

PP/TF prevencijos vidaus kontrolės sistemos spragos. Kaip jas ištaisyti?

2026 m. rugsėjo 17 d.



Sukurta reguliuojamiems sektoriams

„ExpertLab“ yra nišinė konsultacijų įmonė, finansų įstaigoms teikianti platų spektrą paslaugų vieno langelio principu. Sujungiame praktines reguliacinės žinias su kliento poreikiais – **savo klientams suteikdami ir kompetencijas, ir reikiamus resursus, ir rinkos praktiką.**

Kas mus išskiria

Vieno langelio principas

Teikiame plačios apimties teisės, PPTFP, atitikties, rizikų valdymo, finansų ir HR paslaugas.

Individualus požiūris

Kiekvienas sprendimas pritaikomas pagal konkretaus kliento verslo modelį ir rizikos profilį.

Lanksti kainodara

Paslaugų kainodarą sutariame pagal projekto apimtį, sudėtingumą ir poreikius.

Klientas pirmoje vietoje

Nuo augančių įmonių iki įsitvirtinusių finansinių grupių – ta pati kompetencija, tie patys aukšti standartai.

ExpertLAB

2022

Įkurta

25

Ekspertai

50+

Aptarnautų finansų įstaigų



Apdrausta



PP/TF prevencijos pažeidimai kainuoja brangiai

Pažeidimų atvejai Europoje 2025 – 2026 m.



Institucija	Pažeidimo pobūdis	Bauda	Pajamų dydis	Bauda kaip % pajamų
 Coinbase Europe  Airija	Sandorių stebėsenos trūkumai; pavėluotas įtartinų operacijų nustatymas ir pranešimas.	€21,46 mln.	~€417 mln. (vidurkis 2021–2024 m.) ²	5,15%
 Monzo  Jungtinė Karalystė	Klientų rizikos vertinimo ir KYC / EDD kontrolės trūkumai.	€21,1 mln.	~£880 mln.	2,40%
 Nationwide  Jungtinė Karalystė	PP/TF rizikos valdymo ir vidaus kontrolės priemonių trūkumai.	€44,1 mln.	~£4,66 mlrd.	0,95%
J.P.Morgan  J.P. Morgan SE Vokietija	Klientų pažinimo, stebėsenos ir vidaus kontrolės trūkumai.	€45 mln.	€5,90 mlrd.	0,76%
 BARCLAYS  Barclays Bank plc Jungtinė Karalystė	Aukštos rizikos klientų patikros ir finansinių nusikaltimų kontrolės trūkumai.	€39,3 mln.	~£19,04 mlrd.	0,21%
Revolut  Revolut Bank UAB Lietuva	Dalykinių santykių ir operacijų stebėsenos trūkumai.	€3,5 mln.	€2,8 mlrd.	0,13%
 ABN AMRO  ABN AMRO Nyderlandai	Ilgalaikiai klientų pažinimo ir sandorių stebėsenos trūkumai.	€8,5 mln.	€8,72 mlrd.	0,10%

1 Naudotos paskutinių užbaigtų finansinių metų iki baudos skyrimo pajamos: 2025 m. baudoms – 2024 m. duomenys, 2026 m. baudoms – 2025 m. duomenys. Pajamos gali būti pateikiamos kaip „total income“, „operating income“ arba „gross revenues“ ir nėra visiškai palyginamos.

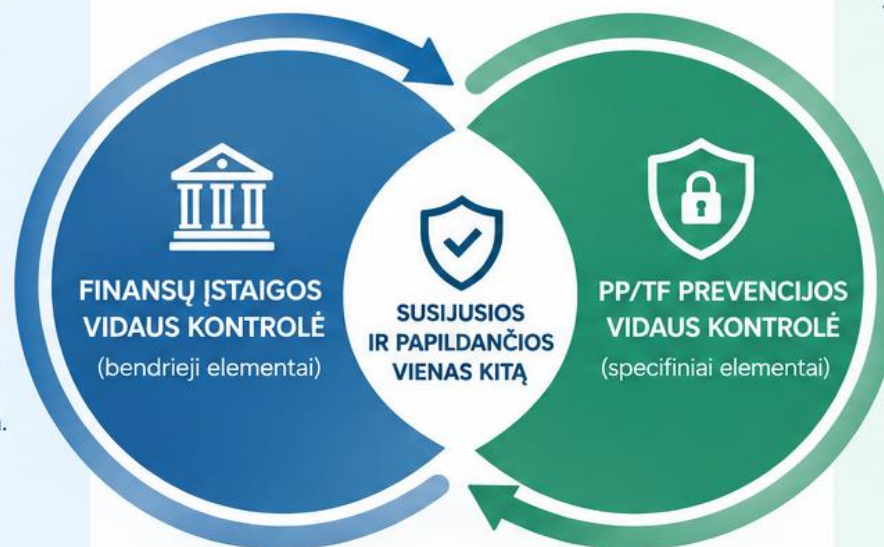
2 Coinbase Europe atveju Airijos centrinis bankas baudos nustatymui naudojo vidutines 2021–2024 m. metines pajamas (–€417 mln.).

Šaltiniai: BaFin, FCA, Central Bank of Ireland, DNB, Lietuvos bankas, institucijų metinės ataskaitos.

Finansų įstaigos vidaus kontrolė –

sistema, kuri padeda užtikrinti, kad įstaigos veikla būtų teisėta, efektyvi, patikima ir valdoma rizika.

- 1  Tinkama organizacinė struktūra, užtikrinanti vertikalius ir horizontalius ryšius.
- 2  Tinkama vidaus informacinė sistema.
- 3  Vidaus norminiuose aktuose nustatyta personalo atsakomybė ir kompetencija.
- 4  Dviguba veiklos procedūrų vidaus kontrolė.
- 5  Vadovybės informavimo sistema, leidžianti laiku priimti sprendimus.
- 6  Rizikos kontrolė ir rizikos valdymas.



