

## IT AUDITAS LIETUVOS SMULKAUS IR VIDUTINIO DYDŽIO ĮMONĖSE

Rasma Janeliūnienė<sup>1</sup>, Ginta Liberytė<sup>2</sup>, Vida Davidavičienė<sup>3</sup>*Vilniaus Gedimino technikos universitetas**El. paštas: <sup>1</sup>rasma.janeliuniene@vgtu.lt; <sup>2</sup>ginta.liberyte@vgtu.lt; <sup>3</sup>vida.davidaviciene@vgtu.lt*

**Santrauka.** Informacinės technologijos užima svarbią vietą organizacijos veikloje siekiant konkurencinio pranašumo. Efektyvus IT valdymas padeda organizacijai optimizuoti darbą, teisingai valdyti resursus, tinkamai siekti užsibrėžtų tikslų. Kaip ir visi veiklai vykdyti reikalingi išteklių, informacinės technologijos ne tik teikia naudą, bet kelia ir tam tikrą grėsmę. Informacinės sistemos tampa organine bet kurios organizacijos dalimi. Šiuolaikinių įmonių veikla neišsivaizduojama ir neįmanoma be naujausių informacinių technologijų. Įmonių veiklą grindžiamą šiuolaikinėmis IT, taip pat jų organizavimą ir valdymą veikia ne tik išorinės aplinkos veiksniai – didelę reikšmę turi ir vidiniai organizaciniai veiksniai bei IS ir valdymo aspektai. Neužtenka tik įsidiesti naują sistemą, ją būtina suderinti su įmonės veiklos procesais, siekiant išnaudoti visus privalumus, būtina vertinti pokyčius ir į juos reaguoti. Siekiant mažinti IT riziką, itin aktualus tampa IT auditas organizacijoje. Straipsnyje analizuojamos egzistuojančios IT audito metodikos, vertinamas IT audito poreikis, Lietuvos smulkaus ir vidutinio dydžio įmonių specifika. Straipsnio tikslas – įvertinti IT audito metodikų taikymo Lietuvos smulkaus ir vidutinio dydžio įmonėse galimybes.

**Reikšminiai žodžiai:** IT auditas, audito metodai, IT rizikos vertinimas, IT auditas Lietuvoje, SVV.

**Įvadas**

Sparčiai augant verslo informacijos kiekiui, išskyla poreikis turėti papildomų priemonių, kurios padėtų organizacijų vadovams greitai, tinkamu metu ir tinkama forma gauti informacijos, reikalingos verslo sprendimams priimti. Diegiamos informacinės sistemos (IS) ir jomis naudojantis sukauptos žinios tampa ypač reikalingos siekiant organizacijoms konkuruoti ir išlikti. Organizacijos, diegdamos IS ir siekdamos didinti veiklos efektyvumą pritaikydamos informacines technologijas, priverstos keisti vidinius procesus, struktūrą ir pan. Vis daugiau taikant informacines sistemas, keičiasi informacijos vaidmuo pačioje organizacijoje. Dėl ypač padidėjusio interneto naudojimo, organizacija kartais tampa iš dalies ar net visiškai priklausoma nuo informacinių technologijų veikimo bei patikimumo. Tampa būtinybe objektyviai įvertinti IS ar jų dalių efektyvumą, naudą bei riziką. Tokio įvertinimo priemonė yra IT auditas (Aleliūnas, Atkočiūnienė 2010; Amancei, Surcel 2010; Debreceny 2006; Iliescu 2010; Radovanović *et al.* 2010; Senft, Gallegos 2009). Mokslininkai akcentuoja IT sistemų efektyvumo ir naudos (kokią naudą jos teikia organizacijai ir jos pelningumui bei efektyvumui, siekiant įgyvendinti organizacijos tikslus) vertinimą (Ginevičius *et al.* 2005; Ginevičius *et al.* 2006; Jakubavičius, Vilys 2008; Oržekauskas, Šmaizienė 2009; Spafford 2003). Dažniausiai analizuojama, kaip efektyviai naudojami IT resursai, koks IT ir organizacijos verslo strategijos santykis, daug dėmesio skiriama IT rizikos valdymui. Mokslininkai vieningai sutaria,

kad informacinių technologijų auditas yra būtina sąlyga efektyviam ir pelningam verslui. M. Petterson (2010) teigia, kad vienas iš pagrindinių IT audito iššūkių yra išlaikyti greitą tempą, taip pat diegti naujas technologijas įmonėje. Praktikoje pasitelkiamos įvairios IT audito metodikos bei standartai (ITGI 2007; ITSMF 2007; INTOSAI 2010; LST ISO/IEC 27002 2009; Val IT 2008).

IT auditas yra gana naujas reiškinys, kurio reikšmingumas yra neginčytinas, tačiau jis kol kas nėra labai dažnas reiškinys Lietuvos įmonėse (ypač SVV įmonėse). Kadangi IT taikymo ypatybės priklauso nuo organizacijos dydžio (veiklos apimtis, darbuotojų skaičius ir pan.), straipsnyje detalčiau bus analizuojamas IT auditas SVV įmonėse. LR įstatymais reglamentuotas įmonių skirstymas: maža įmonė – tai įmonė, kurioje dirba mažiau kaip 50 darbuotojų, įmonės metinės pajamos neviršija 24 mln. litų ar įmonės turto balansinė vertė yra ne didesnė kaip 17 mln. litų ir įmonė yra savarankiška; vidutinė įmonė – įmonė, kurioje dirba mažiau kaip 250 darbuotojų, įmonės metinės pajamos neviršija 138 mln. litų ar įmonės balansinė vertė ne didesnė kaip 93 mln. litų ir yra savarankiška.

*Straipsnio tikslas* – įvertinti IT audito metodikų taikymo galimybes Lietuvos SVV įmonėms.

Siekiant tikslo, analizuojamas IT audito poreikis ir situacija Lietuvos SVV įmonėse, Lietuvos ir pasaulio audito praktika, pasaulio praktikoje taikomos IT audito metodikos. Naudojami metodai: sisteminė literatūros analizė, sugretinimas, statistinių duomenų analizė.

