PATVIRTINTA
Lietuvos Respublikos valstybės kontrolieriaus pavaduotojo
2025 m. balandžio 14 d. įsakymu Nr. APDE-2

VALSTYBĖS KONTROLĖ

INFORMACINIŲ TECHNOLOGIJŲ AUDITO VADOVAS

TURINYS

SANTRUMPOS IR SĄVOKOS

Santrumpos

3E – veiklos audito vertinimo aspektai: ekonomiškumas, efektyvumas ir rezultatyvumas (angl. *economy, efficiency, effectiveness*).

AAI – aukščiausioji audito institucija (Valstybės kontrolė).

CAAT – kompiuterizuotos audito priemonės.

COBIT – Tarptautinės informacinių sistemų audito ir kontrolės asociacijos (ISACA) parengta informacinių sistemų valdymo metodika ir gerosios praktikos rinkinys.

GUID – INTOSAI gairės.

IS – Informacinė sistema.

IT – Informacinės technologijos.

IRT – informacinių ir ryšių technologijų sritis.

IT kontrolės priemonės – IT bendrosios ir taikomųjų programų kontrolės priemonės.

INTOSAI – Tarptautinė aukščiausiųjų audito institucijų organizacija (angl. *International Organization of Supreme Audit Institutions*).

ISACA – Tarptautinė profesinė organizacija orientuota į informacinių technologijų valdymą (anksčiau žinoma kaip Informacinių sistemų audito ir kontrolės asociacija).

IFPP – INTOSAI profesinių nutarimų sistema, apimanti INTOSAI principus (INTOSAI-P), standartus (TAAIS) ir gaires (GUID).

Metodikos svetainė – Valstybinio audito metodikos svetainė.

TAAIS – tarptautiniai aukščiausiųjų audito institucijų standartai.

Vadovas – Informacinių technologijų audito vadovas.

ViPSIS – Veiklos planavimo ir stebėsenos informacinė sistema.

Sąvokos

Atitikties auditas pagal VKĮ[1] – valstybinio audito tipas, kai vertinama audituojamo subjekto veiklos atitiktis teisės aktų ir (ar) kitiems reikalavimams ir gali būti pareiškiama nepriklausoma auditoriaus nuomonė.

Atitikties auditas pagal TAAIS[2] – nepriklausomas įvertinimas, ar tam tikra audito sritis atitinka jai taikomus reikalavimus (kriterijus). Atitikties auditas atliekamas vertinant, ar veikla, finansinės ūkinės operacijos ir informacija visais reikšmingais atžvilgiais atitinka reikalavimus, kurių privalo laikytis audituojamas subjektas.

Audito grupė – audito departamento vadovas, audito grupės vadovas, kiti audito grupės nariai ir valstybinio auditoriaus padėjėjas (-ai).

---

[1] Valstybės kontrolės įstatymas, 2 str. 1 d.

[2] 400-asis TAAIS „Atitikties audito principai“, 12 p.

Audito įrodymai – dokumentuota informacija, kuria auditorius pagrindžia savo pastebėjimus, išvadas ir rekomendacijas.

Audito kriterijus – tam tikras etalonas (normatyvinis standartas, pagrįstas lūkestis, geroji veiklos praktika ar nustatytas parametras (duomuo, matas, savybė, rodiklis)), kuris leidžia įvertinti audito duomenis ir padaryti išvadas apie audituojamo subjekto informacinių technologijų kontrolės priemonių *pakankamumą* ir *patikimumą*.

Audito objektas – audituojamo subjekto (-ų) veikla ar jos dalys (programa, paslaugos ir pan.), sandoriai, informacija ir kt. – tai, kas yra audituojama.

Audito pastebėjimas – audito įrodymų vertinimo ir jų palyginimo su audito kriterijais rezultatas, apimantis ir nuokrypių nuo audito kriterijų priežasčių ir pasekmių vertinimą.

Audito procedūros – tam tikruose audito etapuose atliekami auditoriaus veiksmai siekiant audito tikslų.

Audito procesas – visi audito etapai, apimantys audito planavimą (strateginį ir išankstinį tyrimus), atlikimą (pagrindinį tyrimą), ataskaitos rengimą ir stebėjimą po audito.

Audito rizika – tikimybė, kad dėl įvairių atsiradusių veiksnių ar įvykių gali būti pateikti neteisingi ar neišsamūs pastebėjimai, išvados, rekomendacijos, nepasiektas arba nevisiškai pasiektas audito tikslas, nebus pasiektas laukiamas audito poveikis.

Audito rizikos valdymas – sisteminis valdymo procedūrų ir priemonių taikymas, siekiant nustatyti ir valdyti tikėtinus įvykius, kurie gali reikšmingai paveikti audito procesą, taip pat suteikti pakankamą užtikrinimą, kad audito tikslas bus pasiektas.

Audito sritis – sudėtinė audito objekto dalis, t. y. audito objektą gali sudaryti kelios audito sritys. 4000-ajame TAAIS *audito srities* sąvoka tapatinama su sąvoka *audito objektas*, tačiau šiame vadove ji vartojama siauresne prasme.

Audituojamas subjektas – viešojo sektoriaus subjektas arba kitas juridinis asmuo, kuriam suteiktas ar perduotas valstybės turtas ir (ar) kuriam viešojo sektoriaus subjektas daro lemiamą poveikį, kuriuose Valstybės kontrolė atlieka valstybinį auditą.

Audito tikslas – tiksli formuluotė, ko siekiama auditu.

Atitiktis – audituojamo subjekto veiklos atitiktis teisės aktų ir (ar) kitiems reikalavimams.

Atsakingoji šalis – subjektas, atsakingas už audito srities informaciją, audito srities valdymą ir (ar) rekomendacijų įgyvendinimą bei būtinų pokyčių taikymą.

Darbo dokumentai – dokumentuota informacija apie atliktas audito procedūras, surinktus audito įrodymus ir auditoriaus padarytas išvadas.

Detalieji testai (angl. *substantive testing*) – tai audito procedūra, kurios metu vertinama, ar įdiegtos IT taikomųjų programų kontrolės priemonės yra pakankamos ir patikimos. IT kontrolės priemonių *pakankamumas*, kai kontrolės priemonės sukurtos tokia apimtimi kurių pakanka, kad būtų sudarytos tinkamos sąlygos organizacijai, atsižvelgiant į jos veiklos specifiką ir mastą, siekti savo nustatytų tikslų. IT kontrolės priemonės *patikimos*, kai jos tinkamai sukurtos ir įgyvendinamos taip, kaip numatyta organizacijos politikoje, standarte, tvarkoje, teisės akte, techninėje specifikacijoje ar kitose dokumentuose.

Duomenys (angl. *data*) – reiškia neapdorotą informaciją. Duomenys paprastai saugomi duomenų bazėje ir pateikiami kaip skaičiai, simboliai, ženklai, tekstas, vaizdai. Duomenys vertinami kaip mažiausi faktinės informacijos vienetai.

Ekstrapoliavimas – atrankos rezultatų įvertinimo būdas, kai nustatytos neatitiktys pritaikomos tiriamajai visumai.

Finansinis auditas – valstybinio audito tipas, kai vertinami audituojamo subjekto metinių ataskaitų rinkinių duomenys ir pareiškiama nepriklausoma auditoriaus nuomonė.

Gebos brandos modelis (angl. *Capability Maturity Model (CMM)*) – programų inžinerijos instituto (angl. *Software Engineering Institute*) sukurtas gebos brandos modelis, skirtas padėti organizacijoms, kuriančioms programinę įrangą, įvertinti ir padidinti šios įrangos kūrimo procesų gebą. Modelis reitinguoja šias organizacijas pagal penkių proceso gebos lygių hierarchiją. Pirmas gebos lygis apibūdina nesubrendusius arba chaotiškiausius, o penktasis – brandžiausius arba kokybiškiausius procesus[3].

Informacija – žinios apie faktus, įvykius, daiktus, procesus, idėjas ir kitus objektus, kurios tam tikrame kontekste turi kokią nors prasmę. Informacija gaunama apdorojus duomenis (pvz.: formatuojant, filtruojant, sumuojant, atliekant analizę ar kitas sudėtingesnes operacijas).

Informacinė sistema – strateginės, vadybinės ir operacinės veiklos, susijusios su informacijos rinkimu, apdorojimu, saugojimu, platinimu ir naudojimu, ir su ja siejamų technologijų deriniu. Tokios informacinės sistemos gali skirtis sudėtingumu – nuo paprastos knygos, kurioje rankiniu būdu tvarkomi pinigų gavimo ir mokėjimo įrašai, iki sudėtingesnės, informacinėmis technologijomis grindžiamos sistemos, pvz., 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). Informacinė sistema gali apimti keletą taikomųjų programų.

Išankstinis tyrimas – audito proceso etapas, kurio metu renkama ir įvertinama informacija apie nagrinėjamą veiklos sritį, nustatomos problemos (rizikos) ir, nusprendus atlikti pagrindinį tyrimą, parengiamas audito planas.

IT ištekliai – informacijos, kurią valdo informacinės visuomenės nariai ir kuri apdorojama informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių ir žmogiškųjų išteklių visuma (informacija; paslaugos, infrastruktūra ir taikomosios programos; žmonės, įgūdžiai ir kompetencija).

Informacinės technologijos – ištekliai, reikalingi tam tikrai informacijai gauti, tvarkyti, saugoti ir skleisti: techninė, programinė įranga, komunikacijos ir kita įranga, naudojama bet kokios formos duomenims įvesti, saugoti, apdoroti, perduoti ir išvesti[4].

Informacinių technologijų auditas – informacinių technologijų kontrolės priemonių vertinimas siekiant nustatyti nukrypimų nuo audito kriterijų atvejus, kurie buvo nustatyti atsižvelgiant į atliekamo audito tipą, t. y. finansinį, atitikties arba veiklos.

Informacinių technologijų bendroji kontrolė – kontrolės priemonės, kurios taikomos visiems konkrečios organizacijos IT komponentams, procesams ir duomenims ar informacinių technologijų aplinkai. Šios kontrolės priemonių visuma turi užtikrinti tinkamą kompiuterizuotų taikomųjų programų plėtrą ir įgyvendinimą, taikomųjų

---

[3] Geba – gebėjimai, kompetencija ar ištekliai, kuriuos organizacija gali turėti arba kurie reikalingi organizacijai, veiklos funkcijai ar individualiame lygmenyje, siekiant prisidėti prie organizacijos veiklos tikslų pasiekimo ir užtikrinti vertės kūrimą. Branda – rodo organizacijos brandos lygį, kuris atspindi organizacijos gebėjimą nuosekliai ir pasikartojančiai įgyvendinti veiklos procesus, užtikrinant kokybę ir efektyvumą. T. y. geri organizacijos gebėjimai skatina aukštą brandumo lygį, o aukštas brandumo lygis rodo, kad organizacija turi stiprius gebėjimus vykdyti veiklą.

[4] Informacinių technologijų sąvoka yra platesnė nei informacinės sistemos sąvoka, nes ji apima visus technologinius aspektus, kurie gali būti naudojami bet kurioje informacinėje sistemoje. Pvz., elektroninių ryšių tinklai yra dalis informacinių technologijų, kurie naudojami daugeliui skirtingų IS perduodant duomenis.

programų, duomenų bylų ir kompiuterinių operacijų vientisumą.

Išvada – audito pastebėjimų pagrindu suformuluotas auditoriaus teiginys dėl audituojamo subjekto informacinių technologijų kontrolės pakankamumo ir patikimumo, atsakantis į audito klausimus pagal pasirinktus audito kriterijus.

Laukiamas audito poveikis – tai aprašomojo pobūdžio informacija, apibūdinanti planuojamą audito poveikį ir apibendrinanti siekiamus pokyčius.

Pagrindinis tyrimas – audito proceso etapas, kurio metu renkami audito įrodymai, kuriais remdamasis auditorius turi atsakyti į audito klausimus ir pagrįsti audito ataskaitoje pateiktus pastebėjimus, išvadas ir rekomendacijas.

Problema – įvykis, situacija, veiksnys, galintis neigiamai paveikti tam tikros organizacijos, programos, sistemos ar visos valstybės valdymą.

Pokytis – rekomendacijų įgyvendinimu paskatintas kokybinis ar kiekybinis situacijos pasikeitimas audituotoje srityje.

Pokyčių vertinimo rodikliai – kokybiniai ir kiekybiniai rodikliai, pagal kuriuos vertinami rekomendacijų įgyvendinimo paskatinti pokyčiai audituotoje srityje. Kokybiniai rodikliai – aprašomojo pobūdžio informacija, atskleidžianti pokyčių turinį, svarbą, kontekstą. Kiekybiniai rodikliai nurodo kiekį, kuris gali būti išreiškiamas skaičiumi, santykiu, dalimi ir pan.

Programinė įranga – rinkinys instrukcijų, kurios leidžia kompiuteriui atlikti tam tikras operacijas. Šios instrukcijos yra sukurtos programuotojų naudojant programavimo kalbas. Programinė įranga gali būti bet koks kodas, nuo paprastų skriptų iki sudėtingų sistemų[5]. Pagal paskirtį programinė įranga skirstoma taip:

- ✓ Taikomoji programa – programinė įranga, sukurta atlikti konkrečias užduotis ar funkcijas vartotojui. Ji yra tiesiogiai naudojama vartotojo, pvz.: grafikos dizaino programos, buhalterinės programos, mobiliosios aplikacijos ir pan.
- ✓ Sistemos programa – programinė įranga, kuri valdo ir koordinuoja kompiuterio aparatinę įrangą. Ji suteikia pagrindinę infrastruktūrą, kurioje veikia taikomoji programinė įranga. Pagrindinis sistemos programinės įrangos pavyzdys yra operacinė sistema, tokia kaip *Windows*, *Linux* ar *macOS*. *Draiveriai* (programinė įranga, kuri leidžia operacinei sistemai bendrauti su aparatinės įrangos komponentais) taip pat priklauso šiai kategorijai.
- ✓ Paslaugų programa – specializuota programinė įranga, kuri padeda vartotojui valdyti ir palaikyti kompiuterio sistemą, naudojama optimizavimui, analizei, priežiūrai ir kt. techninėms operacijoms (pvz., diskų valymo, antivirusinės ar atkūrimo programos).

Rekomendacija – valstybinio audito rezultatų pagrindu suformuluoti siūlymai, skirti valstybinio audito metu nustatytoms problemoms išspręsti, siekiant audituojamo (-ų) subjekto (-ų) veiklos gerinimo ir naudos visuomenei didinimo.

Rekomendacijų įgyvendinimo stebėsena – procesas, kurio metu stebimas ir vertinamas rekomendacijų ir joms įgyvendinti suplanuotų priemonių įgyvendinimas, ar audituotas subjektas jas įgyvendino taip, kaip buvo suplanuota rekomendacijų įgyvendinimo plane.

---

[5] Programinė įranga yra priešingybė aparatinės įrangos terminui. Aparatinė įranga apima fizinę kompiuterio dalį (tokią kaip procesorius, atmintis, kietasis diskas), o programinė įranga yra nemateriali ir apima programas, kurios veikia šioje aparatinėje įrangoje.

Rizika – IT veiklos kontekste tai galimybė, kad IT kontrolės trūkumas (pažeidžiamumas) sukels turto ir (ar) lėšų praradimą ir (arba) padarys organizacijai ir (ar) valstybei žalos.

Stebėjimas po audito – procesas, apimantis valstybinio audito ataskaitoje pateiktų rekomendacijų įgyvendinimo ir audito poveikio įvertinimą.

Strateginis tyrimas – audito proceso etapas, kurio metu atliekamas viešojo sektoriaus veiklos sričių nuolatinis stebėjimas, duomenų rinkimas ir veiklos problemų (rizikų) nustatymas, analizė ir audito objektų (temų) atranka.

Taikomųjų programų kontrolės priemonė (angl. *application controls*) – taikomojoje programoje įdiegtos rankinės arba automatizuotos informacinės sistemos procedūros ir funkcijos, kurios turi įtakos sandorių tvarkymui ir gali būti susijusios su pradinių duomenų patikra, korektišku duomenų tvarkymu, duomenų apdorojimu pagal reikalavimuose numatytą veiklos logiką, išvesties duomenų pateikimu ir kontrolės priemonėmis, susijusiomis su pagrindinių duomenų vientisumu ir saugumu.

Valstybinio audito ataskaita – valstybinio audito dokumentas, kuriame pateikiami atlikto valstybinio audito rezultatai.

Valstybinio audito poveikis – tiesioginė ir netiesioginė nauda, kurią sukuria valstybiniai auditai ir aukščiausiosios audito institucijos veikla. Tiesioginis poveikis – tai nauda, kurią lemia konkretaus valstybinio audito rekomendacijų paskatintų pokyčių visuma. Netiesioginis poveikis – nauda, kurią lemia šalyje sukurta ir veikianti valstybinio audito sistema, aukščiausiosios audito institucijos veikla ir valstybinių auditų visuma.

Veiklos auditas – valstybinio audito tipas, kai vertinama audituojamo subjekto veikla ekonomiškumo, efektyvumo ir rezultatyvumo požiūriu.

Vidaus kontrolė – procesas, kurį įgyvendina organizacijos vadovybė ir darbuotojai, siekdami užtikrinti organizacijos tikslų pasiekimą, ataskaitų patikimumą ir veiklos atitiktį teisės aktų reikalavimams[6].

Kitos sąvokos, vartojamos šiame vadove, suprantamos taip, kaip apibrėžta Lietuvos Respublikos valstybės kontrolės įstatyme, Veiklos audito vadove, Finansinio audito vadove, Atitikties audito vadove.

[6] *Treadway* komisijos organizacijų rėmimo komitetas (angl. *The Committee of Sponsoring Organisations of the Treadway Commission*).

ĮŽANGA

Vadovas yra sudėtinė Valstybės kontrolės parengtų metodinių dokumentų, susijusių su audito atlikimu, dalis. Vadovo tikslas – pateikti bendruosius informacinių technologijų audito (kuris atliekamas kaip savarankiškas auditas) ir jo proceso reikalavimus bei juos paaiškinti, siekiant užtikrinti institucijos atliekamų informacinių technologijų auditų kokybę.

Vadovas parengtas vadovaujantis INTOSAI profesinių nutarimų sistemos (IFPP) dokumentais: TAAIS ir GUID, skirtais finansiniams[7], veiklos[8], atitikties[9] ir informacinių technologijų auditams[10]. Naudotasi kitų aukščiausiųjų audito institucijų gerąja šios srities patirtimi, ISACA informacinių sistemų audito standartais ir gairėmis[11], kita ISACA metodine medžiaga ir ekspertų rekomendacijomis.

Atlikdamas informacinių technologijų auditus, auditorius turi taikyti TAAIS ir GUID reikalavimus, kurie Vadove pateikti kaip paryškinti teiginiai, ir vadovautis šiame vadove pateiktais detalesniais reikalavimų paaiškinimais bei praktiniais taikymo aspektais.

Pirmajame Vadovo skyriuje pateikiama informacinių technologijų audito samprata, antrajame apžvelgiami bendrieji informacinių technologijų audito reikalavimai, trečiajame aprašomi veiksmai iki audito, ketvirtajame detaliai analizuojamas informacinių technologijų audito procesas (audito planavimo, atlikimo, ataskaitos rengimo), o penktajame – veiksmai po audito .

Vadove paminėtų klausimynų ir kitų pildomų dokumentų šablonus galima rasti Metodikos svetainėje prie atitinkamo audito proceso žingsnio susijusių dokumentų skiltyje arba Šablonų skiltyje.

---

[7] 200-asis TAAIS „Finansinio audito principai“, 2000-asis TAAIS „Finansinio audito standartas“.

[8] 300-asis TAAIS „Veiklos audito principai“, 3000-asis TAAIS „Veiklos audito standartas“, 3910-osios GUID „Svarbiausi veiklos audito principai“, 3920-osios GUID „Veiklos audito procesas“.

[9] 400-asis TAAIS „Atitikties audito principai“, 4000-asis TAAIS „Atitikties audito standartas“, 4900-osios GUID „Gairės dėl reikalavimų ir kriterijų, kuriuos reikia apsvarstyti nagrinėjant atitikties audito teisėtumo ir tinkamumo aspektus“.

[10] 5100-asis GUID „Informacinių sistemų audito gairės“.

[11] IT audito sistema (ITAF™). Profesinės praktikos sistema IT auditui, 4 leidimas.

1. INFORMACINIŲ TECHNOLOGIJŲ AUDITO SAMPRATA

1.1. Informacinių technologijų audito apibrėžtis

1. Pagal 5100-ąsias GUID informacinių technologijų auditas[12] gali būti apibrėžiamas kaip kontrolės priemonių, susijusių su IT grindžiamomis informacinėmis sistemomis, tikrinimas siekiant nustatyti nukrypimų nuo kriterijų atvejus – kriterijai, savo ruožtu, nustatyti atsižvelgiant į atliekamo audito tipą, t. y. finansinį, atitikties arba veiklos. IT auditas gali būti atliekamas kaip atskiras auditas, kurio metu vertinamos IT kontrolės priemonės atitikties ir (ar) 3E aspektais arba gali būti atliekamas kaip finansinio, veiklos ar atitikties audito dalis, t. y. jungtinis auditas (išsamiau žr. 1.6 poskyryje).

2. INTOSAI IT audito darbo grupės (WGITA) ir INTOSAI vystymo iniciatyvos (IDI) parengtame IT audito vadove[13] IT auditas apibrėžiamas kaip patikinimo dėl to, ar IT sistemų kūrimas, diegimas ir priežiūra atitinka verslo tikslus, apsaugo informacijos turtą ir išlaiko duomenų vientisumą, procesas. Kitaip tariant, IT auditas yra IT sistemų ir IT kontrolės priemonių, skirtų užtikrinti, kad sistemos atitiktų organizacijos poreikius, nepakenkiant saugumui, privatumui, sąnaudoms ir kitiems svarbiems verslo elementams, nagrinėjimas.

3. Dar kituose šaltiniuose[14] pateikiama IT audito sąvoka, pagal kurią tai procesas, kurio metu renkami ir įvertinami įrodymai, siekiant nustatyti, ar kompiuterinė sistema saugo turtą, palaiko duomenų vientisumą, leidžia efektyviai pasiekti organizacijos tikslus ir efektyviai naudoja išteklius. Harvardo universitetas pateikia tokį IT audito apibrėžimą: „Informacinių technologijų auditas – tai organizacijos informacinių technologijų infrastruktūros, taikomųjų programų, duomenų naudojimo ir valdymo, politikos, procedūrų ir veiklos procesų patikrinimas ir įvertinimas pagal pripažintus standartus arba nustatytą politiką. Audito metu įvertinama, ar informacinių technologijų turto apsaugos kontrolės priemonės užtikrina vientisumą ir yra suderintos su organizacijos tikslais ir uždaviniais“[15].

4. Nepaisant gausybės įvairių IT audito sąvokų ir bruožų, bendras šių auditų aspektas yra pateikti išvadą apie tai, kiek IT kontrolės priemonės yra pakankamos[16] ir patikimos[17], kad užtikrintų audituojamojo subjekto veiklos tikslų pasiekimą.

5. Taigi IT auditas yra plati sąvoka, be to, atsižvelgiant į audito tikslą jis gali pasižymėti atitikties auditų (IT kontrolės priemonių atitikties teisės aktų ir (ar) kitiems reikalavimams

---

[12] 5100 GUID vartojama sąvoka „IS auditas“, šiame vadove vartojama sąvoka „IT auditas“, kuri IT sąvokos kontekste turi platesnę reikšmę, žr. Vadove pateiktus informacinės sistemos ir informacinių technologijų sąvokų paaiškinimus.

[13] WGITA – IDI IT audito vadovas (angl. *WGITA – IDI Handbook in IT audit for Supreme Audit Institution*), 2022 m. leidimas.

[14] Indijos AAI Informacinių technologijų audito vadovas.

[15] Kas yra Informacinių technologijų auditas? Prieiga per internetą: https://rmas.fad.harvard.edu/faq/what-does-information-systems-audit-entail#:~:text=An%20Information%20Technology%20audit%20is,recognized%20standards%20or%20established%20policies (žiūrėta 2023-05-22).

[16] IT kontrolės priemonės pakankamos, kai jos sukurtos tokia apimtimi kurių pakanka, kad būtų sudarytos tinkamos sąlygos organizacijai, atsižvelgiant į jos veiklos specifiką ir mastą, siekti savo nustatytų tikslų.

[17] IT kontrolės priemonės patikimos, kai jos tinkamai sukurtos ir įgyvendinamos taip, kaip numatyta organizacijos politikoje, standarte, tvarkoje, teisės akte, techninėje specifikacijoje ar kitose dokumentuose.

vertinimas) ir (ar) veiklos auditų (IT kontrolės priemonių ekonomiškumo, efektyvumo, rezultatyvumo vertinimas) bruožais:

- ✓ veiklos audito kontekste IT auditas galėtų vertinti, ar technologiniai sistemų patobulinimai padėjo įmonei pasiekti savo tikslus;
- ✓ atitikties audito kontekste IT auditas galėtų būti informacinių sistemų, rengiančių atitikties ataskaitas, leidžiančių darbuotojams vykdyti ir kontroliuoti įmonės veiklą, veiksmingumo tyrimas arba vertinimas kaip organizacijoje įdiegtos IT kontrolės priemonės atitinka teisės aktų reikalavimus.

6. Gali būti atvejų, kai IT auditai skirti tik tam tikroms IT sritims įvertinti.

1.2. IT bendroji kontrolė ir taikomųjų programų kontrolė

7. Paprastai atliekant IT auditus auditorius turi suprasti galimą veiklos ir IT riziką, su kuria gali susidurti audituojamas subjektas, ir savo ruožtu ištestuoti ir įvertinti, ar subjekto įdiegtos IT kontrolės priemonės yra pakankamos ir patikimos siekiant įgyvendinti organizacijos tikslus.

8. Vidaus kontrolės sistema – tai politikos, procedūrų ir metodų, užtikrinančių organizacijos turto apsaugą, finansų apskaitos tikslumą ir patikimumą bei valdymo standartų laikymąsi, derinys. IT srityje kontrolės priemonės, kurios yra organizacijos vidaus kontrolės sistemos dalis, skirstomos į dvi kategorijas: IT bendrosios kontrolės ir taikomųjų programų kontrolės (žr. 1 pav.).

1 pav. IT kontrolės priemonės

9. IT bendroji kontrolė yra IT kontrolės sistemos pagrindas. Ji susijusi su bendra aplinka, kurioje IT sistemos yra kuriamos, eksploatuojamos ir prižiūrimos. IT bendrosios kontrolės priemonės nustato bendrą IT veiklos kontrolės sistemą ir užtikrina, kad bendri kontrolės tikslai būtų pasiekti. Šios kontrolės priemonės įgyvendinamos naudojant įvairias priemones, pvz.: politiką, gaires ir procedūras, įdiegiant tinkamą valdymo struktūrą, įskaitant organizacijos IT sistemų valdymo struktūrą. IT bendrosios kontrolės pavyzdžiai yra IT strategijos ir IT saugumo politikos rengimas ir įgyvendinimas, IT valdymo komiteto įsteigimas, IT darbuotojų organizavimas siekiant atskirti prieštaringas pareigas ir nelaimių prevencijos ir atkūrimo planavimas.

10. Taikomosios programos kontrolės priemonės – tai specifinės kontrolės priemonės, būdingos kiekvienai taikomajai programai. Jos taikomos programos segmentams (posistemiams) ir yra susijusios su tokiomis transakcijomis kaip duomenų įvedimas, apdorojimas ir išvestis:

    - ✓ Įvesties kontrolės priemonės turi užtikrinti, kad į taikomąją programą būtų įvesta tik tinkama informacija (reikiamo ilgio, formato, turinio, struktūros, pan.), kuri nebūtų įvesta kelis kartus, įvedama tik asmens, kuris turi reikiamus įgaliojimus, kt.
    - ✓ Apdorojimo kontrolės priemonės turi užtikrinti įvestų duomenų išsamumą ir tikslumą, pvz., kontrolės priemonės, kurios tikrina ir fiksuoja visus atliekamus keitimus, sulygina apdorojamų ir įvestų eilučių skaičių ir kt.
    - ✓ Išvesties kontrolės priemonės užtikrina, kad vartotojams būtų pateiktos naudoti ataskaitos, kurios sudarytos pagal nustatytus reikalavimus, užtikrinant išvedamų duomenų tikslumą ir saugumo reikalavimus (pvz., nuasmeninimas).

11. Visos minėtos kontrolės priemonės paprastai susijusios su organizacijos veiklos procesų logika. Išsamiau apie taikomųjų programų kontrolės priemones žr. 5 priede.

12. IT bendrosios kontrolės priemonės, kitaip nei taikomųjų programų kontrolės priemonės, nėra būdingos tik konkrečioms taikomosioms programoms. IT bendrosios kontrolės tikslas – užtikrinti tinkamą ir saugų organizacijos visos informacinės sistemos ir joje esančių taikomųjų programų kūrimą, veikimą, priežiūrą ir vystymą.

13. IT bendrųjų kontrolės priemonių rengimas ir įgyvendinimas gali turėti didelį poveikį taikomųjų programų kontrolės veiksmingumui. IT bendrosios kontrolės priemonės suteikia programoms reikalingus išteklius (pvz., žmogiškuosius, procesinius, finansinius) ir bazines kontrolės priemones. Jei IT bendrosios kontrolės priemonės yra silpnos, jos labai sumažina kontrolės priemonių, susijusių su IT taikomosiomis programomis, patikimumą, t. y. IT bendrųjų kontrolės priemonių struktūra ir veikimo veiksmingumas labai priklauso nuo to, kokiu mastu vadovybė gali pasikliauti taikomųjų programų kontrole, siekiant valdyti riziką. Todėl atliekant taikomosios programos kontrolės priemonių vertinimą svarbu įvertinti ir IT bendrosios kontrolės priemonių veikimą.

14. IT bendrosios kontrolės priemonės, kurios labiausiai daro poveikį taikomosios programos kontrolės priemonėms, yra šios[18]:

    - ✓ prieigos prie infrastruktūros, taikomųjų programų ir duomenų valdymas;
    - ✓ IS kūrimo valdymas;
    - ✓ IS incidentų, pakeitimų, problemų valdymas;
    - ✓ duomenų atsarginių kopijų ir veiklos tęstinumo valdymas.

1.3. IT kontrolės priemonių tipai

15. Kiekviena organizacija sukuria savo veiklai užtikrinti reikiamą vidaus kontrolės priemonių sistemą, kuri užkerta kelią įvairiems incidentams įvykti, leidžia apsaugoti turtą nuo neteisėtų veiksmų, mažina sukčiavimo rizikas, padeda nustatyti galimai atliktus neteisėtus

[18] INTOSAI IT audito darbo grupė (WGITA) ir INTOSAI vystymo iniciatyva (IDI) parengtas IT audito vadovas, 5 psl.

veiksmus ir pan. IT kontrolės priemonės yra organizacijos vidaus kontrolės dalis, kaip ir vidaus kontrolės priemonės, jos skirstomos į 3 tipus:

- ✓ *Prevencinės kontrolės priemonės*, kurių paskirtis yra užkirsti kelią klaidoms, kenkėjiškai veiklai pasireikšti ir pan. Pavyzdžiui, prevencinės IT kontrolės priemonės gali būti: tam tikri tikrinimo veiksmai, kad į darbą būtų priimamas tik kvalifikuotas ir nepriekaištingą reputaciją turintys personalas; funkcijų, kurios nesuderinamos, atskyrimas, kad būtų mažinama sukčiavimo ar piktnaudžiavimo rizika; fizinės pareigos prie IT išteklių ribojimas, kad pašaliniai asmenys negalėtų laisvai prieiti prie išteklių ir pakenkti organizacijai; duomenų šifravimas, siekiant užkirsti kelią neteisėtam duomenų atskleidimui; taikomosios programos atliekamas automatinis suvedamų duomenų tikrinimas, pvz., ar suvestas asmens kodas yra be klaidų ir kt.
- ✓ *Aptikimo kontrolės priemonės*, kurios aptinka ir praneša apie įvykusį įvykį, klaidą, neveikimą ar piktybinį veiksmą. Tai galėtų būti, pvz.: įdiegta sistema, kuri surenka informaciją apie tinkle fiksuojamus neteisėtus veiksmus ir praneša už saugumą atsakingiems asmenims; vidaus audito atlikimas; veiksmų (angl. *Log*) žurnalų peržiūra; programinio kodo peržiūra; įvairūs patikrinimai ir testavimai siekiant nustatyti defektus ar teisės aktų nesilaikymo atvejus.
- ✓ *Korekcinės kontrolės priemonės*, kurios sumažina grėsmių poveikį, sudaro sąlygas identifikuoti problemų priežastis ir jas pašalinti, taip pat tobulinti esamą kontrolės sistemą, kad būtų sumažintos ateityje galinčios kilti rizikos. Tokios kontrolės priemonės galėtų būti, pvz.: atsarginių duomenų kopijų kaupimas; veiklos tęstinumo planavimas; incidentų ir problemų valdymas; paslaugų lygių valdymas.

16. Auditorius, atlikdamas IT auditą, turi suprasti kokio tipo IT kontrolės priemonės naudojamos audituojamame subjekte, siekiant sumažinti organizacijos rizikas.

1.4. Audito šalys

17. Kiekvienas auditas apima tris tarpusavyje susijusias audito šalis:

- ✓ *auditorių*, kurio pareiga yra surinkti pakankamų ir tinkamų audito įrodymų audito tikslui pasiekti ir pagal tai parengti audito ataskaitą;
- ✓ *atsakingąją šalį (audituojamą subjektą ir kitas institucijas)* – subjektus, atsakingus už audito srities informaciją, audito srities valdymą ir (ar) rekomendacijų įgyvendinimą ir būtinų pokyčių taikymą;
- ✓ *numatomus naudotojus*, kurie yra asmenys ir (ar) institucijos, kuriems auditorius rengia audito ataskaitą. Numatomi naudotojai paprastai yra įstatymų leidžiamoji ir vykdomoji valdžia, visuomenė (piliečiai). Tai gali būti ir su tam tikros politikos įgyvendinimu susijusios organizacijos, suinteresuotos audito ataskaita, konkrečios srities, su kuria susijęs auditas, ekspertai, nevyriausybinės organizacijos, žiniasklaida, akademinė bendruomenė ir kt. Numatomu naudotoju taip pat gali būti atsakingoji šalis. Numatomus naudotojus patartina išsiaiškinti kuo ankstesniame audito etape.

18. Sprendimui, kas yra svarbios atsakingosios šalys ir numatomi naudotojai, turi įtakos audito objektas, tikslas, klausimai, pasirinkti audito kriterijai ir kt. Audito metu svarbu įvertinti

numatomų naudotojų ir atsakingųjų šalių poreikius ir interesus. Taip auditorius gali užtikrinti, kad šiems subjektams audito ataskaita bus naudinga ir suprantama, bet tai jokiu būdu neturėtų neigiamai paveikti auditoriaus nepriklausomumo ir objektyvaus požiūrio.

1.5. Pasitikėjimas ir užtikrinimas atliekant auditą

Kaip ir bet kokio kito audito atveju, IT audito ataskaitų naudotojai nori būti tikri, kad informacija, kurios pagrindu jie priima sprendimus, yra patikima. Todėl auditoriai turi atlikti atitinkamas procedūras, skirtas sumažinti riziką, kad bus pateiktos netinkamos išvados ir ataskaitoje pateikti informaciją, pagrįstą pakankamais ir tinkamais įrodymais.

Numatomiems naudotojams turi būti suteiktas pakankamo lygio užtikrinimas (tai aukšto lygio, tačiau neabsoliutus užtikrinimas, nes dėl auditui būdingų apribojimų auditas negali suteikti absoliutaus užtikrinimo). Kad to pasiektų, auditorius audito ataskaitoje turi aiškiai pateikti audito tikslą, klausimus, kriterijus, apimtį ir visus svarbius apribojimus, metodus, surinktus įrodymus, pastebėjimus ir išvadas. Svarbu, kad numatomiems naudotojams būtų aiškūs ryšiai tarp šių elementų, kad naudotojai suprastų, jog audito kriterijai, audito pastebėjimai ir išvados yra nešališki ir pagrįsti ir kodėl, atsižvelgiant į audito kriterijus ir pastebėjimus, buvo pateiktos tam tikros išvados ir rekomendacijos. Jeigu tai atliekama tinkamai, numatomi naudotojai gali pasitikėti išvadų pagrįstumu. Tokiu atveju laikoma, kad auditorius suteikė užtikrinimą.

1.6. IT auditas ir jungtiniai auditai

19. Pagal GUID 5100 IT auditas gali būti atliekamas:

    - ✓ kaip atskiras IT auditas, kurio metu IT kontrolės priemonės vertinamos 3E ir (ar) atitikties aspektais. Šiuos auditus atlieka VK Informacinių technologijų audito departamentas;
    - ✓ kaip jungtinis auditas, kuris yra platesnio masto audito (finansinio, atitikties ar veiklos) dalis. Šiuo atveju atliekamos IT audito procedūros, kurios padeda pasiekti šių auditų tikslus. Paprastai toks auditas nėra vadinamas jungtiniu auditu, o pasitelkiami IT audito specialistai (ekspertai) kaip dalis TAAIS numatytų finansinio, veiklos ar atitikties audito procedūrų (2 pav.).

2 pav. IT auditas ir jungtiniai auditai

20. Atskiras IT auditas gali būti atliekamas pagal poreikį įtraukiant audito temas į metinį veiklos planą. Atliekant tokį auditą, priklausomai nuo audito tikslo ir pasirinktos problematikos, gali būti pasirenkami skirtingi IT kontrolės vertinimo aspektai, t. y. IT audito metu gali būti vertinami IT kontrolės priemonių atitikties pasirinktiems kriterijams aspektai ir (arba) vertinami esamų IT kontrolės priemonių 3E aspektai (pvz., ar IT plėtros planas parengtas laikantis teisės aktų reikalavimų, ar IT paslaugų tarnyba kokybiškai išsprendžia visus incidentus).

21. Finansinio audito metu paprastai atliekami IT kontrolės priemonių (bendrųjų ir (ar) taikomųjų) vertinimai, kurie susiję su apskaitos IS ir jų veikimo patikimumu. Tokiais atvejais testuojamos pasirinktos IT bendrosios ir (ar) taikomųjų programų kontrolės priemonės, kurios susijusios su tvarkoma finansine atskaitomybe, siekiant įvertinti šių kontrolių veiksmingumą ir įtaką finansinės atskaitomybės tinkamumui ir teisingumui. Daugiau informacijos apie finansinį auditą galima rasti 2000-ajame TAAIS ir Valstybės kontrolės parengtame Finansinio audito vadove.

22. Veiklos audito metu tinkamu IT kontrolės priemonių sukūrimas ir vykdymas traktuojamas kaip vienas veiksnių, užtikrinančių veiklos ekonomiškumą, efektyvumą ir (ar) rezultatyvumą. Tam tikros IT audito procedūros gali būti taikomos siekiant įsitikinti patikimumu duomenų, naudojamų veiklos audito vertinimuose. Daugiau informacijos apie veiklos auditą galima rasti 3000-ajame TAAIS ir Valstybės kontrolės parengtame Veiklos audito vadove.

23. Atliekant atitikties auditą ir kartu vertinant IT kontroles priemones, pagrindinis vertinimo aspektas susijęs su atitiktimi tam tikriems teisės aktų ir (ar) kitiems reikalavimams. Atitikties audito metu priklausomai nuo audito tikslo gali būti vertinama kaip IT kontrolės priemonės atitinka teisės aktų reikalavimus, kitus reikalavimus, bendruosius principus ar IT valdymo gerąją praktiką, pvz., COBIT. Gali būti vertinama tai, kiek įdiegtos IT kontrolės priemonės, kurios skirtos užtikrinti veiklos atitiktį tam tikriems reikalavimams, patikimos ir padeda pasiekti reikiamus tikslus, pvz., organizacijoje veikia taikomoji programa, kurioje saugos įgaliotinis atlieka atitikties vertinimus, tokiais atvejais gali būti vertinamas šios sistemos atliekamų funkcijų pakankamumas atsižvelgiant į teisinį reguliavimą. Daugiau

informacijos apie atitikties auditą galima rasti 4000-ajame TAAIS ir Valstybės kontrolės parengtame Atitikties audito vadove.

24. Planuojant ir atliekant jungtinį auditą:

- ✓ rekomenduojama audito metu taikyti tą TAAIS, kuris atitinka atliekamo audito tipą, pvz., jei atliekamas finansinis auditas – pagrindiniai taikomi turi būti 2000–2999-ieji TAAIS, o užduotims, kurios susijusios su IT kontrolės vertinimu, reikėtų taikyti šio vadovo ir GUID 5100-ojo reikalavimus tiek, kiek tai susiję su minėtų užduočių atlikimu. Bet kuriuo atveju auditoriai turėtų priimti profesinį sprendimą kaip ir kokia apimtimi jungtiname audite bus taikomi tam tikrų TAAIS ir GUID reikalavimai ir šie sprendimai turėtų būti dokumentuoti. Esant neaiškumų dėl TAAIS taikymo konkretaus audito atveju, rekomenduojama konsultuotis su metodologais;
- ✓ audito grupė, kaip visuma, turi dirbti kartu, kad būtų pasiektas bendras audito tikslas. Siekiant veiksmingos IT auditorių integracijos, audito plane turi būti aiškiai nustatyta, kokios IT kontrolės vertinimo užduotys būtinos veiklos, atitikties ar finansinio audito tikslams pasiekti, o IT auditorių atliekamas darbas turi būti išsamiai dokumentuotas. Pagal audito planą IT auditorių parengti darbo dokumentai sukeliami į ViPSIS atitinkamo projekto užduoties aplanką. Darbas ViPSIS vyksta bendra tvarka atsižvelgiant į ViPSIS naudotojo vadovo reikalavimus;
- ✓ IT auditorių ir kitų auditorių keitimasis informacija, bendri susitikimai turėtų vykti pagal audito plane ar darbų grafike suplanuotas procedūras;
- ✓ audito grupę turi sudarytų nariai, kurie būtų kompetentingi kartu atlikti IT audito užduotis, kad būtų pasiekti numatyti finansinio, veiklos ar atitikties audito tikslai.

25. Sprendimai dėl jungtinių auditų atlikimo priimami strateginio planavimo metu. Sprendimas pasitelkti IT audito specialistus (ekspertus) gali būti priimtas tvirtinant audito planą arba strategiją. Atliekant veiklos, finansinį ar atitikties jungtinius IT auditus, VK vidaus ar išorės IT audito specialistai (ekspertai) pasitelkiami vadovaujantis *Valstybės kontrolės metinės veiklos planavimo tvarkos aprašu*.

2. BENDRIEJI IT AUDITO REIKALAVIMAI

26. Bendrieji visų audito rūšių (atitikties, finansinio ir veiklos) reikalavimai numatyti 100-ajame TAAIS „Pagrindiniai viešojo sektoriaus audito principai“. Šie reikalavimai turėtų būti taikomi prieš pradedant auditą ir viso audito proceso metu. 300-ajame TAAIS „Veiklos audito principai“ ir 3000-ajame TAAIS „Veiklos audito standartas“ bendrieji reikalavimai detalizuojami juos pritaikant veiklos auditui, 400-ajame TAAIS „Atitikties audito principai“ ir 4000-ajame TAAIS „Atitikties audito standartas“ – atitikties auditui. Finansinio audito bendrieji reikalavimai detalizuojami 200-ajame TAAIS „Finansinio audito principai“ ir 2000–2899-uosiuose TAAIS. Bendrieji reikalavimai IT auditui nėra išskirti atskiruose standartuose, tačiau jie sutampa su kitų audito tipų bendraisiais reikalavimais.

2.1. Etika ir nepriklausomumas

Susiję TAAIS reikalavimai
Auditorius privalo laikytis AAI nustatytų nepriklausomumo ir etikos procedūrų, kurios turi atitikti TAAIS dėl nepriklausomumo ir etikos. *(3000-ojo TAAIS 21 punktas)* Auditorius, siekdamas, kad audito pastebėjimai ir išvados būtų nešališki ir tokie atrodytų numatomiems vartotojams, privalo pasirūpinti, kad išliktų nepriklausomas. *(3000-ojo TAAIS 21 punktas)* Auditorius privalo laikytis atitinkamų procedūrų, susijusių su objektyvumu ir etika, kurios savo ruožtu turi atitikti susijusius objektyvumo ir etikos TAAIS. *(4000-ojo TAAIS 45 punktas)* Auditorius privalo išlikti objektyvus, kad audito rezultatai ir išvados būtų objektyvūs ir atrodytų tokie trečiosioms šalims. *(4000-ojo TAAIS 48 punktas)*

27. Auditorius turi elgtis sąžiningai, profesionaliai, išlikti nepriklausomas ir objektyvus, turėti reikalaujamą profesinę kompetenciją, išlaikyti profesinį konfidencialumą. 130-asis TAAIS „Etikos kodeksas“ nurodo, kad tai yra vertybės, kuriomis turi būti grindžiamas auditorių etiškas elgesys.

28. Auditorius turi užtikrinti, kad bendravimas su suinteresuotomis šalimis nepakenktų jo nepriklausomumui. Atlikdamas auditą auditorius turi vengti netinkamos bet kurios suinteresuotos šalies įtakos ir išlaikyti objektyvumą, kad jo darbas ir ataskaitos būtų nešališki trečiosioms šalims. Nepriklausomumas leidžia auditoriui atlikti auditą nepatiriant jokios įtakos, galinčios sukompromituoti profesinį sprendimą, veikti principingai, objektyviai ir laikantis profesinio skepticizmo. Turi būti užtikrinta, kad nėra aplinkybių, kurios priverstų pagrįstai suabejoti auditoriaus principingumu, objektyvumu ar profesiniu skepticizmu arba nuspręsti, kad auditorius yra sukompromituotas.

29. Audito grupė ir kiti audito procese dalyvaujantys asmenys privalo vadovautis 130-uoju TAAIS ir *Valstybės kontrolės darbuotojų etikos kodekse* nustatytais etikos reikalavimais ir vertybėmis. Visi audito grupės nariai, pradėdami auditą ar prisijungę prie audito, ir jo procese dalyvaujantys asmenys, pradėdami vykdyti pavestą užduotį, privalo pasirašyti nešališkumo ir nepriklausomumo deklaraciją, kaip tai numatyta *Valstybinių auditų kokybės užtikrinimo vadove*.

30. Išsamesnė informacija apie objektyvumą, nepriklausomumą ir kitus etikos principus bei vertybes pateikta 10-ajame INTOSAI-P „*Meksiko deklaracija dėl AAI nepriklausomumo*“, 9030-osiose GUID „*Su AAI nepriklausomumu susijusios INTOSAI gairės ir geroji praktika*“ ir 130-ajame TAAIS „*Etikos kodeksas*“.

2.2. Profesinis sprendimas, skepticizmas ir reikiamas atidumas

Susiję TAAIS reikalavimai
Auditorius privalo vadovautis profesiniu sprendimu, laikytis skepticizmo principo ir apsvarstyti klausimus iš skirtingų pozicijų, išlikti atviras ir objektyvus įvairių požiūrių bei argumentų atžvilgiu. *(3000-ojo TAAIS 68 punktas)* Audito proceso metu auditorius privalo taikyti profesinį sprendimą. *(4000-ojo TAAIS 71 punktas)* Auditorius privalo išlaikyti profesinį skepticizmą bei atvirą ir objektyvų požiūrį. *(4000-ojo TAAIS 77 punktas)*

Profesinis sprendimas

31. Profesinis sprendimas – tai žinių, įgūdžių ir patirties taikymas audito metu priimant kompetentingus sprendimus dėl audito aplinkybes atitinkančios veiksmų krypties. Taikant profesinį sprendimą svarbu laikytis tinkamo atsargumo ir nuosekliai taikyti visus susijusius profesinius standartus ir etikos principus.

32. Profesinio sprendimo principu auditorius privalo vadovautis viso audito metu. Profesinis sprendimas naudojamas vertinant problemas ir (ar) rizikas, reikšmingumą, apibrėžiant audito objektą, tikslą, klausimus ir kriterijus, apimtį, apsisprendžiant dėl procedūrų, reikalingų surinkti pakankamus ir tinkamus audito įrodymus ir juos įvertinti. Jis taip pat naudojamas vertinant, kokius pastebėjimus, išvadas ir rekomendacijas teikti audito ataskaitoje ir kt. Šis sprendimas labai svarbus analizuojant audito įrodymus ir formuojant jais pagrįstus pastebėjimus ir išvadas.

