5100-osios

GUID

Informacinių sistemų audito gairės

INTOSAI gairės parengtos Tarptautinės aukščiausiųjų audito institucijų organizacijos (INTOSAI) kaip INTOSAI profesinių nutarimų sistemos dalis. Daugiau informacijos galima rasti adresu www.issai.org

INTOSAI

Iki IFPP dokumentas – šis dokumentas buvo parengtas iki sukuriant INTOSAI profesinių nutarimų sistemą (IFPP) 2016 m., todėl formalia paskirtimi gali skirtis nuo naujausių INTOSAI audito gairių.

INTOSAI

INTOSAI 2019 m.

1) Patvirtintas kaip 5300-asis TAAIS „IT audito gairės“ 2016 m.
2) Dokumentas peržiūrėtas ir pervadintas 5100-osiomis GUID „Informacinių sistemų audito gairės“ 2019 m.

TURINYS

1. ĮŽANGA 4
2. ŠIŲ GAIRIŲ TIKSLAS 6
3. SĄVOKOS 7
4. APIMTIS 8
5. IS AUDITO PLANAVIMAS 9
6. IS AUDITO ATLIKIMAS 14
7. IS AUDITO ATASKAITŲ TEIKIMAS 19
8. VEIKSMAI PO AUDITO 20

1 ĮŽANGA

1.1 5100-osiose GUID pateikiama bendra sistema, skirta informacinių sistemų auditui atlikti IFPP struktūroje. Šios gairės skirtos suteikti pagrindą būsimoms 5100–5109 serijos informacinių sistemų audito gairėms rengti pagal IFPP sistemą.

1.2 Šiomis gairėmis nustatyta sistema atitinka *pagrindinius viešojo sektoriaus audito principus* (100-asis TAAIS), *pagrindinius finansinio audito principus* (200-asis TAAIS), *veiklos audito principus* (300-asis TAAIS) ir *atitikties audito principus* (400-asis TAAIS).

1.3 Aukščiausiosios audito institucijos (AAI) yra įgaliotos atlikti vyriausybių ir jų subjektų auditą pagal joms suteiktus audito įgaliojimus[1]. Savo veikla AAI siekia skatinti viešojo administravimo[2] efektyvumą, atskaitomybę, veiksmingumą ir skaidrumą.

1.4 Vyriausybės ir kiti viešojo sektoriaus subjektai nuolat diegia informacinių technologijų (IT) naujoves savo informacinėse sistemose, kad padidintų jų veikimo ir įvairių viešųjų paslaugų teikimo efektyvumą ir veiksmingumą. Taip yra todėl, kad IT suteikia galimybę rinkti, saugoti, apdoroti, gauti ir pateikti informaciją elektroniniu būdu, o tai, savo ruožtu, suteikia daug galimybių pagerinti informacinių sistemų tikslumą, konfidencialumą ir priemonių įgyvendinimą laiku. Be to, viešųjų paslaugų teikimo būdas sparčiai pereina nuo fizinio prie elektroninio, todėl valdžios institucijos turi veikti kaip skaitmeninės platformos, teikiančios paslaugas ir infrastruktūrą kitoms IT grindžiamoms informacinėms sistemoms.

1.5 Audituojamų viešojo sektoriaus subjektų perėjimas prie kompiuterizuotų informacinių sistemų ir elektroninio duomenų apdorojimo labai pakeitė aplinką, kurioje veikia AAI. Viešojo sektoriaus IT išlaidos didėja. Taip pat viešojo

[1] 1-asis INTOSAI-P *Limos deklaracija.*

[2] Jungtinių Tautų Generalinės Asamblėjos rezoliucija Nr. A/66/209.

sektoriaus subjektai privalo taikyti IT vidaus kontrolės priemones, kad būtų užtikrintas duomenų konfidencialumas, vientisumas ir prieinamumas. Todėl AAI būtina tobulinti atitinkamus gebėjimus atlikti išsamų su informacinėmis sistemomis susijusių kontrolės priemonių patikrinimą.

2 ŠIŲ GAIRIŲ TIKSLAS

2.1 100-asis, 200-asis, 300-asis ir 400-asis TAAIS nustato pagrindinius finansinio, veiklos ir atitikties auditų principus. Šie TAAIS yra susiję su bendraisiais principais, procedūromis, standartais ir auditoriaus lūkesčiais. Jie taikomi ir atliekant informacinių sistemų auditą.

2.2 Šių gairių tikslas – pateikti auditoriams nurodymus, kaip atlikti veiklos ir (arba) atitikties auditus, kai jie yra susiję su konkrečiu informacinių sistemų dalyku arba kai informacinių sistemų auditas yra platesnio masto audito, kuris gali būti finansinis, atitikties ar veiklos, dalis.

