LATVIJAS BANKA
EIROSISTĒMA

Vadlīnijas efektīvas sankciju riska pārvaldībā izmantojamās informācijas tehnoloģiju sistēmas izveidei un uzturēšanai

Latvijas Banka 2023. gadā veica tematisko pārbaudi (turpmāk – Tematiskā pārbaude), lai novērtētu 22 kredītiestāžu un nebanku finanšu iestāžu sankciju riska pārvaldības informācijas tehnoloģiju (turpmāk – IT) sistēmu efektivitāti. Tematiskajā pārbaudē tika izvērtētas 45 sankciju pārbaudēm izmantotās IT sistēmas – gan iekšējās, gan trešo pušu nodrošinātās; 4 no pārbaudītajām IT sistēmām bija manuālas.

Tematiskās pārbaudes laikā tika secināts, ka lielākā daļa IT sistēmu, ko iestādes izmanto sankciju pārbaudēm (turpmāk – sankciju skrīnings), vērtējamas kā kopumā efektīvas un lietderīgas. Tematiskajā pārbaudē tika konstatēti arī vairāki labās prakses piemēri. Vienlaikus visām iestādēm tika konstatēti noteiktu veidu trūkumi un nepilnības, līdz ar to iestādēm bija jāizstrādā plāns nepilnību un trūkumu novēršanai.

Vadlīniju mērķis ir informēt finanšu tirgus dalībniekus par rezultātu, kādu Latvijas Banka gaida attiecībā uz efektīvas sankciju skrīninga sistēmas izveides kritērijiem, tostarp kvalitātes kontroles nodrošināšanu, testēšanu, IT sistēmu konfigurāciju pielāgošanu, trešo pušu piegādātāju izmantošanu u. c., kā arī informēt par novērotajiem labās un nevēlamās prakses piemēriem.

Prasību noteikšana sankciju skrīninga sistēmām

Saskaņā ar Starptautisko un Latvijas Republikas nacionālo sankciju likumu visi finanšu tirgus dalībnieki, pamatojoties uz savu darbības veidu un klientu bāzi, veic un dokumentē starptautisko un nacionālo sankciju riska novērtējumu, lai konstatētu, novērtētu, izprastu un pārvaldītu starptautisko un nacionālo sankciju (turpmāk – sankcijas) riskus un nodrošinātu atbilstību normatīvo aktu prasībām. Pamatojoties uz šo novērtējumu, iestādes izveido iekšējās kontroles sistēmu sankciju riska pārvaldīšanai, t. sk. izstrādā un dokumentē attiecīgās politikas un procedūras.

Sankciju skrīningam izmantoto IT sistēmu darbība ir būtiska iekšējās kontroles sistēmas sastāvdaļa, lai nodrošinātu atbilstošu sankciju riska pārvaldību. Sankciju skrīnings būtībā attiecas uz procesu, kurā viena vārdu virkne tiek salīdzināta ar citu, lai atklātu līdzības, kas varētu liecināt par iespējamu atbilstību. IT sistēmu uzdevums ir salīdzināt datus, kas iegūti iestādes darbības ietvaros, piemēram,

klientu un darījumu ierakstus, ar personu vārdiem, atrašanās vietām, citu subjektu ierakstiem sankciju sarakstos.

Tomēr sankciju skrīninga sistēma ir tikai daļa no efektīvas un visaptverošas sankciju riska pārvaldības iekšējās kontroles sistēmas, un sankciju skrīninga pasākumi ir jāpiemēro kopā ar citiem kontroles pasākumiem, piemēram, efektīviem "pazīsti savu klientu" procesiem, darbinieku apmācību, sankcijām pakļauto līdzekļu un aktīvu iesaldēšanu regulējošām procedūrām, iespējamo sankciju pārkāpšanas un apiešanas gadījumu konstatēšanas un ziņošanas procedūrām u. tml.

Pamatojoties uz sankciju riska novērtējumu, iestādēm ir jānosaka un jāievieš atbilstoši sankciju skrīninga pasākumi, kas ir piemēroti, lai pārvaldītu konkrētajai iestādei piemītošo sankciju risku, t. sk. jānovērtē, jāpamato un jādokumentē šādas prasības:

- kāds ir sankciju skrīninga sistēmas nepieciešamais automatizācijas un sarežģītības līmenis;
- kādi sankciju saraksti jāpārbauda;
- kādas datu kopas jāpārbauda;
- kāda ir sankciju skrīninga sistēmas testēšanas regularitāte un kārtība u. c.

1. un 2. piemērs: pārbaudāmo sankciju sarakstu noteikšana un konkrētu sarakstu pārbaudes ierobežojumu noteikšana	
Labā prakse	**Nevēlamā prakse**
Iestāde ir veikusi visaptverošu riska novērtējumu un konstatējusi, ka papildus darījumiem *euro* liela daļa iestādes darījumu tiek veikti ASV dolāros un Lielbritānijas sterliņu mārciņās. Tāpēc papildus obligāto sankciju sarakstiem – Eiropas Savienības (turpmāk – ES), Apvienoto Nāciju Organizācijas (turpmāk – ANO) un Latvijas nacionālo sankciju sarakstiem – darījumi tiek pārbaudīti arī pret Amerikas Savienoto Valstu Ārvalstu aktīvu kontroles biroja (turpmāk – OFAC) un Apvienotās Karalistes Viņas Majestātes Valsts kases (turpmāk – HMT) noteiktajiem sankciju sarakstiem. Turklāt, ņemot vērā iestādes klientu bāzi un piedāvātos produktus, kas ietver arī	Iestāde veic pārbaudes pret ES, ANO, OFAC un Latvijas sankciju sarakstiem. Tomēr iestāde savā sankciju riska novērtējumā nav vērtējusi būtisku informāciju par darījumiem, t. i., valūtu, kurā tiek veikti darījumi, darījumu plūsmu uz dažādām jurisdikcijām. Faktiski iestādē ir ievērojams darījumu skaits dažādās valūtās, kas tiek veikti uz Apvienoto Karalisti. Tāpēc, neveicot pārbaudes pret HMT sankciju sarakstiem, iestāde pakļauj sevi riskam, ka tā varētu tikt iesaistīta HMT noteikto sankciju pārkāpšanā vai apiešanā, kas var radīt arī juridiskus un reputācijas riskus.

