

BANCA NAȚIONALĂ A MOLDOVEI
COMITETUL EXECUTIV

HOTĂRÂREA nr. __
din „__” _____ 2026

**cu privire la aprobarea unor recomandări în domeniul prevenirii și combaterii spălării
banilor și finanțării terorismului**

În temeiul art.27 alin.(1) lit. c) din Legea nr.548/1995 cu privire la Banca Națională a Moldovei, Comitetul executiv

HOTĂRĂȘTE:

1. Se aprobă:
 - 1.1 Recomandările cu privire la implementarea abordării bazate pe risc în scopul prevenirii și combaterii spălării banilor și finanțării terorismului, conform Anexei nr.1
 - 1.2 Recomandările cu privire la monitorizarea tranzacțiilor și activităților clienților în vederea prevenirii și combaterii spălării banilor și finanțării terorismului, conform Anexei nr.2;
 - 1.3 Recomandările cu privire la stabilirea relațiilor transfrontaliere în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, conform Anexei nr.3.
2. Se abrogă:
 - 2.1 Recomandările cu privire la abordarea bazată pe risc a clienților de către bănci în vederea prevenirii și combaterii spălării banilor și finanțării terorismului, aprobate prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr. 96 din 05.05.2011;
 - 2.2 Recomandările cu privire la monitorizarea de către bănci și prestatorii de servicii de plată nebancari a tranzacțiilor și activităților clienților în vederea prevenirii și

- combaterii spălării banilor și finanțării terorismului aprobate prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr. 256 din 19.12.2013 ;
- 2.3 Recomandările cu privire la stabilirea relațiilor transfrontaliere în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, aprobate prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr. 42 din 27.02.2014;
- 2.4 Recomandările cu privire la identificarea beneficiarului efectiv, aprobate prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr. 147 din 31.07.2014.
3. Prezenta hotărâre intră în vigoare la data adoptării.

**PREȘEDINTELE
COMITETULUI EXECUTIV
AL BĂNCII NAȚIONALE A MOLDOVEI**

Anca-Dana DRAGU

Anexa nr. 1
la Hotărârea Comitetului Executiv
al Băncii Naționale a Moldovei
nr.din

RECOMANDĂRI
cu privire la implementarea abordării bazate pe risc în scopul prevenirii și
combaterii spălării banilor și finanțării terorismului

I. Prevederi generale

1. Recomandările cu privire la implementarea abordării bazate pe risc în scopul prevenirii și combaterii spălării banilor și finanțării terorismului (în continuare – *Recomandări*) au ca scop de a oferi entităților supravegheate (în continuare – *entități/entități raportoare*) îndrumări metodologice în procesul creării unor mecanisme interne efective privind identificarea și evaluarea riscurilor de spălarea banilor și finanțare a terorismului (în continuare - SBFT), precum și celor de neaplicare și eludare a sancțiunilor financiare specifice.

2. Recomandările au ca obiect:

a) descrierea principiilor antrenate în aplicarea abordării bazate pe risc în contextul combaterii spălării banilor și finanțării terorismului;

b) orientarea entităților la stabilirea criteriilor și factorilor de risc asociate domeniului prevenirii și combaterii spălării banilor și finanțării terorismului;

c) orientarea entităților asupra identificării și evaluării riscurilor de spălare a banilor și finanțare a terorismului, precum și a riscurilor de neaplicare și eludare a sancțiunilor financiare specifice;

d) susținerea dezvoltării unei înțelegeri comune a ceea ce presupune o abordare bazată pe risc în contextul combaterii spălării banilor și finanțării terorismului.

3. Recomandările sunt elaborate ținând cont de recomandările Grupului de Acțiune Financiară Internațională (FATF-GAFI) privind abordarea bazată pe risc a clienților în vederea combaterii spălării banilor și finanțării terorismului, documentele autorităților de supraveghere a Uniunii Europene în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, documentele Grupului Wolfsberg privind abordarea bazată pe risc în gestionarea riscurilor de spălare a banilor și alte documente și practici internaționale relevante.

4. Termenii și expresiile utilizate în Recomandări au semnificațiile prevăzute în Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și actele normative emise de către Banca Națională a Moldovei (în continuare - BNM) și Serviciul Prevenirea și Combaterea Spălării Banilor (în continuare - SPCSB) pentru implementarea acesteia.

De asemenea, în sensul prezentelor Recomandări, sunt utilizate următoarele noțiuni:

Amenințare - orice persoană sau grup de persoane, obiect ori activitate care ar putea cauza prejudicii potențiale entității, statului, societății, economiei sau sistemului financiar;

Vulnerabilitate - elemente care pot fi exploatate de către amenințările identificate sau care pot susține ori facilita activitățile acestora;

Risc – reprezintă posibilitatea ca entitatea să fie utilizată în scopul spălării banilor sau finanțării terorismului, evaluată prin raportarea la probabilitatea materializării și la impactul potențial al acesteia;

Riscul inerent - reprezintă nivelul de risc la care este expusă entitatea înainte de luarea în considerare a măsurilor de control și de atenuare, determinat în funcție de natura și caracteristicile clienților, produselor, serviciilor și tranzacțiilor, jurisdicțiilor relevante și canalelor de distribuție utilizate;

Riscul rezidual – reprezintă nivelul de risc rămas după luarea în considerare a eficacității politicilor, procedurilor, sistemelor și controalelor implementate pentru gestionarea și atenuarea riscului inerent;

Pondere - reprezintă, în raport cu un set de indicatori, subcategorii de indicatori sau categorii de indicatori pe baza cărora se determină un scor combinat, măsura în care fiecare dintre aceste elemente va influența determinarea scorului combinat. Indicatorii, subcategoriile și categoriile cu o pondere mai mică vor avea o influență mai mică asupra scorului combinat decât indicatorii, subcategoriile și categoriile cu o pondere mai mare.

Toleranța la risc - nivelul maxim de risc pe care o entitate este dispusă să îl accepte la un moment dat sau într-o anumită perioadă determinată.

II. Abordarea bazată pe risc

5. Entitățile întreprind acțiuni privind identificarea și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului în activitatea proprie, ținând cont de evaluarea riscurilor de spălare a banilor și de finanțare a terorismului la nivel național, precum și de criteriile și factorii stabiliți de BNM și SPCSB. În acest scop, entitățile efectuează și actualizează evaluarea riscurilor în domeniul propriu de activitate, cel puțin anual și după fiecare evaluare a riscurilor de spălare a banilor și finanțare a terorismului la nivel național și, după caz, la identificarea criteriilor și factorilor de risc adiționali de către BNM, SPCSB sau însăși entitate. Acest proces presupune, cel puțin:

- a) Identificarea, evaluarea și clasificarea riscurilor inerente ale entității;
- b) Evaluarea calității controalelor de prevenire și combatere a spălării banilor și finanțării terorismului /neaplicare și eludare a sancțiunilor financiare specifice;
- c) Evaluarea și clasificarea riscurilor reziduale;
- d) Implementarea acțiunilor necesare în scopul gestionării și atenuării riscurilor de spălare a banilor și finanțare a terorismului identificate.