2.3 Šių gairių turinį auditoriai gali taikyti audito proceso planavimo, atlikimo, ataskaitų teikimo ir veiksmų po audito etapuose[3].

[3] 100-asis TAAIS.

3 SĄVOKOS

3.1 Informacines sistemas galima apibrėžti kaip strateginės, vadybinės ir operacinės veiklos, susijusios su informacijos rinkimu, apdorojimu, saugojimu, platinimu ir naudojimu, ir su ja siejamų technologijų derinį. Tokios informacinės sistemos gali skirtis sudėtingumu – nuo paprastos knygos, kurioje rankiniu būdu tvarkomi pinigų gavimo ir mokėjimo įrašai, iki sudėtingesnės, informacinėmis technologijomis grindžiamos sistemos, pavyzdžiui, mokesčių apskaičiavimo sistemos, kurioje automatizuoti visi procesai: duomenų rinkimas (pvz., mokesčių deklaracijos, pateikiamos interneto portale), saugojimas serveriuose, vertinimas (grindžiamas programavimu pagal apmokestinimo taisykles) ir pranešimas apie mokesčių poreikį, grąžinimas ir patvirtinimas (realiu laiku arba nustatytais intervalais). Informacinės technologijos apima techninę įrangą, programinę įrangą, komunikacijos ir kitas priemones, naudojamas duomenims įvesti, saugoti, apdoroti, perduoti ir išvesti bet kokia forma.

3.2 Informacinių sistemų auditas gali būti apibrėžiamas kaip kontrolės priemonių, susijusių su IT grindžiamomis informacinėmis sistemomis, tikrinimas siekiant nustatyti nukrypimų nuo kriterijų atvejus – kriterijai, savo ruožtu, buvo nustatyti atsižvelgiant į atliekamo audito tipą, t. y. finansinį, atitikties arba veiklos auditą.

4 APIMTIS

4.1 Auditoriai gali naudotis šiomis gairėmis, atlikdami konkrečius informacinių sistemų veiklos ir (arba) atitikties auditus, taip pat tais atvejais, kai informacinių sistemų auditas yra didesnės apimties audito, kuris gali būti finansinis, atitikties ir (arba) veiklos auditas, dalis.

4.2 Šiose gairėse pateikiama tolesnių rekomendacijų, kaip atlikti informacinių sistemų auditą, panaudojant finansinį, veiklos ir (arba) atitikties auditą, ir nepateikiama kitų papildomų reikalavimų auditui atlikti.

5 IS AUDITO PLANAVIMAS

5.1 Laikydamosi proceso, aprašyto 100-ajame TAAIS, 200-ajame TAAIS (finansinis auditas), 300-ajame TAAIS (veiklos auditas) ir 400-ajame TAAIS (atitikties auditas), AAI gali taikyti rizika pagrįstą IS audito planavimą, atsižvelgdamos į audito tikslus.

5.2 IS audito darbo apimtis nustatoma atsižvelgiant į audito tikslą ir apimtį. Galimi pavyzdžiai:

1) įvertinti atitinkamas bendrosios kontrolės [4] ir taikomųjų programų kontrolės[5] priemones, kurios daro poveikį informacinių sistemų duomenų patikimumui, o tai, savo ruožtu, daro poveikį audituojamos įmonės finansinėms ataskaitoms;

2) gauti užtikrinimą dėl informacinių sistemų procesų atitikties audituojamo subjekto veiklą reglamentuojantiems teisės aktams, politikai ir standartams;

3) gauti užtikrinimą, kad IT ištekliai leidžia efektyviai ir veiksmingai pasiekti organizacinius tikslus ir kad atitinkamos bendrosios ir taikomųjų programų kontrolės priemonės yra veiksmingos siekiant nustatyti ir koreguoti perteklinio, pernelyg didelio ir neveiksmingo informacinių sistemų naudojimo ir valdymo atvejus ar jų išvengti.

[4] Bendrosios kontrolės priemonės – tai rankinės arba automatizuotos procedūros, kuriomis siekiama užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą fizinėje aplinkoje, kurioje kuriamos, prižiūrimos ir veikia informacinės sistemos.

[5] Taikomųjų programų kontrolės priemonės – nuo IT priklausomos rankinės arba automatizuotos informacinės sistemos procedūros, kurios turi įtakos sandorių tvarkymui ir gali būti susijusios su pradinių duomenų patikra, tiksliu duomenų tvarkymu, išvesties duomenų pateikimu ir kontrolės priemonėmis, susijusiomis su pagrindinių duomenų vientisumu.

