

Seminaro darbotvarkė buvo tokia:

1. Įvadinis seminaras, 2005-09-28: Skaityti pranešimai temomis:

- supažindinimas su EUROSAI Informacinių technologijų darbo grupe, jos veikla ir vykdomais projektais;
- supažindinimas su pagrindiniais charakteringais aukščiausiųjų audito institucijų veiklos procesais, informacinių technologijų poveikiu šiems procesams, taip pat informacinių technologijų valdymo uždavinio išskaidymo į 34 pagrindines valdymo sritis (pagal COBIT) ir šių sričių esamo bei siekiamo brandos lygio nustatymo metodais;
- informacinių technologijų projektų sudarymas, panaudojant siekiamo ir esamo informacinių technologijų brandos lygių skirtumus; suformuotų projektų prioritetų nustatymas.

2. Praktinis seminaras, 2005-10-10 (pirmoji diena): Latvijos valstybės kontrolės darbo grupės atliekamos užduotys:

- Latvijos valstybės kontrolės veiklos procesų sąrašo sudarymas, esminių veiklos procesų išrinkimas, veiklos procesų sąrašo sutvarkymas pagal svarbą;
- IT procesų sąrašo sudarymas, šio sąrašo sutvarkymas pagal atskirų COBIT procesų svarbą Latvijos valstybės kontrolės veiklai;
- IT procesų sąrašo sudarymas, įvertinant kiekvieno išrinkto veiklos proceso sąryšio svarbą su konkrečiu COBIT procesu; šio sąrašo sutvarkymas pagal kiekvieno iš jų atitikimų veiklos procesams skaičių;
- šių dviejų sąrašų aptarimas ir palyginimas, bendro COBIT procesų sąrašo sudarymas, pasinaudojant sąrašais, kurie buvo gauti dviem aukščiau paminėtais būdais.

3. Praktinis seminaras, 2005-10-11 (antroji diena): Latvijos valstybės kontrolės darbo grupės atliekamos užduotys:

- bendro COBIT procesų sąrašo analizė: kiekvieno proceso esamo brandos lygio nustatymas pagal COBIT vertinimo metodiką, identifikavimas tų metodikos pagalba nustatytų trūkumų, kurie trukdo pereiti į aukštesnę (siekiamą) brandos lygį;
- veiksmų plano sudarymas, remiantis atskirais esamais ir siektiniais informacinių technologijų valdymo (pagal COBIT) brandos įvertinimais, projektų prioritetų nustatymas ir jų įgyvendinimo rizikos vertinimas.

4. Praktinis seminaras, 2005-10-12 (trečioji diena): Latvijos valstybės kontrolės darbo grupės atliekamos užduotys:

- sudaryto veiksmų plano aptarimas;
- IT savianalizės klausimyno užpildymas⁶⁷.

Kiekvienas IT savianalizės seminaras yra skirtingas ir suteikia daug informacijos, kuri yra naudinga tolimesniam savianalizės metodikos tobulinimui ir seminarų organizavimui.

Seminaras Latvijos valstybės kontrolėje ypatingas tuo, kad pirmąkart svarbiausių IT procesų (pagal COBIT) sąrašas buvo sudaromas analizuojant kiekvieną veiklos procesą (iš jau sudaryto įstaigos veiklos procesų sąrašo), po to šiam procesui priskiriant labiausiai jį įtakojančius (nuo 1 iki 3) COBIT IT procesus. Anksčiau metodika rekomenduodavo sudaryti svarbiausių COBIT IT procesų sąrašą analizuojant visą įstaigos veiklą, tačiau ją neskaidant į atskirus veiklos procesus.

Ši galimybė leidžia dar kartą patikrinti sudaryto svarbiausių COBIT IT procesų sąrašo patikimumą – abiem būdais sudaryti sąrašai turi būti panašūs; o skirtumai gali būti analizuojami, nustatomos šių skirtumų priežastys.

Reikėtų pažymėti, kad įvadinis seminaras, surengtas 12 dienų prieš praktinį vertinimo seminarą buvo tikrai naudingas. Seminaro dalyviai iš anksto žinojo, ko iš jų bus reikalaujama pagrindinio vertinimo seminaro metu, ir galėjo tam tinkamai pasiruošti. Pavyzdžiui, preliminarus įstaigos pagrindinių veiklos procesų sąrašas jau buvo sudarytas, beliko tik jį aptarti ir reitinguoti, o seminaro dalyviai buvo pakankamai gerai susipažinę su COBIT IT procesais.

Vienas iš sunkumų buvo kalba: buvo naudojama tiek anglų, tiek rusų kalba, o pati seminaro medžiaga buvo parengta tiek anglų, tiek ir rusų kalbomis (buvo naudinga seminaro medžiaga, parengta IT seminarui, vykusiame Rusijos Federacijos Sąskaitų Rūmuose 2005 m. balandžio 13-15 d.)

Latvijos valstybės kontrolės darbuotojai, dalyvavę savianalizės seminare (dalyvavo informacinių technologijų, personalo, finansų, audito metodologijos ir praktinio audito sričių atstovai) buvo gerai pasirengę seminarui ir pakankamai susipažinę tiek su bendraisiais įstaigos veiklos procesais, tiek ir su IT valdymo problemomis. Pavyzdžiui, kai buvo vertinama IT procesų (pagal

⁶⁷ JAKIMAVIČIUS, D., MIROŠNIČEKO, V., *Ataskaita apie Informacinių technologijų valdymo savianalizės seminarą, vykusį 2005 m. rugsėjo 28d. ir 2005 m. spalio 10 - 12 d. Latvijos Respublikos valstybės kontrolėje, Ryga (Latvija). LR valstybės kontrolė, 2005.*

COBIT) įtaka bendriesiems įstaigos veiklos procesams, seminaro dalyviai galėjo palyginti nesunkiai priskirti konkrečius informacinių technologijų procesus pagrindiniams įstaigos veiklos procesams.

Seminaro metu taip pat buvo atsakyta į Latvijos kolegų klausimus apie IT strateginio valdymo patirtį Lietuvos Respublikos valstybės kontrolėje: Informacinių technologijų komiteto veikla, kaip nustatomi informacinių technologijų poreikiai, kaip formuojamas informacinių technologijų biudžetas, audito dokumentavimo ir valdymo sistemos kūrimo eiga.

Buvo įdomu sužinoti, kad Latvijos kolegos, nors ir turėdami silpnesnę technologinę bazę, kai kuriose srityse pralenkė Lietuvos Respublikos valstybės kontrolę. Pavyzdžiui, yra naudojama darbo laiko apskaita, ir nors programinės priemonės yra pakankamai elementarios (daroma Microsoft Excel programinėmis priemonėmis), tai leidžia nors apytikriai įvertinti vykdomų auditų kainas.

IT savianalizės seminaras Latvijos valstybės kontrolėje naudingas tiek Lietuvos Respublikos valstybės kontrolei, tiek ir Latvijos Respublikos valstybės kontrolei: ir pažintine prasme, ir siekiant profesinio tobulėjimo. Yra daug panašių dalykų, kuriuos kiekviena iš įstaigų daro panašiai, tačiau kiekviena atskirai.

Išanalizavus ir apibendrinus klausimyno apie IT savianalizės įgyvendinimą Latvijos Respublikos valstybės kontrolėje dalyvių atsakymus paaiškėjo, kad tik 20 % IT savianalizės seminaro dalyvių anksčiau jau buvo dalyvavę panašiam renginyje ir tik 10 % dalyvių daugiau ar mažiau buvo susipažinę su COBIT metodika. Daugumos Latvijos Respublikos valstybės kontrolės darbuotojų dalyvavusių IT savianalizės seminare nuomone, seminaro dalyvių grupė nebuvo tinkamai suformuota. Jų manymu šiame renginyje turėjos dalyvauti struktūrinių padalinių vadovai ir daugiau IT specialistų.