6. Entitățile raportoare adoptă măsuri adecvate și proporționale cu natura, complexitatea și dimensiunea activității desfășurate, în scopul identificării și evaluării riscurilor de spălare a banilor și de finanțare a terorismului la care sunt expuse, ținând cont cel puțin de:

- a) factorii de risc prevăzuți la pct. 16, 17, 19 și 21 și,

b) variabilele de risc asociati, enumerați la pct.18 și 20;

7. Evaluarea riscurilor la nivel de entitate este efectuată în baza unei metodologii proprii, cu considerarea prezentelor Recomandări, adaptate în funcție de natura, dimensiunea și complexitatea activității desfășurate. Metodologia proprie a entității se revizuieste periodic și se actualizează în funcție de evoluțiile în domeniul de activitate, produsele, serviciile, canalele de distribuție noi utilizate, inclusiv tehnologii noi sau aflate în dezvoltare or, după caz a unor modificări survenite în cadrul normativ de prevenire și combatere a spălării banilor și finanțării terorismului.

8. Rezultatele evaluării în domeniul propriu de activitate a riscurilor de spălare a banilor și de finanțare a terorismului sunt consemnate într-un Raport de evaluare, aprobat de către persoana cu funcție de conducere de rang superior desemnată responsabilă de asigurarea conformității politicilor și procedurilor cu cerințele legale privind prevenirea și combaterea spălării banilor și finanțării terorismului din cadrul entității raportoare, și se actualizează anual de entitatea raportoare, iar la cerere se prezintă BNM sau SPCSB.

9. Eficiența abordării bazate pe risc în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului este asigurată atunci când controalele interne ale entității sunt stabilite și implementate proporțional nivelului de risc identificat, astfel încât resursele disponibile să fie alocate prioritar către ariile cu cel mai ridicat risc, iar măsurile aplicate să contribuie la gestionarea și atenuarea eficientă a riscurilor identificate.

10. Implementarea abordării bazate pe risc cuprinde cel puțin următoarele aspecte:

a) identificarea și evaluarea riscului asociat clienților, produselor/ serviciilor oferite, canalelor de distribuției utilizate și jurisdicțiilor implicate;

b) gestionarea și atenuarea riscului identificat, prin implementarea unor sisteme de control intern și măsurilor de precauție proporționale nivelului de risc identificat;

c) menținerea datelor actualizate despre clienți, beneficiarii efectivi ai acestora, precum și tranzacțiile/operațiunile clienților, astfel încât profilul de risc să reflecte situația reală și curentă;

d) monitorizarea continuă a tranzacțiilor și activităților clienților, cu ajustarea frecvenței și intensității monitorizării în funcție de nivelul de risc atribuit clienților, entității și/ sau riscurile emergente.

11. Pentru efectuarea unei evaluări adecvate a riscurilor de spălare a banilor și finanțare a terorismului, entitatea poate consulta, fără a se limita, următoarele surse de informații:

a) Raportul național de evaluare a riscurilor de spălare a banilor și finanțare a terorismului;

b) Rapoarte de evaluare supranaționale (de exemplu, Raportul de evaluare a riscurilor întocmit de Comisia Europeană) sau regionale;

c) Informații de la autoritățile cu funcții de supraveghere (rapoarte de evaluare a riscurilor sectoriale de spălare a banilor și finanțare a terorismului, recomandări, scrisori, etc.);

d) Informații de la SPCSB și organele de drept privind amenințări, alerte și tipologii identificate (rapoarte ale Ministerului Afacerilor Interne, rapoarte ale Serviciului de Informații și Securitate, etc);

e) Informații din listele de sancțiuni sau alte liste menținute de autoritățile competente pentru a identifica persoanele, entitățile, jurisdicțiile sau modelele (tiparele) relevante pentru riscurile de spălare a banilor/finanțare a terorismului și celor asociate eludării sancțiunilor financiare specifice;

f) Cunoștințele angajaților entității și expertiza profesională a acestora, inclusiv având în vedere informațiile obținute în procesul de cunoaștere a clienților, sau de identificare a tranzacțiilor și activităților suspecte, precum și din răspunsurile recepționate de la autoritățile competente în acest context;

g) Informații privind tipologii și riscuri identificate de asociațiile de profil din sectoarele economiei, precum și informațiile din partea asociațiilor profesionale, organizațiilor de statistică și din mediul academic;

h) Informații furnizate de societatea civilă, așa ca indici de corupției și rapoarte de țară;

i) Surse externe credibile, cum ar fi, rapoartele de risc și de informații, și materiale din surse deschise fiabile privind tipologiile, riscurile emergente și activitatea infracțională (așa ca, articole obiective din presă sau articole ale jurnalismului independent de investigație);

î) Alte informații și date statistice relevante cu referire la indicii care atestă tendințe relevante (rata criminalității, infracțiunile asociate fraudelor, evaziunii fiscale, etc.), precum și căror categorii de clienți sunt asociate (zona geografică, vârsta, etc);

12. În procesul de implementare a abordării bazate pe risc, entitatea stabilește nivelul de risc pe care este dispusă să îl accepte, având în vedere natura, dimensiunea și complexitatea activității desfășurate, profilul său de risc și capacitatea de gestionare a riscurilor. Toleranță la risc se raportează la nivelul riscului rezidual și poate fi reflectată, după caz, prin limite privind expunerea la anumite categorii de clienți, produse, servicii, canale de distribuție sau zone geografice cu risc ridicat.

13. Stabilirea toleranței la risc nu poate conduce la neaplicarea sau aplicarea incompletă a obligațiilor prevăzute de cadrul normativ în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului și nici a obligațiilor privind sancțiunile financiare specifice. În cazul în care nivelul riscului rezidual depășește limitele de toleranță stabilite, entitatea întreprinde măsuri suplimentare pentru gestionarea și diminuarea riscului sau, după caz, limitează sau nu inițiază/continuă activitatea sau relația de afaceri care generează expunerea respectivă.

14. Materializarea riscurilor de spălare a banilor și de finanțare a terorismului sau deficiențele în gestionarea acestora pot genera sau amplifica, după caz, riscuri conexe pentru entitate, inclusiv riscuri reputaționale, juridice, de reglementare și operaționale.

III. Identificarea și evaluarea riscului de spălare a banilor și finanțare a terorismului, precum și de neaplicare și eludare a sancțiunilor financiare specifice

15. La desfășurarea procesului de identificare și evaluare a riscului de spălare a banilor și finanțare a terorismului, precum și de neaplicare și eludare a sancțiunilor financiare specifice, entitatea utilizează următoarele etape:

- 1) Identificarea factorilor de risc și variabilele de risc asociate;
- 2) Evaluarea riscului inherent;
- 3) Evaluarea eficienței controalelor interne aplicate de către entitate;
- 4) Determinarea riscului rezidual;
- 5) Implementarea acțiunilor de atenuare a riscurilor identificate.