5.3 Remiantis rizikos vertinimu, IS audito apimtis gali būti nustatoma pagal bet kurią vieną arba visas toliau nurodytas audituojamojo subjekto sritis[6]:

1) IT organizacinę politiką[7];
2) IT srities organizacinę valdymo struktūrą;
3) bendrąsias kontrolės priemones, taikomas automatizuotoje veiklos srityje;
4) turto valdymą;
5) informacinių sistemų kūrimą, įsigijimą ir priežiūrą, įskaitant veiklos procesų apibrėžimą ir susijusią programavimo logiką;
6) IT operacijų valdymą;
7) fizinės aplinkos valdymą;
8) žmogiškųjų išteklių valdymą;
9) komunikacijos valdymą;
10) informacijos saugumo valdymą[8];
11) atitikties įstatymuose nustatytiems reikalavimams valdymą;
12) veiklos tęstinumo ir veiklos atkūrimo valdymą;
13) taikomųjų programų kontrolės priemonių valdymą.

5.4 Apibrėždamos IS audito apimtį, AAI gali pasirinkti audito analizės laikotarpį (pvz., vieneri metai, treji metai ir t. t.). Tinkamas laikotarpis turėtų būti pasirinktas atsižvelgiant į nustatytus audito tikslus.

5.5 Kai IS auditas yra kito audito dalis, AAI turi užtikrinti, kad audito grupė, kaip visuma, dirbtų integruotai, kad būtų pasiektas bendras audito tikslas. Siekdamos veiksmingos integracijos, AAI turėtų apsvarstyti galimybę:

1) išsamiai dokumentuoti IS auditorių atliekamą darbą;
2) parengti IS auditorių ir kitų auditorių keitimosi informacija protokolą;
3) nustatyti, kurios informacinės sistemos ir kontrolės tikslai patenka į audito apimtį.

[6] Dauguma aprašytų sričių pritaikytos pagal ISO/IEC 27001.

[7] Įskaitant strateginio valdymo aspektus.

[8] Įskaitant kibernetinį saugumą.

5.6 AAI turėtų užtikrinti, kad audito grupę sudarytų nariai, kurie būtų kompetentingi kartu atlikti IS audito užduotis, kad būtų pasiekti numatyti audito tikslai.

5.7 Būtinos žinios, įgūdžiai ir kompetencija turėtų būti įgyjami derinant mokymą, įdarbinimą ir išorės išteklių pasitelkimą pagal AAI strateginį planą.

5.8 AAI turėtų užtikrinti, kad IS audito grupės kartu gebėtų:

1) taikyti IT grindžiamos informacinės sistemos techninius elementus, įskaitant visus svarbius naudojamos taikomosios programos atvejus, kad audito proceso metu būtų galima prieiti prie IT infrastruktūros ir ja naudotis;

2) taikyti galiojančias taisykles, nuostatus ir pažinti aplinką, kurioje veikia audituojamo subjekto IT grindžiamos informacinės sistemos;

3) susieti veiklos procesus su audituojamo subjekto informacinės sistemos programavimo logika;

4) taikyti ir veiklos, ir IT žinias, siekiant įvertinti riziką, jog sistemos programa ar konfigūracija gali būti valdoma rankiniu būdu išimtinai tvarkant sandorius;

5) įvertinti taikomosios kontrolės priemonių atitinkamose informacinėse sistemose kūrimą ir išbandyti jų veikimo efektyvumą;

6) taikyti audito metodiką, įskaitant AAI taikomus atitinkamus audito standartus ir gaires;

7) taikyti IT veiklos ir (arba) atitikties kriterijus, su kuriais turi būti lyginami audito pastebėjimai, įskaitant IS valdymo sistemas, pvz., COBIT, ITIL, TOGAF;

8) taikyti IS metodus, skirtus audito įrodymams iš automatizuotų sistemų rinkti;

9) taikyti IS audito priemones, skirtas tokios analizės rezultatams rinkti, analizuoti ir atkurti arba audituotoms funkcijoms pakartotinai atlikti;

10) prisijungti prie IS infrastruktūros ir ją naudoti audito įrodymams rinkti ir saugoti;

11) prisijungti prie IS audito priemonių ir jas naudoti gautiems audito įrodymams analizuoti.