33. Labai svarbu, kad auditorius tinkamai dokumentuotų visus profesinius sprendimus, aiškiai įvardindamas, kokiais kriterijais, faktais, aplinkybėmis ir žiniomis jis rėmėsi priimdamas konkretų profesinį sprendimą ir jį pagrįstų.

Profesinis skepticizmas ir reikiamas atidumas

34. Profesinis skepticizmas reiškia, kad viso audito metu, o ypač vertindamas surinktų įrodymų pakankamumą ir tinkamumą, auditorius turi būti budrus ir kritiškas.

35. Profesinis skepticizmas apima reikiamą atidumą dėl, pavyzdžiui:

- ✓ audito įrodymų, prieštaraujančių kitiems gautiems audito įrodymams;
- ✓ informacijos, kuri kelia abejonių dėl dokumentų ir duomenų patikimumo;
- ✓ atsakymų į paklausimus, kurie bus naudojami kaip audito įrodymai;
- ✓ sąlygų, kurios gali reikšti galimą audituojamo subjekto vadovybės ir (ar) kitų atsakingų asmenų nesąžiningą elgesį, sukčiavimą.

36. Profesinio sprendimo ir skepticizmo laikymasis padeda auditoriui įsigilinti į įvairius požiūrius ir argumentus, geriau apsvarstyti skirtingas pozicijas, išlaikyti objektyvumą ir įvertinti visus audito įrodymus. Be to, tai padeda auditoriui išvengti sprendimo klaidų ar šališkumo ir pateikti objektyvias išvadas remiantis kritiniu visų surinktų audito įrodymų vertinimu.

37. Iš auditoriaus tikimasi, kad jis veiks laikydamasis reikiamo atidumo. Reikiamas atidumas apima kruopštų darbą ir tinkamą rūpinimąsi audito planavimu, įrodymų rinkimu ir vertinimu, pastebėjimų, išvadų ir rekomendacijų pateikimu. Aukštus profesionalaus elgesio standartus reikia išlaikyti viso audito metu – nuo temos parinkimo iki audito ataskaitos pateikimo.

2.3. Audito rizika

Susiję TAAIS reikalavimai
Auditorius privalo aktyviai valdyti audito riziką, siekdamas išvengti pateikti neteisingus ar neišsamius audito pastebėjimus, išvadas ir rekomendacijas, nesubalansuotą informaciją ar siekdamas išvengti situacijos, kad nebus sukurta pridėtinės vertės. *(3000-ojo TAAIS 52 punktas)* Auditorius privalo atlikti procedūras, reikalingas sumažinti neteisingų išvadų parengimo riziką iki priimtino žemo lygio. **(***4000-ojo TAAIS 52 punktas***)**

38. Audito rizika – tai tikimybė, kad dėl įvairių atsiradusių veiksnių ar įvykių gali būti pateikti neteisingi ar neišsamūs pastebėjimai, išvados, rekomendacijos, nepasiektas arba nevisiškai pasiektas audito tikslas, nebus pasiektas laukiamas audito poveikis.

39. Audito rizikos vertinimas skatina auditorių sutelkti dėmesį į pagrindinius audito klausimus, atsižvelgiant į išteklių ir laiko apribojimus. Audito rizika turi būti vertinama ir valdoma viso audito metu. Aktyvus valdymas apima galimos ar žinomos rizikos numatymą, jos valdymo priemonių nustatymą ir dokumentavimą.

Audito rizikos ir patikimumo modelis

Pagal 5100-ąjį GUID IT audito rizikos modelį sudaro trys komponentai:

- ✓ 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;

- ✓ IT kontrolės rizika – tai tikimybė, kad audituojamo subjekto patvirtintomis IT kontrolės priemonėmis gali nepavykti sumažinti neigiamo poveikio, į kurį reaguojant jos buvo sukurtos;
- ✓ neaptikimo rizika – tai tikimybė, kad auditorius nenustatys, kad nėra subjekto patvirtintų IT kontrolės priemonių, kad jos neveikia ar netinkamos, o tai galėtų turėti neigiamą poveikį subjektui.

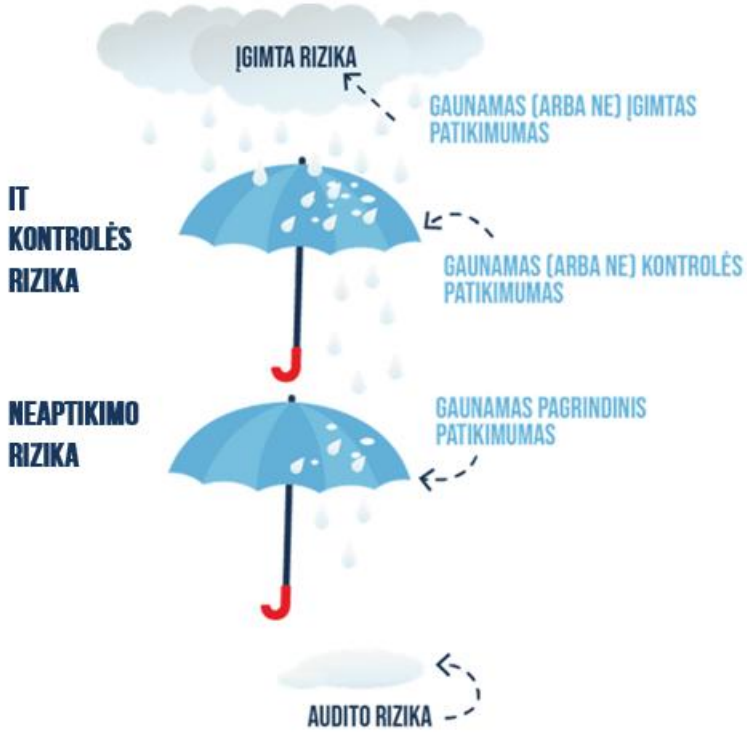
40. Išankstinio tyrimo metu atlikus IT bendrosios ir (ar) taikomosios kontrolės priemonių vertinimą ir nustačius rizikingas IT kontrolės priemonių sritis, auditoriai turėtų apsvarstyti kiekvieną pirmiau nurodytų rizikos komponentų ir pagal tai įvertinti, koks yra audito rizikos lygis. Šie trys audito rizikos komponentai (įgimta, kontrolės ir neaptikimo rizika) turi būti vertinami kartu audito rizikos vertinimo metu, nes jie tiesiogiai vienas kitą veikia. Kuo didesnis auditoriaus įvertintas įgimtos ir (arba) kontrolės rizikos lygis, tuo didesnė bus neaptikimo rizika ir reikės atlikti išsamesnį audito darbą, kad būtų gautas didesnis patikimumas ir neaptikimo rizika būtų sumažinta iki priimtino lygio. Kita vertus, jeigu įgimta rizika normali, o IT kontrolės priemonės tinkamos, tada neaptikimo rizika mažesnė ir galime suplanuoti mažesnės apimties pagrindines audito procedūras reikiamam patikimumui gauti.

41. Bendrą IT audito patikimumą galima gauti iš trijų komponentų:
    - ✓ įgimto patikimumo – gaunamas planavimo metu įvertinus įgimtą riziką, kai nėra nustatyta išskirtinių aplinkybių, kurios didina įgimtą riziką;
    - ✓ kontrolės patikimumo – gaunamas įvertinus, ar IT kontrolė pakankama ir patikima, ar ji laiku užkerta kelią pažeidžiamumams, dėl kurių gali atsirasti neigiamas poveikis organizacijos veiklai ir jos tikslų pasiekimui. Tai atliekama susipažinus su organizacijos veiklos ir IT valdymo aplinka ir IT kontrolės priemonių įgyvendinimo procedūromis bei atlikus IT kontrolės priemonių vertinimą;
    - ✓ pagrindinio patikimumo – gaunamas atlikus pagrindines audito procedūras. Kuo daugiau išsamesnių ir didesnės apimties tinkamų procedūrų auditorius atliks, tuo didesnį pagrindinį patikimumą gaus. Priklausomai nuo gauto įgimto ir IT kontrolės patikimumo teks atlikti daugiau ar mažiau pagrindinių audito procedūrų.

Audito rizikos ir audito patikimumo ryšiai

IT audito rizika yra atvirkštinė audito patikimumui, t. y., jei ši rizika yra maža, pakankamam patikimumui gauti užteks mažiau procedūrų nei tais atvejais, kai audito rizika didelė.

3 pav. Audito patikimumo ir audito rizikos ryšiai



42. Išsamiau apie konkrečius veiksmus, kuriuos auditorius turi atlikti vertindamas audito riziką, pateikta Vadovo 4.1.6 skirsnyje.

2.4. Reikšmingumas

Susiję TAAIS reikalavimai
Auditorius privalo atsižvelgti į reikšmingumą visuose audito proceso etapuose, įskaitant finansinius, socialinius ir politinius srities aspektus, siekiant sukurti kiek įmanoma didesnę pridėtinę vertę. (*3000-ojo TAAIS 83 punktas*) Auditorius privalo nustatyti reikšmingumą, kad suformuotų pagrindą audito planavimui ir galėtų iš naujo jį įvertinti viso audito proceso metu. (*4000-ojo TAAIS 125 punktas*)

43. Reikšmingumas gali būti apibrėžtas kaip santykinė dalyko reikšmė (arba svarba) tomis aplinkybėmis, kuriomis jis nagrinėjamas. Į reikšmingumą auditoriai turėtų atsižvelgti viso audito proceso metu.

44. Reikšmingumas gali būti vertinamas atsižvelgiant į kiekybinius ir kokybinius veiksnius. Kokybiniai veiksniai gali apimti tokius aspektus kaip: ar pastebėjimas atsirado dėl tyčinio (apgaulės) ar netyčinio veiksmo; ar tam tikras audituojamo subjekto veiklos aspektas yra reikšmingas atsižvelgiant į veiklos pobūdį, daromą poveikį, numatomų naudotojų poreikius, socialinę ar politinę svarbą ir kt.; ar pastebėjimas susijęs su skaidrumu ir

atskaitomybe ir pan. Kiekybiniai veiksniai yra susiję su pastebėjimų svarba, kuri išreiškiama skaičiais.

45. Reikšmingumas yra svarbus skirtingais veiklos audito aspektais, pvz.: tikslo, audito kriterijų nustatymas, audito įrodymų vertinimas, dokumentų rengimas ir rizikos, kad bus pateikti netinkami ar nedidelį poveikį turintys audito pastebėjimai ar parengtos netinkamos ataskaitos, valdymas. Auditoriui svarbu atsižvelgti į tai, kad, laikui bėgant, reikšmingumas gali kisti ir priklausyti nuo numatomų naudotojų ir atsakingųjų šalių pozicijos.

46. Pastebėjimai laikomi reikšmingais, kai galima pagrįstai tikėtis, kad jie paskatins numatomus naudotojus priimti atitinkamus sprendimus remiantis auditoriaus ataskaita. Kaip auditorius vertina reikšmingumą, yra jo profesinio sprendimo klausimas, kaip jis suvokia bendruosius numatomų naudotojų poreikius.

47. Plačiau apie reikšmingumą IT audite pateikta Vadovo 4.1.7. skirsnyje.

2.5. Dokumentavimas

Susiję TAAIS reikalavimai
Auditorius privalo pakankamai išsamiai ir detaliai dokumentuoti auditą. (*3000-ojo TAAIS 86 punktas*) Auditorius privalo parengti audito dokumentus, kurie būtų pakankamai išsamūs, kad suteiktų aiškų supratimą apie atliktą darbą, surinktus įrodymus ir padarytas išvadas. Auditorius privalo parengti audito dokumentus laiku, viso audito metu juos atnaujinti ir dokumentuoti įrodymus, palaikančius audito rezultatus, iki išleidžiant audito ataskaitą. (*4000-ojo TAAIS 89 punktas*)

48. Tinkamas dokumentavimas padeda susidaryti aiškią nuomonę apie atliktą audito darbą, leidžia apie auditą išankstinių žinių neturinčiam patyrusiam auditoriui suprasti atlikto audito pobūdį, laiko paskirstymą, apimtį ir rezultatus, gautus audito įrodymus, kuriais grindžiami audito pastebėjimai, išvados ir rekomendacijos, ir visų svarbių dalykų, kuriems būtina taikyti profesinį sprendimą, priežastis.

Darbo dokumentų paskirtis

49. Darbo dokumentai – dokumentuota informacija apie atliktas audito procedūras, surinktus audito įrodymus ir auditoriaus padarytas išvadas. Visas audito procesas nuo planavimo iki audito ataskaitos parengimo turi būti dokumentuojamas. Darbo dokumentai jungia auditoriaus darbą, atliekamą viso audito proceso metu renkant ir vertinant informaciją ir duomenis, ir audito ataskaitą.

50. Darbo dokumentai yra svarbūs, nes:

- ✓ palengvina audito planavimą;
- ✓ pagrindžia ir patvirtina auditoriaus sprendimus, nuomones, pastebėjimus, išvadas ir rekomendacijas;

- ✓ yra informacijos šaltinis rengiant audito ataskaitą ir atsakant į audituojamo subjekto ar kitų subjektų klausimus (padeda apsiginti nuo pretenzijų, teisminių bylų ir kitų teisinių procesų atveju);
- ✓ yra pagrindas prižiūrėti audito procesą ir atlikti audito peržiūrą, užtikrinti audito kokybę;
- ✓ parodo auditoriaus kompetenciją, fiksuoja jo atliktą darbą;
- ✓ užtikrina atlikto darbo atsekamumą.

Darbo dokumentų turinys

51. Yra skirtingo tipo darbo dokumentų:
    - ✓ audito planavimo dokumentai: išankstinio tyrimo planas, audito planas;
    - ✓ rezultatų apibendrinimo dokumentai: išankstinio tyrimo rezultatų apibendrinimas, audito rezultatų suvestinė;
    - ✓ darbo dokumentai, kuriuose dokumentuojamos atliekamos audito procedūros, pateikiami audito įrodymai ir kt.;
    - ✓ kiti darbo dokumentai, kuriuose, pavyzdžiui, dokumentuojami auditorių profesiniai sprendimai, kurie turi įtakos audito planavimui, atlikimui ir rezultatų pateikimui (pvz., sprendimai dėl subjektų ar vertinamų vienetų atrankos, reikšmingumo ir kt.), arba dokumentuojama kita svarbi informacija, turinti įtakos audito metu priimamiems sprendimams (pvz., informacija, gauta įvairiuose susitikimuose, aptarimuose, ir kt.).
52. Reikalavimai audito planavimo ir rezultatų apibendrinimo dokumentų struktūrai ir turiniui pateikti tolesniuose šio Vadovo skyriuose. Darbo dokumentai, kuriuose dokumentuojamos atliekamos audito procedūros ir pateikiami audito įrodymai, turi būti analitinio pobūdžio, t. y. juose turi būti ne tik pateikiama surinkta informacija ir duomenys, bet ir atlikta jų analizė, pateikti vertinimai, išvados. Šiuose dokumentuose turi būti pateikta:
    - ✓ bendra informacija apie darbo dokumentą: dokumento sudarytojo (institucijos ir departamento) pavadinimas, numeris, dokumento pavadinimas ir data, audito ID, darbo dokumento rengėjas;
    - ✓ darbo dokumento tikslas;
    - ✓ atlikto darbo aprašymas: pateikiami surinkti įrodymai, pagrindžiantys auditoriaus pastebėjimus, išvadas ir rekomendacijas;
    - ✓ išvada ir, esant poreikiui, preliminarios rekomendacijos, galimi pokyčių vertinimo rodikliai;
    - ✓ priedai, kuriuose pateikiama su audito įrodymais susijusi, taip pat auditoriaus pastebėjimus ir išvadas patvirtinanti informacija ir dokumentai.
53. Darbo dokumentuose, kuriuose dokumentuojamos atliekamos audito procedūros ir pateikiami audito įrodymai, turi būti pateikiama ši informacija:

- ✓ kaip turi būti: nurodoma, kuo remiantis ir nuo ko bus skaičiuojamas ar matuojamas nuokrypis nuo audito kriterijaus;
- ✓ kaip yra iš tikrųjų: pateikiamos atliktos audito procedūros, surinkti įrodymai, jų analizė;
- ✓ nustatytas nuokrypis: aiškiai įvardijamas nuokrypis nuo audito kriterijaus, jeigu buvo nustatytas;
- ✓ priežastis (-ys), jeigu nustatytas nuokrypis nuo audito kriterijaus. Turi būti nustatomos kiekvieno kriterijaus nuokrypio priežastys, bet auditorius gali konstatuoti, kad kelių kriterijų nuokrypių priežastys yra sutampančios ir pasikartojančios, todėl plačiau jas aprašyti gali viename darbo dokumente, o prie kituose darbo dokumentuose pateiktų nuokrypių pateikti nuorodą į šį darbo dokumentą. Jeigu darbo dokumentuose nebuvo pateiktos priežastys, jos turi būti nurodytos audito rezultatų suvestinėje;
- ✓ pasekmė (-ės), kuri (-ios) atsiranda dėl vieno ar kelių audito kriterijų nuokrypių;
- ✓ audituojamo subjekto nuomonė dėl nustatyto nuokrypio (-ų), jei tokia buvo pateikta ir, esant poreikiui, auditoriaus vertinimas dėl jos. Tai pat gali būti pateikta kitų ekspertų nuomonė dėl nagrinėjamos srities, jeigu ji svarbi nagrinėjamo dalyko kontekste;
- ✓ esant poreikiui audito metu įvykę pokyčiai, kurie turi įtakos auditoriaus pastebėjimams ir išvadai;
- ✓ esant poreikiui gerosios praktikos pavyzdžiai ir kt.

54. Atliekant auditą darbo dokumentai gali būti rengiami audito procedūrai, audito kriterijui, darbo dokumentai jungiantys kelias audito procedūras ar kelis audito kriterijus, taip pat darbo dokumentai, kuriuose vertinama audito sritis ar klausimas pagal visus jam nustatytus kriterijus. Jeigu konkrečiam kriterijui yra rengiami keli darbo dokumentai, turi būti parengtas vertinimą pagal tą kriterijų apibendrinantis darbo dokumentas. Jeigu keliems kriterijams rengiamas vienas darbo dokumentas, išvados turi būti suformuluotos pagal kiekvieną audito kriterijų atskirai.

55. Darbo dokumentuose pateikta informacija turi būti pakankama, patikima ir tinkama pagrįsti auditoriaus pastebėjimus, padarytas išvadas ir pateiktas rekomendacijas. Darbo dokumentai turi būti suprantami, išsamūs, tikslūs, glausti, tvarkingi, jų rengimo sąnaudos neturėtų viršyti teikiamos naudos.

56. Kad būtų galima greitai susipažinti su audito įrodymais ir surasti reikiamą informaciją, dokumento struktūra turi būti logiška. Darbo dokumentuose, kuriuose vertinami audito metu surinkti duomenys ir gauta informacija, reikia pateikti nuorodas į informacijos šaltinius (audituojamo subjekto ar kitų subjektų, asmenų pateikta informacija) ar į konkrečius dokumentus (nurodyti jų pavadinimus, datas, rengėjus ir pan.), kad, prireikus, būtų galima juos surasti. Daugiau informacijos apie nuorodų teikimą galima rasti *Atmintinėje, kaip nurodyti teisės aktus, teisės aktų projektus ar teismų sprendimus galutiniuose Valstybės kontrolės veiklos produktų dokumentuose*.

57. Jeigu darbo dokumente fiksuojamas nuokrypis nuo audito kriterijaus, darbo dokumente ar prieduose privaloma pateikti ne tik nuorodas į šaltinius, bet ir visus su šiuo nuokrypiu

susijusius audito įrodymus, įskaitant visus reikiamus audituojamojo subjekto pateiktus ar iš kitų šaltinių gautus dokumentus.

58. Jeigu dalis įrodymų ar įrodymams vertinti reikalingų dokumentų, duomenų ar informacijos yra pateikiama kituose to paties audito darbo dokumentuose, darbo dokumente reikia pateikti nuorodas į tuos susijusius darbo dokumentus.

59. Išankstinio tyrimo etapo darbo dokumentai turi būti parengti ne vėliau nei patvirtinamas išankstinio tyrimo rezultatų apibendrinimas. Išankstinio tyrimo rezultatų apibendrinimas turi būti parengtas ir patvirtintas iki audito planavimo (išankstinio tyrimo) rezultatų pristatymo Valstybės kontrolės vadovybei, kurio metu aptariamos problemos ir (ar) rizikos. Jeigu yra atliekamas ne visos apimties išankstinis tyrimas ir nerengiamas išankstinio tyrimo rezultatų apibendrinimas (išsamiau Vadovo 4.1.1 skirsnyje), darbo dokumentai turi būti parengti ne vėliau nei audito plano projektas yra pateikiamas peržiūrėti valstybės kontrolieriaus pavaduotojui, kuriam tiesiogiai pavaldus auditą atliekantis departamentas.

60. Pagrindinio tyrimo etapo darbo dokumentai turi būti parengti ne vėliau nei yra patvirtinama audito rezultatų suvestinė. Ši suvestinė turi būti patvirtinta audito departamento vadovo iki audito ataskaitos projekto pateikimo peržiūrėti valstybės kontrolieriaus pavaduotojui, kuriam tiesiogiai pavaldus auditą atliekantis departamentas.

61. Esant poreikiui, darbo dokumentai gali būti patikslinti, bet ne vėliau kaip iki išankstinio tyrimo ataskaitos ar audito ataskaitos pasirašymo.

62. Audito priežiūros ir vidinės peržiūros procedūros plačiau išdėstytos Valstybinių auditų kokybės užtikrinimo vadove.

Darbo dokumentų įforminimas, tvarkymas ir saugojimas

63. Auditas dokumentuojamas ViPSIS. Detalesnė informacija pateikiama ViPSIS naudotojų vadovuose.

64. Jeigu organizuojamas susitikimas su audituojamu subjektu (pvz., siekiant gauti tam tikros informacijos ar aptarti išankstinio tyrimo ataskaitos, valstybinio audito ataskaitos projektus), vadovaujantis Valstybės kontrolės dokumentų valdymo ir naudojimo reglamento nustatyta tvarka gali būti daromas susitikimo garso įrašas, kuris, parengus šio susitikimo protokolą, sunaikinamas.

65. Auditorius turėtų vengti audito darbo dokumentuose ar jų prieduose atskleisti asmens duomenis[19]. Kaip tvarkyti asmens duomenis ir užtikrinti jų saugumą siekiant įgyvendinti Bendrojo duomenų apsaugos reglamento [20] nuostatas, pateikta Asmens duomenų, reikalingų atliekant valstybinį auditą, ES investicijų auditą ir biudžeto politikos stebėsenos vertinimus, gavimo ir tvarkymo gairėse. Kilus klausimų dėl asmens duomenų naudojimo ir tvarkymo, auditorius turėtų konsultuotis su Valstybės kontrolės atitikties pareigūnu.

---

[19] Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

[20] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Europos Sąjungos oficialusis leidinys L 119/1).

66. Darbo dokumentai tvarkomi ir saugomi vadovaujantis *Valstybės kontrolės dokumentų valdymo ir naudojimo reglamentu* ir *ViPSIS naudotojo vadovais*. Valstybinių auditorių veiksmus, susipažįstant su įslaptinta informacija ir ją naudojant valstybinio audito metu, kai šie veiksmai būtini siekiant išvengti įslaptintos informacijos praradimo ar neteisėto atskleidimo, nustato *Paslapčių subjektų ir Valstybės kontrolės įslaptintos informacijos naudojimo ir apsaugos tvarkos aprašas*.

67. Išankstinio tyrimo ir pagrindinio tyrimo darbo dokumento pavyzdinius šablonus galima rasti kompiuterio *MS Word* šablonų skiltyje. Detali informacija kaip juos pildyti pateikta *Darbo dokumentų šablonų pildymo instrukcijose*, kurias galima rasti Metodikos svetainės Šablonų skiltyje.

68. Rengiami oficialūs dokumentai (raštai, audito ataskaitos ir kt.), pateiktys (prezentacijos), infografikai ir siunčiamų el. laiškų parašai turi atitikti Valstybės kontrolės *Vizualinio stiliaus gide* pateiktas rekomendacijas dėl šrifto, teksto formatavimo ir spalvų naudojimo.

69. Išsamesni dokumentavimo reikalavimai, susiję su kiekvienu audito etapu, pateikti atitinkamose audito proceso dalyse.

2.6. Kokybės valdymas

Susiję TAAIS reikalavimai
AAI privalo užtikrinti, kad auditą atliekančių asmenų darbas būtų tinkamai prižiūrimas visuose lygmenyse ir audito etapuose. (*3000-ojo TAAIS 66 punktas*) AAI privalo sukurti ir palaikyti kokybės užtikrinimo sistemą, kurią auditorius privalo taikyti, siekdamas užtikrinti, kad būtų laikomasi visų reikalavimų. AAI taip pat privalo akcentuoti tinkamų, subalansuotų ir teisingų audito ataskaitų, kurios kuria pridėtinę vertę ir atsako į audito klausimus, svarbą. (*3000-ojo TAAIS 79 punktas*) AAI privalo prisiimti atsakomybę už bendrą audito kokybę, kad būtų užtikrinta, jog auditas atliktas laikantis atitinkamų profesinių standartų, įstatymų ir reglamentų, ir jog ataskaitos yra tinkamos atitinkamomis aplinkybėmis. *(4000-ojo TAAIS 80 punktas)*

70. Kokybės valdymo sistema apima tvarkas ir procedūras, sukurtas tam, kad AAI būtų pagrįstai užtikrinta, jog ji ir jos personalas laikosi profesinių standartų ir taikomų teisės aktų nustatytų reikalavimų. Šios sistemos tikslas yra užtikrinti, kad visi atliekami auditai išlaikytų aukštą kokybės lygį. Valstybinių auditų kokybės užtikrinimo nuostatos pateiktos *Valstybinių auditų kokybės užtikrinimo vadove*, parengtame pagal 140-ąjį TAAIS „*AAI kokybės valdymas*“.

2.7. Bendravimas

Susiję TAAIS reikalavimai

Auditorius viso audito metu privalo efektyviai ir tinkamai informuoti audituojamus subjektus ir atitinkamas suinteresuotąsias šalis apie pagrindinius audito aspektus.

(*3000-ojo TAAIS 55 punktas*)

Auditorius privalo užtikrinti, kad bendravimas su suinteresuotosiomis šalimis nesukompromituotų AAI nepriklausomumo ir nešališkumo.

(*3000-ojo TAAIS 59 punktas*)

Viso audito proceso metu auditorius privalo veiksmingu būdu bendrauti su audituojamu subjektu ir su už valdymą atsakingais asmenimis.

(*4000-ojo TAAIS 96 punktas*)

Apie reikšmingus reikalavimų nevykdymo atvejus turi būti informuota atitinkamo lygio vadovybė ir (jeigu taikoma) už valdymą atsakingi asmenys. Taip pat privaloma informuoti apie kitus iš audito kylančius klausimus, kurie yra tiesiogiai susiję su subjektu.

(*4000-ojo TAAIS 99 punktas*)

71. Efektyvus bendravimas yra svarbus nes, palaikant gerą abipusio bendravimo su audituojamu subjektu ir suinteresuotosiomis šalimis atmosferą, galima pagerinti auditoriaus prieigą prie informacijos ir duomenų, be to, tai gali padėti auditoriui geriau suprasti audituojamo subjekto ir suinteresuotųjų šalių požiūrį.

72. Svarbu, kad auditorius palaikytų gerus profesinius santykius su suinteresuotosiomis šalimis, skatintų laisvą ir atvirą keitimąsi informacija, nepažeistų konfidencialumo reikalavimų, vestų diskusijas laikydamasis abipusės pagarbos, suprasdamas kiekvienos suinteresuotosios šalies atliekamas atitinkamas funkcijas ir įsipareigojimus. Visgi toks bendravimas neturi paveikti AAI nepriklausomumo ir nešališkumo.

73. Bendravimas vyksta viso audito metu. Apie bet kokias reikšmingas kliūtis, su kuriomis buvo susidurta audito metu, ir bet kokius reikšmingus nuokrypius ar kitus audito metu nustatytus dalykus (pvz., apgaulės, korupcijos, teisės aktų nesilaikymo atvejai ir kitos situacijos, kai audituojamas subjektas privalo imtis skubių veiksmų, siekdamas išvengti potencialios žalos) derėtų kuo anksčiau pranešti audituojamo subjekto atitinkamo lygio vadovams ar asmenims, atsakingiems už valdymą:

    - ✓ jeigu auditorius nustato apgaulės ar korupcijos atvejus, ar kitus, jo vertinimu, reikšmingus dalykus, jis apie tai audituojamą subjektą informuoja oficialiu raštu;
    - ✓ kitais atvejais audito grupė nusprendžia, ar audituojamąjį subjektą informuoti oficialiu raštu ar el. paštu.

74. Išsamiau bendravimas ir bendradarbiavimas su audituojamu (-ais) subjektu (-ais) skirtingais audito proceso etapais aprašomi Vadovo 4.1 poskyryje „Audito planavimas“, 4.2 poskyryje „Pagrindinis tyrimas“ ir 4.3 poskyryje „Ataskaitos rengimas“.

2.8. Audito grupės įgūdžiai

Susiję TAAIS reikalavimai
AAI privalo užtikrinti, kad visi audito grupės nariai turėtų profesinę kompetenciją, reikalingą auditui atlikti.

(3000-ojo TAAIS 63 punktas, 4000-ojo TAAIS 85 punktas)

Auditorius privalo išlaikyti aukštą profesinio elgesio standartą.

(3000-ojo TAAIS 75 punktas)

Audito metu auditorius privalo būti pasirengęs taikyti naujoves.

(3000-ojo TAAIS 77 punktas)

Jeigu audito komanda negali pasinaudoti patirtimi spręsdama sunkų ar ginčytiną klausimą, turi būti gauta profesionali konsultacija.

(4000-ojo TAAIS 74 punktas)

75. Audito grupė turi būti sudaryta taip, kad jos nariai visi kartu turėtų turėti žinių, įgūdžių ir kvalifikacijos, reikalingos sėkmingai atlikti auditą. Tai reiškia, kad jie turi suprasti tos tipo auditą, kuris yra atliekamas, būti susipažinę su taikomais standartais ir įstatymais, audituojamo subjekto veikla ir sugebėti priimti profesinius sprendimus, turėti patirties juos priimant. Auditorius turi būti profesionalus, kad galėtų atlikti visas jam pavestas užduotis. Auditoriai turėtų kelti savo profesinę kompetenciją nuolat dalyvaudami profesinio tobulinimosi programose.

76. Pagal 5100-ąjį GUID IT audito grupės nariai kartu turėtų gebėti:

- ✓ suprasti IS techninius aspektus (pvz., duomenų bazės konfigūracijas, duomenų perdavimo tinklo topologiją, ugniasienes, IDS/IPS sistemas[21], programinės įrangos pažeidžiamumus, atnaujinimus, licencijavimą, prieigos kontrolės sistemas, atsarginių kopijų sistemas, kt.), visas atitinkamas programų versijas, aktualias atliekant auditą (pvz., yra audituojama IS, kuri veikia skirtingose rinkose (Europoje, Azijoje, JAV), auditorius turi suprasti skirtingas šios IS versijas, kurios pritaikytos atitinkamoms rinkoms);
- ✓ taikyti galiojančias taisykles, nuostatus ir pažinti aplinką, kurioje veikia audituojamo subjekto IT grindžiamos informacinės sistemos;
- ✓ susieti veiklos procesus su audituojamo subjekto informacinės sistemos programavimo logika;
- ✓ naudoti tiek verslo, tiek IT žinias, kad būtų galima įvertinti riziką, jog galimai rankiniu būdu galėjo būti pakeista taikomoji programa ar jos konfigūracija taip, kad būtų galima išimtinai apdoroti sandorius (t. y., neįprastai ar ne pagal standartines taisykles);
- ✓ įvertinti taikomosios kontrolės priemonių atitinkamose informacinėse sistemose kūrimą ir išbandyti jų veikimo efektyvumą;
- ✓ taikyti audito metodiką, įskaitant AAI taikomus atitinkamus audito standartus ir gaires;

[21] IDS (angl. *Intrusion Detection System*) ir IPS (angl. *Intrusion Prevention System*) yra tinklo saugumo sistemos, skirtos aptikti ir reaguoti į kenkėjišką veiklą tinkle.

- ✓ taikyti IT veiklos ir (arba) atitikties kriterijus, su kuriais turi būti lyginami audito pastebėjimai, įskaitant IS valdymo sistemas, pvz., COBIT, ITIL[22], TOGAF[23];
- ✓ taikyti IT audito metodus (technikas), skirtus audito įrodymams iš automatizuotų sistemų rinkti;
- ✓ suprasti ir taikyti CAAT, skirtas rinkti audito įrodymus, juos analizuoti ir atkartoti tokios analizės rezultatus arba pakartotinai atlikti audito procedūras;
- ✓ prisijungti prie IS infrastruktūros ir ją naudoti audito įrodymams rinkti ir saugoti.

77. Audito metu gali kilti sudėtingų ir (ar) ginčytinų klausimų, reikalaujančių kompetencijos ir patirties, kurių IT audito grupė neturi. Tai gali būti klausimai, susiję su konkrečia audito sritimi (pvz., IS pažeidžiamumo ir kiti technologiniai klausimai), teisine, metodine ar kt. kompetencijomis. Prireikus pagalbos, galima kreiptis į teisės, informacinių technologijų, metodologijos ar kitų struktūrinių padalinių darbuotojus arba pasitelkti išorės specialistus (ekspertus) ir (ar) auditorius, kurie pasidalintų specialiomis žiniomis, atliktų konkrečias užduotis ar suteiktų kitą reikiamą pagalbą.

78. Valstybės kontrolės struktūrinių padalinių darbuotojai, išorės specialistai (ekspertai) ir (ar) išorės auditoriai pasitelkiami vadovaujantis *Valstybės kontrolės metinės veiklos planavimo tvarkos aprašu*.

79. Visi auditoriaus sprendimai dėl išorės specialisto (eksperto) ir (ar) išorės auditoriaus darbo pasitelkimo, jų darbo įvertinimo ir panaudojimo turi būti dokumentuoti. Išsamiau apie išorės auditorių ir (ar) išorės specialistų (ekspertų) pasitelkimo planavimą ir jų atlikto darbo panaudojimą žr. Metodikos svetainės Tvarkų ir kitos informacijos skiltyje.

80. Išsamesnė informacija apie auditoriaus profesines kompetencijas ir joms keliamus reikalavimus pateikta 150-ajame TAAIS „*Auditoriaus kompetencija*“, 1950-osiose GUID „*Auditorių kompetencijų sistemos kūrimo gairės*“ ir 1951-osiose GUID „*Auditorių profesinio tobulėjimo kelių kūrimo gairės*“.

81. Būdamas kūrybingas, lankstus ir išradingas auditorius lengviau pastebės galimybes plėtoti naujoviškus informacijos rinkimo ir vertinimo metodus. Skirtinguose audito proceso etapuose galimi skirtingi naujovių diegimo galimybių lygmenys. Didžiausią galimybę diegti naujoves auditorius gali turėti planavimo stadijoje, kol vis dar sprendžia, kokius metodus ir technikas taikyti būtų geriausia. Auditorius taip pat turėtų mokytis iš kitų auditorių ir būti atviras pokyčiams.

---

[22] ITIL (angl. *Information Technology Infrastructure Library*) yra rinkinys geriausių praktikų skirtas IT paslaugų valdymui (ITSM). Jis aprašo procesus, procedūras, užduotis ir patikrinimus, kurie gali būti pritaikyti siekiant užtikrinti efektyvų ir kokybišką IT paslaugų teikimą.

[23] TOGAF (angl. *The Open Group Architecture Framework*) yra standartas ir metodologija, skirta įmonių architektūros kūrimui ir valdymui. Jis buvo sukurtas organizacijos „The Open Group“ ir yra plačiai naudojamas visame pasaulyje įmonių architektūros projektavime ir įgyvendinime.

3. VEIKSMAI IKI AUDITO

Susiję TAAIS reikalavimai
Auditorius privalo pasirinkti audito temas AAI strateginio planavimo metu analizuodamas potencialias temas ir atlikdamas tyrimus, kad galėtų nustatyti rizikas ir problemas. (*3000-ojo TAAIS 89 punktas*) Auditorius privalo pasirinkti audito temas, kurios yra reikšmingos, gali būti audituojamos ir atitinka AAI įgaliojimus. (*3000-ojo TAAIS 90 punktas*) Auditorius privalo pasirinkti audito temas, siekdamas kuo didesnio audito poveikio ir atsižvelgdamas į esamus pajėgumus. *(3000-ojo TAAIS 91 punktas)* Jeigu AAI turi teisę savo nuožiūra parinkti atitikties audito aprėptį, auditorius privalo nustatyti audito sritį, kuri bus įvertinta arba vertinama pagal kriterijus. *(4000-ojo TAAIS 107 punktas)* Jeigu AAI turi teisę savo nuožiūra parinkti atitikties auditų apimtį, auditorius privalo identifikuoti atitinkamus audito kriterijus prieš atlikdamas auditą, kad būtų sudarytas pagrindas išvadai ar nuomonei dėl audito srities parengti. *(4000-ojo TAAIS 110 punktas)* Auditorius privalo aiškiai identifikuoti numatomą (-us) naudotoją (-us) ir atsakingąją šalį bei atsižvelgti į jų vaidmenų poveikį, kad galėtų atlikti auditą ir atitinkamai bendrauti. *(4000-ojo TAAIS 101 punktas)*

82. Už strateginio tyrimo atlikimą yra atsakingas Valstybės kontrolės Planavimo ir poveikio departamentas. Valstybiniai auditai institucijos lygmeniu planuojami ir atrenkami vadovaujantis *Valstybės kontrolės metinės veiklos planavimo tvarkos aprašu*.

4. IT AUDITO PROCESAS

83. IT audito procesą sudaro šie pagrindiniai etapai (3 pav.):

- ✓ audito planavimas: audito inicijavimas, išankstinis tyrimas ir audito plano parengimas;
- ✓ pagrindinis tyrimas;
- ✓ audito ataskaitos arba išankstinio tyrimo ataskaitos parengimas.

4 pav. IT audito proceso etapai

Inicijuojamas auditas ir pradedamas išankstinis tyrimas; renkama ir vertinama informacija apie IT kontrolės priemones ir organizacijos veiklą, identifikuojamos IT kontrolės rizikos, parengiamas išankstinio tyrimo rezultatų apibendrinimas ir, nusprendus atlikti pagrindinį tyrimą, parengiamas audito planas.

Atliekamos audito procedūros pagal audito plane numatytus audito klausimus ir kriterijus; siekiant audito tikslo, surenkami pakankami ir tinkami audito įrodymai, parengiama audito rezultatų suvestinė.

Parengiamas audito ataskaitos arba išankstinio tyrimo ataskaitos projektas (kai auditas užbaigiamas išankstiniu tyrimu); suderinus projektą su audituojamu (-ais) subjektu (-ais) ir pagal poreikį kitomis institucijomis, parengiama galutinė ataskaita ir numatomi naudotojai informuojami apie atlikto audito rezultatus, audito padarytas išvadas ir pateiktas rekomendacijas bei laukiamą audito poveikį.

84. IT audito proceso etapai ir reikalavimai išsamiau aprašyti tolesnėse Vadovo dalyse.

4.1. Audito planavimas

85. Išankstinio tyrimo tikslas – surinkti ir įvertinti informaciją apie nagrinėjamą veiklos ir IT sritį, nustatyti IT kontrolės priemonių rizikas, apsispręsti, ar tikslinga atlikti pagrindinį tyrimą.

86. Tinkamas planavimas padeda užtikrinti, kad:

- ✓ bus įvardytos aktualios ir svarbios IT kontrolės (bendrosios ir (ar) taikomųjų programų) priemonių rizikos, kurios toliau bus vertinamos pagrindinio tyrimo metu;

- ✓ audito ištekliai (finansiniai, žmogiškieji, materialiniai ir kiti) bus paskirstyti atsižvelgiant į riziką;
- ✓ auditas bus tinkamai organizuotas ir valdomas.

87. Išankstinio tyrimo metu pagrindinis dėmesys skiriamas susipažinti su audituojamo (-ų) subjekto (-ų) veikla ir IT aplinka, susijusia su audito objektu, atnaujinti arba patikslinti strateginio tyrimo metu identifikuotas ar nustatyti naujas galimas problemas ir ar) rizikas, išsiaiškinti, ar bus galima jas audituoti (plačiau apie tai šio skirsnio tolesniuose skyreliuose). Išankstinio tyrimo apimtis priklauso nuo auditoriaus žinių apie audituojamą subjektą ir objektą.

88. Planavimo procesą sudaro šie pagrindiniai etapai:
    - ✓ inicijuojamas auditas;
    - ✓ audituojamas subjektas oficialiu raštu informuojamas apie pradedamą auditą;
    - ✓ parengiamas išankstinio tyrimo planas;
    - ✓ surenkama informacija ir susipažįstama su audituojama sritimi, audituojamo subjekto vykdoma veikla, IT valdymu (IT kontrolėmis, ištekliais) ir kitais aktualiais klausimais;
    - ✓ atliekamas IT bendrosios ir (ar) taikomųjų programų kontrolės priemonių įvertinimas, siekiant nustatyti rizikas (įgimta, IT kontrolės, neaptikimo rizika) ir įvertinti rizikos lygį;
    - ✓ nustatomas reikšmingumas kiekybiniu ir (ar) kokybiniu atžvilgiu;
    - ✓ atrenkami galimi IT kontrolės priemonių trūkumai (pažeidžiamumai) audituojamojo aplinkoje ir nustatomos audituotinos sritys, esant poreikiui ir turint visus reikiamus duomenis atliekama vienetų, kurie bus detaliai testuojami (pvz.: IT projektai, incidentai, pakeitimai, paslaugos), atranka. Išankstinio tyrimo rezultatai pateikiami išankstinio tyrimo rezultatų apibendrinimo dokumente;
    - ✓ rengiamas audito planas, kuriame nurodomi audito objektas, tikslas, apimtis, apribojimai, audito klausimai, kriterijai, procedūros, metodai, suplanuojami audito ištekliai ir darbų terminai;
    - ✓ su audituojamu subjektu aptariami išankstinio tyrimo rezultatai, audito kriterijai ir kita informacija;
    - ✓ audito planas tvirtinamas ir audito subjektas informuojamas apie planavimo rezultatus.

89. Išankstiniam tyrimui kartu su audito plano parengimu paprastai skiriama apie 30 proc. viso auditui skirto laiko. Didžiąją dalį šio laiko reikėtų panaudoti pagrindiniam tyrimui.

90. Išankstinio tyrimo etapas baigiamas parengus išankstinio tyrimo rezultatų apibendrinimą. Jeigu nusprendžiama atlikti pagrindinį tyrimą, rengiamas audito planas. Jeigu nusprendžiama jo neatlikti, auditas baigiamas išankstinio tyrimo ataskaita (išsamiau žr. Vadovo 4.3 poskyryje).

4.1.1. Audito inicijavimas

91. Audito tikslui, vizijai, lūkesčiams ir ištekliams aptarti iki audito inicijavimo audito departamento vadovas organizuoja susitikimą su Valstybės kontrolės vadovybe. Susitikime strateginį tyrimą atlikusio departamento darbuotojas pristato audito temą ir tikslą. Taip pat sutariama, ar valstybės kontrolierius ir (ar) valstybės kontrolieriaus pavaduotojas, kuriam tiesiogiai pavaldus auditą atliekantis departamentas, planuoja dalyvauti susitikime su audituojamu subjektu pradedant auditą.

92. Inicijuojant auditą reikia įsitikinti, kad audito grupė turi reikiamų kompetencijų, įskaitant projekto valdymo žinių, kaip to reikalauja 5100-asis GUID, taip pat, kad auditui numatyti ištekliai yra pakankami.

93. Vipsis turi būti nurodyti (jeigu iki tol nebuvo nurodyti) su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis departamentas, suderinti audito objektas, tikslas, pagrindinis (-iai) audituojamas (-i) subjektas (-ai).

94. Auditas, kartu ir išankstinis tyrimas pradedamas ViPSIS patvirtinus audito pradžią. Detalesnė informacija, kaip inicijuoti ir dokumentuoti auditą ViPSIS, pateikiama *ViPSIS naudotojo vadovuose*.

95. Esant išskirtinėms aplinkybėms, auditas gali būti pradėtas be strateginio tyrimo (pvz., įtraukus į Valstybės kontrolės metinį veiklos planą Seimo nutarimu pavestą atlikti auditą) ir (ar) be išankstinio tyrimo, ir (ar) atliekant ne visos apimties išankstinį tyrimą (pvz., strateginio tyrimo metu identifikuotos faktais ir (ar) pavyzdžiais pagrįstos problemos (rizikos) ir nereikia rinkti papildomos informacijos ir kt.). Sprendimas neatlikti išankstinio tyrimo ar tam tikrų išankstinio tyrimo etapų turi būti suderintas su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis departamentas.

4.1.2. Informavimas apie audito pradžią

96. Audituojamas subjektas turi būti informuotas oficialiu raštu apie pradedamą auditą ne vėliau kaip per 2 savaites nuo jo pradžios (rašto šabloną galima rasti Metodikos svetainės Šablonų skiltyje). Informavimo tikslas – suteikti audituojamam subjektui pagrindinę informaciją apie numatomą auditą (objektą, tikslą, apimtį ir atlikimo terminą, grupės narių ir audituojamo subjekto atsakomybę) ir paaiškinti, ko iš jo tikimasi, siekiant, kad auditas vyktų sklandžiai (pvz., gali būti prašoma paskirti kontaktinius asmenis, pateikti svarbius duomenis ir pan.).

97. Pradėjus auditą, kuo anksčiau turi būti inicijuojamas susitikimas su audituojamojo subjekto vadovais. Susitikime turi dalyvauti audito grupės vadovas ir audito departamento vadovas. Jeigu lūkesčių aptarimo susitikime su vadovybe buvo taip sutarta, į pirmą susitikimą arba į atskirai organizuojamą susitikimą kviečiamas dalyvauti valstybės kontrolierius ir (ar) valstybės kontrolieriaus pavaduotojas, kuriam tiesiogiai pavaldus auditą atliekantis departamentas. Dalyvauti jame gali būti kviečiami visi audito grupės nariai.

98. Audituojamasis subjektas apie planuojamą pradėti auditą gali būti informuojamas iš anksto (ne anksčiau nei 4 savaitės iki audito pradžios, ir ne anksčiau negu įvyko lūkesčių aptarimas su vadovybe). Šį informavimo būdą rekomenduojame rinktis tada, kai yra naudinga iki audito pradžios su audituojamuoju subjektu susitarti dėl atsakingo asmens už bendradarbiavimą su auditoriais skyrimo, paprašyti, kad iki audito pradžios būtų paruošti auditui (išankstiniam tyrimui) reikalingi duomenys ir informacija, kurių parengimas gali

užtrukti dėl jų didelių apimčių ar pan., taip pat, jeigu reikia suderinti susitikimą su aukšto lygio audituojamojo subjekto vadovais, kurių darbotvarkė paprastai būna pakankamai užimta, ar kitų priežasčių. Siunčiamas tas pats raštas, kaip ir pradėjus auditą.

99. Audituojamas subjektas taip pat turi būti informuojamas oficialiu raštu ar el. paštu, jeigu išankstinio tyrimo metu pasikeitė audito grupės nariai ar kita reikšminga informacija (pvz.: audito atlikimo terminas, apimtis, numatytas laikinas audito sustabdymas ir kt.).