## IT Lietuvos SVV įmonėse

Informacinių technologijų vaidmuo organizacijoje priklauso nuo daugelio veiksnių, tokių kaip įmonės veikla, dydis bei kompiuterizacijos lygis. IT ypač svarbios SVV įmonėse, nes taikant informacines technologijas įmonė tampa lankstesnė, konkurencingesnė ir gali koncentruotis būtent į vartotoją, o ne tik į gamybos priemones (Taylor, Glezen 1988; Ginevičius *et al.* 2005; Ginevičius *et al.* 2006; Elskytė, Raudeliūnienė 2006; Davidavičienė 2008). LR statistikos departamento duomenimis (2010a), per pastaruosius penkerius metus 5,2 % padaugėjo įmonių, savo veikloje naudojančių kompiuterius, 11 % – įmonių, naudojančių internetą. 2010 m. kompiuteriais naudojosi 96,9 % (2005 m. – 91,7 %), internetu – 96,2 % (2005 m. – 85,2 %) apdirbamosios gamybos ir paslaugų sektoriaus įmonių. Kompiuterius kasdieniame darbe bent kartą per savaitę naudojo 32,8 % gamybos ir paslaugų įmonių darbuotojų, internetą – 29,7 % (2009 m. – atitinkamai 31,4 % ir 28,8 %).

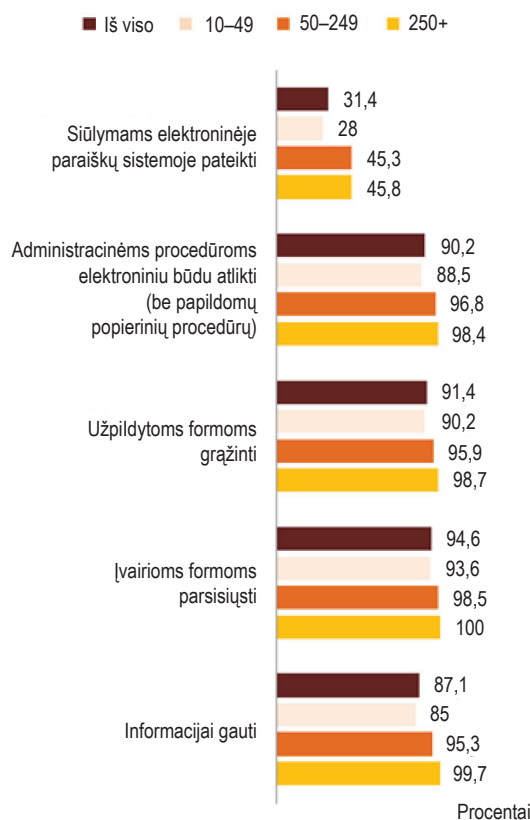
2010 m. interneto tinklalapį ar svetainę turėjo 65,2 % gamybos ir paslaugų įmonių (2009 m. – 61,7%). 39,4 % įmonių nurodė, kad interneto tinklalapiuose buvo skelbiami įmonių prekių ar paslaugų katalogai ir kainynai, 17 % įmonių teikė galimybę pasirinkti norimo produkto formą ar dizainą, 17,1 % – galimybę užsisakyti, rezervuoti ar pirkti norimus produktus.

Beveik visos įmonės (92,9 %) naudojo internetą bankų ir kitų finansinių institucijų paslaugoms, daugiau kaip pusė įmonių (50,6 %) – darbuotojams mokyti ir šviesti. 95 % įmonių 2009 m. internetą naudojo bendraudamos su valstybės institucijomis (2008 m. – 90,4 %) (1 pav.). 2010 m. pradžioje skaitmenines tapatybės identifikavimo priemones naudojo 68,9 % įmonių, kuriose dirbo 10 ir daugiau darbuotojų (2009 m. – 23,9 %).

Apibendrinant galima teigti, kad:

- Dėl vis didėjančių verslo poreikių, konkurencijos, informacijos kiekio informacinės technologijos sparčiai plinta SVV įmonėse.
- Vis daugiau SVV įmonių naudojami plačiajuosčiu internetu, kuris užtikrina patikimą bei saugų duomenų perdavimo ryšį.
- 2010 m. SVV įmonėse įvairių rūšių informacinių sistemų panaudojimo tendencija augo, o tai rodo vis didėjančią IT paklausą.

Augantis IT naudojimas SVV įmonėse sukuria konkurencinį pranašumą, galimybę optimizuoti verslo procesus ir pan., tačiau taip pat kyla iššūkių siekiant užtikrinti informacijos saugumą (2 pav.). 2010 m. elektroninės saugos priemonės naudojo 90,4 % įmonių. 2010 metų duomenų



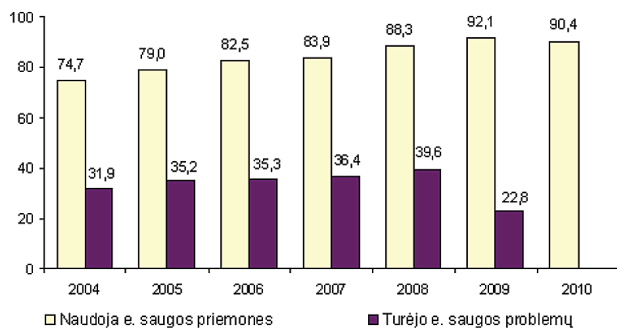
**1 pav.** Bendravimo internetu su valstybės institucijomis tikslai pagal įmonių dydžio grupes (% , 2009 m.) (LR statistikos departamentas 2010b)

**Fig. 1.** Purpose of communication with public authorities over the Internet, by size group (% in 2009) (Source: Statistics Department of Lithuania 2010b)

apie e. saugumo problemas LR statistikos departamentas neteikia, tačiau 2009 m. duomenys rodo, kad 22,8 % įmonių buvo susidūrusios su tokiomis problemomis. CERT-LT duomenimis, 2009 m. dažniausiai susidurta su tinklų ir informacijos saugumo problemomis: kompiuteriniai virusai (95,2 %), nepageidaujami elektroniniai laišakai (SPAM) (1,0 %), elektroninės paslaugos trikdymo ataka (0,3 %), neteisėtas turinys (0,6 %), užvaldymas (1,4 %), klastojimas (0,3 %), manipuliacija (0,1 %) ir kiti incidentai (1,0 %).

