Nav klasificēts

~~DIENESTA VAJADZĪBĀM~~

Ministru kabineta rīkojuma projekta "Par IT projekta izstrādi un ieviešanu" sākotnējās ietekmes novērtējuma ziņojums (anotācija)

I. Tiesību akta projekta izstrādes nepieciešamība		
1.	Pamatojums	Finanšu un kapitāla tirgus komisija sadarbībā ar Finanšu ministriju ir izstrādājusi Ministru kabineta rīkojuma projektu pēc savas iniciatīvas.
2.	Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība	Finanšu un kapitāla tirgus regulēšanas un pārraudzības stratēģija 2015.–2017. gadam nosaka, ka noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas (turpmāk - AML) jautājumi joprojām ir viena no Finanšu un kapitāla tirgus komisijas (turpmāk – FKTK) prioritārajām jomām. FKTK veikto finanšu un kapitāla tirgus dalībnieku (turpmāk – tirgus dalībnieki) darbības pārbaužu laikā vēl ar vien tiek atklāti būtiski normatīvo aktu pārkāpumi, kā arī vērojama tirgus dalībnieku nepietiekama izpratne par AML risku. Ņemot to vērā, FKTK veic vairākus uzraudzības procesu pilnveidošanas pasākumus AML jomā. Lai nepieļautu finanšu sistēmas izmantošanu noziedzīgi iegūtu līdzekļu legalizācijai, terorisma finansēšanai vai šādu darbību mēģinājumiem, FKTK turpina uz risku balstītas uzraudzības īstenošanu AML jomā atbilstoši Eiropas finanšu sektora regulatoru 2016. gada 16.novembrī apstiprinātajām vienotajām vadlīnijām. Vadlīnijas izstrādātas, pamatojoties uz Eiropas Savienības AML Direktīvas 2015/849 48. pantu, un to mērķis ir harmonizēt AML uzraudzības prasības un metodes Eiropas Savienības dalībvalstīs. Saskaņā ar vadlīnijām dalībvalstīm ir jāpilnveido uzraudzības modelis (procedūru, procesu, mehānismu un sistēmu kopums) atbilstoši katras valsts noteiktajiem riska faktoriem. Riska faktoru identifikācija balstās uz iegūtās informācijas pamata. Valstu regulatoriem (t.sk. FKTK) jāpārliecinās, ka viņu rīcībā ir atbilstoša informācija un tās apstrādes kapacitāte, kā arī nepieciešamības gadījumā jāveic papildus pasākumi, lai to nodrošinātu. FKTK vairākās uzraudzības jomās (izņemot AML jomu) ir ieviesusi agrīnā brīdinājuma rādītāju sistēmu, kas ļauj savlaicīgi identificēt negatīvas tendences banku veiktajās darbībās, attīstīt risku novērtējuma ziņojumu analītiku un paaugstināt atklāto trūkumu novēršanas efektivitāti Agrīnā brīdinājuma rādītāju sistēma (turpmāk – sistēma). arī ir viena no AML uzraudzības procesa sastāvdaļām. Šajā gadījumā sistēma ir dažādu IT risinājumu un

Nav klasificēts

~~DIENESTA VAJADZĪBĀM~~

Nav klasificēts

Deklasificēts pamatojums: FM 16.10.2025. vēstule Nr. 13.7-13/12/3081

I.Stafeci 17.10.2025.