4.1.3. Išankstinio tyrimo plano parengimas

Susiję TAAIS reikalavimai
Auditoriai privalo planuoti auditą taip, kad jis būtų kokybiškas, atliktas ekonomiškai, efektyviai, rezultatyviai ir laiku, laikantis gero projektų valdymo principų. (*3000-ojo TAAIS 96 punktas*) Auditorius privalo parengti ir dokumentuoti audito strategiją ir audito planą, kurie kartu apibūdintų, kaip bus atliekamas auditas siekiant parengti atitinkamomis aplinkybėmis tinkamas ataskaitas, reikalingus išteklius ir audito darbo tvarkaraštį. *(4000-ojo TAAIS 137 punktas)*

100. Pradėjus išankstinį tyrimą ne vėliau kaip per 2 savaites parengiamas išankstinio tyrimo planas (šabloną galima rasti Metodikos svetainės Šablonų skiltyje). Šio plano tikslas – suplanuoti reikiamus darbus, jų atlikimo terminus, audito kokybės užtikrinimo procedūras audito planavimo metu, išteklius ir kt. Jame nurodoma:

- ✓ *Santrumpos ir sąvokos*. Pateikiamos išankstinio tyrimo plane vartojamos santrumpos ir sąvokų paaiškinimai (išnašose nurodant sąvokų paaiškinimo šaltinius).
- ✓ *Pagrindinė informacija apie auditą*: audito ID, audito objektas, audituojamas (-i) subjektas (-ai) ir audituojamas laikotarpis, apribojimai, vidinę peržiūrą atliekantis asmuo.
- ✓ *Išankstinio tyrimo metu planuojamos atlikti procedūros*: konkrečios procedūros aprašymas, ją atliekantis asmuo, užduoties (procedūros) atlikimo pradžios ir pabaigos terminai, pateikimo vidinei peržiūrai terminas, planuojamas darbo dienų skaičius. Jeigu vidinę peržiūrą atlieka ne tik audito grupės vadovas, bet ir srities vadovas (-ai), ją atliekantis asmuo nurodomas prie atitinkamos procedūros.
- ✓ *Išankstinio tyrimo rezultatų apibendrinimo ir audito plano rengimo grafikas:* numatomi darbai, darbo pradžios ir pabaigos terminai, atsakingas asmuo.
- ✓ *Planuojami ištekliai:*
  - kiekvieno audito grupės nario planuojamas darbo dienų skaičius;
  - kitos išlaidos – nurodomas išlaidų pavadinimas (pvz., komandiruotės, išorės specialistų (ekspertų) pasitelkimo), trumpas aprašymas ir preliminari suma. Planuojant komandiruotes, ekspertų pasitelkimą arba kitas auditui reikalingas išlaidas, turi būti vadovaujamasi *Valstybės*

kontrolės metinės veiklos planavimo tvarkos apraše ir kituose atitinkamuose teisės aktuose numatytais reikalavimais.

- ✓ *Kita reikšminga informacija.*

101. Už išankstinio tyrimo plano parengimą yra atsakingas audito grupės vadovas. Rengiant šį planą pagal poreikį dalyvauja ir kiti audito grupės nariai. Išsamiau audito grupės narių atsakomybė ir veiksmai rengiant šį planą aprašyti *Valstybinių auditų kokybės užtikrinimo vadove.*

102. Paaiškėjus naujoms aplinkybėms (pvz. įtraukiamas naujas audituojamas subjektas, kuris nebuvo identifikuotas audito pradžioje), dėl kurių reikalingos papildomos išankstinio tyrimo plane nenumatytos procedūros, išankstinio tyrimo planas turi būti patikslintas ir nurodyta tikslinimo priežastis.

4.1.4. Susipažinimas su audituojama sritimi

Susiję TAAIS reikalavimai
Planavimo etape auditorius privalo įgyti faktinių ir metodinių žinių. *(3000-ojo TAAIS 98 punktas)* Auditorius privalo suprasti audituojamą subjektą ir jo aplinką, įskaitant subjekto vidaus kontrolę, kad galėtų veiksmingai planuoti ir vykdyti auditą. *(4000-ojo TAAIS 131 punktas)*

103. Siekiant, kad auditas būtų tinkamai suplanuotas, auditorius turi įgyti pakankamai žinių apie audituojamą sritį, audituojamo (-ų) subjekto (-ų) veiklą ir IT valdymą, tarp jų ir IT bendrąsias kontroles, ir turimus IT išteklius. IT auditas gali apimti vieną organizaciją arba sistemą, į kurią patenka įvairūs vykdomosios valdžios lygiai ar subjektai. Tokiais atvejais, kai IT auditas apima daugiau nei vieną subjektą, auditoriai turi gauti supratimą apie visus subjektus, kurių veikla patenka į audito objektą.

104. Iki išankstinio tyrimo arba jo pradžioje (ne vėliau kaip per dvi savaites nuo audito inicijavimo) audito grupė su atsakingu Valstybės kontrolės Planavimo ir poveikio departamento darbuotoju inicijuoja susitikimą, kuriame šis pristato ir supažindina su visa strateginio tyrimo metu surinkta ir, esant poreikiui, iki audito inicijavimo atnaujinta medžiaga, susijusia su konkrečiu auditu, įskaitant laukiamą audito poveikį, laukiamus pokyčius ir jų vertinimo rodiklius (jeigu jie buvo nurodyti atliekant strateginį tyrimą ir rengiant pasiūlymus institucijos metiniam veiklos planui sudaryti).

105. Siekdamas susipažinti su audituojama sritimi, audituojamu subjektu ir jo aplinka, auditorius turi suprasti:

- ✓ kokie yra organizacijos tikslai ir kaip veikia veiklos procesai;
- ✓ kaip organizuotas IT valdymas, turimi IT ištekliai ir kokie yra IT tikslai.

106. Susipažįstant su audituojamo subjekto atliekama veikla, paprastai analizuojama:

- ✓ kokie teisės aktai reglamentuoja audituojamo (-ų) subjekto (-ų) veiklą ir audito objektą, koks jų turinys;

- ✓ kokia audituojamo (-ų) subjekto (-ų) organizacinė struktūra ir pavaldumo ryšiai, valdymo procesai, už audituojamą veiklą atsakingi darbuotojai;
- ✓ kokie audituojamam subjektui bendrai ir konkrečiai audituojamai veiklai skiriami ištekliai (įskaitant finansinius, žmogiškuosius, materialinius ir IT išteklius bei su jais susijusius valdymo procesus); koks yra planuojamos audituoti subjekto (-ų) veiklos pobūdis (objekto svarba, sąsajos su strateginiais šalies dokumentais, subjekto vieta valstybės hierarchinėje struktūroje, vykstantys procesai, plėtros tendencijos ir kt.);
- ✓ koks yra planuojamos audituoti veiklos pobūdis (objekto svarba, sąsajos su strateginiais šalies dokumentais, subjekto vieta valstybės hierarchinėje struktūroje, vykstantys procesai, plėtros tendencijos ir kt.);
- ✓ kokias programas, priemones, susijusias su audito objektu, vykdo audituojamas (-i) subjektas (-ai), kokie jų rezultatai;
- ✓ kokie numatomi audito rezultatų naudotojai, kokia vidaus ir išorės aplinka (suinteresuotos organizacijos, produktų (paslaugų) gavėjai ir kt.) veikia audituojamą (-us) subjektą (-us);
- ✓ kokie šioje srityje atliktų auditų ar tyrimų rezultatai;
- ✓ kitus, auditoriaus nuomone, svarbius dalykus.

107. Susipažįstant su audituojamo subjekto IT valdymu, gali būti analizuojama:

- ✓ kokia yra IT valdymo politika, IT strateginiai tikslai, uždaviniai, priemonės, rezultatai;
- ✓ kaip IT procesai ir IT tikslai susiję su organizacijos veiklos procesais ir tikslais;
- ✓ kokie teisės aktų reikalavimai, susiję su IT, taikomi organizacijai;
- ✓ koks IT biudžetas, kokia jo struktūra;
- ✓ kokie IT projektai įgyvendinami ar planuojami įgyvendinti, kokie jų tikslai ir rezultatai;
- ✓ kokios yra IT bendros kontrolės priemonės, kokie IT procesai yra organizacijoje ir kaip jie įgyvendinami;
- ✓ kokią administravimui ir kritinėms veiklos funkcijoms skirtą programinę, techninę įrangą valdo, tvarko organizacija, koks IS sudėtingumas, subjekto priklausomybė nuo programų;
- ✓ koks programinės ir techninės įrangos gyvavimo ciklas (pvz., programinė įranga tik kūrimo stadijoje, ar ji jau skurta ir naudojama arba anuliuojama);
- ✓ kokie funkciniai ir nefunkciniai reikalavimai taikomi IS, kokios kontrolės priemonės (funkcionalumai) įdiegtos taikomosiose programose ir koks jų tikslas (pagal poreikį, pvz., jei audito objektas yra taikomoji programa)[24];

[24] Tokią informaciją galima rasti IS bendrojoje techninėje dokumentacijoje ir funkcijų (plėtinių) detaliuosiuose techniniuose specifikacijose (dokumentuose).

- ✓ kokie duomenys tvarkomi organizacijoje ir kiek yra jautrių, kritinių duomenų, kokie saugumo standartai, priemonės taikomos organizacijoje siekiant užtikrinti šių duomenų konfidencialumą, vientisumą ir prieinamumą;
- ✓ kokia organizacijos ir IT architektūra (duomenų, taikomųjų programų, infrastruktūros), kokios IS tvarkomos ir valdomos;
- ✓ kokia IS kūrimo aplinka, audituojamo subjekto pasirinkti IS įsigijimo arba kūrimo būdai, mastas, technologijos, įsigijimo arba kūrimo tikslai, IS naudojimo būdai;
- ✓ kokia IT organizacinė struktūra, kokie vidiniai žmogiškieji ištekliai skirti IT funkcijai organizacijoje, kokios IT funkcijos ir atsakomybės, kaip jos paskirstytos IT sistemoje;
- ✓ kokie išorės ištekliai (angl. *outsourcing*) ir kiek jų dalyvauja įgyvendinant tam tikras IT funkcijas, projektus;
- ✓ kokios yra IT rizikos, kurias organizacija nustato, kaip šios rizikos valdomos, koks yra IT rizikos apetitas ir rizikos pajėgumai;
- ✓ kokie nustatyti IT veiklos rezultatus matuojantys rodikliai (angl. *KPI*), kokie yra šių rodiklių rezultatai;
- ✓ kokios kontrolės priemonės įdiegtos taikomosiose programose ir koks jų tikslas;
- ✓ koks yra incidentų, pakeitimų, problemų mastas, jų išsprendimo dinamika;
- ✓ kiek ir kokie vidiniai ir išorės IT auditai, savianalizė (angl. *control self-assessment*) ir kiti vertinimai IT srityje organizacijoje atliekami, kokie jų rezultatai, ar pašalinti nustatyti pažeidimai, ištaisytos klaidos ir laiku įgyvendintos rekomendacijos;
- ✓ kiti auditoriaus nuomone svarbus dalykai.

108. Išankstinio tyrimo metu, siekiant susipažinti su organizacijos IT bendrosios kontrolės priemonėmis ir nustatyti rizikingas sritis, rekomenduojama naudoti pavyzdinį klausimyno šabloną „Klausimynas IT bendrosios kontrolės vertinimui atlikti“ (šabloną galima rasti Metodikos svetainės Šablonų skiltyje). Jis pildomas viso audito metu, t. y. pradedamas pildyti planavimo etape ir baigiamas pagrindinio tyrimo metu. Išankstinio tyrimo metu rekomenduojama susipažinti su visomis klausimyne nurodytomis IT bendrosios kontrolės priemonėmis (pagal COBIT IT proceso bazinės praktikos), kurios veikia organizacijoje. Pagrindinio tyrimo metu klausimynas toliau pildomas tik ta dalimi, kuriai audito plane suplanuotos atlikti audito procedūros.

109. Minėtame klausimyne pagal kiekvieną IT procesą (kuris paprastai suprantamas kaip IT bendrosios kontrolės priemonė) pateikta:

- ✓ instrukcijos išankstiniam tyrimui, siekiant susipažinti su organizacijos IT valdymu;
- ✓ klausimai skirti išankstiniam tyrimui, siekiant nustatyti galimas IT bendrosios kontrolės priemonių rizikas (žaliai pažymėti klausimyno langeliai);

- ✓ klausimai skirti pagrindiniam tyrimui, siekiant įvertinti kontrolės priemonių tinkamumą ir patikimumą, kurie sudaryti atsižvelgiant į COBIT5 metodikoje pateikiamas IT procesų bazines praktikas (angl. *Base Practices*) ir su tuo susijusiomis veiklomis (angl. *Activities*). Kai kuriais atvejais klausimai detalizuoti atsižvelgiant į teisės aktų reikalavimus, ISO standartuose ir ITIL praktikos vadovuose pateiktas IT kontrolės priemonių praktikos nuostatas;
- ✓ rekomendacijos pagal kiekvieną klausimą kokias audito procedūras galima atlikti ir kokie galimi informacijos šaltiniai.

110. Kadangi IT srityje vykstantys procesai sparčiai keičiasi ir tai gali turėti įtakos audito planavimui, analizuojant IT audito objektą ir aplinką, auditoriui taip pat svarbu suprasti, kokie esminiai pasikeitimai vyksta audito metu ir ar planuojama atlikti pokyčius nagrinėjamoje srityje. Tai, kokios apimties susipažinimas su audituota sritimi turi būti atliktas, yra auditoriaus profesinis sprendimas, bet turi būti atsižvelgta į audito tikslą, turimus išteklius ir suplanuotą audito laiką.

111. Susipažinimo metu auditorius taip pat turi suprasti tai, kokios taikomosios programos, susijusios su audito objektu, yra įdiegtos organizacijos IS ir kaip jos veikia, kaip vyksta informacijos apdorojimo ir perdavimo procesas IS, kokios yra taikomosios programos kontrolės (įvesties, proceso ir išvesties) priemonės. Susipažįstant su IS rekomenduojama atlikti šių programų nuoseklią peržiūrą – nuo duomenų suvedimo iki rezultato gavimo. Kiek tokių stebėjimų reikia atlikti – yra auditoriaus profesinis sprendimas, priklausomai nuo organizacijos naudojamos infrastuktūros sudėtingumo, realizuotų funkcinių reikalavimų gausos. Informacija apie organizacijos IS, auditui aktualias taikomąsias programas fiksuojama IS suvestinėje. Apie taikomųjų programų kontrolės priemonių vertinimą išsamiau žr. Vadovo 5 priede.

Informacijos ir duomenų šaltiniai bei jų rinkimo būdai

112. Informacija ir duomenys audito planavimo metu renkama nagrinėjant įvairius rašytinius ir skaitmeninius šaltinius (audituojamo subjekto ir kitų institucijų parengtus dokumentus, duomenų bazėse esančius duomenis), bendraujant su audituojamo subjekto ar kitų institucijų atstovais, apklausiant produktų (paslaugų) gavėjus, kitus suinteresuotus asmenis ir tos srities ekspertus. Auditorius gali pasirinkti ir kitus, jo manymu, tinkamus informacijos ir duomenų rinkimo būdus. Apie duomenų rinkimo metodus išsamiau pateikta Metodikos svetainės Audito metodų skiltyje. Renkant informaciją gali būti naudojami šie (ar kiekvienu konkrečiu atveju auditoriaus nuožiūra kiti, tinkantys pagal aplinkybes) informacijos ir duomenų šaltiniai:

- ✓ teisės aktai ir kiti dokumentai, reglamentuojantys audituojamo objekto ir subjekto veiklą (įstatymai, nutarimai, taisyklės, įstatai, nuostatai ir kt.);
- ✓ audituojamo subjekto veiklos planavimo ir atsiskaitymo už veiklos rezultatus dokumentai (strateginiai, metiniai veiklos planai, programos, veiklos ataskaitos ir kt.), audituojamo subjekto pranešimai spaudai;
- ✓ audituojamo subjekto vidaus dokumentai (finansinė atskaitomybė, vidaus audito ataskaitos, sprendimai, procedūrų tvarkos aprašai, komitetų protokolai ir kt.);
- ✓ audituojamo subjekto su IT susiję dokumentai (IS nuostatai, specifikacijos, IT padalinių nuostatai ir pareigybių aprašymai, IT standartai, procedūros, tvarkos,

sutartys su tiekėjais, IT projektų ataskaitos ir kt. su IT susijusi organizacinė ir techninė dokumentacija);

- ✓ audituojamo subjekto ar kitų susijusių šalių duomenų bazėse, saugikliuose ar duomenų ežeruose saugomi duomenys (valstybės duomenų valdymo IS duomenų ežeras, atvirų duomenų portalai, valstybės ir žinybinių registrų duomenų bazės, vidinės IS, kt.);
- ✓ audituojamo subjekto veiklą prižiūrinčių ar kontroliuojančių ir jam pavaldžių institucijų informacija, susijusi su nagrinėjama sritimi;
- ✓ kitų (Lietuvos ir užsienio šalių) institucijų atlikti auditai (ir valstybiniai auditai), tyrimai, vertinimai, apklausos, ekspertų išvados, konferencijų medžiaga ir kt.;
- ✓ oficialūs ir audituojamo subjekto turimi statistiniai duomenys;
- ✓ žodžiu ar raštu audituojamo subjekto darbuotojų, ekspertų, kitų suinteresuotų šalių atstovų pateikta informacija.

113. Auditorius gali pasirinkti ir kitus, jo profesiniu sprendimu, tinkamus informacijos ir duomenų šaltinius. Auditorius gali pasirinkti ir kitus, jo manymu, tinkamus informacijos ir duomenų rinkimo būdus. Reikalingų žinių įgijimas yra nuolatinis informacijos rinkimo ir vertinimo visuose audito etapuose procesas. Svarbu, kad auditorius palygintų informacijos gavimo išlaidas ir pridėtinę vertę, kurią auditui suteikia ši informacija.

114. Siekiant surinkti visą reikiamą informaciją pagal išankstinio tyrimo plane numatytus klausimus, rekomenduojama pagal kiekvieną klausimą parengti išsamų reikiamų šaltinių sąrašą ir subjektus, kurie reikiamus duomenis arba informaciją valdo ar gali valdyti (pavyzdinis dokumentų sąrašas pateikiamas Vadovo 1 priede). Šis reikiamos informacijos sąvadas turėtų būti aptartas su atitinkamu subjektu, kuris valdo ar gali valdyti reikiamą informaciją, dėl galimybės ją gauti, aptariant galimus apribojimus dėl informacijos turinio ar jos gavimo, duomenų pateikimo terminus, prieigos prie duomenų būdus ir kitus svarbius klausimus, kurie gali būti susiję su prašoma informacija. Toks aptarimas leis subjektui aiškiau suprasti kokio turinio duomenis jis turi pateikti auditoriams, kokiais formatais ir kada.

115. Planavimo etape surinktą informaciją gali reikėti patikslinti pagrindinio tyrimo metu, nes reikalingų žinių įgijimas yra nuolatinis informacijos ir duomenų rinkimo ir vertinimo visuose audito etapuose procesas. Išankstinio tyrimo metu taip pat svarbu patikrinti, ar reikalinga informacija ir duomenys yra prieinami ir patikimi, išbandyti įvairius informacijos ir duomenų rinkimo ir vertinimo metodus.

116. Jeigu išankstinio tyrimo metu nustatomi nauji duomenų šaltiniai, gaunama papildomos informacijos, kuri gali būti naudinga laukiamiems audito pokyčiams vertinti, pasikeitus situacijai ar esant kitoms aplinkybėms, laukiamas audito poveikis, pokyčiai ir juos parodantys rodikliai, kurie buvo nurodyti atliekant strateginį tyrimą ir rengiant pasiūlymus institucijos metiniam veiklos planui sudaryti, turi būti aktualizuojami audito plane. Išsamiau valstybinio audito poveikio vertinimo procesą reglamentuoja *Valstybinio audito poveikio vertinimo metodika*.

Auditui aktualių duomenų gavimas ir jų kokybės analizė

117. Audito planavimo metu turi būti atlikta duomenų ir jų šaltinių analizė:

- ✓ *Duomenų šaltinių identifikavimas*. Nustatomi visi galimi duomenų šaltiniai, kurie gali būti susiję su audito objektu (pvz.: atvirų duomenų portalai, audituojamų subjektų valdomos ir (ar) tvarkomos informacinės sistemos[25], jų duomenų bazės, valstybės duomenų valdysenos informacinė sistema ir pan.).

- ✓ *Duomenų struktūros ir savybių supratimas*. Nagrinėjama aktualių duomenų struktūra (stulpelių atributai, duomenų tipai ir kt. savybės) ir kokie duomenys kaupiami. Tai padeda suprasti, kaip duomenys organizuoti ir kaip juos galima panaudoti audite.

- ✓ *Duomenų ryšių tarp skirtingų šaltinių identifikavimas*. Susipažįstama su duomenų ryšiais tarp skirtingų duomenų šaltinių (toje pačioje ar skirtingose organizacijose). Tai padeda suvokti, kaip skirtingi duomenų elementai yra susiję ir kaip galima išnaudoti šiuos ryšius duomenų analitikai.

- ✓ *Duomenų panaudojimo galimybių analizė*. Įvertinama, kokios analitinės procedūros galėtų būti atliktos siekiant audito tikslo. Vertinama, kas galėtų atlikti analitines procedūras (auditorius, kitų VK struktūrinių padalinių darbuotojai, išorės specialistai (ekspertai)), ar reikėtų panaudoti specializuotus analitinius įrankius.

- ✓ *Duomenų prieinamumo vertinimas*. Nustačius, kad vienos ar kelių sistemų duomenys bus naudojami audite, vertinamos prieigos prie duomenų galimybės ir galimi prieigos apribojimai.

118. Jeigu duomenų analizės pagrįstai neįmanoma atlikti išankstinio tyrimo metu (pvz., audituojamas subjektas laiku nepateikė duomenų), priežastys pateikiamos išankstinio tyrimo darbo dokumentuose ir šios procedūros suplanuojamos audito plane.

119. Atlikus duomenų paiešką ir analizę bei turint preliminarų auditui reikiamų duomenų sąrašą, esant poreikiui, su duomenis valdančiais subjektais aptariama, ar jie turės galimybę auditoriams pateikti norimos apimties, formato, aktualumo duomenų rinkinius. Jei yra galimybė, duomenų analizei atlikti turi būti renkami pirminiai duomenys, kurie nėra apibendrinti ar kitaip agreguoti (išskyrus, kai audito poreikiams reikalingi tokie duomenys).

120. Nusprendus naudoti informacinių išteklių (IS, registrų, jų duomenų bazėse kaupiamus) duomenis kaip audito įrodymus, turi būti įvertinta, ar audituojamo subjekto duomenų kokybės užtikrinimo kontrolės priemonių sistema yra patikima ir sudaro sąlygas pasitikėti jo pateiktais duomenimis. Šis vertinimas atliekamas pildant *Duomenų kokybės kontrolės priemonių tikrinimo klausimyną* (šabloną galima rasti Metodikos svetainės Šablonų skiltyje). Užpildęs jį, auditorius priima profesinį sprendimą, ar galima pasitikėti duomenimis ir juos naudoti kaip audito įrodymus. Kai duomenimis pasitikėti negalima, bet kitų auditui reikiamų duomenų nėra, auditorius priima profesinį sprendimą dėl audito klausimų, kriterijų ir (ar) procedūrų tikslinimo, keitimo arba atsisakymo.

121. Jeigu audito grupėje nėra reikiamų kompetencijų šiam vertinimui atlikti, galima pasitelkti kitų Valstybės kontrolės struktūrinių padalinių darbuotojus ar išorės specialistus (ekspertus). Toks profesinis sprendimas turi būti dokumentuojamas.

---

[25] Visa informacija apie viešojo sektoriaus įsteigtas valstybės informacines sistemas kaupiama www.registrai.lt.

122. Jeigu kito Valstybės kontrolės audito (veiklos, finansinio, atitikties ar IT) metu jau buvo atliktas tos pačios informacinės sistemos ir joje kaupiamų duomenų patikimumo vertinimas ir po šio vertinimo audituojamo subjekto informacinėje sistemoje neįvyko jokių esminių pasikeitimų (pvz., integracijos su kitomis sistemomis pokyčiai, pagrindinių taikomosios programos funkcijų atnaujinimas, kuris keičia duomenų apdorojimo tvarką ir tikrinimo algoritmus, ir pan.), ir audito grupės vertinimu atliktas darbas tinka jų audito tikslams pasiekti, audito grupė gali pasinaudoti atliktu duomenų patikimumo vertinimu. Jeigu nuo pastarojo tokio vertinimo praėjo 3 metai, rekomenduojama atlikti naują duomenų patikimumo vertinimą.

123. Auditorius, gavęs duomenų rinkinius iš duomenis valdančių subjektų, turi įvertinti:

- ✓ ar yra visi reikiami duomenys (pvz., nėra tuščių, praleistų laukų);
- ✓ ar jie yra visos apimties ir išsamūs (pvz., viso prašomo laikotarpio);
- ✓ ar jie yra aktualūs ir pateikiama naujausia informacija;
- ✓ ar jie atitinka turinio ir formato reikalavimus (pvz., viename stulpelyje nėra skirtingų duomenų; datos lauke yra įrašyta data, ne tekstas);
- ✓ ar duomenų rinkinyje pateikta informacija sutampa su duomenimis, surinktais iš kitų šaltinių (pvz., organizacijos svetainės, atvirų duomenų portalo, apklausos duomenys sutampa su subjekto pateiktaisiais) ir kt.

124. Duomenų rinkinių vertinimas atliekamas tiek išankstinio, tiek pagrindinio tyrimo metu.

125. Jei įvertinus pirmiau nurodytas aplinkybes nustatyta, kad duomenų rinkinys yra tinkamas, bet turi formatavimo ar kitokių trūkumų, auditorius prieš pradėdamas naudoti duomenis turėtų atlikti jų tvarkymo veiksmus (pvz., panaikinti tuščius, nereikalingus ar besidubliuojančius laukus, nustatyti tinkamus duomenų formatus (data, tekstas, skaičius), atskirti reikiamus duomenis į kelis stulpelius ir kt.). Kai duomenų rinkinys yra netinkamas ir auditorius pats negali atlikti tvarkymo veiksmų, auditorius prašo subjekto ištaisyti trūkumus ir pateikti duomenis pakartotinai.

126. Pagal 5100-ąjį GUID, jeigu iš duomenis valdančio subjekto gaunami duomenys iš IS duomenų bazės ar saugyklos, subjekto turi būti prašoma raštu pateikti:

- ✓ duomenų šaltinius su duomenų rinkinio sukūrimo laiko žyma, kad būtų užtikrintas jų vientisumas, autentiškumo patvirtinimas [26] ir negalėjimas atsisakyti atsakomybės[27];
- ✓ išgavimo parametrus, naudojamus duomenų rinkiniui sukurti (pvz., naudotos SQL (angl. *Structured Query Language*) užklausos tekstas), sukurtus automatizuotos ataskaitos parametrus arba kitus struktūruotų ar nestruktūruotų duomenų išgavimo parametrus.

127. Jeigu audituojamas subjektas atsisako pateikti duomenis, kuriuos Valstybės kontrolės žiniomis jis turi turėti savo IS, audito departamento vadovas ViPSIS fiksuoja audito riziką

---

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

[27] 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.

ir su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis departamentas, aptaria šios rizikos valdymo priemones.

4.1.5. IT kontrolės priemonių vertinimas rizikai nustatyti

128. Planavimo metu, susipažinus su audituojama sritimi, audituojamu subjektu ir jo aplinka ir siekiant identifikuoti IT bendrųjų ir (ar) taikomųjų kontrolės priemonių rizikas, IT auditoriai turėtų atlikti veikiančių IT kontrolės priemonių vertinimą, kad suprastų, ar gali būti tikri, jog esamos IT kontrolės priemonės neturi trūkumų (pažeidžiamumų), t. y. jos yra:

    - ✓ *patikimos,* kai praktikoje IT kontrolės priemonės tinkamai sukurtos ir įgyvendinamos taip, kaip numatyta organizacijos politikoje, standarte, tvarkoje, teisės akte, techninėje specifikacijoje ar kitose dokumentuose;
    - ✓ *pakankamos*, kai kontrolės priemonės sukurtos tokia apimtimi kurių pakanka, kad būtų sudarytos tinkamos sąlygos organizacijai, atsižvelgiant į jos veiklos specifiką ir mastą, siekti savo nustatytų tikslų.

129. Atsižvelgiant į IT audito tikslą, išankstinio tyrimo metu IT kontrolės priemonių vertinimas gali būti nukreiptas:

    - ✓ tik į IT bendrosios kontrolės priemonių vertinimą arba
    - ✓ į IT bendrosios kontrolės ir į tam tikrų taikomųjų programų, kurios aktualios auditui, kontrolės priemonių vertinimą.

130. Vertinimas turėtų apimti audituojamo subjekto politikos sritis, procesus, žmones ir sistemas. Atlikus preliminarų IT kontrolės vertinimą nustatomos rizikingos IT kontrolės sritys, kuriose galimai yra trūkumų (pažeidžiamumų). Informacija apie tai fiksuojama IT bendrosios kontrolės vertinimo klausimyne, pateikiamos nuorodos į dokumentus, kurie patvirtina nustatytas rizikas. Užpildytas klausimynas pridedamas prie darbo dokumento, kuriame pagal klausimyną turėtų būti agreguojama informacija taip, kad ją galima būtų toliau panaudoti rizikos vertinimo metu ir rengiant išankstinio tyrimo rezultatų apibendrinamąjį dokumentą. Kaip rengiami darbo dokumentai – išsamiau žr. Vadovo 2.5 poskyryje.

131. Jeigu kito Valstybės kontrolės audito (veiklos, finansinio, atitikties ar IT) metu jau buvo atliktas to paties audituojamo subjekto IT bendrosios kontrolės ir tų pačių taikomųjų programų, kurias planuojama vertinti, vertinimas, ir po jo audituojamo subjekto IT bendrojoje kontrolėje ir IS neįvyko jokių esminių pasikeitimų (pvz., įdiegta nauja prieigos kontrolės politika arba panaikinti esami kontrolės procesai, įvesta nauja IT valdymo struktūra, pakeista integracija su kitomis sistemomis, atnaujintos pagrindinės taikomosios programos funkcijos ir pan.), ir, audito grupės vertinimu, atliktas darbas tinka jų audito tikslams pasiekti, audito grupė gali pasinaudoti atliktu IT bendrosios kontrolės ir (ar) taikomosios programos kontrolės priemonių vertinimu. Tačiau, jeigu nuo pastarojo tokio vertinimo praėjo 3 metai, rekomenduojama atlikti naują vertinimą.

132. Auditorius gali priimti profesinį sprendimą išankstinio tyrimo metu pagal surinktą informaciją atlikti preliminarų IT procesų gebos vertinimą pagal COBIT metodiką. Gebos vertinimas leidžia auditoriams suprasti organizacijoje veikiančius IT procesus ir kokios kontrolės priemonės yra silpnos. Kaip atlikti šį vertinimą detaliai aprašyta ISACA knygose „Vertintojo vadovas naudojant COBIT5“, „Procesų vertinimo modelis naudojant COBIT5“. IT procesų gebos modelis ir pagrindiniai vertinimo principai trumpai pateikti Vadovo 2

priede. Išankstinio tyrimo metu preliminariai atliekant IT gebos vertinimą pildoma IT procesų gebos vertinimo forma (šabloną galima rasti Metodikos svetainės Šablonų skiltyje).

133. Pagal poreikį išankstinio tyrimo ar pagrindinio tyrimo metu, atliekant tam tikrų IT kontrolės priemonių vertinimą, gali būti naudojamos ISACA teminės audito programos[28], kuriose nurodytos galimos audito procedūros, pvz., skirtos kibernetiniam saugumui, IT strateginiam planavimui, pakeitimų valdymui ir kt. įvertinti.

4.1.6. Audito rizikos vertinimas

134. IT auditai turi būti atliekami remiantis rizika grįstu audito metodu. Taikant šį metodą audituojamame subjekte turi būti identifikuojamos įgimtos rizikos, IT kontrolės rizikos dėl kurių gali pasireikšti neigiamas poveikis organizacijai ir jos tikslams (pvz.: gali atsirasti finansiniai nuostoliai, veiklos procesų klaidos, ekonominės sankcijos, sumažėti klientų pasitikėjimas ar pasitenkinimas teikiamomis paslaugomis) bei valdoma neaptikimo riziką.

135. Audito rizikos vertinimas sudaro sąlygas nustatyti audito sritis, kurioms turėtų būti skiriama daugiau dėmesio pagrindinio tyrimo metu ir apsispręsti dėl audito procedūrų, kuriuos reikės atlikti pagrindinio tyrimo metu, apimties. Vadovo 4.1.9.5 skirsnyje „Audito procedūros, informacijos ir duomenų šaltiniai bei metodai“ pateikta audito procedūrų apimties schema, kuria auditorius vadovaujasi visuose audituose priimdamas sprendimus dėl audito procedūrų pobūdžio ir apimties.

136. Į audito riziką reikėtų atsižvelgti viso audito metu:

- ✓ audito planavimo metu, įskaitant audito procedūrų planavimą;
- ✓ audito procedūrų atlikimo metu;
- ✓ atliktų audito procedūrų įvertinimo metu;
- ✓ rengiant audito ataskaitą.

Įgimtos rizikos vertinimas

137. 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.

138. Įprastomis sąlygomis egzistuojanti įgimta rizika laikoma normalia. Ypatingomis sąlygomis atsirandanti rizika gali būti vertinama kaip padidinta įgimta rizika – paprastai ji atsiranda ten, kur didesnę įtaką turi individualūs sprendimai, kur įvyksta nenumatytos aplinkybės, esminiai pasikeitimai, veikla susijusi su sudėtingais procesais, ją reglamentuoja sudėtingi teisės aktai ir pan.

139. Įgimtos rizikos pavyzdžiai:

- ✓ audituojamo subjekto IS, kurios teikia paslaugas didžiajai daliai visuomenės, turi įgimtą riziką, kad, piko metu visiems naudotojams prisijungus, šios sistemos pajėgumai nebus pakankami ir sistema gali nulūžti;
- ✓ vartotojų anonimiškumas, ypač elektroninių ryšių tinkle, yra įgimta rizika;

[28] ISACA auditų programas galima rasti oficialioje ISACA interneto svetainėje.

- ✓ įgimta rizika gali būti susijusi su ypatingos svarbos statusą turinčiomis IS, nes saugumo spragų jose buvimas gali sudaryti sąlygas ypač didelei žalai atsirasti.

140. Šią riziką audito grupė vertina remdamasi subjekto veiklos išmanymu. Siekiant įvertinti audituojamame subjekte IT valdymo sistemos įgimtą riziką, audito grupė, susipažinusi su audituojamo subjekto veikla, jo IT valdymo sistema bei pasinaudodama Vadovo 3 priede pateiktu pavyzdiniu įgimtos rizikos veiksnių sąrašu, sutikrina ar audituojamoje srityje yra arba nėra minėtame priede nurodytų ir kitų auditoriaus nustatytų įgimtos rizikos veiksnių. Vertindama, ar IT valdymo sistemai būdinga padidinta ar normali rizika, audito grupė taip pat turi įvertinti šios rizikos reikšmingumą, t. y. koks nustatytos rizikos mastas ir tikimybė jai pasireikšti ir tai dokumentuoti. Auditoriai turėtų mažiau dėmesio skirti rizikai, kuri yra labai didelė, bet mažai tikėtina, ar tai, kuri yra nedidelė, bet tikėtina. Rizika, kurią auditoriai laiko tiek didele, tiek labai tikėtina, yra vertinama kaip reikšminga. Reikšmingos rizikos nustatymas yra auditoriaus profesinis sprendimas.

141. Vadovo 3 priede pateiktų įgimtos rizikos veiksnių sąrašas nėra baigtinis, todėl auditoriai atlikdami įgimtos rizikos vertinimą kiekvienu atveju gali nustatyti ir daugiau šios rizikos veiksnių, kuriuos turėtų įtraukti į vertinimą. Toliau įgimtos rizikos vertinimo rezultatai naudojami nustatant, kokia bus pasirinkta IT audito apimtis ir audito procedūros (išsamiau žr. 4.1.9 skirsnyje „Audito apimties nustatymas“).

IT kontrolės rizikos vertinimas

142. IT kontrolės rizika – tai tikimybė, kad audituojamo subjekto patvirtintomis IT kontrolės priemonėmis gali nepavykti sumažinti neigiamo poveikio, į kurį reaguojant jos buvo sukurtos. Pavyzdžiui, reikia užtikrinti, kad prieigą prie konfidencialių duomenų turėtų tik įgalioti darbuotojai, todėl nustatyta kontrolės priemonė, 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 audituojamajam 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.

143. Kuo didesnė nustatyta įgimta rizika, tuo stipresnė turi būti audituojamo subjekto IT kontrolės sistema, kad galėtų padėti sumažinti neigiamą poveikį, kuris gali įvykti dėl padidintos įgimtos rizikos. Tokiu atveju susipažindamas su IT kontrolės sistema auditorius turi ypač atkreipti dėmesį į tai, ar yra sukurtos ir veikiančios kontrolės procedūros tose srityse, kuriose nustatyta padidinta įgimta rizika. Kita vertus, net jei ši rizika nėra nustatyta, dėl kiekviename subjekte egzistuojančios normalios įgimtos rizikos taip pat gali atsirasti neatitikčių, todėl bet kuriame audituojamame subjekte turi būti sukurta tinkamai veikianti IT kontrolės sistema. Todėl net ir nesant padidintos įgimtos rizikos, IT kontrolės priemonių pakankamumas ir patikimumas turėtų būti įvertintas audituojamame subjekte.

144. IT kontrolės riziką vertina auditorius, susipažinęs su audituojama sritimi (išsamiau žr. 4.1.4 skirsnyje), remdamasis jo paties atliktu IT kontrolės priemonių vertinimu (išsamiau žr. 4.1.5 skirsnyje). Auditorius kontrolės riziką gali įvertinti kaip mažą, vidutinę arba didelę kiekvieno IT kontrolės priemonės vieneto atveju ir, atsižvelgęs į rezultatus, nustatyti bendrą IT kontrolės rizikos lygį (žr. 1 lentelę.).

1 lentelė. IT kontrolės priemonių vertinimas ir susijusi kontrolės rizika

Didelė rizika	IT kontrolės priemonės nėra arba ji netinkamai sukurta, arba yra netinkamai įgyvendinama ar netinkamai veikia
Vidutinė rizika	IT kontrolės priemonė yra įdiegta ir tinkamai sukurta, tačiau turi įgyvendinimo arba veikimo trūkumų
Maža rizika	IT kontrolės priemonė yra tinkamai sukurta ir neturi įgyvendinimo arba veikimo trūkumų arba yra smulkių/nereikšmingų trūkumų (kurie neturi jokio poveikio)

145. IT valdymo gebos vertinimą atlikti rekomenduotina, bet nėra privaloma. Jei išankstinio tyrimo metu preliminariai buvo atliktas IT valdymo gebos vertinimas pagal COBIT metodiką, auditoriai gautus gebos vertinimo rezultatus gali naudoti kartu vertinant IT kontrolės rizikos lygį pagal pirmiau nurodytą modelį (1 lentelė), rekomenduojama vertinti kad esant 0–1 gebai – kontrolės rizika didelė, 2–3 gebai – vidutinė, 4–5 – maža. Kiekvienu atveju auditorius priima profesinį sprendimą, koks gebos lygis kuriam IT kontrolės rizikos lygiui priskirtinas. Šie sprendimai turi būti dokumentuojami.

146. IT kontrolės rizikos vertinimo rezultatai fiksuojami išankstinio tyrimo rezultatų apibendrinimo dokumente (šabloną galima rasti Metodikos svetainės Šablonų skiltyje), kaip numatyta Vadovo 4.1.8 skirsnyje „Išankstinio tyrimo rezultatų apibendrinimas“. IT kontrolės rizikos vertinimo rezultatai kartu su įgimtos rizikos vertinimo rezultatais naudojami nustatant kokia bus pasirinkta IT audito apimtis (detaliau žr. 4.1.9 skirsnyje „Audito apimties nustatymas“).

Neaptikimo rizikos valdymas

147. Neaptikimo rizika – tai tikimybė, kad auditorius nenustatys, kad nėra subjekto patvirtintų IT kontrolės priemonių, kad jos neveikia ar netinkamos, o tai galėtų turėti neigiamą poveikį subjektui. Tai rizika, kurią auditorius gali kontroliuoti suplanuodamas tinkamas ir pakankamas audito procedūras. Neaptikimo rizika nėra atskirai vertinama įverčiu, ji tik susijusi su audito procedūrų pobūdžiu, laiku ir apimtimi, kurias nustato auditorius, siekdamas sumažinti audito riziką iki priimtinai žemo lygio. Pavyzdžiui, neaptikimo rizika, susijusi su taikomųjų programų sistemos saugumo pažeidimų nustatymu, paprastai yra didelė, jei nėra viso audito laikotarpio reikiamų registracijos (angl. log) žurnalų. Neaptikimo rizika, susijusi su atkūrimo po ekstremalių įvykių planų trūkumo nustatymu, paprastai yra maža, jei jos buvimas yra lengvai patikrinamas.

148. Tinkamas audito planavimas, audito grupės sudarymas, profesinio skepticizmo taikymas, audito darbo priežiūros vykdymas ir peržiūros atlikimas padidina audito procedūrų efektyvumą ir sumažina tikimybę, kad auditorius gali pasirinkti netinkamą audito procedūrą, netinkamai pritaikyti tinkamą audito procedūrą arba klaidingai interpretuoti audito rezultatus.

149. Neaptikimo rizikos lygis tiesiogiai priklauso nuo įvertinto įgimtos ir IT kontrolės rizikos lygio ir parodo, kokios apimties audito procedūrų reikėtų pagrindinio tyrimo metu:

- ✓ kuo didesnis įgimtos ir IT kontrolės rizikos lygis, tuo daugiau pagrindinio tyrimo metu reikia atlikti audito procedūrų, kad iki reikiamo lygio sumažėtų neaptikimo rizikos lygis;

- ✓ kuo mažesnis įgimtos ir IT kontrolės rizikos lygis, tuo mažiau pagrindinio tyrimo metu galima atlikti audito procedūrų, nes, kitoms rizikoms esant mažoms, galima toleruoti didesnę neaptikimo riziką.

150. Neaptikimo riziką galima sumažinti, bet ne pašalinti – tam tikra šios rizikos tikimybė visada išlieka. Neaptikimo rizikos mažinimo būdai:

- ✓ gerai suplanuoto, struktūrizuoto audito atlikimas kiek įmanoma aiškiau ir detaliau identifikuojant įgimtą ir kontrolės riziką – tinkamų ir pakankamų audito procedūrų numatymas ir atlikimas;
- ✓ su audito valdymu susijusios neaptikimo rizikos (audito atlikimo rizikos) identifikavimas ir jai valdyti priemonių nustatymas (dokumentuojama audito projekte ViPSIS, audito plane nurodoma pagal poreikį).

151. Su audito valdymu susijusios neaptikimo rizikos veiksnių pavyzdžiai:

- ✓ *Duomenų prieinamumas, pakankamumas, tinkamumas ir patikimumas.* Gali kilti rizika, kad audito metu nebus gauti arba bus gauti nepakankami, netinkami ir (ar) nepatikimi duomenys, reikalingi tinkamiems, pakankamiems audito įrodymams surinkti ir audito klausimams atsakyti. Tai gali įvykti dėl įvairių priežasčių, įskaitant skirtingų informacijos šaltinių prieinamumo trūkumą arba pateiktų duomenų kokybės ir patikimumo trūkumą. Taip pat yra rizika, kad dėl audituojamo subjekto veiksmų (pvz., netinkamo bendradarbiavimo) reikalinga informacija gali būti negauta laiku arba iš viso negauta. Yra rizika ir dėl galimo klaidingų duomenų pateikimo ar net apgaulės.
- ✓ *Auditorių kompetencija ir patirtis*. Audito grupės nariai gali neturėti pakankamai žinių, profesinių įgūdžių, analitinių ar kitų gebėjimų, būtinų sėkmingam planuojamos audituoti srities įvertinimui. Nepakankama patirtis ar žinių trūkumas gali sumažinti audito kokybę ir turėti neigiamos įtakos audito rezultatų tinkamumui ir patikimumui.
- ✓ *Ištekliai*. Egzistuoja rizika, kad turimų žmogiškųjų, finansinių, materialinių ir (ar) laiko išteklių gali nepakakti audito tikslui pasiekti. Įvairūs veiksniai, pvz.: papildomų ekspertų poreikis, mokymai ar netikėtai išaugusios išlaidos technologinėms priemonėms, gali padidinti audito kainą ir taip viršyti planuotą biudžetą bei sumažinti tikėtiną audito pridėtinę vertę.

152. Jeigu auditoriai nustato audito valdymo riziką, turi būti nustatytos ir priemonės ją valdyti. Taip audito metu kylančios problemos bus sprendžiamos operatyviau ir efektyviau. Audito rizikos valdymas – sisteminis audito projekto valdymo procedūrų ir priemonių taikymas, siekiant nustatyti ir valdyti tikėtinus įvykius, kurie gali reikšmingai paveikti audito procesą, taip pat suteikti pakankamą užtikrinimą, kad audito tikslas bus pasiektas. Kylančios rizikos ir jų valdymo priemonės aptariamos audito grupėje ir dokumentuojamos audito projekte Valstybės kontrolės Veiklos planavimo ir stebėsenos informacinėje sistemoje (toliau – ViPSIS), o audito plane nurodomos pagal poreikį. Jeigu reikia, atliekami numatytų audito rizikos valdymo priemonių pakeitimai.

153. Apibendrinant galima pasakyti, kad audito grupė turi nustatyti:

- ✓ kokių nesklandumų galėtų kilti atliekant auditą;
- ✓ kokia tikimybė, kad tie nesklandumai kils;

- ✓ koks būtų jų poveikis audito rezultatams ir kokybei;
- ✓ ką galima padaryti, kad nesklandumų atsiradimo tikimybė būtų mažesnė;
- ✓ kaip rizika galėtų būti valdoma, jei ji kiltų.

154. Kaip ir kitos, ši rizika ir jos valdymo priemonės turi būti aptartos audito grupėje. Pokalbiai su audituojamu subjektu ir kitomis susijusiomis šalimis gali padėti išaiškinti neaptikimo rizikos veiksnius ir jos valdymo priemones.

155. Auditoriai viso audito metu turi stebėti ir vertinti audito riziką ir, jeigu reikia, atlikti numatytų audito rizikos valdymo priemonių pakeitimus.

Apgaulės ir korupcijos rizikos vertinimas

Susiję TAAIS reikalavimai
Planuodamas auditą, auditorius privalo įvertinti apgaulės riziką ir būti pasirengęs galimai apgaulei viso audito metu. *(3000-ojo TAAIS 73 punktas)* Auditorius privalo įvertinti apgaulės riziką viso audito proceso metu ir vertinimo rezultatą įforminti dokumentais. *(4000-ojo TAAIS 58 punktas)* Atliekant atitikties auditą, jeigu auditorius pastebi reikalavimų nevykdymo atvejus, kurie gali rodyti apgaulę ar neteisėtus veiksmus, jis turi išlaikyti profesinį apdairumą ir informuoti apie tokius atvejus atsakingą instituciją. Auditorius privalo laikytis deramo apdairumo ir nesutrukdyti galimiems būsimiems teisiniams procesams ar tyrimams. *(4000-ojo TAAIS 225 punktas)*

156. Nors audito tikslas nėra atskleisti apgaulę ir korupciją, kaip nustato TAAIS reikalavimai, auditoriai turi įvertinti apgaulės ir korupcijos riziką ir imtis tam tikrų veiksmų jų atžvilgiu. Apgaulė apibrėžiama kaip tyčinis vieno ar kelių asmenų – audituojamo subjekto vadovybės, darbuotojų, už valdymą atsakingų asmenų ar trečiųjų šalių – veiksmas, siekiant gauti neteisėtos naudos[29]. Tai gali būti, pvz.: slaptai sutartas paramos skyrimas ar sutarčių sudarymas, klaidingos informacijos pateikimas, tyčinis informacijos iškraipymas, nuslėpimas, vagystė, neteisėti veiksmai, „dėkingumo mokesčiai“ ir kt.

157. Auditorius viso audito metu turi laikytis profesinio skepticizmo ir pripažinti galimybę, kad neatitiktis dėl apgaulės ir korupcijos gali egzistuoti nepaisant ankstesnės auditoriaus darbo su audituojamu subjektu patirties ir nuomonės apie aukščiausio lygio vadovų ir už valdymą atsakingų asmenų sąžiningumą ir principingumą.

