Eksperdi kaasamise ja siseaudiitori töö kasutamise[[1]](#footnote-2) raampõhimõtted Virtuaalvääringu teenuse pakkuja (VASP) auditeerimisel

**Sisukord**

[Sissejuhatus ja raampõhimõtete eesmärk 1](#_Toc116589297)

[1. Lepingueelsed tegevused 2](#_Toc116589298)

[2. Lepingute sõlmimine 3](#_Toc116589299)

[3. Planeerimine/Riskihindamine 4](#_Toc116589300)

[4. Töö teostamine 4](#_Toc116589301)

[5. Eksperdi kokkuvõte ja aruandlus 5](#_Toc116589302)

[Lisa 1: Info, mida IT audiitor vajab, selleks, et teha pakkumine vandeaudiitorile tema kaasatuse tarbeks finantsauditis 6](#_Toc116589303)

[Lisa 2: Teenust osutava organisatsiooni 1. tüüpi ja 2. tüüpi aruanded 7](#_Toc116589304)

[Lisa 3: Siseaudiitori poolt teostatavad näidisprotseduurid 9](#_Toc116589305)

[Lisa 4: Väited 13](#_Toc116589306)

# Sissejuhatus ja raampõhimõtete eesmärk

Käesolevad raampõhimõtted on mõeldud abistamaks audiitoreid ja neid, keda audiitor eksperdina kaasab. Põhimõtete koostamisel oleme lähtunud rahvusvahelise auditeerimise standardi ISA (EE) 620 põhimõtetest, kuid käesolev dokument ei asenda seda standardit ega ole ainuüksi piisav standardi nõuete mõistmiseks. Küll võib raampõhimõtetest olla kasu VASPide audiitorkontrolli kontekstis eksperdi töö ulatuse määramisel. Käesolev dokument ei anna ette kindlaid protseduure, mida ekspert audiitori töö toetamiseks teeb ning dokumendis viidatud protseduuride näidised ei ole ammendavad. Näidiste kasutamisel tuleb arvestada asjaoluga, et Audiitorkogu ei kanna vastutust näidiste kasutamisest tuleneda võivate kahjude osas. Raampõhimõtete rakendamisel on vajalik kutsealase otsustuse rakendamine; dokument ei pruugi olla antud teema osas kõikehõlmav ega ole mõeldud asendama asjakohaseid regulatsioone ega vastavasisulisi rahvusvahelisi standardeid.

# Lepingueelsed tegevused

* 1. Pakkumuse tegemiseks asjakohase info küsimine kliendilt (sh RABile taotlusega esitatavad dokumendid[[2]](#footnote-3)) ja info avalikest allikatest otsimine -> otsustus, kas ekspert kaasata kooskõlas standardiga ISA (EE) 620[[3]](#footnote-4) või mitte. IT audiitori kaasamisel võib töömahu hindamisel olla vajalik ka info, mis on loetletud lisas 1.
		1. Siseauditi funktsioonist arusaam (sh. kliendi nõusolekul kaaluda otsesuhtlust).
		2. VASPi äritegevuseks oluliste väliste teenuse pakkujate tuvastamine ning selliste teenuse pakkujate puhul 1. tüüpi või 2. tüüpi (vt lisa 2) aruande olemasolu väljaselgitamine kooskõlas ISA 402 nõuetega.
	2. Eksperdi kompetentsuse, sõltumatuse, eetika hindamine kooskõlas standardiga ISA (EE) 620 (sh arvestada IT standardi/raamistiku kasutamisega töövõtus, kui asjakohane)

*Selgituseks: Audiitor peab hindama, kas audiitori eksperdil on audiitori eesmärkide seisukohast vajalik kompetentsus, võimekused ja objektiivsus. Audiitori väliseksperdi puhul peab objektiivsuse hindamine hõlmama järelepärimist huvide ja suhete kohta, mis võivad tekitada ohu selle eksperdi objektiivsusele.[[4]](#footnote-5)*