PP/TF prevencijos vidaus kontrolės

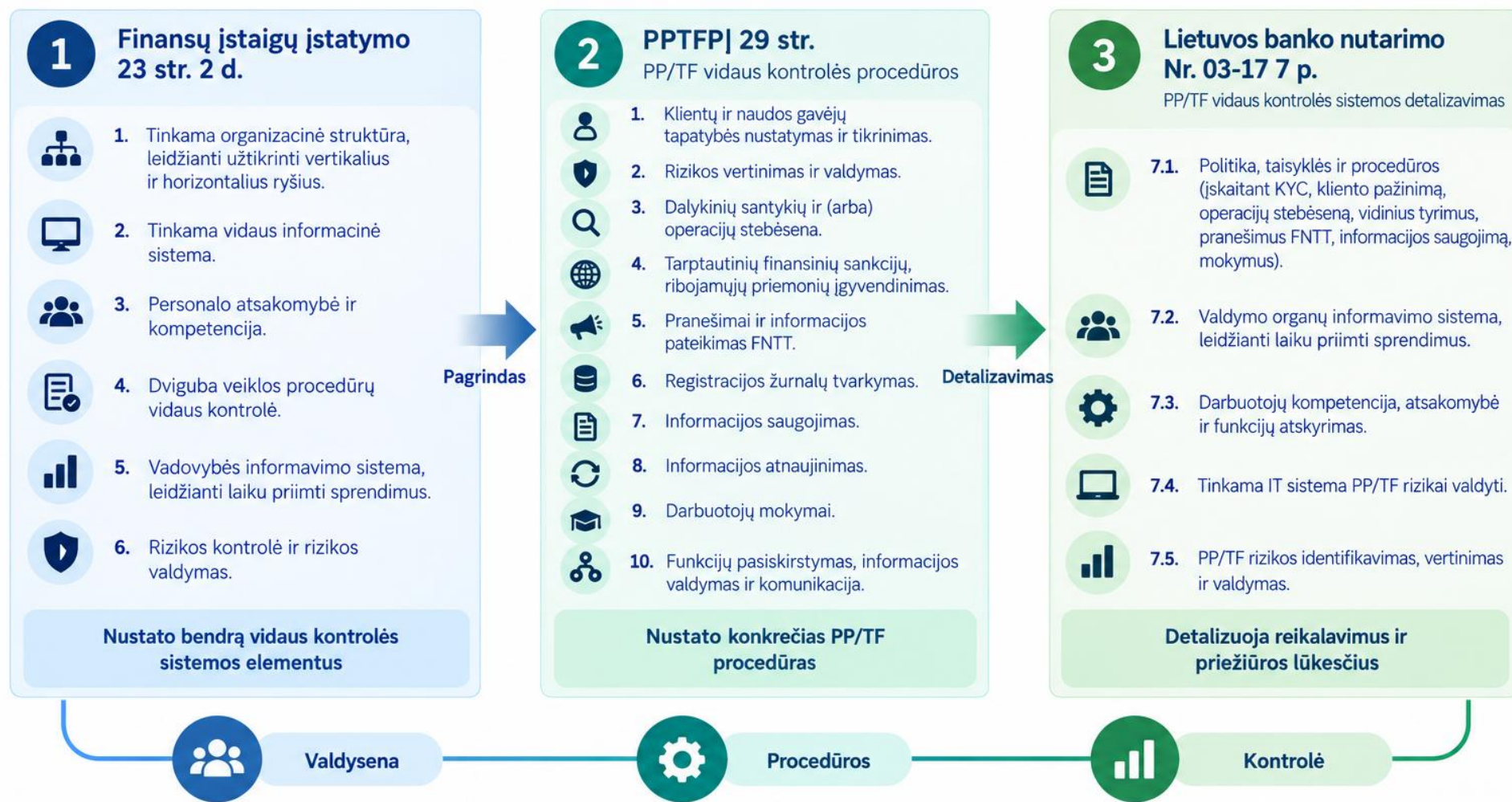
sistema – finansų įstaigos vidaus kontrolės dalis, skirta užkirsti kelią pinigų plovimo ir teroristų finansavimo rizikoms ir jas valdyti.

- 1  PP/TF prevencijos politika ir procedūros (KYC, klientų stebėsena, įtartinų operacijų tyrimas, pranešimai FNTT, informacijos saugojimas, mokymai ir kt.).
- 2  Valdymo organų informavimo sistema, leidžianti laiku priimti sprendimus dėl PP/TF rizikos valdymo.
- 3  Darbuotojų kompetencija, atsakomybė, funkcijų atskyrimas ir paskirstymas.
- 4  Tinkama IT sistema, užtikrinanti nenutrūkstamą duomenų kaupimą, apdorojimą ir panaudojimą.
- 5  PP/TF rizikos identifikavimas, vertinimas ir valdymas.



Šaltiniai: Finansų įstaigų įstatymo 23 str. 2 d. ir LB nutarimo Nr. 03-17 7 punktas.