158. *Apgaulė* apima faktų ir (ar) svarbios informacijos tyčinį iškraipymą, siekiant neteisėtai gauti turtinę naudą (materialinis interesas). Apgaulė galėtų apimti manipuliaciją, falsifikavimą ar sukeitimą dokumentų, neteisėtą lėšų pasisavinimą ar išeikvojimą, dokumentų apie sandorių rezultatus nuslėpimą ar klaidų juose padarymą, realiai

[29] 3910-osios GUID „Svarbiausi veiklos audito principai“, 91 p.

neegzistuojančių sandorių fiksavimą, sąmoningai klaidingą įstaigos apskaitos politikos taikymą.

159. *Korupcija* – piktnaudžiavimas įgaliojimais siekiant naudos sau ar kitam asmeniui viešajame ar privačiame sektoriuje. Korupcinio pobūdžio nusikalstamos veikos:

- ✓ kyšininkavimas, prekyba poveikiu, papirkimas, piktnaudžiavimas;
- ✓ nusikalstamos veikos, padaromos viešajame sektoriuje arba teikiant administracines ar viešąsias paslaugas piktnaudžiaujant įgaliojimais ir tiesiogiai ar netiesiogiai siekiant naudos sau ar kitam asmeniui: neteisėtas teisių į daiktą įregistravimas, tarnybos pareigų neatlikimas, valstybės paslapties atskleidimas, neteisėtas politinių partijų ir politinių kampanijų finansavimas, sukčiavimas, turto pasisavinimas arba iššvaistymas, komercinės paslapties atskleidimas, nusikalstamu būdu gauto turto legalizavimas, neteisingų duomenų apie pajamas, pelną ar turtą pateikimas, kišimasis į valstybės tarnautojo ar viešojo administravimo funkcijas atliekančio asmens veiklą, tarnybos paslapties atskleidimas, dokumento suklastojimas ar disponavimas suklastotu dokumentu;
- ✓ kitos nusikalstamos veikos, kuriomis siekiama kyšio, papirkimo arba nuslėpti ar užmaskuoti kyšininkavimą, prekybą poveikiu ar papirkimą.

  Papildomi aplinkybių, rodančių apgaulės galimybę, pavyzdžiai pateikti Metodikos svetainės Tvarkų ir kitos informacijos skiltyje.

160. Korupcinio pobūdžio teisės pažeidimas – administracinis nusižengimas, darbo pareigų pažeidimas ar tarnybinis nusižengimas, padaromas piktnaudžiaujant įgaliojimais ir tiesiogiai ar netiesiogiai siekiant naudos sau ar kitam asmeniui, taip pat korupcinio pobūdžio nusikalstama veika.

161. *Apgaulei ir korupcijai įtakos turintys veiksniai.* Auditoriams būtina suprasti apgaulės ir korupcijos motyvacijos ir organizacinius veiksnius. Neprivaloma kiekvieno audito metu įvertinti visų veiksnių (ne)buvimo, tačiau viso audito metu reikia išlaikyti tinkamą profesinį atidumą ir laiku identifikuoti galimą apgaulės ir korupcijos riziką. Veiksnių buvimas nebūtinai reiškia, kad įvyko apgaulė ar korupcija.

162. *Motyvacijos veiksniai:*

- ✓ ekonominė motyvacija – finansinis poreikis ar pelnas. Tai pagrindiniai apgaulės ir korupcijos stimulai. Dažnai asmenys, nuteisti už apgaulę ir korupciją, turi nepakeliamų finansinių problemų ir neturi jokių teisėtų pajamų šaltinių;
- ✓ šykštumas – asmenys, turintys valdžią ir įgaliojimų, dažnai įvykdo apgaulės ir korupcijos veiksmus iš godumo ir šykštumo;
- ✓ pripažinimas ar prestižas – asmenys gali norėti didesnio pripažinimo ar prestižo iš pavydo, keršto ar išdidumo. Jie dažnai būna garantuoti, kad jų padėtis yra aukščiau nei kitų ir gali likti nedemaskuoti ir neišaiškinti, įvykdę apgaulę ar korupciją;
- ✓ moralinis pranašumas – vienas motyvų gali būti pernelyg didelis savęs įvertinimas, esą turi moralinį pranašumą ar valdžią kitiems, kuriuos laiko aukomis.

163. *Organizaciniai veiksniai:*

- ✓ nepakankama vidaus kontrolės sistema – jei organizacija neturi patikimos vidaus kontrolės sistemos, tai gali sukurti palankias sąlygas apgaulei ir korupcijai, nes trūksta veiksmingų prevencijos ir atskleidimo mechanizmų;
- ✓ silpnos etikos normos – organizacijose, kuriose nėra aiškiai apibrėžtų etikos normų arba jos nėra tinkamai įgyvendinamos, yra didesnė korupcijos ir apgaulės rizika;
- ✓ neefektyvi priežiūra ir atskaitomybė – nepakankama darbuotojų veiksmų priežiūra ir neaiški atskaitomybė, skaidrumo ir atvirumo kultūros trūkumas gali sudaryti palankias sąlygas netinkamam elgesiui;
- ✓ organizaciniai pokyčiai – dideli organizaciniai pokyčiai, pvz., restruktūrizavimas, gali paskatinti piktnaudžiavimo atvejus;
- ✓ komunikacijos trūkumas – nepakankama ar netinkama komunikacija tarp vadovų, darbuotojų ir skyrių gali sukurti nesusipratimus, kuriuos gali išnaudoti asmenys, siekiantys piktnaudžiauti ir kt.

164. Vertindamas apgaulės rizikos veiksnius, auditorius turi atkreipti dėmesį į tai, kad apgaulės rizika įvertinama apsvarsčius tris jai būdingas sąlygas (apgaulės rizikos veiksnius) kiekvieno audituojamo subjekto atžvilgiu:
    - ✓ skatinimas arba spaudimas įvykdyti apgaulę (pvz., viešojo sektoriaus darbuotojai dažnai jaučia spaudimą teikti aukštos kokybės paslaugas turint nepakankamus išteklius reikiamai kokybei išlaikyti);
    - ✓ galimybė įvykdyti apgaulę (pvz., sudėtinga įdarbinimo aplinka arba pakankamai kvalifikuoto personalo trūkumas ir dėl to silpna vidaus kontrolė gali sudaryti galimybes pasireikšti apgaulei);
    - ✓ sugebėjimas pateisinti (pagrįsti) netinkamus veiksmus (pvz., paprastai žemesnis atlyginimų lygis viešajame sektoriuje, lyginant su privačiu, gali skatinti darbuotojus pateisinti neteisėtą lėšų naudojimą).

165. Vertindamas apgaulės ir korupcijos riziką, auditorius gali pasinaudoti *Apgaulės ir korupcijos rizikos vertinimo klausimynu* (šabloną galima rasti Metodikos svetainės Šablonų skiltyje). Esant poreikiui klausimynas gali būti papildytas kitais reikiamais klausimais.

166. Kai tame pačiame audituojamame subjekte atliekami keli Valstybės kontrolės auditai (veiklos, finansiniai, atitikties ir (ar) IT), kurių audituojamas laikotarpis persidengia, vėliau auditą pradėjusi audito grupė turėtų susisiekti su anksčiau jį pradėjusia grupe ir išsiaiškinti, ar toks klausimynas buvo pildomas. Jeigu buvo, rekomenduojame juo pasinaudoti.

167. Jeigu nustatoma apgaulės riziką didinančių veiksnių (atsižvelgiant į audito tikslą), auditoriai turėtų susipažinti su atitinkamomis vidaus kontrolės sistemomis ir išsiaiškinti, ar egzistuoja požymiai kokių nors neatitikimų, galinčių kliudyti veiklai.

168. Kai auditorius nustato apgaulės riziką, kurios vadovai nekontroliavo ar kontrolė nebuvo pakankama, arba jei, auditoriaus nuomone, subjekto rizikos vertinimui būdingi esminiai trūkumai, auditorius apie šiuos vidaus kontrolės trūkumus turi oficialiu raštu informuoti audituojamą subjektą.

169. Jeigu audito metu atskleidžiama apgaulė arba gaunama informacija, iš kurios galima spręsti, kad yra apgaudinėjama, auditorius turi oficialiu raštu pranešti apie tai

audituojamo subjekto vadovams (jei nekyla abejonių dėl jų sąžiningumo). Jeigu manoma, kad apgaulėje galėjo dalyvauti vadovai arba darbuotojai, vykdantys vidaus kontrolę, auditorius turi nedelsdamas apie tai pranešti tiems, kam pavestos valdymo funkcijos (pvz., jei įtariama, kad apgaulėje galėjo dalyvauti konkrečiai ministerijai pavaldžios įstaigos vadovas, apie tai pranešama tos ministerijos vadovybei).

170. Audito metu nustačius apgaulės ar korupcijos požymius ar aplinkybes, rodančias apgaulės ar korupcijos galimybę, turi būti konsultuojamasi su Valstybės kontrolės Teisėtumo užtikrinimo departamento teisininku dėl poreikio ir galimybės perduoti informaciją pagal kompetenciją atitinkamai teisėsaugos institucijai. Audito departamento vadovas, įvertinęs surinktą informaciją, inicijuoja darbo dokumento dėl medžiagos perdavimo atitinkamai teisėsaugos institucijai tikslingumo parengimą ir jį kartu su reikiamais dokumentais, pagrindžiančiais galimą apgaulę ar korupciją, teikia Teisėtumo užtikrinimo departamentui. Šis departamentas ne vėliau kaip per 7 darbo dienas nuo gavimo dienos vertina pateiktą medžiagą ir pateikia savo išvadą dėl medžiagos perdavimo teisėsaugos institucijai tikslingumo ir pagrįstumo. Prireikus, Teisėtumo užtikrinimo departamentas medžiagą aptaria su audito grupe. Teisėtumo užtikrinimo departamentui pateikus pastabas, jei reikia, surenkami papildomi audito įrodymai. Valstybės kontrolieriaus pavaduotojas, kuriam yra tiesiogiai pavaldus audito departamentas, gavęs iš audito departamento vadovo visą medžiagą kartu su Teisėtumo užtikrinimo departamento išvada per 5 darbo dienas priima sprendimą dėl medžiagos perdavimo teisėsaugos institucijai tikslingumo ir pagrįstumo. Jei priimamas sprendimas perduoti, audito departamento vadovas organizuoja jos perdavimą atitinkamai teisėsaugos institucijai.

4.1.7. Reikšmingumo nustatymas

171. IT audite reikšmingumas suprantamas kaip IT kontrolės priemonių trūkumų (pažeidžiamumų) svarba atsižvelgiant į šių trūkumų (pažeidžiamumų) daromą neigiamą poveikį organizacijos veiklai ir jos tikslų pasiekimui, ir išorės vartotojams, kurie naudojasi organizacijos IT ištekliais.

172. Reikšmingumas turi būti vertinamas viso audito metu:

- ✓ išankstinio tyrimo etape – vertinant reikšmingas audituotinas rizikas, nustatant audito tikslą, audito apimtį, kriterijus, audito procedūrų pobūdį, laiką ir apimtį;
- ✓ pagrindinio tyrimo etape – vertinant įrodymus, nagrinėjant pasikeitusias aplinkybes ir (ar) naują informaciją, dėl kurios gali prireikti peržiūrėti numatytas procedūras, vertinant pastebėjimus;
- ✓ audito ataskaitos rengimo etape – darant galutines išvadas dėl nustatytų IT kontrolės priemonių trūkumų (neatitikimų) reikšmingumo.

173. Vertindami reikšmingumą, auditoriai turėtų atkreipti dėmesį į:

- ✓ duomenų konfidencialumą, vientisumą, prieinamumą ir kritiškumą;
- ✓ IS sistemas, nuo kurių priklauso kritiniai organizacijos veiklos procesai;
- ✓ naudojamų taikomųjų programų skaičių ir tipą;
- ✓ IS besinaudojančių vidinių ir išorinių vartotojų skaičių;
- ✓ el. ryšių tinklų kritiškumą;

- ✓ IT išteklių išlaikymo kainą;
- ✓ potencialių klaidų kainą;
- ✓ svarbios ir gyvybiškai svarbios informacijos praradimo išlaidas, skaičiuojant pinigus ir laiką, skirtą atkurti, bet ir praradus reputaciją ir įvaizdį;
- ✓ per laikotarpį apdorotų prisijungimų, operacijų arba užklausų skaičių;
- ✓ paslaugų lygio susitarimo reikalavimus ir galimų nuobaudų kainą;
- ✓ potencialias baudas už teisinių, norminių ir sutartinių reikalavimų nesilaikymą;
- ✓ IT operacijų perdavimą trečiajai šaliai;
- ✓ įstatymų ir kitų teisės aktų laikymąsi ir pan.

174. Svarbu atkreipti dėmesį į audito rizikos vertinimo rezultatus ir galimų kontrolės priemonių trūkumų apimtį bendrame kontekste. Pvz., gali pasitaikyti atvejų, kai įgimta rizika normali, bet nustatyta daug nedidelių IT kontrolės priemonių trūkumų (pažeidžiamumų), kurie gali atrodyti nereikšminti, todėl susidaro vaizdas, kad IT kontrolės rizika galimai yra maža. Tačiau dėl to, kad šių trūkumų (pažeidžiamumų) bendra visuma yra didelė, egzistuoja galimybė, kad susikaupę keli tokių trūkumų (pažeidžiamumų) atvejai turės didelį poveikį organizacijai ir IT kontrolės rizika turėtų būti vertinama kaip vidutinę ar didelę.

175. Auditorius turėtų nustatyti tiek kiekybinį, tiek kokybinį reikšmingumą. Kai neįmanoma ar netikslinga jų nustatyti, tokį profesinį sprendimą ir jo pagrindimą auditorius turi dokumentuoti.

176. Atliekant auditą reikšmingumas gali kisti ir priklausyti nuo numatomų vartotojų ir atsakingųjų šalių pozicijos. Todėl audito planavimo metu nustatytas kiekybinis ir (ar) kokybinis reikšmingumas turi būti peržiūrimas audito rezultatų vertinimo etape ir įvertinta, ar jis tebėra tinkamas ir aktualus pagal aplinkybes ir atitinkamai pakeičiamas pagal poreikį.

177. Reikšmingumas tiesiogiai susijęs su laukiamu audito poveikiu. Kuo didesnis reikšmingumas, tuo labiau tikėtina, kad galimos išvados ir rekomendacijos bus pakankamai reikšmingos ir naudingos, sukurs siekiamą pokytį ir (ar) turės svarbų poveikį audituojamam subjektui ar visuomenei.

178. Reikšmingumo nustatymo rezultatai fiksuojami išankstinio tyrimo apibendrinimo dokumente (šabloną galima rasti Metodikos svetainės Šablonų skiltyje).

Kiekybinis reikšmingumas

179. Kiekybinis reikšmingumas – tai skaitinė vertė, nustatoma taikant palyginamojo rodiklio (pvz., su audito objektu susijusios išlaidos ar pajamos) procentinę dalį, kuri, auditoriaus nuomone, atspindi priemones, kurias numatomas (-i) naudotojas (-ai), labiausiai tikėtina, laiko svarbiomis. Paprastai taikomas nuo 0,5 iki 5 proc. reikšmingumas. Pavyzdžiui, pasirinkus 5 proc. reikšmingumą ir nustačius, kad nuo metinio IT biudžeto vertės tai sudaro 10 tūkst. Eur, reikšmingais būtų laikomi visi galimi IT kontrolės priemonių trūkumai (pažeidžiamumai), dėl kurių organizacija galėtų patirti nuostolių, viršijančių šią sumą. Šis pasirinkimas yra auditoriaus profesinis sprendimas, kuris turi būti pagrįstas auditoriaus IT kontrolės sistemos, jos rizikos, dalyko jautrumo ir numatomų naudotojų poreikių

įvertinimu. Kuo audito objektas ar jo sritis aktualesnė, jautresnė, nustatyta daugiau galimų IT kontrolės priemonių trūkumų, tuo pasirenkamas reikšmingumo procentinis lygis turėtų būti mažesnis, taip mažesnės skaitinės reikšmės būtų laikomos reikšmingomis.

180. Kadangi rizikos pobūdis, dalykų jautrumas ir IT kontrolės priemonių veiksmingumas gali būti skirtingas audito objekto srityse, auditorius gali apsvarstyti galimybę nustatyti kelias reikšmingumo ribas skirtingoms audito sritims (pvz., IT saugumo srityje vertinant kritines IS smulkiems trūkumams gali būti nustatytas didesnis reikšmingumas nei kitoms IS).

181. Be ribinės procentinės dalies, kiekybinis reikšmingumas gali būti nustatytas kaip konkretus IT kontrolės priemonių trūkumų (pažeidžiamumų) skaičius. Paprastai toks kiekybinis reikšmingumas naudojamas IT kontrolės priemonių testavimo metu (atvejų, kai nesuveikė planuojamos IT kontrolės priemonės, skaičius), siekiant įvertinti, ar tam tikros IT kontrolės priemonės veikė efektyviai visą audituojamą laikotarpį, t. y. kiek nustatyta nuokrypių (pvz., 1 iš 15), neatsižvelgiant į jų vertę.

182. Audito planavimo metu nustatytas kiekybinis reikšmingumas turi būti peržiūrimas audito rezultatų vertinimo etape ir įvertinta, ar jis tebėra tinkamas pagal aplinkybes ir, atitinkamai, pakeistas pagal poreikį. Turi būti įvertintas kiekvienos nustatytos galimos audituoti rizikos reikšmingumas (ar ji reikšminga ar nereikšminga). Dėl reikšmingumo priskyrimo auditorius priima profesinį sprendimą.

Kokybinis reikšmingumas

183. Kokybinis reikšmingumas – tai kokybiniai veiksniai, kurie reikšmingi dėl savo pobūdžio, konteksto ar kitų priežasčių. Kartais kokybiniai veiksniai gali būti svarbesni nei kiekybiniai. Kai kuriais atvejais kokybiniai gali lemti tai, kad ir mažesnė neatitikčių suma bus laikoma reikšminga, kitais atvejais šie aspektai gali būti nesusiję su kiekybine verte ar suma.

184. Neįmanoma pateikti visų reikšmingų klausimų sąrašo, nes jie labai skiriasi priklausomai nuo audito objekto ir audituojamo subjekto. Vertindamas, ar audito klausimui taikytinas kokybinis reikšmingumas, auditorius turi žinoti (numanyti) su audito objektu ir audituojamu subjektu susijusius specifinius klausimus, kurie domina valstybinio audito ataskaitos naudotojus.

185. IT kontrolės priemonių trūkumai (pažeidžiamumai) yra reikšmingi, kai jie daro neigiamą poveikį organizacijos veiklai ir jos tikslų pasiekimui, pavyzdžiui:

- ✓ galimai bus patirti reikšmingi finansiniai nuostoliai;
- ✓ padaryta reputacinė žala organizacijai;
- ✓ prarasti jautrūs duomenys;
- ✓ neveiks kritinė infrastruktūra;
- ✓ bus neigiamai paveikti organizacijos arba institucijos vidiniai veiklos procesai;
- ✓ bus neigiamai paveikti išorės subjektų, kurie naudojasi organizacijos IT ištekliais, veiklos procesai;
- ✓ pažeisti IT saugą reglamentuojančių teisės aktų reikalavimai;
- ✓ IT išteklių neefektyvus, neracionalus naudojimas;

- ✓ neteisėti IT sandoriai tarp susijusių šalių ir kt.

186. Rekomenduojama vertinant reikšmingumą atsižvelgti ir į audituojamo subjekto nustatytus rizikų poveikio rodiklius, kuriuos organizacija taiko vertinant savo veiklos ir IT rizikas. Šie rodikliai gali atskleisti papildomos informacijos koks organizacijos požiūris į rizikų neigiamą poveikį, kurie poveikio aspektai yra labai svarbus, o kurie ne.

187. IT kontrolės priemonių trūkumai (pažeidžiamumai) reikšmingi, kai jie turi korupcijos, apgaulės požymių, kai šiais trūkumais domisi Seimo Audito ir kiti komitetai, komisijos ar visuomenė, kai gali būti padaryta žala valstybės biudžetui, pažeistas viešasis interesas. Vertinant reikšmingumą reikia atsižvelgti ir į svarbius dalykus, kurie gali paveikti audito ataskaitos vartotojų, tokių kaip įstatymų leidžiamoji ar vykdomoji valdžia, sprendimų priėmimą.

188. Atliekant kokybinį reikšmingumo vertinimą, auditorius priima profesinį sprendimą dėl IT kontrolės priemonių trūkumų (pažeidžiamumų) reikšmingumo lygio, t. y. ar jie reikšmingi ar ne. Kuo nustatytų trūkumų (pažeidžiamumų) galimas neigiamas poveikis organizacijai didesnis, tuo jų reikšmingumo lygis bus aukštesnis. Rekomenduojama didesnį reikšmingumą nustatyti IT kontrolės priemonių trūkumams (pažeidžiamumams) dėl kurių gali atsirasti 185 p. nurodytas neigiamas poveikis ar jie gali būti susiję su 187 p. numatytomis aplinkybėmis.

189. Reikšmingumo lygis gali būti nustatytas ir atsižvelgiant į tai, kurios IT kontrolės priemonės organizacijai yra svarbiausios. Šių priemonių svarbumas nustatomas atlikus organizacijos veiklos tikslų ir IT tikslų sugretinimą vadovaujantis COBIT metodika. Kaip atlikti tikslų sugretinimą išsamiau pateikta *COBIT5 leidinyje „Organizacijos IT valdymo ir vadovavimo metodika“*. Naudoti šios knygos B, C, D prieduose pateikiamas tikslų hierarchijos lenteles reikėtų atsargiai, nes kiekvienos organizacijos situacija skiriasi. Be to, lentelės neturėtų būti naudojamos automatiškai, o tik kaip bendroji ryšių visuma ir atsižvelgiant į faktinius audituojamos organizacijos ir IT tikslus. Rekomenduojama veiklos ir IT tikslų sugretinimo rezultatus aptarti su audituojamu subjektu, šis sugretinimas turi būti dokumentuojamas. Atlikus sugretinimą nustatoma, ar IT kontrolės priemonės svarba pagrindinė (P) ar antraeilė (A). IT kontrolės priemonės reikšmingumo lygis yra didesnis, kai atlikus sugretinimą nustatoma, kad ryšis tarp organizacijos tikslų ir IT tikslų yra pagrindinis (P)[30]. Ši sugretinimo procedūra nėra privaloma, auditoriai priima profesinį sprendimą dėl poreikio atlikti minėtą procedūrą ir jos rezultatų panaudojimo vertinant IT kontrolės priemonių reikšmingumą.

190. Nustačius, kad IT kontrolės priemonių trūkumas (pažeidžiamumas) susijęs su svarbiausiomis IT kontrolės priemonėmis, jis gali būti laikomos daugiau reikšmingu. Bet kuriuo atveju verta pasitikrinti, ar sugretinimo rezultatai parodo tas sritis, kurių netinkamas veikimas gali sukelti reikšmingas pasekmes organizacijai ir jos tikslų pasiekimui. Reikšmingumo vertinimo rezultatai fiksuojami išankstinio tyrimo rezultatų apibendrinimo dokumente, kaip numatyta Vadovo 4.1.8 skirsnyje.

191. Audito planavimo metu nustatytas kiekybinis ir (ar) kokybinis reikšmingumas turi būti peržiūrimas audito rezultatų vertinimo etape – įvertinama, ar jis tebėra tinkamas pagal aplinkybes, ir atitinkamai pakeičiamas pagal poreikį. Turi būti įvertintas kiekvienos nustatytos rizikos reikšmingumas ir dėl to priimamas auditoriaus profesinis sprendimas.

---

[30] COBIT5 leidinys „Organizacijos IT valdymo ir vadovavimo metodika“, 2013 m. (versija 2013-10-31).

4.1.8. Išankstinio tyrimo rezultatų apibendrinimas

192. Išankstinio tyrimo rezultatų apibendrinimas, surinkus ir įvertinus informaciją ir duomenis apie nagrinėtą sritį, pateikiami išankstinio tyrimo rezultatai ir sprendimas dėl tolesnio audito atlikimo ar neatlikimo (audito užbaigimu išankstinio tyrimo ataskaita). Audito planavimo rezultatų apibendrinimas turi būti parengtas ir patvirtintas iki audito planavimo rezultatų pristatymo Vadovybei, kurio metu aptariamos rizikos. Išankstinio tyrimo rezultatų apibendrinimo parengimą organizuoja audito grupės vadovas. Audito grupės atsakomybė rengiant išankstinio tyrimo rezultatų apibendrinimą išsamiau aprašyta *Valstybinių auditų kokybės užtikrinimo vadove*.

193. Išankstinio tyrimo rezultatų apibendrinime (šabloną galima rasti Metodikos svetainės Šablonų skiltyje) turi būti nurodyta:

- ✓ *Santrumpos ir sąvokos*. Pateikiamos vartojamos santrumpos ir sąvokų paaiškinimai (išnašose nurodomi sąvokų paaiškinimo šaltiniai).
- ✓ *Audito objektas*.
- ✓ *Informacija apie nustatytas ir atrinktas rizikas*. Šioje dalyje pateikiamos išankstinio tyrimo metu nustatytos IT kontrolės (bendrųjų ir taikomųjų programų kontrolės priemonių) rizikos:
  - Rizikos sugrupuojamos pagal atitinkamas sritis.
  - Riziką rekomenduojama įvardinti paprastu, aiškiu ir trumpu sakiniu. Rizika apibūdinama keliais sakiniais, pateikiant esminius faktus ir (ar) pavyzdžius ir pateikiant nuorodą į darbo dokumentą (-us), kuriame (-iuose) ji analizuota. Rekomenduojama nurodyti ir galimas rizikos priežastis ir pasekmes, jeigu tokios buvo identifikuotos išankstinio tyrimo metu. Taip pat aprašant riziką pateikiama informacija apie pokyčius, įvykusius nagrinėtoje srityje po strateginio tyrimo atlikimo (pvz., tam tikros strateginio tyrimo metu nustatytos problemos buvo išspręstos ar yra sprendžiamos).
  - Taip pat pateikiama informacija apie IT kontrolės priemonės svarbą (pagal poreikį), rizikos lygį, rizikos reikšmingumą ir jo pagrindimas, pažymima, ar rizika atrenkama tolesniam testavimui, pateikiamos priežastis, kodėl rizika nėra atrinkta tais atvejais, jei rizikos lygis didelis arba vidutinis ir rizika yra reikšminga. Auditorius pagal poreikį gali pateikti papildomos informacijos.
- ✓ *Laukiamas audito poveikis*. Pateikiamas aprašymas, kokią tikėtiną naudą audito rezultatai duos tobulinant nagrinėjamą sritį. Išsamiau valstybinio audito poveikio vertinimo procesą reglamentuoja Valstybinio audito poveikio vertinimo metodika.
- ✓ *Sprendimas dėl pagrindinio tyrimo atlikimo*. Nurodoma, ar bus atliekamas pagrindinis tyrimas. Jeigu šis tyrimas nebus atliekamas, nurodomos priežastys, dėl kurių siūloma jo neatlikti.

  Priežasčių, kuriomis remiantis vertėtų svarstyti galimybę nutraukti auditą ir baigti jį išankstinio tyrimo ataskaita, pavyzdžiai:
  - audituojamas subjektas ėmėsi veiksmų problemoms spręsti;

- yra rizika, kad audito įtaka pokyčiams bus maža ar jos nebus, nebus pasiektas laukiamas audito poveikis arba audito kaštai viršys galimą naudą;
- nėra reikiamos kvalifikacijos auditorių, galinčių atlikti auditą, o ekspertų paslaugos labai brangios, nėra galimybių pasitelkti ekspertų;
- audituojami subjektai nekaupia duomenų, kurių reikia didžiajai daliai ar visiems pakankamiems ir tinkamiems audito įrodymams surinkti, ir pan.

✓ *Išankstinio tyrimo ataskaitos rengimo grafikas* (pildomas nusprendus neatlikti pagrindinio tyrimo ir auditą baigti išankstinio tyrimo ataskaita).

✓ *Planuojami ištekliai* (pildomi nusprendus neatlikti pagrindinio tyrimo ir auditą baigti išankstinio tyrimo ataskaita).

194. Auditorius priima profesinį sprendimą, kokias ir dėl kokių priežasčių rizikos yra atsirenkamos tolimesniam testavimui. Šis sprendimas priimamas atsižvelgiant į audito tikslą, turimas kompetencijas, audito išteklius, laiką (skirtą auditui atlikti), kitas reikšmingas aplinkybes ir rizikas. Atrinkdami rizikingas IT kontrolės priemones auditoriai turi apsispręsti ir dėl audito apimties, apie tai išsamiau Vadovo 4.1.9 skirsnyje.

195. Tolimesniam testavimui turėtų būti atrinktos IT kontrolės rizikos, kurių rizikos lygis yra didelis (IT kontrolės priemonės nėra arba ji netinkamai sukurta, arba yra netinkamai įgyvendinama ar netinkamai veikia, žr. 144 p.), ir IT kontrolės priemonės, kurios yra kiekybiškai ir (ar) kokybiškai reikšmingos (pvz., kai nustatoma, kad dėl IT kontrolės priemonių trūkumo (pažeidžiamumo) gali atsirasti finansiniai nuostoliai, gali būti sutrukdytas valstybei svarbių funkcijų įgyvendinimas, neteikiamos paslaugos daugumai vartotojų, kyla grėsmė duomenų konfidencialumui, vientisumui ir kt., žr. 185, 187 p.).

196. Rekomenduojama testavimui atrinkti rizikas, kurių rizikingumo lygis yra vidutinis (IT kontrolės priemonė yra įdiegta ir tinkamai sukurta, tačiau turi įgyvendinimo ar veikimo trūkumų, žr. 144 p.), ir jos yra reikšmingos, bet audito grupė dėl šių rizikų įtraukimo priima profesinį sprendimą remdamasi turimais ištekliais ir tikėtina šių rizikų vertinimo nauda.

197. Jeigu nusprendžiama neatlikti tolesnių audito procedūrų, parengiama išankstinio tyrimo ataskaita. Apie tai išsamiau Vadovo 4.3.2 skirsnyje.

198. Jeigu nusprendžiama atlikti pagrindinį tyrimą, parengiamas audito planas. Apie tai išsamiau Vadovo 4.1.11 skirsnyje. Rengiant audito planą, esant poreikiui išankstinio tyrimo rezultatų apibendrinimas gali būti patikslintas, pavyzdžiui, jeigu buvo išgryninti galimai nauji IT kontrolės priemonių trūkumai ir pan. Patikslintas apibendrinimas ViPSIS pateikiamas kartu su audito plano projektu. Esant poreikiui, ten pat pateikiami ir patikslinti išankstinio tyrimo darbo dokumentai.

4.1.9. Audito apimties nustatymas

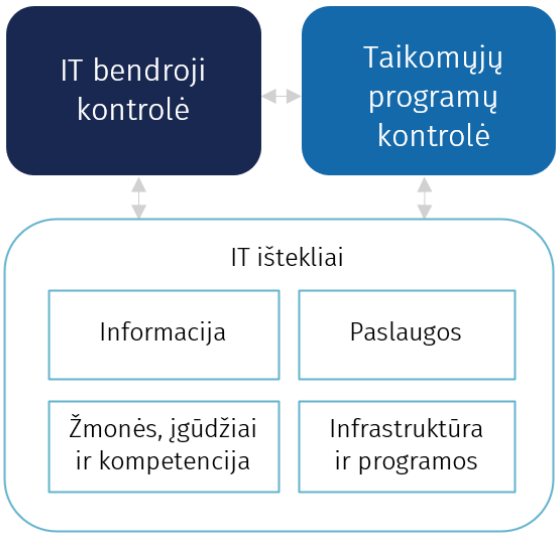
4.1.9.1. Audito objektas ir tikslas

Susiję TAAIS reikalavimai
Auditorius privalo nustatyti veiklos audito sritį (objektą).

Susiję TAAIS reikalavimai
(3000-ojo TAAIS 29 punktas) Auditorius privalo aiškiai formuluoti audito tikslą, kad būtų aiškūs klausimai, į kuriuos reikės atsakyti, ir kad būtų galima parengti logišką audito planą. *(3000-ojo TAAIS 36 punktas)*

199. Audito objektas nurodo, kas yra audituojama. Paprastai IT audito objektas gali būti tam tikros IT bendrosios kontrolės priemonės ir (ar) taikomųjų programų kontrolės priemonės. IT kontrolės priemonių vertinamas turėtų apimti IT išteklius: informaciją, paslaugas, infrastruktūrą ir taikomąsias programas, žmones, įgūdžius ir kompetencijas (5 pav.). Atsižvelgus į audito tikslą, audito objektas gali būti susijęs tik su IT bendrąja kontrole. Tais atvejais, kai tikslas susijęs su taikomųjų programų kontrolės priemonių tinkamumo ir (ar) pakankamumo vertinimu, audito objektas turėtų apimti tiek IT bendrosios kontrolės, tiek taikomųjų programų kontrolės priemonių vertinimą.

5 pav. IT audito objektas



200. Audito tikslas nurodo, ko siekiama atliekant auditą. Tikslas turi būti suformuluotas taip, kad atlikus auditą būtų įmanoma padaryti aiškią ir nedviprasmišką išvadą, ar jis pasiektas. Aiški ir glausta tikslo formuluotė apsaugo audito grupę nuo pernelyg plačios audito apimties.

201. Audito tikslas gali būti suvokiamas kaip bendras (pagrindinis) audito klausimas apie audito objektą, į kurį auditorius turi atsakyti remdamasis gautais audito įrodymais. Paprastai IT audito tikslas gali būti nukreiptas atsakyti į klausimą, ar audituojamo subjekto patvirtintos IT kontrolės priemonės yra pakankamos ir patikimos.

202. IT audito tikslas turi būti suformuluotas atsižvelgiant į pasirinktas audituoti rizikas ir jų reikšmingumą, nustatytas išankstinio tyrimo metu, ir atsižvelgiant į tai, kokio tipo bus vykdomas auditas – finansinis, atitikties ar veiklos. 5100-ajame GUID pateikiami galimi IT audito tikslų pavyzdžiai pagal atliekamo audito tipą:

- ✓ įvertinti IT bendrosios kontrolės ir taikomųjų programų kontrolės priemones, kurios daro poveikį audituojamos įmonės finansinėms ataskaitoms (finansinis auditas);

- ✓ įvertinti IT procesų atitiktį audituojamo subjekto veiklą reglamentuojantiems teisės aktams, politikai ir standartams (atitikties auditas);
- ✓ įvertinti IT išteklius, ar jie leidžia efektyviai ir veiksmingai pasiekti organizacinius tikslus (veiklos auditas);
- ✓ įvertinti ar atitinkamos IT bendrosios ir taikomųjų programų kontrolės priemonės yra veiksmingos siekiant nustatyti ir koreguoti perteklinio IS valdymo atvejus ar jų išvengti (veiklos auditas).

203. Pagal 5100-ąjį GUID, atsižvelgus į audito tikslą, auditoriui gali būti svarbu IT kontrolės priemonių: kūrimas, nes galima vertinti IT kontrolės priemonių dizainą, ar jis yra tinkamas; įgyvendinimas, nes galima vertinti, ar IT kontrolės priemonės (kai jos tinkamai sukurtos) yra įgyvendinamos praktikoje kaip numatyta; veiksmingumas, kai renkami įrodymai, ar pasiekti kokybiški IT proceso rezultatai, atsižvelgiant į atitinkamą IT kontrolės priemonės tikslą.

204. Nusprendę, koks bus IT audito objektas ir tikslas, IT auditoriai turi apsispręsti ir dėl audito apimties. Šie sprendimai paprastai priimami tuo pačiu metu. IT audito apimties nustatymas turėtų apimti sprendimą dėl audito atlikimo masto, atsižvelgiant į audituojamo subjekto IT valdymo sistemos aprėptį, audituotinas IT kontroles, nagrinėjamą laikotarpį, taip pat audito tipą (finansinis, atitikties ar veiklos auditas). Iš esmės tai yra audito ribų nustatymas arba apibrėžimas.

205. Apibrėžiant IT audito apimtį, pasirenkamas audituojamas laikotarpis (pvz., vieneri, treji metai ir t. t.). Tinkamas laikotarpis turėtų būti pasirinktas atsižvelgiant į nustatytus audito tikslą ir objektą. Analizuojant esamą subjekto veiklą, gali pakakti vieno ataskaitinio laikotarpio. Analizuojant veiklos rodiklius ir jų kitimo tendencijas (nustatant reikšmingus pokyčius) paprastai turėtų būti audituojama ne mažiau kaip du ataskaitiniai laikotarpiai.

206. IT audito apimtis priklauso ir nuo to, ar audito objektas susijęs su tam tikros:

- ✓ *Programos vertinimu*. Atliekant tokio pobūdžio IT auditą būtų siekiama įvertinti tam tikros su IRT sritimi susijusios programos (pvz., kibernetinio saugumo programa) tinkamumą spręsti tam tikras problemas, programos sandarą, vykdymą, rezultatus ir poveikį. Daugiausia dėmesio audito metu turėtų būti skiriama programos rezultatams ir poveikiui vertinti. Tarptautinėje praktikoje vertinant programas neapsiribojama vien ekonomiškumo, efektyvumo ir rezultatyvumo analize. Naudojami ir kiti vertinimo aspektai: tinkamumas, naudingumas, tęstinumas. Programų auditų atlikimas plačiau aprašytas Valstybės kontrolės parengtose Programų audito atlikimo gairėse.
- ✓ *Organizacijos vertinimu*. Atliekant tokio pobūdžio IT auditą būtų siekiama įvertinti tik audituojamoje organizacijoje taikomas IT bendrąsias ir (ar) taikomųjų programų kontroles priemones, jų veiksmingumą ir poveikį organizacijos tikslų pasiekimui. Esant poreikiui tokio audito apimtyje gali būti atliekamas ir organizacijos IT valdymo gebos lygio vertinimas. Organizacijos IT auditas gali padėti išsiaiškinti organizacijos IT kontrolės stipriąsias ir silpnąsias puses, įvertinti IT valdymo efektyvumą ir tolesnio IT valdymo tobulinimo galimybes.
- ✓ *Sistemos vertinimu*. Atliekant tokio pobūdžio IT auditą būtų siekiama įvertinti tam tikros IT srities (sistemos) valdymą, apimant sistemoje veikiančių ir turinčių bendrų tikslų institucijų veiklos vykdymo, tarpusavio koordinavimo, taupaus ir

efektyvaus lėšų naudojimo, nustatytų tikslų pasiekimo tyrimą. Pvz., nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui srityje suinteresuotos šalys yra policija, Krašto apsaugos ministerija, Nacionalinis kibernetinio saugumo centras, prokuratūra, todėl, pasirinkus IT audito objektu šiuos nusikaltimus, IT auditas būtų sisteminio pobūdžio. Atliekant sisteminius IT auditus IT bendroji kontrolė gali būti suprantama plačiąja prasme kaip tam tikrų politikų, standartų ir kt. įgyvendinimas šalies mastu.

207. Pasirinkus audito objektą gali paaiškėti, kad yra tam tikri ribojimai, dėl kurių nėra galimybės atlikti reikiamos apimties audito. IT audito apribojimai turi būti nurodyti kiekviename IT audito etape ir atitinkamu lygmeniu ir dokumentuoti. Pvz., apribojimais galėtų būti nepakankama prieiga prie duomenų ir informacijos, tinkamos proceso dokumentacijos trūkumas. Dėl šių apribojimų išvadas darydami IT auditoriai turi taikyti kitus tyrimo ir analizės metodus. Jei dėl įvairių apribojimų tam tikroje srityje nebus galimybės atlikti vertinimų ir pateikti pastebėjimų arba išvadų, išankstinio tyrimo metu auditoriai gali priimti sprendimą nenagrinėti tam tikrų sričių pagrindinio tyrimo metu.

4.1.9.2. Audituojami subjektai

208. Atlikęs išankstinio tyrimo procedūras ir norėdamas apibrėžti audito apimtį, auditorius įvertina, ar reikia patikslinti audituojamą (-us) subjektą (-us), kuriame (-iuose) pagrindinio tyrimo metu atliks audito procedūras, t. y. papildyti tais, kurie nebuvo priskirti audituojamiesiems subjektams atliekant išankstinį tyrimą. Paprastai IT audito metu audituojamieji subjektai yra IS valdytojas ir (ar) IS tvarkytojas, tačiau atliekant sisteminius IT auditus gali būti pasirinktos ir kitos susijusios šalys, pvz., išorinių IS, kurios integruojasi su auditui aktualia IS, valdytojai ir (ar) tvarkytojai.

209. Kai audituojamoje srityje veikia daug vienarūšių audituojamųjų subjektų (pvz.: savivaldybės, mokyklos, ligoninės ir pan.), auditorius paprastai gali neturėti galimybės audito procedūras atlikti visuose juose. Todėl auditorius atlieka audituojamųjų subjektų atranką. Jeigu pagrindinio tyrimo metu audito procedūras planuojama atlikti keliuose subjektuose, turi būti dokumentuotas atitinkamas sprendimas, kuris, esant poreikiui, turi apimti ir audituojamų subjektų atranką (išsamiau apie atranką žr. Vadovo 4.1.10.3 skirsnyje). Svarbu užtikrinti, kad pasirinkti subjektai tinkamai reprezentuotų visumą.

210. Pasirenkant audituojamus subjektus svarbi auditoriaus profesinė patirtis, geras audituojamos srities suvokimas. Pasirenkant audituojamus subjektus atsižvelgiama į:

- ✓ jų reikšmingumą (pvz.: lėšų dydis, veiklos rezultatų rodikliai ir kt.);
- ✓ nustatytą riziką (išankstinio tyrimo metu pastebėtas problemas);
- ✓ geografinį išsidėstymą (pvz.: regionai, apskritys ir kt.);
- ✓ tiriamą laikotarpį (pvz.: faktinis laikotarpis, vieneri ar daugiau metų);
- ✓ ankstesnių auditų rezultatus ir kt.

4.1.9.3. Audito klausimai

Susiję TAAIS reikalavimai
Auditorius privalo aiškiai formuluoti audito tikslą, kad būtų aiškūs klausimai, į kuriuos reikės atsakyti, ir kad būtų galima parengti logišką audito planą.

(3000-ojo TAAIS 36 punktas)

Jei audito tikslas formuluojamas kaip audito klausimas, kuris išskaidomas į smulkesnius klausimus, auditorius privalo užtikrinti, kad juos sietų bendra tema, jie papildytų vienas kitą, nesidubliuotų, apimtų visus audito aspektus ir būtų skirti atsakyti į bendrąjį audito klausimą.

(3000-ojo TAAIS 37 punktas)

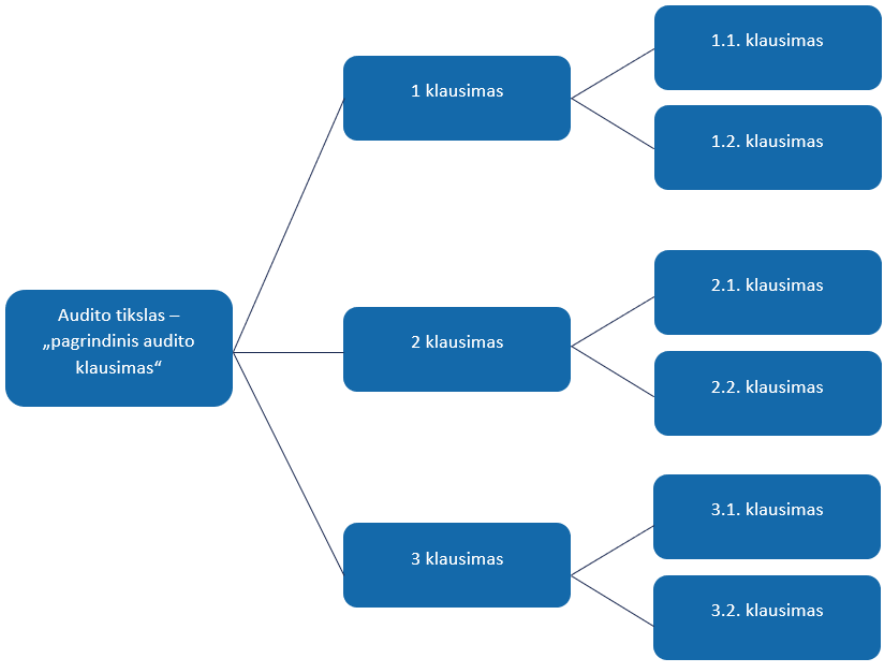
211. Atrinkus audituoti rizikas ir patikslinus audito objektą bei tikslą, svarbu suformuluoti audito klausimus, į kuriuos reikės atsakyti pagrindinio tyrimo metu.

212. Audito klausimai turi būti aiškiai apibrėžti ir nedviprasmiški, pagrįsti visapuse galimų IT kontrolės priemonių trūkumų analize. Auditoriui svarbu tinkamai pasirinkti klausimus, nes nuo to priklausys, ar auditas bus prasmingas ir bus įsigilinta į audituojamos srities esmę. Jei klausimai nebus tinkamai suformuluoti, gali būti sudėtinga surinkti pakankamus ir tinkamus audito įrodymus, kurie padėtų į juos atsakyti. Klausimai turi būti suformuluoti taip, kad leistų auditoriui daryti išvadas ir būtų išvengta nereikalingo darbo.

213. Rekomenduojama formuluoti ne daugiau kaip tris pirmo lygmens klausimus. Jie išskaidomi į smulkesnius. Vieno lygmens klausimų turi būti daugiau nei vienas ir, rekomenduotina, ne daugiau nei septyni.

214. Visų lygmenų klausimai turi būti susiję su pasirinktomis audituoti IT kontrolės rizikomis, audito objektu ir tikslu. To paties lygmens klausimai savo prasme turi būti lygiaverčiai, papildyti vienas kitą ir nesidubliuoti. Kiekvieno lygmens klausimai turi apimti aukštesnio lygmens klausimų pagrindinius aspektus, jie turi padėti atsakyti į aukštesnio lygmens klausimus. Pirmo lygmens klausimai turi apimti visus audito tikslo aspektus, jie turi būti skirti atsakyti į pagrindinį audito klausimą, t. y. padėti pasiekti audito tikslą (žr. 6 pav.). Audito klausimai nurodomi audito plane.

6 pav. Audito klausimų lygmenys



215. IT audite pirmo lygio klausimai gali būti siejami su tam tikrų IT kontrolės priemonių tikslais ir jų rezultatais, pavyzdžiui, ar užtikrinamas IT strateginis planavimas arba ar užtikrinamas IT rizikų valdymas, t.t.

216. Antro lygmens klausimai gali detalizuoti savo apimtyje IT kontrolės priemonių elementų aspektus, pvz.: ar IT strateginiame plane numatyti tikslai susiję su organizacijos veiklos tikslais, ar sudarant arba atnaujinant strateginį planą dalyvauja visos suinteresuotos šalys, pan.; ar kiekvienais metais atliekamas IT rizikų vertinimas, ar visos nepriimtinos rizikos yra tvarkomos.

217. Pagrindinio tyrimo metu auditoriui gaunant vis daugiau informacijos apie audituojamą sritį ir įgyjant vis daugiau žinių, klausimai gali būti tikslinami, kad geriau atspindėtų audito objektą, laukiama jo poveikį. Tai neturėtų būti daroma dažnai. Kadangi audito klausimai turi būti aptarti su audituojamu subjektu, dažnas jų keitimas pagrindinio tyrimo metu gali sukelti abejonių audito profesionalumu, objektyvumu ir sąžiningumu.

4.1.10. Audito kriterijų nustatymas ir procedūrų planavimas

4.1.10.1. Audito kriterijai

Susiję TAAIS reikalavimai
Auditorius privalo nustatyti tinkamus audito kriterijus, atitinkančius audito tikslą ir audito klausimus ir susijusius su ekonomiškumo, efektyvumo ir (arba) rezultatyvumo principais. *(3000-ojo TAAIS 45 punktas)* Planuodamas ir (arba) atlikdamas auditą, auditorius privalo aptarti audito kriterijus su audituojamu subjektu. *(3000-ojo TAAIS 49 punktas)* Jeigu AAI turi teisę savo nuožiūra parinkti atitikties auditų apimtį, auditorius privalo identifikuoti atitinkamus audito kriterijus prieš atlikdamas auditą, kad būtų sudarytas pagrindas išvadai ar nuomonei dėl audito srities parengti. *(4000-ojo TAAIS 110 punktas)*

218. Audito kriterijus – tam tikras etalonas (normatyvinis standartas, pagrįstas lūkestis, geroji veiklos praktika ar nustatytas parametras (duomuo, matas, savybė, rodiklis)), kuris leidžia įvertinti audito duomenis ir padaryti išvadas apie audituojamo subjekto IT valdymą, IT kontrolės priemonių pakankamumą ir patikimumą.