Prieš IT savianalizės seminarą ir jo metu pateiktoje medžiagoje ir moderatorių paaiškinimuose Latvijos valstybės kontrolės darbuotojų grupė pasigedo realių pavyzdžių. Be to daug sunkumų sukėlė kalbos barjeras, todėl jei tokį seminarą kartotų ateityje, tai norėtų kuo daugiau medžiagos turėti išverstos į gimtąją kalbą. O paties IT savianalizės seminaro metu daugiau dėmesio skirtų IT ir veiklos procesų sugretinimui.

Kaip ir Lietuvos Respublikos valstybės kontrolės atstovai, tai ir Latviai buvo patenkinti IT savianalizės metu gautais rezultatais.

Latvijos Respublikos valstybės kontrolės IT savianalizės seminaro dalyviai išskyrė šiuos privalumus:

- Aiškus IT savianalizės eigos planas.
- Galimybė tiesioginėms diskusijoms tarp IT darbuotojų ir auditorių.
- Galimybė išsiaiškinti IT problemas per trumpą laiko tarpą.
- Galimybė pagerinti IT veiklą.

Trūkumai:

- Gauti rezultatai gali sukelti vadovybės nepasitenkinimą.

- Per trumpas laikas suprasti ir įsisavinti COBIT procesams ir įvertinti jų brandą.
- Kalbos barjerai.

Vis tik bendrai paėmus Latvijos Respublikos valstybės kontrolės IT savianalizės seminaro dalyviai vienbalsiai patvirtino, kad IT savianalizės metodika yra efektyvus IT valdymo įrankis ir tokius seminarus būtinai reiktų kartoti ateityje.

4.3 IT savianalizės seminaras Ukrainos Respublikos sąskaitų rūmuose

Vienas iš paskutiniųjų Informacinių technologijų savianalizės seminarų 2006 m. liepos 31 d. - rugpjūčio 2 d. įvyko Ukrainos Respublikos sąskaitų rūmuose, kuri yra viena iš EUROSAI Informacinių technologijų darbo grupės narių.

Kaip rekomenduojama IT savianalizės metodikoje, seminarui turi vadovauti moderatorius iš kitos šalies, todėl darbo autorė buvo pakviesta vadovauti IT savianalizės seminarui.

IT savianalizės metodika numato, kad seminaras turėtų trukti ne mažiau 2 dienų, gali būti ir 3 dienos; be to, turi būti numatytas laikas seminaro dalyviams susipažinti su metodikoje aptariama medžiaga, ypač su COBIT „Valdymo gairėmis“ (angl. *Management Guidelines*). Todėl, esant galimybei, siūloma surengti įvadinį seminarą likus 10-14 dienų iki pagrindinio seminaro. Deja, tokios galimybės nebuvo ir teko metodinę medžiagą persiųsti elektroniniu paštu prieš seminarą, o įvadinę paskaitą perskaityti pirmąją seminaro dieną iškart prieš praktinius užsiėmimus. Kaip paaiškėjo seminaro eigoje, dalyviams buvo sunkoka įsisavinti teoriją per tokį trumpą laikotarpį ir jei kitą kartą pakartotų IT savianalizę, tai pageidautų įvadinės paskaitos bent savaitę prieš praktines dalis. Taip galėtų pasikartoti IT savianalizės metodiką bei COBIT išskiriamus IT procesus.

Seminaro darbotvarkė buvo tokia:

1. Įvadinis seminaras, 2006-07-31 (iki pietų): Skaityti pranešimai temomis:

- Supažindinimas su Lietuvos Respublikos valstybės kontrolės Informacinių technologijų valdymo ir audito departamento struktūra ir veikla.
- Supažindinimas su EUROSAI IT darbo grupe, jos veikla ir vykdomais projektais.
- Supažindinimas su pagrindiniais charakteringais aukščiausiųjų audito institucijų veiklos procesais, informacinių technologijų poveikiu šiems procesams, taip pat informacinių technologijų valdymo uždavinio išskaidymo į 34 pagrindines valdymo sritis (pagal COBIT) ir šių sričių esamo bei siekiamo brandos lygio nustatymo metodais.
- Informacinių technologijų veiksmų plano sudarymas, panaudojant siekiamo ir esamo informacinių technologijų būklės skirtumus; suformuotų projektų prioritetų nustatymas.

2. Praktinis seminaras, 2006-07-31 (po pietų): Ukrainos Respublikos sąskaitų rūmų darbo grupės atliekamos užduotys:

- Ukrainos sąskaitų rūmų veiklos procesų sąrašo sudarymas, esminių veiklos procesų išrinkimas, veiklos procesų sąrašo sutvarkymas pagal svarbą.
- Informacinių technologijų esamos padėties ir ateities poreikių įvertinimas atsižvelgiant į veiklos procesus (BVC formos užpildymas).
- Informacinių technologijų COBIT procesų sąrašo sudarymas, įvertinant kiekvieno išrinkto veiklos proceso sąryšio svarbą su konkrečiu COBIT procesu; šio sąrašo sutvarkymas pagal kiekvieno iš jų atitikimų veiklos procesams skaičių.

3. Praktinis seminaras, 2006-08-01: Ukrainos Respublikos sąskaitų rūmų darbo grupės atliekamos užduotys:

- Gautų pirmos dienos rezultatų ir COBIT procesų sąrašo aptarimas.
- Bendro COBIT procesų sąrašo analizė: kiekvieno proceso esamo brandos lygio nustatymas pagal COBIT vertinimo metodiką, identifikavimas tų metodikos pagalba nustatytų trūkumų, kurie trukdo pereiti į aukštesnį (siekiamą) brandos lygį.
- Veiksmų plano sudarymas, remiantis atskirais esamais ir siektiniais informacinių technologijų valdymo (pagal COBIT) brandos įvertinimais, projektų prioritetų nustatymas ir jų įgyvendinimo rizikos vertinimas.

4. Praktinis seminaras, 2006-08-02: Ukrainos Respublikos sąskaitų rūmų darbo grupės atliekamos užduotys:

- Veiksmų plano sudarymas, remiantis atskirais esamais ir siektiniais informacinių technologijų valdymo (pagal COBIT) brandos įvertinimais, projektų prioritetų nustatymas ir jų įgyvendinimo rizikos vertinimas (pratęsimas).
- Sudaryto veiksmų plano ir kitų seminaro metu gautų rezultatų aptarimas dalyvaujant atstovui iš Ukrainos Respublikos sąskaitų rūmų vadovybės.
- Anketų užpildymas.

Ukrainos sąskaitų rūmų darbo grupę sudarė vienuolika atstovų iš audito, analitikos ir metodikos, informacinių technologijų ir informacijos valdymo, tarptautinių ryšių, finansų valdymo, personalo valdymo veiklos sričių. Visi dalyviai buvo savarankiškai susipažinę su prieš seminarą atsiųsta medžiaga. Taip pat pakankamai susipažinę tiek su bendraisiais įstaigos veiklos procesais, tiek ir su IT valdymo problemomis. Be to prieš sudarant grupę iš anksto buvo atsižvelgta į tai, kad seminaro dalyviai turėtų pakankamus anglų kalbos įgūdžius.

Seminaras vyko sklandžiai, nors darbo grupei tiek IT savianalizės metodika, tiek praktinis COBIT pritaikymas buvo visiškai nauji dalykai. Seminaro dalyviai atidžiai išklause įvadinės paskaitos ir išsiaiškinę iškilusius klausimus perėjo prie praktinių užduočių. Užduotys buvo atliekamos labai atsakingai. Tuo pačiu buvo gilinamasi į IT savianalizės metodiką ir COBIT procesus. Gauti rezultatai atitiko darbo grupės narių lūkesčius.