Etapa 1: Identificarea factorilor de risc și variabilele de risc asociate

16. Factorii de risc privind **clienții** care ar putea duce la creșterea riscului de spălare de bani și finanțare a terorismului, sunt:

1) clienții care întârzie nejustificat, refuză să prezinte sau furnizează documente și informații incomplete, neveridice sau neverificabile în procesul de identificare și cunoaștere a clientului;

2) clienții care desfășoară activități și/sau efectuează tranzacții (operațiuni) în circumstanțe neobișnuite, fără a se limita la:

a) tranzacții semnificative, complexe și neordinare care aparent nu au un scop legal sau economic;

b) transferuri multiple de mijloace bănești sau fragmentate între agenții economici și/sau persoane fizice din diferite jurisdicții, fără un scop economic clar;

c) efectuează plăți/transferuri călătorind fără un scop bine definit în alte localități;

d) formează grupuri de persoane ce tranzacționează multiplu în diferite locații;

e) clienții care nu prezintă informație despre plătitor/beneficiarul plății (adresa, informații de contact, etc) sau prezintă informație incompletă;

f) clienții despre care se cunoaște că au fost implicați în activități infracționale sau au fost sancționați sau sunt menționați în rapoarte specializate care descriu tipologii și criterii de risc;

g) persoane juridice sau construcții juridice cu rol de structuri de administrare a activelor personale;

h) entități corporative care au acționari nominali sau acțiuni la purtător;

i) structura de proprietate a societății pare neobișnuit sau excesiv de complexă, având în vedere natura activității societății;

î) clientul este o entitate juridică sau o construcție juridică creată sau constituită într-o jurisdicție în care nu are activitate economică reală, nici o prezență economică substanțială sau o justificare economică aparentă;

j) clientul este deținut, în mod direct sau indirect, de una sau mai multe entități sau construcții menționate la litera î).

3) clienții a căror structură a fondatorilor (asociaților) este complexă și nu permite identificarea beneficiarului efectiv sau clienții a căror beneficiari efectivi sunt rezidenți ai unor țări/zone enumerate la pct.19.

4) clienți sau beneficiari efectivi sunt persoane expuse politic (PEP), membrii de familie ai PEP, persoane cunoscute ca fiind persoane asociate PEP;

5) clienții sau beneficiarii efectivi care au legături cu sectoare asociate frecvent cu un risc mai ridicat de corupție, precum: domeniul construcțiilor; industria farmaceutică și domeniul sănătății; comerțul cu arme și sectorul apărării; industriile extractive și achizițiile publice etc.;

6) clienții care își desfășoară activitatea în țările/jurisdicțiile enumerate la pct.19 sau care își au sediul/domiciliul în aceste țări/jurisdicții, sau clienții care mențin relații de afacere cu agenții economici cu sediul în aceste țări;

7) clienții a căror activitate presupune utilizarea intensă a mijloacelor bănești în numerar:

a) dealeri angro și cu amănuntul de produse, inclusiv agricole, agenți economici care facilitează schimbul sau transferul de mijloace bănești și bunuri, inclusiv dealeri auto;

b) cazinourile (inclusiv internet-cazinourile), organizațiile care organizează și desfășoară tombola, loterii sau jocuri de noroc;

8) organizațiile de caritate (filantropie) sau alte organizații necomerciale, activitatea cărora de colectare sau distribuire a mijloacelor și bunurilor în scopuri filantropice, religioase, culturale, de învățământ, sociale sau scopuri analogice poartă un caracter neobișnuit și nu corespunde documentului de constituire și statutului aprobat;

9) organizațiile de caritate (filantropice) sau alte organizații necomerciale din țările/jurisdicțiile care acordă finanțare sau sprijin pentru activități teroriste sau pe teritoriul cărora activează organizații teroriste desemnate;

10) clienții care, în activitatea lor, nu acționează în numele propriu și în același timp efectuează tranzacții complexe și neordinare, cum ar fi:

a) agenții imobiliari, în cazul în care efectuează tranzacții (operațiuni) pentru clienții lor privind vânzarea și cumpărarea de bunuri imobile;

b) participanții profesioniști la piața valorilor mobiliare;

c) avocații, notarii sau alte persoane care practică activitatea profesională independentă și contabilii, atunci când aceștia pregătesc sau efectuează tranzacții (operațiuni) în numele clientului legate de următoarele activități: vânzări și cumpărări de imobile; administrarea banilor, obligațiunilor sau a altor active ale clientului; administrarea conturilor bancare sau a obligațiunilor; organizarea contribuțiilor pentru crearea sau administrarea agenților economici; crearea, administrarea sau conducerea persoanelor juridice sau aranjamentelor legale (de exemplu, fonduri de investiții) și vânzarea și cumpărarea agenților economici;

d) furnizorul de servicii pentru fiducii sau societăți care prestează unor terți, cu titlu profesional, oricare dintre următoarele servicii: constituirea de societăți sau de alte persoane juridice; exercitarea funcției de director sau secretar al unei societăți, de partener în cadrul unei asocieri sau a unei funcții similare legate de alte persoane juridice ori organizarea ca o altă persoană să exercite astfel de funcții; furnizarea unui sediu social, a unei adrese comerciale, poștale sau administrative și a oricăror altor servicii conexe pentru o societate, o asocierie sau orice altă persoană juridică sau construcție juridică; exercitarea funcției de acționar pe seama unei persoane alta decât o societate cotate pe o piață reglementată care face obiectul cerințelor de divulgare a informațiilor în conformitate cu dreptul Uniunii Europene sau al unor standarde internaționale echivalente ori organizarea ca o altă persoană să exercite o astfel de funcție;

11) clienții - rezidenți ai zonelor economice libere a căror activitate este complexă și neordinară;

12) clienții a căror activitate este legată de domeniul sportului (de exemplu: cluburi sportive, asociații sportive etc.);

13) dealeri de metale și pietre prețioase sau de bunuri cu valoare înaltă (dealeri cu obiecte de artă sau antichități, dealerii de bijuterii, perle, case de licitații, case de amanet, etc.);

14) clienți – producători de armament, precum și dealerii și intermediarii acestora;

15) clienții care se regăsesc în rapoarte media negative sau alte surse relevante, de exemplu, existența de acuzații împotriva clientului sau a beneficiarului efectiv privind comiterea de infracțiuni sau a unor acte de terorism, sau au fost blocate activele acestora ca urmare a unor acțiuni administrative sau penale, etc.

17. Factorii de risc care ar putea duce la creșterea riscului asociat produsului, serviciului sau tranzacției, sunt:

a) serviciile sau produsele identificate de către organizațiile internaționale ca servicii sau produse ce impun un risc sporit, cum ar fi: relațiile cu instituțiile financiare corespondente care oferă servicii persoanelor care nu sunt clienți (payable through accounts), servicii bancare de gestionare și păstrare personalizată a portofoliilor de active, etc;

b) serviciile sau produsele ce implică comerțul cu metale prețioase sau pietre prețioase, tranzacționarea și livrarea bancnotelor și monedelor, cambiilor, a altor instrumente financiare la purtător;

c) tranzacțiile (operațiunile) de finanțare a comerțului internațional, cum ar fi acreditivele documentare, tratele etc.;

d) produsele sau serviciile implică flux ridicat de numerar;

e) produsele sau serviciile facilitează sau încurajează tranzacțiile de valori mari;

f) operațiunile cu instrumente financiare străine;

g) servicii sau produsele care permit păstrarea anonimului etc.;

h) transferuri de mijloace bănești către activități ilegale de jocuri prin internet;

i) transferuri de mijloace bănești în scopul revendicării de câștiguri, achitării de taxe pentru angajare sau oportunități de cumpărături misterioase, care indică asupra unei potențiale fraude de consum;

î) transferuri de mijloace bănești către clienți care împart aceleași date de contact (adresă, email, telefon, etc.) în lipsa unei explicații rezonabile despre această partajare;

j) produsele/serviciile asociate comerțului și/sau tranzacțiilor (operațiunilor) cu activele/monedele virtuale;

k) plăți primite de la terți necunoscuți sau neasociați;

l) tranzacții legate de petrol, arme, produse din tutun, obiecte de artă și alte obiecte de importanță arheologică, istorică, culturală și religioasă sau obiecte rare cu valoare științifică, precum și fildeș și specii protejate.

m) alte servicii sau produse ce pot impune riscuri sporite de spălare a banilor și finanțare a terorismului.