219. Audito kriterijai suteikia pagrindą įvertinti įrodymus, pateikti pastebėjimus ir parengti išvadas siekiant audito tikslo. Auditorius surinktiems duomenims vertinti pasirenka audito kriterijus atsižvelgdamas į audito objektą ir tikslą ir numatytus žemiausio lygmens audito klausimus.

220. IT audite audito kriterijai nėra standartizuoti, auditorius nustato juos kiekvienam auditui individualiai.

221. Parinkdamas audito kriterijus, auditorius turėtų atsakyti į klausimą – kokią situaciją pagrįstai laikytume tinkama ir kaip ją įmanoma išmatuoti. Taigi numatomi audito kriterijai turi suteikti pagrindą pagrįstai įvertinti esamą situaciją ir surinktus audito įrodymus.

222. Audito kriterijai suformuoja pagrindą, kuriuo remiantis nustatomos audito procedūros ir jų apimtis, darbo dokumentų turinys, renkami ir vertinami audito įrodymai, formuluojami audito pastebėjimai ir išvados dėl audito tikslo. Audito kriterijai padeda auditoriui atsakyti į klausimus:

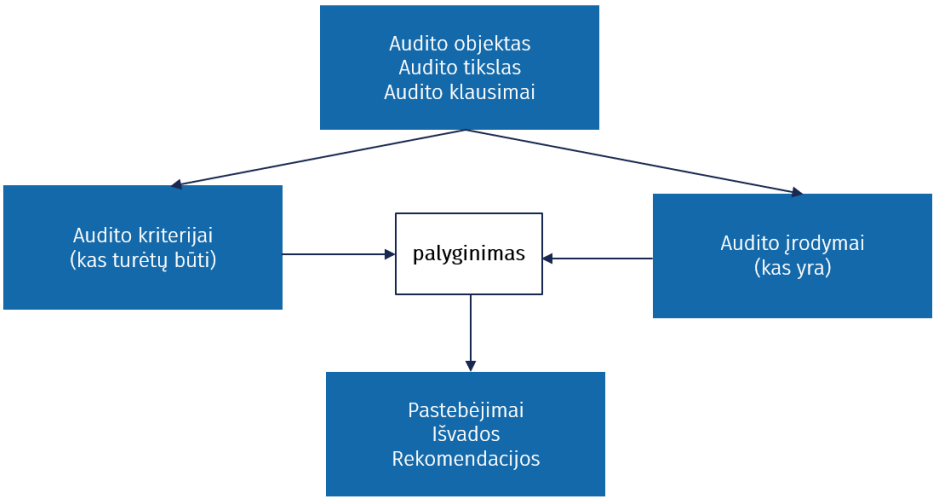
- ✓ ar IT kontrolės priemonės sukurtos taip, kad jos sudarytų prielaidas efektyviai vykdyti organizacijos veiklą, mažinti veiklos rizikas, padėti organizacijai įgyvendinti jos tikslus;
- ✓ ar praktikoje IT kontrolės priemonės įgyvendinamos taip, kaip jos turėtų būti įgyvendinamos;
- ✓ ar IT ištekliai naudojami racionaliai, ekonomiškai, teisėtai, kt.

223. Audito kriterijai, kai jie buvo aptarti su audituojamais subjektais ir audituojamieji su jais sutiko, leidžia suformuoti bendrą audito grupės ir subjekto požiūrį į audito rezultatus (faktus, tendencijas, išvadas ir rekomendacijas), sumažinti ginčų su subjektu tikimybę.

224. Surinkti įrodymai, nustatyti faktai parodo, kokia yra esama IT valdymo būklė, ji palyginama su tuo, kokia ji turi būti pagal pasirinktus audito kriterijus (žr. 7 pav.). Vertinimas gali būti trejopas:

- ✓ jeigu audito metu nustatoma, kad faktinė IT valdymo būklė neatitinka nustatytų nagrinėjamos srities kriterijų, konstatuojami IT valdymo trūkumai (pažeidžiamumai) ir vertinama, kaip (kokiomis priemonėmis) šiuos trūkumus (pažeidžiamumus) reikia tobulinti; šiuo tikslu pateikiamos rekomendacijos;
- ✓ jeigu vertinama IT valdymo būklė (faktinė situacija) atitinka nustatytus kriterijus, tai rodo, kad subjekto veikla yra tinkama;
- ✓ jeigu faktinė IT valdymo būklė, lyginant su nustatytu standartu, yra geresnė, o jos rodikliai aukštesni, galima konstatuoti esant gerąją praktiką.

7 pav. Audito kriterijų reikšmė audito procese



225. Audito kriterijų šaltiniai gali būti:

- ✓ visuotinai pripažinti (ir užsienio valstybių) veiklos standartai;

- ✓ įstatymuose ir kituose teisės aktuose nustatytos normos ir reikalavimai, susiję su audituojamu klausimu;
- ✓ audituojamo subjekto, jo veiklą prižiūrinčio ar kontroliuojančio subjekto, pvz., jo steigėjo patvirtinti reikalavimai (veiklos normos, standartai ar kontrolės priemonės);
- ✓ institucijos ar programos veiklos tikslai ir kt.;
- ✓ analogišką veiklą vykdančio kito subjekto patvirtintos veiklos normos, standartai ar kontrolės priemonės; gerosios praktikos pavyzdžiai;
- ✓ profesiniai standartai;
- ✓ nepriklausomų ekspertų patarimai ir techninės žinios;
- ✓ veiklos, procesų valdymo, vadovavimo, administravimo praktika ir principai;
- ✓ mokslinės žinios, moksliniai tyrimai, statistiniai duomenys ir kita patikima informacija;
- ✓ bendroji vadybos ar specialioji mokslinė literatūra;
- ✓ klientų arba vartotojų lūkesčiai.

226. Svarbiausiais šaltiniais laikomi oficialūs standartai (įstatymuose ir kituose teisės aktuose iškelti tikslai, Seimo ar Vyriausybės priimti teisės aktai) ir moksliškai pagrįsti standartai, kurių šaltiniai – speciali mokslinė literatūra, profesiniai reikalavimai ar geroji praktika.

227. Vienas IT audito kriterijų šaltinių gali būti COBIT metodika, pvz., tam tikras vertinimo kriterijus gali būti pasirenkamas kaip tam tikro COBIT proceso, kuris susijęs su klausimu, bazinė praktika ir (ar) šio proceso rezultatų pasiekimo vertinimo kriterijus (-ai). IT procesų bazines praktikas galima rasti COBIT5 knygoje „Procesų vertinimo modelis, naudojant COBIT5“ arba pavyzdiniame klausimyne IT bendrosios kontrolės priemonių vertinimui atlikti.

228. Klausimų formulavimas nebūtinai visais atvejais turi atitikti IT proceso bazinės praktikos formuluotes, kadangi praktikoje dėl teisinio reguliavimo ar institucijos įdiegtų kontrolės priemonių tam tikri kontrolės priemonių aspektai gali turėti kitus pavadinimus ar formuluotes. Tokiais atvejais rekomenduojama taikyti praktikoje esančius terminus ir žodyną, kad audituojamajam subjektui būtų aiškus turinys.

229. Audito kriterijų formulavimui gali būti naudojamos ir IT valdymo reikalavimus nustatančių teisės aktų nuostatos, pvz., kadangi yra nustatytas išsamus kibernetinio saugumo reikalavimų sąrašas, kurį organizacija privalo įgyvendinti, kaip kriterijus gali būti pasirinktas tam tikras reikalavimas, kurio atitiktį svarbu patikrinti. Pasirenkant audito kriterijus reiktų atsižvelgti ir į audituojamojo naudojamas, savo veikloje įdiegtas IT gerąsias praktikas, pvz., ITIL (angl. *Information Technology Infrastructure Library*)[31], ISO ar kitus standartus.

230. Jeigu auditoriai neranda pagrįstų, objektyvių, suprantamų ir tinkamų audito kriterijų arba nėra tikri kurią gerosios praktikos (standartų) sistemą taikyti, jie turėtų klausti tos srities ekspertų, prašyti atsakyti į klausimus: koks idealus audito kriterijus galėtų būti esant nepriekaištingoms sąlygoms konkrečioje srityje, kiek jis atitinka racionalumo reikalavimus

[31] ITIL – tai paslaugų valdymo teorija, orientuota į darbo optimizavimą bei kokybės užtikrinimą IT paslaugas teikiančiose struktūrose. Ši teorija paremta knygų rinkiniu, kuriame sukaupta ir apibendrinta pasiteisinusi IT valdymo praktika.

ir geriausią žinomą ir galimą palyginti praktiką. Kita alternatyva, siekiant apibrėžti ir pagrįsti patikimus ir realius kriterijus, – diskusijos su suinteresuotomis institucijomis. Ekspertų ir kitų institucijų atsakymus auditorius turėtų vertinti pats, remdamasis savo profesine kompetencija.

231. Jeigu auditorius taiko audituojamo subjekto nustatytus veiklos kriterijus ar standartus, jis turi išlikti atsargus. Tokių standartų laikymasis nebūtinai reiškia veiksmingą IT valdymą, todėl auditorius turi nepamiršti, jog subjektas gali nustatyti nepagrįstai žemus standartus, kad tikrai galėtų juos įvykdyti.

232. Audito kriterijai gali būti kokybiniai arba kiekybiniai:

- ✓ kiekybiniai, kurie skaitine išraiška rodo, kiek buvo pasiekta, vertina atitiktį tam tikrai skaitinei reikšmei ir pan. (pvz., ne mažiau nei 95 proc. IT projektų įgyvendinta laiku; 100 proc. kritinių incidentų sprendžiama pagal numatytus terminus ir pan.). Jie gali būti absoliutūs ar santykiniai;
- ✓ kokybiniai, kurie rodo kaip buvo teikiami produktai (paslaugos) (pvz., kiek patogu naudotis skurta taikomąja programa, ar IS naudotojai patenkinti teikiamomis paslaugomis, IS pateikiamos informacijos aiškumas).

233. Audito metu rekomenduojama nustatyti ne tik kiekybinius, bet ir kokybinius kriterijus.

234. Audito kriterijai gali būti orientuoti į tai:

- ✓ *ko tikimasi*, atsižvelgiant į pagrįstus principus, mokslines žinias ir gerąją praktiką;
- ✓ *kaip galėtų būti*, jei sąlygos būtų geresnės arba
- ✓ *kaip turėtų būti* pagal įstatymus, teisės aktus ar tikslus.

235. Auditorius audito kriterijams turi nustatyti (kai įmanoma) vertinimo skales, kurių reikšmės parodytų, kokia IT valdymo būklė yra netinkama, tinkama arba vertintina kaip gerosios praktikos pavyzdys. Auditorius turėtų nustatyti ne tik kriterijaus vertinimo skales, bet ir tolerancijos ribas (kai įmanoma ir tikslinga), kurios leistų objektyviai vertinti, ar nustatytas nuokrypis yra reikšmingas. Tolerancijos ribos apibrėžia priimtiną veiklos rezultatų ar procesų nukrypimo nuo nustatytų standartų ar normų lygį, kuris dar laikomas tinkamu ir nesukelia reikšmingų rizikų ar neigiamų pasekmių. Tolerancijos ribos yra naudingos, kai tam tikri nedideli neatitikimai neturi esminės įtakos veiklos rezultatams ir leidžia išvengti neigiamo vertinimo, kai nuokrypiai nereikšmingi.

236. Tinkami audito kriterijai, susiję su teisėtumu ar tinkamumu, turi būti:

- ✓ *objektyvūs*: pasirenkami tokie kriterijai, kurių niekaip negali paveikti auditoriaus ar audituojamo subjekto šališkumas, subjektyvios nuomonės. Jais vadovaudamiesi audito faktus vertinantys asmenys (audituojamas subjektas, audito grupė, vadovai ar kt.) suformuluos tokias pat audito išvadas;
- ✓ *aktualūs*: šie kriterijai kyla iš audito objekto informacijos, kuri padeda numatomam (-iems) naudotojui (-iems) priimti sprendimus, yra svarbūs ir loginiais arba priežastiniais ryšiais susiję su audito tikslu, sritimi, rizikomis ar klausimais;
- ✓ *išsamūs*: kriterijai būna išsamūs, kai audito objekto informacijoje, parengtoje pagal šiuos kriterijus, nėra praleista svarbių veiksnių, kurie, galėtų paveikti

numatomo (-ų) naudotojo (-ų) sprendimus. Tai reiškia, kad audito metu turi būti pasirinkta tiek reikšmingų ir tokių audito kriterijų, kad būtų galima atsakyti į audito klausimus ir pasiekti audito tikslą. Jie apima visus svarbius veiksnius ir yra prasmingi;

- ✓ *patikimi*: šie kriterijai leidžia padaryti nuoseklias išvadas, t. y., kitas auditorius, tokiomis pat aplinkybėmis naudojantis patikimus kriterijus, prieina prie tų pačių išvadų. Jie turi būti gauti ar sudaryti (išvestiniai) iš oficialių šaltinių;
- ✓ *suprantami*: šie kriterijai leidžia įvertinti audito objekto informaciją, kurią gali suprasti numatomas (-i) naudotojas (-ai). Suprantami audito kriterijai yra aiškiai suformuluoti (išreikšti aiškiais, visiems suprantamais, priimtinais dydžiais ir sąvokomis, nedviprasmiški), suvokiami numatytiems naudotojams ir padeda suformuluoti aiškias išvadas. Jų negalima interpretuoti įvairiais skirtingais būdais;
- ✓ *naudingi*: šie kriterijai lemia rezultatus ir išvadas, kurios atitinka naudotojo (-ų) informacijos poreikius;
- ✓ *palyginami*: šie kriterijai atitinka kriterijus, kurie yra naudojami kitų panašių agentūrų atitikties audituose ar veiklose ir kurie buvo naudojami audituojamo subjekto ankstesniuose atitikties audituose;
- ✓ *priimtini*: dėl šių kriterijų paprastai susitaria nepriklausomi šios srities ekspertai, audituojami subjektai, įstatymų leidėjas, žiniasklaida ir plačioji visuomenė;
- ✓ *prieinami*: kriterijai, kurie yra prieinami numatomam (-iems) naudotojui (-ams) taip, kad jie galėtų suprasti atlikto audito darbo pobūdį ir audito ataskaitos pagrindą.

237. Audito kriterijai formuluojami išankstinio tyrimo metu surinkus pakankamai informacijos apie nagrinėjamą sritį, audituojamo subjekto aplinką, pasirinkus rizikas ir suformulavus audito klausimus. Šių kriterijų tinkamumui įtaką gali daryti pagrindinio tyrimo metu gauti duomenys. Atsižvelgiant į juos, kriterijai gali būti tikslinami. Audito kriterijai nurodomi audito plane. Paprastai jie formuluojami žemiausio lygmens audito klausimams.

238. *Audito kriterijų aptarimas su audituojamu subjektu*. Audituojamas subjektas turi žinoti, kokiais standartais remdamasi audito grupė vertina jo vykdomą veiklą, todėl visi audito kriterijai (ir juos patikslinus audito metu) turi būti aptarti su audituojamo subjekto atstovais (susitikimų, susirašinėjimo su jais metu). Tai ypač svarbu, kai audito kriterijai nėra tiesiogiai nustatyti įstatymų ar kitų oficialių dokumentų, kai jie nėra akivaizdūs ir gali kelti ginčų su audituojamu subjektu ir kai yra nustatomi bei tobulinami atliekant auditą. Taip galima nustatyti dėl kriterijų kylančius nesutarimus, juos aptarti ir, tikėtina, įveikti šiuos nesutarimus ankstyvame etape. Aptariant kriterijus svarbu, kad auditorius išklausytų audituojamo subjekto argumentus, bet nepamirštų, kad subjektas gali siekti nuslėpti trūkumus. Audito kriterijai turi būti aptarti su audituojamu (-ais) subjektu (-ais) iki audito plano patvirtinimo.

239. Jeigu audituojamas subjektas nesutinka su planuojamais taikyti audito kriterijais, kyla rizika, kad nepripažins ir audito metu nustatytų faktų, vertinimo ir išvadų turinio. Tokiu atveju auditorius turi papildomais argumentais sustiprinti konkrečių audito kriterijų tinkamumą ir argumentuoti jų parinkimą, nurodydamas subjekto nuomonę ir argumentus, kodėl jis nesutinka. Nesutarimas tarp audituojamo subjekto ir audito grupės dėl audito kriterijų pasirinkimo nėra pagrindas auditoriams atsisakyti savo pozicijos šių kriterijų atžvilgiu. Esant nesutarimui, auditoriai turėtų šį faktą ir savo bei audituojamo subjekto

nuomonę ir argumentus pateikti darbo dokumente, o audito procese jų pagrindimui skirti daugiau dėmesio. Ginčo atveju rekomenduojama gauti vidaus ir (ar) išorės eksperto nuomonę. Galutinį sprendimą dėl kriterijų nustatymo priima auditorius, todėl svarbu, kad jis išliktų nepriklausomas šio proceso metu.

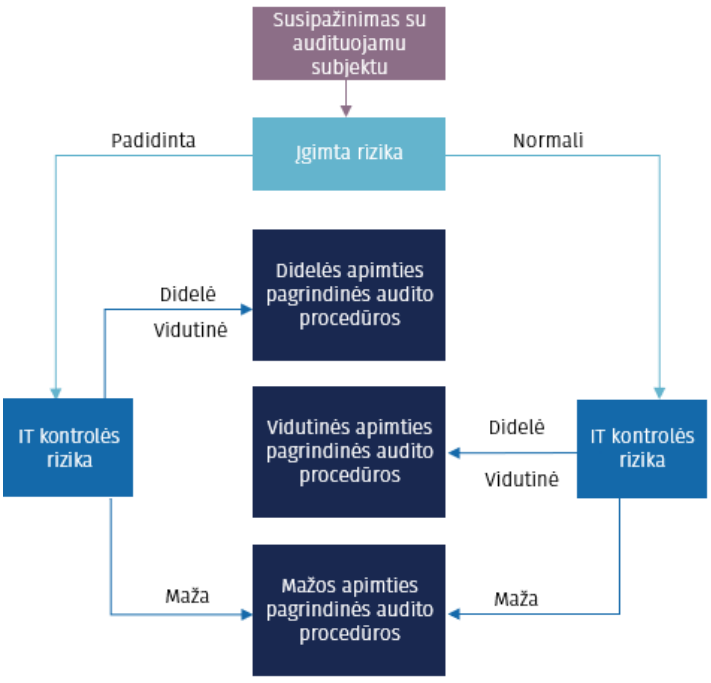
4.1.10.2. Audito procedūros, informacijos ir duomenų šaltiniai bei metodai

Susiję TAAIS reikalavimai
Planuodamas auditą, auditorius privalo suplanuoti audito procedūras, kurių bus laikomasi renkant pakankamus ir tinkamus audito įrodymus, skirtus audito tikslui pasiekti ir atsakyti į audito klausimą (-us). *(3000-ojo TAAIS 101 punktas)*

240. Tam, kad surinktų tinkamų ir pakankamų audito įrodymų kiekvienam numatytam audito kriterijui įvertinti ir atsakytų į audito klausimus, auditorius turi suplanuoti ir audito plane pateikti reikiamas audito procedūras. Jos paprastai planuojamos atskirai kiekvienam audito kriterijui. Jeigu konkreti procedūra suteikia galimybę gauti įrodymų keliems audito kriterijams, tai nurodoma audito plane ir darbo dokumentuose. Kiekvienai audito procedūrai atlikti reikalinga informacija ir (ar) duomenys gaunami, apdorojami ir vertinami taikant jai tinkamiausius metodus. Audito plane reikia prie kiekvienos suplanuotos audito procedūros nurodyti reikalingus informacijos ir (ar) duomenų šaltinius ir planuojamus taikyti metodus.

241. Audito procedūrų apimtis IT audite paprastai nustatoma remiantis rizikos vertinimu. Įvertinus audito rizikos lygį, auditorius priima sprendimą dėl audito procedūrų, kurios turės būti atliktos pagrindinio tyrimo metu. Auditoriai priimdami sprendimą, kokios apimties audito procedūras būtina atlikti (didelės, vidutinės ar mažos, įskaitant ir detaliuosius testus), vadovaujasi 8 pav. pateikta schema.

8 pav. Atliekamų audito procedūrų apimties schema



242. Pagal 5100-ąjį GUID, atsižvelgus į audito tikslą, auditoriui gali būti svarbu IT kontrolės priemonių:

- ✓ *Kūrimas*. Šiuo atveju auditorius vertina IT kontrolės priemonių dizainą, ar jis yra tinkamas. Kai auditorių domina IT kontrolės priemonių kūrimas (dizainas), gali pakakti pokalbio arba dokumentais pagrįstų veiklos taisyklių patikrinimo. Siekiant įvertinti, ar organizacijos IT kontrolės priemonių kūrimas (dizainas) tinkamas, rekomenduojama vadovautis COBIT metodikoje pateikiamu procesų informaciniu modeliu, IT procesu aprašymais, kuriuos galima palyginti su organizacijoje egzistuojančia IT valdymo architektūra. Auditoriaus profesiniu sprendimu gali būti naudojama ir kita visuotinai pripažinta geroji praktika (pvz., ISO, ITIL). Vertinant IT kontrolės priemones per kūrimo prizmę, vertinami atitikties tam tikriems reikalavimams aspektai.

- ✓ *Įgyvendinimas*. Šiuo atveju auditorius vertina, ar nustatytos IT kontrolės priemonės (kai jos tinkamai sukurtos) yra įgyvendinamos praktikoje taip kaip numatyta, visa apimtimi ir nuosekliai per visą reikiamą laikotarpį. Tikrinant IT kontrolės priemonių įgyvendinimą pokalbio gali nepakakti – gali prireikti atlikti „ėjimo per sistemą“ testą arba duomenų analizę, kad būtų galima pagrįsti, jog sukurtos IT kontrolės priemonės buvo tinkamai įgyvendintos. Jei organizacijos IT kontrolės priemonių dizainu pasitikėti negalima (jis turi svarbių trūkumų (pažeidžiamumų), neatitinka teisės aktų reikalavimų, pan.), rekomenduojama įgyvendinimo vertinimą atlikti remiantis minėtos pasirinktos gerosios praktikos reikalavimais. Vertinant kaip įgyvendinamos IT kontrolės priemonės, vertinami tiek atitikties, tiek 3 E aspektai.

- ✓ *Veiksmingumas*. Šiuo atveju auditoriaus vertinimas yra dar gilesnis ir renkami įrodymai, ar pasiekti kokybiški proceso rezultatai, atsižvelgiant į atitinkamą IT kontrolės priemonės tikslą. Atsižvelgiant į audito tikslus, gali būti vertinamas IT kontrolės priemonės proceso efektyvumas, t. y., ar jį galima padaryti dar efektyvesnį optimizuojant veiksmus, siekiant sinergijos su kitais kontrolės mechanizmais ir persvarstyti prevencijos, aptikimo ir koregavimo pusiausvyrą. Vertinant IT kontrolės priemones per veiksmingumo prizmę, audito metu vertinami 3 E aspektai.

243. Didelės apimties pagrindinės IT audito procedūros gali apimti visus tris vertinimo lygius – IT kontrolės priemonių kūrimo, įgyvendinimo ir efektyvumo, vidutinės apimties – kelis šių lygių, o mažos – vieną. Jei vertinant IT bendrosios kontrolės priemonių kūrimą nustatyta, kad jų dizainas blogai sukurtas (pvz., nėra esminių kontrolės priemonių, kontrolės sistema turi daug neapibrėžtumų, daugumoje atvejų neatitinka gerosios praktikos), veiksmingumo vertinimo rekomenduojama neatlikti, kol nebus pašalinti nustatyti trūkumai, priešingu atveju gali būti neracionalu ar netikslinga vertinti jų veiksmingumą. Atlikdami didelės ar vidutinės apimties procedūras auditoriai gali priimti sprendimą pagrindinio tyrimo metu atlikti IT bendrosios kontrolės gebos vertinimą pagal COBIT metodiką.

244. Jei atlikus rizikos vertinimą nustatoma, kad IT bendrosios kontrolės rizika didelė ar vidutinė, rekomenduojama pagrindinio tyrimo metu, atsižvelgiant į audito tikslą, atsirinkti ir atlikti ir tam tikrų taikomųjų programų, kurios labiausiai pažeidžiamos dėl IT bendrosios kontrolės trūkumų ir turi neigiamą poveikį duomenų prieinamumui, vientisumui ir konfidencialumui, kontrolės priemonių detaliuosius testus. Dėl detaliųjų testų apimties žr. žemiau „Atrankos atlikimas“.

245. Jei audito objektas (nustatytas strateginio tyrimo metu) yra taikomųjų programų kontrolės priemonės (informacinė sistema), pagrindinės audito procedūros turi apimti IT bendrosios kontrolės priemonių testus, nes ši kontrolė tiesiogiai daro įtaką taikomosios programos kontrolės priemonių pakankamumui ir patikimumui. Tokiais atvejais IT bendrosios kontrolės priemonių vertinimo ir taikomosios programos kontrolės priemonių vertinimo procedūrų apimtis pasirenkamos atsižvelgiant į Vadovo 241 p. nurodytą schemą pagal jų rizikos įvertinimo rezultatus ir 4.1.10.3 skirsnyje pateikiamas nuostatas dėl atrankos atlikimo.

246. Informacija apie duomenų šaltinius paprastai surenkama išankstinio tyrimo metu, kai vyksta susipažinimas su audituojama sritimi, audituojamo subjekto veikla ir IT valdymu. Rengdamas audito planą auditorius turi suprasti kokių papildomų duomenų ir informacijos reikės gauti pagrindinio tyrimo metu, siekiant atlikti pagrindines audito procedūras (detaliuosius testus). Apie duomenų šaltinius plačiau pateikta Vadovo 4.1.4 skirsnyje.

247. Audito procedūros atliekamos naudojant informacijos ir duomenų rinkimo ir vertinimo metodus, kurie išsamiau pateikti Metodikos svetainės Audito metodų skiltyje. Atliekant taikomųjų programų testus be šių procedūrų ir metodų gali būti naudojami specifiniai metodai, kuriuos praktikoje naudoja programinės įrangos testuotojai (pvz.: sprendimų medis, ribinių verčių analizė, naudojimo atvejų testavimas, klaidų spėjimas, tiriamasis testavimas, kt.)[32]. Apie taikomųjų programų kontrolės priemonių testavimą žr. plačiau Vadovo 5 priede.

248. Pagrindinio tyrimo metu dažnai atsiranda keblumų gaunant ir įvertinant reikalingus duomenis ir informaciją, todėl išankstinio tyrimo metu rekomenduojama išbandyti duomenų ir informacijos rinkimo ir vertinimo metodus, siekiant įsitikinti, kad juos bus įmanoma taikyti pagrindinio tyrimo metu ir gauti būtinų įrodymų, atsakyti į audito klausimus. Šis pratimas reikalingas ne tik tam, kad auditorius geriau susipažintų su audituojamos srities informacija, bet ir tam, kad būtų maksimaliai išvengta situacijos, kai audito plane suplanuotų procedūrų negalės atlikti pagrindinio tyrimo metu (pvz., dėl to, kad tokių duomenų, kurie būtų reikalingi audito kriterijui įvertini, audituojamieji nekaupia ir pan.).

249. Praktinės problemos, susijusios su išlaidomis ir galimybe surinkti duomenis, gali apriboti tam tikrų metodų pasirinkimą. Tokiu atveju auditorius turi suplanuoti alternatyvias procedūras, kurios leistų gauti tinkamų ir pakankamų įrodymų arba spręsti dėl konkretaus audito klausimo, kriterijaus tikslinimo ar atsisakymo.

250. Auditorius pasirenka tinkamiausią audito procedūrą ir metodą, kad galėtų sumažinti įvertintą audito riziką iki priimtinai mažo lygio. Rinkdamasis procedūras ir metodus auditorius turėtų vadovautis savo profesine nuovoka, atsižvelgdamas į IT kontrolės priemonių vertinimo rezultatus, IT kontrolės rizikos lygį, testavimo tikslus, populiacijos pobūdį. Bet kurio šių metodų naudojimas neturi paveikti audituojamo subjekto taikomųjų programų sistemos ir jos duomenų vientisumo. Audito metu esant poreikiui gali būti naudojamos ir kompiuterizuotos audito priemonės (CAAT) (žr. Vadovo 4 priede).

251. Auditorius, priklausomai nuo nagrinėjamo klausimo, gali atlikti pagrindines procedūras:

- ✓ tam tikrą dieną (tam tikru laiko momentu) – auditorius tik surenka audito įrodymus, kad tuo metu IT kontrolės priemonės buvo pakankamos ir patikimos. Pvz., toks vertinimas gali būti atliekamas kai svarbu įvertinti aktualiausią IT bendrosios

[32] Programinės įrangos testavimo metodus žr.: ISO/IEEC/IEEE 29119–4:2021 Programinės įrangos ir sistemų inžinerija – Programinės įrangos testavimas – 4 dalis: Bandymo metodai.

kontrolės ir (ar) taikomosios programos kontrolės priemonių būklę ir nėra aktualu vertinti istorinės informacijos;

- ✓ per visą laikotarpį – auditorius surenka audito įrodymus, kad IT kontrolės priemonės buvo pakankamos ir patikimos svarbiais audituojamojo laikotarpio tarpsniais. Pvz., finansų audito metu gali būti aktualu įvertinti tai, kaip IT kontrolės priemonės veikė visą audituojamą laikotarpį ir ar jomis galima pasitikėti, arba IT audito metu svarbu įvertinti tai, kokia incidentų registravimo ir jų sprendimo dinamika buvo 2–3 metų laikotarpiu;

- ✓ tarpiniu laikotarpiu (prieš jo pabaigą) – auditorius surenka audito įrodymus apie IT kontrolės priemonių pakankamumą ir patikimumą laikotarpiui nesibaigus. Audito procedūras atliekant prieš laikotarpio pabaigą, gali būti lengviau nustatyti rimtas problemas ankstyvoje audito stadijoje, taigi ir išspręsti jas vadovybei padedant arba parengti veiksmingą audito metodą joms spręsti. Tokiais atvejais auditorius turėtų gauti papildomų įrodymų dėl likusio laikotarpio.

252. Testuojant IT kontrolės priemonių veikimą per ilgesnį laikotarpį svarbu atkreipti dėmesį į tai, ar per šį laikotarpį IT valdyme nebuvo esminių pasikeitimų ir ar seniau veikusi sistema bus aktuali išvadoms pateikti.

253. Turėtų būti parengtos išsamios, tarpusavyje nesidubliuojančios ir viena kitą papildančios audito procedūros ir metodai, kurie audito plane turi būti aiškiai aprašyti. Visi audito procedūras atliekantys auditoriai turėtų suprasti, kaip kiekvienas atskiras klausimas ir numatytos audito procedūros yra susijusios su audito tikslu.

254. Siekiant ištestuoti IT bendrąją ir (ar) taikomųjų programų kontrolės priemones, auditorius atsižvelgęs į išankstinio tyrimo metu surinktą informaciją ir nustatytas rizikas turėtų parengti šių kontrolės priemonių testavimo klausimynus.

4.1.10.3. Atrankos atlikimas

Susiję TAAIS reikalavimai
Auditorius privalo naudoti audito atranką, kai tai tinkama, kad pateiktų faktų kiekį, pakankamą daryti išvadas apie tiriamą visumą, iš kurios buvo atlikta atranka. Planuodamas audito atranką, auditorius privalo atsižvelgti į audito procedūros tikslą ir tiriamos visumos, iš kurios bus padaryta atranka, charakteristikas. *(4000-ojo TAAIS 172 punktas)*

255. Audito plano rengimo metu auditorius turi apsispręsti, kokią dalį tiriamosios visumos audituoti ir, jeigu nuspręsta audituoti mažiau nei visą (100 proc.), atlikti pačią atranką. Paprastai audite galima:

- ✓ pasirinkti tikrinti visus vienetus – tai visos (100 proc.) tiriamosios visumos tikrinimas. Šis metodas tinkamas, kai vienetų skaičius yra nedidelis, o vertė – didelė; rizika buvo įvertinta kaip reikšminga arba kompiuterizuotos audito priemonės (CAAT) leidžia efektyviai patikrinti visus vienetus;

- ✓ atlikti atranką – tai audito procedūrų atlikimas mažiau kaip 100 proc. audito objektui ar sričiai svarbios tiriamosios visumos vienetų. Atrankai atlikti gali būti taikoma:

- Statistinė atranka – tai duomenų atrinkimas ir įvertinimas, siekiant pateikti išvadą apie visumą, remiantis tikimybių teorijos dėsniais. Atliekant ją, imties vienetai (pvz., projektai, sutartys, respondentai ir kt.) turi būti atrinkti taip, kad kiekvienas atrankos vienetas iš visumos turėtų galimybę būti atrinktas (patekti į imtį). Tik atlikęs statistinę atranką auditorius galės gauti užtikrinimą dėl visos tiriamosios visumos.

- Nestatistinė atranka – tai tam tikrų imties vienetų atrinkimas iš visumos, priklausantis nuo auditoriaus profesinio sprendimo. Šis metodas gali būti taikomas, kai norima atsirinkti elementus dėl jų specifinių savybių, pvz., tai gali būti didelės vertės ar rizikos objektai. Tai efektyvus audito įrodymų rinkimo metodas, bet nėra statistinė atranka, todėl rezultatų negalima pritaikyti visai populiacijai.

- Statistinės ir nestatistinės atrankos kombinacija – tai kelių etapų atranka, kai tam tikri reikšmingiausi elementai (pvz., didžiausi, rizikingiausi ir kt.) atrenkami profesiniu sprendimu, o likusiems elementams taikoma statistinė atranka.

256. Rekomenduojame taikyti statistinę atranką arba statistinės atrankos ir aukštos vertės elementų 100 proc. testavimo kombinaciją, nes tik šie metodai garantuoja rezultatų reprezentatyvumą ir apskaičiuojamą rezultatų paklaidą.

Atrankos procesas

257. Pagrindiniai atrankos etapai:

1. *Atrankos tikslo nustatymas.* Auditorius turi nuspręsti, ar atrankos tikslas yra gauti objektyvius ir visą populiaciją apibendrinančius rezultatus, ar gauti specifinę informaciją apie tam tikrą grupę ar reiškinį, kuri nėra skirta atspindėti visos populiacijos. Atrankos tikslas nurodomas darbo dokumentuose.

2. *Tiriamos visumos nustatymas.* Atliekant atranką reikia žinoti, kokia yra tiriamoji visuma ir koks jos dydis.

3. *Tiriamosios visumos suskaidymas.* Atrankai vykdyti visada geriau turėti kuo labiau homogenišką (vienalytę) tiriamąją visumą. Kai visuma palyginti nevienoda, rekomenduotina įvertinti galimybę ją suskaidyti į mažesnes dalis. Pavyzdžiui, jeigu turima duomenų visuma apima visų audituojamu laikotarpiu incidentų pavadinimus, kiekius ir kainas, auditoriui gali būti naudinga turimą duomenų visumą suskirstyti į mažesnes grupes (pvz., saugos incidentai ir kiti incidentai), kurios nagrinėjamos atskirai – taip gaunamos tikslesnės įžvalgos. Kriterijai, pagal kuriuos skaidytume, gali būti labai įvairūs ir priklauso nuo nagrinėjimo audito klausimo ir kriterijaus: pvz., pagal tam tikras logines grupes, vietoves (miestas / kaimas), datas ir pan.

   Skaidyti į mažesnes tiriamas visumas tikslinga ir tada, jei matoma, kad yra labai išsiskirianti tam tikrų elementų grupė, kurią galima būtų nagrinėti 100 proc. ar kitu profesiniu sprendimu pasirinktu metodu. Likusia tiriamąja visuma šiuo atveju laikomi visi likę vienetai ir šiai visumos daliai taikomas tinkamiausias atrankos metodas. Jeigu tiriamoji visuma buvo suskaidyta, darbo dokumentuose reikia nurodyti, kaip ir kodėl ji buvo suskaidyta į mažesnes dalis.

4. *Atrankos būdo ir metodo pasirinkimas.* Kaip pateikta pirmiau, atrankos būdas gali būti statistinis, nestatistinis arba kombinuotas. Statistinė ir nestatistinė atranka gali būti atliekama taikant įvairius metodus. Tinkamiausias būdas ir metodas parenkamas atsižvelgiant į tiriamą visumą ir atrankos tikslą. Nuo tikslo daugiausiai priklauso jos būdo pasirinkimas, o nuo turimų duomenų (elektroniniai ar popieriniai, homogeniški ar ne ir pan.) – atrankos metodo pasirinkimas. Norint gauti užtikrinimą dėl visos tiriamosios visumos, reikia taikyti statistinius atrankos metodus. Kitais atvejais gali būti tinkami ir nestatistiniai atrankos metodai. Darbo dokumentuose reikia nurodyti pasirinktą atrankos būdą (statistinė ar nestatistinė) ir metodą (-us). Jei pasirenkamas nestatistinis atrankos būdas, šis pasirinkimas turi būti papildomai argumentuotas. Atrankos metodai išsamiau pateikti Metodikos svetainės Atrankos skiltyje.

5. *Imties dydžio nustatymas.* Nuo imties dydžio priklauso tyrimų rezultatų reprezentatyvumas ir paklaida. Kuo didesnė imtis, tuo mažesnė rezultatų paklaida ir tikslesnės tyrimo išvados, ir atvirkščiai – kuo mažesnė imtis, tuo didesnė rezultatų paklaida ir mažiau tikslios tyrimo išvados. Darbo dokumentuose nurodoma, kaip ir kodėl buvo pasirinktas tam tikras imties dydis, kokią dalį tiriamosios visumos sudaro imtis procentais, jeigu jos dydis nebuvo skaičiuojamas taikant imties dydžio nustatymo formulę. Esant galimybei galima nurodyti imties procentą ir pagal vertę. Atrankos vienetai gali būti piniginiai arba fiziniai vienetai (pvz.: IT projektai, incidentai, IT rizikos, IT problemos, ūkinės operacijos ir pan.).

6. *Imties vienetų atrinkimas.* Taikant pasirinktą atrankos būdą ir metodą iš visumos (populiacijos) atrenkami konkretūs vienetai testavimui. Darbo dokumentuose nurodoma, kaip buvo atrinkti konkretūs vienetai (pvz., sisteminėje atrankoje kiekvienas n-asis vienetas pradedant nuo x-ojo vieneto).

7. *Reikiamų audito procedūrų su atrinktais vienetais atlikimas ir rezultatų apibendrinimas.* Atlikus reikiamas procedūras, turi būti apibendrinami rezultatai, kurie pateikiami darbo dokumentuose. Jeigu buvo taikyta statistinė atranka, auditorius įvertina nustatytus nuokrypius ir priima profesinį sprendimą dėl jų pritaikymo visumai, iš kurios testuotas vienetas buvo atrinktas. Šis atrankos rezultatų vertinimo būdas vadinamas klaidų ekstrapoliavimo į visumą būdu. Ekstrapoliavimo būdai išsamiau pateikti Metodikos svetainės Atrankos skiltyje.

258. Audito planavimo metu turi būti atlikti atrankos proceso 1–5 etapai, nurodyti pastraipoje aukščiau ir reikiama informacija (tiriamoji visuma ir jos dydis, atrankos būdas ir metodas, imties dydis) pateikta audito plane. Atkreipiame dėmesį, kad audito plane nurodyti planuojamą atrankos būdą ir imties dydį svarbu, nes ši informacija būtina procedūroms suplanuoti ir jų atlikimui reikalingiems ištekliams įvertinti (kiek reikės žmonių ir kiek darbo dienų konkrečiai procedūrai atlikti). 6 etapas „Imties vienetų atrinkimas“ planavimo metu atliekamas, jeigu turimos reikiamos tiriamosios visumos.

259. Jeigu auditorius neturi galimybės planavimo etape atlikti 3–6 atrankos etapų (pvz.: surinkus naujausius duomenis laukiama, kol subjektas audituojamas; į audito planą įtraukiami nauji audituojami subjektai ir duomenų bus prašoma pagrindinio tyrimo metu; audituojamieji negalėjo pateikti duomenų, nes jie laikomi decentralizuotai popierinėse bylose ir nėra apyrašų, iš kurių galima atlikti atranką ir pan.), audito plane nurodomos priežastys, kodėl atrankos atlikti negalima ir kad ji bus atliekama pagrindinio tyrimo metu. Šiuo atveju audito plane taip pat turi būti įvardijama, ką laikysime tiriamąja visuma.

260. Tik išskirtiniais atvejais, kai rengiant audito planą neturima jokios informacijos apie planuojamą tiriamą visumą (ir jos nebuvo galima gauti išankstinio tyrimo metu), plane galima nenurodyti imties dydžio, nurodant, kad jis bus apskaičiuojamas gavus reikiamus duomenis.

261. Atrankos darbo dokumento pavyzdinį šabloną galima rasti kompiuterio *MS Word* šablonų skiltyje. Detaliau kaip jį pildyti pateikta *Atrankos darbo dokumento pildymo instrukcijoje*, kuri pateikta Metodikos svetainės Šablonų skiltyje.

Imties dydžio nustatymas

262. Audito išankstinio tyrimo etape, remiantis 8 pav. pateikta audito procedūrų apimties schema, įvertinus įgimtą ir IT kontrolės priemonių patikimumą, reikia nustatyti, kokios apimties audito procedūros bus atliekamos.

263. Imties dydis IT bendrosios kontrolės testams (kai tiriamoji visuma mažiau negu 300 vienetų) nustatomas atsižvelgiant į tiriamąją visumą ir įgimtos rizikos vertinimą (2 lentelė):

2 lentelė. Minimalus imties dydis IT bendrosios kontrolės testams

Tiriamoji visuma	Įgimta rizika	IT kontrolės priemonės testų imties dydis
1	Padidinta	1
	Normali	
2-4	Padidinta	2
	Normali	
5-12	Padidinta	2-5
	Normali	
13-52	Padidinta	15
	Normali	5
53-250	Padidinta	40
	Normali	20
>250	Padidinta	60
	Normali	25

264. Kai tiriamoji visuma 300 vienetų ir daugiau, imties dydis apskaičiuojamas naudojantis pateikta imties dydžio nustatymo formule. Ji parengta su dažniausiai taikomu 95 proc. patikimumo ir 5 proc. paklaidos lygiu.

Imties dydis = tiriamoji visuma * 384,16 / (tiriamoji visuma + 383,16)

265. Jeigu yra poreikis taikyti kitus patikimumo ir paklaidos lygius, imties dydį galima apskaičiuoti vadovaujantis rekomenduojamomis internete pateikiamomis skaičiuoklėmis (pavyzdžiai pateikti Metodikos svetainės Tvarkų ir kitos informacijos skiltyje).

266. Jeigu atranka atliekama dviem etapais, imties dydis didinamas 20 proc. Kaip atlikti dviejų etapų atranką išsamiau žr. Metodikos svetainės Atrankos skiltyje.

267. Nusprendus atlikti taikomųjų programų kontrolės priemonių testavimą yra atliekami detalieji testai. Tokiais atvejais pasirenkant imties dydį reikia atsižvelgti į tai, ar taikomosios kontrolės priemonės rankinės (kai darbuotojas fiziškai atlieka tikrinimo veiksmus, pvz., sulygina suvestą informaciją IS su dokumentais) ar automatizuotos (žmogaus veiksmų nėra, tikrinimus atlieka IS pagal įdiegtą funkciją) ir koks yra taikomųjų kontrolės priemonių vykdymo dažnumas.

268. ISACA leidinyje „COBIT ir aplikacijų kontrolė. Valdymo gidas“[33] rekomenduoja atrinkti daugiau testuojamų vienetų (pavyzdžių), kai kontrolė yra rankinė ir ji atliekama dažniau, o automatizuotomis kontrolės priemonėmis galima atrinkti mažiau pavyzdžių arba taikyti vieno pavyzdžio principą, jei automatizuota kontrolė audituojamu laikotarpiu nesikeitė ir IT bendroji kontrolė organizacijoje veikia efektyviai. Žemiau pateikiami minimalūs imties dydžių pavyzdžiai, kuriuos minėtoje knygoje rekomenduojama pasirinkti testuojant vieną taikomųjų programų kontrolės priemonę (žr. 3 lentelę).

3 lentelė. Minimalus imties dydis IT taikomųjų programų kontrolės priemonių detaliems testams

Kontrolės tipas	Kontrolės suveikimo dažnumas	Minimalus pavyzdžių kiekis
Rankinė	Vieną ar daugiau kartų per dieną	25
Rankinė	Kas savaitę	5
Rankinė	Kas mėnesį	2
Rankinė	Kas ketvirtį	2
Rankinė	Kasmet	1
Automatizuota	1 pavyzdys vienai taikomajai kontrolei su sąlyga, kad IT bendroji kontrolė yra efektyvi.	

Šaltinis – ISACA leidinys „COBIT ir aplikacijų kontrolė. Valdymo gidas“[34].

269. Jei išankstinio tyrimo metu, įvertinus įgimtą riziką ir atlikus IT bendrosios kontrolės testus, nustatyta, kad:

- ✓ įgimta rizika yra padidinta, o IT bendrosios kontrolės rizika yra didelė ar vidutinė, auditorius detaliųjų testų padidina 50 proc. nuo minimalaus pavydžių kiekio, nurodyto 3 lentelėje;
- ✓ įgimta rizika yra normali, o IT kontrolės rizika didelė ar vidutinė, auditorius detaliųjų testų padidina 20 proc. nuo minimalaus pavydžių kiekio, nurodyto 3 lentelėje;
- ✓ įgimta rizika yra padidinta ar normali, o IT bendrosios kontrolės rizika yra maža, auditorius detaliųjų testų kiekį pasirenka pagal 3 lentelėje nurodytą minimalų pavyzdžių kiekį.

270. Detaliųjų testų apimtis taip pat gali priklausyti nuo to, kokius specifinius testavimo metodus planuojama naudoti taikomosios programos funkcijos testavimo atveju (pvz., sprendimų medis, ribinės vertės analizės, kt.)[35] ir nuo to, kiek parametrų ir su jomis susijusių kombinacijų ši programa sukuria atlikdama tam tikrą pasirinktą testuoti funkciją. Pavyzdžiui, pasirinkta testuoti nedarbo išmokos apskaičiavimo funkcija, bet skirtingomis išmokos mokėjimo sąlygomis algoritmas gali apskaičiuoti skirtingą rezultatą, todėl tokiais atvejais reikia ištestuoti visus galimus skaičiavimo variantus ir įsitinkinti, ar funkcija veikia tinkamai.

[33] ISACA leidinys „COBIT ir aplikacijų kontrolė. Valdymo gidas“ (angl. „CobiT and Application Controls: A Management Guide“), 56 psl.

[34] Ten pat.

[35] Programinės įrangos testavimo metodai pateikiami ISO/IEEC/IEEE 29119–4:2021 Programinės įrangos ir sistemų inžinerija – Programinės įrangos testavimas – 4 dalis: Bandymo metodai.

4.1.11. Reikiamų išteklių įvertinimas

271. Išankstinio tyrimo metu reikia įvertinti, kokie ištekliai (žmogiškieji, finansiniai, materialiniai, laiko ir kt.) bus reikalingi pagrindiniam tyrimui atlikti. Turi būti įvertinta ir audito grupės narių kompetencija.

272. Tais atvejais, kai audito grupė neturi reikalingų žinių ar specialių įgūdžių, turi būti apsvarstyta galimybė pasitelkti ekspertų iš pačios AAI. Pvz., gali būti nustatytas poreikis pasitelkti AAI IT auditorius. Gali būti priimtas sprendimas pasinaudoti išorės specialistų (ekspertų) ir (ar) išorės auditorių darbu. Planavimas pasitelkti ir pasinaudoti išorės auditorių, vidaus auditorių ir (ar) išorės specialistų (ekspertų) atliktu darbu ir jų atlikto darbo panaudojimas ir dokumentavimas išsamiau aprašyti Metodikos svetainės Tvarkų ir kitos informacijos skiltyje. Kitų Valstybės kontrolės struktūrinių padalinių darbuotojai, išorės specialistai (ekspertai) ir išorės auditoriai pasitelkiami vadovaujantis *Valstybės kontrolės metinės veiklos planavimo tvarkos aprašu*.