5.9 AAI turėtų apsvarstyti įvairias galimybes skirti žmogiškųjų išteklių IS auditams atlikti. Galima būtų sukurti centrinę grupę, kurią sudarytų IT

specialistai, padedantys kitoms AAI audito grupėms atlikti šiuos auditus, arba nukreipti IT specialistus pagal poreikį. Didėjant IS auditų skaičiui, AAI gali apsvarstyti galimybę sukurti specialią IS audito grupę arba padalinį. Šiai grupei turėtų būti patikėta atsakomybė atlikti visus AAI IS auditus ir bendradarbiauti su kitomis AAI grupėmis, kurios jau yra susipažinusios su audituojamu subjektu, kad greitai perprastų subjekto funkcijas ir atitinkamus veiklos procesus. Kadangi technologijos vis labiau integruojamos į informacines sistemas, AAI galėtų užtikrinti, kad visi auditoriai įgis reikiamų IS audito įgūdžių.

5.10 Kai ištekliai yra riboti, AAI gali pasitelkti išorės išteklius, pavyzdžiui, IT konsultantus, rangovus, specialistus ir ekspertus, IS auditui atlikti. AAI turėtų užtikrinti, kad tokie išorės specialistai būtų tinkamai parengti ir atitiktų AAI taikomas profesinio elgesio ir IS audito procesų bei produktų gaires ir kad būtų vykdoma tinkama jų veiklos stebėsena, atsižvelgiant į dokumentais įformintą sutartį arba paslaugų lygio susitarimą ir užtikrinant atitinkamą AAI darbuotojų dalyvavimą audito planavimo, atlikimo, ataskaitų teikimo ir veiksmų po audito etapuose. Todėl AAI privalo turėti kvalifikuotų ir kompetentingų darbuotojų, kurie vykdytų išorės išteklių naudojimo stebėseną ir užtikrintų, kad būtų laikomasi gairių ir paslaugų lygio susitarimų.

5.11 Atlikdami IS audito rizikos vertinimą, auditoriai gali taikyti 100-ajame, 200-ajame, 300-ajame ir 400-ajame TAAIS nustatytus principus kartu su principais, kurie taikomi audituojant konkrečią IS audito sritį, kaip išdėstyta toliau:

1) įgimta rizika – tai tikimybė, kad tam tikros audituojamo subjekto IT grindžiamų informacinių sistemų savybės dėl savo pobūdžio gali turėti neigiamą poveikį funkcijos, kurią subjektas įgaliotas atlikti, vykdymui. Pavyzdžiui, audituojamo subjekto informacinė sistema, kuri turi pateikti informaciją visiems visuomenės nariams, kelia įgimtą veiklos rezultatų riziką, kad, viršijus numatytą didžiausią naudotojų ribą, informacinė sistema gali nereaguoti ir informacija nebus prieinama jokiam naudotojui. Nors audituojamas subjektas gali patvirtinti kontrolės priemones, kad sumažintų įgimtą riziką, daugeliu atvejų subjektui gali tekti tiesiog toleruoti tokios rizikos buvimą priklausomai nuo priimtino rizikos lygio. Įgimtą riziką galima įvertinti prieš auditoriams vertinant kontrolės ar neaptikimo rizikos poveikį;

2) IS kontrolės rizika – tai tikimybė, kad audituojamo subjekto patvirtintomis IT kontrolės priemonėmis gali nepavykti sumažinti neigiamo poveikio, į kurį reaguojant jos buvo sukurtos. Pavyzdžiui, audituojamo subjekto informacinė sistema, kuria reikia užtikrinti, kad prieigą prie konfidencialių duomenų turėtų tik įgalioti darbuotojai, gali patvirtinti kontrolės priemonę, pagal kurią reikalaujama, kad norintys gauti prieigą darbuotojai pateiktų naudotojo vardą ir slaptažodį. Kontrolės rizika šiuo

atveju yra ta, kad naudotojo vardas ir slaptažodis nėra pakankamai saugūs ir kad leidimo neturintys darbuotojai gali juos nuspėti pakartotiniais bandymais. Dėl to prarandamas konfidencialumas ir gali būti padarytas neigiamas poveikis subjektui. Subjektas, kuris primygtinai reikalauja naudoti saugius, sudėtingus slaptažodžius, kuriuos sudaro raidžių, skaičių ir specialiųjų simbolių derinys, ir užtikrina, kad informacinė sistema užkirstų kelią prieigai prie naudotojo vardo, viršijant tam tikrą skaičių nesėkmingų bandymų, turės mažesnę kontrolės riziką nei tas, kuris netaiko tokių reikalavimų;

3) neaptikimo rizika – tai tikimybė, kad auditorius nenustatys, kad nėra subjekto patvirtintų IT kontrolės priemonių, kad jos sugedusios ar netinkamos, o tai galėtų turėti neigiamą poveikį subjektui.