tirdzniecības finansēšanas produktus, iestāde nolemj pārbaudīt darījumus attiecībā uz divējāda lietojuma preču sarakstu[1].	
Iestāde, pamatojoties uz detalizētu risku izvērtējumu, ir secinājusi, ka, ņemot vērā tās ieviestās dažādās alternatīvās kontroles, nav lietderīgi veikt datu skrīningu pret "*Weak Aliases*" jeb "vājajiem pseidonīmiem"[2] (turpmāk – "*Weak Aliases*"), jo sankciju skrīninga sistēma rada daudz viltus pozitīvu rezultātu, kas negatīvi ietekmē sankciju skrīninga sistēmas darbības lietderību, un pastāv neliela varbūtība, ka skrīnings pret "*Weak Aliases*" ļautu iestādei identificēt sankcijām pakļautu fizisko vai juridisko personu, ņemot vērā papildus izstrādātās kontroles risku mazināšanai. Iestāde ir konstatējusi, ka OFAC nav noteikusi obligātu prasību nodrošināt pārbaudes arī pret "*Weak Aliases*"[3], tomēr citas organizācijas (ES un ANO) nav sniegušas skaidru paziņojumu par minēto aspektu. Ņemot vērā visu minēto un papildus izstrādātās kontroles, iestāde nolemj neveikt "*Weak Aliases*" pārbaudes un dokumentē šādu lēmumu, kurā ir skaidri definēti un pamatoti lēmuma iemesli (ietverot arī testēšanu, kad tas ir nepieciešams) un ir izklāstīti	Iestāde neveic datu pārbaudi pret "*Weak Aliases*", tomēr iestāde nav dokumentējusi šādu lēmumu un nav novērtējusi ar šādu lēmumu saistītos riskus. Turklāt iestāde veic skrīningu pret sankciju sarakstiem, ko nodrošina trešās puses pakalpojumu sniedzējs. Trešās puses pakalpojumu sniedzējs sankciju sarakstos iekļauto personu/vienību ierakstus iedala noteiktos vārdu veidos jeb kategorijās saskaņā ar oficiālajiem sankciju sarakstiem, kas ļauj noteikt, kurš vārda tips ir "*Weak Aliases*". Tomēr papildus oficiālajam vārdu kategoriju iedalījumam trešās puses pakalpojumu sniedzējs, lai padarītu sankciju skrīninga sistēmas darbību efektīvāku, var izstrādāt savu subjektīvo kategoriju iedalījumu un, pamatojoties uz noteiktiem kritērijiem, var pieņemt lēmumu pārklasificēt vārda veidu. Piemēram, vārda veids, kas oficiālajā sankciju sarakstā tiek noteikts kā "*strong*" jeb "spēcīgs", tiek pārklasificēts par "*weak*" jeb "vājš". Tomēr iestāde nezina, ka trešās puses pakalpojumu sniedzējs veic šādu vārdu veidu pārklasificēšanu. Līdz ar to iestāde nav informēta par riskiem, kas saistīti ar šādu lēmumu – nepārbaudīt

[1] Termins "divējāda lietojuma preces" šā dokumenta kontekstā nozīmē preces, programmatūru un tehnoloģijas, ko var izmantot gan civiliem, gan militāriem mērķiem, jo īpaši terorismam.

[2] "Vājš pseidonīms" (arī "vājš") ir termins, kas apzīmē plašu vai vispārēju sankcijām pakļautas personas vai vienības pseidonīmu, kas ir iekļauts oficiālajā sankciju sarakstā un kas var radīt lielu daudzumu viltus brīdinājumu, ja šādu nosaukumu skrīnings tiek veikts, izmantojot IT sistēmas automatizētu pārbaudi.

[3] OFAC ir paziņojusi, ka OFAC noteikumi skaidri nenosaka nekādu īpašu pārbaudes režīmu. Finanšu iestādēm un citām iestādēm ir jāveic pārbaudes izvēle, pamatojoties uz to apstākļiem un atbilstības pieeju. Tomēr kopumā OFAC nesagaida, ka personas pārbaudīs "vājas AKA ["*Weak Aliases*"], bet sagaida, ka šādas AKA var izmantot, lai palīdzētu noteikt, vai "trāpījums", kas izriet no citas informācijas, ir precīzs". Skat. Ārvalstu aktīvu kontroles birojs (treasury.gov).

attiecīgie riski, kas izriet no šāda lēmuma pieņemšanas.	nosaukumu veidus, kas saskaņā ar oficiālajiem sarakstiem ir "spēcīgi", bet saskaņā ar trešās puses pakalpojumu sniedzēju klasifikāciju tiek identificēti kā "*Weak Aliases*" jeb "vāji".

Lai noteiktu, kāds automatizācijas un sarežģītības līmenis nepieciešams sankciju skrīninga sistēmas funkcionalitātei, t. i., manuāls vai automātisks IT risinājums vai abu veidu kombinācija, iestāde ņem vērā vismaz šādus faktorus – sniegto pakalpojumu specifiku, kā arī dienas vai mēneša darījumu skaitu un klientu skaitu. Iestādei jāspēj pamatot, ka pasākumi, ko tā ir veikusi, lai pārvaldītu sankciju risku, ir atbilstoši riskiem, kuriem iestāde ir pakļauta, ņemot vērā iestādes sankciju riska novērtējumu.