Siekiant mažinti e. saugumo problemas ir eliminuoti riziką, pirmiausia tikslinga atlikti IT auditą, kuris sudaro prielaidas įmonės IT rizikai sumažinti. Tuo tikslu reikia įvertinti: įmonės verslo procesus, veiklos specifiką, naudojamą informacines technologijas, apsaugos priemones, kylančią grėsmę ir pasaulio praktiką.

Didelių įmonių vadovai, suvokdami IT svarbą organizacijai, renka skirtingus IT valdymo (t. p. audito) modelius. Pavyzdžiui: AB „Swedbank“, UAB „Bitė Lietuva“ ir UAB „Ingman ledai“ naudoja Cobit; ITIL yra pasirinkusi AB „Lietuvos energija“, AB „DnB NORD bankas“.



**2 pav.** Įmonės, susidūrusios su elektroninės saugos problemomis, % (LR statistikos departamentas 2010b)

**Fig. 2.** Companies, faced with the challenges of electronic security, in % (Source: Statistics Department of Lithuania 2010b)

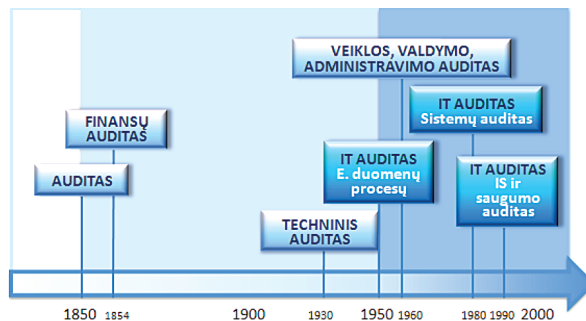
Viena iš IT audito nepopuliarumo SVV įmonėse priežasčių galėtų būti tai, kad tik 2002 m. Lietuvoje buvo įkurtas Tarptautinės informacinių sistemų audito ir valdymo asociacijos (ISACA) skyrius (šiuo metu asociacijoje yra per 50 narių). 2008 m. LR Vyriausybė priėmė nutarimą pavesti nacionalinio CERT funkcijas Lietuvos Respublikos ryšių reguliavimo tarnybai (RRT). CERT-LT – tai Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio misija yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. CERT-LT koordinuoja ir įgyvendina programinius sprendimus, susijusius su tinklų ir informacijos saugumu, atlieka prevencinę veiklą, teikia informaciją apie naujausias grėsmės galimybes kompiuterių naudotojams. Valstybė nereguliuoja privalomai vykdyti įmonių IT auditą. Tačiau numatytais atvejais gali būti atliekamas IS (informacinių sistemų) auditas.

Dažniausiai šiuo metu Lietuvoje IT auditoriams tenka ne tik vertintojų, bet ir IT konsultantų vaidmuo.

### IT audito turinys

Siekiant identifikuoti IT audito elementus, jo atlikimo SVV pjūvius, būtina įvertinti šį procesą plačiaja prasme. Analizuojant IT auditą, tikslinga atsižvelgti ir į audito raidą (3 pav.). Istorškai susiklostė, kad auditas atsirado ir dažniausiai suvokiamas bei plačiausiai analizuojamas siejant jį su finansinės veiklos vertinimu – tai yra finansų auditu.

Tačiau tiek praktikoje, tiek moksle egzistuoja žymiai daugiau audito rūšių (Aleliūnas, Atkočiūnienė 2010; Amancei, Surcel 2010; Grundey 2008; Iliescu 2010; INTOSAI 2010; Kaziliūnas 2008; Lakis 2007; Lakis 2008; Lo, Marchand 2004; Mackevičius 2001; Mattsson, Olsson 2006; Oržekauskas, Šmaižienė 2009; Peto 2006;



**3 pav.** Audito raida (sudaryta autorių pagal: Amancei, Surcel 2010; Iliescu 2010; Lo, Marchand 2004; Mattsson, Olsson 2006; Oržekauskas, Šmaižienė 2009; Peto 2006; Puškorius 2004; Senft, Gallegos 2009; Taylor 1988)

**Fig. 3.** Development of Audit (compiled by the authors: Amance, Surcel 2010; Iliescu 2010; Lo, Marchand 2004; Mattsson, Olsson 2006; Oržekauskas, Šmaižienė 2009; Peto 2006; Puškorius 2004; Senft, Gallegos 2009; Taylor 1988)

Puškorius 2004; Radovanović *et al.* 2010; Senft, Gallegos 2009; Taylor, Glezen 1988):

*finansinis auditas* (finansinės veiklos analizė ir vertinimas), *valdymo auditas* (organizacijų valdymo struktūros ir sistemos pagrįstumo ir tikslingumo, jos funkcionavimo, naudojamų IS turėjimas ir jų panaudojimo lygio vertinimas, kartu vertinant galimybes transformuotis reaguojant į vykstančius pokyčius);

*administravimo auditas* (organizacijos administravimo sistemos vertinimas: dokumentų valdymas, procedūros, komunikavimo sistemos veikimas, IS įsisavinimas ir naudojimas, kontrolė ir atsiskaitymas, darbuotojų pareiginės instrukcijos, jų atitikimas priskirtoms ir faktiškai atliekamoms pareigoms);

*veiklos auditas* (visų galimų organizacijos veiklos sričių, pvz., rinkotyros ir rinkodaros, prekybinės veiklos, logistikos sistemų veikimo, gamybos paruošimo ir jos vykdymo, atsargų valdymo, verslo modelio vertinimas. Jis kartais įvardijamas kaip informacijos auditas);

*techninis auditas* (įvairių įrenginių, energetinės sistemos veikimo ir efektyvumo vertinimas ir pan.);

*IT auditas* (įrodymų apie tai, kaip informacinės sistemos palaiko duomenų vientisumą, saugumo reikalavimus ir leidžia įmonei efektyviai siekti naudos bei panaudoti resursus, rinkimas ir vertinimas);

*saugumo auditas* (IS audito dalis: vertina vidaus kontrolės būklę informacijos apsaugos srityje, teikia rekomendacijas būklei pagerinti, vertina tiek informacijos saugumo lygį, tiek administruojant informaciją IT priemonėmis).