PP/TF prevencijos vidaus kontrolės sistema



Šaltinis: FRD skirti nurodymuose, kuriais siekiama užkirsti kelią PP/TF

PP/TF rizikos valdymo 8 principai



Šaltinis: FRD skirti nurodymuose, kuriais siekiama užkirsti kelią PP/TF

Interesų konfliktų valdymas

Praktinis pavyzdys: organizacijos struktūra ir atskaitomybės linijos

Valdymo organai, komitetas ir pagrindinės funkcijos

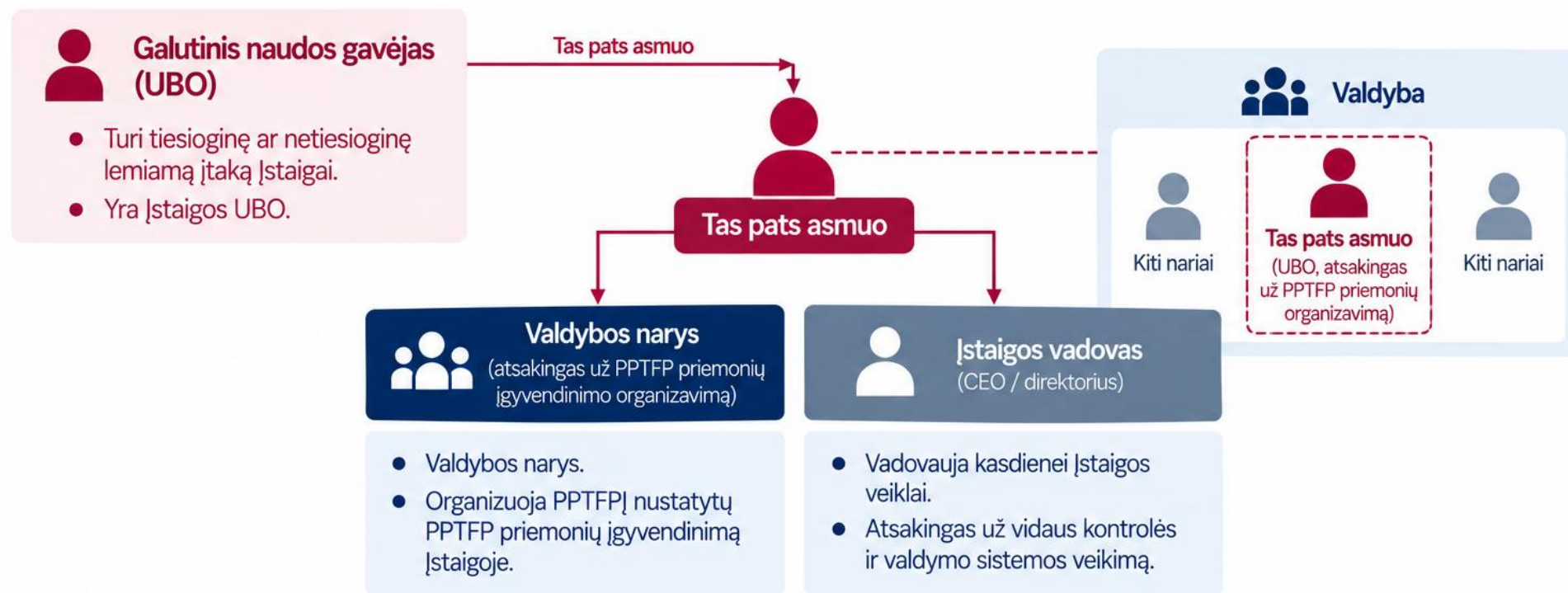


Galimi interesų konfliktai ir dual hatting pavyzdžiai

- Akcininkas A – vadovas ir valdybos narys (nuosavybės ir vykdomosios funkcijos derinys).
- CRO – valdybos narys ir komiteto narys (nepriklausomumo ir priežiūros objektyvumo klausimai).
- Akcininkas B – valdybos narys ir komiteto narys (sprendimų priėmimo koncentracija).
- 2 iš 3 valdybos narių yra akcininkai – kas reiškia, kad priežiūros ir valdymo funkcijos realiai nėra atskirtos.

Praktinis pavyzdys: UBO eina kelias funkcijas Įstaigoje

Tas pats asmuo yra UBO, valdybos narys, atsakingas už PPTFP priemonių organizavimą, ir Įstaigos vadovas