		procedūru kopums. Daļa no risinājumiem un IT produktiem satur šauri specifisku padziļinātu riska faktoru analīzes un aizdomīgu darījumu identificēšanas kompetenci. 2017. gadā FKTK plāno turpināt pilnveidot agrīnā brīdinājuma rādītāju sistēmu, pielāgojot to aktuālajām AML uzraudzības prasībām, un panākt, ka šī sistēma tiek aktīvi izmantota AML uzraudzības darbā. Sistēmai savlaicīgi un pārskatāmi jāsniedz AML uzraudzības vajadzībām nepieciešamā informācija par tirgus dalībnieku klientu darbību, kā arī jāveic klientu darījumu atlase, pamatojoties uz noteiktajiem AML riska faktoriem. Sistēmai jāatbalsta pilnvērtīga potenciāli aizdomīgo darījumu shēmā konstatēto darījumu analīze un pārbaužu ietvaros veicamais analītiskais process. Sistēmas ietvaros jānodrošina saņemtās informācijas glabāšana atbilstoši augstākajiem drošības standartiem. Esošais AML uzraudzības modeļa IT nodrošinājums nav pilnīgs un nenodrošina pietiekošu atbalstu AML uzraudzības vajadzībām: -nepieciešamās informācijas par tirgus dalībnieku klientu profilu un darījumiem efektīvu saņemšanu, validāciju un apstrādi; -automatizētu būtiskāko darījumu analīzes procesu nodrošinājumu klātienes un neklātienes pārbaužu vajadzībām; -metodes un rīkus efektīvākai analizējamo datu apstrādei un analīzei; -automatizētās, datos balstītas metodes savlaicīgai potenciāli aizdomīgu lielu noziedzīgo darījumu shēmu, kuras izveidojuši tirgus dalībnieku klienti, identificēšanai, kā arī potenciālu pasākumu identificēšanai to apturēšanā; -parametros un saņemtajos datos balstītu paaugstināta riska tirgus dalībniekiem noteikto pastiprinātās uzraudzības režīmu (*monitoringu*), kas vērsts uz to, lai tirgus dalībnieki ar nepietiekamu iekšējās kontroles sistēmas kapacitāti varētu strādāt ierobežoti, tādējādi mazinot kaitējumu Latvijas finanšu sistēmas reputācijai; -efektīvi (ātrdarbīgi) uzturēt visaugstākos AML uzraudzības procesa kvalitātes kontroles standartus; -analītiskos rīkus, kuri atbalsta informācijas sagatavošanu par atsevišķu tirgus dalībnieku, vai tirgus segmentu riska profilu, kā arī palīdz veikt to dinamikas uzraudzību. Minēto problēmu risināšanai un riska faktoru identificēšanai no tirgus dalībniekiem papildus

		nepieciešams iegūt un apstrādāt liela apjoma informāciju. Vienlaicīgi nepieciešams nodrošināt iegūtās informācijas augstu drošības līmeni, tai skaitā arī personas datu aizsardzību. Katras valsts riska faktori ir atšķirīgi no citām valstīm un šī iemesla dēļ izvirzītā mērķa sasniegšanai tirgū piedāvātie risinājumi nenodrošina visas nepieciešamās vajadzības. Sistēmas veidošana ietver kompleksu pasākumu kopumu, kura ietvaros nepieciešams veikt pieejamo risinājumu analīzi, nepieciešamo komponenšu konfigurāciju un papildus izstrādes vadību (turpmāk – IT projekts). IT projekts uzskatāms par liela apjoma sarežģītu informācijas tehnoloģiju projektu, kura realizāciju paredzēts pabeigt 2018. gadā. IT projekta mērķis ir izveidot tirgus dalībnieku automatizētu klientu darījumu uzraudzības sistēmu, kas savlaicīgi nodrošinātu riskantu darījumu atklāšanu un izmeklēšanu (*Case Management System*). AML uzraudzības kvalitāte un lielo aizdomīgo darījumu shēmu, kas ir tikušas un var tikt atkārtoti īstenotas, izmantojot Latvijas finanšu sistēmu, savlaicīga identifikācija, ir vitāli svarīga tās ekonomiskās drošības interesēm, t.i. valsts finanšu sektora ilgtermiņa attīstības, stabilitātes un reputācijas nodrošināšanai. Ar finanšu pakalpojumu sniegšanu saistīto noziedzīgi iegūto līdzekļu legalizācijas risku uzraudzība, kas nodrošina augstu AML atbilstības līmeni pakalpojumu sniedzējiem, ir būtisks priekšnoteikums valsts kredītreitinga paaugstināšanai, kas tiešā veidā ietekmē valsts spēju aizņemties finanšu resursus starptautiskajos finanšu tirgos par izdevīgākām procentu likmēm, kā ir minēts Pasaules Bankas ekspertu 2016. gada vasarā veiktā novērtējuma ziņojumā. Kredītreitinga aģentūras īpašu vērību pievērš AML jautājumiem, it īpaši kritiski vērtējot gadījumus, ka lielu starptautisku krāpniecisku darījumu shēmās ir iesaistījušās vairākas Latvijas bankas. Šādi gadījumi liecina par valsts finanšu sektora nepietiekamu gatavību izpildīt AML prasības un negatīvi ietekmē valsts finanšu sektora normatīvās atbilstības vērtējumu. Rezultātā valsts iegūst zemāku kredītreitingu kā sekas, aizņemoties finanšu resursus starptautiskajos tirgos, ir spiesta maksāt augstākus procentus par aizdevumiem. Vienlaikus IT projekts dos iespēju nodrošināt visaptverošu Starptautisko un Latvijas Republikas nacionālo sankciju likuma prasību izpildes kontroli, tai skaitā veicot dažādas informācijas automatizētu skrīningu pret speciālajiem (sankciju) sarakstiem.