3. un 4. piemērs: sankciju skrīninga sistēmas automatizācijas līmeņa noteikšana	
Labā prakse	**Nevēlamā prakse**
Iestāde ir veikusi sankciju riska novērtējumu un izvērtējusi tās sniegtos pakalpojumus un produktus, klientu darījumu skaitu dienā/mēnesī, esošo klientu skaitu, jaunu klientu piesaistīšanas intensitāti, kā arī noteikusi, ka, lai nodrošinātu atbilstošu sankciju riska pārvaldību, nepieciešams ieviest automātisku IT sistēmas risinājumu gan darījumu, gan klientu sankciju skrīningam. Ņemot vērā iestādes ierobežotās tehniskās iespējas, iestāde nolemj sankciju skrīningam izmantot trešās puses pakalpojumu sniedzēja piedāvāto IT rīku. Iestādes vadība izprot efektīvas sankciju skrīninga sistēmas nozīmi un ir piešķīrusi pietiekamus resursus, kas nepieciešami jaunajam IT rīkam. Iestādes sankciju speciālists un IT speciālisti ir iesaistīti sadarbībā ar trešās puses pakalpojumu sniedzēju jaunā IT risinājuma ieviešanā, lai nodrošinātu, ka tiek izpildītas visas iestādes noteiktās prasības un jaunais	Iestāde iepriekš piedāvāja ierobežotu produktu klāstu un tādēļ veica tikai manuālu sankciju skrīningu publiski pieejamos avotos, kas bija piemērots risinājums tās sankciju riska pārvaldībai. Iestāde ir sākusi piedāvāt jaunu produktu. Tomēr pirms jaunā produkta ieviešanas iestāde, veicot produkta mērķa riska izvērtējumu, nevērtēja, vai līdzšinējie sankciju skrīninga pasākumi būs efektīvi, lai nodrošinātu jaunajam produktam raksturīgo risku pārvaldību. Praksē pēc jaunā produkta ieviešanas iestādes darbinieki, kas nodrošināja manuālā sankciju skrīninga veikšanu, nebija spējīgi veikt nepieciešamās pārbaudes atbilstoši iestādes iekšējās procedūrās noteiktajiem termiņiem, tādējādi radot kavējumus uzdevumu izpildē gan attiecībā uz darījumu uzraudzības, gan "pazīsti savu klientu" procesiem, kā arī palielinot sankciju risku un klientu sūdzību skaitu.

IT rīks ir pienācīgi integrēts ar citām iestādes IT sistēmām, t. sk. pirms ieviešanas attiecīgi tiek pārbaudīts.	
Iestāde ir veikusi riska novērtējumu un secinājusi, ka, ņemot vērā sniegtos pakalpojumus, būtu nesamērīgi ieviest automātisku sankciju pārbaudi ienākošajiem un izejošajiem maksājumiem. Iestāde piedāvā tikai ierobežotu tādu produktu klāstu, kas ir novērtēti kā zema līdz vidēji zema riska produkti, un tās klientu bāze ir salīdzinoši maza. Iestāde ir ieviesusi papildu kontroles, proti, tās produktu ierobežojumi paredz, ka iestādes pakalpojumus var saņemt tikai Latvijas rezidenti, pakalpojuma saņemšanai klients izmanto tikai kontu citā kredītiestādē, kas ir reģistrēta ES, un iestāde nepieņem trešo personu maksājumus. Turklāt iestāde regulāri novērtē faktisko maksājumu plūsmu, lai noteiktu, vai praksē ir ievēroti noteiktie produktu ierobežojumi un tiek efektīvi pārvaldīts sankciju risks.	Iestāde ir ieviesusi automatizētu sankciju skrīninga rīku, bet tā funkcionalitāte nav pietiekami detalizēti izvērtēta. Piemēram, iestādei nav zināms, ka skrīninga rīkā ir ļoti ierobežoti testēšanas algoritmi sakritību identificēšanai, kas nenodrošinās efektīvu un lietderīgu sankciju ierakstu identificēšanu, ja pārbaudāmais ieraksts ir nepilnīgs vai tam piemērota manipulācija. Līdz ar to skrīninga rīka funkcionalitāte nav pietiekami efektīva, lai nodrošinātu sankciju riska atbilstošu pārvaldību, ņemot vērā iestādes pakalpojumu veidu, apjomu un klientu bāzi.

Lai izveidotu efektīvu sankciju skrīninga sistēmu, iestādei ir nepieciešams noteikt, kādu veidu dati par klientiem un darījumiem ir iestādes rīcībā, lai attiecīgi nepieciešamo datu kopu varētu integrēt skrīninga sistēmā. Ja kāds noteikts datu kategoriju kopums nav iekļauts skrīninga sistēmā, tas būtu attiecīgi jāpamato un jādokumentē.

5. un 6. piemērs: atbilstošo datu kategoriju, kas būtu jāpakļauj sankciju skrīningam, noteikšana	
Labā prakse	**Nevēlamā prakse**
Uzsākot sadarbību ar klientu, iestāde veic visaptverošu "pazīsti savu klientu" procesu, kura laikā tiek identificēta arī klienta īpašumtiesību struktūra, patiesais labuma guvējs, personas, kurām ir pilnvaras pārstāvēt klientu, un citas ar klientu saistītas personas, piemēram, fiziskās un juridiskās personas valdes vai īpašumtiesību struktūrā, kuras, iespējams, kontrolē klientu vai īsteno dominējošu ietekmi. Iestāde regulāri pārbauda pret sankciju sarakstiem savu klientu bāzi, tostarp pašu klientu, klienta pārstāvjus, patieso labuma guvēju un citas saistītās personas, kam varētu būt iespēja kontrolēt vai ietekmēt klientu. Iestāde ir noteikusi un dokumentējusi, kuri datu lauki ir jāpārbauda, piemēram, vārds un uzvārds vai uzņēmuma nosaukums, dzimšanas datums, reģistrācijas numurs, valstspiederība, adrese utt., lai nodrošinātu, ka skrīnings sniedz visprecīzākos rezultātus. Iestāde nodrošina to, ka "pazīsti savu klientu" informācija tiek regulāri aktualizēta un ka izmaiņu gadījumā tiek veikts klienta un ar to saistīto personu skrīnings.	Uzsākot sadarbību ar klientu, iestāde veic visaptverošu "pazīsti savu klientu" procesu, kura laikā tiek iegūta visa nepieciešamā informācija. Tomēr iestāde nodrošina regulāru skrīningu tikai par klientu, tā pārstāvjiem un klienta patieso labuma guvēju. Taču gadījumā, kad klienta lielākais kapitāldaļu turētājs ir juridiskā persona, kura ir sankcijām pakļauta persona, iestāde nav spējīga identificēt, ka klienta līdzekļi ir nekavējoties jāiesaldē, jo skrīninga sistēmā informācija par juridisko personu ir izslēgta no pārbaudes tvēruma.
Darījumu izvērtēšanā iestāde ir noteikusi, kuri datu lauki ir jāpārbauda, piemēram, darījumā iesaistīto pušu nosaukumi, finanšu iestādes, tostarp darījumā iesaistītās korespondentbankas, brīvā teksta lauks, adreses lauks, IP adrese (kas ir būtiski, lai nodrošinātu atbilstību	Iestāde sniedz tirdzniecības finansēšanas pakalpojumus un ir ieviesusi noteiktus kontroles pasākumus, lai pārvaldītu ar sankcijām saistītos riskus. Tomēr iestāde nav izstrādājusi detalizētu procedūru, kurā būtu ietverti nepieciešamie datu lauki skrīningam situācijā, kad tiek sniegti tirdzniecības