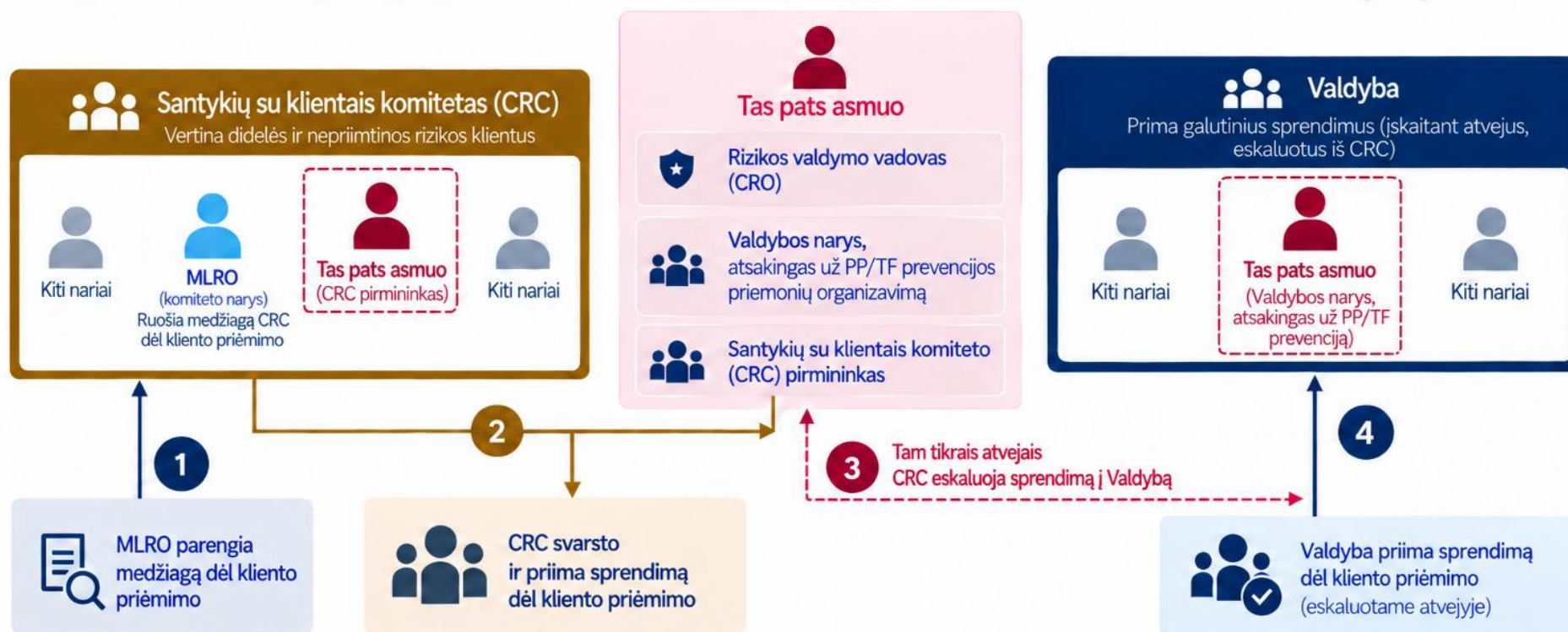


Galima interesų konflikto rizika

- Tas pats asmuo vienu metu yra Įstaigos UBO, valdybos narys, atsakingas už PPTFP priemonių įgyvendinimo organizavimą, ir Įstaigos vadovas.
- Tai lemia valdymo ir priežiūros funkcijų neskaidymą, asmens vaidmenų koncentraciją ir gali sudaryti potencialų interesų konfliktą.
- Iki gali turėti neigiamą poveikį valdymo sprendimų nepriklausomumui ir objektyvumui, net jei formaliai taikomasi interesų konfliktų valdymo taisyklių.

Praktinis pavyzdys: vieno asmens funkcijų koncentracija

Tas pats asmuo dalyvauja sprendžiant dėl kliento priėmimo tiek CRC komitete, tiek Valdyboje



Galima interesų konflikto rizika

- Tas pats asmuo eina tris pareigas Banke: Rizikos valdymo vadovas (CRO), Valdybos narys, atsakingas už PP/TF prevencijos priemonių organizavimą, ir Santykių su klientais komiteto (CRC) pirmininkas.
- MLRO, kuris yra CRC komiteto narys, rengia medžiagą dėl kliento priėmimo, o tas pats asmuo vėliau dalyvauja priimant sprendimą CRC lygmenyje ir (kai eskaluojama) Valdybos lygmenyje.
- Didelė funkcijų koncentracija viename asmenyje, kartu su dalyvavimu priimant sprendimus tiek CRC, tiek Valdyboje, gali mažinti funkcijų atskyrimą ir sukurti potencialų interesų konfliktą.
- Tai gali paveikti valdymo sprendimų nepriklausomumo ir objektyvumo suvokimą, net jei laikomasi formalių interesų konflikto taisyklių.

PPTFP vidaus kontrolės sistema

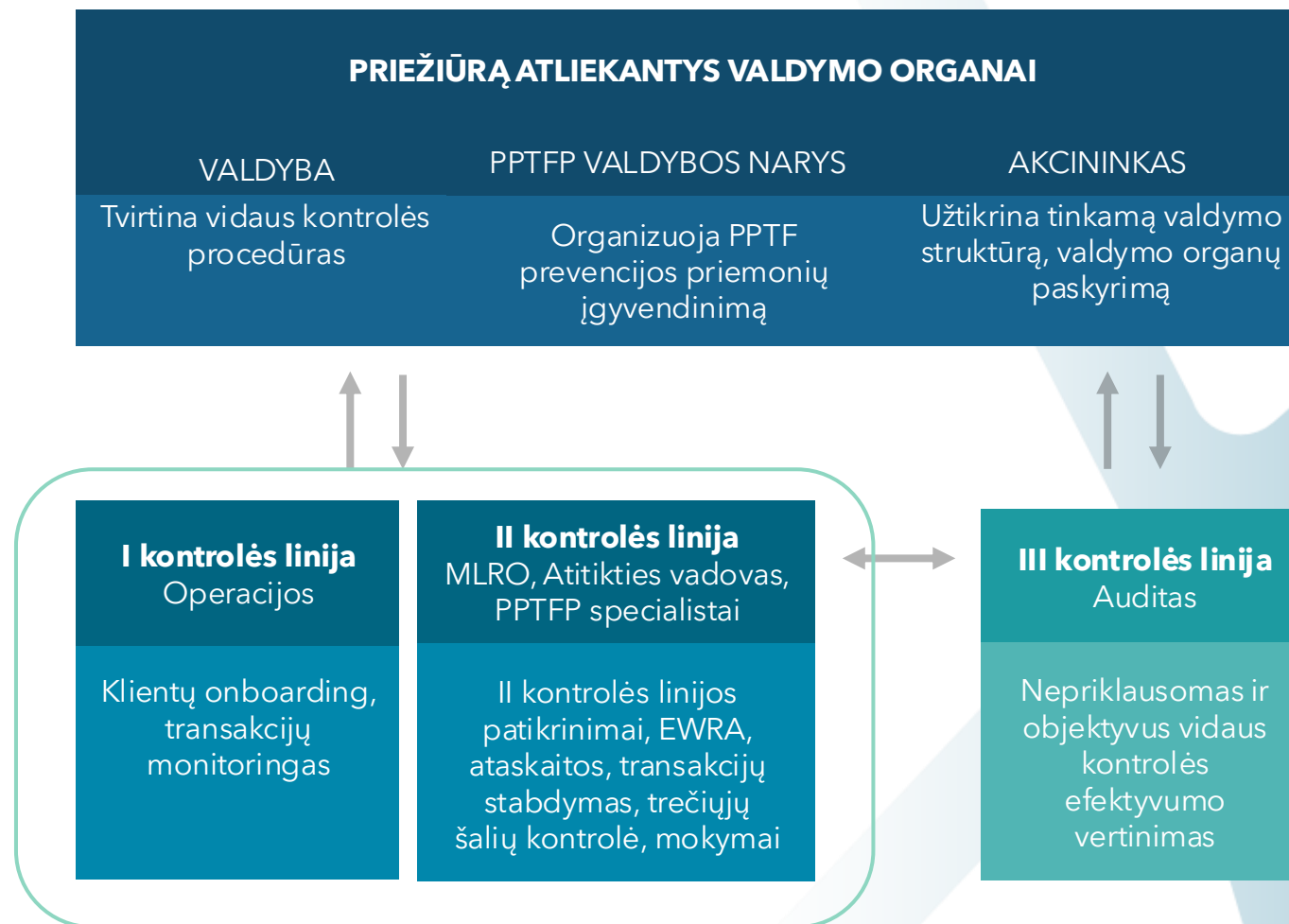
Auditų, patikrinimų ir nepriklausomų vertinimų metu identifikuojamos vidaus kontrolės spragos