5.12 Rizika pagrįstiems IT grindžiamų sistemų vertinimams atlikti AAI gali pasirinkti jų paskirtį atitinkančią metodiką. Metodikos gali būti įvairios – nuo paprastų audituojamo subjekto IT aplinkos rizikos pobūdžio klasifikacijų į aukštą, vidutinį ir žemą, remiantis AAI žiniomis apie subjektą ir jo aplinką bei AAI IS audito grupės profesiniu vertinimu, iki sudėtingesnių skaitmeninių skaičiavimų, kuriais remiantis kiekybiškai įvertinamas rizikos reitingas pagal objektyvius iš audituojamo subjekto surinktus duomenis[9].

5.13 Sprendimas dėl IS audito reikšmingumo gali būti priimamas laikantis bendros sistemos, pagal kurią AAI priimamas sprendimas dėl reikšmingumo. Reikšmingumo perspektyva gali skirtis priklausomai nuo IS audito pobūdžio. Reikšmingumas viešojo sektoriaus finansinio, veiklos ir atitikties auditams, pagal kurį nustatomas reikšmingumas IS auditui, aprašytas 100-ajame, 200-ajame, 300-ajame ir 400-ajame TAAIS[10].

[9] IT darbo grupės IDI IT audito vadovas aukščiausiosioms audito institucijoms.

[10] 200-asis TAAIS *Finansinio audito principai*, 300-asis TAAIS *Veiklos audito principai*, 400-asis TAAIS *Atitikties* audito principai.

6 IS AUDITO ATLIKIMAS

6.1 Atsižvelgdamos į audito pobūdį, tam tikrais atvejais AAI gali atlikti IS auditus pagal finansinio audito (200-asis TAAIS), veiklos audito (300-asis TAAIS) ir atitikties audito (400-asis TAAIS) procesą.

6.2 Atlikdami IS auditą, auditoriai turėtų prašyti audituojamo subjekto užtikrinti tinkamą bendradarbiavimą ir pagalbą, įskaitant galimybę susipažinti su įrašais ir informacija. Pasikonsultavę su audituojamu subjektu, auditoriai turėtų nustatyti tokį prieigos prie elektroninių duomenų režimo formatą, kuris būtinas analizei atlikti. Prieigos prie duomenų režimas būtų skirtas konkrečiai AAI.

6.3 Prieš pradėdami kontrolės priemonių vertinimą informacinėje sistemoje, auditoriai turėtų geriau susipažinti su sistemos architektūra, pagrindiniais duomenis ir jų šaltiniais, kad nustatytų reikiamas audito priemones ir metodus.

6.4 Jeigu iš audituojamo subjekto gaunama didelė duomenų krūva[11], auditoriai turėtų užtikrinti, kad prie kiekvienos duomenų krūvos būtų pridėtas audituojamo subjekto lydraštis. Tokiame lydraštyje turėtų būti nurodyta:

1) duomenų šaltinis (su nuoroda į laiko žymą, susijusią su duomenų krūvos / maišos numerio sukūrimu), kad būtų užtikrintas duomenų vientisumas, autentiškumo patvirtinimas[12] ir negalėjimas atsisakyti atsakomybės[13];

2) išgavimo parametrai, naudojami duomenų krūvai sukurti, t. y. naudotos užklausos ir (arba) analizuotos ataskaitos;

3) negavę tokio audituojamo subjekto lydraščio, auditoriai turėtų parengti vidaus dokumentus, kuriuose būtų nurodyta svarbi informacija, pvz.,

[11] Duomenų krūvos („duomenų sąvartynai“) – dideli duomenų kiekiai, perduodami iš vienos sistemos ar vietos į kitą.

[12] Autentiškumo patvirtinimas – naudotojo tapatybės tikrinimo veiksmas – ISACA terminų žodynas.

[13] Negalėjimas atsisakyti atsakomybės (atsakomybės už veiksmus prisiėmimas) apibrėžiamas kaip užtikrinimas, kad šalis vėliau negalės paneigti pateiktų duomenų; duomenų vientisumo ir kilmės įrodymo pateikimas, kurį gali patikrinti trečioji šalis – ISACA terminų žodynas.

data, kada duomenys buvo perduoti, iš kurios rinkmenos buvo sukurta duomenų krūva, ar duomenys buvo gauti iš darbinės, ar iš kokios nors kitos aplinkos ir t. t.