Nors IT savianalizės seminaras Ukrainos sąskaitų rūmuose nebuvo išskirtinis, nes viskas vyko gan griežtai laikantis metodikos, bet vis tik surinkta daug informacijos, kuri yra naudinga tolimesniam savianalizės metodikos tobulinimui ir seminarų organizavimui. Bendraujant su dalyviais paaiškėjo, kad viena iš pagrindinių seminaro problemų buvo kalbos barjeras. Nors seminaro medžiaga buvo parengta tiek anglų, tiek ir rusų kalbomis, daugelis pageidavo, kad visa metodinė medžiaga ir tuo pačiu COBIT būtų rusų kalba, nes Ukrainoje ši kalba yra plačiai paplitusi.

Dalyviams buvo labai smalsu sužinoti bent truputėlį statistikos apie tai, kaip vyko analogiški seminarai kitų šalių audito institucijose ir kokie gauti rezultatai.

Seminaro metu kolegos iš Ukrainos sąskaitų rūmų labai domėjosi apie Lietuvos Respublikos valstybės kontrolės patirtį informacinių technologijų strateginio valdymo srityje. Jiems buvo įdomu sužinoti apie Informacinių technologijų komiteto veiklą, nes kol kas tokio komiteto pas juos nėra.

Kitas aktualus klausimas buvo, kaip planuojamas biudžetas IT išigyti, kokiais būdais išsiaiškinami vartotojų poreikiais ir galutinis etapas – kaip vykdomi viešieji pirkimai. Diskutuojant šiomis temomis buvo abipusė nauda, nes valstybių įstatyminė bazė labai panaši ir aptariamoms problemoms buvo aktualios ne tik kolegoms iš Ukrainos sąskaitų rūmų, bet ir man.

Daugelis seminaro dalyvių domėjosi *IDEA* programine įranga, kaip ji pritaikoma Lietuvos Respublikos valstybės kontrolėje ir ar nuo to tampa efektyvesnis auditorių darbas. Taip pat buvo pageidavimų daugiau papasakoti apie naująją audito dokumentavimo ir valdymo sistemą *TeamMate*, jos įsigijimo ir diegimo etapus.

Įdomu tai, kad nors ir turėdami silpnesnę technologinę bazę (didžioji dauguma kompiuterių su *Pentium* III procesoriais, CRT monitoriai, tik kai kurie vartotojai turi nešiojamus kompiuterius ir t.t.), IT valdyme Ukrainos sąskaitų rūmai yra gerokai pažengę į priekį. Pvz. dauguma procesų yra dokumentuoti, parengtos tvarkos ir jų laikomasi. Ypatingas dėmesys skiriamas sistemų saugumui. Dėl to daugelis vartotojų negali naudotis internetu, o jei tokia galimybė suteikiama, tai labai griežtai paskirstomi interneto ištekliai.

Išanalizavus ir apibendrinus klausimyno apie IT savianalizės įgyvendinimą Ukrainos Respublikos sąskaitų rūmuose dalyvių atsakymus paaiškėjo, kad apie 30 % IT savianalizės seminaro dalyvių anksčiau jau buvo dalyvavę panašiam renginyje ir 60 % dalyvių daugiau ar mažiau buvo susipažinę su COBIT metodika. Daugumos Latvijos Respublikos valstybės kontrolės darbuotojų dalyvavusių IT savianalizės seminare nuomone, seminaro dalyvių grupė buvo tinkamai suformuota. Tačiau keli dalyviai pastebėjo, kad galėjo būti daugiau atstovų iš audito padalinių ir daugiau IT specialistų.

IT savianalizės metu dalyviams sunkumų sudarė tai, kad COBIT neišverstas į rusų kalbą. Todėl ateityje jei rengtų tokį seminarą, tai esant galimybei, kaip ir latviai pasiruoštu kuo daugiau medžiagos jiems labiausiai priimtina kalba. Be to, pačiam IT savianalizės įgyvendinimui skirtų daugiau laiko, o jo

metu daugiau diskutuoti. Dar viena svarbi pastaba – atrinkti ir įvertinti ne mažiau, kaip 20 IT procesų brandą, nors metodikoje rekomenduojama ne daugiau, kaip 15.

IT savianalizės metu gauti rezultatai nenustebino Ukrainos sąskaitų rūmų atstovų, bet ir nenuvylė. Buvo atrasta tiek problemų, kiek ir tikėtasi, bet iš esmės rezultatai labai geri.

Ukrainos Respublikos sąskaitų rūmų IT savianalizės seminaro dalyviai išskyrė šiuos metodikos ir jos taikymo privalumus:

- Metodika sukurta COBIT pagrindu.
- Galimybė susieti IT ir veiklos procesus.
- Nustatyti pagrindines IT valdymo problemas.
- Skatina bendradarbiavimą tarp IT ir kitų struktūrinių padalinių.
- Galimybė sulygtinti rezultatus su kitomis AAI.

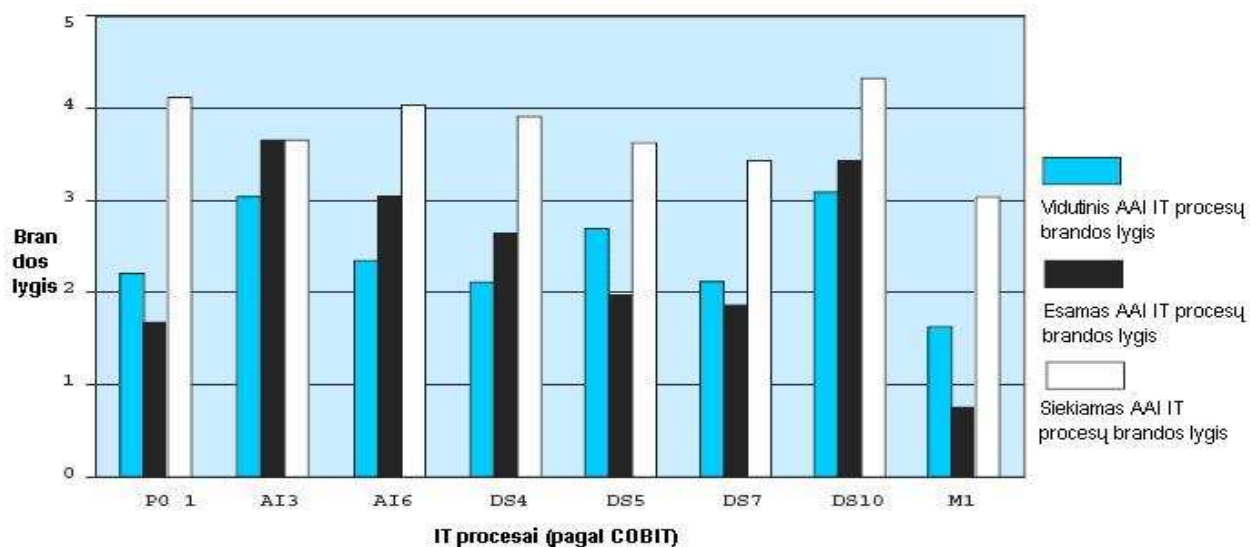
Trūkumai:

- COBIT labiau skirtas verslo organizacijoms, todėl kai kurie aspektai sunkiai priderinami viešajam sektoriui.
- Metodikoje numatyta per mažai laiko IT savianalizei įgyvendinti.

Ukrainos sąskaitų rūmų atstovai dalyvavę IT savianalizės seminare taip pat patvirtino, kad IT savianalizės metodika yra efektyvus IT valdymo įrankis ir tokius seminarus būtinais reikėtų kartoti ateityje.