sektorālajām sankcijām, ko piemēro konkrētiem reģioniem). Iestāde ir ņēmusi vērā atšķirības dažādu veidu darījumu ziņojumos (piemēram, SEPA un SWIFT maksājumiem).	finansēšanas pakalpojumi. Darbinieki, kuri ir atbildīgi par tirdzniecības finansēšanas dokumentācijas manuālu pārbaužu veikšanu, nepārbauda informāciju par darījumā iesaistīto kuģi (tostarp Starptautiskās Jūrniecības organizācijas (SJO) numurus). Līdz ar to iestāde nav spējīga konstatēt, ka tirdzniecības finansēšanas darījumā iesaistītajam kuģim ir piemērotas sankcijas.

Pilnveidota vārdu un uzvārdu salīdzināšanas tehnoloģija ir būtisks nosacījums efektīvas sankciju skrīninga sistēmas izveidei, lai varētu identificēt iespējamās sakritības, kurās transliterācijas, nepareizi uzrakstītu, nepilnīgu vai trūkstošu datu dēļ dati – vai nu oficiālajos sarakstos, vai iestādes iekšējos reģistros – ir fiksēti atšķirīgi. Sankciju skrīninga sistēmām jāspēj piemērot izplūdušās loģikas jeb "*fuzzy logic*" algoritmus, t. i., uz algoritmiem balstītu paņēmienu, kura mērķis ir atrast sankciju ieraksta vārda (vārdu virknes) sakritību, ja pārbaudāmās informācijas saturs nav identisks ar sankciju ierakstu, bet tā pareizrakstībai, pierakstam vai skanējumam ir tuva sakritība ar saturu, kas ietverts datu kopā, kuru izmanto skrīningam. Attiecīgi sankciju skrīninga sistēma būtu jākalibrē tā, lai, piemēram, kalibrējot algoritma sakritības procentuālo daļu, skrīninga sistēma ne tikai brīdina par precīzu atbilstību (kad tiek ģenerēts brīdinājums, ja sistēmā pārbaudāmie dati precīzi sakrīt ar sankciju sarakstā ietvertajiem), bet arī gadījumā, ja ar pārbaudāmās informācijas saturu būtu veiktas noteiktas manipulācijas.

Iestādēm jāapzinās, ka, samazinot "*fuzzy logic*" procentuālo sakritību daļu vai mainot algoritma parametrus, palielināsies brīdinājumu, daļa no kuriem būs viltus pozitīvi rezultāti, skaits. Minētais var negatīvi ietekmēt skrīninga sistēmas lietderību. Tāpēc iestādēm "*fuzzy logic*" parametri būtu jākalibrē tā, lai nodrošinātu abus procesus – to, ka sistēma darbojas pēc iespējas efektīvāk (netiek izlaists neviens vai tiek izlaists minimāls skaits sankciju ierakstu), bet tajā pašā laikā tā darbojas arī lietderīgi, t. i., sankciju skrīninga sistēma ģenerē kvalitatīvus brīdinājumus un nerada lielu skaitu viltus pozitīvu rezultātu, kas varētu prasīt nesamērīgus resursus šādu brīdinājumu izvērtēšanai, tostarp varētu radīt kavējumus brīdinājumu apstrādē un izraisīt virkni operacionālo risku, t. sk. klientu sūdzību risku. Iestādēm būtu jāveic izvērtēšana un testēšana, lai noteiktu atbilstošos sankciju skrīninga sistēmas kalibrēšanas pasākumus.

Publiskajos avotos ir pieejami dažādu veidu "*fuzzy logic*" algoritmi, kurus iespējams izmantot. Novērtējot, kurus algoritmus piemērot ir efektīvāk vai kuriem algoritmiem pievēršama lielāka uzmanība, būtu jāveic atbilstoša

izvērtēšana un testēšana. Tabulā norādīti biežāk izmantotie "*fuzzy logic*" sakritību algoritmi (piemēri norādīti angļu valodā, ņemot vērā tehnisko terminu specifiku):