Trijų kontrolės linijų modelis PPTFP vidaus kontrolės sistemoje

Formuojamas atsižvelgiant į organizacijos veiklos pobūdį, apimtį, veiklos rizikingumą ir sudėtingumą

Gali būti vykdoma pasitelkiant trečiąsias šalis (su tam tikromis išimtimis)

AMLA vėluoja paskelbti gaires dėl kriterijų, aktualių kontrolės priemonių aprėpties nustatymui

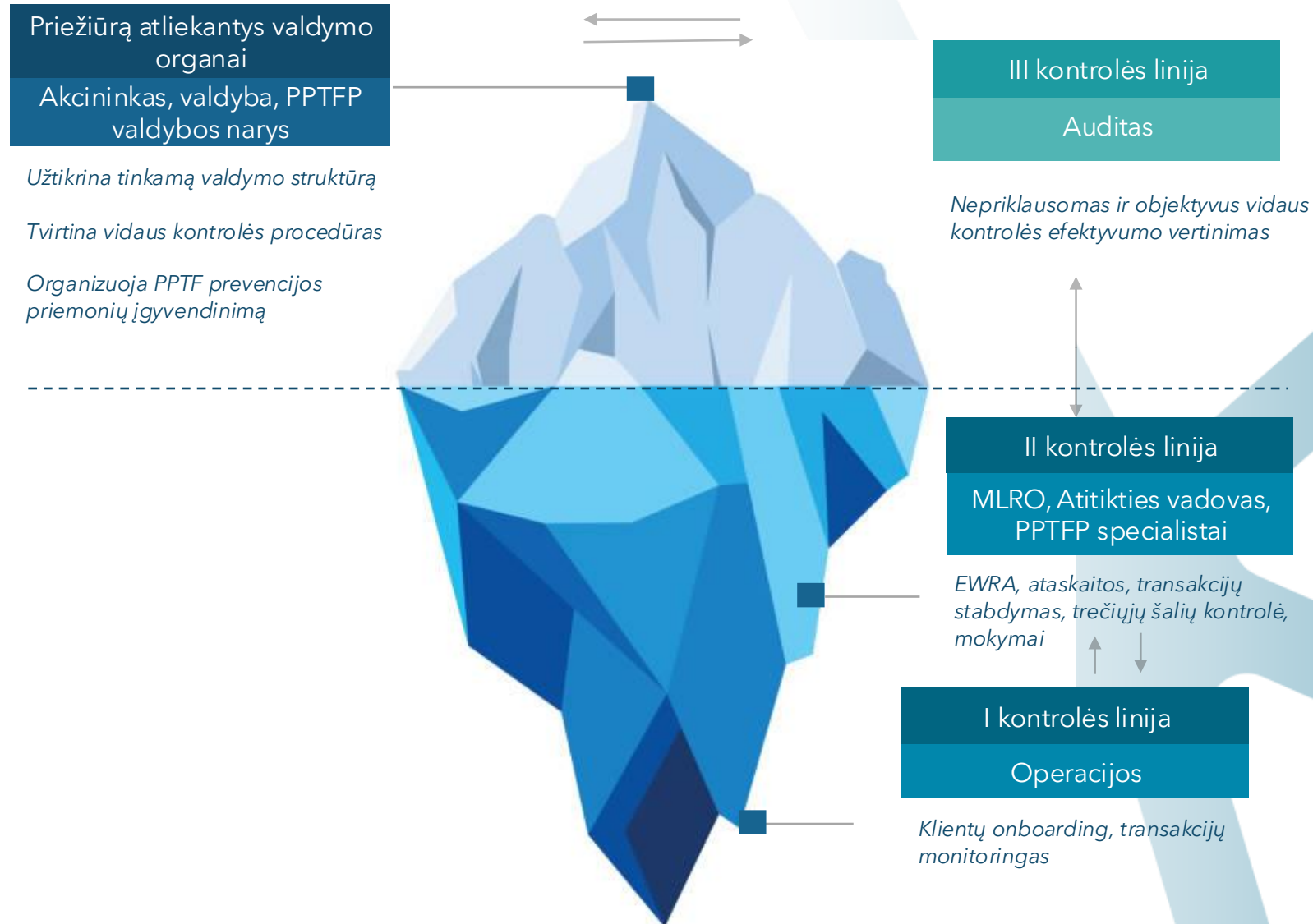


Trijų kontrolės linijų modelis PPTFP vidaus kontrolės sistemoje

Formuojamas atsižvelgiant į organizacijos veiklos pobūdį, apimtį, veiklos rizikingumą ir sudėtingumą.