273. Planuojant auditą, reikia įvertinti įvairius veiksnius, turinčius įtakos audito išlaidoms. Pvz., reikia atsižvelgti į tai, kad labai plati ar susijusi su dideliu audito subjektų skaičiumi (jų geografinis paplitimas) audito tema arba brangios išorės specialistų (ekspertų) paslaugos gali pareikalauti didelių finansinių išteklių.

4.1.12. Audito plano rengimas

274. Nusprendus tęsti auditą, rengiamas audito planas (šabloną galima rasti Metodikos svetainės Šablonų skiltyje), kuriame numatomi audito klausimai ir kriterijai, su jais susijusios audito procedūros, leidžiančios surinkti tinkamus ir pakankamus audito įrodymus audito tikslui pasiekti ir kt.

275. Audito planas rengiamas siekiant suplanuoti reikiamus darbus, jų atlikimo terminus, audito kokybės užtikrinimo procedūras, išteklius ir kt. audito tikslui pasiekti. Auditas yra projektas, todėl jam taikomi projektų valdymo principai. Į tai reikia atsižvelgti tiek planuojant audito darbus, tiek juos vykdant, tiek įgyvendinant reikiamus pokyčius projekto įgyvendinimo eigoje.

276. Audito plano parengimas – paskutinis audito planavimo proceso etapas. Audito grupės atsakomybė rengiant audito planą išsamiau aprašyta *Valstybinių auditų kokybės užtikrinimo vadove*.

277. Išankstinio tyrimo metu iki audito plano patvirtinimo su audituojamu subjektu turi būti aptariamos (susitikimuose ir (ar) susirašinėjant su juo) išankstinio tyrimo problemos (rizikos), planuojami audito klausimai, kriterijai, audito apimtis, metodai ir kt. Taip auditoriui bus lengviau nustatyti sritis, kuriose gali kilti nesutarimų, ir suplanuoti, kaip pagrindinio tyrimo metu surinkti papildomų įrodymų. Nesutarimas tarp audituojamo subjekto ir audito grupės dėl kriterijų ar kitų audito plano elementų pasirinkimo nėra pagrindas auditoriams atsisakyti savo pozicijos jų atžvilgiu. Esant nesutarimų, auditoriai turėtų šį faktą ir argumentus pateikti darbo dokumente, o audito procese jų pagrindimui skirti daugiau dėmesio. Ginčo atveju rekomenduojama gauti eksperto nuomonę. Galutinį sprendimą priima auditorius, todėl svarbu, kad jis liktų nepriklausomas šio proceso metu.

Audito plano struktūra

278. Audito planą sudaro šios dalys:

- ✓ *Santrumpos ir sąvokos.* Pateikiamos audito plane vartojamos santrumpos ir sąvokų paaiškinimai (išnašose nurodomi sąvokų paaiškinimo šaltiniai).
- ✓ *Pasirinktos audituoti rizikos.* Šioje dalyje įvardijamos pasirinktos audituoti IT kontrolės rizikos, o jų aprašymas pateikiamas išankstinio tyrimo rezultatų apibendrinime, kuris yra laikomas audito plano priedu. Rizikos priskiriamos tam tikroms IT sritims ar IT procesams ir nurodoma, kokiais aspektais bus vertinama rizika.
- ✓ *Pagrindinė informacija apie auditą*:
  - audito ID, audito objektas, tikslas, audituojamas laikotarpis;
  - audituojamas (-i) subjektas (-ai). Jeigu buvo atlikta audituojamų subjektų atranka pagrindinio tyrimo procedūroms atlikti, šioje dalyje taip pat pateikiama nuoroda į atrankos darbo dokumentą;
  - apribojimai, jeigu yra. Šioje dalyje pateikiami audito objektui, tikslui, apimčiai, metodams ar duomenims taikomi kokie nors apribojimai. Jų gali atsirasti dėl auditoriaus pagrįsto sprendimo nevertinti tam tikrų dalykų, susijusių su audito objektu ir (ar) tikslu, arba dėl audituojamo (-ų) subjekto (-ų) veiksmų ar veiklos, kai nėra galimybės atlikti tam tikrų procedūrų ar gauti tam tikrų duomenų;
  - apibendrintas įgimtos, IT kontrolės rizikos vertinimo rezultatas, t. y. nurodoma, ar įgimta rizika laikoma padidinta ar normali, ar IT kontrolės rizika didelė ar vidutinė ar maža;
  - nustatytas kiekybinis ir (ar) kokybinis reikšmingumas, t. y. koks reikšmingumas buvo taikomas ir pasirinkti atitinkamo reikšmingumo parametrai, sąlygos ir pan.;
  - audito valdymo rizika ir jos valdymo priemonės. Kylančios rizikos ir jų valdymo priemonės aptariamos audito grupėje ir dokumentuojamos audito projekte ViPSIS, o audito plane nurodomos pagal poreikį, pavyzdžiui, jei dėl nustatytos rizikos reikšmingumo auditorius suplanuoja atitinkamas procedūras audito plane;
  - pasitelkiami Valstybės kontrolės darbuotojai, turintys specialiųjų žinių, ir (ar) išorės specialistai (ekspertai) ir (ar) išorės auditoriai. Išsamiau šio vadovo 2.8 poskyryje „Audito grupės įgūdžiai“;
  - vidinę peržiūrą atliekantys asmenys ir peržiūros terminai ar periodiškumas.
- ✓ *Audito klausimai, kriterijai, procedūros, informacijos šaltiniai, metodai, atsakingi asmenys ir terminai.* Nurodomi:
  - audito klausimai, į kuriuos reikia atsakyti, norint pasiekti audito tikslą;
  - audito kriterijai ir jų šaltiniai. Jei tam tikri kriterijai neturi formalių šaltinių, audito plane turi būti nurodoma „Audituojamas subjektas pritaria“ ir pateikiama nuoroda į dokumentą, kuriame pateikiami kriterijų aptarimo su audituojamu subjektu rezultatai. Jeigu audituojamas subjektas nepritarė kriterijams, plane nurodoma „Audito subjektas nepritaria“ ir pateikiama nuoroda į dokumentą, kuriame pateikiama auditoriaus papildoma

argumentacija, kodėl nusprendžiama kriterijaus nekeisti. Kiekvienas audito kriterijus ir su juo susijusi informacija pateikiama atskiroje eilutėje;

- informacijos šaltiniai, procedūros ir metodai. Šioje dalyje kiekvienam audito kriterijui reikia aiškiai nurodyti planuojamas atlikti audito procedūras (veiksmus), o prie kiekvienos iš jų – iš kokių šaltinių, kokiuose audituojamuose subjektuose, kokio laikotarpio ir kokie duomenys bus renkami, kokiais metodais bus renkama ir vertinama informacija. Audito grupės vadovas turėtų nuspręsti, kuris audito įrodymų gavimo metodas ar jų derinys bus tinkamas, patikimas ir įrodymų gavimo sąnaudos neviršys jų teikiamos naudos. Kiekviena audito procedūra ir su ja susijusi informacija pateikiama atskiroje eilutėje. Jeigu ta pati procedūra taikoma keliems kriterijams, ji aprašoma prie vieno kriterijaus, o prie kitų teikiama nuoroda į procedūrą. Jeigu procedūros yra labai smulkios ir (ar) jų atlikimo laikas yra trumpas (pvz., kelios dienos), galima procedūrų nenurodyti atskirose eilutėse. Jeigu išankstinio tyrimo metu buvo surinkta dalis arba visa reikiama informacija pagal audito plane numatomą audito kriterijų, plane nereikėtų planuoti jau atliktų procedūrų. Kai surinkta visa reikiama informacija, prie audito kriterijaus reikia nurodyti, kad papildomos audito procedūros nebus atliekamos ir pateikti nuorodą į darbo dokumentą (-us), kuriame informacija dokumentuota. Surinkus dalį reikiamos informacijos nurodoma, kokia buvo surinkta ir suplanuojamos papildomos procedūros trūkstamiems įrodymams surinkti;

- informacija apie atranką. Nurodoma tiriamoji visuma ir jos dydis, kokią dalį tiriamosios visumos planuojama audituoti (ar bus vertinami visi vienetai, ar atlikta jų atranka). Taikant atranką nurodomas jos būdas ir metodas, planuojamas imties dydis ir kas laikoma imties vienetu, pateikiama nuoroda į darbo dokumentą (-us), kur dokumentuota atranka. *Informacijos pateikimo pavyzdys: audito tiriamąją visumą sudaro 1 000 incidentų. Imties dydis – 40 incidentų. Bus taikoma sisteminė atsitiktinė atranka, nuoroda į atrankos darbo dokumentą.*

  Informacija apie atranką pateikiama prie pirmojo audito kriterijaus, kuriam atsakyti bus naudojami atrinktos imties duomenys, prie kitų audito kriterijų, kuriems taikoma ta pati tiriamoji visuma ir imtis, informacijos apie atranką kartoti nereikia – nurodoma, kad atrankos informacija pateikta prie X kriterijaus.

  Jeigu auditorius neturi galimybės atlikti atrankos planavimo etape (pvz., laukiama, kol audituojamas subjektas surinks naujausius duomenis, į audito planą įtraukiami nauji audituojami subjektai ir duomenų bus prašoma pagrindinio tyrimo metu ir pan.), audito plane pateikiamos priežastys, kodėl atrankos atlikti negalima, ir nurodoma, kad ji bus atliekama pagrindinio tyrimo etape. Šiuo atveju audito plane turi būti įvardijama, ką laikysime tiriamąja visuma;

- kiekvienos audito procedūros (užduoties) atlikimo pradžios ir pabaigos terminai, pateikimo vidinei peržiūrai terminas, planuojamas darbo dienų skaičius ir asmenys, atsakingi už konkrečių procedūrų (užduočių) atlikimą. Jeigu vidinę peržiūrą atlieka ne tik audito grupės vadovas, bet ir srities vadovas (-ai), vidinę peržiūrą atliekantis asmuo nurodomas prie atitinkamos procedūros.

Audito procedūrų atlikimo laikas planuojamas nustatant laiką konkretiems darbams atlikti. Apskaičiuojant reikalingą laiką (pvz.: klausimynų sudarymui, susitikimams, pokalbiams ir pan.), rekomenduojama naudotis ankstesnių auditų patirtimi, atsižvelgti ir į laiką, reikalingą komandiruotėms. Procedūrų (užduočių) terminai turi būti kiek įmanoma realesni, nustatyti atsižvelgiant į kitas užduotis, mokymus (jei žinomos datos planavimo metu), atostogas ir pan. Kai kurie darbai tikriausiai remsis kitų darbų rezultatais, todėl jie turi būti atliekami numatyta seka. Reikia numatyti laiką įvairiems aptarimams su audituojamu subjektu, laiką audito kokybės procedūroms užtikrinti.

- ✓ *Planuojami ištekliai.* Pateikiama apibendrinta informacija apie audito grupės narių planuojamą darbo dienų skaičių, informacija apie visas kitas su auditu susijusias papildomas išlaidas: planuojamas komandiruočių, ekspertų pasitelkimo, papildomų paslaugų (pvz., apklausų) įsigijimo ir kitas išlaidas. Reikia įvertinti, kokie ištekliai (žmogiškieji, finansiniai, materialiniai, laiko ir kt.) bus reikalingi auditui atlikti.

- ✓ *Pagrindiniai audito terminai.* Rengiant audito planą, šioje dalyje nurodomi pagrindinio tyrimo audito procedūrų atlikimo pradžios ir audito rezultatų suvestinės patvirtinimo datos, audito ataskaitos projekto pateikimo audituojamam (-iems) subjektui (-ams) data, audito pabaigos data. Pagal poreikį gali būti nurodyti kiti darbai ir suplanuoti jiems terminai.

- ✓ *Laukiamas audito poveikis.* Pateikiamas trumpas aprašymas, kokią tikėtiną naudą audito rezultatai duos tobulinant nagrinėjamą sritį. Aprašytas audito poveikis toliau turi būti detalizuojamas, pateikiant:

  - pokyčių tipą: nurodoma, kokio pokyčio pobūdžio tikimasi;
  - pokyčių vertinimo kiekybinius arba kokybinius rodiklius: pateikiamas jų sąrašas ir, jei yra galimybė, pradinės reikšmės. Šiame etape turėtų būti nustatytas bent vienas pokytį apibūdinantis kiekybinis rodiklis;
  - pokyčių aprašymą: trumpai aprašomas planuojamas (-i) pokytis (-iai).

  Išsamiau apie audito poveikio vertinimą pateikiama *Valstybinio audito poveikio vertinimo metodikoje*.

Audito plano tikslinimas

279. Viso audito metu gavus naujos svarbios informacijos (ar dėl kitų priežasčių), audito planas turi būti patikslintas (pvz.: patikslinti audito klausimai, kriterijai, procedūros, terminai, audito grupės nariai ir kt.).

280. Jeigu audito plane atliekami reikšmingi pakeitimai (pvz.: keičiamas audito tikslas, audito klausimai, kriterijai arba įtraukiami nauji arba išbraukiami audito klausimai, kriterijai, įtraukiami nauji audituojami subjektai, pasikeitė audito grupės nariai, keičiasi audito pabaigos laikas ir kt.), turi būti nurodomos priežastys.

281. Atkreiptinas dėmesys, kad reikšmingus audito plano pakeitimus rekomenduojama suderinti su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis departamentas. Dėl nukreipimo valstybės kontrolieriaus pavaduotojui sprendimą priima audito departamento vadovas.

282. Apie reikšmingus audito plano pakeitimus oficialiu raštu ar el. paštu turi būti informuojamas (-i) audituojamas (-i) subjektas (-ai). Reikšmingi audito plano pakeitimai (pvz., susiję su audito tikslu, klausimais, kriterijais ir pan.) turi būti aptarti su audituojamu (-ais) subjektu (-ais) ne vėliau kaip iki jam pateikiant audito ataskaitos projektą.

4.1.13. Informavimas apie audito planavimo rezultatus

283. Ne vėliau kaip per 2 savaites nuo audito plano patvirtinimo audituojamas subjektas turi būti informuojamas oficialiu raštu ar el. paštu apie:

- ✓ nagrinėtas IT sritis,
- ✓ pasirinktas audituoti rizikingas IT kontrolės priemones,
- ✓ audito tikslą,
- ✓ audito klausimus,
- ✓ pasirinktus audito kriterijus,
- ✓ audituojamus subjektus,
- ✓ audituojamą laikotarpį,
- ✓ laukiamą audito poveikį,
- ✓ kitus, audito grupės narių nuomone, svarbius dalykus.

284. Esant audito grupės ir (ar) audituojamo subjekto poreikiui, turi būti organizuojamas susitikimas audito planavimo rezultatams aptarti. Susitikime paaiškinama, kokios IT sritys buvo nagrinėtos, kokios IT kontrolės priemonės pasirinktos tolesniam vertinimui, nurodomas audito tikslas, klausimai ir pasirinkti kriterijai, audituojami subjektai, laikotarpis, laukiamas audito poveikis ir, esant galimybei, pokyčiai ir juos parodantys rodikliai ir kita, audito grupės narių nuomone, svarbi informacija. Gali būti nuspręsta neteikti tam tikros informacijos apie išankstinio tyrimo rezultatus, jeigu yra rizika, kad jos atskleidimas neigiamai paveiks pagrindinio tyrimo procesą ir (ar) rezultatus.

4.2. Pagrindinis tyrimas

285. Pagrindinio tyrimo tikslas – surinkti pakankamus ir tinkamus audito įrodymus, kuriais remdamasis auditorius galėtų atsakyti į audito klausimus ir pagrįsti audito ataskaitoje pateiktus pastebėjimus, išvadas ir rekomendacijas.

286. Pagrindinis tyrimas yra išankstinio tyrimo tąsa – audito darbai atliekami remiantis parengtu audito planu. Šio plano reikia laikytis atsižvelgiant į numatytus atlikti darbus, išteklius, terminus ir kokybę.

287. Pagrindinio tyrimo metu gavus naujos svarbios informacijos ar susidūrus su problemomis renkant įrodymus gali prireikti patikslinti audito planą. Patartina kuo mažiau reikšmingai jį keisti, išskyrus atvejus, kai tokie pakeitimai būtini. Visi reikiami pakeitimai turi būti fiksuojami laiku, kad, atsižvelgiant į reikiamus pakeitimus, esant poreikiui būtų tinkamai perplanuojami audito grupės narių darbai.

288. Pagrindinis tyrimas pradedamas ViPSIS sistemoje patvirtinus audito planą. Pagrindiniam tyrimui paprastai skiriama apie 40 proc. viso auditui skirto laiko.

4.2.1. Audito procedūrų atlikimas įrodymams surinkti

Audito procedūros

Susiję TAAIS reikalavimai
Auditorius privalo palyginti gautus audito įrodymus su nustatytais audito kriterijais, kad suformuotų audito rezultatus, reikalingus audito išvadai (-oms) parengti. *(4000-ojo TAAIS 179 punktas)* Remdamasis audito rezultatais ir reikšmingumu, auditorius privalo parengti išvadą, ar audito sritis visais reikšmingais atžvilgiais atitinka taikomus kriterijus. *(4000-ojo TAAIS 184 punktas)*

289. Audito procedūrų tikslas yra surinkti audito įrodymus, kurie leistų patvirtinti nuokrypį nuo audito kriterijų arba paneigti tokio nuokrypio buvimą.

290. Auditorius audito procedūras atlieka pagal audito plane jam numatytus klausimus ir laikydamasis nustatytų terminų. Vadovaudamasis profesiniu sprendimu ir skepticizmu, auditorius įvertina, ar buvo surinkti pakankami ir tinkami audito įrodymai. Auditoriai turėtų atlikti audituojamo subjekto IT kontrolės sistemos (IT bendrosios ir (ar) taikomųjų programų kontrolės priemonių) vertinimą, kad patikrintų jos pakankamumą ir patikimumą per visą audituojamą laikotarpį. Atliekant vertinimą pildomas *IT bendrosios kontrolės vertinimo klausimynas* (šabloną galima rasti Metodikos svetainės Šablonų skiltyje).

291. IT kontrolės priemonių vertinimas gali būti atliekamas taikant tinkamą šių metodų derinį: pokalbį, apklausą, stebėjimą, vadinamuosius ėjimo per sistemą (angl. *walk through*) testus, srauto diagramas (angl. *flow charts*), duomenų fiksavimą ir analizę, patvirtinimą, perskaičiavimą, pakartotinį apdorojimą ir trečiosios šalies patvirtinimą, ar kitus metodus (išsamiau apie metodus žr. Metodikos svetainės Audito metodų skiltyje) ir CAAT priemones, nurodytus Vadovo 4 priede.

292. IT bendrosios kontrolės priemonių vertinimo apimtį sudaro patikrinimas, pvz., ar:

- ✓ IT politika apibrėžta, patvirtinta ir apie ją pranešta;
- ✓ sukurta ir veikia IT valdymo struktūra;
- ✓ reguliariai atliekama IT turto inventorizacija ir yra nustatyti turto papildymo, atnaujinimo ir nurašymo reikalavimai;
- ✓ apibrėžti ir veikiantys dalijimosi informacinių sistemų infrastruktūra ir bendrosiomis paslaugomis su kitais viešaisiais subjektais procesai;
- ✓ informacinių sistemų kūrimo, įsigijimo ir priežiūros procesai apibrėžti, patvirtinti ir apie juos pranešta (įskaitant pokyčių valdymo procesą);

- ✓ informacinių technologijų operacijų procesai (vidinis ir išorinis paslaugų teikimas, paslaugų susitarimai) apibrėžti, patvirtinti ir apie juos pranešta;
- ✓ patvirtintos priemonės fiziniam saugumui ir numatytoms fizinėms darbo sąlygoms užtikrinti;
- ✓ patvirtintos žmogiškųjų išteklių mokymo ir informuotumo didinimo priemonės, siekiant užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą, atitiktį IS politikos ir valdymo struktūros reikalavimams;
- ✓ patvirtintos priemonės, skirtos įvairių IT komunikacijos būdų ir kanalų konfidencialumui, vientisumui ir prieinamumui užtikrinti;
- ✓ patvirtintos informacijos saugumo valdymo priemonės;
- ✓ patvirtintos atitikties teisės aktų reikalavimams valdymo priemonės;
- ✓ patvirtintos veiklos tęstinumo ir veiklos atkūrimo valdymo priemonės, kt.

293. Jei išankstinio tyrimo metu atliekant IT kontrolės priemonių vertinimą surinkta pakankamai įrodymų, kurie patvirtina tam tikrų IT kontrolės priemonių netinkamumą ir (ar) nepakankamumą, auditoriaus profesiniu sprendimu tokiais atvejais gali būti nutarta pagrindinio tyrimo metu neatlikti papildomų audito procedūrų. Išankstinio tyrimo metu surinkti įrodymai panaudojami toliau pildant klausimyno klausimus, skirtus įvertinti IT kontrolės priemonių veiksmingumą pagrindinio tyrimo metu. Tokiu atveju rekomenduojama pagrindinio tyrimo metu tik atnaujinti išankstinio tyrimo metu surinktą informaciją, siekiant įvertinti pasikeitimus, kurie galėjo įvykti atliekant pagrindinį tyrimą.

294. Jei audito plane numatyta atlikti IT valdymo gebos vertinimą, jis atliekamas pagal COBIT metodikoje pateiktą procesų gebos vertinimo modelį. IT geba gali būti nustatoma įvertinant visą IT bendrąją kontrolę (suteikiant vieną bendrą balą) arba įvertinant IT procesų kontrolę (suteikiant balus kiekvienam procesui). Kaip atlikti gebos vertinimą detaliai aprašyta ISACA knygose „Vertintojo vadovas naudojant, COBIT5“, „Procesų vertinimo modelis, naudojant COBIT5“. IT procesų gebos modelis ir pagrindiniai vertinimo principai trumpai pateikti Vadovo 2 priede.

295. Vertinant taikomųjų programų kontrolės priemones tinkamumo ir patikimumo aspektais atliekami detalieji testai. Spręsdamas, ar šių programų kontrole galima pasikliauti, auditorius turėtų įsitikinti, kad kontrolė veikė veiksmingai, kaip numatyta techninėje dokumentacijoje, visą audituojamą laikotarpį. Taikomųjų programų kontrolės vertinimas ir etapai išsamiau pateikti Vadovo 5 priede. Kontrolės priemonės yra unikalios kiekvienai taikomajai programai, todėl IT audito vadove pateikiamos tik pagrindinės kontrolės testavimo užduotys. Detaliuosius testus auditoriai individualiai parengia kiekvienai testuojamai IS.

296. Jeigu audito metu buvo pasitelkta išorės auditorių ir (ar) specialistų (ekspertų) ar buvo naudojamasi jų ar vidaus auditorių atliktu darbu, auditorius turi įvertinti jų atlikto darbo tinkamumą audito tikslams. Išsamiau žr. „Audito komandos įgūdžiai“.

297. Svarbu nepamiršti, kad IT auditą, kaip ir kitas audito rūšis, galima laikyti projektu, kuriam reikalingas palyginti lankstus valdymas. Jam būdingas nuolatinis sugrįžimas pasitikrinti, ar, gavus naujų žinių ir įrodymų, tebegalioja anksčiau padarytos prielaidos ir vis dar tinkami jomis paremti profesiniai sprendimai, t. y. nuolat pasitikrinti, ar audito plane numatyti audito klausimai, kriterijai ir procedūros yra vis dar tinkami, o, esant poreikiui, juos pakeisti ar patikslinti.

Audito įrodymų pakankamumas ir tinkamumas

Susiję TAAIS reikalavimai
Auditorius privalo surinkti pakankamai tinkamų audito įrodymų, kad galėtų suformuluoti audito tikslą ir audito klausimus atitinkančius audito pastebėjimus, išvadas bei pateikti rekomendacijų, jeigu reikia ir jeigu tai nustato AAI įgaliojimai. *(3000-ojo TAAIS 106 punktas)* Auditorius privalo planuoti ir atlikti procedūras, reikalingas surinkti pakankamus ir tinkamus audito įrodymus išvados su pasirinktu užtikrinimo lygiu parengimui. *(4000-ojo TAAIS 144 punktas)*

298. Audito įrodymai yra dokumentuota informacija, kuria auditorius pagrindžia savo pastebėjimus, išvadas ir rekomendacijas. Audito įrodymai turi būti pakankami ir tinkami, kad įtikintų ataskaitos skaitytoją, jog audito pastebėjimai ir išvados yra pagrįsti.

299. Įrodymų *tinkamumas* susijęs su audito įrodymų kokybe. Jis reiškia, kad audito įrodymai turi būti aktualūs, svarbūs, pagrįsti ir patikimi:

- ✓ aktualumas ir svarba nurodo, kiek audito įrodymai yra logiškai susiję ir svarbūs audito tikslui ir nagrinėjamiems audito klausimams;
- ✓ pagrįstumas rodo, kiek audito įrodymai suteikia reikšmingą ar protingą pagrindą išmatuoti vertinamą objektą;
- ✓ patikimumas rodo, kiek audito įrodymai yra paremti patvirtinančiais duomenimis, gautais iš įvairių (skirtingų) šaltinių; ar įrodymai, pakartotinai patikrinus, leidžia suformuluoti tokius pat audito pastebėjimus.

300. *Pakankami audito įrodymai* – audito įrodymų kiekio matas, tai yra kiekybės požiūriu pakankama informacija audito tikslui pasiekti, audito pastebėjimams ir išvadoms pagrįsti.

301. Audito įrodymų pakankamumas negali atsverti tinkamumo, t. y. surinkęs daugiau, bet netinkamų įrodymų, auditorius negalės gauti pagrįstų išvadų. Auditorius turi surinkti pakankamai tinkamų įrodymų.

302. Audito įrodymų pakankamumą ir tinkamumą turi įvertinti pats auditorius. Vertindamas jis turi atsižvelgti į:

- ✓ tikslą, kuriam bus naudojami įrodymai: paremiančių audito metu nustatytus faktus įrodymai tikslumas turi būti didesnis negu bendro pobūdžio informacijos, pateiktos audito ataskaitoje;
- ✓ audito klausimo, kriterijaus reikšmingumą: dažniausiai, kuo reikšmingumo lygis aukštesnis, tuo įrodymai turi būti svaresni;
- ✓ tai, kad kuo didesnė rizika, kad ataskaitoje pateikti faktai sukels ginčų, tuo įrodymai turi būti svaresni;
- ✓ tai, kiek yra nepriklausomas įrodymų šaltinis: tais įrodymais, kurie surenkami iš nepriklausomų šaltinių, reikėtų pasitikėti labiau;
- ✓ vidaus kontrolės vertinimo rezultatus, nustatytas klaidas, apgaulę ir kt.

Audito įrodymų šaltiniai ir pobūdis

303. Audito įrodymų patikimumas priklauso nuo jų šaltinio ir pobūdžio; taip pat svarbūs metodai, kuriais renkami įrodymai.

304. Pagal šaltinį įrodymai gali būti:

- ✓ surinkti paties auditoriaus (interviu, apklausos, tiesioginis tikrinimas ar stebėjimas, tikslinių grupių pagalba ir kt.);
- ✓ gauti iš audituojamo subjekto (skaitmeniniai duomenys iš duomenų bazės, dokumentai, veiklos ataskaitos ir kt.);
- ✓ gauti iš trečiųjų šalių (produktų (paslaugų) gavėjai, suinteresuotosios organizacijos, nagrinėjamos srities ekspertai, oficialios statistikos duomenys ir kt.).

305. Pagal pobūdį įrodymai yra:

- ✓ dokumentiniai (įvairių dokumentų, skaitmeninių duomenų, kitų informacijos šaltinių peržiūra);
- ✓ vizualieji (patikrinimas, stebėjimas, turto apžiūrėjimas);
- ✓ žodiniai (audituojamo subjekto atstovų, trečiųjų šalių apklausa ir (ar) pokalbiai, tikslinės grupės, ekspertų grupės);
- ✓ analitiniai (skaičiavimai, santykių, tendencijų, dėsningumų analizė, palyginimai ir kt.).

306. Skirtingo pobūdžio ir gauti iš skirtingų šaltinių audito įrodymai turi savo privalumų ir trūkumų. Vertinant jų patikimumą, atsižvelgiama į tai, kad:

- ✓ gautieji iš nusimanančios, patikimos ir objektyvios trečiosios šalies yra patikimesni už gautuosius iš audituojamo subjekto vadovų arba kitų asmenų, kurie turi tiesioginį interesą;
- ✓ paties auditoriaus gautieji patikimesni už audituojamo subjekto pateiktus įrodymus;
- ✓ iš audituojamo subjekto gautieji patikimesni, kai jo vidaus kontrolės sistema yra veiksminga;
- ✓ dokumentiniai įrodymai paprastai yra patikimesni už žodinius (pvz., interviu metu surinktus įrodymus reikia patvirtinti iš kitų šaltinių gauta informacija);
- ✓ originalūs dokumentai patikimesni už kopijas;
- ✓ daugiau nei keletu interviu paremti įrodymai yra patikimesni už paremtus vienu pokalbiu;
- ✓ žodiniai įrodymai, gauti tokiomis sąlygomis, kuriomis žmonės gali laisvai kalbėti, yra patikimesni už gautus esant aplinkybėms, kai žmonės gali jaustis nesaugiai;

- ✓ pokalbio metu gauti žodiniai įrodymai, kurie yra dokumentuoti ir patvirtinti audituojamo subjekto rašytine forma, yra patikimesni tik už žodinę raštiškai nepatvirtintą informaciją. Jeigu pokalbio metu gauta informacija patvirtina reikšmingą kriterijaus nuokrypį, ji privalo būti su subjektu suderinta raštu;
- ✓ įrodymai, surinkti auditoriams tiesiogiai stebint, skaičiuojant ar tikrinant, yra patikimesni už netiesiogiai gautuosius.

307. Norint atlikti teisingus vertinimus ir suformuluoti tinkamas išvadas, įrodymai turi būti surinkti iš įvairių (skirtingų) šaltinių (ne mažiau dviejų). Audito įrodymai laikomi patikimais, kai įvairių (skirtingų) šaltinių ir (ar) skirtingo pobūdžio įrodymai sutampa. Jeigu jie nesutampa, auditorius turi nuspręsti, kokių papildomų procedūrų reikia neatitikties priežastims nustatyti ir (ar) gauti papildomų įrodymų. Kai dėl objektyvių priežasčių neįmanoma gauti įrodymų iš įvairių (skirtingų) šaltinių, auditorius turi priimti profesinį sprendimą, ar tokie įrodymai gali būti naudojami pastebėjimams ir išvadoms pagrįsti. Visi auditoriaus profesiniai sprendimai turi būti dokumentuojami.

308. Rinkdami įrodymus, auditoriai turi teisę naudotis audituojamo subjekto turima informacija, tačiau negali pavesti jo personalui atlikti duomenų analizės ar kitų audito procedūrų, kurias pagal audito planą turi atlikti pats auditorius. Turi būti renkami tik su audito tikslu ir nagrinėjamais klausimais susiję duomenys.

309. Negalima reikalauti tokios informacijos, kuri nekaupiama subjekte ar kurią kaupti subjektui nėra pavesta teisės aktais. Tačiau, jeigu auditorius yra įsitikinęs, kad tokios informacijos kaupimas ir jos naudojimas yra būtinas tam, kad audituojamas subjektas galėtų tinkamai vykdyti IT procesus, gali raštu prašyti pateikti tokią informaciją. Jeigu tokios informacijos kaupimas ir valdymas buvo įtrauktas kaip vienas audito kriterijų, o audituojamas subjektas jos nepateikė, auditorius fiksuoja nuokrypį nuo audito kriterijaus.

310. Auditorius turi vengti pavesti audituojamiems subjektams daryti dokumentų, kurie yra tik informacijos šaltinis, kopijas. Rekomenduojama kopiją daryti tik tada, kai šie dokumentai būtini IT kontrolės priemonių trūkumams ar pažeidimams įrodyti ir nėra kito būdo gauti patikimą informaciją.

311. Atliekant IT auditus, auditoriams gali tekti susipažinti ir naudoti informaciją, kuri pagal įstatymus yra valstybės, tarnybos, profesinė, komercinė ar kitokia paslaptis arba yra privati informacija ar kurios paviešinimas gali pakenkti teisėtiems valstybės, audituojamo subjekto ar trečiųjų asmenų interesams (pvz., informacija apie kritinę valstybės informacinę infrastruktūrą). Jeigu ši informacija panaudojama pagrįsti audito išvadas, gali būti nuspręsta neviešinti valstybinio audito ataskaitos arba tam tikrų jos dalių, tai suderinus su valstybės kontrolieriaus pavaduotoju, kuriam yra tiesiogiai pavaldus auditą atliekantis departamentas. Valstybės kontrolės darbuotojų veiksmus, kurie būtini siekiant išvengti valstybės ar tarnybos paslaptimi pripažintos informacijos praradimo ar neteisėto atskleidimo, nustato *Paslapčių subjektų ir Valstybės kontrolės įslaptintos informacijos naudojimo ir apsaugos tvarkos aprašas.*

4.2.2. Audito procedūrų rezultatų vertinimas

Susiję TAAIS reikalavimai

Auditorius privalo išanalizuoti surinktą informaciją ir užtikrinti, kad audito pastebėjimai yra objektyvūs ir atitinka audito tikslą ir audito klausimus. Esant poreikiui audito tikslo ir audito klausimų formuluotės gali būti patikslintos.

(3000-ojo TAAIS 112 punktas)

Auditorius privalo palyginti gautus audito įrodymus su nustatytais audito kriterijais, kad suformuotų audito rezultatus, reikalingus audito išvadai (-oms) parengti.

(4000-ojo TAAIS 179 punktas)

Remdamasis audito rezultatais ir reikšmingumu, auditorius privalo parengti išvadą, ar audito sritis visais reikšmingais atžvilgiais atitinka taikomus kriterijus.

(4000-ojo TAAIS 184 punktas)

312. Kai audito įrodymai yra surinkti, auditorius turi įvertinti, ar jie yra pakankami ir tinkami (rekomenduojama nelaukti, kol bus surinkti visi įrodymai pagal planą, o vertinti jų pakankamumą ir tinkamumą pagal klausimus). Remdamasis šiuo įvertinimu, auditorius turi nuspręsti, ar reikia surinkti daugiau arba galbūt kitokių įrodymų. Rekomenduojama šį įsivertinimą atlikti kuo anksčiau, siekiant išvengti rizikos, kad audito pabaigoje įvertinus, jog nebuvo surinkta tinkamų ir pakankamų audito įrodymų, nebeliks laiko reikiamiems surinkti.

313. Pagrindinio tyrimo metu, atliekant suplanuotas audito procedūras, renkami įrodymai, įvertinamas jų pakankamumas ir tinkamumas. Siekdamas atsakyti į audito klausimus, auditorius kriterijus (kokia situacija laikytina tinkama) palygina su įrodymais (faktine situacija) ir nustato nuokrypius (IT kontrolės priemonių trūkumus (pažeidžiamumus)) nuo to, kas turėtų būti.

314. Nustačius nuokrypį, įvertinamos jo priežastys ir pasekmės. Tai leidžia auditoriui suformuluoti audito pastebėjimus.

    - ✓ Audito pastebėjimas – tai audito įrodymų vertinimo ir jų palyginimo su audito kriterijais rezultatas, apimantis ir nuokrypių nuo audito kriterijų priežasčių ir pasekmių vertinimą. Paprastai pastebėjimas apima vieno kriterijaus vertinimą.

315. Analizuodamas IT kontrolės priemonių trūkumus (pažeidžiamumus), auditorius gali pastebėti šiuos jų tipus:

    - ✓ sisteminės – neatitiktys, kurios gali turėti bendrą bruožą, pvz.: sandorio tipas, vieta ar laikotarpis. Tokiomis aplinkybėmis auditorius gali nuspręsti nustatyti visus tos tiriamosios visumos elementus, kurie turi bendrą bruožą, ir atlikti papildomas jų audito procedūras;
    - ✓ anomalijos – kad neatitiktis būtų laikoma anomalija, auditorius turėtų būti labai tikras, kad ji nėra būdinga visumai. Auditorius šį tikrumą įgyja atlikdamas papildomas audito procedūras su kitais panašiais imties vienetais, kad gautų pakankamų tinkamų audito įrodymų, jog neatitiktis neturi įtakos likusiai imčiai. Kai neatitiktis yra pripažįstama anomalija, jos galima neįtraukti į ekstrapoliavimą;
    - ✓ kitos – kiekvienos neatitikties atveju auditorius turi išsiaiškinti, ar neatitiktis neturi sisteminei neatitikčiai arba anomalijai būdingų savybių ir ar nereikia atlikti papildomų audito procedūrų. Įvertinęs, kad neatitiktis nėra sisteminė arba anomalija, auditorius ją turėtų ekstrapoliuoti.

316. Svarbu išsiaiškinti, kodėl yra nuokrypių nuo audito kriterijų (IT kontrolės priemonių trūkumų (pažeidžiamumų)), bet priežastys turi būti pateiktos išlaikant atsargumą. Svarbu atsižvelgti į audituojamo subjekto požiūrį į IT kontrolės priemonių trūkumų (pažeidžiamumų) priežastis. Jeigu šis požiūris nėra pagrįstas įrodymais, auditorius negali jo laikyti pagrįstu arba teisingu.

317. Kiekvienu nustatytu atveju priežastys (pvz.: darbuotojų trūkumas, silpnas IT funkcijos finansavimas, nepakankamas vadovybės požiūris į IT kontrolės sistemą, jos būklę, pan.) gali skirtis arba skirtingų IT kontrolės priemonių trūkumų (pažeidžiamumų) būti vienodos, nes jos veikia visą IT kontrolės sistemą.

318. IT kontrolės priemonių trūkumai (pažeidžiamumai) gali atsirasti dėl vienos šių priežasčių arba jų derinio:

- ✓ žmogiškoji klaida (atsitiktinis atvejis);
- ✓ apgaulės ar korupcijos apraiškos (tyčia);
- ✓ dėl vadovybės skiriamo nepakankamo dėmesio IT sričiai;
- ✓ dėl taikomo IT kontrolės priemonių įgyvendinimo sudėtingo, nepakankamo, neaiškaus reglamentavimo;
- ✓ dėl nepakankamų žinių ar netinkamo reglamentavimo taikymo;
- ✓ dėl silpnos priežiūros, stebėsenos ir netinkamai audituojamo subjekto parinktų taikyti IT kontrolės priemonių;
- ✓ dėl IT išteklių (žmogiškųjų, finansinių ar kt.) trūkumo;
- ✓ dėl kitų priežasčių.

319. Pasekmės gali būti nustatytos kaip kažkas, kas jau įvyko, arba kaip galimas poveikis ateityje, numatomas remiantis loginiu mąstymu. Pastebėjimų pobūdis, po vertintos veiklos praėjęs laikas ir (ar) po to įvykę pokyčiai lemia, ar auditorius gali nurodyti faktines ar galimas pasekmes.

320. Faktinės pasekmės – jau įvykusi praeityje arba susidariusi dabartinė padėtis, nulemta audito metu nustatytų veiklos trūkumų. Turint faktines pasekmes ir galint įrodyti, kad jos iš tiesų kilo dėl nustatytų veiklos trūkumų, galima paprasčiau pagrįsti, kodėl reikia imtis taisomųjų veiksmų.

321. Galimos pasekmės paprastai apibūdinamos kaip logiškos pasekmės, kurios gali atsirasti, jeigu nustatyti veiklos trūkumai nebus ištaisyti. Galimos pasekmės neturi tvirto pagrindo, todėl auditorius turi jas naudoti atsargiai, ypač nesant susijusių įrodymų ar jeigu tokių pasekmių panašiose situacijose nebuvo pastebėta praeityje.

322. Pasekmės dėl IT kontrolės priemonių trūkumų (pažeidžiamumų) gali būti:

- ✓ išlaidos, kurias organizacija patyrė dėl nustatytų IT kontrolės priemonių klaidų;
- ✓ darbuotojų darbo valandų praradimas, prastovos;
- ✓ žala, kylanti dėl teisės aktų reikalavimų nesilaikymo;
- ✓ klientų pasitenkinimo IT paslaugomis sumažėjimas;

- ✓ kaina darbų, kuriuos reikėjo pakartotinai atlikti arba perdaryti, siekiant ištaisyti IT kontrolės priemonių trūkumus (pažeidžiamumus);
- ✓ rizika nepasiekti tam tikrų užsibrėžtų organizacijos tikslų, veiklos rezultatų;
- ✓ kitos pasekmės.

323. Vertindamas pasekmes, auditorius atsižvelgia į audito kiekybinį ir kokybinį reikšmingumą, nustatytą išankstinio tyrimo metu. Auditorius turėtų atskirai įvertinti kiekvieną nuokrypį nuo audito kriterijaus – IT kontrolės priemonės trūkumą (pažeidžiamumą) ir įvertinti, ar jie yra reikšmingi atskirai ir (ar) kartu.

324. Remdamasis pastebėjimais auditorius formuluoja išvadas ir rekomendacijas.

325. Išvada – tai audito pastebėjimų pagrindu suformuluotas auditoriaus vertinamasis teiginys, atsakantis į audito klausimą pagal jam pasirinktus audito kriterijus. Išvados paprastai formuluojamos audito rezultatų suvestinėje ir pateikiamos audito ataskaitoje.

326. Darbo dokumente taip pat gali būti formuluojamos išvados – tais atvejais, kai tame darbo dokumente vertinami visi audito klausimui suformuluoti audito kriterijai. Kitu atveju, jeigu darbo dokumente vertinamas tik vienas ar dalis klausimui suformuluotų kriterijų, pateikiami pastebėjimai pagal tame dokumente nagrinėtus audito kriterijus (detali informacija kaip pildyti darbo dokumentų šablonus pateikta *Darbo dokumentų šablonų pildymo instrukcijose*, kurias galima rasti Metodikos svetainės Šablonų skiltyje).

327. Rekomendacija – tai valstybinio audito rezultatų pagrindu suformuluotas siūlymas, skirtas valstybinio audito metu nustatytiems IT kontrolės priemonių trūkumams (pažeidžiamumams) išspręsti, siekiant audituojamo (-ų) subjekto (-ų) veiklos gerinimo ir naudos visuomenei didinimo. Pateikiamos rekomendacijos turi būti susietos su pastebėjimais ir išvadomis ir turi būti formuluojamos kaip pokytis, kurio siekiama sprendžiant įvardytą problemą (išsamiau apie rekomendacijų formulavimą žr. Vadovo 4.3.1 skirsnyje).

328. Auditorius, atlikdamas audito procedūras, turi nuosekliai dokumentuoti rezultatus. Išsamiau apie dokumentavimą žr. Vadovo 2.5 poskyryje.

4.2.3. Bendravimas su audituojamuoju subjektu

329. Viso audito atlikimo metu audito įrodymai turi būti aptariami su audituojamu subjektu – atsakingais asmenimis ir pagal poreikį su vadovybe, audituojamo subjekto nuomonė pateikiama darbo dokumentuose. Iki audito ataskaitos projekto pateikimo audituojamam subjektui neturi likti neaptartų įrodymų. Audito įrodymų aptarimas sumažina nesutarimų tarp auditoriaus ir audituojamo subjekto riziką ir gali pagreitinti audito ataskaitos pateikimą. Kilus nesutarimų, auditorius neprivalo atsisakyti ginčytinų įrodymų arba savo vertinimų, tačiau nesutarimo faktas turi būti dokumentuotas. Tokiais atvejais rekomenduojama konsultuotis su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis departamentas, Teisėtumo užtikrinimo departamento darbuotojais ar metodologais. Auditorius turi gauti iš audituojamo subjekto atstovų dokumentus, kuriais jie pagrindžia savo nuomonę.

330. Esant reikšmingų nesutarimų dėl audito pastebėjimų ir išvadų, būtina gauti audituojamo subjekto darbuotojų ir (ar) pagal poreikį vadovybės raštišką nuomonę ir argumentus konkrečiu ginčytinu klausimu. Tokiais atvejais auditorius turi įvertinti, ar audituojamo subjekto nuomonę tikslinga pateikti ir audito ataskaitoje.

331. Jeigu auditorius įtaria, kad audituojamo subjekto vadovybės nariai yra susiję su nustatytais teisės aktų pažeidimais, apie tai privalo oficialiu raštu pranešti aukštesnio lygio įstaigos vadovui ir, jei būtina, teisėsaugos institucijoms. Valstybinio audito metu nustačius faktų, aplinkybių ir (ar) pažeidimų, kuriuos turėtų nagrinėti atitinkamos teisėsaugos institucijos, ir nusprendus valstybinio audito dokumentus perduoti pagal kompetenciją atitinkamai teisėsaugos institucijai, tai atliekama konsultuojantis su Teisėtumo užtikrinimo departamento teisininkais.

332. Jeigu pagrindinio tyrimo metu auditorius nustato papildomų IT kontrolės priemonių trūkumų (pažeidžiamumų), jis turi įvertinti jų reikšmingumą. Jeigu jos reikšmingos ir glaudžiai susijusios su audito objektu ir tikslu, auditorius atsižvelgdamas į tai turi įtraukti naujus audito klausimus, kriterijus į audito planą ar koreguoti esamus ir informuoti (oficialiu raštu ar el. paštu) apie tai audituojamą subjektą. Jeigu auditorius priima profesinį sprendimą, kad papildomai nustatyti IT kontrolės priemonių trūkumai (pažeidžiamumai) nėra reikšmingi ir (ar) nėra glaudžiai susiję su audito objektu ir tikslu, naujų klausimų, kriterijų į audito planą gali netraukti, bet apie nustatytus IT kontrolės priemonių trūkumus (pažeidžiamumus) reikia informuoti audituojamą subjektą: rekomenduojama jo atsakingus asmenis informuoti oficialiu raštu ar el. paštu (atsižvelgus į nustatyto trūkumo (pažeidžiamumo) reikšmingumą). Prieš informuojant, naudinga nustatytus minėtus trūkumus su subjekto atsakingais asmenimis aptarti žodžiu. Tai leis lengviau ir tiksliau parengti raštą. Auditorius gali priimti profesinį sprendimą nereikšmingus trūkumus pranešti audituojamam subjektui žodžiu, bet darbo dokumentuose turi būti fiksuojami visi su jo atsakingais asmenimis svarstyti klausimai.

4.2.4. Audito rezultatų suvestinės parengimas

333. Audito rezultatų suvestinės tikslas – įsitikinti, kad surinkti pakankami ir tinkami audito įrodymai, leidžiantys atsakyti į audito klausimus pagal nustatytus kriterijus, pateikti svarbių pastebėjimų, išvadų ir rekomendacijų bei informaciją apie laukiamą poveikį ir pokyčių vertinimo rodiklius. Audito rezultatų suvestinė turi būti parengta iki audito ataskaitos projekto pateikimo peržiūrėti valstybės kontrolieriaus pavaduotojui, kuriam tiesiogiai pavaldus auditą atliekantis audito departamentas.

334. Audito rezultatų suvestinėje (šabloną galima rasti Metodikos svetainės Šablonų skiltyje) turi būti pateikta:

- ✓ *Santrumpos ir sąvokos*. Pateikiamos audito rezultatų suvestinėje vartojamos santrumpos ir sąvokų paaiškinimai (išnašose nurodomi sąvokų paaiškinimo šaltiniai).
- ✓ *Pagrindinė informacija apie auditą*: audito ID, audito objektas, tikslas, audituojamas (-i) subjektas (-ai), audituojamas laikotarpis, apribojimai.
- ✓ *Audito įrodymų vertinimas*:
  - audito plane nurodyti klausimai;
  - audito kriterijai;
  - atsakymai į visų lygmenų klausimus pagal kiekvieną kriterijų nurodant:
    - nustatytus nuokrypius (nurodoma ir tai, jeigu nuokrypių nenustatyta) nuo audito kriterijų (IT kontrolės priemonių trūkumus (pažeidžiamumus)), audito įrodymų santrauka ir atliktos procedūros, šaltiniai ir metodai, kuriais buvo gauti audito įrodymai;

- nustatytos neatitikties palyginimas su reikšmingumu – įvertinama, ar nustatytos neatitiktys (kiekviena atskirai arba kartu su kitomis, jei susijusios) reikšmingos kiekybiškai ir (ar) kokybiškai;
- nuorodos į atitinkamus darbo dokumentus;

- preliminarios išvados ir pastebėjimai, nurodant:
  - apibendrintą atsakymą pagal kiekvieną klausimą;
  - pastebėjimus pagal kiekvieną kriterijų;
  - problemos / nuokrypio nuo kriterijaus priežastis ir pasekmes. Tais atvejais, kai auditorius negali pagrįsti priežasčių, tai turi būti nurodyta prie konkretaus audito klausimo ar kriterijaus;
  - atsižvelgus į nustatytą reikšmingumą, ar pastebėjimus ir išvadą (-as) planuojama pateikti audito ataskaitoje ar rašte;

- preliminarios rekomendacijos. Taip pat nurodoma, ar rekomendaciją (-as) planuojama pateikti ataskaitoje ar rašte.