18. Atunci când entitatea identifică riscul asociat produselor, serviciilor sau tranzacțiilor va lua în considerare următoarele variabile de risc:

a) scopul relației de afaceri, a contului sau serviciului solicitat;

b) regularitatea sau durata relației de afaceri;

- c) nivelul activelor care urmează a fi depuse de un client sau dimensiunea tranzacțiilor efectuate;
- d) nivelul de transparență sau de opacitate al produsului, serviciului sau tranzacției;
- e) complexitatea produsului, serviciului sau tranzacției;
- f) valoarea sau dimensiunea produsului, serviciului sau tranzacției.

19. Factorii de risc care ar putea duce la creșterea riscului asociat **zonelor geografice** asociate clientului, beneficiarului efectiv sau relației de afaceri al acestuia, sunt:

a) țări de destinație (jurisdicții), identificate de către GAFI, care fac obiectul unei monitorizări sporite sau/și țări cu deficiențe strategice de conformitate în sistemele lor de combatere a spălării banilor și finanțării terorismului;

b) țările de destinație (jurisdicțiile) care, conform unor surse credibile (evaluări reciproce, rapoarte detaliate de evaluare sau rapoarte de monitorizare publicate), nu dispun de sisteme efective de prevenire și combatere a spălării banilor și a finanțării terorismului;

c) țările de destinație (jurisdicțiile) care, conform unor surse credibile, au un nivel ridicat al corupției sau al altor activități infracționale;

d) țările de destinație (jurisdicțiile) care sunt supuse unor sancțiuni, embargouri sau măsuri similare, instituite de către organizațiile internaționale de profil, conform angajamentelor asumate de către Republica Moldova;

e) țările de destinație (jurisdicțiile) care acordă finanțare sau sprijin pentru activități teroriste sau pe teritoriul cărora activează organizații teroriste desemnate;

f) țări identificate în baza unor surse credibile sau în temeiul unor procese recunoscute ca permițând secretul financiar prin:

- crearea de bariere în calea cooperării și a schimbului de informații cu alte jurisdicții;

- legi stricte privind secretul de afaceri sau secretul bancar care împiedică instituțiile și angajații acestora să furnizeze autorităților competente informații referitoare la clienți, inclusiv prin amenzi și sancțiuni;

- controale deficitare în ceea ce privește crearea de entități juridice sau constituirea de construcții juridice;

- lipsa unor cerințe de înregistrare sau păstrare într-o bază de date centrală sau într-un registru central a informațiilor privind beneficiarii efectivi ai clientului.

g) țările sau jurisdicțiile, identificate de către entitate sau autoritățile competente, care nu se conformează standardelor internaționale în materie de transparență fiscală și schimb de informații.

20. Entitatea va lua în considerare că natura și scopul relației de afaceri determină, în mod frecvent, importanța relativă a factorilor de risc specifici fiecărui stat sau zonă geografică, și anume:

a) în cazul în care fondurile utilizate în relația de afaceri provin din străinătate, nivelul infracțiunilor principale asociate spălării banilor și eficacitatea sistemului juridic al unui stat respectiv vor fi deosebit de relevante;

b) în cazul în care fondurile sunt primite din sau transferate către jurisdicțiile în care se știe că activează grupări implicate în acte de terorism, entitatea va analiza în ce măsură

aceasta poate genera suspiciuni, având în vedere informațiile deținute cu privire la scopul și natura relației de afaceri;

c) în cazul în care clientul este o instituție de credit sau financiară, entitatea va acorda o atenție sporită caracterului adecvat al regimului de prevenire și combatere a spălării banilor sau a finanțării terorismului din statul respectiv, precum și eficacității supravegherii pe linia combaterii spălării banilor sau a finanțării terorismului;

d) în cazul în care clientul reprezintă o construcție juridică sau fiducie, entitatea va avea în vedere măsura în care statul în care este înregistrat clientul și, după caz, beneficiarul efectiv, respectă standardele internaționale privind transparența fiscală.

21. Factorii de risc care ar putea duce la creșterea riscului asociat **canalelor de distribuție** prin intermediul căruia clientul obține produsele sau serviciile pe care le solicită, sunt:

- a) măsura în care relația de afaceri se desfășoară cu prezență fizică sau la distanță;
- b) prezența unui intermediar la desfășurarea relațiilor cu clientul (agent, sucursală, o altă parte terță);
- c) desfășurarea relației de afaceri cu clientul prin intermediul mijloacelor electronice, digitale și de e-banking.

22. La analiza riscurilor de eludare a sancțiunilor financiare țintite entitatea atrage atenție suplimentară asupra următorilor indicatori de risc specifici:

- a) schimbările în structura de proprietate și control a clientului, care pot conduce la ascunderea asocierii administratorilor, acționarilor și beneficiarilor efectivi cu lista persoanelor desemnate;
- b) existența asocierilor dintre client sau persoanelor care controlează clientul și /sau partenerii acestuia cu jurisdicții supuse unor sancțiuni, embargouri sau alte măsuri similare, instituite de către organizațiile internaționale de profil;
- c) falsificarea documentelor asociate activității clientului în scopul ascunderii bunurilor comercializate, a beneficiarului acestor bunuri, a jurisdicției beneficiare, precum și a altor parteneri implicați (companie de transport, intermediarul/brokerul, nava utilizată pentru transportul bunurilor, valoarea și tipul bunurilor, etc);
- d) efectuarea transferurilor complexe și neordinare ce presupun ascunderea beneficiarilor reali, utilizarea intermediarilor neasociați, a jurisdicțiilor netransparente, a instituțiilor financiare multiple, disimularea părților implicate și a bunurilor comercializate.

Etapă 2: Identificarea riscului inerent

23. Procesul de evaluare a riscurilor la nivelul entității este proporțional cu natura, dimensiunea, complexitatea și profilul de risc al activității acesteia. Pentru entitățile cu o activitate de dimensiuni reduse sau cu un grad scăzut de complexitate, metodologia de evaluare poate fi adaptată corespunzător, fără a afecta identificarea, evaluarea și înțelegerea adecvată a riscurilor relevante. În situația în care entitatea oferă produse și servicii variate ori complexe, dispune de multiple structuri sau subdiviziuni interne ori

deține o bază de clienți eterogenă, procesul de evaluare va avea un grad mai ridicat de complexitate și detalieri.

24. Pentru identificarea și înțelegerea principalelor amenințări la care poate fi supusă entitatea, se realizează analiza activității acesteia, având în vedere aria geografică de activitate, numărul și tipologia clienților, natura produselor/ serviciilor oferite, precum și canalele prin care acestea sunt distribuite. Astfel, pentru evaluarea riscului inerent, în dependență de aria de activitate, entitatea poate utiliza indicatorii specifici de risc reflectați în categoria/subcategoriile de risc din *anexa nr. 1*.