4.4 Gautų rezultatų analizė

Kiekviena šalis, atlikusi IT savianalizės seminarą, gautus rezultatus ne tik panaudoja vidinėms įstaigos problemoms spręsti, o taip pat siunčia į savianalizės projekto koordinatoriui – Šveicarijos federalinei audito įstaigai. Projekto posėdžių metu dalyvaujant visoms 6 projekto narėms rezultatai išanalizuojami ir apibendrinami. Pavyzdžiui, IT savianalizės rezultatai naudojami, siekiant nustatyti svarbiausius IT procesus daugelyje Europos AAI, įvertinti jų brandos lygius, pasiūlyti priemones IT brandai pagerinti. Vienas iš rezultatų analizės pavyzdžių pateikiamas 5 pav. Taip pat remiantis gautais rezultatais numatomos savianalizės metodo tobulinimo kryptys.



5 pav. Link etalono⁶⁸.

Apibendrinant vykusius savianalizės seminarus, galima teigti, kad seminarai buvo naudingi ir suteikė naujų žinių, ne tik kaip IT gali pagerinti įstaigos veiklą, tačiau kokie reikalingi įstaigos vadovybės sprendimai IT veiklai gerinti. Metodika numato, kad savianalizės išvados turi būti perkeltos į „veiksmų planą“, skirtą įvardinti ir išspręsti pagrindinius uždavinius, kad pagerėtų tiek IT, tiek ir bendroji įstaigos veikla.

Metodika sudaro galimybę lyginti atskirų aukščiausiųjų audito įstaigų informacinių technologijų būklę, tačiau tokiu atveju IT vertinimo kriterijai turėtų būti taikomi vienodai visose savianalizė atliekančiose institucijose, nes įvertinimas „2“ vienoje institucijoje gali būti suvokiamas kaip „palyginti geras“, kitoje – kaip „palyginti blogas“.

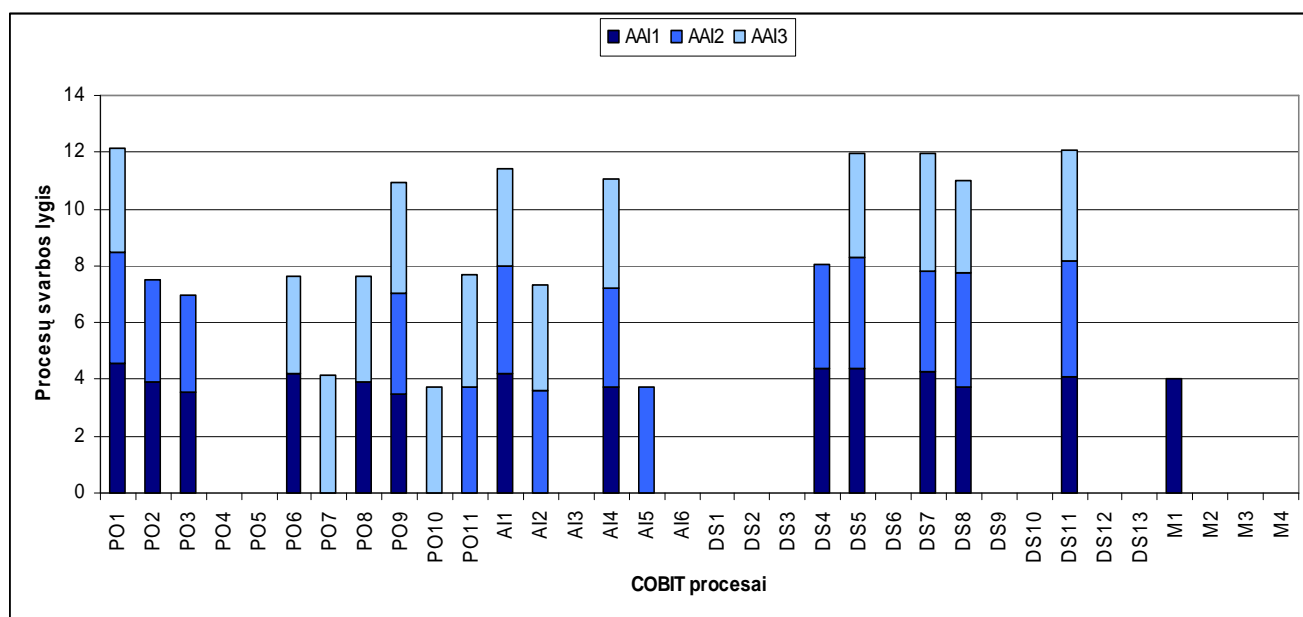
Svarbiausieji IT procesai nustatyti IT savianalizė seminarų metu kitų šalių AAI:

- PO1 Apibrėžti strateginį IT planą
- DS5 Užtikrinti sistemų saugumą
- DS7 Apmokyti vartotojus
- PO10 Valdyti IT projektus
- DS11 Prižiūrėti duomenis
- AI2 Įsigyti ir prižiūrėti taikomąją programinę įrangą
- DS10 Sekti, spręsti problemas ir skundus
- AI6 Kontroliuoti IT sistemų pokyčius
- M1 Stebėti procesus
- PO4 Apibrėžti IT organizacinę struktūrą ir veiksmus
- AI1 Automatizavimo sprendimų paieška

⁶⁸ EUROSAT IT Working Group, IT Self-assessment, Lankstinukas, Nyderlandai, 2005.

- AI3 Įsigyti ir prižiūrėti technologinę infrastruktūrą
- DS4 Užtikrinti nuolatinį sistemų funkcionavimą

Tokią statistiką galima gauti ir iš Lietuvos, Latvijos ir Ukrainos atliktų IT savianalizių rezultatų. Remdamiesi grafikus, kuris pavaizduotas 6 pav. Galima pastebėti, kad didžioji dalis svarbiausių IT procesų sutampa su kitų šalių nustatytais svarbiausiais IT procesais. Atsižvelgiant į tai, kad IT savianalizės metodikoje išipareigojama neskelbti AAI rezultatų, o tik statistinius duomenis, todėl toliau darbe tris Lietuvos, Latvijos ir Ukrainos AAI užkoduosime, kaip AAI1, AAI2 ir AAI3.