Vertinant audito raidą ir jo rūšis, galima daryti išvadą, kad IT auditas informaciniame amžiuje glaudžiai susijęs su visomis kitomis auditavimo rūšimis, nes informacinės technologijos tampa neatskiriama bet kurio organizacijos vei-

klos proceso dalis. Taigi informacinių technologijų auditas toliau traktuojamas kaip specializuotas auditas, kurio metu peržiūrimi ir aprašomi visi informacinių sistemų aspektai, įtraukiant techninę ir programinę įrangą, IT aplinką bei sistemų kūrimą. IT auditas apima su IT susijusios rizikos nustatymą ir informacijos įvedimo, apdorojimo ir išvedimo kontrolės aprašymą (Aleliūnas, Atkočiūnienė 2010).

Vertinant SVV organizacijų IT audito galimybes, tikslinga identifikuoti galimus ir svarbiausius IT audito pjevius.

Visų pirma, reikia įvertinti problemas, su kuriomis organizacijos susiduria konkuruodamos, ir būdus, kuriais informacinės sistemos gali suteikti konkurencinį pranašumą skirtingais verslo lygiais (IT gali sumažinti valdymo sąnaudas, informacijos gavimo ir analizės išlaidas, sudaro prielaidas pajamoms didinti mažinant vidutinį valdymo lygio tarnautojų skaičių, mažoms įmonėms sudaro prielaidas didinti pajėgumą nedidinant darbuotojų skaičiaus). Kadangi IT audito tikslas yra identifikuoti ir įvertinti prioritetinius IT įmonės poreikius, stiprybes, galimybes, grėsmės atvejus, išskirti reikšmingesnę veiklą, kurią reikia įsisavinti, tai turi būti siejama su verslo procesais. Tačiau IT poreikių vertinimo tikslas – nustatyti naudojamas technologijas ir jų atitiktį verslo strategijai ir organizacijos poreikiams. IT turi padėti organizacijai sumažinti išlaidas, diferencijuoti ir pakeisti konkurencinę erdvę. Išskiriami trys strateginiai organizacijų naudojimosi informacinėmis technologijomis lygiai (Ginevičius *et al.* 2005): *gamybos* lygiu strategija gali būti nukreipta į mažiausias gamybos išlaidas; *organizacijos* lygiu – tai gali būti produkcijos ar paslaugų diferencijavimas; *verslo* lygiu – pakeisti rinką.

Kitas svarbus aspektas – organizacijos veiklos pobūdis. Nuo jo priklausys, koks IT naudojimo lygis vykdamas auditą bus pagrindinis. Pagal veiklos pobūdį organizacijos skirstomos į 5 kategorijas (Ginevičius, Sūdžius 2008; Jurkštienė *et al.* 2008): 1) gamybos įmonės; 2) technologijos įmonės (kurios nuo pirmosios grupės skiriasi aukštesne darbuotojų kvalifikacija); 3) verslo ir finansinių paslaugų įmonės; 4) turizmo, mažmeninės prekybos, sveikatos, švietimo ir pramogų paslaugų įmonės; 5) vietos paslaugų įmonės.

Ne mažiau svarbus kalbant apie IT auditą – organizacijos vadovų požiūris į pačias informacines technologijas ir tokio audito būtinumą. Skiriami trys įmonių tipai pagal tai, kaip organizacijų vadovai supranta IT audito būtinybę (Bakshi 2006):

- *Pirmajai grupei* priklauso progresyvios, pažangios ir visiškai kompiuterizuotos organizacijos. Jos ne tik gerai supranta IT audito būtinybę, bet ir jį periodiškai atlieka, siekdamas išvengti klaidų ir praradimų silpniausiose sistemos vietose.

- *Antrąją grupę* sudaro įmonės, kurių vadovai susipažinę su IT audito reikalingumu, tačiau nenoriai sutinka, kad tai būtina.

- *Trečiosios grupės* organizacijos nemato būtinybės atlikti auditą; joms reikalingi kompiuterizuoti procesai, tačiau nėra nuo jų stipriai priklausomos.

SVV įmonės labai retai priskiriamos (arba pačios save identifikuoja) pirmosios grupės atstovams. Tačiau atsižvelgiant į statistinius rodiklius, akivaizdu, kad IT auditas tampa svarbus ir antrosios bei trečiosios grupės atstovams. Dažniausiai kaip svarbiausios IT valdymo sritys SVV įmonėms yra įvardijamos: duomenų apsauga nuo praradimo, interneto ryšio patikimumas ir apsauga nuo interneto keliamų pavojų. SVV yra jautresnės incidentams ir nenumatytiems įvykiams, kurie gali sustabdyti darbą keletui dienų. Pavyzdžiui, net 43 % įmonių darbas kuriam laikui sutriktų, jei įmonė dėl tam tikrų priežasčių netektų savo duomenų; 26 % įmonių dėl to patirtų didelių finansinių nuostolių, o 21 % iš viso negalėtų tęsti savo veiklos (RAIT atliktos Lietuvos SVV įmonių apklausos duomenys (Likevičius 2006)). Taigi vykdamas SVV įmonių IT auditą, akcentuotinas duomenų saugumas.

Mokslininkai pabrėžia skirtingas IT rizikos vertinimo apimtis ir gylį, kurie priklauso nuo organizacijos veiklos, informacinių vertybių, patirties informacijos saugos užtikrinimo srityje ir finansinių galimybių (Aleliūnas, Atkočiūnienė 2010; Rainys 2006; Stewart 2004). Siekiant identifikuoti tinkamiausią IT audito metodiką, SVV įmonėms būtina atsižvelgti į tai, kad: SVV organizacijų ištekliai yra riboti, todėl būtina vengti nereikalingų auditavimo veiksmų (turėtų būti audituojami tik organizacijai kritiškai svarbūs aspektai). Svarbiausi audituojami objektai nustatomi atsižvelgiant į organizacijos veiklą, struktūrą ir informacinių technologijų svarbą įmonės veikloje.

Nėra vieno IT audito standarto, kadangi šis procesas priklauso nuo daugelio veiksnių, tokių kaip organizacijos tipas, technologijų naudojimo paskirtis ir lygis, vadovų požiūris ir pan. (Iliescu 2010; ITGI 2007; ITSMF 2007; Jakubavičius, Vilys 2008; LST ISO/IEC 27002 2009; Radovanović *et al.* 2010; Senft, Gallegos 2009). Tačiau daugelis IT audito modelių turi panašią struktūrą ir žingsnių seką (Jakubavičius, Vilys 2008). IT audito seka yra panaši į kitų audito rūšių (1 lentelė).