25. În vederea evaluării riscului inerent de spălare a banilor și finanțare a terorismului poate fi utilizate mai multe metode de evaluare, printre care: cea cantitativă, prin determinarea ponderii unor produse, servicii, clienți, activități etc. în totalul acestora din cadrul entității, astfel încât să se determine nivelul de expunere la risc, sau prin metoda calitativă, prin construirea unei matrice cu ponderi de evaluare alocate fiecărei categorii de risc, cu luarea în calcul a ponderii și impactului fiecărui indicator specific ce influențează riscul general de spălare a banilor și finanțare a terorismului analizat.

26. Cu titlu orientativ, entitatea poate utiliza, pentru identificarea și evaluarea riscului inerent, o metodologie bazată pe atribuirea de scoruri și ponderi categoriilor și indicatorilor de risc relevanți activității sale, inclusiv indicatorilor prevăzuți în *anexa nr. 1*. Entitatea poate utiliza și alte scale de evaluare, praguri sau metode de agregare, cu condiția ca acestea să fie adecvate naturii, dimensiunii, complexității și profilului său de risc, să fie documentate și să permită reflectarea corespunzătoare a riscurilor identificate.

Un exemplu de aplicare a unei metodologii de scorare este prezentat în continuare:

- a) *Pasul 1* - atribuirea unei valori numerice (scor) variind de la 1 (cel mai mic nivel de risc) până la 4 (cel mai ridicat nivel de risc) indicatorilor specifici de risc relevanți.
- b) *Pasul 2* - atribuirea unei pondere fiecărei categorii de indicatori de risc, în dependență de relevanța acestora activității entității. Ponderea atribuită categoriei de indicatori de risc trebuie să reflecte importanța riscului asociat fiecărei categorii, iar valoarea totală a acesteia va constitui 100%.
- c) *Pasul 3* - determinarea scorului combinat pentru toate categoriile de indicatori de risc ținând cont de ponderea atribuită fiecărei categorii, având în vedere scorul atribuit indicatorilor specifici de risc.
- d) *Pasul 4* - determinarea riscului inerent al entității prin efectuarea calculului complet al riscului asociat fiecărui indicator în dependență de ponderea atribuită categoriei din care face parte.
- e) *Pasul 5* - în baza scorului obținut, încadrarea riscului inerent al entității, după cum urmează:

Scor < 1,75:	<i>Risc scăzut</i>
1.75 ≤ Scor < 2,5:	<i>Risc mediu</i>
2.5 ≤ Scor < 3,25:	<i>Risc substanțial</i>
Scor ≥ 3,25:	<i>Risc ridicat</i>

Etapă 3: Evaluarea controalelor aplicate de entitate

27. După identificarea și evaluarea riscurilor inerente de spălarea banilor și finanțării terorismului în cadrul entității, se va examina eficacitatea sistemelor de gestionare și control al riscurilor aplicate de către entitate. Obiectivul este de a evalua amploarea măsurilor de atenuare a riscurilor aplicate de entitate și de a verifica dacă acestea sunt adecvate în raport cu profilul de risc asociat. În urma evaluării, se va decide dacă măsurile de atenuare a riscurilor aplicate sunt proporționale cu riscurile de SB/FT identificate, inclusiv în ceea ce privește categoriile de clienți, produsele și serviciile oferite, expunerile față de zona geografică și canalele de distribuție.

28. În vederea evaluării eficacității controalelor și a gradului de conformare a programelor de prevenire și combatere a spălării banilor și finanțării terorismului (în continuare - PCSBFT), entitățile pot utiliza indicatorii sistemului de control PCSBFT reflectați în anexa nr.2.

29. Un exemplu de utilizare de către entitate a metodologiei de evaluare a calității controalelor de prevenire și combatere a spălării banilor și finanțare a terorismului, este redat în continuare:

- a) *Pasul 1* - atribuirea unei valori numerice (scor) variind de la 1 (cel mai înalt nivel al calității) până la 4 (cel mai mic nivel al calității) indicatorilor de control relevanți.
- b) *Pasul 2* - atribuirea unei pondere fiecărei categorii de indicatori de control, în dependență de relevanța acestora activității entității. Ponderea atribuită categoriei de indicatori de control trebuie să reflecte importanța riscului asociat acestei categorii, iar valoarea totală a acestora va constitui 100%.
- c) *Pasul 3* - în dependență de scorul atribuit indicatorilor de calitate a controlului, entitatea va determina scorul combinat pentru toate categoriile de indicatori ținând cont de ponderea atribuită fiecărei categorii.
- d) *Pasul 4* - determinarea calității controlului PCSBFT entității prin efectuarea calcului complet asociat fiecărui indicator în dependență de ponderea categoriei din care face parte.
- e) *Pasul 5* - în baza scorului obținut, entitatea va încadra controlul PCSBFT al entității după cum urmează:

Scor < 1,75: Calitatea Foarte bună a controalelor

1,75 ≤ Scor < 2,5: Calitatea bună a controalelor

2,5 ≤ Scor < 3,25: Calitatea moderată a controalelor

Scor ≥ 3,25: Calitatea slabă a controalelor

30. La evaluarea eficienței controalelor interne ale entității în scopul atenuării riscului general de spălare a banilor și finanțare a terorismului, urmează a fi considerate cerințele actelor normative pe care entitățile au obligația să le implementeze în procesul de cunoaștere a clientelei, în special cu referire la:

- a) politicile și procedurile interne aprobate;
- b) implementarea cerințelor de identificare și evaluare a riscurilor de SB/FT;
- c) implementarea măsurilor de precauție față de clienți proporțional riscurilor specifici de SB/FT identificate;
- d) implementarea cerințelor de raportare a activităților/ tranzacțiilor suspecte;

e) implementarea procedurilor de monitorizare, compilare, păstrare și actualizare a listei persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive internaționale, conform cerințelor Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

f) implementarea sistemelor informatice specializate destinate monitorizării continue a tranzacțiilor, depistarea activităților/ tranzacțiilor suspecte;

g) instruirea continuă a angajaților în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, etc.;

31. Regulile privind cunoașterea clientului au drept scop formarea unei înțelegeri adecvate la nivelul entității a profilului fiecărui client, a naturii relației de afaceri și a tipului de tranzacții (operațiunilor) preconizate. Regulile privind cunoașterea clientului vor include:

a) identificarea și verificarea identității fiecărui client în termenele și condițiile prevăzute de cadrul normativ aplicabil;

b) aplicarea unor măsuri adecvate bazate pe risc, pentru identificarea și verificarea identității beneficiarului efectiv;

c) obținerea de informații suplimentare în vederea cunoașterii activității clientului, inclusiv a scopului și a naturii relației de afaceri, a sursei mijloacelor bănești, precum și a tipului de tranzacții (operațiuni) preconizate a fi efectuate.

32. În procesul de aplicare a măsurilor de cunoaștere a clienților se va lua în considerare faptul că nu toate activitățile/ tranzacțiile, conturile sau categoriile de clienți sunt supuse unui mecanism uniform de monitorizare. Modalitatea și intensitatea monitorizării va depinde de profilul de risc al fiecărui client, de tipul de produs sau serviciu utilizat, de sediul (reședința) clientului, precum și de locul în care sunt efectuate tranzacțiile (operațiunile).