6.5 Auditoriai turėtų atlikti audituojamo subjekto patvirtintos IT kontrolės (bendrosios ir taikomųjų programų kontrolės) vertinimą, kad patikrintų jos patikimumą ir pakankamumą. Vertinimas gali būti atliekamas taikant tinkamą šių metodų derinį: pokalbį, klausimyną, stebėjimą, „ėjimo per sistemą“ (*walk through*) testus, srauto diagramas (*flow charts*), duomenų fiksavimą ir analizę, patvirtinimą, perskaičiavimą, pakartotinį apdorojimą ir trečiosios šalies patvirtinimą. IT kontrolės priemonių vertinimo apimtį sudaro patikrinimas, ar:

1) IS politika apibrėžta, patvirtinta ir apie ją pranešta;
2) sukurta ir veikia IS valdymo struktūra;
3) reguliariai atliekama IS turto inventorizacija ir yra nustatyti papildymo, atnaujinimo ir nurašymo reikalavimai;
4) apibrėžti ir veikia dalijimosi informacinių sistemų infrastruktūra ir bendrosiomis paslaugomis su kitais viešaisiais subjektais procesai;
5) informacinių sistemų kūrimo, įsigijimo ir priežiūros procesai apibrėžti, patvirtinti ir apie juos pranešta (įskaitant pokyčių valdymo procesą);
6) informacinių technologijų operacijų procesai (vidinis paslaugų teikimas, išorinis paslaugų teikimas, paslaugų susitarimai) apibrėžti, patvirtinti ir apie juos pranešta;
7) patvirtintos priemonės fiziniam saugumui ir numatytoms fizinėms darbo sąlygoms užtikrinti;
8) patvirtintos žmogiškųjų išteklių mokymo ir informuotumo didinimo priemonės, siekiant užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą, taip pat atitiktį IS politikos ir valdymo struktūros reikalavimams;
9) patvirtintos priemonės, skirtos įvairių komunikacijos būdų ir kanalų konfidencialumui, vientisumui ir prieinamumui užtikrinti;
10) patvirtintos informacijos saugumo valdymo priemonės;
11) patvirtintos atitikties teisės aktų reikalavimams valdymo priemonės;
12) patvirtintos veiklos tęstinumo ir veiklos atkūrimo valdymo priemonės;
13) kiekvienoje informacinėje sistemoje įdiegtos taikomųjų programų kontrolės priemonės yra tinkamos ir patikimos. Toks vertinimas turėtų

apimti taikomųjų programų svarbių sudedamųjų dalių nustatymą, taikomųjų programų svarbos subjektui nustatymą, esamų dokumentų peržiūrą, pokalbius su darbuotojais, taikomųjų programų kontrolės priemonių rizikos ir jos poveikio subjektui supratimą, testų, skirtų tokių taikomųjų programų priemonių tinkamumui ir patikimumui patikrinti, parengimą.

6.6 Atsižvelgiant į IS audito tikslą, bendrosios ir taikomųjų programų kontrolės priemonių vertinimas turėtų apimti audituojamo subjekto politikos sritis, procesus, žmones ir sistemas.

6.7 Priklausomai nuo audito tikslo, auditoriui gali būti svarbūs kontrolės priemonių kūrimas, įgyvendinimas ir veiksmingumas. Kai auditorių domina kontrolės priemonių kūrimas, gali pakakti pokalbio arba dokumentais pagrįstų veiklos taisyklių patikrinimo. Kai auditoriui svarbu kontrolės priemonių įgyvendinimas, pokalbio gali nepakakti – gali prireikti atlikti „ėjimo per sistemą“ testą arba duomenų analizę, kad būtų galima pagrįsti, jog sukurtos kontrolės priemonės buvo tinkamai įgyvendintos. Galiausiai, jei auditorius yra suinteresuotas kontrolės priemonių veiksmingumu, gali prireikti patikrinti operacijų imtį, siekiant parodyti, ar kontrolės priemonės buvo veiksmingos per atitinkamą laikotarpį.

6.8 Auditoriai taip pat turėtų atsižvelgti į tai, kokį poveikį bendrosios kontrolės įrodymai gali turėti įrodymų, reikalingų gauti patikinimą dėl taikomųjų programų kontrolės veikimo, pobūdžiui, pateikimui laiku ir mastui. Jei auditorius gavo pakankamai tinkamų audito įrodymų, susijusių su bendrosios kontrolės priemonių, kurios padeda darbuotojams gauti loginę prieigą prie IT sistemų ir pokyčių valdymo darbinėje aplinkoje, veiksmingumu, galima padaryti išvadą dėl automatizuotų taikomųjų programų kontrolės procedūrų veiksmingumo. Tai galima padaryti testuojant mažesnę operacijų imtį, nes bendros IT aplinkos veiksmingumas suteikia auditoriui įrodymų, koks yra taikomųjų programų kontrolės veiksmingumas atitinkamu laikotarpiu. Jei taikomos rankinio naudojimo kontrolės procedūros, auditoriams gali tekti testuoti tokį imties dydį, kuris atitiktų pasirinktą patikimumo lygį.