Pabrėžtina, kad IT audite turi atspindėti tokie SVV įmonių poreikiai kaip: produkto padėtis rinkoje, užtikrinanti įmonės konkurencingumą ir tvarią plėtrą; veiklos automatizavimas, informacinių technologijų pokyčiai; bendrojo pobūdžio problemos ar funkcijos, reikalaujančios inovacinių sprendimų; perdavimo priemonės; techninė pagalba, intelektinė nuosavybė.

**1 lentelė.** Audito procesas (sudaryta autorių pagal: Botha, Boon 2003; Gheorghe 2010; Iliescu 2010; Jakubavičius, Vilys 2008; Oržekauskas, Šmaižienė 2009; Senft, Gallegos 2009)

**Table 1.** Audit process (concluded by the authors: Botha, Boon 2003; Gheorghe 2010; Iliescu 2010; Jakubavičius, Vilys 2008; Oržekauskas, Šmaižienė 2009; Senft, Gallegos 2009)

Audito procesas	IT audito procesas
Audito poreikio atsiradimas organizacijoje.	Audituojamos srities nustatymas.
Audito vykdytojų parinkimas. Audito tikslų ir uždavinių nustatymas (programos parengimas, derinimas, koregavimas ir tvirtinimas).	Audito tikslų nustatymas.
Audito programos vykdymo plano sudarymas, jo derinimas su organizacija, koregavimas ir tvirtinimas.	Audito programos vykdymo plano sudarymas, jo derinimas su organizacija, koregavimas ir tvirtinimas.
Audito vykdymas, gautų audito rezultatų analizė ir vertinimas, ataskaitos rašymas, pateikimas organizacijai, svarstymas ir tvirtinimas.	Informacinės architektūros apibrėžimas, informacinio turto identifikavimas, saugumo rizikos vertinimas, kontrolės vertinimas, atitikties testavimas, pagrindinės įrangos testavimas, gautų audito rezultatų analizė ir vertinimas.
Būtinų pokyčių programos įgyvendinimo parengimas, svarstymas ir tvirtinimas. Darbuotojų psichologinis paruošimas ir apmokymas, pokyčių įgyvendinimas.	Ataskaita apie nustatytas silpnąsias vietas.
Atliktų ir įgyvendintų pokyčių pakartotinis auditas, monitoringas.	

## IT audito metodikos

Siekiant suformuoti rekomendacijas SVV IT audito procesui, tikslinga atlikti egzistuojančių metodikų, standartų bei modelių vertinimą atsižvelgiant į jau identifikuotus SVV poreikius ir specifiką. Audito koncepcijos paprastai atsispindi tam tikruose audito standartuose ir etikos kodeksuose, tiksliau tariant, yra jų pagrindas. Audito standartai – tai taisyklės, principai ir procedūros, kurios nustato audito atlikimą ir auditorių veiklą (Aleliūnas, Atkočiūnienė 2010). Juos rengia tokios organizacijos kaip: Tarptautinė standartizacijos organizacija (ISO); Tarptautinė elektrotechnikos komisija (IEC); Vidaus auditorių asociacija (IIA), Tarptautinė apskaitininkų federacija (IFAC), Tarptautinė aukščiausiųjų audito institucijų organizacija (INTOSAI), Tarptautinės informacinių sistemų audito ir valdymo asoci-

acijos (ISACA). Labiausiai paplitę standartai ir metodikos yra: CobIT, ITIL, ISO/IEC ir kiek mažiau paplitusi nauja metodika Val IT.

*CobIT* (angl. *Control Objectives for Information and Related Technologies*) – viena iš populiarių IT valdymo metodikų, kuriama ir palaikoma tarptautinės ISACA organizacijos bei ITGI. CobIT skirta organizacijos valdymui, kontrolei ir auditui. Ši metodika sujungia verslo ir IT tikslus, suteikia galimybę stebėti informacijos sistemos brandą. Taip pat leidžia optimizuoti IT resursus, tokius kaip taikomosios programos, informacija, infrastruktūra ir žmonės (Radovanović *et al.* 2010). Pirmoji CobIT versija buvo sukurta kaip priemonė auditui. Dabar CobIT turi keturias pagrindines dalis: planavimas ir organizavimas, pirkimas ir įdiegimas, naudojimas ir aptarnavimas, taip pat monitoringas. CobIT daugiau skirta didelėms įmonėms, kurios privalo laikytis tam tikrų reglamentų. CobIT užtikrina kompleksines rizikos analizės ir audito planavimo priemones (medžiaga audito programai, geros praktikos atvejų analizė ir gairės). Speciali CobIT versija „Quickstart“ skirta SVV įmonėms, atsižvelgiant į jų poreikius (t. y. ribotus išteklius) (ITGI 2007).

*Val IT* (angl. *Value Management IT*) – tai sistema, leidžianti kurti pridėtinę verslo vertę, kai investuojama į informacines technologijas. Tai patvirtintos valdymo ir techninių reikalavimų gairės, skirtos investicijoms į IT planuoti, vertinti, valdyti ir kt. Yra trys pagrindinės Val IT sritys: vertės strateginis valdymas, portfelio valdymas ir investicijų valdymas (Val IT 2008). Val IT tikslas – užtikrinti organizacijos pelną optimizuojant išlaidų ir rizikos balansą. Val IT sukurtas CobIT pagrindu ir papildo jį IT investicijų vertinimo aspektu.

*ITIL* – (angl. *Information Technology Infrastructure Library*) – ITT verslo valdymo metodika, orientuota į IT paslaugų valdymo standartus, darbo optimizavimą ir kokybės užtikrinimą IT kompanijose ar įmonių IT padaliniuose. ITIL yra suderinamas su ISO-9000. ITIL tikslas – optimizuoti IT procesus, kad jie tenkintų organizacijos poreikius, užtikrinant IT kokybę ir mažinant išlaidas. ITIL v3 versija apima penkias sritis: paslaugų strategija, paslaugų kūrimas, paslaugų įvedimas, paslaugų vykdymas, nuolatinis paslaugų gerinimas (ITSMF 2007).