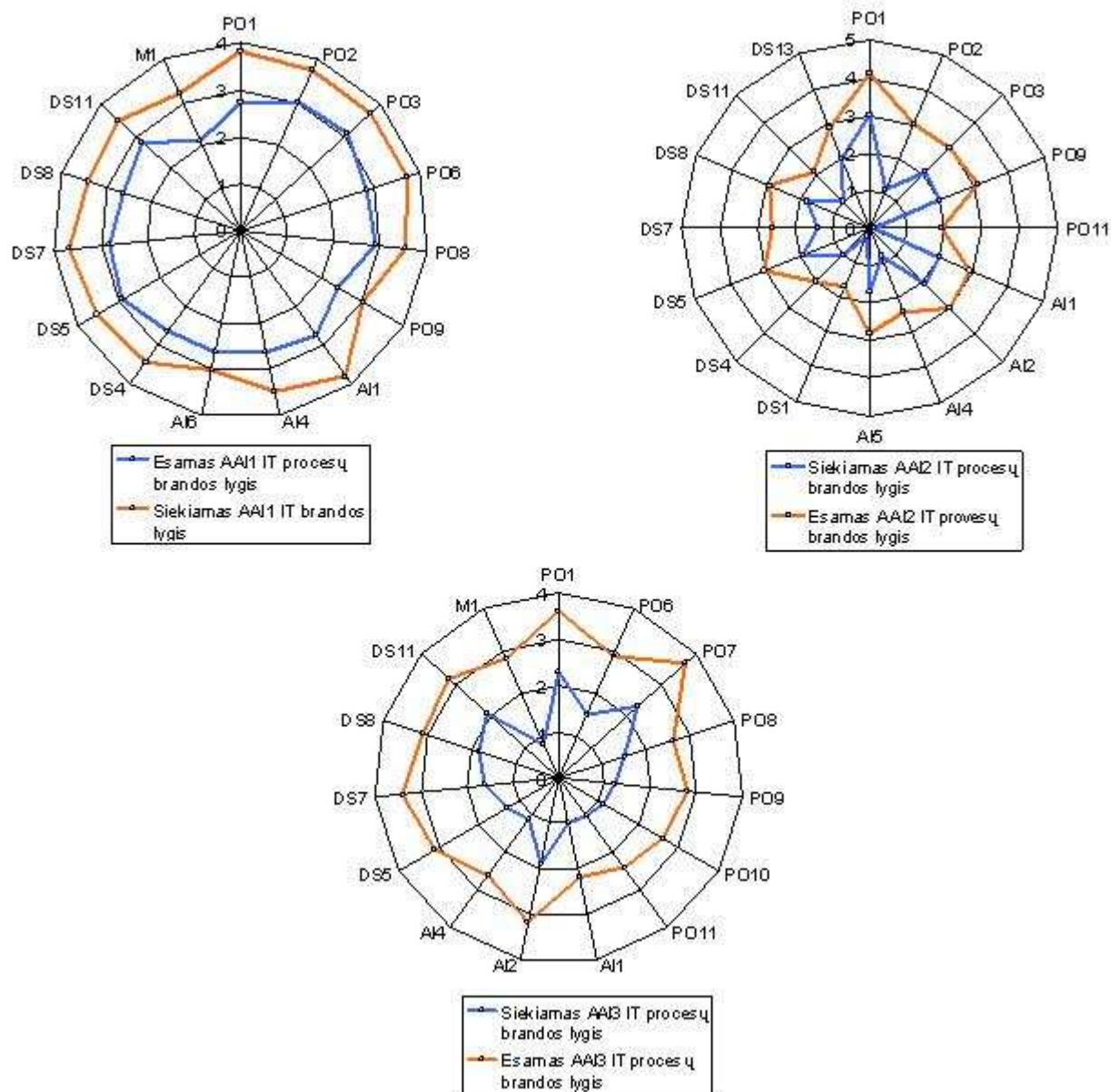


6 pav. Svarbiausia IT procesai nustatyti Lietuvos, Latvijos ir Ukrainos AAI⁶⁹.

Viena iš problemų kylančių nustatinėjant IT procesų svarbą yra IT savianalizės dalyvių kompetencijos IT srityje trūkumas ir tai dažniausiai įtakoja neteisingą supratimą apie COBIT IT procesus. Be abejonės tokiu atveju ir vertinimas gali neatitikti realios situacijos. Pagal COBIT metodiką šį vertinimą turėtų atlikti IT specialistai. Bet iš kitos pusės šis seminaras tam ir vykdomas, kad išgauti tiek IT specialistų nuomonę tiek ir vartotojų.

Nustatant IT procesų brandos lygį vėlgi susiduriame su ta pačia problema. Tačiau čia yra ir kitų sunkumų. IT branda nustatoma remiantis COBIT kiekvienam IT procesui aprašytais brandos lygio reikalavimais, Bet ne specialistui suvokti ir suprasti COBIT kalbą yra ištis sunku. Todėl branda turi būti nustatinėjama diskutuojant, t.y. specialistas turėtų pakomentuoti kiekvieno IT proceso esamą brandos situaciją konkrečioje AAI ir visa grupė nuspręstų, kurį brandos lygį ta situacija atitinka pagal COBIT.

⁶⁹ Sukurta darbo autorės.



7 pav. IT procesų esamas ir siekiamas brandos lygiai nustatyti Lietuvos, Latvijos ir Ukrainos AAI⁷⁰.

Aukščiausias brandos lygis pasiektas įgyvendinant šiuos procesus:

- PO3 Pasirinkti technologinę kryptį
- AI2 Įsigyti ir prižiūrėti taikomąją programinę įrangą
- AI3 Įsigyti ir prižiūrėti technologinę infrastruktūrą
- AI4 Sukurti ir atnaujinti IT naudojimo procedūras
- AI6 Kontroliuoti IT sistemų pokyčius

⁷⁰ Sukurta darbo autorės.

- DS5 Užtikrinti sistemų saugumą
- DS10 Sekti, spręsti problemas ir skundus
- DS11 Prižiūrėti duomenis

Pagal bendrus atliktų IT savianalizė sudarytų veiklos planų duomenis paskutinėje projekto grupės ataskaitoje yra išskirta, kad dauguma AAI turėtų tobulinti šiuos procesus:

- Parengti strateginį IT planą;
- Didesnį dėmesį kreipti vartotojų mokymui ir praktiniams užsiėmimams IT srityje;
- Gerinti vidinį bendravimą tarp AAI darbuotojų ir IT specialistų;
- Gerinti IT projektų valdymą;
- Gerinti informacinių sistemų integravimą ir standartizavimą;
- Tobulinti dokumentų valdymo sistemos naudojimą
- Sukurti aiškias kontrolės procedūras IT resursų valdymui

Jeigu svarbiausių IT veiklos susiejimas su tiesiogine AAI veikla, svarbiausių IT procesų išskyrimas, jų brandos lygio įvertinimas ir veiksmų plano nustatymas labiausiai naudingi yra pačioms AAI siekiant ir įgyvendinant IT valdymą, tai anketos apie IT savianalizės įgyvendinimą (2 priedas) nuoširdus užpildymas yra ypatingai svarbus IT savianalizės projekto grupei. Kiekvienas pastebėjimas gali tapti priežastimi tobulinti IT savianalizės metodikai.

4.5 Naujausios 4.0 IT savianalizės metodikos pristatymas

2007 metų pradžioje EUROSAI IT darbo grupė atnaujintą IT savianalizės metodiką, kuri gali būti naudojama aukščiausiose audito institucijose kuriant ir įgyvendinant IT strateginį valdymą. Naujoji metodikos versija susideda iš šių dalių:

- metodikos apibūdinimas.
- *Power Point* pateiktis, kuri pristatomas IT savianalizės seminaro metu.
- *Excel* lentelės, kurios palengvina tiek grupės tiek seminaro moderatoriaus darbą surenkant duomenis bei atliekant jų statistinę analizę.

Visa tai galima rasti EUROSAI IT darbo grupė internetiniame puslapyje www.eurosai-it.org.

Vienas iš pagrindinių IT savianalizės metodikos 4.0 versijos privalumų yra tas, kad ji visiškai suderintas su COBIT 4.0 versija. Ankstesniuose šio darbo skyriuose jau buvo pristatyta, kad COBIT yra globalus geros praktikos rinkinys skirtas informacinių technologijų kontrolei. 4.0 versijoje taip pat atnaujintos darbo lentelės, parengta nauja prezentacija.

4.6 Skyriaus apibendrinimas

IT savianalizės seminarai jau yra įvykę dvidešimt šešiuose EUROSAI Aukščiausiose audito institucijose iš kurių trijuose (Latvijoje, Lietuvoje ir Ukrainoje) vadovavo šio darbo autorė. Analizuojant IT savianalizės įgyvendinimą Latvijos Respublikos valstybės kontrolėje pagrindinis išskirtinumas yra tai, kad pirmąkart svarbiausių IT procesų (pagal COBIT) sąrašas buvo sudaromas analizuojant kiekvieną veiklos procesą (iš jau sudaryto įstaigos veiklos procesų sąrašo), po to šiam procesui priskiriant labiausiai jį įtakojančius (nuo 1 iki 3) COBIT IT procesus. Anksčiau metodika rekomenduodavo sudaryti svarbiausių COBIT IT procesų sąrašą analizuojant visą įstaigos veiklą, tačiau ją neskaidant į atskirus veiklos procesus. Ši galimybė leidžia dar kartą patikrinti sudaryto svarbiausių COBIT IT procesų sąrašo patikimumą – abiem būdais sudaryti sąrašai turi būti panašūs; o skirtumai gali būti analizuojami, nustatomos šių skirtumų priežastys.