* + 1. Kompetentsus on seotud audiitori eksperdi eriteadmiste olemuse ja tasemega.
		2. Võimekus on seotud audiitori eksperdi võimega rakendada seda kompetentsust töövõtutingimustes. Võimekust mõjutavad tegurid võivad hõlmata näiteks geograafilist asukohta ning aja ja ressursside kättesaadavus.
		3. Objektiivsus on seotud nende võimalike mõjudega, mida erapoolikus, huvide konflikt või teiste mõju võib avaldada audiitori eksperdi kutsealasele või ärialasele otsustusele.
		4. Asjaolude hulka audiitori eksperdi kompetentsuse, võimekuste ja objektiivsuse hindamisel kuulub see, kas selle eksperdi töö allub töö tehnilistele läbiviimise standarditele või muudele kutsealastele või majandusharu nõuetele, näiteks kutseorganisatsiooni või majandusharuliidu eetikastandarditele ja muudele liikmelisusega seonduvatele nõuetele, litsentse andva organisatsiooni akrediteerimisstandarditele või seadusest või regulatsioonist tulenevatele nõuetele.
	1. Audiitor sõlmib potentsiaalse kliendi ja potentsiaalse eksperdiga konfidentsiaalsuskokkuleppe (sh kliendi aktsept konkreetse eksperdi projekti kaasamise kohta[[5]](#footnote-6)).
	2. Eksperdi töömahu (tunnid ja hind) määramine.

# Lepingute sõlmimine

* 1. Klient ja audiitorettevõtja
		1. teenuseks raamatupidamise aastaaruande audit/ülevaatus ja/või omavahendite nõuetele vastavuse kontroll
		2. soovitame eksperdi kaasamisel kaaluda järgmiste lõikude modifitseerimist[[6]](#footnote-7):
			1. Lepingu täitjad
			2. Lepingu kestvus (tunnid)
			3. Lepingu maksumus
			4. Konfidentsiaalsus
	2. Audiitorettevõtja ja ekspert

*Selgituseks: muuhulgas peab audiitori eksperdiga lepingu sõlmimisel arvestama, et leping peab olema kirjalik ja, kui asjakohane, sätestama järgmised asjaolud (vt ISA 620 lõik 11 ja lõigud A23–A31 ja ISA 620 lisa 1):*

Kokku tuleb leppida vähemalt:

* + - 1. Teenuse sisu ehk lepingu ese, sh järgitavad põhimõtted või standardid, töö tulem ja töö üleandmine-vastuvõtmine
			2. Aeg, kestvus, tähtaeg, maksumus
			3. Eksperdi poolt töö dokumentatsiooni üleandmine ja konfidentsiaalsus-kohustus
			4. Audiitori seadusest tulenev vastutus (AudS § 49 lg 2), ekspert vastutab samadel alustel

Soovitame tutvuda ka Audiitorkogu kodulehel avaldatud VASPi audiitorkontrolli lepinguid puudutavate materjalidega.

# Planeerimine/Riskihindamine

**Eksperdi töö eesmärk 1:** ekspert kirjeldab audiitori jaoks VASPi süsteemi või siis veendub VASPilt saadud süsteemikirjelduse vastavuses tegelikkusele.

* 1. Selgita välja, millega siseaudiitor tegeleb ja kas seda saab järgneva töö osas kasutada (vt lisa 3).
	2. Olemasolu korral omanda ja tutvu VASPi äritegevuseks oluliste väliste teenuse pakkujate 1. tüüpi või 2. tüüpi aruannetega.
	3. Süsteemi kaardistamine, protsesside ja kontrollide kirjeldus, sh:
		1. Kaardista kõik keskkonnad, mille kaudu FIAT raha ja virtuaalvääringu ülekanded toimuvad.
		2. Süsteemi ülesehituse usaldusväärsuse hindamine.
		3. Rahakottide asukohad ja arhitektuur.
		4. Hot/cold wallets. Enimkasutatud aadressid.
		5. Kuidas on tagatud varadele juurdepääs? Privaatvõtmete haldus.
		6. Kolmandate osapoolte poolt pakutavate teenuste sertifikaadid.

**Eksperdi töö eesmärk 2**: tuvasta väärkajastamise riskid ja disaini vastuseks protseduurid

* + 1. pettuse riskid;
		2. tuvastatud vead;
		3. vigade esinemise tõenäosus;
		4. rahapesu (AML) riskid;
		5. turvariskid (kliendi vara kaotamise/varastamise võimalikkus).