*ISO 27002 Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)* – standartas, kurį 2000 m. patvirtino Tarptautinė standartizacijos organizacija (ISO) ir Tarptautinė elektrotechnikos komisija (IEC). Standartas nustato gaires ir bendruosius principus, kaip inicijuoti, įgyvendinti, prižiūrėti ir gerinti informacijos saugumo valdymą organizacijoje. Standartas apima pagrindinius informacijos saugos aspektus: saugumo politiką, organizacijos saugumą,

turto klasifikaciją ir kontrolę, fizinį ir aplinkos saugumą, asmeninį saugumą, komunikacijos ir operacijų valdymą, prieigos kontrolę, sistemų vystymą ir palaikymą, verslo tęstinumo valdymą ir suderinamumą (LST ISO 27002 2009; Spafford 2003).

Kiekviena iš pristatytų metodikų padeda optimizuoti informacinių technologijų procesus ir IT efektyvumą organizacijoje, tačiau siekiant parengti IT audito SVV įmonėms rekomendacijas, tikslinga atlikti jų palyginamąją analizę (2 lentelė).

**2 lentelė.** IT audito metodikų palyginimas SVV (sudaryta autorių pagal: Iliescu 2010; ITGI 2007; ITSMF 2007; LST ISO/IEC 27002 2009; Nurguzhina 2007; Radovanović *et al.* 2010; Senft, Gallegos 2009; Spafford 2003; Val IT 2008)

**Table 2.** Comparison of SMB IT audit methodology (concluded by the authors: Iliescu in 2010, ITGI 2007; itSMF 2007, ISO / IEC 27002 in 2009; Nurguzhina 2007; Radovanović *et al.* 2010; Senft, Gallegos 2009, Spafford 2003, Val IT 2008)

	CobIT	ITIL	ISO 27002	Val IT
Mažos diegimo sąnaudos	-	+	+	-
Galima diegti dalimis	-	+	-	+
Paprastas realizavimas	-	+	~	-
Saugumo kontrolė	~	-	+	~
Formuluoja konkrečias rekomendacijas, kaip įgyvendinti pokyčius	-	+	-	+
Formuluoja rekomendacijas, kokie pokyčiai turėtų būti inicijuoti	+	-	+	-
Orientuojamasi į: auditorių	+	~	-	-
IT vartotoją	+	+	+	-
vadovą	+	-	-	+
Orientuota į organizacijas, kurioms IT auditas privalomas (reglamentuotas įstatymais)	+	-	+	-
Žymėjimo reikšmės: (-) – ne / nėra, (+) – taip / yra, (~) – vidutiniškai				

Akcentuotina tai, kad svarbiausia rinktis tokią metodiką, kuri atitiktų pagrindinius organizacijos procesus ir poreikius. Taigi SVV įmonė, prieš pasirinkdama IT audito metodiką, turi aiškiai suformuluoti tikslus, t. y. kokio rezultato siekia (padidinti saugumą, sumažinti riziką, sumažinti darbo sąnaudas, įvertinti situaciją, sertifikuoti įmonės IT ir pan.). Ne visais atvejais gali pakakti vienos iš analizuojamų metodikų. Lentelėje išskirtos pagrindinės keturių metodikų (Cobit, ITIL, ISO, Val IT) savybės.

Kiekviena iš išvardintų metodikų, siekiant tenkinti rinkos bei vartotojų poreikius turi supaprastintas (orientuotas į SVV) versijas: CobIT – Quickstar, ITIL – FITS, Val IT – akcentuojama galimybė diegti etapais (dalimis). Tačiau ISO 27002 standartas jokių supaprastintų versijų neteikia, nes SVV susiduria su tokia pat saugumo rizika kaip ir didelės organizacijos.

Atlikus palyginamąją analizę, galima teigti, kad:

- CobIT užtikrina įmonės IT efektyvumą, padeda apibrėžti IT procesus, praktiką, kontrolės metodus. Ribojimai SVV įmonių atveju yra: apskaitos audito akcentavimas, būtinybė taikyti pilną CobIT versiją, labiau orientuotą į organizacijas, kurių IT veiklą reglamentuoja įstatymai. Kaip privalumas yra tai, kad CobIT orientuotas vertinti visas IT auditu suinteresuotas grupes, t. y. auditorius, IT naudotojus (vartotojus), vadovus (asmenis, kurie suinteresuoti IT efektyvumo didinimu ir saugumo užtikrinimu).
- ITIL orientuota į darbo optimizavimą bei kokybės užtikrinimą IT kompanijose ir įmonių IT padalinuose. Kaip privalumas SVV įmonėms – galimybė diegti dalimis. Ribotumas – orientuota į paslaugų sektoriaus įmones, akcentuojami IT procesai. Kita vertus, skirtingai nei CobIT, ITIL nekelia ypatingų reikalavimų, susijusių su auditu, todėl diegimas yra žymiai paprastesnis.
- ISO akcentuojamas informacijos saugumas ir rizikos valdymas. Negali būti laikomas visapuse IT valdymo priemone. Privalumas – orientuota į bet kokių IT sistemų, duomenų, veiklos saugumo užtikrinimą. Ribotumas: negalima diegti dalimis, nėra formuluojamos konkrečios rekomendacijos, kokiomis priemonėmis reikėtų užtikrinti saugumą ir įgyvendinti pokyčius.
- Val IT metodikoje daugiau dėmesio skiriama investicijoms ir organizacijos vertei kurti. Kaip privalumas – galimybė diegti dalimis, konkrečių rekomendacijų formulavimas IT modernizuoti ir procesams optimizuoti. Tai aktualiausia vadovams sprendimų priėmimo procese. Kaip trūkumas, atsižvelgiant į SVV įmonių poreikius, gali būti įvardintos didelės sąnaudos.

Kiekviena iš nagrinėtų metodikų turi savo specifiką, nors specialistai neretai jas apibūdina kaip universalias. Taigi įvertinus įmonės tikslus, poreikius ir alternatyvias metodikas, gali tekti priimti sprendimą pasitelkti kelias metodikas vienu metu. SVV įmonės dažniau renkasi supaprastintas vienos ar kelių metodikų versijas.

## Išvados

IT auditas sudaro prielaidas įmonės IT rizikai mažinti, kai įvertinami įmonės verslo procesai, veiklos specifika, naudojamos informacinės technologijos, apsaugos priemonės, grėsmės atvejai, pasaulio praktika ir pan. Išanalizavus informacinių technologijų įsisavinimo lygį SVV įmonėse, įvertinus šio tipo įmonių poreikius, galima teigti, kad siekiant mažinti e. saugumo problemas ir eliminuoti su IT susijusią riziką bei didinti SVV įmonių veiklos efektyvumą, būtina sąlyga tampa IT auditas.