		Uzraudzības ietvaros analizējamā darījumu informācija bieži ietver datus, kas tiek vai arī var tikt izmantoti tiesībsargājošo iestāžu veiktās izmeklēšanas interesēs saistībā ar iespējamiem terorisma finansēšanas un masu iznīcināšanas ieroču izplatības gadījumiem. Līdz ar to identificētu minēto aizdomīgu darījumu shēmu informācijai ir jānodrošina pietiekama konfidencialitāte, lai ziņojumiem par aizdomīgajiem darījumiem sekojošās izmeklēšanas darbības būtu efektīvas. Arīnacionālo sankciju likuma noteikto prasību izpildes kontrolei analizējamajai informācijai ir jānodrošina paaugstināta konfidencialitāte un datu aizsardzības prasības. Jāatzīmē, ka augstāk minētās prasības ir specifiskas un raksturīgas tikai AML uzraudzības procesos ietvertajai informācijai Minēto datu aizsardzības nenodrošināšana augstā līmenī var novest arī pie uzticēšanās zuduma finanšu uzraudzībai kopumā, negatīvi ietekmēt tirgus dalībnieku un to klientu attiecības un attiecīgi finanšu stabilitāti valstī. Ņemot vērā minēto, ja IT projekts netiks īstenots un attiecīgi tirgus dalībnieku automatizēta klientu darījumu uzraudzības sistēma netiks izstrādāta, nebūs iespējams savlaicīgi identificēt lielo aizdomīgo darījumu shēmas, kas var tikt īstenotas, izmantojot Latvijas finanšu sistēmu, kā arī nodrošināt uzraudzībā un izmeklēšanā apstrādājamo datu paaugstinātu aizsardzību - tādējādi tiks apdraudēta valsts ekonomiskā drošība – t.i. valsts finanšu sektora ilgtermiņa attīstība un stabilitāte un Latvijas valsts reputācija starptautiskajos finanšu tirgos. Lai pilnveidotu esošo klientu darījumu uzraudzību un sasniegtu IT projekta mērķi, projekta ietvaros plānots veikt attiecīgās aktivitātes, tai skaitā: - esošās situācijas analīze un labāko ES un ASV piemēru analīze; - tehniskās specifikācijas izstrāde tehniskajam risinājumam; - specializētas programmatūras iegāde, konfigurēšana un pielāgošana (*customization*); - vairāku FKTK informācijas sistēmu pilnveidošana; - sadarbības tīkla veidošana ar līdzīgām organizācijām Latvijā, ES. Sistēmai un tās komponentēm jānodrošina industrijas prasībām atbilstoša informācijas aizsardzība, darbības nepārtrauktības un avārijas atjaunošana. Ņemot vērā, ka plānotajai sistēmai paredzama

		būtiska ietekme uz finanšu sektora uzraudzību, tad jāizvērtē prasības ievērot IT sistēmām atbilstošus standartus: SSAE 16, ISO/IEC 27001, ISO/IEC 27017. Privātuma nodrošināšanai jāpiemēro ISO/IEC 27018 standartu prasības. Sistēmas attīstības scenārijos jāizvērtē iespēja veidot iekšējās datu uzglabāšanas un apstrādes sistēmas vai izmantot tādu mākoņskaitļošanas pakalpojumu sniedzēju pakalpojumus, kuri ir sertificēti atbilstoši iepriekš minētajiem standartiem, kā arī atbilstoši Eiropas Savienības un ASV noslēgtajam ietvaram (EU-U.S. Privacy Shield Framework) un normatīvajiem aktiem, kas ir izdoti, lai ieviestu Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai piemērotu krimināLsodus, un par augstāk minēto datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. Izvērtējums jāveic no atbilstošo pasākumu ieviešanas un uzturēšanas izmaksu viedokļa. IT projekta sagatavošanai un realizācijai nepieciešams piesaistīt vietējos un ārvalstu AML IT sistēmu speciālistus, kuri uzdevumu izpildi veic, balstoties uz savu Latvijas un starptautisko pieredzi darbā ar datu bāzu veidošanu, transakciju monitoringa un klientu lietu vadības sistēmām (*AML/AFC Transaction Monitoring Software; Case Management Software*). AML uzraudzībā izmantojamā informācija ietver ar likumu aizsargājumus datus, tai skaitā fizisku personu datus, kuriem jānodrošina augsta līmeņa aizsardzība atbilstoši spēkā esošajām Eiropas Savienības un Latvijas normatīvo aktu prasībām. Dati par fiziskām personām ietver arī datus par politiski nozīmīgām personām, tai skaitā valsts augstākajām amatpersonām un ar viņiem cieši saistītām personām. Līdz ar to IT projektā iesaistītajiem pakalpojumu sniedzējiem un produktu piegādātājiem ir jābūt no Latvijas valstij draudzīgām valstīm (tai skaitā NATO dalībvalstis), ar kurām tā sadarbojas atbilstoši valsts drošības interesēm. IT projektu paredzēts īstenot četrās projekta fāzēs (projekta fāžu aprakstā ietvertās darbības un risinājumi ir izklāstīti vispārējā detalizācijas līmenī, risinājumu detalizācija paredzēta projekta īstenošanas laikā): **1. IT projekta identifikācija**, kas ietver šādas darbības: - problēmas formulēšana; - nepieciešamā tirgus dalībnieku iesniedzamā datu