# Töö teostamine

**Eksperdi töö eesmärk 3**: veenduda (vastavalt nimetatud asjakohasele standardile/raamistikule), et platvormi(de)l/tegevuskeskkonnas toimunud tehingud ja saldod on kajastatud andmetes C,A,E,V,R&O,P (täielikkus, täpsus, olemasolu, väärtuse hindamine, omandiõigus, esitusviis, vt lisa 4), teostades sel eesmärgil protseduurid, näiteks (NB! Protseduuride loetelu ei ole ammendav):

* + 1. Programmi muutuste (*manage change)* ja juurdepääsu õiguste (*user rights*) kontrollide testimine.
		2. Kliendilt saadud andmefaili kontrollimine vs avalikud andmed (sh andmete täielikkuse kontroll).
		3. Andmefaili kontrollimine vs raamatupidamine.
		4. *Offchain transactions* (tehingute, mida ei saa avalikust allikast kontrollida) kontroll.
		5. Tuvastasime, kas vara kuulub ettevõttele järgneva alusel… (rights&obligations)
		6. ISACA poolt välja töötatud Blockchain Framework Audit Program kohased järgnevad protseduurid: ISACA väljatöötatud programm, mis koosneb järgnevatest elementidest: Governance, Infrastructure, Data Management, Key Management, Smart Contracts ja on kättesaadav ISACA kodulehel[[7]](#footnote-8).
		7. *Whitepaperis* kirjeldatud token’i iseloomustuse ja reaalse koodi võrdlemine – kas *token* toimib nii nagu on ette nähtud. Plokiahelas võib olla mitmeid osapooli, kes saavad koodi kontrollida ja seda ka teevad ning annavad ka avalikke hinnanguid. Ekspert hindab, kas kolmandate isikute poolt juba läbi viidud kontrollid ja nende hinnangud on usaldusväärsed ja kas on vaja teatud osi koodist ka ise üle kontrollida.

# Eksperdi kokkuvõte ja aruandlus

Eksperdi aruanne peab olema kirjalik ja sisaldama vähemalt järgnevaid elemente

* 1. Kes oli ekspert, sh kirjeldada kompetentsust, võimekust ja objektiivsust ning sõltumatust[[8]](#footnote-9) (näiteks, kas on rakendatud mõne eriala organisatsiooni sõltumatuse raampõhimõtteid või arvestusala kutseekspertide eetikakoodeksi sõltumatuse nõudeid)
	2. Informatiivne kokkuvõte tehtud töö kohta, mis on järelduse aluseks, sh
		1. Mis standardi kohaselt töö teostati
		2. Mis oli töö ulatus (milliseid infosüsteeme käsitleti, mis oli vaadeldav periood, mis olid käsitletavad küsimused ja muu asjakohane) ja eesmärk
		3. Millised olid protseduurid
	3. Millised olid leiud
	4. Järeldus/kokkuvõte/arvamus
	5. Allkiri ja kuupäev

# Lisa 1: Info, mida IT audiitor vajab, selleks, et teha pakkumine vandeaudiitorile tema kaasatuse tarbeks finantsauditis

* VASPi poolt RABile esitatud IT süsteemide kirjeldus
* IT audiitor vajab teavet selle kohta, mis on auditi kriteeriumid - nt milliste regulatsioonide alusel seda auditit tehakse, mille auditeerimist seal nõutakse jne.
* Mis on auditi skoop, kas käsitlusalasse kuulub kogu ettevõtte tegevus või soovitakse seda kitsendada vaid ühe tootega/teenuse vms muuga
* Ligikaudne ülevaade, palju on teenuseid/põhiprotsesse, mis skoopi kuuluvad?
* Palju on töötajaid ettevõttes?
* Palju on IT-töötajaid?
* Kas ettevõte teeb IT ise või ostab väljast infra, arenduse, halduse?
* Kas on olemas infoturbejuht?
* Kas on olemas andmekaitsespetsialist?
* Kas on olemas riskijuht?
* Kas riskihaldus on loodud ja juurutatud? Kas riskihaldus on asutuses tervikuna juurutatud või ainult infoturbe vaatest?
* Kas ISMS on juurutatud?
* Kui palju on seotud poliitikaid, protseduure, juhendeid juba valmis, mida tuleb hindamisel läbi vaadata ja analüüsida (dokumentide arv ja ca lehekülgede arv kokku)
* Mis on ajaline raam, mis ajaks on vaja audit teostada?
* Mis on audiitori hinnangul maht antud töödeks?
* Millisel kujul, mis formaadis ja kui pikk peab olema auditi lõpptulemus, mis tulemust oodatakse?
* Kas auditi tulemusel eeldatakse protsesside toimivuse ja dokumentatsiooni kontrollimist või ka tehnilise kontrolle? Kui soovitakse tehnilisi kontrolle, siis milliseid ja mis ulatuses?