De asemenea, sistemul de monitorizare, în cadrul abordării bazate pe risc, poate utiliza praguri valorice, scenarii și criterii calibrate în funcție de profilul de risc, fără ca acestea să conducă la excluderea automată de la monitorizare a activității sau tranzacțiilor (operațiunilor) clientului. Pragurile, scenariile și criteriile utilizate se revizuiesc periodic pentru a se asigura că rămân adecvate și proporționale cu profilul de risc al clientului și cu natura activităților desfășurate.

Etapă 4: Determinarea riscului rezidual

33. Nivelul riscului rezidual se raportează la limitele de toleranță la risc stabilite de entitate, după aplicarea măsurilor de control și de atenuare. În cazul în care nivelul riscului rezidual depășește limitele de toleranță stabilite sau măsurile existente nu asigură o atenuare adecvată a riscurilor identificate, entitatea revizuieste eficacitatea controalelor aplicate și adoptă măsuri suplimentare de gestionare și diminuare a riscurilor.

34. În funcție de nivelul determinat și de limitele de toleranță stabilite, riscurile reziduale pot fi clasificate în:

a) riscuri acceptate – riscuri care, după aplicarea măsurilor de control și de atenuare relevante, se situează în limitele de toleranță stabilite de entitate și nu necesită măsuri suplimentare imediate, fără a exclude monitorizarea și reevaluarea periodică;

b) riscuri care necesită măsuri suplimentare de atenuare – riscuri pentru care controalele existente nu reduc suficient nivelul de expunere și pentru care entitatea trebuie să consolideze ori să introducă măsuri suplimentare de gestionare și diminuare.

35. Cu titlu orientativ, entitatea poate utiliza o metodologie de determinare a riscului rezidual prin combinarea nivelului riscului inerent cu evaluarea eficacității controalelor aplicate. Metodologia utilizată trebuie să fie documentată, proporțională cu profilul de risc al entității și să permită reflectarea adecvată a efectului măsurilor de control asupra riscului inerent.

Un exemplu de utilizare de către entitate a metodologiei de identificare și evaluare a riscului rezidual în baza scorurilor obținute pentru riscul inerent și calitatea controalelor PCSBFT, este redat în continuare:

- a) *Pasul 1* - în cazul în care scorul numeric obținut aferent calității controalelor PCSBFT în cadrul entității este mai mare decât scorul numeric obținut pentru riscul inerent, entitatea va considera riscul rezidual egal cu riscul inerent.
- b) *Pasul 2* - în cazul în care scorul numeric obținut aferent calității controalelor PCSBFT în cadrul entității este mai mic sau egal cu scorul numeric obținut pentru riscul inerent, entitatea va considera riscul rezidual ca o medie între scorul obținut pentru calitatea controalelor PCSBFT și scorul riscului inerent.
- c) *Pasul 3* - în baza scorului obținut, va încadra riscul rezidual al entității după cum urmează:

Scor < 1,75:	Risc scăzut
1.75 ≤ Scor < 2,5:	Risc mediu
2.5 ≤ Scor < 3,25:	Risc substanțial
Scor ≥ 3,25:	Risc ridicat

36. Pentru identificarea și evaluarea riscurilor inerente de spălare a banilor și finanțare a terorismului, entitatea poate utiliza și alte metode, exemple relevante fiind ilustrate sumar în anexa nr.3 și nr.4, care se bazează pe analiza combinată a diferitor factori de risc și măsuri de control în funcție de experiențele anterioare, de situațiile identificate în practică, precum și de contextul specific în care entitatea își desfășoară activitatea. Impactul potențial reflectă gravitatea consecințelor asociate materializării riscului de spălare a banilor sau de finanțare a terorismului, inclusiv efectele pe care aceasta le poate produce asupra expunerii entității la riscuri juridice, operaționale, financiare sau reputaționale.

Etapă 5: Implementarea acțiunilor de atenuare a riscurilor identificate

37. În rezultatul exercițiului de evaluare a riscurilor, entitatea va demara implementarea abordării bazată pe riscuri în cadrul activității desfășurate. Pentru asigurarea unui nivel sporit de eficiență, evaluarea riscului trebuie să fie o parte componentă, bine detaliată și integrată în cadrul sistemului de conformitate. Funcția de conformitate organizată corespunzător, exercitată în mod eficient și cuprinzător reprezintă

un indicator al angajamentului de prevenire, detectare și gestionare a situațiilor de neconformitate.

38. Politicile și procedurile de conformitate în domeniul combaterii spălării banilor și finanțării terorismului trebuie să fie comunicate clar, înțelese și respectate de întreg personalul care interacționează cu clienții. Aceasta include, în mod special, angajații responsabili de aplicarea măsurilor de identificare a clienților, de procesul de păstrare a datelor și raportare a anumitor tipuri de tranzacții către autoritățile competente. Angajații din prima linie trebuie să dispună de informațiile necesare pentru a procesa și finaliza în mod corect tranzacțiile, precum și pentru a identifica clienții și a păstra datele relevante, în conformitate cu politicile interne și cadrul normativ aplicabil.

39. În același context, politicile și procedurile ar trebui să includă domeniile de activitate ale entității vulnerabile riscului spălării banilor și finanțării terorismului și urmează să seteze responsabilitățile personalului la diferite nivele ierarhice, modul de aprobare a inițierii/ continuării relațiilor de afaceri cu clienți cu risc sporit, și acțiunile implementate care să conducă la diminuarea riscului de spălare a banilor și finanțare a terorismului.

40. În vederea asigurării gestionării eficiente a riscului de spălare a banilor și finanțare a terorismului entitatea va alocă resursele necesare (personal, timp, echipamente, informație etc.) proporțional profilului de risc asumat, iar procesul de evaluarea a riscului va include etape de revizuire periodice, pentru a testa și verifica eficacitatea acestuia și a cadrului de conformitate asociat domeniului prevenirii și combaterii spălării banilor și finanțării terorismului.

41. Având în vedere caracterul dinamic al metodelor de spălare a banilor și finanțare a terorismului, entitatea va asigura monitorizarea continuă a tendințelor, tipologiilor și factorilor de risc relevanți și va revizui periodic modelul intern de evaluare a riscurilor, precum și modul de aplicare a abordării bazate pe risc în relația cu clienții, în conformitate cu cadrul normativ aplicabil. Totodată, evaluările periodice ale riscurilor vor include testarea caracterului robust al metodologiei utilizate și a fiabilității surselor de informații utilizate, în vederea identificării și remedierii eventualelor deficiențe metodologice sau operaționale.