✓ *Apibendrintas vertinimas* – atsakymas į audito tikslą, ar IT bendrosios ir (ar) taikomųjų programų kontrolės priemonės yra veiksmingos.

✓ *Laukiamas audito poveikis:* turi būti nurodytas planuojamas audito poveikis; kiekvienai preliminariai rekomendacijai nurodomi: pokyčiai, jų tipas, vertinimo rodikliai ir matavimo vienetai, pateiktos pokyčiams vertinti pasirinktų rodiklių pradinės, siekiamos ir periodinės reikšmės, jų fiksavimo datos, duomenų šaltiniai ir rodiklio detalaus apskaičiavimo ar vertinimo aprašymas. Išsamiau apie audito poveikio vertinimą pateikiama *Valstybinio audito poveikio vertinimo metodikoje.*

335. Audito rezultatų suvestinės pagrindu rengiama audito ataskaita. Parengus audito rezultatų suvestinę, parengiamas audito užbaigimo grafikas.

336. Jeigu rengiant ir (ar) derinant audito ataskaitos projektą atsiranda poreikis patikslinti audito rezultatų suvestinę ir (ar) darbo dokumentus, tikslinimai atliekami pagal 4.3.1 skirsnyje „Audito ataskaitos projekto rengimas“ pateiktus reikalavimus.

4.3. Ataskaitos rengimas

Susiję TAAIS reikalavimai
Auditorius privalo laiku pateikti išsamias, įtikinamas, lengvai skaitomas ir subalansuotas ataskaitas. *(3000-ojo TAAIS 116 punktas)* Auditorius privalo pateikti išvadą audito ataskaitoje. Išvada gali būti išreikšta kaip nuomonė, išvada, atsakymas į konkrečius audito klausimus ar rekomendacijos. *(4000-ojo TAAIS 191 punktas)*

Auditorius privalo parengti audito ataskaitą remdamasis išsamumo, objektyvumo, pateikimo laiku, tikslumo ir priešpriešos principais.

(4000-ojo TAAIS 202 punktas)

337. Audito ataskaitos tikslas – informuoti numatomus vartotojus apie atlikto audito rezultatus, auditorių padarytas išvadas, pateiktas rekomendacijas, laukiamą audito poveikį.

338. Ataskaitoje pateikiami audito pastebėjimai, išvados ir rekomendacijos turi būti pagrįsti pakankamais ir tinkamais audito įrodymais.

339. Audito ataskaitai parengti paprastai skiriama apie 30 proc. viso auditui skirto laiko.

340. Vadovo 4.3.2 skirsnyje „Išankstinio tyrimo ataskaitos rengimas“ pateikiami išankstinio tyrimo ataskaitos, kuri rengiama nusprendus neatlikti pagrindinio tyrimo ir auditą baigti audito planavimo etape, rengimo reikalavimai.

4.3.1. Audito ataskaitos projekto rengimas

341. Audito ataskaitos projekto rengimą organizuoja audito grupės vadovas, kuris užtikrina, kad projektas būtų parengtas audito plane numatytais terminais. Rengiant projektą gali dalyvauti ir kiti audito grupės nariai. Išsamiau audito grupės atsakomybė ir veiksmai rengiant audito ataskaitos projektą aprašyti *Valstybinių auditų kokybės užtikrinimo vadove*.

342. Jeigu rengiant audito ataskaitos projektą iki jo pateikimo valstybės kontrolieriaus pavaduotojui, kuriam tiesiogiai pavaldus auditą atliekantis audito departamentas, buvo gauta naujos informacijos ar nustatyta naujų faktų, dėl kurių keitėsi audito rezultatai (auditoriaus vertinimai, išvados, rekomendacijos ar kt.), šie pakeitimai turi būti dokumentuoti (patikslinti anksčiau rengti arba parengti nauji darbo dokumentai) ir atitinkamai patikslinta audito rezultatų suvestinė.

343. Kai gauta nauja informacija iš esmės nekeičia audito rezultatų (auditoriaus vertinimų, išvadų, rekomendacijų ar kt.), audito grupė sprendžia:

- ✓ ar tikslinti tik audito rezultatų suvestinę (netikslinant darbo dokumentų);
- ✓ ar tikslinti audito rezultatų suvestinę ir patikslinti ar parengti naujus darbo dokumentus.

344. Jeigu po audito ataskaitos projekto pateikimo valstybės kontrolieriaus pavaduotojui, kuriam tiesiogiai pavaldus auditą atliekantis audito departamentas, arba derinant jį su audituojamu subjektu buvo gauta naujos informacijos ar nustatyta naujų faktų, dėl kurių keitėsi audito rezultatai (auditoriaus vertinimai, išvados, rekomendacijos ar kt.), nėra redaguojami anksčiau parengti ir patvirtinti darbo dokumentai ir audito rezultatų suvestinė. Šie pakeitimai turi būti dokumentuoti naujuose darbo dokumentuose (atsižvelgus į gautą informaciją, tai gali būti nauji darbo dokumentai ar atnaujinti dokumentai ankstesnių darbo dokumentų pagrindu) ir atitinkamai ViPSIS įkeliama nauja patikslinta audito rezultatų suvestinė. Tai dokumentuojama atskiroje ViPSIS procedūroje, kaip tai numatyta *ViPSIS naudotojų vadovuose*.

345. Kai gauta nauja informacija iš esmės nekeičia audito rezultatų (auditoriaus vertinimų, išvadų, rekomendacijų ar kt.), audito grupė sprendžia:

- ✓ ar tikslinti tik audito rezultatų suvestinę (nerengiant naujų darbo dokumentų);

- ✓ ar tikslinti audito rezultatų suvestinę ir parengti naujus darbo dokumentus.

346. Visais atvejais audito rezultatų suvestinėje turi būti nurodytos atliktų pakeitimų / patikslinimų priežastys ir pateikiama nuoroda į dokumentą, kuriame pateikta atnaujinta informacija.

Audito ataskaitai keliami reikalavimai

347. Siekiant užtikrinti, kad ataskaita būtų parengta kokybiškai ir būtų aktuali visiems jos vartotojams, ji turi atitikti šiuos principus:

    - ✓ *išsamumo principas* reikalauja, kad audito ataskaita apimtų visą reikalingą su audito tikslu ir klausimais susijusią informaciją, argumentus ir būti pakankamai detali, kad skaitytojas lengvai suprastų audito objektą, pastebėjimus, išvadas ir rekomendacijas. Skaitytojas taip pat turi žinoti, ar audito objektui, tikslui, apimčiai, metodams ar duomenims taikomi kokie nors apribojimai, kad galėtų pagrįstai interpretuoti ataskaitoje pateiktus pastebėjimus, išvadas ir rekomendacijas ir nebūtų suklaidintas.

    - ✓ *objektyvumo principas* reikalauja, kad auditorius taikytų profesinį sprendimą ir skepticizmą, siekdamas užtikrinti, kad ataskaita būtų faktiškai teisinga ir kad rezultatai ir išvados būtų nešališki, nepriklausomi, subalansuoti ir tinkami pagal aplinkybes. Ją reikėtų rašyti neutraliu stiliumi, tinkamai atskleidžiant ne tik neigiamus, bet ir teigiamus veiklos aspektus (t. y. atspindėti tai, kas iš tikrųjų buvo nustatyta, o ne pernelyg pabrėžti veiklos trūkumus). Teigiamų aspektų pateikimas gali padėti pagerinti kitų organizacijų, kurios susipažino su ataskaita, veiklą. Ataskaitos teiginiai turi būti pagrįsti išsamiomis žiniomis, audito objekto visumos suvokimu. Remdamasis pagrindiniais argumentais, skaitytojas galės geriau suprasti išvadas ir rekomendacijas;

    - ✓ *pateikimo laiku ir svarbos principas* reiškia ataskaitos parengimą tinkamu metu, kad ji išliktų aktuali numatomam (-iems) naudotojui (-ams). Ataskaitos turinys turi būti svarbus, sudominti skaitytojus ir turėti pridedamąją vertę. Ataskaita turi būti parengta tuo metu, kai jos labiausiai reikia tam tikriems pokyčiams, kad jos nauda būtų kiek galima maksimali, kad joje pateikta informacija galėtų naudotis įstatymų leidžiamosios, vykdomosios valdžios atstovai ir kitos suinteresuotosios šalys;

    - ✓ *tikslumo ir konsultavimosi principas* reiškia faktų tikslumo patikrinimą su audituojamu subjektu. Ataskaitoje pateikti įrodymai turi teisingai ir visapusiškai atitikti faktus. Tikslumu skaitytojai užtikrinami, kad ataskaitos duomenys yra patikimi;

    - ✓ *priešpriešos principas* suponuoja atsakingo subjekto atsakymų pateikimą, kai tinkama, ir jų įvertinimą;

    - ✓ *aiškumo principas* reiškia, kad nepaisant IT audito techninio pobūdžio ataskaita turi būti lengvai skaitoma ir suprantama. Aiški struktūra ir antraštės leidžia perteikti sudėtingus klausimus ir interpretuoti rezultatus. Visa informacija pateikiama logiška seka. Turi būti paaiškintos vartojamos specialiosios sąvokos, terminai ir santrumpos, neturi būti vartojami dviprasmiški žodžiai. Paveikslų ir kitos vaizdinės informacijos naudojimas padeda aiškiau perteikti mintis;

- ✓ *glaustumo principas* reiškia, kad ataskaitoje neturi būti su audito tikslu nesusijusių ar nereikšmingų faktų, nereikalingų detalių. Tačiau, atliekant sudėtingus auditus, reikia pateikti pakankamą informaciją, kad skaitytojai, neturintys specialiųjų žinių, galėtų suprasti jos turinį;
- ✓ *įtikinimo principas* reiškia, kad audito ataskaita turi būti logiškai išdėstyta ir rodyti aiškų ryšį tarp audito tikslo, klausimų, kriterijų, pastebėjimų, išvadų, ir rekomendacijų. Turi būti įtikinamai pateikti ir audito pastebėjimai su visais svarbiais argumentais;

348. Auditoriai turėtų atsižvelgti į galimą neigiamą poveikį, kurį galėtų daryti paskelbta IT audito ataskaita. Pavyzdžiui, jeigu IT audito ataskaitoje nustatoma tam tikra audituojamo subjekto IT saugumo rizika ir apie ją pranešama prieš patvirtinant būtinas rizikos mažinimo kontrolės priemones, informacinės sistemos pažeidžiamumas gali būti paviešintas visuomenei. Tokiu atveju, siekdami išvengti galimo neigiamo poveikio audituojamam subjektui, auditoriai gali apsvarstyti galimybę teikti ataskaitą tik po to, kai bus patvirtintos būtinos kontrolės priemonės, arba priimti sprendimą neviešinti tam tikrų ataskaitos dalių.

Audito ataskaitos struktūra

Susiję TAAIS reikalavimai
Audito ataskaitoje auditorius privalo nurodyti audito kriterijus ir jų šaltinius. *(3000-ojo TAAIS 122 punktas)* Auditorius privalo užtikrinti, kad audito pastebėjimai būtų aiškiai susieti su audito tikslu ir klausimais, arba turi paaiškinti, kodėl to padaryti buvo neįmanoma. *(3000-ojo TAAIS 124 punktas)* Jeigu reikia ir jeigu tai nurodyta AAI įgaliojimuose, auditorius privalo pateikti konstruktyvias rekomendacijas, kurios padėtų šalinti audito metu nustatytus trūkumus ar problemas. *(3000-ojo TAAIS 126 punktas)* Audito ataskaita turi apimti šiuos vienetus (tačiau nebūtinai šia tvarka): a) pavadinimą; b) audito standartų identifikavimą; c) trumpą santrauką (jeigu tinkama); d) audito srities aprašymą ir apimtį (audito mastą ir ribojimus); e) audito kriterijus; f) paaiškinimus ir naudotų metodų pagrindimą; g) rezultatus; h) išvadą (-as), pagrįstą (-as) atsakymais į konkrečius audito klausimus, arba i) nuomones; j) audituojamo subjekto atsakymus (jeigu tinkama); k) rekomendacijas (jeigu tinkama). *(4000-ojo TAAIS 210 punktas)*

349. Audito ataskaitoje (šabloną galima rasti Metodikos svetainės Šablonų skiltyje) turi būti:

- ✓ Antraštinis (titulinis) lapas

- ✓ Turinys
- ✓ Pagrindiniai faktai
- ✓ Santrauka
- ✓ Įžanga
- ✓ Audito rezultatai
- ✓ Rekomendacijų įgyvendinimo planas
- ✓ Priedai:

- Santrumpos ir sąvokos
- Audito kriterijai, atliktos procedūros ir taikyti metodai
- Pokyčių vertinimo rodiklių duomenys
- Kiti priedai

350. **Pagrindiniai faktai**. Šioje dalyje pateikiama skaičiais išreikšta svarbiausia informacija apie audito objektą ir rezultatus, į kurią auditoriai nori atkreipti ataskaitos skaitytojų dėmesį. Informacija pateikiama skaičiais išreikštais rodikliais ir trumpu paaiškinimu. Paprastai mažos apimties audito ataskaitose (neviršija 10 psl. be antraštinio lapo, turinio, pagrindinių faktų lapo ir priedų) pagrindinių faktų dalis gali būti nerengiama.

351. **Santrauka** – viena svarbiausių ataskaitos dalių. Ji turi sudominti skaitytojus. Informacija turi būti pateikta taip, kad skaitytojas suprastų atlikto audito esmę ir rezultatus.

352. Santraukos struktūra (skirsniai):

- ✓ Audito svarba
- ✓ Audito tikslas ir apimtis
- ✓ Pagrindiniai audito rezultatai
- ✓ Rekomendacijos

353. Paprastai nedidelės apimties audito ataskaitose santrauka neteikiama, o audito svarba, audito tikslas ir apimtis pateikiami ataskaitos įžangoje, o išvados ir rekomendacijos – audito rezultatų dalies skyriuose.

354. Dalyje „Audito svarba“ skaitytojas trumpai supažindinamas su audito objektu ir esama situacija, nurodoma (-os) problema (-os), kurią (-ias) reikia spręsti arba kodėl pasirinkome atlikti auditą šia tema.

355. Dalyje „Audito tikslas ir apimtis“ pateikiamas audito tikslas ir pagrindiniai audito klausimai, audituojamas (-i) subjektas (-ai), audituojamas laikotarpis. Prireikus pateikiami audito objektui, tikslui, apimčiai, metodams ar duomenims taikomi kokie nors apribojimai. Šių apribojimų gali atsirasti dėl auditoriaus pagrįsto sprendimo nevertinti tam tikrų dalykų, susijusių su audito objektu ir (ar) tikslu, arba dėl audituojamo (-ų) subjekto (-ų) veiksmų ar veiklos, kai nėra galimybės atlikti tam tikrų procedūrų ar gauti tam tikrų duomenų. Apribojimų nurodymas sumažina numatomų vartotojų nepagrįstus lūkesčius. Šioje dalyje taip pat nurodoma, kad auditas atliktas pagal TAAIS.

356. Audito pastebėjimų, išvadų ir rekomendacijų formulavimas – vienas svarbiausių darbų audito procese, nes kokybiški pastebėjimai, išvados ir rekomendacijos yra pagrindas pagerinti audituojamo subjekto IT valdymą ir kontrolės sistemos efektyvumą. Netinkamas jų formulavimas gali ne tik sumenkinti auditoriaus darbo rezultatus, bet ir sumažinti pasitikėjimą aukščiausiąja audito institucija. Formuluojant pagrindinius pastebėjimus ir rengiant išvadas bei rekomendacijas, reikia matyti bendrą vaizdą ir nebūti smulkmeniškam. Tai turi perteikti pagrindines audito ataskaitos mintis. Pagrindinių pastebėjimų, išvadų ir rekomendacijų patikimumas priklauso nuo audito rezultatų dalyje pateiktų įrodymų ir audito pastebėjimų.

357. Dalyje „Pagrindiniai audito rezultatai“ apibendrinami svarbiausi audito rezultatai ir pateikiamas apibendrintas vertinimas – atsakymas į audito tikslą, ar IT bendrosios ir (ar) taikomųjų programų kontrolės priemonės yra veiksmingos.

358. Pagrindiniai audito rezultatai turi būti:

- ✓ apibendrinantys ataskaitos dalies „Audito rezultatai“ poskyriuose ir (ar) skirsniuose pateiktus svarbiausius pastebėjimus ir išvadas, nurodomos jų priežastys ir pasekmės;
- ✓ pateikti aiškiai, suprantamai ir konkrečiai. Rekomenduojama naudoti ne abstrakčias frazes, tokias kaip „dauguma“ arba „kai kurie“, o skaičius, procentus ir proporcijas, nes tai suteikia vertinimui konkretumo ir rodo, kad ataskaita grindžiama audito rezultatais.

359. Audito metu įvykę pokyčiai, kuriuos tikslinga pateikti valstybinio audito ataskaitoje, pateikiami pagal poreikį santraukoje ir (ar) audito rezultatų dalyje.

360. Rekomendacijos formuluojamos apibendrinus ir susisteminus nustatytus IT kontrolės priemonių trūkumus (pažeidžiamumus). Rekomendacijos pagrindas – nustatyto IT kontrolės priemonių trūkumo (pažeidžiamumo) priežastis, t. y. dėl ko jis atsirado ir turi būti pašalintas (ištaisytas). Siekdamas parašyti veiksmingas rekomendacijas, auditorius jau audito planavimo etape turi galvoti apie galimas rekomendacijas.

361. Atsižvelgiant į rekomendacijų įgyvendinimu siekiamų pokyčių svarbą audituojamai sričiai, rekomendacijos yra grupuojamos į didelės, vidutinės ir mažesnės svarbos. Didelės ir vidutinės svarbos rekomendacijos pateikiamos audito ataskaitoje, o mažesnės svarbos – tik rašte (oficialiame) audituojamam subjektui.

362. Esant poreikiui, didelės ir vidutinės svarbos rekomendacijos gali būti pateiktos rašte (oficialiame) audituojamam subjektui iki pateikiant jam audito ataskaitos projektą. Nepriklausomai nuo to, ar šios rekomendacijos buvo įgyvendintos ar nebuvo įgyvendintos iki ataskaitos projekto pateikimo audituojamam subjektui, jos turi būti pateiktos ataskaitos projekte. Jeigu didelės ir vidutinės svarbos rekomendacijos:

- ✓ buvo įgyvendintos iki audito ataskaitos projekto parengimo, jos pateikiamos ataskaitos audito rezultatų dalyje;
- ✓ nebuvo įgyvendintos iki audito ataskaitos projekto parengimo, jos pateikiamos ataskaitos santraukoje rekomendacijų dalyje ir rekomendacijų įgyvendinimo plane.

363. Rekomendacijų priskyrimą svarbai reglamentuoja *Valstybinio audito poveikio vertinimo metodika*.

364. Rekomendacijos turi būti:

- ✓ aiškios, suprantamos ir logiškos;
- ✓ susijusios su audito tikslu, pagrindiniais audito pastebėjimais ir išvadomis;
- ✓ skirtos konkrečiam adresatui. Jeigu IT kontrolės priemonės trūkumo (pažeidžiamumo) priežastis susijusi su audituojamo subjekto vidaus veikla ir jo priimamais sprendimais, rekomendacija teikiama audituojamam subjektui. Jeigu priežastis nesusijusi su audituojamo subjekto vidaus veikla, rekomendacija turi būti skirta pagal kompetenciją kitai institucijai;
- ✓ naudingos, t. y. skirtos tobulinti subjekto IT valdymą ir kontrolės sistemą;
- ✓ formuluojamos kaip pokytis, kurio siekiama sprendžiant pastebėjime įvardytą problemą;
- ✓ skirtos pašalinti esmines IT kontrolės priemonės trūkumo (pažeidžiamumo) priežastis;
- ✓ nurodančios, ką rekomenduojama keisti, paliekant subjektui pasirinkimo teisę, kaip tai padaryti. Jeigu auditoriai turi pakankamai pagrindimo, kaip geriausiai tai galima padaryti, gali būti nurodoma ir jos įgyvendinimo priemonė (-ės) ar būdas (-ai);
- ✓ suformuluotos taip, kad būtų įgyvendinamos, o įgyvendinimą būtų galima fiksuoti;

365. Siekiant rekomendacijų poveikio turi būti bendradarbiaujama su audituojamu subjektu. Svarbu užtikrinti, kad jos būtų nukreiptos į problemos ir jos priežasties pašalinimą, pokytį ir jo rodiklių pasiekimą.

366. Įžanga. Pagrindinė jos paskirtis – glaustas bendros informacijos apie audituojamą sritį pateikimas (svarbi informacija, susijusi su audito objektu, subjektu). Rekomenduojama (pagal galimybę) informaciją įžangoje teikti schematiškai. Ji neturi būti pernelyg ilga (rekomenduojama apimtis iki 2 psl.). Jeigu, auditoriaus nuomone, skaitytojui reikia išsamesnių duomenų, jie gali būti pateikti prieduose.

367. Audito rezultatai. Šioje dalyje nurodomi audito metu nustatyti IT kontrolės priemonių trūkumai (pažeidžiamumai). Pateikiant audito rezultatus, turi būti aiškus ir lengvai patikrinamas nustatyto audito objekto, tikslo, klausimų, kriterijų, gautų įrodymų, audito pastebėjimų ir suformuluotų išvadų, rekomendacijų ir laukiamo audito poveikio ryšys.

368. Kiekviename audito rezultatų dalies skyriuje pateikiama:

- ✓ audito kriterijus (-ai) ir jo šaltinis (-iai) (šaltiniai nurodomi kartu su kriterijumi tekste arba pateikiami išnašose);
- ✓ audito pastebėjimai – audito įrodymų palyginimas su audito kriterijais;
- ✓ priežastys, kurios lėmė nuokrypio (IT kontrolės priemonės trūkumo (pažeidžiamumo)) nuo audito kriterijaus atsiradimą;
- ✓ esamos pasekmės organizacijos ar kitai veiklai arba tikėtinos, jei audituojamo subjekto vadovybė nesiims tinkamų priemonių valdyti nustatytą IT trūkumą (pažeidžiamumą);

- ✓ nustatyti teigiami dalykai ir geroji audituojamo (-ų) subjekto (-ų) IT valdymo praktika (pagal galimybę);
- ✓ galimi nustatytų problemų sprendimo būdai (pagal galimybę ir nedubliuojant rekomendacijų);
- ✓ audito metu įvykę pokyčiai (pagal poreikį);
- ✓ audituojamo subjekto, eksperto nuomonė (pagal poreikį). Paprastai tai daroma, jei audituojamas subjektas nesutinka su auditoriaus vertinimais dėl tam tikrų dalykų.

369. Kiekvienu atveju audito grupė sprendžia, kaip pateikti informaciją (pvz.: audito kriterijai ir jų šaltiniai gali būti pateikti kaip įžanginė skyriaus dalis arba kiekviename poskyryje).

370. Ataskaitos teiginys gali būti labiau įtikinamas ir suprantamas, jeigu jį patvirtina konkretus pavyzdys. Siekiant geriau suprasti vertinamą dalyką, rekomenduojama naudoti iliustracijas – lenteles, paveikslėlius, nuotraukas ir pan. Iliustracijos turi būti suprantamos ataskaitos skaitytojui. Pavyzdžių ir iliustracijų skaičius ataskaitoje turi būti racionalus, rekomenduojama juos teikti tik esminiais klausimais.

371. Audito rezultatų dalyje, jei tinkama, nurodomi audito apimties apribojimai.

372. Rekomendacijų įgyvendinimo planas.

Audito rekomendacijų įgyvendinimo plane turi būti pateikta:

- ✓ laukiamas audito poveikis;
- ✓ pastebėjimai, pateikiant kiekvieno pagrindinio audito rezultato esmę;
- ✓ rekomendacijos (pokyčiai, kurių siekiama), jų svarba ir įgyvendinimo terminai;
- ✓ pokyčių vertinimo rodikliai ir jų reikšmės (pradinė ir siektina);
- ✓ priemonės, reikalingos IT kontrolės priemonės trūkumui (pažeidžiamumui) išspręsti, ir jų įgyvendinimo terminai;
- ✓ subjektai, kuriems pateiktos rekomendacijos ir subjektai, kurie įgyvendins rekomendacijų priemones.

373. Tais atvejais, kai dėl rekomendacijos priimtinumo ir jos įgyvendinimo su subjektu, kuriam skiriama rekomendacija, nepasiekiama bendro sutarimo, rekomendacijų įgyvendinimo plano priemonės pateikimo eilutėje nurodoma subjekto nuomonė dėl įgyvendinimo.

374. Išsamiau apie audito rekomendacijų įgyvendinimo plane reikiamą nurodyti informaciją ir plano pildymo pavyzdžiai pateikiami *Valstybinio audito poveikio vertinimo metodikoje*.

375. Priedai. Jeigu ataskaitos tekste pateiktiems faktams ar argumentams pagrįsti reikia papildomos informacijos, ji gali būti pateikta prieduose. Ataskaitos priedai – įvairaus turinio dokumentai, kurie turi aiškų ryšį su audito rezultatų dalimi ir ją papildo arba paaiškina. Priedai turi būti lengvai suprantami ataskaitos skaitytojui.

376. Pirmajame audito ataskaitos priede „Santrumpos ir sąvokos“ pateikiamos ataskaitoje vartojamos santrumpos ir sąvokos. Jeigu jų nėra daug (neviršija 10 vnt.), jos teikiamos ne priede, o ataskaitos tekste (skliaustuose ar išnašose).

377. Antrajame ataskaitos priede „Audito kriterijai, atliktos procedūros ir taikyti metodai“ nurodoma:

- ✓ audito ataskaitos skyrių ar poskyrių pavadinimai;
- ✓ taikyti audito kriterijai;
- ✓ atliktos audito procedūros, informacijos ir duomenų rinkimo bei vertinimo metodai, kurie buvo taikyti siekiant surinkti įrodymus ir pagrįsti jais skyriuje ar poskyryje teikiamus faktus, pastebėjimus ir kt. Esant poreikiui, šioje skiltyje gali būti pateikiami auditorių atlikti įvairūs skaičiavimai, detali informacija apie atliktą atranką ir kt.

378. Trečiajame audito ataskaitos priede „Pokyčių vertinimo rodiklių duomenys“ nurodomi šių rodiklių duomenys. Rengiant audito rekomendacijų įgyvendinimo planą turi būti ne tik nustatyti ir su audituojamu subjektu suderinti pokyčių vertinimo rodikliai, jų siekiamos reikšmės ar pageidaujama pokyčio kryptis, bet ir turi būti sutarta, kas ir kada surinks ir pateiks pokyčių vertinimui reikalingus duomenis (tai ypač svarbu, jei jų vertinimui reikalingi viešai neprieinami administraciniai duomenys, kuriais disponuoja audito subjektas ar kitos viešojo sektoriaus institucijos). Išsamiau apie trečiame priede reikiamą nurodyti informaciją žr. *Valstybinio audito poveikio vertinimo metodikoje*.

379. Ataskaita turi būti parengta vadovaujantis *Valstybės kontrolės dokumentų valdymo ir naudojimo reglamentu*. Valstybinio audito ataskaitos įforminimo reikalavimai, praktiniai rašymo patarimai ir pavyzdžiai nustatyti ir pateikti *Veiklos audito ataskaitų rašymo gairėse*.

4.3.2. Išankstinio tyrimo ataskaitos rengimas

380. Išankstinio tyrimo ataskaitos, nusprendus neatlikti pagrindinio tyrimo, parengimą organizuoja audito grupės vadovas. Rengiant ją pagal poreikį dalyvauja ir kiti audito grupės nariai. Audito grupės atsakomybė ir veiksmai išsamiau aprašyti *Valstybinių auditų kokybės užtikrinimo vadove*.

381. Iki išankstinio tyrimo ataskaitos projekto pateikimo audituojamam subjektui turi būti aptarti (susitikimo ir (ar) susirašinėjimo su juo metu) išankstinio tyrimo rezultatai ir subjektas informuojamas, kad auditas baigiamas išankstiniu tyrimu. Aptarimas sumažina nesutarimų tarp auditoriaus ir audituojamo subjekto riziką ir gali pagreitinti išankstinio tyrimo ataskaitos pateikimą. Kilus nesutarimų, auditorius neprivalo atsisakyti ginčytinų įrodymų arba savo vertinimų, tačiau nesutarimo faktas turi būti dokumentuotas. Tokiais atvejais rekomenduojama konsultuotis su valstybės kontrolieriaus pavaduotoju, kuriam tiesiogiai pavaldus auditą atliekantis audito departamentas, Teisėtumo užtikrinimo departamento darbuotojais ar metodologais. Auditorius turi gauti iš audituojamo subjekto atstovų dokumentus, kuriais jie pagrindžia savo nuomonę. Esant reikšmingų nesutarimų dėl išankstinio tyrimo rezultatų, būtina gauti audituojamo subjekto darbuotojų ir (ar) pagal poreikį vadovybės raštišką nuomonę ir argumentus konkrečiu ginčytinu klausimu. Tokiais atvejais auditorius turi įvertinti, ar audituojamo subjekto nuomonę tikslinga pateikti ir išankstinio tyrimo ataskaitoje.

Išankstinio tyrimo ataskaitos struktūra

382. Išankstinio tyrimo ataskaitą (šabloną galima rasti Metodikos svetainės Šablonų skiltyje), nusprendus neatlikti pagrindinio tyrimo, sudaro:

- ✓ Antraštinis (titulinis) lapas.
- ✓ Turinys.
- ✓ *Pagrindiniai faktai (pagal galimybę).* Šioje dalyje pateikiama skaičiais išreikšta svarbiausia informacija apie audito objektą ir išankstinio tyrimo rezultatus, į kurią auditoriai nori atkreipti ataskaitos skaitytojų dėmesį. Informacija pateikiama skaičiais išreikštais rodikliais ir trumpu paaiškinimu.
- ✓ *Santrauka.* Santraukos struktūra (skirsniai):
  - Audito objekto svarba. Šioje santraukos dalyje pateikiamas trumpas audito objekto ir esamos situacijos pristatymas, nurodoma problema (-os), kurią (-ias) reikia spręsti arba kodėl pasirinkome atlikti auditą šia tema.
  - Išankstinio tyrimo tikslas ir apimtis. Nurodomas išankstinio tyrimo tikslas, pagrindiniai išankstinio tyrimo klausimai arba sritys, audituojamas (-i) subjektas (-ai), audituojamas laikotarpis. Šioje dalyje taip pat nurodoma, kad išankstinis tyrimas atliktas pagal TAAIS. Prie tikslo pateikiama išnaša, kurioje trumpai paaiškinama, kas yra išankstinis tyrimas ir kad išankstinio tyrimo atveju rekomendacijos nėra teikiamos.
  - Pagrindiniai išankstinio tyrimo rezultatai. Trumpai pateikiamos nustatytos problemos ir nurodomi išankstinio tyrimo metu audituotoje srityje nustatyti pokyčiai ir (ar) kitos priežastys, dėl kurių auditas baigiamas išankstiniu tyrimu.

    Nedidelės apimties išankstinio tyrimo ataskaitoje (neviršija 10 psl. be priedų) santrauka neteikiama. Tokiu atveju audito objekto svarba, išankstinio tyrimo tikslas ir apimtis, audituotoje srityje nustatyti pokyčiai ir priežastys, dėl kurių auditas baigiamas šiuo tyrimu, pateikiami išankstinio tyrimo rezultatų dalyje.
- ✓ *Išankstinio tyrimo rezultatai.* Išankstinio tyrimo rezultatų dalies struktūra:
  - Nagrinėta sritis. Glaustai pateikiama bendra informacija apie audituotą veiklos sritį (svarbi informacija, susijusi su audito objektu, subjektu (-ais)).
  - Nustatytos problemos. Pateikiamos išankstinio tyrimo metu nustatytos problemos, kurios turi būti pagrįstos tam tikrais faktais, pavyzdžiais ir, esant galimybei, pateikiamos priežastys ir pasekmės.
- ✓ *Priedai.* Pirmajame priede pateikiamos santrumpos ir sąvokos. Antrajame pateikiami išankstinio tyrimo metu taikyti informacijos rinkimo ir vertinimo metodai. Jeigu reikia, pateikiami ir kiti priedai, skirti pagrįsti ataskaitoje pateiktus faktus ir argumentus.

383. Išankstinio tyrimo ataskaitoje rekomendacijos audituojamam subjektui neteikiamos. Šio tyrimo ataskaitos įforminimo reikalavimai, praktiniai rašymo patarimai ir pavyzdžiai nustatyti ir pateikti *Veiklos audito ataskaitų rašymo gairėse*.

Išankstinio tyrimo ataskaitos projekto derinimas ir galutinės ataskaitos pateikimas

384. Siunčiant oficialiu raštu išankstinio tyrimo ataskaitos projektą susipažinti audituojamam subjektui ir pagal poreikį kitoms institucijoms, lydraštyje nurodomas pastabų pateikimo terminas (ne trumpesnis kaip 10 darbo dienų). Jeigu su subjektu ar kita institucija yra susijusi ne visa, o dalis projekto, lydraštyje gali būti nurodyta, su kokiomis dalimis, pastraipomis ar kt. prašoma susipažinti ir pateikti pastabas. Esant poreikiui organizuojamas projekto aptarimas. Jis turi būti organizuojamas, jeigu audituojamas subjektas ir (ar) kitos minėtos institucijos pateikė svarbių pastabų ar kitos svarbios informacijos, kurią reikėtų aptarti. Projekto aptarime dalyvauja audito grupė, pagal poreikį kiti Valstybės kontrolės darbuotojai, audituojamo subjekto vadovai ir (ar) atsakingi asmenys bei kitų institucijų atstovai.

385. Raštu gavus audituojamo subjekto ir (ar) kitų institucijų pastabų, turi būti parengtas darbo dokumentas, kuriame, įvertinus pastabas, argumentuotai nurodoma, ar būtina į jas atsižvelgti ir jei ne, nurodomos priežastys. Jeigu, įvertinus pastabas (ir gavus įrodymų) nusprendžiama į jas atsižvelgti, tikslinamas ataskaitos projektas. Jeigu auditoriai mano, kad į pastabas atsižvelgti netikslinga, išankstinio tyrimo ataskaitoje gali būti teikiama audituojamo subjekto ir (ar) kitų minėtų institucijų atstovų nuomonė ir auditorių papildomi argumentai, paaiškinantys auditorių poziciją.

386. Išankstinio tyrimo ataskaita ne vėliau kaip per 5 darbo dienas nuo jos pasirašymo dienos, išskyrus atvejus, kai teisės aktuose nustatytas kitoks terminas, oficialiu raštu siunčiama audituojamam subjektui ir pagal poreikį kitoms institucijoms. Lydraštyje nurodoma, ar buvo atsižvelgta į pateiktas pastabas dėl išankstinio tyrimo ataskaitos projekto. Išsamiau audito grupės atsakomybė ir veiksmai rengiant išankstinio tyrimo ataskaitą aprašyti *Valstybinių auditų kokybės užtikrinimo vadove*.

387. Išankstinio tyrimo ataskaita ne vėliau kaip per 10 darbo dienų (išimtiniais atvejais – per kitą viešinimo strategijoje nustatytą terminą) nuo jos pasirašymo dienos oficialiu raštu siunčiama audituojamo subjekto steigėjui, Lietuvos Respublikos Seimo Audito komitetui, o prireikus ir kitiems subjektams.

Audito rezultatų viešinimas

388. Audito rezultatų viešinimo procesą organizuoja Komunikacijos departamentas. Pranešimų spaudai rengimą ir skelbimą reguliuoja *Valstybės kontrolės pranešimų spaudai rengimo ir skelbimo tvarkos aprašas*.

4.3.3. Audito ataskaitos projekto derinimas ir galutinės ataskaitos pateikimas

Susiję TAAIS reikalavimai
Auditorius privalo suteikti audituojamam subjektui galimybę pateikti pastabų dėl audito pastebėjimų, išvadų ir rekomendacijų prieš AAI paskelbiant savo audito ataskaitą. *(3000-ojo TAAIS 129 punktas)* Auditorius privalo dokumentuoti audituojamo subjekto komentarų vertinimą, įskaitant atliktų audito ataskaitos pakeitimų arba gautų pastabų atmetimo priežastis. *(3000-ojo TAAIS 130 punktas)*

Audito ataskaitos projekto derinimas

389. Siekiant paprastesnio galutinio ataskaitos projekto derinimo su audituojamu subjektu ir konstruktyvaus bei teigiamo dialogo, rengiamas projekto dalis rekomenduojama aptarti su audituojamo subjekto atstovais, atsakingais už konkrečias auditorių analizuojamas sritis. Aptarimo būdus pasirenka audito grupės vadovas. Tai gali būti susitikimai, susirašinėjimai ir kt. Auditoriai turi stengtis sužinoti visus audituojamo subjekto argumentus, kad galutinio derinimo metu neatsirastų naujų ir galbūt lemiamų argumentų, dėl kurių keistųsi auditoriaus vertinimas. Pateiktiems argumentams ieškoma galimų kontrargumentų, įvertinami įvairūs požiūriai. Svarbu audituojamo subjekto atstovus informuoti, kad nėra derinamas galutinis tekstas ir jis gali keistis atsižvelgus į kitus ataskaitoje teikiamus dalykus.

390. Parengtas audito ataskaitos projektas turi būti suderintas su audituojamu subjektu ir kitomis institucijomis, kurių atžvilgiu buvo suformuluoti pastebėjimai, išvados ir (ar) kurioms buvo pateiktos rekomendacijos. Ataskaitos projektas turi būti pateiktas audituojamam (-iems) subjektui (-ams) susipažinti ne vėliau kaip 3–4 savaitės iki audito pabaigos.

391. Siunčiant oficialiu raštu ataskaitos projektą susipažinti audituojamam subjektui ir kitoms institucijoms, kurių atžvilgiu buvo suformuluoti pastebėjimai, išvados ir (ar) kurioms buvo pateiktos rekomendacijos, lydraštyje nurodomas pastabų pateikimo terminas (ne trumpesnis kaip 10 darbo dienų). Nurodoma, kad kartu su pastabomis dėl audito ataskaitos projekto turi būti pateiktos ir priemonės rekomendacijoms įgyvendinti, subjektai, kurie įgyvendins numatytas priemones, ir jų terminai. Jeigu su audituojamu subjektu ar kita institucija yra susijusi ne visa, o dalis projekto, lydraštyje gali būti nurodyta, su kokiomis dalimis, pastraipomis ar kt. yra prašoma susipažinti ir pateikti pastabas.

392. Esant poreikiui organizuojamas projekto ir audituojamo subjekto siūlomų priemonių rekomendacijoms įgyvendinti, taip pat pokyčių vertinimo rodiklių aptarimas. Jis turi būti organizuojamas, jei audituojamas subjektas ir (ar) kitos minėtos institucijos pateikė pastabų ar kitos svarbios informacijos, kurią reiktų aptarti.

393. Raštu gavus audituojamo subjekto ir (ar) kitų minėtų institucijų pastabų, turi būti parengtas darbo dokumentas, kuriame, įvertinus pastabas, argumentuotai nurodoma, ar būtina į jas atsižvelgti ir, jei ne, nurodomos priežastys.

394. Ataskaitos projekto aptarime dalyvauja audito grupė, pagal poreikį kiti Valstybės kontrolės darbuotojai, audituojamo subjekto vadovai ir (ar) atsakingi asmenys. Gali būti kviečiami institucijų, kurių atžvilgiu buvo suformuluoti pastebėjimai, išvados ir (ar) kurioms buvo pateiktos rekomendacijos, atstovai. Aptarime gali dalyvauti valstybės kontrolierius ir (ar) valstybės kontrolieriaus pavaduotojas. Aptariamos audituojamo subjekto ir (ar) kitų minėtų institucijų pateiktos priemonės rekomendacijoms įgyvendinti, rekomendacijų įgyvendinimo terminai, su audito poveikio vertinimu susiję aspektai ir kita reikšminga informacija.

395. Jeigu, įvertinus pastabas (ir gavus įrodymų) nusprendžiama į jas atsižvelgti, tikslinamas ataskaitos projektas. Jeigu auditoriai mano, kad į pastabas atsižvelgti netikslinga, audito ataskaitoje paprastai teikiama audituojamo subjekto ir (ar) kitų minėtų institucijų atstovų nuomonė ir auditorių papildomi argumentai, paaiškinantys auditorių poziciją.

Galutinės audito ataskaitos pateikimas

396. Audito ataskaita ne vėliau kaip per 5 darbo dienas nuo jos pasirašymo dienos, išskyrus atvejus, kai teisės aktuose nustatytas kitoks terminas, oficialiu raštu siunčiama

audituojamam subjektui ir kitoms institucijoms, kurių atžvilgiu buvo suformuluoti pastebėjimai, išvados ir (ar) kurioms buvo pateiktos rekomendacijos. Lydraštyje nurodoma, ar buvo atsižvelgta į pateiktas pastabas dėl audito ataskaitos projekto. Išsamiau audito grupės atsakomybė ir veiksmai rengiant audito ataskaitą aprašyti *Valstybinių auditų kokybės užtikrinimo vadove*.

397. Audito ataskaita ne vėliau kaip per 10 darbo dienų (išimtiniais atvejais – per kitą viešinimo strategijoje nustatytą terminą) nuo jos pasirašymo dienos oficialiu raštu siunčiama audituojamo subjekto steigėjui, Lietuvos Respublikos Seimo Audito komitetui, kitiems Seimo komitetams ir komisijoms pagal sritį, o prireikus – ir kitiems subjektams.

4.3.4. Audito rezultatų viešinimas

398. Audito rezultatų viešinimo procesą organizuoja Komunikacijos departamentas. Pranešimų spaudai rengimą ir skelbimą reguliuoja *Valstybės kontrolės pranešimų spaudai rengimo ir skelbimo tvarkos aprašas*.

5. VEIKSMAI PO AUDITO

Susiję TAAIS reikalavimai
Auditorius privalo stebėti (kai tinkama), kaip įgyvendinamos ankstesnių auditų rekomendacijos, o AAI privalo, jei įmanoma, pranešti įstatymų leidžiamajai institucijai, koks buvo išvadų ir visų susijusių korekcinių veiksmų poveikis. *(3000-ojo TAAIS 136 punktas)* Auditorius, atlikdamas veiksmus po audito, privalo sutelkti dėmesį į tai, ar audituotas subjektas tinkamai išsprendė problemas ir per protingą laiką pagerino dėl tokių problemų susiklosčiusią padėtį. *(3000-ojo TAAIS 139 punktas)* Auditorius gali nuspręsti, kai tai yra tinkama, stebėti, kaip įgyvendinamos audito ataskaitoje pateiktos nuomonės / išvados / rekomendacijos reikalavimų nevykdymo atvejais. *(4000-ojo TAAIS 232 punktas)*

399. Valstybės kontrolė turi tinkamai pranešti apie savo veiksmų po audito rezultatus, kad galėtų pateikti grįžtamąjį ryšį įstatymų leidžiamajai institucijai, vykdomajai valdžiai, suinteresuotosioms šalims ir visuomenei. Patikima informacija apie rekomendacijų įgyvendinimo būklę, auditų ir susijusių korekcinių veiksmų atlikimo poveikis gali padėti parodyti Valstybės kontrolės vertę ir naudą.

400. Veiksmai po audito apima audito rekomendacijų įgyvendinimo stebėseną ir audito poveikio įvertinimą. Audito poveikio vertinimas pradedamas vykdant rekomendacijų priemonių įgyvendinimo stebėseną ir baigiamas patvirtinus audito rekomendacijų įgyvendinimo ir poveikio vertinimo ataskaitą valstybės kontrolieriaus nustatyta tvarka.

401. Už veiksmų po audito atlikimą yra atsakingas Valstybės kontrolės Planavimo ir poveikio departamentas. Rekomendacijų įgyvendinimo stebėseną ir audito poveikio įvertinimą reglamentuoja *Valstybinio audito rekomendacijų pateikimo ir įgyvendinimo stebėsenos tvarkos aprašas* ir *Valstybinio audito poveikio vertinimo metodika*.

PRIEDAI

Informacinių technologijų audito vadovo
1 priedas

Pavyzdinis dokumentų (duomenų) sąrašas susipažinimui su organizacijos veikla ir IT valdymu

Nr.	Dokumentai (duomenis)
1.	Organizacijos strateginiai dokumentai, veiklos ataskaitos
2.	Organizacijos nuostatai, įstatai
3.	Organizacijos struktūros schema, padalinių nuostatai
4.	Personalo valdymo politika, informacija apie IT žmogiškuosius išteklius (suplanuotų, užpildytų etatų skaičius), taikomą kompetencijų modelį, informacija apie paskirtus saugos įgaliotinius (fizinės saugos, IT saugos, asmens duomenų saugos, kt.)
5.	IT strategija, IS plėtros planai, infrastruktūros pajėgumų plėtros planai
6.	IT padalinio nuostatai, pareigybių aprašymai, atsakomybių sąrašas pagal valdomas arba tvarkomas IS
7.	Teisės aktai, kurie susiję su organizacijos veikla, vidinės tvarkos, procedūrų aprašai, standartai, kurie aprašo IT procesus, saugumo politikos dokumentai
8.	IT architektūros schema
9.	Sąrašas valdomų, tvarkomų IS (administracinės ir pagrindinių funkcijų vykdymui skirtų), jų nuostatai, techninė specifikacija
10.	Techninės įrangos sąrašas
11.	Tinklo architektūros schemos
12.	IT biudžetas, detalus IT išlaidų sąrašas
13.	IT įgyvendintų ar įgyvendinamų projektų sąrašas
14.	IT pirkimų sąrašas
15.	Informacija apie turimus duomenų centrus, serverines
16.	Informacija apie debesijos paslaugas, kuriais naudojasi organizacija
17.	Tvarkomų duomenų sąrašas, detalizuojant kritinius duomenis ir sąsają su IS
18.	Duomenų bazės lentelių išrašas, detalizuojant ryšius tarp lentelių
19.	Tiekėjų sąrašas ir jų teikiamos paslaugos
20.	IT paslaugų katalogas
21.	IS naudotojų vadovai
22.	IT padalinio ataskaitos
23.	Informacija apie nustatytų IT veiklos rodiklių (angl. KPI), paslaugų lygio susitarimo rodiklių (angl. *SLA*) vykdymo rezultatus
24.	IS naudotojų ir jų prieigos teisių matrica
25.	Atliktų IT auditų ataskaitos
26.	Savęs vertinimo (angl. *self-assessments*) ataskaitos
27.	Naudotojų pasitenkinimo teikiamomis IT paslaugomis vertinimo dokumentai
28.	Pakeitimų, užklausų, incidentų (ir saugumo), problemų sąrašas
29.	Veiklos tęstinumo ir atstatymo planai
30.	Rizikų registras ir jų tvarkymo planas, ir saugumo rizikų (organizacijos ir IT, jei sudaromi atskirai)

IT procesų gebos vertinimas pagal COBIT metodiką

Kiekvieno vertinamo proceso geba išreiškiama balais nuo 0 iki 5. Kuo aukštesnis proceso gebos lygis, tuo brangesnis proceso vykdymas ir mažesnė rizika, kad procesas nepasieks numatyto tikslo.

Nustatydami vertinimo apimtį, auditoriai turėtų pasirinkti, kuriuos IT procesus reikės vertinti. Pasirinkimas turėtų būti atliekamas atsižvelgiant į organizacijai aktualius veiklos tikslus, t. y. panaudojus COBIT tikslų hierarchijos sąsajas, nustatant galimus vertintinus procesus.