Standardid/raampõhimõtted, millest juhindumist IT audiitor lubada saab:

* Üldistest standarditest saaks eeldada ISO 27000 seeria standardeid ja E-ITSi, aga konkreetsemad standardid/raamistikud/põhimõtted peaksid sõltuma auditi kriteeriumitest (vt ülal infovajadus)

# Lisa 2: Teenust osutava organisatsiooni 1. tüüpi ja 2. tüüpi aruanded

On ettevõtteid, kes ostavad nende äritegevuse teatud aspektid sisse teenust osutavalt organisatsioonilt. Paljud selliste organisatsioonide poolt osutatavad teenused on majandusüksuse ärialase põhitegevuse lahutamatuks osaks, kuid ei ole finantsaruannete auditi seisukohast asjassepuutuvad. Finantsaruannete auditi seisukohast on majandusüksuse sisseostetavad teenused asjassepuutuvad kui need teenused ja kontrollid nende üle on osa auditeeritava ettevõtte infosüsteemist, sh osa finantsaruandluse seisukohast olulistest seotud äriprotsessidest.

Kui audiitor ei ole võimeline omandama teenust osutavast organisatsioonist piisavat arusaamist otse, sest tal puudub vastavateks protseduurideks ligipääs, saab audiitor (olemasolu korral) teostada protseduure ja toetuda 1. või 2. tüüpi aruandele[[9]](#footnote-10).

1. tüüpi aruanne on aruanne kontrollide kirjelduse ja ülesehituse kohta teenust osutavas organisatsioonis, milles sisaldub:

(i) teenust osutava organisatsiooni juhtkonna poolt koostatud teenust osutava organisatsiooni süsteemi, kontrollieesmärkide ja määratud kuupäeva seisuga kavandatud ja rakendatud seotud kontrollide kirjeldus ja

(ii) teenuse osutaja audiitori aruanne, mille eesmärgiks on edastada põhjendatud kindlus ja mis sisaldab teenuse osutaja audiitori arvamust teenust osutava organisatsiooni süsteemi, kontrollieesmärkide ja seotud kontrollide kirjelduse kohta ning kontrollide ülesehituse sobivuse kohta määratud kontrollieesmärkide saavutamiseks;

2. tüüpi aruanne on aruanne kontrollide kirjelduse, ülesehituse ja nende toimimise tulemuslikkuse kohta teenust osutavas organisatsioonis, milles sisaldub:

(i) teenust osutava organisatsiooni juhtkonna poolt koostatud kirjeldus teenust osutava organisatsiooni süsteemi, kontrollieesmärkide ja seotud kontrollide kohta, nende ülesehituse ja rakendamise kohta määratud kuupäeva seisuga või kogu määratud perioodi jooksul ja mõningatel juhtudel nende toimimise tulemuslikkuse kohta kogu määratud perioodi jooksul ja

(ii) teenuse osutaja audiitori aruanne, mille eesmärgiks on edastada põhjendatud kindlus ja milles sisaldub:

a. teenuse osutaja audiitori arvamus teenust osutava organisatsiooni süsteemi, kontrollieesmärkide ja seotud kontrollide kirjelduse kohta, kontrollide ülesehituse sobivuse kohta määratud kontrollieesmärkide saavutamiseks ja kontrollide toimimise tulemuslikkuse kohta ja

b. teenuse osutaja audiitori poolt läbiviidud kontrollide testide ja nende tulemuste kirjeldus;

Teenust osutav organisatsioon võib tellida, et teenuse osutaja audiitor raporteerib tema kontrollide kirjelduse ja ülesehituse kohta (1. tüüpi aruanne) või tema kontrollide kirjelduse ja ülesehituse ning nende toimimise tulemuslikkuse kohta (2. tüüpi aruanne). 1. tüüpi või 2. tüüpi aruandeid võib välja anda rahvusvahelise kindlustandvate teenuste standardi (International Standard on Assurance Engagements, ISAE) 3402 järgi või standardite järgi, mille on kehtestanud volitatud või tunnustatud standardeid kehtestav organisatsioon (mis võib kasutada muid nimetusi, näiteks A- või B-tüüpi aruanded).