Text Matching	**Text Manipulation**	**Word Manipulation**	**Date Adjustment**
Soundex	Text Character Add	Word Delete	Add Subtract Date
Levenshtein Distance	Text Character Delete	Word Swapping	Swap Day and Month Date Valid
Metaphone 3	Text Character Add and Delete	Word Joining	Swap Decade of Year
	Text Character Reversing	Word Separating	
	Text Contextual Start	Word Moving	
	Text Contextual End	Abbreviation Combined	
	Text Contextual Complete	Abbreviation Combined Dot	
	Fat Finger Replace	Abbreviation Combined Space	
	Text Character Add Repetition	Abbreviation Combined Dot Space	
	Text Character Remove Repetition	Word Joining with Hyphen	
	Text Alphanumeric Swap	Word Reordering	
	Text Phonetic Character Replace	Add Initial	
	Text Character Add Special Characters	Add Initial Dot	
	Initial Letters Change	Name Duplicate	
	Add Subtract Number	Duplicated Name Remove	
	Number Add	Initial Join Space Delete	
	Number Swap	Digit to Text	
	Number Remove	Text to Digit	
		Ordinal Number Abbreviate	
		Ordinal Number Expand	

7. un 8. piemērs: "*fuzzy logic*" parametru noteikšana un lēmumu pieņemšana par papildu kontrolēm, lai uzlabotu skrīninga lietderību	
Labā prakse	**Nevēlamā prakse**
Iestāde ir kalibrējusi "*fuzzy logic*" sakritību parametrus līdz noteiktam līmenim, kas nodrošina, ka skrīninga sistēma darbojas gan efektīvi, gan lietderīgi. Parametri ir noteikti un pārbaudīti, pamatojoties uz visaptverošu testēšanu, kurā tika pārbaudīti dažādi modeļi. Iestāde ir izveidojusi testēšanas vidi, kura ir pēc iespējas līdzīgāka iestādes produkcijas videi. Iestāde pirms iestatījumu ieviešanas produkcijas vidē veica sistēmas testēšanu un dokumentēja šo procesu. Saskaņā ar iestādes iekšējiem noteikumiem iestāde noteiktā regularitātē atkārtoti novērtē noteiktos parametrus un veic nepieciešamās izmaiņas, kuras tiek pārbaudītas un apstiprinātas pirms izmaiņu ieviešanas produkcijas vidē.	Iestāde ir nolēmusi mainīt "*fuzzy logic*" sakritību parametrus, lai palielinātu skrīninga sistēmas efektivitāti attiecībā uz manipulēto datu pārbaudēm. Tomēr iestāde nav novērtējusi, kā šādas izmaiņas ietekmēs skrīninga sistēmas lietderību. Šā lēmuma rezultātā iestādes darbinieki saskaras ar ievērojami lielāku brīdinājumu skaitu dienā. Darbinieki nevar kvalitatīvi izmeklēt brīdinājumus noteiktajā termiņā, tāpēc brīdinājumi tiek slēgti kā viltus pozitīvi bez pienācīgas izvērtēšanas.
Iestāde ir ieviesusi papildu pasākumus sankciju skrīninga sistēmas lietderības paaugstināšanai, piemēram, "balto sarakstu", kurā sistēma iekļauj izplatītākos brīdinājumus, kas ir viltus pozitīvi rezultāti. Iestādei ir detalizēta procedūra, kas nosaka šāda saraksta izveidi un izmantošanu, tostarp to, kā šis saraksts tiek pārskatīts, atjaunināts, grozīts utt. Iestāde regulāri novērtē minētā pasākuma efektivitāti, veic attiecīgas pārbaudes un vajadzības gadījumā ievieš atbilstošas izmaiņas.	Iestāde ir ieviesusi papildu pasākumus sankciju skrīninga sistēmas lietderības paaugstināšanai, t. i., ieviesusi "balto sarakstu". Tomēr, ņemot vērā, ka iestādei nav detalizētas procedūras, kas regulētu šāda saraksta izmantošanu, iestāde nav iekļāvusi "balto sarakstu" to datu tvērumā, kuri iestādei būtu regulāri jāpārbauda, lai noteiktu gadījumus, kad saraksts būtu jāpārskata un jāatjaunina. Tāpēc, piemēram, ja ir noteikts jauns sankciju režīms, iestāde var tikt pakļauta riskam, ka "baltajā sarakstā" ir dati, kuriem potenciāli būtu jārada pozitīva sankciju sakritība.

Sankciju skrīninga sistēmas galvenie aspekti, kas būtu regulāri jānovērtē un jāuzrauga

Ņemot vērā Tematiskās pārbaudes rezultātus un uzsverot efektīva sankciju skrīninga pasākumu nozīmi, ir svarīgi, lai katra iestāde regulāri novērtē, izprot, uzrauga un uzlabo savas skrīninga sistēmas darbību. Tas ietver šādu aspektu novērtējumu:

- tiek pārbaudīti visi nepieciešamie sankciju saraksti un visas sankciju režīma programmas, lai tās ir "ieslēgtas" un darbojas pareizi (piemēram, ES sankciju režīms pret Krieviju, ES izveidotais teroristu saraksts utt.);
- tiek pārbaudītas visas attiecīgās datu kategorijas (t. i., visi klienti, ar attiecīgajiem klientiem saistītās puses, citas datu kategorijas, piemēram, IP adreses utt.), darījumu lauki (t. i., maksātājs, maksājuma saņēmējs, maksājumā iesaistītās finanšu iestādes, darījuma apraksta/brīvā teksta lauks utt.);
- sankciju saraksti un citi dati, attiecībā uz kuriem sistēmā tiek veikta pārbaude, ir atjaunināti un pareizi;
- sistēmas sankciju ierakstu nesakritības līmenis ir zems vai vienāds ar nulli; ja skrīninga sistēma nav identificējusi sankciju ierakstus (klientu/transakciju skrīnings), iestādei ir jābūt informētai par iemesliem, kādēļ IT sistēma nebija identificējusi sankciju ierakstus, tai ir jāveic pasākumi, lai novērtētu un mazinātu jebkādu risku, un tai ir jābūt dokumentētiem iemesliem, kāpēc šāds risks ir pieļaujams (piemēram, iestāde nolemj neveikt pārbaudi attiecībā pret "*Weak Aliases*" vai nolemj neveikt pārbaudi pret divējāda lietojuma preču sarakstiem);
- iestādes sankciju skrīninga sistēma integrēti ar citām kontrolēm datu kvalitātes nodrošināšanai (tādām kā pasākumi, lai nodrošinātu klientu datu kvalitāti, piemēram, klients nevar tikt akceptēts, ja trūkst dzimšanas datuma vai citu identifikācijas datu) spēj identificēt "*fuzzy logic*" sakritību, t. i., iestāde spēj efektīvi identificēt iespējamo sankciju ierakstu, ja pārbaudāmajam ierakstam ir manipulācijas vai pārrakstīšanās kļūdas, t. sk., ja vārdā un datumā ir veiktas manipulācijas;
- skrīninga sistēma darbojas lietderīgi, t. i., sistēma ģenerē kvalitatīvus brīdinājumus, un skrīninga sistēma nerada lielu skaitu viltus pozitīvu rezultātu, tostarp attiecībā uz ierakstiem par personām, kam nav piemērotas sankcijas;
- iestādei ir pietiekami resursi, lai kvalitatīvi un noteiktajos termiņos apstrādātu un izmeklētu brīdinājumus, t. i., apstrādājamo brīdinājumu skaits nerada operacionālos riskus, kas var izraisīt kavējumus vai pazemināt darījumu uzraudzības vai "pazīsti savu klientu" procesu kvalitāti.