6.9 Remdamiesi IT kontrolės priemonių vertinimu, auditoriai turėtų nustatyti prioritetines sritis, kuriose turėtų būti atliekami IT kontrolės priemonių detalieji testai, naudojant įvairias kompiuterizuotas audito priemones (CAATs), darant tyrimus, renkant ir analizuojant duomenis. Auditoriai gali parengti ir atlikti detaliuosius testus audito tikslams pagrįsti. Auditoriai gali pasirinkti tinkamas CAAT, atsižvelgdami į savo reikalavimus.

6.10 Auditoriai turėtų naudoti CAAT, taikydami tokius IS audito metodus, kaip naudotojo žurnalo analizė, pranešimai apie išimtis, sumų skaičiavimas pagal laukelius, rinkmenų palyginimas, stratifikacija, pavyzdžių atranka, dvigubos

patikros, trūkumų aptikimas, planavimas, virtualūs lauko skaičiavimai ir t. t. CAAT naudojimo privalumai – didelio duomenų kiekio analizė, skirtingų duomenų rinkinių testų pakartojamumas pagal skirtingus kriterijus bei automatizuotas audito testų ir rezultatų dokumentavimas su laiko žymomis.

6.11 Priklausomai nuo ribotų išteklių ir audito kaštų bei naudos santykio, auditoriai ne visada gali turėti galimybę išnagrinėti visus atvejus, sandorius, modulius ar IT sistemas. Tokiu atveju, atsižvelgdamos į reikšmingumą, AAI turėtų patvirtinti detaliųjų testų audito imtį, kuri leistų padaryti pagrįstas audito išvadas. AAI turėtų naudoti atitinkamus CAAT skirtingų tipų pavyzdžių atrankai atlikti ir nustatyti tinkamus imties dydžius, priklausomai nuo pagrindinių įgimtų ir kontrolės rizikų. Audito imtys[14] sudaromos siekiant suteikti auditoriui pagrįstą pagrindą daryti išvadas dėl visos duomenų tiriamosios visumos, remiantis audito imčiai taikytų audito procedūrų ir analizės išvadomis. Auditoriai turėtų atsižvelgti į audito procedūros tikslą ir tiriamosios visumos, iš kurios bus sudaroma imtis, ypatumus ir nustatyti imties dydį, kurio pakaktų imties rizikai sumažinti iki priimtino lygio. Auditas IT aplinkoje turėtų palengvinti 100 proc. populiacijos analizę, ypač preliminaraus vertinimo etape. Tačiau detaliesiems testams atlikti gali prireikti audito atrankos. Atlikdami atranką finansinio audito srityje, IS auditoriai pavyzdžių atrankai[15] gali taikyti 2530-ąjį TAAIS.

6.12 Auditoriai turėtų užtikrinti, kad būtų surinkta ir dokumentuota pakankamai patikimų ir tikslių elektroninių įrodymų audito pastaboms pagrįsti. Tokius elektroninius įrodymus turėtų sudaryti duomenų rinkmenos, naudotojų žurnalai, analitiniai modeliai, valdymo informacinių sistemų ataskaitos ir t. t.; jie turėtų būti tinkamai surinkti ir saugomi taip, kad jais remiantis būtų galima gauti patikinimą dėl audito proceso tikslumo ir pagrįstumo. IS audito metu surinktuose įrodymuose turėtų būti reikiamos laiko žymos ir išsami informacija apie atliktos duomenų analizės etapus, kad būtų aišku, kada įrodymai buvo sukurti, saugomi ir paskutinį kartą pakeisti, siekiant sumažinti vėlesnių pokyčių riziką.

6.13 IS audito dokumentai turėtų būti apsaugoti nuo bet kokių pakeitimų ir neteisėto ištrynimo. AAI turėtų parengti naujus arba pritaikyti esamus IS audito dokumentų saugojimo standartus, kad jie atitiktų su IS auditu susijusių dokumentų saugojimo reikalavimus. Taip nustatytas saugojimo laikotarpis turėtų būti kiekvienai AAI privalomas ir jos veiklą reglamentuojančiais nuostatais įtvirtintas įpareigojimas. Ypatingas dėmesys turėtų būti skiriamas šių duomenų rinkmenoms, formatui, tikėtinai naudojimo trukmei ir saugojimo reikalavimams, siekiant užtikrinti, kad duomenys būtų įskaitomi per kiekvienos AAI duomenų saugojimo ir archyvavimo politikoje nustatytą laikotarpį. Dėl to gali prireikti

[14] 2530-asis TAAIS *Finansinis auditas, Audito atranka*, 6–9 dalys.