# Lisa 3: Siseaudiitori poolt teostatavad näidisprotseduurid

Üldine

* Riskide kaardistamine suures pildis, kus keskenduda kriitilisematele kohtadele hilisemates auditites. Mis meetodikat kasutatakse? Kuidas toimub *follow-up*? Millistele allikatele tuginetakse riskide hindamisel?
* Siseprotseduurid üldisemas vaates, kas on olemas RahaPTS § 14? Kas sisemised protseduurid kirjeldavad sisemisi protsesse või on üldised? Kas formaalsed nõuded on täidetud (st kes protseduuri kinnitas, kes on omanik, kui tihti toimub uuendamine, kas töötajatele on tutvustatud), kas on arvesse võetud ka juhendeid?
* Riskihindamine, -isu (kas protseduurid on olemas RahaPTS §10, §13) ja kas neid on hinnatud esialgse riskiisuga? Kas on võetud arvesse rahvusvahelisi standardeid riskide hindamiseks, on formaalsed nõuded täidetud? Kuidas riskide hindamine on üldse üles ehitatud, kuidas toimub kaitseliinide vaheline tööjaotuse jagamine, kes kinnitab riskide hindamised?
	+ Kas ja kuidas sätestatakse kliendi riskid ja jälgitakse neid? Kas kliendi riskide hindamiseks on koostatud riskimudel (mis võtab arvesse kõrge riski indikaatoreid), mis on aluseks riski muutmisele?
	+ Kas kõrge riskiga kliendiga ärisuhte loomisel on võetud arvesse seadusest tulenevalt kooskõlastamise protsessi (lähi juhatuse liikme või tema poolt volitatud isik)?

KYC protsessid:

* Isiku tuvastamine – kas tehnilised nõuded infotehnoloogiliste vahendite abil tuvastamisel on vastavad (kui kogu äri ja isikutuvastamine toimub infotehnoloogiliste vahendite abil)? Millist informatsiooni/andmeid kasutatakse isikuandmete verifitseerimisel? Mis andmete alusel käib isikusamasuse tuvastamine, mis andmed salvestuvad, kas on piisav andmete pakett (versus seadus)? Testid (vt nt iga 10. kliendisuhte loomist, kas on piisav?).
* Juriidiliste isikute tuvastamine – milliste dokumentide alusel ning kuidas on kontrollitud nende õigsust? Testimised.
* Kuidas on *onboard*’itud *Merchant*’e ja nende kliente (kui aktsepteeritakse *Merchant*’e)?
* Kuidas on välditud kliendisuhet *shell bank*’idega?

Tooted/Teenuse osutamine

* Kas hinnatakse tooteid/teenuseid enne nende aktsepteerimist? Milline on protseduur selleks?
* Kas teenust osutatakse P2P ja/või B2B?
* Kas on teenuseid edasi antud ja millistel tingimustel, kas on tehtud leping ja koolitused?
* Kolmandate osapoolte hindamine, lepingud, tegelik teenuse osutamine.
* Kas ettevõte osutab teenuseid, mis on seotud „*decentralised exchanges*“?
* Teenuste osutamine kõrge riskiga kolmandates riikides. Ülepiirilise teenuseosutamise puhul (ntx B2B), kuidas maandatakse riski kõrge riskiga (kolmandates) riikides teenuse osutamisel?
* Toote vastavuskontroll (kas näiteks KYC ja tehingute andmebaasis kajastub seadusega ette nähtud andmed; kas KYC ja tehingute andmebaas on seotud? Risk PEP tuvastamisel), sh siis RahaPTS § 46, § 47 (KYC andmete kogumine, säilitamine).

Kliendisuhte/tehingute monitoorimine (RahaPTS § 23) – kas süsteem annab automaatselt teada, et vaja kliendiandmeid uuendada, milliseid kliendiandmeid uuendatakse (püsivad vs muutuvad andmed), millisel teel/viisil andmeid uuendatakse, kas süsteemid toimivad, kuhu andmed liiguvad jne. Kas kliendisuhte/tehingute monitoorimine (juhendis kirjutatu) vastab KYC ja tehingute andmebaasi põhimõtetele (mingitel juhtudel tehingute andmebaasi ise midagi implementeerida ei saa, näiteks riskiriigid)?