Lietuvos Respublikos Valstybės kontrolėje surengtas IT savianalizės seminaras, kuriam vadovavo šio darbo autorė, buvo antrasis tokio pobūdžio renginys šioje institucijoje. Kadangi dauguma dalyvių ne tik buvo dalyvavę pirmojoje IT savianalizėje, bet ir turėjo labai gerus COBIT pagrindus, todėl savianalizė buvo atliekama ypač atsakingai. Sudarytas išsamus pagrindinių ir antrinių veiklos procesų sąrašas, jie sugretinti su COBIT procesais, o jų branda nustatoma diskusijų metu išklausanč beveik kiekvieno dalyvio argumentų. Parengtas veiksmų plano projektas, kuris buvo išanalizuotas ir apsvarstytas IT valdymo komitete, o vėliau įtrauktas į Lietuvos Respublikos valstybės kontrolės Informacinių technologijų strateginį plėtros planą. Tačiau, kaip parodė praktika Lietuvos Respublikos valstybės kontrolėje, kuo atsakingiau norint atlikti IT savianalizę, tuo daugiau laiko sugaištama. Jeigu pirmoji (pilotinė) IT savianalizė buvo atlikta per nepilnas dvi dienas, tai antrasis savianalizės seminaras tęsėsi net keturias dienas, neskaitant to, kad įvadinė paskaita buvo pravesta savaitę prieš praktinį IT savianalizės įgyvendinimą Lietuvos Respublikos valstybės kontrolėje.

Ukrainos Respublikos sąskaitų rūmuose IT savianalizės seminaras buvo vykdomas laikantis metodikoje nurodyto plano, nes laiko buvo skirta tik 2,5 dienos. Nors IT savianalizės seminaras Ukrainos sąskaitų rūmuose nebuvo išskirtinis, bet vis tik surinkta daug informacijos, kuri naudinga tiek tolimesniam savianalizės metodikos tobulinimui ir seminarų organizavimui, tiek efektyvesniam Ukrainos Respublikos sąskaitų rūmų IT valdymui įgyvendinti.

Apibendrinant Latvijos, Lietuvos ir Ukrainos AAI IT savianalizės seminaro įgyvendinimo atsiliepimus, galima teigti, jog IT savianalizė yra naudinga tuo, kad:

- galima išsiaiškinti IT poreikius, kurie padėtų efektyviau įgyvendinti AAI uždavinius;
- IT valdymas peržiūrimas visos institucijos mastu, todėl galima atrasti beveik visas IT strateginio valdymo spragas;

- diskusijų metu tarp IT ir kitų padalinių atstovų per trumpą laiko tarpą išsiaiškinti IT problemas;
- išbandyti IT savianalizės metodiką ir tuo pačiu įgyti žinių apie COBIT.

Pagrindiniai trūkumai, kuriuos išskyrė Latvijos, Lietuvos ir Ukrainos AAI IT savianalizės seminaro:

- Dalyviai turi turėti aukštą žinių lygį IT ir COBIT srityje, be to COBIT labiau skirtas verslo organizacijoms, todėl kai kurie aspektai sunkiai priderinami viešajam sektoriui;
- Trūksta detalesnio kiekvieno IT savianalizės etapo aprašymo;
- Metodikoje numatyta per mažai laiko IT savianalizei įgyvendinti;
- Kalbos barjerai: pageidautina, kad ir IT savianalizės metodika ir COBIT būtų gimtąja kalba.

Metodika sudaro galimybę lyginti atskirų Aukščiausiųjų audito įstaigų informacinių technologijų būklę. Tuo galima įsitikinti peržvelgus priešpaskutiniame šio darbo paragrafe pateiktus įvairių šalių AAI IT savianalizės metu gautų rezultatų analizės pavyzdžius. Dažniausiai analizuojami ir sulyginami kiekvienos šalies AAI atrinkti IT pricesai (pagal COBIT), apibendrinama, kurių IT procesų branda yra aukščiausia, o kuriuos dar reikia tobulinti. Remiantis sudarytais veikslių planais, sudaromas pagrindinių problemų sąrašas.

Atsižvelgiant į atliktų IT savianalizių rezultatus, dalyvių pastabas ir į tai, kad 2005 m. buvo išleista 4.0 COBIT versija, 2007 metų pradžioje EUROSAI IT darbo grupė atnaujini ir IT savianalizės metodiką.

IŠVADOS

1. Apžvelgus ir išanalizavus įvairius literatūros šaltinius, galima prieiti prie išvados, kad informacinių technologijų strateginis valdymas – tai sudėtinė bendrojo organizacijos valdymo dalis, nuo kurios priklauso, kaip efektyviai informacinės technologijos remia ir plėtoja bendruosius organizacijos veiklos procesus.

2. IT strateginis valdymas AAI yra svarbus, nes informacija yra strateginis išteklius atliekant valstybinius auditus.

3. EUROSAT IT darbo grupės parengta IT savianalizės metodika yra pakankamai aiški ir pritaikoma AAI. Rezultatai, gauti daugelyje IT savianalizės renginių, vykusių skirtingu laiku ir skirtingų šalių Aukščiausiose audito institucijose, leidžia nustatyti pagrindinius aukščiausiųjų audito institucijų veiklos procesus, įvertinti jų ryšį su informacinių technologijų COBIT procesais, nustatyti svarbiausių COBIT procesų brandos lygį ir sudaryti veiksmų planą aukštesnei brandai pasiekti.

4. Informacinių technologijų savianalizės metodiką rengė Aukščiausiųjų audito institucijų darbuotojai, ši metodika yra taikoma daugelyje Europos Aukščiausiųjų audito institucijų, tačiau pati metodika gali būti universali, ir jos taikymas viešojo sektoriaus įstaigose bei organizacijose yra galimas tiek, kiek viešojo sektoriaus įstaigos ir organizacijos sugeba nustatyti bendruosius savo veiklos procesus ir susieti juos su informacinių technologijų procesais.

5. Rekomenduotina informacinių technologijų savianalizę atlikti reguliariai, o paskutinės savianalizės rezultatai galėtų tarnauti kaip priemonė aukštesniam informacinių technologijų valdymo brandos lygiui pasiekti. Kartojant tokius seminarus ir pati informacinių technologijų savianalizės metodika taptų efektyvesnė, nes audito institucijos atstovai įgytų daugiau patirties ją pritaikant. Informacinių technologijų savianalizė taip pat gali būti naudojama rengiant informacinių technologijų strategijas.