Neefektīvas vai nelietderīgas sankciju skrīninga sistēmas darbības biežākie iemesli

Parasti tas, ka skrīninga sistēma nedarbojas, kā paredzēts, var būt viena vai vairāku šādu iemeslu dēļ:

- neatbilstoša konfigurācija (piemēram, skrīninga sistēma brīdina tikai par precīzām vai gandrīz precīzām sankciju ierakstu atbilstībām);
- sankciju skrīninga sistēmas lietderība netiek vērtēta kopā ar sistēmas efektivitāti. Rezultātā sistēma varētu būt ļoti efektīva sankciju ierakstu un manipulēto ierakstu identificēšanā, tomēr viltus pozitīvo rezultātu skaits ir pārāk liels, līdz ar to sistēmas darbība ir nelietderīga, radot operacionālos riskus, vai otrādi – sistēmas darbība ir ļoti lietderīga ar nelielu viltus pozitīvo rezultātu skaitu, tomēr sistēma ir neefektīva manipulētu ierakstu identificēšanā;
- notiek pārmērīga paļaušanās uz tehnoloģiskiem risinājumiem un trešo pušu pakalpojumu sniedzējiem un iestādei ir ierobežota izpratne par sankciju skrīninga sistēmas konfigurāciju;
- skrīninga sistēma tiek izmantota ar "lietošanai gatava" vai rūpnīcas iestatījumiem, nepielāgojot to iestādes specifikai un riskiem;
- sankciju skrīninga sistēmas versija, noteikumi vai iestatījumi nav atjaunināti saprātīgā termiņā vai pēc būtiskām izmaiņām sankciju noteikumos;
- ārējā pakalpojumu sniedzēja izveidotais sankciju saraksts nav pilnībā atjaunināts;
- konstatētas problēmas iestāžu izmantoto sarakstu sinhronizēšanā ar ārējā pakalpojumu sniedzēja sarakstu atjauninājumiem;
- sarakstu pārvaldība – tiek pārbaudīts pārāk daudz vai pārāk maz sankciju avotu;
- nav veikta IT sistēmas testēšana vai testēšanas apjoms ir bijis pārāk ierobežots;
- nav izstrādāta testēšanas vide vai tā būtiski atšķiras no produkcijas vides, vai nav skaidra testēšanas procedūra;
- noziedzīgi iegūtu līdzekļu legalizācijas novēršanas un sankciju riska pārvaldības darbinieku vāja iesaiste sankciju skrīninga sistēmas izveidē vai uzturēšanā;
- trūkumi izmaiņu pārvaldības procesos, piemēram, sankciju skrīninga sistēmas tehniskie aspekti netiek ņemti vērā, kad tiek veiktas izmaiņas citos iestādes procesos;

- nepietiekams vadības atbalsts sankciju skrīninga sistēmas ieviešanā, uzlabošanā un testēšanā.

Testēšanas metodes

Lai izprastu skrīninga sistēmas iespējas un izaicinājumu jomas, ir nepieciešama iesaiste skrīninga sistēmas izveidē un tās testēšana. Sankciju skrīninga sistēmu testēšanai izmantojamas divas galvenās pieejas.

1. **Produkcijas datu testēšana**: šajā metodē izmanto produkcijas datus (iestādes klientu vai darījumu datus) kā datu kopu, pret kuru tiek pārbaudīta sistēmas veiktspēja. Šis ir noderīgs tests, lai novērtētu dažādu sliekšņu, iestatījumu un konfigurāciju ietekmi uz to brīdinājumu skaitu, kas tiek ģenerēti par iestādes esošo datubāzi/iepriekšējiem darījumiem. Šāda veida testēšana mēra operacionālo risku. Vienlaikus šāda testēšana nesniedz pietiekamu pārliecību par atbilstības riskiem, kas saistīti ar skrīninga sistēmām.

2. **Sintētisko datu testēšana**: šajā metodē izmanto sintētiskos datus (mākslīgi ģenerētus datus, kas atdarina reālo datu īpašības, bet nav iegūti no faktiskiem, esošiem ierakstiem) kā datu kopu, pret kuru tiek pārbaudīta sistēmas veiktspēja. Izveidojot testu, kas sastāv no sintētiskiem datiem, un precīzi zinot, kāds ir katra testā iekļautā ieraksta statuss, iespējams precīzi analizēt visas novirzes testa rezultātos.

Piemērojot sintētisko datu testēšanas metodi sankciju skrīningam, publicētie sankciju ieraksti tiek iekļauti testā, lai noteiktu, vai skrīninga sistēma ģenerē brīdinājumus par eksistējošiem sankciju ierakstiem. Ja sistēma neģenerē brīdinājumu par eksistējošu sankciju ierakstu, iestāde var identificēt, kurš ieraksts ir izlaists, un noskaidrot tā iemeslu, kā arī veikt nepieciešamos pasākumus sistēmas darbības uzlabošanai. Produkcijas datu testēšanā un sintētisko datu testēšanā tiek izmantotas atšķirīgas vērtību un metrikas skalas, līdz ar to labā prakse ir sankciju skrīninga sistēmas efektivitātes un lietderības noteikšanai izmantot abas metodes.