Gali būti vykdoma pasitelkiant trečiąsias šalis (su tam tikromis išimtimis)

AMLA vėluoja paskelbti gaires dėl kriterijų, aktualių kontrolės priemonių aprėpties nustatymui



Vidaus kontrolēs trūkumai

Kokius vidaus kontrolės trūkumus matome praktikoje?

Valdysena

Kvalifikacijos ir resursų trūkumas

Už PPTFP atsakingi asmenys skiriami patirties neturintys darbuotojai arba itin siauros specializacijos specialistai, pvz. PPTFP valdybos nariu skiriamas patirties neturintis valdybos narys, rizikingos ir didelės organizacijos MLRO skiriamas 1 m. patirtį turintis transakcijų monitoringo specialistas.

Ribota trečiųjų šalių kontrolė

Nevertinamas tinkamumas iki santykių užmezgimo, neatliekami testavimai ir periodiniai vertinimai, kokybės kontrolė (backlog, sankcijų patikros, sandorių stebėsenos taisyklių kūrimas).

Audito ataskaitų nepateikimas vadovybei

Audito ataskaitos derinimas pasibaigia II kontrolės linijoje, t.y. audito ataskaita nėra pristatoma valdybai, nėra vykdoma rekomendacijų įgyvendinimo stebėseną.

Kokybės kontrolės trūkumai

Neproporcinga kokybės užtikrinimo imtis, formalistinės ataskaitos.

Interesų konfliktai

Tas pats asmuo atlieka ir operacinius darbus ir kokybės kontrolę, MLRO atlieka operacinius darbus, CEO tvirtina aukštos rizikos klientus (nors struktūroje yra PPTFP valdybos narys), pardavimus atliekantys darbuotojai atlieka rizikų vertinimą.

Formalus vadovybės įsitraukimas

PPTFP valdybos nario įsitraukimas apribotas metinių ataskaitų peržiūra, ataskaitos stokoja "turinio", valdybos protokoluose nėra fiksuojami PPTFP klausimų nagrinėjimai, diskusijos, PPTFP valdybos narys nedalyvauja EWRA, auditų procesuose, nėra atliekama trūkumų šalinimo stebėseną, nevykdoma KRI stebėseną.

Akcinių dalyvavimas PPTFP procesuose

Strateginiai verslo tikslai tiesiogiai arba netiesiogiai daro įtaką kliento rizikos vertinimui ir priimtinumui.

Dokumentavimo trūkumai

Formalūs valdybos protokolai, nesaugomi trečiųjų šalių vertinimo/testavimo įrodymai, atsakingų asmenų kompetencijos vertinimai, mokymų atlikimą įrodantys įrašai ir t.t.

Kokius vidaus kontrolės trūkumus matome praktikoje?

Operacijos

Individualios rizikos vertinimas

Vertinimo įrankiai nėra pritaikyti organizacijos specifikai, stokoja išsamumo. Neaiškos rizikos lygio *override* taisyklės, neišsamios klientų anketos.

Sandorių stebėsenos taisyklės

Naudojami organizacijos specifikos neatliepiantys scenarijai bei taisyklės, netinkamai sukalibruoti naudojami stebėsenos įrankiai.

Dalykinių santykių užmezgimas neužbaigus kliento pažinimo procedūrų

Dalykiniai santykiai užmezgami, o kai kuriais atvejais mokėjimo operacijos vykdomos neužbaigus viso kliento pažinimo proceso.

Klientų duomenų atnaujinimas

Vėluojama laiku atnaujinti klientų duomenis, nėra įdiegta mechanizmų, užtikrinančių klientų duomenų atnaujinimą pasikeitus su klientais susijusioms aplinkybėms (pvz., pasibaigus kliento asmens tapatybę patvirtinančių dokumentų galiojimo terminui).

Sustiprinto tapatybės nustatymo priemonių taikymo trūkumai

Nustačius aukštą kliento keliamą PPTF riziką, sustiprinto tapatybės nustatymo priemonės taikos tik formaliai arba apskritai nėra taikomos, pvz., atsakingo asmens pritarimas pradėti/tęsti dalykinius santykius su aukštos rizikos klientu nėra dokumentuojamas, nėra renkami kliento turto ar lėšų kilmę pagrindžiantys dokumentai.

Formali mokėjimo operacijų įspėjimų (alertų) analizė

Analizuojant mokėjimo operacijų įspėjimus (alertus), pateikiami komentarai yra deklaratyvūs ir dažnai apsiriboja trumpomis pastabomis. Juose nepateikiama pakankamai argumentų, pagrindžiančių, kodėl kliento veikla nelaikoma įtartina.

Informacijos saugojimo ir dokumentavimo trūkumai

Klientų individualios rizikos vertinimo rezultatai, mokėjimo operacijų įspėjimų (alertų) analizės ir kiti dokumentai ar patikrų rezultatai saugomi tokiu formatu (pvz., *xlsx*), kuris neužtikrina informacijos apsaugos nuo vėlesnio jos koregavimo.

Kaip užtikrinti efektyvų/pakankamą vadovybės dalyvavimą vidaus kontrolėje?*

**Atsižvelgiant į organizacijos veiklos pobūdį, apimtį, veiklos rizikingumą ir sudėtingumą.*

1 Minimalūs reguliaciniai reikalavimai

- LR PPTFĮ
- LB nurodymai
- EBA gairės
- AMLR

2 Kvalifikacija ir patirtis

- Tik turint pakankamai žinių ir kompetencijos galima pagrįstai kvestionuoti priimamus sprendimus bei taikomų kontrolės priemonių veiksmingumą. AMLR šį reikalavimą sustiprina.

3 Įsitraukimo įrodumumas

- Valdymo organo (ypač valdybos nario) įsitraukimas turi būti pagrindžiamas įrodymais – valdybos posėdžio minutės, metinės ataskaitos vertinimas, analizavimas, aktyvus įsitraukimas politikų/procesų derinime, komentarų teikimas audito ataskaitos derinime ir pan.