6. Pačią IT savianalizės metodiką būtų galima tobulinti:

- atsižvelgiant į tai, kad labai daug atliko sugaištama sudarant AAI veiklos procesų sąrašą ir juos suskirstant į pagrindinius ir antrinius, šiuo momentu jau yra pakankamai duomenų

iš įvairių šalių AAI, kuriuose jau atlikta IT savianalizė, kad sudaryti bendrą pagrindinių AAI veiklos procesų sąrašą;

- detaliau aprašant BVC ir COBIT vertinimo skales (tiksliai paaiškinant ką kokia įvertinimo reikšmė reiškia);
- daugiau dėmesio skirti veiklos ir IT procesų susiejimui, nes tai yra vienas iš esminių metodikos aspektų. IT savianalizės metodikoje šio etapo aprašymas yra nepakankamai išsamus (pvz. neaišku kaip galima pritaikyti duomenis gaunamus užpildžius BVC formą);

7. AAI ar kitos organizacijos įgyvendinusios IT savianalizę turėtų įsisąmoninti, kad IT savianalizė yra tik priemonė IT strateginiam valdymui pagerinti, bet pats IT strateginis valdymas yra nenutrūkstantis procesas.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

Mokslinė literatūra:

1. ACCA *Lynchpin for International Stresam: Audit framework*. United Kingdom: AT Foulks Lynch LTD, 2000. 125 p. ISBN 0 7483 4201 X.
2. GREMBERGEN, Wim Van, *Strategies for Information Technology Governance*, USA: Idea Group Publishing, 2004. 406 p. ISBN:1591402840.
3. СКОБАРА, В. В. *Аудит: методология и организация*. Москва: Дело и Сервис, 1998. С.3.
4. EUROSAI IT Working Group, *A methodology for IT self-assessment by SAI's*. Version 2.0, Bern: 2004, P. 46.
5. ГУЗИК, Сергей, *Стандарт CobiT Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТю ISACA.ru*, 2002, p. 31.
6. Informatikon Systems Audit and Control Association. *2004 CISA Review Manual*, USA: 2004.
7. IT Governance Institute, *COBIT 3rd Executive Summary*. 3rd ed. USA: ITGI, 2000. 122 p. ISBN 1-893209-15-6.
8. IT Governance Institute, *COBIT 3rd Implementation Tool Set*. 3rd ed. USA: ITGI, 2000. 92 p. ISBN 0-893209-16-14.
9. IT Governance Institute, *COBIT 4.0*. 4th ed. USA: ITGI, 2005. 194 p. ISBN 1-933284-37-4.
10. KATKUS, A. *Valstybinė ekonominė kontrolė*. Vilnius: Mintis, 1997. 301 p.
11. MACKEVIČIUS, J. *Auditas: teorija, praktika, perspektyvos*. Vilnius: Lietuvos mokslas, 2001. 837 p. ISBN 9986-795-05-3.
12. MATICKIENĖ, I. *Audito planavimas ir organizavimas*. Kaunas: Technologija, 1997. 140 p.
13. Rizikos analizės vadovas. *Administracinių ir techninių gebėjimų stiprinimas užtikrinant duomenų informacinių technologijų ir jomis perduodamų duomenų apsaugą*. Lietuvos Respublikos Vidaus Reikalų Ministerija.-Vilnius: Vaga.- 2005. – 161 p. ISBN 54150118271.
14. ШОХИН, С.О., ВОРОНИНА, Л. И. *Бюджетно-финансовый контроль и аудит: Теория и практика применения в России*. Москва: Финансы и статистика, 1997.
15. VAITKEVIČIŪTĖ, V. *Tarptautinių žodžių žodynas*. Vilnius: Žodynas, 2001. 1039 p.

Kitos bibliografinės nuorodos:

16. *ABBY Product Overview* [interaktyvus]. Moscow: ABBYY Software, 1996-2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.abbyy.com/products/>>.
17. *ACL – Data You Can Trust. Results You Can See* [interaktyvus]. Canada: ACL Services Ltd., 2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.acl.com>>.

18. *Arthur Andersen* [interaktyvus]. USA: Wikimedia Foundation Inc., 2002– [žiūrėta 2007-04-20]. Prieiga per internetą: <http://en.wikipedia.org/wiki/Arthur_Andersen>.
19. BAKSHI, Sunil, Control Self-assessment for Information and related technology. *Information Systems Control Journal*, 2004, vol. 1, p. 10-18.
20. *Board Briefing on IT Governanc* [interaktyvus]. 2nd ed. USA: IT Governance Institute, 2004, [žiūrėta 2007 m. kovo 23 d.]. Prieiga per internetą: <http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf>.
21. *COBIT 4rd edition brochure* [interaktyvus], USA: Information Systems Audit and Control Association (ISACA), 2007- [žiūrėta 2007-04-17]. Prieiga per internetą: <http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Obtain_COBIT.htm>.
22. *Court of Audit of the Republic of Slovenia* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.rs-rs.si>>.
23. *Enron* [interaktyvus]. USA: Wikimedia Foundation Inc., 2002– [žiūrėta 2007-04-20]. Prieiga per internetą: <<http://en.wikipedia.org/wiki/Enron>>.
24. *EUROSAI-IT Working Group, Objectives* [interaktyvus]. Netherlands: EUROSAI IT Working Group Secretariat - [žiūrėta 2006 m. sausio 12 d.]. Prieiga per internetą: <<http://www.eurosai-it.org/9282201/v/index.htm>>.
25. HUISSOUD Michel, *So you like IT self assessments?*, Bratislava 2006.
26. *IDEA – Data Analysis Software* [interaktyvus]. Canada: CaseWare IDEA Inc., 2007– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.caseware-idea.com/fsh.asp>>.
27. Informacijos technologija. *Informacijos saugumo valdymo praktikos kodeksas* (tapatus ISO/IEC 1799:2000). Lietuvos standartizacijos departamentas. 2004, LST ISO/IEC 17799:2004 lt.
28. INTOSAI (International Organization of Supreme Audit Institutions), *Statutes* [interaktyvus]. JAV: INTOSAI, 2004– [žiūrėta 2007-03-25]. Prieiga per internetą: <<http://www.intosai.org/blueline/upload/12estatut.pdf>>.
29. *IS auditing procedure: Control Risk self-assessment (CRSA)* [interaktyvus]. USA: Information Systems Audit and Control Association [žiūrėta 2007-04-21]. Prieiga per internetą: <<http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31605>>.
30. JAKIMAVIČIUS, Dainius, *ATASKAITA apie EUROSAI Informacinių technologijų darbo grupės 2-ąjį pasitarimą, vykusį 2004 m. kovo 29 - 30 d. Berne (Šveicarija)*, 2004.
31. JAKIMAVIČIUS, Dainius, *Įvadas į Informacinių technologijų valdymo savianalizę*. Seminaro medžiaga, 2005.

32. JAKIMAVIČIUS, D., MIROŠNIČEKO, V., *Ataskaita apie Informacinių technologijų valdymo savianalizės seminarą, vykusį 2005 m. rugsėjo 28d. ir 2005 m. spalio 10 - 12 d. Latvijos Respublikos valstybės kontrolėje, Ryga (Latvija). LR valstybės kontrolė, 2005.*
33. *Kas yra CobIT?*[interaktyvus]. Lietuva: Asociacija ISACA Lietuva, 2003– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.isaca.lt/lt/cobit/>>.
34. LAINHART IV John W., *International Standards provide Guidance for IT Governance* [interaktyvus]. USA: International Federation of Accountants, 2001- [žiūrėta 2007-04-21]. Prieiga per internetą: <<http://www.ifac.org/Library/Article.tmpl?NID=99097368215895>>.
35. LAKIS, V. Audito raida Lietuvoje ir sistemos kūrimo problemos. *Ekonomika*. 2002, Nr.58. P.106.
36. Lietuvos Respublikos valstybės kontrolės įstatymas. *Valstybės Žinios*. Vilnius: Lietuvos Respublikos Seimo leidykla, 2001-12-13, Nr. 112-4070.
37. *Lietuvos Respublikos valstybės kontrolė* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.vkontrolė.lt>>.
38. MANTELAERS, Paul, *The Strategic Importance of IT for SAIs*. Seminaro medžiaga. Vilnius, 2005.
39. *Netherlands Court of Audit* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.rekenkamer.nl>>.
40. *Office of the Auditor General of Norway* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.riksrevisjonen.no>>.
41. *Sistemos „Microsoft Office“ produkto informacija* [interaktyvus]. United State: Microsoft Corporation, 2007– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://office.microsoft.com/lt-lt/default.aspx>>.
42. *Spanish Court of Audit* [interaktyvus]. [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.tcu.es>>.
43. *Summary of the Provisions of the Sarbanes-Oxley Act of 2002* [interaktyvus]. USA: AICPA, 2004-2006– [žiūrėta 2007-04-20]. Prieiga per internetą: <<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>>.
44. *Swiss Federal Audit Office* [interaktyvus], [žiūrėta 2007-04-18]. Prieiga per internetą: <<http://www.efk.admin.ch/english/index.htm>>.
45. ХРАМЦОВСКОЙ, Н.А. *Выходит новая версия стандарта CobiT* [interaktyvus]. Москва: Электронные Офисные Системы, 2005– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.eos.ru/eos/163336>>.
46. *What is TeamMate?* [interaktyvus]. New York: PricewaterhouseCoopers, 2006-2007– [žiūrėta 2007-04-10]. Prieiga per internetą: <<http://www.pwc.com/Extweb/service.nsf/docid/443881F8A1DA32D0852568B6001A514E>>.