[15] Ten pat.

duomenis pakeisti iš vieno formato į kitą, kad jie neatsiliktų nuo technologijų pažangos ir nepasentų.

6.14 Tikrindami trečiųjų šalių auditorių parengtas technines ataskaitas su technologijomis susijusiais klausimais, auditoriai turėtų patvirtinti atitinkamas procedūras, skirtas gauti patikinimą, susijusį su tokių ataskaitų[16] atitikties, finansiniais ar veiklos audito aspektais. Jei taikant tokias procedūras remiamasi tokių ataskaitų turiniu, šis faktas turėtų būti tinkamai atskleistas.

6.15 TAAIS nurodo, kad auditoriai turėtų užtikrinti veiksmingą bendravimą viso audito proceso metu ir nuolat informuoti audituojamą subjektą visais su auditu susijusiais klausimais (žr. 100-ojo TAAIS 43 punktą). Atliekant auditą, kurio dalis yra IS auditas, apie IS audito rezultatus tam tikrais atvejais subjektui gali būti pranešama atskiru raštu. Tokiais atvejais svarbu paaiškinti, kaip šio audito rezultatai yra susiję su kitais pranešimais, kurie yra to paties finansinio, veiklos ar atitikties audito dalis, ir kiek IS audito rezultatai gali būti svarbūs atitinkamai AAI audito ataskaitai.

[16] Kai auditas yra finansinio audito dalis, auditoriai gali naudotis 2402-uoju TAAIS „Audito svarstymai, susiję su paslaugų organizaciją naudojančia įmone“.

7

IS AUDITO ATASKAITŲ TEIKIMAS

7.1 Kadangi IS auditas gali būti finansinis (200-asis TAAIS), veiklos (300-asis TAAIS) arba atitikties (400-asis TAAIS) auditas, auditoriai turėtų atsižvelgti į atitinkamus ataskaitų teikimo reikalavimus. Kiekviena konkreti AAI turi savo reikalavimus. Be to, kiekviena AAI gali turėti nusistačiusi savo ataskaitų teikimo ribas, pagrįstas audito pastebėjimų reikšmingumu. Taip pat ir auditorius, teikdamas IS audito ataskaitas, gali laikytis teisės aktais nustatytų vidinių finansinės ir techninės informacijos atskleidimo apribojimų.

7.2 Auditoriai turėtų atkreipti dėmesį į profesinės kalbos vartojimo ribojimą ir į tai, kad tam tikra ataskaitoje pateikta informacija (pvz., slaptažodžiai, naudotojo vardai, tapatybės duomenys ir asmeninė informacija) yra neskelbtina. Nepaisant techninio IS audito pobūdžio, auditoriai turėtų užtikrinti, kad ataskaita būtų visiškai suprantama audituojamo subjekto vyresniajai vadovybei, suinteresuotiesiems subjektams ir plačiajai visuomenei. Auditoriai ataskaitose gali pateikti pakankamai išsamų terminų žodyną, kuriame pateikiama kryžminė nuoroda į akronimo ar termino apibrėžtį ir situacija pagrįstas paaiškinimas, kaip tai veikia kontroliuojamoje aplinkoje.

7.3 Auditoriai turėtų atsižvelgti į galbūt neigiamą poveikį, kurį galėtų daryti paskelbta IS audito ataskaita. Pavyzdžiui, jeigu IS audito ataskaitoje nustatoma tam tikra audituojamo subjekto informacinės sistemos saugumo rizika ir apie ją pranešama prieš patvirtinant būtinas rizikos mažinimo kontrolės priemones, informacinės sistemos pažeidžiamumas gali būti paviešintas visuomenei. Tokiu atveju, siekdami išvengti galbūt neigiamo poveikio audituojamam subjektui, auditoriai gali apsvarstyti galimybę teikti ataskaitą tik po to, kai bus patvirtintos būtinos kontrolės priemonės, arba neinformuoti apie visą tikrąją saugumo riziką.

8 VEIKSMAI PO AUDITO

8.1 Kadangi informacinių sistemų auditas grindžiamas vienu ar keliais pagrindiniais audito tipais, auditoriai turėtų laikyti, kad veiksmų po audito reikalavimai, keliami tokiam auditui, atitinka veiksmų po audito reikalavimus, keliamus finansiniam (200-asis TAAIS), veiklos (300-asis TAAIS) ir atitikties (400-asis TAAIS 400) auditams.