4 Prieiga prie pagrindinių PPTFP rizikos rodiklių

- Atsižvelgiant į organizacijos veiklos dydį, IT resursus, valdymo organas turi turėti galimybę gauti aktualiausius PPTFP veiklos rodiklius

Pavyzdiniai PPTFP rizikų rodikliai (KRI)

KRI parodo, ar organizacija neartėja prie rizikingos situacijos, jeigu artėja, kokių priemonių reikia imtis

Pavyzdys

PPTFP KRI	Kokią informaciją gauna vadovas?
EWRA rekomendacijų neįgyvendinimas: ● Vėluoja <5% rekomendacijų įgyvendinimas ● Vėluoja >5<10% rekomendacijų įgyvendinimas ● Vėluoja >10% rekomendacijų įgyvendinimas	Resursų/kompetencijų trūkumo indikacija
Aukštos rizikos klientų dalies padidėjimas ● < +1 p. p. ● +1-3 p. p. ● > +3 p. p.	Klientų portfolio rizikingumo dinamikos duomenys, galimi KYC/rizikos vertinimo proceso trūkumai
Periodinis klientų duomenų neatnaujinimas: ● Vėluoja <5% klientų duomenų atnaujinimas ● Vėluoja >5% klientų duomenų atnaujinimas ● Vėluoja >10% klientų duomenų atnaujinimas	Galimas backlog formavimasis

Vidaus kontrolės sistemos spraga dažnai prasideda nuo formalaus Valdybos vaidmens

Tipinis pavyzdys – įmonės visos veiklos PPTF rizikos vertinimas

Dažna spraga

Valdyba posėdžio protokole tik formaliai pažymi, kad rizikos vertinimo ataskaita ir veiksmų planas patvirtinti, tačiau pats vertinimas iš esmės nėra analizuojamas ar kvestionuojamas, valdybai pateikiama tik vertinimo ataskaita (be vertinimo įrankio ir metodologijos), nėra vykdoma trūkumų šalinimo stebėseną.

Valdybos vaidmuo - realus rizikos valdymas

Valdyba, o ypač už PPTFP atsakingas Valdybos narys:

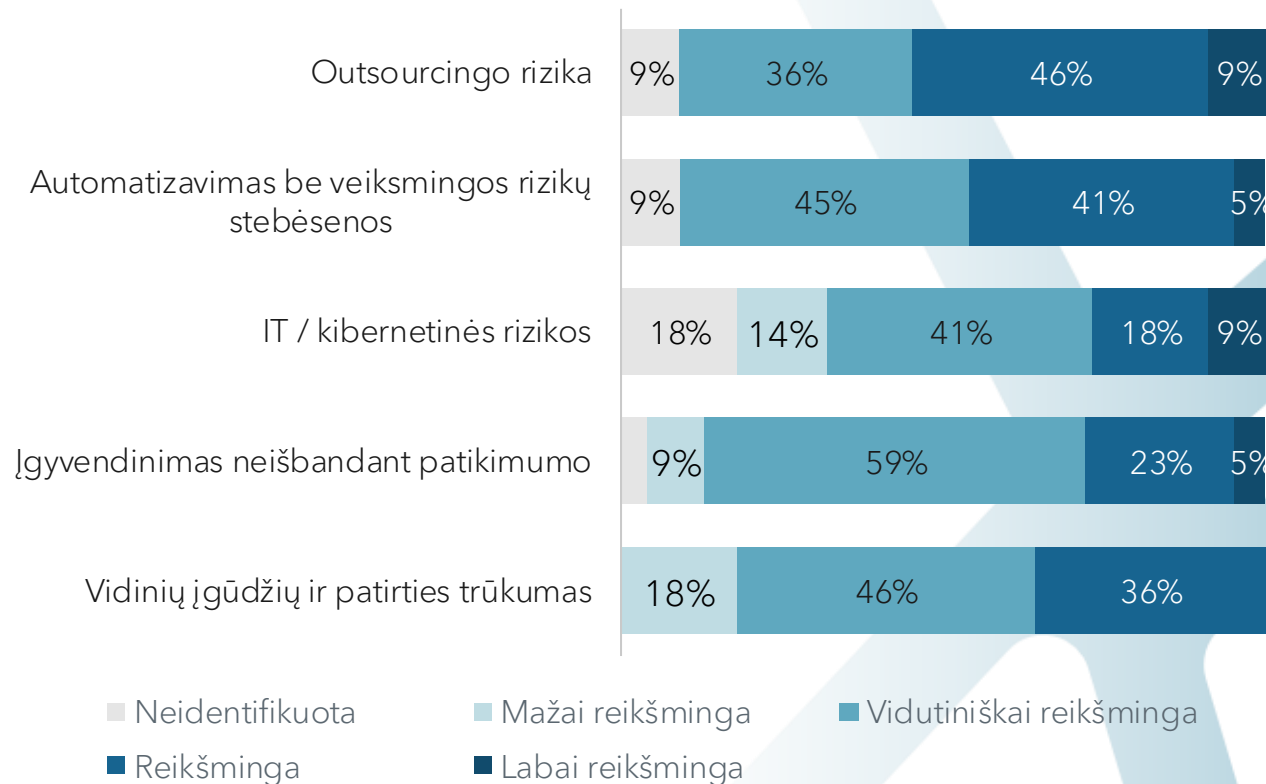
- Išsamiai susipažįsta su vertinimo metodika, svarbiomis prielaidomis, vertinimo rezultatais
- Proaktyviai kvestionuoja vertinimo metodologiją, faktinį pagrįstumą, patį vertinimą bei siūlomas veiksmų plano priemones
- Priima pagrįstus rizikos valdymo sprendimus, nustato prioritetus, užtikrina tam reikalingus išteklius
- Reguliariai gauna informaciją apie veiksmų plano įgyvendinimo eigą, vėlavimus, reikšmingus kontrolės trūkumus ir jų pašalinimą.