SUMMARY

(Implementation of IT Self-assessment Methodology in National Audit Institutions)

The object of the thesis is the IT self-assessment methodology developed and successfully applied by the EUROSAI Information Technology Working Group. *The aim* of the thesis is to present IT self-assessment methodology as a means to identify the relationship between performance of the Supreme Audit Institutions and possibilities provided by the information technology; to assess maturity of information technology and to envisage measures for strengthening of maturity level; to assess this methodology on the basis of results of its practical application. The main *goals of the thesis* are the following:

8. To present conception of strategic management of information technologies and its importance to performance of the Supreme Audit Institutions;
9. To review set of the best practice of COBIT, because IT self-assessment methodology was developed by the EUROSAI Information Technology Working Group on the basis of it;
10. To introduce the development of IT self-assessment methodology, as well as its aims, goals, and requirements raised for IT self-assessment methodology;
11. To describe in detail action course of this methodology;
12. To explore advantages and weaknesses of the IT self-assessment methodology by analysing results of IT self-assessment seminars in various Supreme Audit Institutions.

The thesis is *relevant*, because there is still no knowledge on development methods of IT management processes in public institutions. Often development of information technologies is separated from main performance processes of institutions, therefore it is important to link processes of IT and performance, as well as to identify maturity level of IT and to find strong and weak points of an organization. The possibility to use COBIT is especially important here, because COBIT is a tool for management of information technologies. The thesis is useful both in scientific and practical sense for all those interested in and working in the area of IT management.

Basically the thesis is founded on international best practice set COBIT and IT self-assessment methodology developed by the SAI. The review and analysis of various sources of literature related to the topic of the thesis was performed.

PRIEDAI

1 priedas. Lietuvos Respublikos valstybės kontrolės veiklos procesai

- **Įstaigos valdymas**
 - **Institucijos strategijos formavimas**
 - *Asignavimų planavimas*
 - *Ilgalaikis institucijos vystymas*
 - *Funkcinių strategijų sudarymas*
 - *Metiniai priemonių planai*
 - **Rizikos valdymas**
 - **Sprendimų priėmimas ir kontrolė**
 - *Vidaus auditas*
- **Auditas**
 - **Audito planavimas**
 - *Bendrosios audito programos sudarymas*
 - *Koordinacinių planų sudarymas*
 - *Konkreto audito planavimas*
 - *audito tikslų nustatymas*
 - *rizikos vertinimas*
 - **Audito atlikimas ir dokumentavimas**
 - *Duomenų gavimas iš subjekto*
 - *Specialistų pasitelkimas*
 - *Įrodymų dokumentavimas*
 - *Ataskaitos ir išvados rengimas ir derinimas, sprendimo priėmimas, IS brandos nustatymas*
 - **Audito duomenų sisteminimas ir valdymas**
 - *Išvadų dėl valstybės ataskaitų rengimas*
 - *Išvados dėl valstybės biudžeto projekto rengimas*
 - *Audito savikainos ir efektyvumo nustatymas*
 - **Poauditinė veikla**
 - **Audito kokybės užtikrinimas**
 - *Audito metodikos rengimas ir tobulinimas*
 - *Vidinė detalioji peržiūra*
 - *Vidinė bendroji peržiūra*
 - *Išorinė peržiūra*
- **Personalo valdymas**
 - Personalo planavimas
 - Personalo apskaita, duomenų valdymas ir naudojimas
 - Personalo mokymas
 - Personalo karjeros planavimas
 - Personalo rotacija
 - Tarnautojų vertinimas
 - Personalo atranka ir įdarbinimas
 - Motyvavimas ir skatinimas
 - Darbo laiko apskaita

- **Informacijos valdymas**
 - **Informacijos saugojimas**
 - *Audito duomenys*
 - *Administraciniai duomenys*
 - **Išorės komunikavimas**
 - *Tarptautinis bendradarbiavimas*
 - *Audito medžiagos perdavimas išorei*
 - *Santykiai su klientais*
 - *Ataskaitos ir išvados publikavimas*
 - *Metinė VK veiklos ataskaita*
 - *Viešieji ryšiai*
 - *Išorės duomenų bazių naudojimas*
 - **Vidaus komunikavimas**
 - *Dokumentų valdymas (informacijos departamentas)*
 - *Biblioteka*
 - *Vidaus duomenų bazių naudojimas*
- **Informacinių technologijų valdymas**
 - Rengti VK informacinių technologijų strategijos projektą, organizuoti jos įgyvendinimą
 - Administruoti VK informacinę infrastruktūrą, leidžiančią kaupti, tvarkyti ir saugoti administracinę ir audito informaciją
 - kurti, diegti ir administruoti VK kompiuterizuotos informacinės sistemos apsaugos priemones, užtikrinti technologinę duomenų apsaugą;
 - teikti informacinių technologijų valdymo pagalbą VK padaliniams.
- **Teisinės paslaugos**
 - Teisinė pagalba administravimui
 - Teisinė pagalba auditui
 - Teisės aktų analizė
- **Finansų valdymas**
 - Finansų apskaita
 - Finansų planavimas ir valdymas
- **Turto valdymas**
 - Materialinių poreikių išsiaiškinimas
 - Turto apsauga ir palaikymas
 - Turto įsigijimas, viešieji pirkimai
 - Materialinių vertybių apskaita

1 priedas. Klausimynas apie IT savianalizės įgyvendinimą



AAI IT savianalizės seminaro įvertinimo klausimynas EUROSAI IT darbo grupė



Įvadas

- Tikslas: surinkti kuo daugiau informacijos, kuria remiantis būtų galima tobulinti AAI IT savianalizės procesą ir pačią metodiką.

Kiekvieno IT savianalizės seminaro dalyvio įvertinimas:

Nr	Klausimas:	Atsakymas:
1	Ar anksčiau esate susidūrę su IT savianalize? (taip/ne)	
2	Ar iki IT savianalizės seminarą žinojote ką nors apie COBIT? (taip/ne)	
3	Jūsų nuomone, ar tinkamai buvo sudaryta IT savianalizės grupė? (taip/ne) Jei ne, tai kokius asmenis siūlytumėte įtraukti?	
4	Kaip Jūs manote ar Jums pakako medžiagos ir pagalbos/paaiškinimų (prieš IT savianalizės seminarą ir jo eigoje), reikalingų sėkmingam IT savianalizės įgyvendinimui? (taip/ne) Jei ne, ko Jūsų manymu trūko?	
5	Jeigu Jūsų institucija nuspręstų pakartoti IT savianalizės seminarą, ką darytų kitaip?	
6	Ar IT savianalizės rezultatai pateisino Jūsų lūkesčius? Prašome pakomentuoti.	
7	Ar Jūs sudarėte veiksmų planą ateičiai?	

8	Po to, kai IT savianalizės seminaras įgyvendintas Jūsų AAI, kaip manote kokie yra jo pagrindiniai privalumai ir trūkumai?	
9	Kaip Jūs manote, ar IT savianalizė yra efektyvus valdymo įrankis? Kodėl?	
10	Ar būtų naudinga pakartoti IT savianalizės seminarą?	