Anexa nr. 1 Riscul Inerent

Categorie	Subcategorie	Puncte de referință
Clienți		Numărul clienților persoane juridice Numărul clienților persoane fizice Numărul clienților Persoane Expuse Politic (PEP) rezidente (inclusiv membri ai familiei și asociați apropiați) Numărul clienților Persoane Expuse Politic (PEP) nerezidente (inclusiv membri ai familiei și asociați apropiați)

		Numărul de clienți cu cel puțin o tranzacție în anul precedent Numărul de clienți noi în anul precedent Numărul clienților organizații non-profit Numărul de organizații non-profit cu tranzacții transfrontaliere către/dinspre țări cu risc înalt Numărul clienților persoane juridice cu structură complexă de proprietate Numărul de clienți cu activități cu risc ridicat Numărul de clienți cu reședință/activitate în țările cu risc înalt (persoane fizice) Numărul de clienți cu reședință/activitate în țările cu risc înalt (persoane juridice) Numărul de clienți cu tranzacții transfrontaliere care implică țări cu risc înalt Numărul de clienți ocazionali Numărul de tranzacții ocazionale efectuate de clienți ocazionali Numărul de clienți asociați solicitărilor SPCSB, a căror materie sau natură a solicitării este legată de PCSBFT Numărul de clienți a căror activitate presupune lucrul intensiv cu mijloace bănești în numerar Numărul de clienți care își desfășoară activitatea și/sau efectuează tranzacții (operațiuni) în circumstanțe neobișnuite
Produce, Servicii și tranzacții	Conturi de plată	Numărul conturilor de plăți Numărul tranzacțiilor de intrare în conturi în anul precedent Valoarea totală a tranzacțiilor de intrare în conturi (MDL) în anul precedent Numărul tranzacțiilor de ieșire din conturi în anul precedent Valoarea totală a tranzacțiilor de ieșire din conturi (MDL) în anul precedent
	IBAN-uri virtuale (vIBAN)	Numărul total de conturi principale cu vIBANS conectate Numărul de tranzacții pe IBAN-uri virtuale (intrare) în anul precedent Valoarea totală (MDL) a tranzacțiilor pe IBAN-uri virtuale (intrare) în anul precedent Numărul de tranzacții pe IBAN-uri virtuale (ieșire) în anul precedent Valoarea totală (MDL) a tranzacțiilor efectuate pe IBAN-uri virtuale în anul precedent Numărul total de IBAN-uri reemise Numărul total de IBAN-uri reemise în cazul în care utilizatorul final nu este client al entității raportoare
	Carduri preplătite	Numărul total de carduri preplătite emise în anul precedent Valoarea totală (MDL) a cardurilor preplătite emise în cursul anului precedent Valoare totală (MDL) restantă pentru cardurile preplătite emise în anul precedent Numărul total de clienți care utilizează carduri preplătite Numărul total de clienți care utilizează carduri preplătite cu mai mult de 3 carduri preplătite
	Împrumuturi	Numărul total și valoarea (MDL) a împrumuturilor restante Numărul total și valoarea (MDL) a împrumuturilor acordate în cursul anului precedent Numărul total și valoarea (MDL) a creditelor garantate cu active în

		circulație cu garanții în numerar Numărul total și valoarea (MDL) a rambursărilor de împrumuturi din anul precedent Numărul total și valoarea (MDL) a împrumuturilor rambursate prematur în cursul anului precedent Numărul total și valoarea (MDL) a rambursărilor de împrumuturi din țări cu grad de risc sporit în cursul anului precedent Numărul total și valoarea (MDL) a creditelor de consum acordate în anul precedent care nu sunt asociate cu achiziționarea vreunui produs/serviciu
	Factorizare	Numărul total de contracte de factoring acordate în anul precedent Valoarea totală (MDL) a contractelor de factoring acordate în cursul anului precedent Valoarea totală (MDL) a contractelor de factoring acordate debitorilor stabiliți în țări cu grad de risc sporit în cursul anului precedent
	Contracte de asigurare de viață	Suma totală a primelor brute emise în anul precedent (încasate) Suma totală (în MDL) a valorii de răscumpărare a contractelor de asigurare la sfârșitul anului precedent % din totalul primelor brute subscrise (suma) plătite direct brokerului de asigurări de viață în anul precedent % din contracte (sumă) care nu sunt utilizate pentru contracte cu risc scăzut
	Schimb valutar (cu numerar)	Numărul de tranzacții de schimb valutar efectuate în cursul anului precedent (vânzare) Numărul de tranzacții de schimb valutar efectuate în cursul anului precedent (cumpărare) Numărul de tranzacții de schimb valutar efectuate în cursul anului precedent, în care tranzacția depășește 1000 de euro echivalent (vânzare) Numărul de tranzacții de schimb valutar efectuate în anul precedent, în care tranzacția depășește 1000 de euro echivalent (cumpărare) Valoarea totală (MDL) a tranzacțiilor de schimb valutar efectuate în cursul anului precedent (vânzare) Valoarea totală (MDL) a tranzacțiilor de schimb valutar efectuate în cursul anului precedent (cumpărare) Valoarea (MDL) a tranzacțiilor de schimb valutar numerar-numerar efectuate în cursul anului precedent
	Investiții, Servicii și Activități (recepționarea și transmiterea comenzilor)	Numărul de clienți cu amănuntul Numărul de clienți profesioniști % din valoarea ordinelor transmise care implică instrumente financiare nelistate, altele decât instrumente financiare emise de entitatea obligată sau de grupul acesteia Numărul de clienți reglementați în domeniul PCSBFT din țări cu grad de risc sporit

	Investiții, Servicii și activități (păstrarea unui cont de custodie)	Numărul de clienți cu amănuntul Numărul de clienți profesioniști % din activele aflate în custodie pentru care entitatea obligată nu are o relație comercială directă cu investitorul final Numărul de clienți reglementați în domeniul PCSBFT din țări cu grad de risc sporit
	Investiții, Servicii și Activități (Managementul portofoliului)	Numărul de clienți cu amănuntul Numărul de clienți profesioniști Total active aflate în administrare Numărul de clienți pentru care clientul deține active totale cu o valoare de cel puțin 5.000.000 EUR echivalent
	Remitere de bani	Numărul total de plăți prin remitere de bani în anul precedent (încasate) Numărul total de plăți prin remitere de bani în anul precedent (ieșite) Valoarea totală (MDL) a plăților remitențe din anul precedent (încasate) Valoarea totală (MDL) a plăților remitențe din anul precedent (ieșite) Numărul total de tranzacții de remitere de bani de peste 1000 de euro echivalent în anul precedent (intrare) Numărul total de tranzacții de remitere de bani de peste 1000 de euro echivalent în anul precedent (ieșire)
	Managementul Averii	Număr total de clienți cu active totale în administrare peste o valoare de cel puțin 5.000.000 EUR echivalent Numărul total de clienți care se încadrează în definiția serviciilor bancare private Număr total de clienți cu active totale peste o valoare de cel puțin 50.000.000 EUR echivalent
	Servicii de corespondență	Valoarea totală (MDL) a tranzacțiilor executate în numele clientului respondent în anul precedent (intrare) Valoarea totală (MDL) a tranzacțiilor executate în numele clientului respondent în anul precedent (ieșire) Valoarea totală (MDL) a tranzacțiilor efectuate prin conturi de plată (payable through accounts) în anul precedent (încasări) Valoarea totală (MDL) a tranzacțiilor efectuate prin conturi de plată în anul precedent (ieșiri) Valoarea totală (MDL) a tranzacțiilor efectuate prin conturi imbricate (nested accounts) în anul precedent (intrare) Valoarea totală (MDL) a tranzacțiilor efectuate prin conturi imbricate în anul precedent (ieșire)
	Finanțarea comerțului	Numărul total de clienți utilizatori de servicii de finanțare comercială Numărul total de tranzacții de finanțare a comerțului din anul precedent (intrare) Numărul total de tranzacții de finanțare a comerțului din anul precedent (ieșiri)