Iestādei, veicot sankciju skrīninga sistēmas efektivitātes analīzi, būtu jānodrošina, ka vismaz vienam no vārdiem, attiecībā uz ko ir ģenerēta sakritība saistībā ar sankciju ierakstu, ir pietiekama sakritību saikne (t. i., līdzība, saistība) ar sankciju ierakstu, pret kuru tiek veikta pārbaude. Ja savstarpējās saiknes nav, tad būtu jāuzskata, ka skrīninga sistēma nav ģenerējusi brīdinājumu par sakritību, kas iestādei attiecīgi būtu jāvērtē.

Iestādes, izmantojot uz risku balstītu pieeju, saprātīgu iemeslu dēļ var pielāgot sankciju skrīninga sistēmas "*fuzzy logic*" sakritību iespējas un ģenerēto brīdinājumu līmeni, taču šādai uz risku balstītai pieejai jābūt precīzi definētai, dokumentētai un pamatotai ar pierādījumiem.

Testēšanas veidi

Var izšķirt trīs galvenos skrīninga sistēmu testēšanas veidus.

1. **Ticamības pārbaude**: tā ir neatkarīga un pilnvērtīga sintētisko datu pārbaude, kas sastāv no sankciju ierakstu un manipulēto sankciju ierakstu ("*fuzzy logic*" testēšana) analīzes, kā arī ierakstu, kas nav sankciju sarakstos, analīzes. Ticamības pārbaudes rezultātu secinājumos jāiekļauj pilnvērtīga analīze par katras datu kopas efektivitātes (konstatētās sakritības un neģenerētie brīdinājumi) un lietderības (brīdinājumu līmenis) vērtējumu. Pārbaudes datu kopas minimālajam apjomam ir jābūt tādam, lai tas būtu statistiski nozīmīgs, ievērojot arī iestādes lielumu un darbības specifiku, tajā jāiekļauj ne tikai sankciju ieraksti no oficiāliem sarakstiem un papildu sarakstiem, ja tādi tiek izmantoti saskaņā ar iestādes riska novērtējumu, bet arī manipulēti sankciju ieraksti un ieraksti, kuri nav ietverti sankciju sarakstos (tīrie ieraksti).

Atbilstoši starptautiskās labās prakses piemēriem minimālajai testa datu kopai būtu jāsastāv no vismaz 1500 ierakstiem. Ticamības pārbaudes datnēs jāiekļauj atbilstošs daudzums privātpersonu, juridisko personu, BIC (kredītiestādes identifikācijas kods) kodu (tikai darījumu skrīninga ietvaros) un divējāda lietojuma preču (tikai darījumu skrīninga ietvaros), ja vien nepastāv izsvērts un pamatots iemesls izslēgt kādu konkrētu sankciju ierakstu veidu. Tā kā pārbaudes tvērums attiecas uz fiziskām un juridiskām personām, tajā būtu jāiekļauj arī visi pseidonīmu veidi ("vājš", "spēcīgs" u. c.), kas ir daļa no ticamības pārbaudes.

Iestādēm būtu jānodrošina atbilstoša ticamības pārbaude (paštestēšana vai neatkarīga testēšana, izmantojot ārpakalpojumu sniedzējus, kuriem ir nepieciešamā pieredze un kompetence šādu pārbaužu veikšanai) šādos gadījumos:

- regulāra pārbaude atbilstoši iekšēji noteiktajai regularitātei, bet ne retāk kā reizi 18 mēnešos, vērtējot iekšējās kontroles sistēmas, tostarp sankciju skrīninga sistēmas, darbības efektivitāti un lietderību. Saskaņā ar starptautiskajiem labās prakses piemēriem testēšanu ieteicams veikt vienu reizi 12 mēnešos;
- pārbaude, kad tiek ieviesta jauna sankciju skrīninga sistēma;
- pārbaude, ja produkcijas vidē tiek ieviests nozīmīgs sistēmas atjauninājums vai jauninājums;
- pārbaude, ja esošās sistēmas iestatījumi vai konfigurācijas tiek būtiski mainītas produkcijas vidē.

Ticamības pārbaudes pārskatā ir jābūt skaidri un detalizēti dokumentētai informācijai par rezultātiem, lai tos varētu izmantot sankciju riska pārvaldības iekšējās kontroles sistēmas darbības efektivitātes izvērtēšanai.

2. **Iteratīva pārbaude**: tā ir sistēmas pielāgošanas un optimizācijas pārbaude, kura ietver gan sintētisko datu testēšanas, gan produkcijas datu testēšanas metodi.

Iteratīvās pārbaudes mērķis ir novērtēt un optimizēt iestādes skrīninga sistēmas darbību.

Sintētisko datu testēšanu iteratīvajā pārbaudē ietver ar mērķi izmērīt atbilstības risku un dažādu robežvērtību, iestatījumu un konfigurāciju ietekmi uz sistēmas efektivitāti (konstatētās sakritības un neģenerētie brīdinājumi), kā arī lietderību (brīdinājumu līmeni) attiecībā uz ierakstiem, kas ir sankciju sarakstos, manipulētiem ierakstiem un ierakstiem, kas nav ietverti sankciju sarakstos. Pārbaudes datu apjomu vajadzētu noteikt atbilstoši iestādes lielumam un darbības specifikai, iekļaujot tajā sankciju ierakstus no obligātajiem sankciju sarakstiem, kas iestādēm ir jāpārbauda, kā arī papildu sarakstiem, ja tādi tiek izmantoti saskaņā ar iestādes riska novērtējumu, manipulētus sankciju ierakstus un ierakstus, kas nav ietverti sankciju sarakstos.