		apjoma noteikšana; - jaunu noteikumu datu iesniegšanai sagatavošana un apstiprināšana; - projekta ideju un koncepcijas izstrāde un attīstīšana. FKTK Atbilstības kontroles departamentā jau ir izveidota specializēta struktūrvienība (Darījumu analīzes daļa) darbam ar IT projekta ietvaros saņemamo informāciju. **2. IT projekta vadības dokumentācijas izstrāde un projekta vadība**, kas ietver šādas darbības: - IT projekta vadības un uzraudzības struktūru izveide; - IT projekta vadības vienības *(Project Management Office – PMO)* pamatojuma, pienākumu un uzdevumu noteikšana; - IT projekta dokumentācijas satura un sagatavošanas plāna izstrāde; - informācijas sistēmas biznesa procesu un darba plūsmu analīze un apraksta sagatavošana; - IT projekta tehniskā risinājuma un arhitektūras izstrāde (*Technical Infrastructure Design*), piedāvājot vismaz divus alternatīvus IT tehniskā risinājuma variantus (IT risinājumi tiek pirkti no programmatūras piegādāja un IT risinājumi tiek speciāli izstrādāti FKTK vajadzībām), ievērojot koncepcijā izvēlēto modeli; - tehniskā risinājuma darbības organizatoriskā apraksta izstrāde; - IT projekta tehnisko risinājumu analīze un izvērtēšana; - katra IT projekta aptuveno tehniskā risinājuma izveides, ieviešanas un uzturēšanas izmaksu posteņu un to summu noteikšana, kā arī tehnisko risinājumu formulēšana informācijas drošības un operatīvās pieejas nodrošināšanai; - izvēlētā IT projekta tehniskā risinājuma ekspertīze un korekcija. **3. IT projekta īstenošana**; IT projekta galvenās komponentes ir datu bāze un klientu darījumu monitoringa, analīzes un izmeklēšanas sistēma: **<u>3.1. Datu bāzes izveidošana (informācijas sistēma):</u>** - AML datu noliktavas (*Data Warehouse - DWH*) tehniskās arhitektūras izstrāde; - datu plūsmas saņemšanas un apstrādes principiālās shēmas izstrāde; - informācijas sistēmas dokumentācijas izstrāde; - informācijas sistēmas tehnoloģisko un drošības