Vertinimo proceso metu reikia nustatyti, ar buvo pasiekti konkretūs procesų atributai, kurie priskirtini 1–5 gebos lygiui. Kiekvienas proceso atributas vertinamas naudojant vertinimo skalės reikšmes: N; P; L; F. Pasiekimo proc. nustatomas vertintojo priimtu profesiniu sprendimu atsižvelgiant į nustatytus faktus.

Sutrumpinimas	Aprašymas	Kiek proc. pasiekta
N – nepasiektas	Nėra arba beveik nėra faktų, įrodančių, kad atliekant proceso vertinimą nustatytas atributas yra pasiektas.	0–15
P – iš dalies pasiektas	Yra tam tikrų faktų, įrodančių, kad atliekant proceso vertinimą nustatyti proceso atributai yra iš dalies pasiekti ir kad buvo taikomas tam tikras atributo siekimo metodas. Kai kurie atributo pasiekimo aspektai gali būti nenuspėjami.	>15–50
L – didžiąja dalimi pasiektas	Yra faktų, įrodančių, kad atliekant proceso vertinimą nustatyti proceso atributai yra iš esmės pasiekti ir kad buvo taikomas sisteminis atributo siekimo metodas. Vertinamame procese gali būti tam tikrų silpnųjų vietų, susijusių su šiuo atributu.	>50–85
F – visiškai pasiektas	Yra faktų, įrodančių, kad atliekant proceso vertinimą nustatyti proceso atributai yra visiškai pasiekti ir kad buvo taikomas išsamus ir sisteminis atributo siekimo metodas. Vertinamame procese nėra jokių svarbių silpnųjų vietų, susijusių su šiuo atributu.	>85–100

1-as gebos lygio atributas, skirtingai nuo 2–5 gebos lygių, vertinamas pagal knygos „COBIT procesų vertinimo modelis, naudojant COBIT5“ 3 skyriuje „Procesų perspektyva ir proceso atlikimo rodikliai“ kiekvienam procesui nurodytas bazines praktikas ir darbo produktus.

2–5 gebos lygių vertinimas yra pagrįstas bendraisiais proceso gebos rodikliais, kurie nurodyti minėtos knygos 4 skyriuje „Proceso gebos rodikliai“.

Gebos lygiai		Procesų atributai	Kada laikoma, kad gebos lygis pasiektas
0 lygis	Nevykdomas: procesas neįgyvendintas arba nepasiekia jam keliamų tikslų	-	
1 lygis	Vykdomas: vykdant procesą yra pasiekiami proceso tikslai	Proceso atlikimas	Proceso atlikimas: L–F
2 lygis	Valdomas: procesas valdomas, o jo rezultatai yra tinkamai apibrėžti,	2.1. Proceso vykdymo valdymas 2.2. Darbo produktų valdymas	1.1. Proceso atlikimas: F 2.1. Proceso vykdymo valdymas: L–F 2.2. Darbo produktų valdymas: L-F

Gebos lygiai		Procesų atributai	Kada laikoma, kad gebos lygis pasiektas
	kontroliuojami ir palaikomi		
3 lygis	Apibrėžtas: standartinis procesas yra apibrėžtas ir naudojamas visoje organizacijoje	3.1. Proceso apibrėžimas 3.2. Proceso įdiegimas	1.1. Proceso atlikimas: F 2.1. Proceso vykdymo valdymas: F 2.2. Darbo produktų valdymas: F 3.1. Proceso apibrėžimas: L–F 3.2. Proceso įdiegimas: L–F
4 lygis	Prognozuojamas: apibrėžtas procesas vykdomas nustatytose ribose	4.1. Proceso matavimas 4.2. Proceso kontrolė	1.1. Proceso atlikimas: F 2.1. Proceso vykdymo valdymas: F 2.2. Darbo produktų valdymas: F 3.1. Proceso apibrėžimas: F 3.2. Proceso įdiegimas: F 4.1. Proceso matavimas: L–F 4.2. Proceso kontrolė: L–F
5 lygis	Optimizuojamas:	5.1. Proceso inovatyvumas 5.2. Proceso optimizavimas	1.1. Proceso atlikimas: F 2.1. Proceso vykdymo valdymas: F 2.2. Darbo produktų valdymas: F 3.1. Proceso apibrėžimas: F 3.2. Proceso įdiegimas: F 4.1. Proceso matavimas: F 4.2. Proceso kontrolė: F 5.1. Proceso inovatyvumas: L–F 5.2. Proceso optimizavimas: L–F

Vertintojas pirmiausia patikrina, ar egzistuoja bendroji praktika ir ar ši praktika padeda pasiekti proceso rezultatus. Sukuriami bendrieji darbo produktai suteikia papildomų įrodymų, kad bendrosios praktikos buvo taikomos. Vertindamas šias praktikas ir rezultatus auditorius turi susieti teorinį COBIT modelį su organizacijos faktiškai vykdomais procesais.

Proceso gebos lygį galima laikyti pasiektu, jei didžiąja dalimi (L) ar visiškai (F) pasiekti proceso atributai. Jei gebos lygio visi atributai visiškai (F) pasiekti, vertinamas kitas gebos lygis. Kaip atlikti gebos vertinimą detaliai aprašyta ISACA knygose „Vertintojo vadovas naudojant, COBIT5“, „Procesų vertinimo modelis, naudojant COBIT5“.

Vertinant procesų gebą gali būti naudojamas pavyzdinis proceso gebos vertinimo formos šablonas. Apibendrinant visų procesų gebos lygių rezultatus, gali būti naudojamas procesų vertinimo rezultatų apibendrinimo formos šablonas. Šie šablonai pateikti Metodikos svetainės Šablonų skiltyje.

Įgimtos rizikos veiksnių sąrašas

Toliau išvardyti rizikos veiksniai nėra baigtiniai ir priklausomai nuo atliekamo audito – veiklos, finansinis, atitikties – gali būti aktualūs kiti įgimtos rizikos veiksniai. Auditorius turėtų visada įvertinti su sukčiavimu ir teisės aktų pažeidimais susijusią įgimtą riziką.

Įgimtos rizikos veiksniai, susiję su IT strateginiu valdymu ir IT plėtros programomis:

- ✓ IT strategijos sudėtingumas, neaiškūs ir nerealistiški IT strateginiai tikslai;
- ✓ organizacijos veiklos ir IT plėtros prioritetai ir tikslai labai skiriasi;
- ✓ esamų IT programos finansavimo arba tinkamumo finansuoti taisyklių pakeitimas;
- ✓ sudėtingi, neįprasti arba didelės vertės IT plėtros sprendimai;
- ✓ tokio pobūdžio veikla, kuri tradiciškai laikoma itin paveikiama sukčiavimo arba korupcijos rizikos (pvz., IT viešieji pirkimai);
- ✓ skubūs veiksmai (pvz., pagalba ekstremaliųjų situacijų atveju) arba veiksmai, kuriems nėra visapusiškai taikomos įprastos kontrolės priemonės;
- ✓ tikslų neatitinkantys IT valdymo kriterijai (angl. KPI) (per platūs, pernelyg ribojantys, nesvarbūs);
- ✓ veiklos administravimas, apimantis sudėtingą IT turto vertinimą ar gautų prekių ir paslaugų sąnaudų apskaičiavimą (pvz., kai sutartyse nustatytos kainų koregavimo formulės);
- ✓ konkretūs dalykai, paminėti vidaus ir išorės audito ataskaitose, spaudoje ir kt.

Įgimtos rizikos veiksniai, susiję su organizacine struktūra ir žmogiškaisiais ištekliais:

- ✓ geografiškai suskaidyta organizacija, kurioje yra daug išsibarsčiusių teritorinių vienetų;
- ✓ neaiškus atsakomybės pasidalijimas IT padalinyje;
- ✓ neaiškus atsakomybės pasidalinimas tarp IS valdytojo ir tvarkytojo;
- ✓ IT procesai arba IT projektai, kuriuose dalyvauja daug partnerių (koordinavimo problemos, silpnos valdymo ir ryšių struktūros);
- ✓ IT padalinio per maža arba per didelė personalo kaita;
- ✓ IT veiklos sritis, kurioje IT padalinio personalas neturi patirties arba turi tik ribotą patirtį;
- ✓ veikla, kuri yra labai priklausoma nuo nedidelio pagrindinių darbuotojų skaičiaus;
- ✓ nepakankamas personalas, žemos kvalifikacijos, nepatyrę, menkai motyvuoti darbuotojai arba vadovybė;

- ✓ dažni organizacinės struktūros pasikeitimai;
- ✓ konkretūs dalykai, paminėti vidaus ir išorės audito ataskaitose, spaudoje ir kt.

Įgimtos rizikos veiksniai, susiję su *IT infrastruktūra*:

- ✓ pasenusios IT programinės, techninės įrangos naudojimas;
- ✓ diegiamos naujos technologijos, kurios dar nėra išbandytos;
- ✓ skirtingų technologijų gausa;
- ✓ neaiški, sudėtinga IT architektūra;
- ✓ daug įvairių integracijų tarp IS posistemių;
- ✓ per didelė priklausomybė nuo vieno tiekėjo (pvz., įrangos tiekėjas turi išskirtinę priežiūros sutartį, yra vienintelis detalių ir medžiagų, programinės įrangos ir kt. tiekėjas);
- ✓ neatliekamas infrastruktūros pažeidžiamumų testavimas;
- ✓ IT turto išeikvojimas arba vagystė;
- ✓ Vidaus auditas neatlieka IT auditų, neturi kompetencijų atlikti tokio pobūdžio auditų;
- ✓ konkretūs dalykai, paminėti vidaus ir išorės audito ataskaitose, spaudoje ir kt.

Kompiuterizuotos audito priemonės (CAAT)

CAAT yra IT priemonės, padedančios auditoriui atlikti įvairius automatizuotus, detaliuosius testus ir įvertinti IT sistemą, kontrolės priemones arba duomenis. Jos labai naudingos, jeigu didelė dalis audituojamo subjekto duomenų yra prieinami elektroniniu formatu. CAAT nauda:

- ✓ didelių apimčių duomenų detalųjį testavimą ir analizę galima atlikti greičiau ir paprasčiau;
- ✓ testus galima lengvai pakartoti su skirtingais failais ar duomenimis;
- ✓ keičiant parametrus galima parengti lanksčius ir sudėtingus testus;
- ✓ audito testai ir jų rezultatai dokumentuojami automatiškai;
- ✓ efektyviau naudojami audito ištekliai.

Naudojant CAAT atsiranda išlaidų, susijusių su licencijuota programine įranga, suderinama techninė įranga ir kvalifikuoto audito personalo darbu. Todėl sprendžiant, ar atliekant IT auditą naudoti CAAT, reikia atsakyti į šiuos klausimus:

- ✓ ar CAAT naudojimas suteikia auditui papildomą vertę;
- ✓ ar testai bus naudojami kituose arba ateities audituose audituojant tą patį arba kitą veiklos pobūdžiu ir veikla panašų subjektą;
- ✓ ar operacijos apdorojamos internetu (*on-line*) ir (arba) realiu laiku;
- ✓ ar kitų audito metodų naudojimas lems didesnes išlaidas ir papildomą auditui skirtą laiką.

Žinomų CAAT pavyzdžiai:

- ✓ bendrosios paskirties audito programinė įranga kuriama taip, kad atitiktų specifinius auditorių reikalavimus. Į ją įeina įprasti testai, kuriuos atlieka IT auditą vykdantys auditoriai, ir bendrosios funkcijos, pvz., duomenų gavybos (angl. *extraction*), apibendrinimo, pasenusių duomenų identifikavimo, stratifikacijos, dublikatų tikrinimo ir t. t.;
- ✓ duomenų gavybos (angl. *data mining*) įrankiai padeda atrasti struktūras dideliuose duomenų rinkiniuose, išgauti informaciją iš šių rinkinių ir konvertuoti ją į suprantamą struktūrą tolesniam naudojimui per duomenų vizualizaciją;
- ✓ konkrečiai pramonės šakai skirta audito programinė įranga kuriama siekiant tokio funkcionalumo, kuris padėtų vykdyti bendras audito funkcijas, susijusias su konkrečiomis pramonės šakomis. T. y., panaudojama specifinė pramonės šakos logika kuriant audito užklausas ir t. t. Tokia programinė įranga naudojama pramonės šakose, kuriose veiklos procesai yra gerai dokumentuoti ir nusistovėję, pvz.: bankininkystės, gamybos, naftos ir dujų, krovinių gabenimo ir kitose;

- ✓ paslaugų (angl. *Utility*) programos atlieka funkcijas, skirtas padėti analizuoti, konfigūruoti, optimizuoti ar palaikyti IT infrastruktūrą. Pagrindiniai su auditu susijusių paslaugų programų pavyzdžiai, be kita ko, yra versijų kontrolės paslaugų programos, klaidų paieškos programos (angl. *debuggers*), disko vietos analizatoriai, failų valdymo bei tinklo paslaugų valdymo ir sistemos aplinkos (angl. *system profilers*) programos;

- ✓ gerai išvystytose sistemose integruoti audito moduliai (specializuota audito programinė įranga), kuriantys standartizuotas ir specializuotas ataskaitas. Šios funkcijos integruotos į įmonės išteklių planavimo (angl. *Enterprise Resource Planning; ERP*) programas. Be to, egzistuoja standartinė programinė įranga, kuri suteikia IT auditoriams prieigą prie ERP duomenų su skaitymo teisėmis per sąsaja grįstas programas;

- ✓ duomenų analizės įrankiai, kurie leidžia įkelti, tvarkyti, transformuoti gautus duomenų rinkinius ir juos įvairiai analizuoti, rašyti duomenų analizės skriptus, pateikti įvairius grafikus ir formuoti analizės ataskaitas;

- ✓ saugumo analizės įrankiai – tai platus priemonių rinkinys, kuris apima tinklo analizės įrankius, pažeidžiamumo vertinimo priemones, taikomųjų programų saugumo analizės įrankius, pan. Šie įrankiai sudaro prielaidas nustatyti saugumo rizikas, turimus saugumo trūkumus ir pažeidžiamumus;

- ✓ kiti įrankiai, kurie gali būti naudingi audito metu, pvz.: braižyti procesus, leidžiantys daryti duomenų ekstrakcijas, atlikti teksto kokybinę analizę, leidžiantys daryti transkripcijas, apibendrinti ir kitaip analizuoti skirtingo formato tekstinius failus, vaizdus, garso ar vaizdo įrašus.

Auditorius, norintis naudoti CAAT priemones konkrečios srities auditui atlikti, turėtų turėti pakankamai žinių ir kompetencijos naudotis atitinkamomis CAAT priemonėmis. Prieš pradedant auditą su duomenų analizei skirtomis CAAT priemonėmis svarbu suprasti ir gauti informaciją apie subjekto turimus duomenis, lentelių ar failų ryšius, duomenų bazių žodyną, duomenų dydį arba formatą, kitą reikiamą informaciją.

Naudojant CAAT priemones gali būti naudojami tęstiniai duomenys, pvz., tikrinant įdiegtų kontrolės priemonių tinkamumą. Svarbu turėti aktualius ir reikiamos apimties tęstinius duomenis, todėl auditorius prieš paleisdamas CAAT su tęstiniais duomenimis turi apgalvoti tai, kokių duomenų jam reikės tokioms procedūroms atlikti.

Taikomųjų programų kontrolės priemonių vertinimas

Išankstinio tyrimo metu auditorius turi suprasti, kaip taikomoji programa veikia. Šiuo tikslu rekomenduojama peržiūrėti taikomosios programos nuostatus, techninę specifikaciją ir kitus techninius dokumentus, atlikti pokalbius su IS naudotojais ir, esant poreikiui, vystytojais.

Surinkus informaciją apie taikomąją programą ir jos vykdomas funkcijas rekomenduojama:

- ✓ sudaryti testavimui atrinktų taikomųjų programų kontrolės priemonių (funkcijų ar plėtinių) ir jų aprašymų sąrašą, suskirstyti šias priemones pagal organizacijos veiklos procesus ir (arba) kontrolės tipus;
- ✓ parengti trumpą taikomosios sistemos aprašymą (schemą), nurodyti pagrindinius posistemius ir jų tikslus, kaip vyksta veiklos procesai posistemyje ir duomenų apsikeitimas tarp posistemių, kaip ir iš kokių šaltinių informacija įvedama, kaip ir kur išvedama, kokios integracijos realizuotos su išorės sistemomis, pagrindines tvarkomas duomenų bylas, apytiksliai kokios yra transakcijų apimtys ir kt. IS funkcijų schema turi būti tiek detali, kad auditoriui būtų aišku, kokie pagrindiniai veiklos procesai atliekami sistemoje ir kaip jie nuosekliai vyksta. Siekiant sudaryti IS veikiančių procesų schemą galima naudoti CAAT, kurie pagal operacijų įrašų žurnalus (angl. *Log*) ar kitą programos saugomą informaciją išgauna duomenis apie veikiančius procesus ir juos atvaizduoja.

Kad auditorius suprastų, kaip auditui aktuali taikomoji programa veikia, kokias operacijas nuo proceso pradžios iki pabaigos atlieka, rekomenduojama išankstinio tyrimo metu atlikti IS veikimo nuoseklios peržiūros testą. Jei IS yra sudėtinga, toks testas būtinas ir jį reikėtų atlikti kelis kartus, siekiant geriau susipažinti su IS veikimo mechanizmu.

Susipažinus su IS, surinkus informaciją apie IT bendrosios kontrolės ir veiklos rizikas, remiantis IT audito vadove nurodytu rizikos atrankos modeliu, auditoriai turi atrinkti (jei neplanuojama testuoti visas kontroles) reikšmingiausias taikomųjų programų kontrolės priemones detaliajam testavimui. T. y. nebūtina testuoti visų taikomosios programos kontrolės priemonių, tačiau susitelkti į tas, dėl kurių netinkamo veikimo gali atsirasti grėsmė organizacijos pagrindinei veiklai, jos rezultatams. Finansinio audito atveju turėtų būti atsirenkamos kontrolės priemonės, kurios susijusios su reikšmingo iškraipymo rizika, t. y. atsirenkamos tos, kurios yra atsakas į minėtas rizikas ir mažina jų neigiamą poveikį finansų apskaitos tinkamumui ir teisingumui.

Siekiant tinkamai atlikti taikomųjų programų kontrolės priemonių (funkcijų ar plėtinių), kurios yra atrinktos, testavimą, svarbu pasirinkti tinkamus testavimo metodus. Praktikoje gali būti naudojami klasikiniai audito metodai (išsamiau apie juos pateikta Metodikos svetainės Audito metodų skiltyje), tačiau šiuo atveju gali būti pasirenkami ir specifiniai metodai, kuriuos taiko programinės įrangos testavimo specialistai, pvz.: sprendimų medis, ribinių verčių analizė, naudojimo atvejo testavimas, klaidų spėjimas, tiriamasis testavimas, kt. Norėdamas praktikoje naudoti šiuos metodus, auditorius turi išmanyti teorinius ir praktinius jų taikymo aspektus.

Apsisprendus dėl testavimo metodų, parengiami taikomųjų programų kontrolės priemonių testavimo klausimynai (testai), pagal kuriuos vertinamos šios priemonės. Atsižvelgę į testuojamos IS specifiką auditoriai turėtų parengti savo poreikiams pritaikytą taikomosios programos kontrolės priemonių testavimo klausimyną (-us) (testus). Rekomenduojama juos parengti išankstinio tyrimo metu, bet galima ir pagrindinio tyrimo metu, bet tokiu atveju klausimynams sudaryti atitinkamai audito plane turi būti suplanuotas laikas.

Rengiant taikomųjų programų kontrolės priemonių testus turi būti išanalizuota techninė ir kita su atitinkama priemone susijusi dokumentacija: pateikiami reikalavimai, kaip ši priemonė turi veikti praktikoje (funkciniai veiklos reikalavimai). Auditorius, rengdamas klausimynus, gali pasinaudoti pavyzdiniu testavimo scenarijų sąrašu (pateikiama žemiau). Taip pat galima išanalizuoti organizacijos taikytus testavimo scenarijus, susijusius su testuojamomis kontrolės priemonėmis (kurie buvo atlikti programinės įrangos kūrimo ar jos modernizavimo, modifikavimo metu) ir, jei minėti scenarijai yra tinkami ir jais galima pasitikėti, juos panaudoti rengdamas savo testavimo klausimynus. Jei tinka, gali būti naudojami ir ankstesnių auditų testavimo scenarijai.

Parengus klausimynus, ten kur tinkama turi būti parengti testavimui reikalingi duomenys. Jie gali būti gauti iš subjekto duomenų bazės arba savarankiškai sukuriami. Tęstinių duomenų apimtis priklauso nuo pasirinkto testuoti laikotarpio ir funkcijos veikimo konteksto. Tvarkant tęstinius duomenis turi būti laikomasi kibernetinio ir asmens duomenų saugumo reikalavimų. Tęstiniuose duomenyse negali būti naudojami asmens duomenys. Esant didelei duomenų apimčiai, rekomenduojama testuojant taikomųjų programų kontroles naudoti CAAT priemones, kurios gali palengvinti testavimo procesą, pvz., automatiniu būdu sugeneruoti reikiama duomenų rinkinį su užpildytomis reikšmėmis.

Testavimo metu auditorius turi patikrinti, ar pasirinkta testuoti kontrolės priemonė veikia taip, kaip nurodyta techninėje ar kitoje susijusioje dokumentacijoje. Jei testuojant nustatoma veikimo trūkumų (taikomosios programos kontrolės priemonė neveikia taip, kaip turi veikti pagal reikalavimus), vertinama, kad ši priemonė veikia neefektyviai ir ja negalima pasitikėti. Jei audituojamu laikotarpiu įvairiais etapais buvo taikomos iš esmės skirtingos taikomųjų programų kontrolės priemonės (pvz., laikotarpio pradžioje veikė viena, vėliau ji buvo pakeista arba patobulinta), kiekvieną iš jų reikia ištestuoti atskirai.

Automatinės kontrolės priemonės testuojamos IS tęstinėje aplinkoje, prie kurios prieigą suteikia audituojamas subjektas. Ši prieiga suteikiama laikantis audituojamo subjekto patvirtintos prieigos prie IS teisių suteikimo tvarkos reikalavimų.

Taikomųjų programų kontroles galima suskirstyti į:

- ✓ įvesties;
- ✓ apdorojimo;
- ✓ išvesties;
- ✓ taikomosios programos saugumo.

Tai yra bendrojo pobūdžio taikomųjų programų kontrolės, bet IS gali būti įdiegtos specifinės kontrolės, sukurtos atsižvelgiant į organizacijos veiklos specifiką.

Įvesties kontrolės priemonės

Kontrolės tikslas – įsitikinti, kad į taikomąją programą įvedami duomenys yra tikslūs, autentiški, išsamūs, anksčiau nebuvo naudojami ir įvedami tiksliai be dubliavimo tik tam įgaliojimus turinčių asmenų. Duomenų įvesties kontrolė ypač svarbi, siekiant išvengti taikomųjų programų klaidų, sukčiavimo atvejų ir užtikrinant taikomosios programos vientisumą. Duomenų įvesties kontrolė gali būti pripažinta esanti netinkama, jei taikomojoje programoje įdiegtas kontrolės priemones galima apeiti, o jos duomenis – pakeisti arba įvesti kitais būdais. Prieš testuojant gaunama reikiama prieiga prie bandomosios IS aplinkos ir reikiama rolė. Testuojamos visos galimos sąlygos arba variantai ir fiksuojama, ar IS reaguoja tinkamai į skirtingas sąlygas.

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
Pirminių dokumentų tvarkymo kontrolės	✓ Pirminių dokumentų rengimo ir įvedimo procedūros yra dokumentuotos. ✓ Užtikrinamas duomenų, suvestų į IS, atsekamumas su pirminiu dokumentu, pagal kurį informacija buvo suvesta (pvz., indeksas, data ir laikas). ✓ Yra netinkamų dokumentų grąžinimo procedūros ir tokių atvejų reguliarios peržiūros.	✓ Patikrinama, ar duomenų parengimo procedūros dokumentuotos, aiškios, atnaujintos ir atitinka praktikoje atliekamus duomenų parengimo veiksmus. ✓ Ištraukiamas tam tikro laikotarpio operacijų sąrašas ir patikrinama, ar operacijos turi ID, datos ir laiko žymas, ar pagal jas galima atsekti su kuriais pirminiais dokumentais jie susiję, pvz., tam tikras transakcijos ID susiejamas su atitinkamos sąskaitos faktūros numeriu. ✓ Patikrinama, ar pagal nustatytus kriterijus patikrinus, ar dokumentai, kurių informacija turi būti suvesta į IS, yra tinkami; jei jie netinkami, vykdoma grąžinimo procedūra. ✓ Patikrinama, ar reguliariai vykdomos dokumentų grąžinimų peržiūros procedūros, peržiūrima susijusi dokumentacija, kurioje užfiksuotas peržiūros faktas (ataskaitos, protokolai, tarnybiniai raštai, kt.).
Įvedamų duomenų tikrinimo, validavimo kontrolės	✓ Finansų verčių pagrįstumo ir apribojimų patikros. ✓ Formato ir privalomų laukų patikros, standartizuoti įvesties laukai. ✓ Sekos (pvz., trūkstamų elementų), diapazono ir turinio	✓ Vienu atveju užpildomi visi privalomi laukai, kitu – privalomi laukai paliekami neužpildyti (visi kartu, paeiliui po vieną, kt. variantai). ✓ Laukeliuose, kur priimamas tik tekstas, vienu atveju užpildomas tekstas, kitu – suvedami skaičiai, simboliai, kt. Analogiškos procedūros

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
	(tam tikrų skaičių, teksto, kt.) patikros. ✓ Kryžminės patikros, pvz., tam tikros sutartys galioja tik su tam tikrais įmokų kodais). ✓ Įvesties galimo dubliavimo patikrinimai, pvz., ar įvedant nėra pasikartojančių sąskaitų faktūrų. ✓ Įvestų duomenų galiojimo patikrinimai, pvz., kelionės data nepatenka į rezervacijos laikotarpį. ✓ Esant duomenų perdavimui iš vienos IS į kitą per sąsają, tikrinamas gautų visų duomenų išsamumas ir pagrįstumas, įskaitant datą, laiką, duomenų dydį, įrašų apimtį, šaltinio autentiškumo patvirtinimą ir kt.	atliekamos su laukeliais, kur turi būti įrašomi skaičiai. ✓ Į laukelius, kurie tikrina tam tikro įvesto turinio elementus (pvz., banko sąskaitos turinio logiką), įvedami visi reikiami elementai, kitu atveju – ne visi (pvz., įvedama sąskaita be LT). ✓ Jei laukelyje yra numatytas apimties apribojimas (pvz., įvesti galima tik nuo 5 iki 20 simbolių), suvedama tiek, kiek galima, ir mažiau ar daugiau simbolių negu galima. ✓ Suvedami besidubliuojantys, neteisingi įrašai, kuriuos sistema turi identifikuoti. ✓ Sulyginama perduotų ir gautų duomenų informacija: suma, data ir laikas. Taigi reikės gauti duomenis iš skirtingų šaltinių įvykių žurnalų ir juos palyginti.
Klaidų tvarkymo kontrolės	✓ Įestų duomenų klaidų fiksavimas ir pranešimas apie tai, sistemoje generuojant informaciją, kas blogai atlikta arba kokios klaidos nustatytos (klaidos pranešimas). ✓ Neleidžiama atlikti kito veiksmo, kol klaidos yra neištaisytos arba leidžiama jų nepaisyti. ✓ Jautrių operacijų taisymai, klaidų nepaisymai ir pan. gali turėti papildomų ribojimų, pvz., gali taisyti tik tam tikrą rolę turintis darbuotojas arba gavęs kito darbuotojo leidimą. ✓ Klaidų nepaisymo kontrolės priemonės, t. y. gali būti leidžiama sistemoje nepaisyti tik tam tikras klaidas, tokiu atveju sistema sutikrina atliktą klaidos nepaisymo veiksmą su atitinkama sąlyga.	✓ Testuojami visi analizuojami atvejai, kai turi būti sugeneruotas klaidos pranešimas (pagal neigiamus testavimo scenarijus) ir fiksuojama, ar IS reaguoja tinkamai. ✓ Įvedama netinkama informacija ar atliekami netinkami veiksmai ir fiksuojama, ar pateikta klaidos informacija (pranešimas), ar ji atitinka įvykusios klaidos turinį. ✓ Bandoma atlikti kitą veiksmą sistemoje, nors prieš tai dar nėra ištaisyta klaida. ✓ Tikrinamos leidžiamos klaidų nepaisymo sąlygos, bandant atlikti veiksmus, kurie neatitinka nustatytų apribojimų. ✓ Jei tam tikrus klaidų taisymus turi peržiūrėti kitas asmuo, patikrinama, ar tai vyksta (auditorius turi prašyti suteikti jam atitinkamas dvi roles). ✓ Palyginama, ar sistemos žurnale yra užfiksuoti visi auditoriaus atlikti klaidingi veiksmai, jų taisymai, nepaisymo atvejai.

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
	✓ Visos klaidos ir jų taisymai ar nepaisymai fiksuojami sistemos žurnale. ✓ Tam tikrą laikotarpį neištaisytų klaidų kontrolės priemonės, pvz., pasibaigus taisymo terminui įgaliotiems asmenims siunčiami pranešimai apie tokius atvejus. ✓ Yra klaidų administravimo ir jų peržiūros procedūros. ✓ Yra generuojamos klaidų ir susijusių elementų ataskaitos, kurios periodiškai peržiūrimos.	✓ Nustatomas klaidų taisymo terminas (trumpas, pvz., 1 d.) ir patikrinama, ar neatlikus jokių taisymo veiksmų sistema nusiunčia atitinkamą rolę turinčiam asmeniui pranešimą apie tai. ✓ Peržiūrimos klaidų administravimo ir peržiūros procedūros, atliekami testavimo veiksmai pagal peržiūros etapus, ar jie atlikti. ✓ Sugeneruojamos visos klaidų ataskaitos, kurias turi generuoti sistema, patikrinamas jų turinys ir ar pateikia teisingą informaciją apie auditoriaus atliktus klaidingus veiksmus, jų taisymus, nepaisymo atvejus.
Įvesties autorizavimas, tvirtinimas ir prieigos teisių atskyrimas	✓ Yra sudarytas sąrašas atsakingų darbuotojų (priskirtos rolės), kurie gali įvesti į IS duomenis ir juos keisti, kitiems darbuotojams (rolėms) sistema to atlikti neleidžia. ✓ Sistemoje įdiegtas prieigos teisių atskyrimas, kai vienas darbuotojas negali atlikti visų proceso veiksmų, pvz., įvesties, patvirtinimo ir apmokėjimo. ✓ Yra įdiegtas įvestų duomenų patvirtinimo mechanizmas, pvz., antras darbuotojas kiekvienu atveju atlieka įvestų duomenų patvirtinimo veiksmą (keturių akių principas). ✓ Tam tikrais atvejais, kai atliekamos didelės vertės įvesties operacijos, turi būti gautas kito darbuotojo leidimas arba tvirtinimas, pvz., padalinio vadovo. ✓ Nesant tam tikro atsakingo darbuotojo tvirtinimo veiksmo, kai tai turi būti atlikta, sistema neleidžia įvykdyti kito veiksmo.	✓ Patikrinama, ar viską, ką testuojamoji rolė gali atlikti sistemoje duomenų įvedimo metu, jai leidžiama atlikti, patikrinami neleidžiami veiksmai, ar juos sistema blokuoja (rekomenduojama padaryti kiekvienai testuojamai rolei veiksmų sąrašą, ką galima atlikti ir ko ne, ir pagal tai žymėti testo rezultatus). ✓ Peržiūrima pareigybių (rolių) atskyrimo matrica, kuri parengta organizacijos (jei tokios nėra, auditorius turi parengti matricą ir joje nurodyti, kurios pareigybės neturi atlikti viena kitos funkcijų), ir pagal ją patikrinama, ar sistemoje šios rolės tinkamai atskirtos, t. y. su A rolės teisėmis atliekami veiksmai, kuriuos gali atlikti tik B rolę turintis asmuo, kuris negali atlikti turėdamas A rolę. Patikrinami visi galimi tikrinamų rolių variantai, pvz., testuojamas A, B, C rolių atskyrimas, testuojama ar: A gali atlikti B veiksmus, A gali atlikti C veiksmus, A gali atlikti B ir kartu C veiksmus; B gali atlikti A veiksmus, B gali atlikti C veiksmus, B gali atlikti A ir kartu C veiksmus; C gali atlikti A veiksmus, C

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
		gali atlikti B veiksmus, C gali atlikti A ir kartu B veiksmus. ✓ Vykdomos tam tikros operacijos (reikėtų identifikuoti visą jų sąrašą), kurių metu turi būti gauti reikiami patvirtinimai, ir patikrinama, ar įvykdžius operaciją galima toliau atlikti veiksmus negavus patvirtinimo iš atitinkamą rolę turinčio darbuotojo.

Apdorojimo kontrolės priemonės

Kontrolės tikslas – užtikrinti duomenų vientisumą ir apsisaugoti nuo apdorojimo klaidų per visą operacijos apdorojimo ciklą, t. y. nuo duomenų gavimo iš įvesties posistemės iki jų išsiuntimo į duomenų bazę arba išvesties posistemę. Šios kontrolės užtikrina, kad galiojantys įvesties duomenys būtų apdorojami tik vieną kartą ir kad klaidingų operacijų aptikimas nesutrukdytų galiojančių operacijų apdorojimui. Daugelis apdorojimo kontrolės priemonių yra tokios pačios kaip įvesties kontrolės priemonės, tačiau jos naudojamos apdorojimo operacijose.

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
Automatizuoti skaičiavimai	Atliekant konkrečius skaičiavimus pagal vieną ar daugiau įvesties ir saugomų duomenų elementų gaunami kiti duomenų elementai, pvz., darbo užmokesčio, delspinigių, paslaugos kainos, bendros sumos ar vidurkio apskaičiavimas.	Pagal specifikacijas nustatomi visi testuojami skaičiavimų scenarijai ir formulės (pvz., jei yra A+B+C sąlygos, apskaičiuojama suma X pagal formulę Nr. 1; jei yra A+B sąlygos, apskaičiuojama suma Y pagal formulę Nr. 2, kt.) ir įvedus reikiamus duomenis patikrinama, ar sistema apskaičiuoja reikiamas sumas ir ar rezultatas teisingas.
Duomenų tikrinimas, validavimo patikrinimai	✓ Įdiegtos kontrolės priemonės, kurios atlieka kryžminius sutikrinimus, pvz., įvestų duomenų eilučių suma tam tikru laikotarpiu sulyginama su skaičiumi į vieną failą agreguoto rinkinio eilučių, palyginami iš skirtingų šaltinių gauti tie patys skaičiai, kurie turi sutapti (pvz., likučių sutikrinimas, kliento pateiktos ir	✓ Tikrinant kontroles, kurios atlieka kryžminį sutikrinimą, į tęstinę aplinką įvedama netinkama informacija ir vertinama, ar kryžminis tikrinimas nustato klaidų, pvz., jei tikrinami kliento duomenys su duomenų bazėje esančiais, suvedami duomenys kliento, kurio duomenų bazėje nėra, arba suvedami klaidingi kliento duomenys, pvz., nurodomas neteisingas vardas, adresas, telefonas

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
	duomenų bazėje turimos informacijos sulyginimas). ✓ Įrašų dubliavimo patikrinimai, pvz., patikrinama, ar nėra pasikartojančių eilučių atlikus tam tikras apdorojimo operacijas. ✓ Duomenų bazėje esančių duomenų tikrinimai, pvz., tuščių įrašų, duomenų formatų, apribojimų, kt.	ir pan. Tikrinami visi galimi kryžminio tikrinimo variantai. ✓ Taip pat atliekamas teigiamas testas, kai suvedami visi tinkami duomenys, ir vertinama, ar sistema reaguoja tinkamai, nerodo klaidų. ✓ Tikrinant duomenų bazėje esančių duomenų tinkamumą, reikėtų turėti specifinių duomenų bazės veikimo ir SQL žinių. Organizacijoje gali būti įdiegtos automatizuotos duomenų kokybės užtikrinimo priemonės, kurios duomenų bazės lygiu atlieka kontrolės priemones, auditorius turi susipažinti, kokios apimties ir kurių elementų stebėseną ši sistema atlieka, peržiūrėti stebėsenos ataskaitas.
Klasifikatorių tikrinimas	✓ Pagal organizacijos veiklos poreikius IS klasifikatoriuose gali būti įvedami tam tikri įkainiai, lygiai ar kiti kintamieji, kurie vėliau naudojami automatiniuose skaičiavimuose ar apdorojimo procesuose. ✓ Konfigūracijos peržiūrimos ir atnaujinamos pagal įvykusius pokyčius arba tai atliekama nuolatos sutartu laiku.	✓ Patikrinkite, ar IS klasifikatoriuose įvesta aktuali informacija, ar konfigūracijos atitinka organizacijos veiklos poreikius, siekiant įsitikinti, jog operacijos vykdomos pagal iš anksto nustatytus parametrus ir leistinus nuokrypius. ✓ Peržiūrimi dokumentai, sistemoje fiksuoti istoriniai įrašai, įrodantys, kad reguliariai atliekamos klasifikatorių ir kitų konfigūracijų peržiūros.
Operacijų nuoseklumo, verslo taisyklių tikrinimas	✓ Operacijos sistemose vyksta tam tikra seka kaip nurodyta specifikacijoje. ✓ Sistema reaguoja į nustatytas verslo taisykles, pagal kurias ji sukurta.	✓ Pirmiausia reikia sužinoti ir suprasti verslo taisykles, kurios taikomos numatytai programai ar sistemos procesui. Tai gali apimti skirtingus reikalavimus, ribojimus arba logiką, kurią turi atitikti programa. ✓ Sudarykite verslo taisyklių žemėlapį (angl. *business rules mapping*), t. y. sąrašą, lentelę arba schemą, kurioje reikėtų nurodyti, kokia, kur ir kaip verslo taisyklė turi būti taikoma sistemoje ar procesui, kokia proceso seka. Tai padės palyginti numatytas taisykles su realia sistemos veikla. ✓ Pagal sudarytą verslo taisyklių žemėlapį patikrinkite, ar sistema

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
		veikia taip, kaip jose numatyta. Peržiūrėkite programos nustatymus, elgsenos scenarijus ir išorinius rezultatus, kad įsitikintumėte, jog jie visiškai atitinka šias taisykles. ✓ Lyginkite gautus rezultatus su verslo taisyklių žemėlapio duomenimis. Patikrinkite, ar sistemoje nėra neatitikimų, klaidų ar nenumatytų atvejų, kurie prieštarauja verslo taisyklėms.
Veiksmų stebėjimas (angl. *audit trails*)	✓ Sistemos žurnaluose (angl. *log*) fiksuojamos atliktos operacijos, pvz., veiksmų žurnale įrašoma, koks darbuotojas, kada ir kokį veiksmą atliko, kokios automatinės operacijos ir kada įvyko. ✓ Automatinis duomenų pakeitimų (pvz., po įvedimo veiksmo tam tikra informacija buvo pakeista, papildyta, ištrinta, kt.) stebėjimas, kuris susiejamas su atitinkamu naudotoju, kuris atliko pakeitimą. ✓ Automatiniai pranešimai atitinkamas pareigas turintiems asmenims apie fiksuotus sistemoje atliktus nejprastus veiksmus.	✓ Atliekamos įvairios operacijos, kurios vėliau palyginamos su sistemos žurnaluose fiksuotomis operacijomis, siekiant nustatyti, ar visi atlikti veiksmai fiksuojami, ar aišku, kas ir kada juos atliko. ✓ Atliekami duomenų keitimai, kurie palyginami su sistemos žurnaluose fiksuotomis keitimų operacijomis, siekiant nustatyti, ar visi atlikti keitimai fiksuojami, ar aišku, kas ir kada juos atliko. ✓ Patikrinama, ar specifikacijoje numatyti pranešimai, atlikus sistemoje tam tikrus nejprastus veiksmus, yra siunčiami tam tikriems darbuotojams.
Išsamumo (užbaigtumo) tikrinimas	Sistemoje gali būti privalomi laukai ar operacijos, kurių neatlikus negalima užbaigti operacijos, todėl sistema gali tikrinti, ar visiškai viskas atlikta.	✓ Atliekami veiksmai, kai sistemoje nėra užpildomi reikiami laukai arba tam tikros formos neprikabinamos, ar neatliekami reikiami žymėjimai, ir vertinama, ar sistema neleidžia užbaigti operaciją, kol visiškai nėra užbaigti reikiami veiksmai. Atliekami visi galimi scenarijai, pvz., neužpildomi duomenys, bet prikabinami visi reikiami dokumentai, arba neužpildomi duomenys (jų dalis) ir neprikabinami reikiami dokumentai ir pan. ✓ Atliekamas teigiamas testas, kai visi reikiami veiksmai sistemoje atliekami, dokumentai prikabinami ir procesas užbaigiamas.

Išvesties kontrolės priemonės

Tikslas – įsitikinti, kad taikomosios programos pateikiama išvestis yra išsami, tiksli, teisinga ir laiku pateikta.

Kontrolės tipas	Kontrolės pavyzdys	Galimi testavimo scenarijai
Išvesties formato tikrinimas	✓ Taikomoji programa apdoroja duomenų failą ir sugeneruoja išvesties failą. Išvesties failas turi turėti visus reikiamus laukus ir duomenis, kuriuos tikimasi gauti. ✓ Išvesties failas turi būti išvedamas konkrečiais formatais, pvz., *csv*, *pdf*, *xlsx*.	✓ Tikrinama, ar programa tinkamai sugeneruoja išvesties failą su visais laukais ir duomenimis pagal turimą formą, standartą, pvz., turi būti išvesta tam tikros formos ataskaita arba turi būti išvestas *MSExcel* failas, kuriame turi būti tam tikri stulpeliai su užpildyta tam tikra informacija. Sugeneravus ataskaitą ar atitinkamą failą tikrinama, ar yra visi jam privalomi laukai, elementai, viskas užpildyta ir pan. Tikrinama, ar reikiama failo struktūra ir visi elementai pateikiami visuose dokumentuose, kurie sugeneruoti skirtingais formatais. ✓ Generuojami failai skirtingais formatais, kurie turi būti sugeneruoti pagal techninę dokumentaciją.
Duomenų tikslumo tikrinimas	✓ Išvesties ataskaitoje sugeneruojami duomenys, kurie turi būti tikslūs ir pateikti tokį rezultatą, kurio tikimasi, pvz., darbų ataskaitoje pateikiami apskaičiuoti tam tikrų darbų rodiklių rezultatai, o pirkimų ataskaitoje pateikiamos planuotų ir įvykdytų pirkimų sumos. ✓ Sistema automatiškai pagal tam tikras taisykles sutikrina generuojamo išvesties rezultato tikslumą ir, esant klaidoms, pateikia klaidos pranešimą, pvz., sutikrinama, ar įvesta bendra suma sutampa su išvesties ataskaitoje pateikiama bendra suma.	✓ Į bandomąją sistemą įvedami tam tikri duomenys ir patikrinama, ar po atliktų apdorojimo operacijų ataskaitose išvedama tiksli ir teisinga informacija, pvz., įvedami įvykdytų pirkimų duomenys, kurių bendra vertė 10 tūkst. Eur, sugeneruojama pirkimų ataskaita ir patikrinama, ar išvesties suma yra 10 tūkst. Eur. ✓ Jei sistema ataskaitoje turi pateikti įvykdytų viešųjų pirkimų vidurkį dviem skaičiais po kablelio, patikrinama ar išvesties duomenyse pateikiamas tikslus pirkimų vidurkis, kurio tikimasi, t. y. pagal turimus duomenis apskaičiuojama, koks turi būti vidurkio rezultatas, ir jis palyginamas su ataskaitoje nurodytais išvesties duomenimis. ✓ Jei žinoma apie tam tikrus keitimus, galima patikrinti, ar išeities duomenys tikslūs ir atsižvelgia į šiuos keitimus, pvz., 10 mėn. buvo įtrauktas naujas produktas, tokiu atveju nuo 10 mėn.

		peržiūrima, ar išvesties duomenys įskaito ir informaciją apie naują produktą. ✓ Jei nėra galimybės pagal įvesties ir išvesties rezultatus patikrinti duomenų tikslumo, gali prireikti atlikti kodo peržiūrą ar kitus specifinius testus, siekiant įvertinti, ar kontrolė suprojektuota tinkamai ir yra įdiegta. Tokiam tikrinimui atlikti reikės turėti specifinių techninių IT žinių.
Išvesties rezultatų peržiūra	✓ Išvedant duomenis iš duomenų bazės į svetainę ar kitą šaltinį, atliekamos rankinės peržiūros ar automatiniai sutikrinimai dėl išvesties tinkamumo, pvz., darbuotojas patikrina, ar kitoje sistemoje išvesti duomenys buvo visa apimtimi perduoti. ✓ Išvedamas failas ar ataskaita privalomai peržiūrimi atsakingo darbuotojo dėl tinkamumo, atitikties, galimų klaidų.	✓ Peržiūrimos esamos procedūros ir ataskaitos, kuriose turi būti nustatytos funkcijos dėl išvesties kontrolės vykdymo, peržiūrimos priežiūros ataskaitos. ✓ Peržiūrimi incidentai, kurie susiję su išvesties klaidomis, identifikuojama, ar tai nėra susiję su peržiūros kontrolės neefektyviu veikimu.
Prieiga prie išvesties duomenų	✓ Prieiga prie išvesties duomenų gali būti suteikta tik tam tikrą rolę turintiems darbuotojams, pvz., duomenų, kurie paleidžiami atlikti mokėjimus bankui, išvestis gali autorizuoti tik finansų padalinio vadovas. ✓ Tam tikras jautrias ataskaitas apie darbuotojus, jų darbo rezultatus gali matyti tik tam tikro padalinio vadovas, vadovaujantis atitinkamiems darbuotojams.	✓ Identifikuojamos darbuotojų rolės, kurios turi teisę prieiti prie tam tikrų išvesties duomenų. Gaunamos reikiamos rolės darbuotojų, kurie gali ir negali prieiti prie tam tikrų ataskaitų. Turint rolę, kuri visiškai neturi prieigos prie ataskaitų, bandoma sugeneruoti visas ataskaitas. Arba turint rolę, kuri gali tik tam tikras ataskaitas peržiūrėti, bandoma generuoti kitas, kurių ji negali matyti. ✓ Taip pat tikrinama, ar sistema generuoja visas ataskaitas, kurias gali peržiūrėti tam tikrą rolę turintis darbuotojas, pvz., tam tikras darbuotojas gali peržiūrėti 5 ataskaitas, bandoma jas visas generuoti.

Taikomosios programos saugumo kontrolės

Kontrolės tikslas – įsitikinti, ar taikomoji programa užtikrina pagrindinių duomenų bylų apsaugą.

Testuojant programos saugumą paprastai patikrinama kaip įgyvendinamos prieigos prie duomenų procedūros (slaptažodžio politikos įgyvendinimas, prieigos teisių valdymas, kt.). Fizinė ir loginė prieiga prie taikomosios programos pagrindinių duomenų bylų (angl. *master data files*) turi būti ribojama ir kontroliuojama. Pagrindinių duomenų pakeitimus gali atlikti tik įgalioti asmenys, o jų atliekami veiksmai turi būti tinkamai kontroliuojami. Taikomosios programos pakeitimų procedūros turėtų būti tinkamai dokumentuotos, valdomos įgaliotų vadovų ir vėliau peržiūrimos atsakingų asmenų. Pagrindinių duomenų bylų ir juose esančių įrašų vientisumas turėtų būti patvirtinamas periodiškai juos suderinant su nepriklausomai saugomais įrašais, pvz., duomenų bylų atsarginėmis kopijomis.

Jei pildant bendrosios kontrolės vertinimo klausimyną, buvo išanalizuotas saugumo klausimas ir jo apimtyje išnagrinėtas prieigos prie auditui aktualios IS valdymo ir kiti saugumo klausimai, tai atliekant taikomosios programos kontrolės priemonių testus pakartotinai saugumo priemonių vertinti nėra būtina, išskyrus atvejus, jei bendrosios kontrolės vertinimo klausimyne atsakyta ne į visus reikiamus aspektus.