Produkcijas datu testēšanu iteratīvajā pārbaudē ietver ar mērķi izmērīt operacionālo risku un dažādu robežvērtību, iestatījumu un konfigurāciju ietekmi uz tādu brīdinājumu līmeni, kas ģenerēti, veicot pašas iestādes klientu bāzes vai vēsturisko darījumu skrīningu. Minētie dati sniedz iestādei informāciju par jaunu robežvērtību, iestatījumu vai konfigurāciju darbības lietderību.

3. **Saraksta atjaunināšanas pārbaude**: šis pārbaudes veids palīdz nodrošināt, ka datu avoti ir atjaunināti. Sarakstu atjaunināšanas pārbaudi ieteicams veikt periodiski vai pēc tam, kad ir publicēti sankciju sarakstu atjauninājumi. Visbiežāk šādu pārbaudi veic sintētisko datu testēšanas ietvaros. Sarakstu atjaunināšanas pārbaude parasti sastāv tikai no noteikta skaita ierakstu, t. i., no jauna pievienoto sankciju ierakstu, pārbaudes, bet alternatīva pieeja ir veikt testēšanu pret visiem sankciju sarakstiem. Vienlaikus tiek sagaidīts, ka iestādes nekavējoties savās sistēmās ieviesīs jaunos sankciju ierakstus vismaz attiecībā uz obligāti piemērojamiem sankciju sarakstiem (ANO, ES, Latvijas).

Paļaušanās uz trešajām personām

Ja iestāde sankciju izvērtēšanai izmanto trešo personu risinājumus, jāņem vērā, ka pilnīga paļaušanās uz ārējā pakalpojumu sniedzēja iespējām nav pieļaujama. Katra iestāde ir atbildīga par sankciju riska efektīvas pārvaldības nodrošināšanu neatkarīgi no tā, vai sankciju skrīningam tiek izmantots iekšējais vai ārējais risinājums. Vienlaikus tiek sagaidīts, ka iestāde ir noteikusi pakalpojumu sniedzējam pienākumu nodrošināt sankciju saraksta atjaunināšanu IT rīkā nekavējoties, tiklīdz ir publicēti jauni sankciju ieraksti, vismaz attiecībā obligāti piemērojamiem sankciju sarakstiem (ANO, ES, Latvijas).

9. piemērs: sadarbība ar trešo pušu pakalpojumu sniedzējiem	
Labā prakse	**Nevēlamā prakse**
Iestāde ir izstrādājusi politiku/procedūras, lai regulāri	Iestāde attiecībā uz sankciju skrīninga sistēmu pilnībā paļaujas uz

uzraudzītu trešās puses pakalpojumu sniedzēja, kas nodrošina iestādei sankciju skrīninga rīku, darbības, kas ietver arī regulāras pārbaudes un piemēru testēšanu (*sample test*). Pārbaudes ietver arī vērtējumu, cik ātri un efektīvi trešās puses pakalpojumu sniedzējs ievieš jaunos sankciju grozījumus/režīmus, t. sk., vai sankciju sarakstos ir iekļauti visi nepieciešamie obligātie saraksti. Tāpat pārbaudes ietvaros vērtē, kādus algoritmus pakalpojumu sniedzējs izmanto, lai identificētu sankciju ierakstus, ja ar pārbaudāmo ierakstu ir veiktas manipulācijas, un cik efektīvi sistēma darbojas. Noslēdzot līgumu ar trešās puses pakalpojumu sniedzēju, iestāde ir nodrošinājusi, ka līgumā ir iekļautas arī prasības par sistēmas uzlabošanas pasākumiem, tostarp tādiem uzlabojumiem, kas izriet no iestādes riskiem, specifikas un ieteikumiem.	trešās puses pakalpojumu sniedzēju. Iestādes darbiniekiem, kas atbild par sankciju riska pārvaldību, nav pietiekamas izpratnes par to, kā darbojas IT sistēma, kādi datu avoti tiek izmantoti, kā tiek identificēti jauni sankciju ieraksti un cik ātri tie tiek ieviesti IT sistēmā, tostarp, kādi sankciju ieraksti (piemēram, pseidonīmu veidi) tiek ņemti vērā.

Secinājums

Šajās vadlīnijās ietvertie labās prakses piemēri un ieteikumi uzsver efektīvas sankciju skrīninga sistēmas darbības nozīmību, t. sk. izklāstīts sagaidāmais rezultāts attiecībā uz labās prakses piemēru ieviešanu, lai finanšu tirgus dalībnieki sekmīgi izpildītu normatīvo aktu prasības attiecībā uz sankciju riska pārvaldību. Iestādēm regulāri jāveic riska novērtējums, jādokumentē sankciju skrīninga sistēmas konfigurēšanas un testēšanas rezultāti un jāievieš nepieciešamie pasākumi atbilstoši iestādes specifiskajiem riskiem. Vienlaikus ir svarīgi atcerēties, ka nepieciešama holistiska pieeja, apvienojot sankciju skrīningu ar citiem kontroles pasākumiem, piemēram, efektīviem "pazīsti savu klientu" procesiem, darbinieku apmācību, sankcijām pakļauto līdzekļu iesaldēšanas procedūrām utt.

Papildus minētajam Tematiskās pārbaudes ietvaros tika identificēti izplatītākie neefektīvas skrīninga sistēmas izveides iemesli, piemēram, neatbilstoša konfigurācija, atjauninājumu trūkums un noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas un sankciju riska pārvaldības komandas vāja iesaiste sankciju skrīninga sistēmu izveidē, testēšanā

un uzturēšanā. Tāpēc Latvijas Banka aicina iestādes regulāri izvērtēt, testēt un uzraudzīt skrīninga sistēmas, nodrošinot, ka tās efektīvi identificē sankciju ierakstus, vienlaikus samazinot viltus pozitīvo rezultātu skaitu. Lai visaptveroši novērtētu sistēmas veiktspēju, ieteicams izmantot dažādas testēšanas metodes.