		prasību apraksta sagatavošana; - informācijas sistēmas ieviešanas prasību noteikšana; - informācijas sistēmas tehniskās specifikācijas izstrāde; - prasību darbam ar informācijas sistēmu izstrāde; - informācijas sistēmas lietotāju struktūras, lomu un atbildības noteikšana; - veicamo darbu plāna un laika grafika sagatavošana, ievērojot IT projekta īstenošanas laika grafiku; - informācijas sistēmas risinājuma ekspertīze un korekcija; - informācijas sistēmas lietotāju apmācības prasību noteikšana; - rekomendāciju formulēšana sistēmas ieviešanas risku mazināšanai; - informācijas sistēmas drošības un veiktspējas auditu veikšanas plāna sagatavošana; - tehnisko resursu piegādes plāna sagatavošana. **3.2. Klientu darījumu monitoringa, analīzes un izmeklēšanas sistēmas izstrāde (*Case management system* – CMS).** Aizdomīgu darījumu noteikšanas metodoloģija paredz darījumu atlasei izmantot vairākus klientu darījumu „uzvedības" modeļus, tai skaitā: - prognozējams modelis - šī modeļa pamatā ir noteikumi jeb scenāriji (*rules*), kuri tiek izstrādāti ņemot vērā attiecīgos riska faktorus; - neprognozējams modelis - šajā modelī tiek izmantoti robežlielumi, kuri raksturo novirzes no parastās darbības (*anomaly detection*); - kompleksais modelis - klientu darījumi tiek izvērtēti ņemot vērā jau iepriekš zināmas noziedzīgu darījumu shēmas (*predictive model*) un - asociatīvās saites modelis, kurā izmanto sociālo tīklu informācijas analīzi (*social network analysis*). IT projekta izstrādes gaitā nepieciešams noteikt vispārīgās un specifiskās prasības CMS sistēmai. Datu filtrēšanai paredzēts izvērtēt šādu uzņēmumu rīku izmantošanas iespējas: *World Check, World Compliance, Lexis-Nexis, Bloomberg, Tomson Reuters*; papildus datu filtrēšanai būtu jāizstrādā specifikācija speciālajiem sarakstiem *(„black list")* un jāveic sankciju filtrēšanas instrumentu izvērtējums (OFAC, UN, EU u.c.). CMS izstrādes vai iegādes pakalpojumu iepirkumam nepieciešams sagatavot iepirkuma dokumentāciju, tai skaitā tehnisko specifikāciju. Tāpat šajā IT projekta fāzē tiks izpētītas prasības CMS

		atbalsta un servisa nodrošināšanai IT projekta ietvaros (izstrādes laikā) un garantijas laikā; izpētītas prasības funkcionālo izmaiņu dokumentēšanai attiecīgajās veidojamās datu bāzes (DB) shēmās, DB objektu aprakstos un dokumentos projekta ietvaros (izstrādes laikā) un garantijas laikā; definētas prasības pieejai darbam ar sistēmu; sagatavotas sistēmas un to atsevišķu daļu testēšanas plāna dokumentāciju, nosakot atbildīgos un viņu pienākumus; sagatavoti testa piemēri un to apraksti; veikta testēšana, sagatavoti ziņojumi par problēmām, to risinājumiem un atkārtota testa izpilde; definētas prasības CMS uzturēšanā iesaistītā tehniskā personāla apmācībai; izvērtēti alternatīvie CMS izveides un attīstības scenāriji. **4. IT projekta novērtējums** (monitorings un audits). Šī IT projekta fāze paredz IT projekta izstrādes uzraudzību, kvalitātes kontroli un testēšanu, kas ietver šādas darbības: - projekta izveides uzraudzības un kvalitātes nodrošināšanas pasākumu kopuma izstrāde; - projekta izveides kvalitātes kontroles veikšana un tās atbilstība tehniskajām specifikācijām un iepirkumu līgumiem; - projekta pieņemšana un pārbaudes (akcepta testēšana); - projekta ieviešana un iekšējo procesu pārmaiņu (*Change Management*) vadība. Lai sasniegtu saimnieciski efektīvāko un funkcionāli vērtīgāko rezultātu, sistēmas izveide notiks pakāpeniski, katrā solī izvērtējot sasniegtos rezultātus. Sistēmas izveidei nepieciešamo specializēto produktu un pakalpojumu apjoms un tai skatā cenas tiks precizētas projekta izstrādes un ieviešanas laikā. FKTK ir ieguvusi indikatīvus rādītājus izmaksām un veikusi to provizorisku novērtējumu, izmantojot pieņēmumus, un strukturējusi iepirkumu ietvaru, uzrunājot potenciālos piegādātājus, pakalpojumu sniedzējus un organizācijas, kurās sistēma ir izveidota. Indikatīvi noteiktās maksimālās projekta izmaksas ir 500 000 *euro*. IT projekta iepirkuma publiska izsludināšana saskaņā ar Publisko iepirkumu likumu (attiecīgi publiskojot informāciju par iepirkumu), kā arī informācijas, kas nepieciešama piedāvājumu sagatavošanai, nodošana vairākiem pakalpojumu sniedzējiem, dotu iespēju uzraugāmajiem subjektiem iegūt papildus informāciju un netiešas norādes uz uzraudzības tehnoloģiskajam nodrošinājumam paredzētajām metodēm, tehnikām un