* Kas monitooritakse kliendi asukohta (riskiriikide implementeerimine KYC/tehingute andmebaasi)?
* Kas virtuaalvääringu ostmisel/müümisel analüüsitakse ka vastaspoole rahakotte?
* Kas isik saab kasutada oma kontot juba enne raha depositeerimist oma nimeliselt pangakontolt?
* Kas igal isikul on ainult üks kasutajakonto, kuidas maandatakse riskid mitmete kontode loomisel iga isiku suhtes (IP-aadress, kas programmid tuvastavad VPN ühendusi jne)? Millised tehingu monitoorimise stsenaariumid on võimalikud?
* Mis hetkel sõlmitakse ärisuhe (kestvusleping) vs juhuti tehtav tehing (VASPidele keelatud).
* Kuidas toimub rahaliste vahendite/rikkuse allika tuvastamine? Testid.
* Tehingu skriining ja monitooring – mis funktsionaalused (see on põhjalikum hindamine)?
* Kuidas hoitakse *audit trail’*i (kas kirjakastis või on CRM), kas see info on kustutatav?
* Sanktsioonid – kas teostatakse ka lisaks manuaalseid kontrolle kliendiportfellile?

Teavitamine

* Kui on avastatud *red flag*’e, kas on teavitatud RABi, kas ja millistel juhtudel on ettevõtte sisene teavitamine käinud (mis liini pidi, kas õigete inimeste kaudu), kas kontaktisik analüüsinud kliendisuhet ning teavitanud sellest tulenevalt vajadusel RABi? Testimised.

Koolitused

* Kuna üldjuhul on VASPides vähe töötajaid, siis mis ametipositsioon on esimeses kaitseliinis, kas teda on koolitatud, kas ja kui tihti ta kontrollib kliendi *onboard*’imise kinnitamisi, tehinguid jne?
* Koolitused – kas on tehtud (üldine RahaPTS-st tulenev kohustus, pluss toote koolitused) ja kellele (kõik töötajad vs kliendisuhtega seonduvad kliendid)?

Andmekaitse

* Kliendi andmete uuendamine toimub vastavalt seadusele, kui palju klientide andmeid on uuendamata?

Raporteerimine

* Kommunikatsioon, suhtluskanalid. Kas info on ülevalt alla või alt üles liikuv?
* Ülevaated, koosolekute raportid (kas teavitatakse kuidagi uutest koosoleku protokollidest, kuidas toimub ettevõtte sisene teavitus, info liikumine?). Töötajatelt Kontaktisikule, Kontaktisikult RABile, üldine raporteerimine juhatusele.

Töötajad

* Ligipääsuõigused- mitmed inimesed on seotud erinevate ülesannetega?
* Kas võtmeisikute suhtes on tehtud hindamisi ja sellest näiteks RABi teavitatud?
* Kuidas on töötajaid värvatud – kas on seatud eelnevalt tingimused ametikohale, mis kanalit pidi on töötajaid otsitud ning mis kriteeriumite alusel on töötajaid värvatud?
* Kes on tegelikud juhid ettevõttes? Hinnata seda läbi auditite (nö vaikimisi), kuna see on olnud RABil üks olulisemaid kriteeriumeid *on-site* kontrollides. Kes võtavad vastu otsuseid? Kas ettevõtte tegevus toimub tegelikult Eestis?

Spetsiifilisemad küsimused:

* Does the company have cryptocurrency wallets for the purpose of its business?
* Which services does the company provide?
* Does the company issue, or has previously issued, digital tokens for the purpose of financing the company’s business or operations?
* Are tokens issued?
* Does the company have authorisation from its customers to access their private keys?
* How cryptocurrencies (hot/cold) and security measures are used?
* Does the company work with crypto foundations, individual miners or mining pools, ICO beneficiaries?
* Has the company ever received proceeds of a token offering from any company associated or linked with the company or any of the company’s directors or controllers?
* Does the company offer services that are related to the use of blockchain technology, such as tokenisation projects or cryptocurrency custody?
* What types of Virtual Assets does the business support or intend to support? How is listing organised (if applicable)?
* Does the business offer products and services that enable or allow for reduced transparency and increased obfuscation of financial flows?
* Does the business have the ability to mitigate the risks associated with transactions with heightened levels of anonymity?
* How does the business evaluate the implementation of travel rule amongst its VASP clients?