Siekiant identifikuoti IT audito elementus, atlikta audito raidos analizė, kuri parodė, kad IT auditas glaudžiai susijęs su kitomis audito rūšimis (finansų, veiklos, valdymo, techniniu administravimo auditu). Dažniausiai kaip svarbiausios IT valdymo sritys SVV įmonėms yra įvardijamos: duomenų apsauga nuo duomenų praradimo, interneto ryšio patikimumas bei apsauga nuo interneto keliamų grėsmės atvejų. SVV yra jautresnės incidentams ir nenumatytiems įvykiams.

SVV organizacijų išteklių yra riboti, todėl būtina vengti nereikalingų auditavimo veiksmų. Atsižvelgiant į SVV įmonių finansines galimybes, kritiškai vertinant jų veiklos procesus ir reikmes, atlikta siūlomų IT audito metodikų analizė sudaro prielaidas tinkamai IT audito metodikai pasirinkti:

- organizacijos, glaudžiai susijusios su IT kiekvieną dieną bei vykdančios veiksmus ar procesus internete, turėtų pasirūpinti informacijos saugumu (ISO 27002 standartas).
- organizacijos, kurios orientuojasi į paslaugų teikimą, jų gerinimą, turėtų apsvarstyti ITIL metodikos pasirinkimo galimybę (arba supaprastintą jos versiją FITS).
- organizacijos, kurioms IT veikla yra itin svarbi (informacija turi būti patikima, o jų veiklą reglamentuoja ne tik Lietuvos Respublikos, bet ir kitų šalių įstatymai), turėtų rinktis CobIT metodiką (arba supaprastintą jos versiją Quickstart).

## Literatūra

Aleliūnas, I.; Atkočiūnienė, Z. 2010. Informacijos auditas kitų audito rūšių kontekste, *Informacijos mokslai* 54: 7–16. ISSN 1392-0561.

Amancei, C.; Surcel, T. 2010. Increasing the Efficiency of IT Audit Methodology by Using the Organizations Tolerance to IT Systems Availability, *Informatica Economica* 14(1): 62–66. ISSN 1790-2769.

Bakshi, Ch. 2006. *Information System Audit for Companies – Voluntary or Compulsory?* [interaktyvus], [žiūrėta 2010 m. lapkričio 20 d.]. Prieiga per internetą: <[http://www.icaai.org/resource\\_file/10000433-436.pdf](http://www.icaai.org/resource_file/10000433-436.pdf)>.

Botha, H.; Boon, J. A. 2003. The Information Audit: Principles and Guidelines, *Libri* 53: 23–38. ISSN 0024-2667.

Davidavičienė, V. 2008. Change management decisions in the information age, *Journal of Business Economics and Management* 9(4): 299–307. doi:10.3846/1611-1699.2008.9.299-307

Debreceny, R. S. 2006. Reengineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls, in *The Proceedings of the 39th Hawaii International Conference on System Sciences* 8: 1–10. doi:10.1109/HICSS.2006.407

Elskytė, V.; Raudeliūnienė, J. 2006. ITT plėtros sąlygotų verslo pokyčių vadyba, *Organizacijų vadyba: sisteminiai tyrimai* 38: 53–66. ISSN: 1392-1142.

Gheorghe, M. 2010. Audit Methodology for IT Governance, *Informatica Economica* 14(1): 32–42. ISSN: 1790-2769.

Ginevičius, R.; Bivainis, J.; Melnikas, B.; Paliulis, N.; V. Rutkauskas, A.; J. Staškevičius, A.; Pabedinskaitė, A.; Šečkutė, L.; Tamošiūnas, A. 2005. *Šiuolaikinis verslas: tobulinimo prioritetai*: kolektyvinė monografija. Vilnius: Technika. 448 p. ISBN 9986-05-832-5.

Ginevičius, R.; Paliulis, N. K.; Chlivickas, E.; Merkevičius, J. 2006. *XXI amžiaus iššūkiai: organizacijų ir visuomenės pokyčiai*: monografija. Vilnius: Technika. 548 p. ISBN 9955280573.

Ginevičius, R.; Sūdžius, V. 2008. *Organizacijų teorija*. Vilnius: Technika. 325 p. ISBN 978-9955-288-150-4.

Grundey, D. 2008. Audit System: Development and Problems, *Transformations in Business & Economics* 7(3): 192–196. ISSN 1648-4460.

Iliescu, F. M. 2010. Auditing IT Governance, *Informatica Economica* 14(1): 93–102. ISSN 0024-2667.

INTOSAI Working Group on IT Audit. 2010. *Office of the Comptroller and Auditor General*. IT Audit Monograph Series #1.

ITGI. 2007. *CobiT 4.1 – Framework, Control, Objectives, Management Guidelines and Maturity Model*. USA: IT Governance Institute. 213 p.

ITSMF. 2007. *An Introductory Overview of ITIL V3*. London: UK Chapter of the it SMF. 58 p.

Jakubavičius, A.; Vilys, M. 2008. Technology audit: initial tool for supporting innovation in SMES, in *The 5th International Scientific Conference „Business and Management“*. Selected papers. Ed. by R. Ginevičius, A. V. Rutkauskas, K. Didenko, T. Polajeva, J. Saeė. May 16–17, 2008. Vilnius, Lithuania. Vilnius: Technika, 267–272. ISBN 978-9955-28-311-9.

Jurkštienė, A.; Darškuvienė, V.; Dūda, A. 2008. Management control systems and stakeholders' interests in Lithuanian multinational companies: cases from the telecommunications industry, *Journal of Business Economics and Management* 9(2): 97–106. ISSN 1611-1699. doi:10.3846/1611-1699.2008.9.97-106

Kaziliūnas, A. 2008. Problems of auditing using quality management systems for sustainable development of organizations, *Technological and Economic Development of Economy* 14(1): 64–75. ISSN 1392-8619. doi:10.3846/2029-0187.2008.14.64-75

Lakis, V. 2007. *Audito sistema: raida ir problemos*: monografija. Vilnius: VU leidykla. 286 p. ISBN 978-9955-33-054-7.