		rīkiem, kas ļautu tiem veidot scenārijus uzraudzības kritēriju apiešanai (piemēram, pārskatīt līdzšinējos darījumus un piestrādāt pie negodīgu darījumu shēmu nomaskēšanas vai arī veikt pasākumus sniedzamās informācijas koriģēšanai), tādējādi pazeminot tās efektivitāti. Minētā informācija jo sevišķi attiecas uz: - kredītiestāžu iesniegtās informācijas validācijas un verifikācijas metodēm; - FKTK uzraudzības funkciju ietvaros pielietojamajām metodoloģijām, datu analīzes parametriem un kontroles algoritmiem; - informācijas analīzei pielietotajām tipoloģijām; - informācijas filtrēšanai (screening) izvēlētajām speciālajām datu bāzēm; - paredzētajiem informācijas apmaiņas kanāliem un to tehnoloģiskās realizācijas principiem, kas nepieciešami, lai operatīvi nodrošinātu atbildes atbilstoši kompetento iestāžu pieprasījumiem. Tāpat IT projekta iepirkuma publiska izsludināšana arī paaugstinātu risku, ka no kāda pakalpojumu sniedzēja tiek iegūta specifiska informācija, ka FKTK rīcībā esošie uzraudzības tehniskie līdzekļi šobrīd nenodrošina vairākas mūsdienīgam uzraudzības procesam būtiskas darbības (datu validāciju, kā arī informācijas verifikāciju, salīdzinot tos ar citu sniegto informāciju; regulāru iesniegto datu filtrēšanu, izmantojot speciālos sarakstus un jau iepriekš sniegto informāciju; vairāku banku sniegtās informācijas apvienotu analīzi, lai noteiktu slēptu saistīto klientu grupu darbību, kā arī atsevišķu banku saskaņotu rīcību, realizējot necaurspīdīgu darījumu shēmas, u.tml.). Vienlaikus informācijas par IT projektu publiskošana var radīt atsevišķu ieinteresēto personu vēlmi kavēt un pretdarboties IT sistēmas izstrādei un ieviešanai vispār, piemēram, izmantojot Publisko iepirkumu likumā paredzētās iespējas apstrīdēt prasības iepirkumam vai tā rezultātus. Atbilstoši Publisko iepirkumu likuma (likums stājās spēkā 01.03.2017.) 3. panta astotajai daļai šo likumu nepiemēro, ja tā piemērošana varētu radīt kaitējumu būtisku valsts drošības interešu aizsardzībai; par būtisku valsts drošības interešu aizsardzību katrā konkrētajā gadījumā lemj Ministru kabinets; šā izņēmuma piemērošanas pamats nav ne steidzamība, ne arī aizsargājama informācija pati par sevi, ja tās aizsardzību var nodrošināt iepirkuma procedūrās saskaņā ar šo likumu vai aizsardzības un drošības jomas iepirkumus

		regulējošiem normatīvajiem aktiem. Izvērtējot minētos argumentus, secināms, ka ne Publisko iepirkumu likuma piemērošana, ne arī Aizsardzības un drošības jomas iepirkumu likuma piemērošana, t.sk. slēgta konkursa vai konkursa procedūras ar sarunām piemērošana, nenodrošina informācijas par IT projekta realizāciju neizpaušanu. Turklāt minēto likumu piemērošanas gadījumā būtiski pieaugtu risks, ka tiek izpausta arī specifiska FKTK rīcībā esošā informācija par uzraudzības procesos izmantojamo informāciju un metodēm, tādējādi radot neatgriezenisku kaitējumu Latvijas finanšu sistēmas drošībai un reputācijai, ņemot vērā, ka šāda informācija būtu nododama vairākiem piegādātājiem, kuru patiesos nodomus, piedaloties iepirkumā, FKTK nevar izvērtēt un vadīt. Līdz ar to Ministru kabinetam tiek lūgta atļauja piemērot Publisko iepirkumu likuma 3. panta astoto daļu, lai nodrošinātu būtisku valsts ekonomiskās drošības interešu aizsardzību.
3.	Projekta izstrādē iesaistītās institūcijas	Finanšu un kapitāla tirgus komisija
4.	Cita informācija	Nav.

Anotācijas II, III, IV, V un VI sadaļa – projekts šīs jomas neskar.

Finanšu ministre D. Reizniece-Ozola