# Lisa 4: Väited

Väited tehinguklasside ja sündmuste ning seotud avalikustatava informatsiooni kohta auditeeritaval perioodil:

1. toimumine – tehingud ja sündmused, mis on kajastatud või avalikustatud, on toimunud ja puudutavad majandusüksust;
2. täielikkus – kõik tehingud ja sündmused, mis oleksid pidanud olema kajastatud, on kajastatud, ja kogu seotud avalikustatav informatsioon, mis oleks pidanud finantsaruannetes sisalduma, sisaldub neis;
3. täpsus — kajastatud tehingute ja sündmustega seotud summad ja muud andmed on asjakohaselt kajastatud ning seotud avalikustatav infomatsioon on asjakohaselt mõõdetud ja kirjeldatud;
4. periodiseerimine – tehingud ja sündmused on kajastatud õiges arvestusperioodis;
5. klassifitseerimine – tehingud ja sündmused on kajastatud nõuetekohastel kontodel;
6. esitusviis – tehingud ja sündmused on asjakohaselt koondatud või jagatud ja selgelt kirjeldatud ning nendega seotud avalikustatav informatsioon on asjakohane ja arusaadav, arvestades rakendatava finantsaruandluse raamistiku nõudeid;

Väited kontosaldode kohta ning seotud avalikustatava informatsiooni kohta perioodi lõpul:

1. olemasolu – varad, kohustised ja huvid omakapitalis on olemas;
2. õigused ja kohustused – majandusüksus on varade omanik või kontrollib õigusi varadele, ja kohustised on majandusüksuse kohustused;
3. täielikkus – kõik varad, kohustised ja huvid omakapitalis, mis oleksid pidanud olema kajastatud, on kajastatud ja kogu seotud avalikustatav informatsioon, mis oleks pidanud finantsaruannetes sisalduma, sisaldub neis;
4. täpsus, väärtuse hindamine ja jaotus – varad, kohustised ja huvid omakapitalis sisalduvad finantsaruannetes asjakohastes summades ning seotud avalikustatav informatsioon on asjakohaselt mõõdetud ja kirjeldatud;
5. klassifikatsioon – varad, kohustised ja huvid omakapitalis on kajastatud nõuetekohastel kontodel;
6. esitusviis – varad, kohustised ja huvid omakapitalis on asjakohaselt koondatud või jagatud ja selgelt kirjeldatud ning nendega seotud avalikustatav informatsioon on asjakohane ja arusaadav
1. Siseaudiitori töö kasutamist reguleerib rahvusvaheline auditeerimise standard ISA (EE) 610. Käesolevas dokumendis viitame siseaudiitorite tööle, et kirjeldada nende võimalikke tegevusi VASPide kontekstis ja viidata suhtluse tähtsusele teiste ekspertide töö ulatuse määramisel [↑](#footnote-ref-2)
2. Määratletud RahaPTS § 70 lg 3 – lg 4 [↑](#footnote-ref-3)
3. ISA (EE) 620 Audiitori eksperdi töö kasutamine [↑](#footnote-ref-4)
4. ISA (EE) 620 lõik 9 [↑](#footnote-ref-5)
5. Kuigi ISA standardid ega RahaPTS seda otseselt ei nõua, leiame, et selline eelnev kokkulepe võib olla otstarbekas [↑](#footnote-ref-6)
6. Vaata ka näidiseid <https://www.audiitorkogu.ee/est/metodoloogiakomisjoni-naidispohjad> [↑](#footnote-ref-7)
7. <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KtQ8EAK> [↑](#footnote-ref-8)
8. Esitada informatsioon, mille alusel audiitor saaks kompetentsust, võimekust ja objektiivsust hinnata [↑](#footnote-ref-9)
9. Täpsemad nõuded sätestab rahvusvaheline auditterimise standard ISA (EE) 402 Teenust osutavat organisatsiooni kasutava majandusüksuse auditi puhularvessevõetavad asjaolud [↑](#footnote-ref-10)