- Lakis, V. 2008. Independent auditing development tendencies, *Technological and Economic Development of Economy* 14(2): 171–183. doi:10.3846/1392-8619.2008.14.171-183
- Likevičius, V. 2006. Nuomonė: ar smulkiam verslui reikia IT valdymo sprendimų? [interaktyvus], [žiūrėta 2011 m. sausio 13 d.]. Prieiga per internetą: <http://www.delfi.lt/news/daily/technology/nuomone-ar-smulkiam-verslui-reikia-it-valdymo-sprendimu.d?id=11565526>.
- Lo, E. C.; Marchand, M. 2004. Security Audit: A Case Study, in *The Canadian Conference „Electrical and Computer Engineering“* 2–5 May 2004, 1: 193–196. doi:10.1109/CCECE.2004.1344989
- LR statistikos departamentas. 2010a. *Informacinės technologijos Lietuvoje* [interaktyvus], [žiūrėta 2011 m. sausio 13 d.]. Prieiga per internetą: <http://www.stat.gov.lt/lt/catalog/pages\_list?id=1125>.
- LR statistikos departamentas. 2010 b. *Informacinių technologijų naudojimas įmonėse* [interaktyvus], [žiūrėta 2011 m. sausio 10 d.]. Prieiga per internetą: <http://www.stat.gov.lt/lt/news/view?id=8027>.
- LST ISO/IEC 27002:2009 *Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)*. Vilnius, 2009. 98 p.
- Mackevičius, J. 2001. *Auditas: teorija, praktika, perspektyvos*: monografija. Vilnius: Lietuvos mokslas. 827 p. ISBN 9986-795-04-4.
- Mattsson, B.; Olsson, P. 2006. Environmental Audits and Life Cycle Assessment, in Dillon, M.; Griffith (Eds.). *Auditing in the Food Industry – From Safety and Quality to Environmental and Other Audits*, Woodhead Publishing, 217 p. ISBN 1-85573-450-8.
- Nurguzhina, M. 2007. *IT security and risk management: ISO 17799* [interaktyvus], [žiūrėta 2011 m. sausio 10 d.]. Prieiga per internetą: <http://citebm.business.illinois.edu/TWC%20Class/Project\_rports\_Spring2007/Business%20Risk%20Management/mnurguz2/MNurguz2.pdf>.
- Oržekauskas, P.; Šmaižienė, I. 2009. Organizacijų valdymo ir administravimo audito modeliavimas, *Ekonomika ir vadyba* 14: 1163–1169. ISSN 1822-6515.
- Peto, D. 2006. Generalized Risk Assessment Index for Information Systems Auditing, in *28<sup>th</sup> Int. Conf. Information Technology Interfaces ITI 2006, Cavtat, Croatia, 2006*. 97–102. doi:10.1109/ITI.2006.1708459
- Petterson, M. 2010. *Finding Career Variety and Stability Through Certification*. [interaktyvus], [žiūrėta 2010 m. gruodžio 7 d.]. Prieiga per internetą: <http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/@ISACA-Volume9,28April2010.aspx>.
- Puškorius, S. 2004. *Veiklos auditas*: monografija. Vilnius: Lietuvos teisės universiteto Leidybos centras. 351 p. ISBN 9955-563-66-4.
- Radovanović, D.; Radojević, T.; Lucić, D.; Sarac, M. 2010. Analysis Of Methodology For IT Governance and Information Systems Audit, in *The 6<sup>th</sup> International Scientific Conference „Business and Management“*: Selected papers, vol. 2. by R. Ginevičius, A. V. Rutkauskas, R. Počas. (Eds.). May 13–14, 2010. Vilnius, Lithuania. Vilnius: Technika, 943–950. doi:10.3846/bm.2010.126
- Rainys, R. 2006. Tinklų ir informacijos saugumas. Tyrimai ir incidentų valdymas, *Elektronika ir elektrotechnika* 6(70): 1–6. ISSN 1392 – 1215.
- Senft, S.; Gallegos, F. 2009. *Information Technology Control and Audit*. Third ed. Boca Raton, USA: Taylor & Francis Group. 774 p. ISBN 10: 1420065505.
- Spafford, G. 2003. *The Benefits of Standard IT Governance Frameworks* [interaktyvus], [žiūrėta 2010 m. gruodžio 7 d.]. Prieiga per internetą: <www.itsmwatch.com/itil/article.php/2195051>.
- Stewart, A. 2004. On Risk: Perception and Direction, *Computers & Security* 23(5): 362–370. doi:10.1016/j.cose.2004.05.003
- Taylor, D.; Glezen G. 1988. *Auditing: Integrated Concepts and Procedures*. 4th edition. New York: John Wiley & Sons. 845 p. ISBN-10: 0471856517.
- Val IT Framework 2.0. 2008. [interaktyvus], [žiūrėta 2011 m. sausio 7 d.]. Prieiga per internetą: <http://www.isaca.org/Knowledge-Center/Research/Documents/ValIT-Framework2.0-Jul-2008.pdf>.

## POSSIBILITIES OF IT AUDIT IN SMALL AND MEDIUM SIZE COMPANIES IN LITHUANIA

R. Janeliūnienė, G. Liberytė, V. Davidavičienė

### Abstract

Information and communication technologies (ICT) have a decisive influence on the competitiveness of an organization. The efficiency of ICT management is a key factor in the process of production optimization, resource planning and management and other activities concerning the objectives of the organization. ICT like other resources have not only advantages, but also causes certain challenges for organizations. Information systems become an organic part of the organization. Thus, it is hard to imagine a contemporary organization where information and communication technologies are not used. The organizations, where activity success is based on ICT, are affecting external and internal factors as well as the ability to manage ICT and use different information systems. Success is not guaranteed by implementing a new information system or technology, because business processes should be evaluated taking into account the ability to react to potential changes. In order to prevent ICT risk, IT audit becomes extremely important within the organization. The aim of the article is to evaluate the possibilities of applying the existing IT audit methodologies (such as ITIL, CobIT, Val IT, ISO) in small and medium size organizations of Lithuania. The paper analyzes the significance and need of IT audit in small and medium size companies, identifies the features of such companies and proposes the existing IT audit methodologies. The methods of scientific literature analysis and comparison and statistical data analysis have been applied in the article.

**Keywords:** IT audit, audit methods, small and medium size companies, IT risk evaluation.