Realus, veiksmingas ir įrodymais pagrįstas valdymo organo įsitraukimas rizikų valdyme tampa dar svarbesnis artėjant ES PPTFP paketo įsigaliojimui, ypač atvejais, kai EWRA vertinimui pasitelkiama trečioji šalis.

„Daugiau nei pusė visų EBA apklausoje dalyvavusių institucijų mano, kad **„RegTech” sprendimų paslaugų pirkimas iš išorės kelia didelę arba labai didelę riziką.**“

36% apklaustų institucijų nurodo, kad organizacijoms trūksta vidinių įgūdžių ir patirties, būtinų siekiant užtikrinti veiksmingą RegTech sprendimų naudojimą.

Rizikos reikšmingumas, % atsakiusiųjų, TOP 5 rizikų



Kaip užtikrinti trečiųjų šalių kontrolę?

PPTFP reguliavimas finansų rinkos dalyviams nustato platų pareigų spektrą, kurių vykdymui pasitelkti kompetentingas trečiasis šalis ne tik nėra draudžiama – toks veiklos modelis reguliavime yra aiškiai numatytas ir skatinamas kaip viena iš priemonių užtikrinti veiksmingą reikalavimų įgyvendinimą

1 Minimalūs reguliaciniai reikalavimai

- LR PPTFPĮ
- LB nurodymai
- EBA gairės
- AMLR

3 Kontrolės įrodomumas

- Kontrolė turi būti pagrįsta įrodymais (pvz. IT sistemų atveju - testavimo įrašai, backlog atveju - kokybės ir kiekybės rodiklių stebėseną)

5 Auditas

- Periodinio kontrolės vertinimo imtyje turi būti įtraukiamas trečiųjų šalių veiklos kontrolės vertinimas arba inicijuojami specializuoti patikrinimai, auditai.

2 Aiškūs susitarimai

- Sutartyje aiškiai nurodoma paslaugų apimtis, kokybės užtikrinimas, atsakomybės, paslaugų teikėjo techninės galimybės (pvz. pateikti veiklos įrašus)

4 Investicija į atranką

- Žinomas prekės ženklas nereiškia kokybės ženklo – organizacijai labai svarbu įvertinti paslaugų teikėjo patirtį/kvalifikaciją konkrečioje užduotyje, technines galimybes atliepti organizacijai taikomus reguliacinius reikalavimus

Backlog funkcijų perdavimas ir kontrolė

Operacinio pobūdžio veiksmų perdavimas

Susikaupusio sandorių ir operacijų stebėsenos darbo (angl. backlog) perdavimas išorės paslaugų teikėjui daugeliu atvejų yra optimalus sprendimas, derinant laikinus tačiau reikšmingus papildomų resursų kaštus, veiklos efektyvumą ir atlikimo terminus.

Dažna spraga

Įmonė pasitelkia išorės paslaugų teikėją, tačiau neužtikrina pakankamų vidinių išteklių ir dėmesio tinkamam perduotų funkcijų valdymui ir priežiūrai. Paslaugų teikėjo veiklos stebėseną vykdoma formaliai, nepakankamai nuosekliai arba tik epizodiškai.

Geroji praktika

- Tinkamai įvertinamas ir atrenkamas išorės paslaugų teikėjas
- Įmonė skiria deramą dėmesį ir pakankamus išteklius
- MLRO arba už PPTFP organizavimą atsakingas Valdybos narys vykdo nuolatinę kontrolę (pvz., kassavaitinę) – stebi veiklos rodiklius (įskaitant kokybės patikras) ir rengia susitikimus dėl darbų eigos bei iškilusių iššūkių aptarimo
- Valdyba reguliariai (pvz., kas mėnesį) informuojama apie rezultatus, juos svarsto ir įvertina

PPTFP ir BDAR – skirtingi, tačiau neatsiejamai susiję reguliavimai

PPTFP prevencijos reguliavimas reikalauja tvarkyti didelį kiekį asmens duomenų, periodiškai juos atnaujinti ir saugoti, BDAR – priešingai – užtikrinti duomenų kiekio mažinimo principą. Organizacijos tikslas – dėti maksimalias pastangas balansui išlaikyti.

Privatumo pranešimas

Duomenų tvarkymo tikslai, kategorijos, teisinis pagrindas, duomenų saugojimo terminai, duomenų perdavimas

Duomenų tvarkymo sutartys

Perduodant PPTF, sukčiavimo prevencijos, sankcijų įgyvendinimo funkcijas atlikti partneriams būtina reglamentuoti tarpusavio santykius, perduodamų duomenų apimtį, saugumo reikalavimus ir kitas esmines sąlygas

Dalijimosi informacija partnerystė

AMLR įtvirtina pareigą prieš pradedant vykdyti partnerystės veiklą atlikti poveikio duomenų apsaugai vertinimą

1

2

3

4

5

Duomenų subjektų informavimas

Jeigu Bendrovė tvarko specialiųjų kategorijų duomenis, būtina apie tai informuoti klientą

Poveikio duomenų apsaugai vertinimas

Jeigu Bendrovė pati arba per partnerius dideliu mastu tvarko specialiųjų kategorijų duomenis arba informaciją apie teismų nuosprendžius, būtina atlikti poveikio asmens duomenų apsaugai vertinimą.

Ačiū už dėmesį!



Sigita Zavišienė

Associate Partner

Finance & Banking



Tel.: +370 612 23196

El. p.: sigita.zavisiene@expertlab.lt



Agnė Dačkienė

Associate Partner

Audit, Risk & Compliance



Tel.: +370 604 14132

El. p.: agne.dackiene@expertlab.lt