		Valoarea totală (MDL) a tranzacțiilor de finanțare comercială din anul precedent (intrare) Valoarea totală (MDL) a tranzacțiilor de finanțare comercială din anul precedent (ieșire)
	Bani electronici	Numărul de tranzacții cu monedă electronică din anul precedent (intrare) Numărul de tranzacții cu monedă electronică din anul precedent (ieșire) Valoarea totală (MDL) a tranzacțiilor cu monedă electronică din anul precedent (intrare) Valoarea totală (MDL) a tranzacțiilor cu monedă electronică din anul precedent (ieșire) Numărul total de tranzacții cu monedă electronică efectuate în anul precedent în condițiile aplicării derogărilor prevăzute de cadrul normativ aplicabil de la anumite măsuri de precauție privind clientela. Valoarea (în MDL) a tranzacțiilor cu monedă electronică efectuate în anul precedent în condițiile aplicării derogărilor prevăzute de cadrul normativ aplicabil de la anumite măsuri de precauție privind clientela.
	Servicii TCSP (Trust or Company Service Providers – Furnizori de Servicii pentru Fiducii și Societăți)	Numărul total de clienți persoane juridice care au utilizat servicii TCSP în anul precedent
	Administrarea OPCVM-urilor (UCITS - Undertakings for Collective Investment in Transferable Securities – Organisme de Plasament Colectiv în Valori Mobiliare)	Numărul de clienți investitori individuali Numărul de clienți investitori profesioniști Total active aflate în administrare Total active gestionate în instrumente financiare nelistate
	Administrarea FIA-urilor (AIF – Alternative Investments Funds – Fonduri Alternative de Investiții)	Numărul de fonduri deschise Numărul de fonduri închise Total active aflate în administrare Total active gestionate în instrumente financiare nelistate Active, altele decât instrumentele financiare, astfel cum sunt definite în secțiunea C a anexei 1 la Directiva UE 2014/65 privind piețele instrumentelor financiare
	Servicii de custodie în siguranță	Numărul total de clienți care utilizează casete de valori
	Finanțare colectivă	Valoarea totală (MDL) a proiectelor de finanțare din anul precedent Numărul total de proiecte finanțate în anul precedent Numărul total de donatori din țări cu risc ridicat Numărul total de proiecte în care proprietarul provine dintr-o țară cu risc ridicat Numărul total de proiecte finanțate în scopuri filantropice în anul precedent

	Tranzacții în numerar	Numărul de tranzacții în numerar din anul precedent (retrageri) Numărul de tranzacții în numerar din anul precedent (depozite) Valoarea totală (MDL) a tranzacțiilor în numerar din anul precedent (retrageri) Valoarea totală (MDL) a tranzacțiilor în numerar din anul precedent (depozite) Numărul total de persoane fizice tranzacții totale în numerar de peste 50.000 EUR echivalent în cursul anului precedent Numărul total de persoane juridice tranzacții totale în numerar de peste 500.000 EUR echivalent în cursul anului precedent
Zone Geografice		Numărul de tranzacții primite în anul precedent, în funcție de țară Valoarea totală (MDL) a tranzacțiilor primite în anul precedent, pe țări Numărul de tranzacții efectuate în anul precedent, în funcție de țară Valoarea totală (MDL) a tranzacțiilor efectuate în anul precedent, pe țări Valoarea totală (MDL) a investițiilor în organisme de plasament colectiv (OPC) ale entității, pe țări Numărul de investitori pe țări (pentru AMC-uri – Asset Management Companies (companii care gestionează active)) Valoarea totală a investițiilor (MDL) pe țări (pentru AMC-uri) Valoarea totală (MDL) a tuturor activelor pe țări (pentru FI - Investment Fund și AMC) Numărul de instituții înființate în țări străine cărora le furnizați servicii de corespondență (pe țări) Valoarea totală a fondurilor primite și transferate în numele clienților respondentului, în funcție de țara în care se află înființarea respondentului Valoarea totală a fondurilor de ieșire transferate în numele clienților respondentului, în funcție de țara de stabilire a respondentului Numărul de sucursale pe țări Numărul de filiale pe țări Țara în care se află proprietarul entității (compania-mamă)
Canale de distribuție		Numărul de clienți noi înscrși de la distanță în anul precedent Numărul de clienți noi înregistrați în anul precedent de către terți Numărul de clienți noi înregistrați în anul precedent de către terți care nu sunt supuși direct supravegherii PCSBFT Numărul de agenți pe țări Numărul de distribuitori pe țări Valoarea totală a primelor brute emise prin contracte de asigurare emise prin brokeri, defalcată în funcție de țara în care sunt stabiliți brokerii Numărul de parteneri de tip „white labeling (marcare albă)” în funcție de țara de înființare

Anexa nr. 2
Controale PCSBFT

Categorie	Subcategorie	Puncte de referință
Guvernanța PCSBFT	1. Rolul și responsabilitățile organului de conducere	Data (datele) la care a fost aprobată de conducere ultima versiune a politicilor și procedurilor ce vizează: - identificarea și verificarea inițială a identității clientului și beneficiarilor efectivi - identificarea și verificarea continuu a identității clientului și beneficiarilor efectivi - Monitorizarea tranzacțiilor - Raportarea tranzacțiilor suspecte - Verificarea continuu a relațiilor de afaceri - Verificarea sancțiunilor financiare
	2. Sisteme de control intern și raportare	Data la care rapoartele privind următoarele aspecte de PCSBFT au fost prezentate conducerii superioare în ultimul an calendaristic: - domeniile în care ar trebui implementate sau îmbunătățite controalele PCSBFT și îmbunătățirile recomandate; - acțiuni de monitorizare a conformității și un plan de activități ale responsabilului cu conformitatea PCSBFT; - un raport de progres al oricăror programe de remediere semnificative; - adecvarea resurselor umane și tehnice din cadrul funcției de conformitate PCSBFT; - principalele constatări ale evaluării riscurilor de SBFT la nivelul întregii companii; - modificări ale metodologiei de evaluare a profilurilor de risc ale clienților; - clasificarea clienților pe categorii de risc; - date statistice privind tranzacțiile neobișnuite și suspecte; - Constatările auditurilor interne și externe, după caz, legate de combaterea spălării banilor și a finanțării terorismului; Activități și plan de instruire în domeniul PCSBFT.
		Numărul de deficiențe restante la sfârșitul anului calendaristic? Din care: - numărul de deficiențe cu grad ridicată - numărul de deficiențe pentru care remedierea depășește termenul inițial cu mai mult de 6 luni - numărul de deficiențe critice pentru care remedierea depășește termenul inițial cu mai mult de 6 luni
	3. Externalizarea și dependența de terți	Sarcini externalizate de entitatea raportoare (în totalitate sau parțial) către furnizori de servicii: cunoașterea clientelei (CDD) - Instruiri - Monitorizarea tranzacțiilor

		- Rapoarte de tranzacții suspecte - Verificarea sancțiunilor - Detectarea PEP Verificări de monitorizare a conformității - % din sarcinile externalizate de combatere a spălării banilor și a finanțării terorismului care sunt acoperite de un acord scris care guvernează relația externalizată - Existența sarcinilor de combatere a spălării banilor și a finanțării terorismului (PCSBFT) externalizate către un furnizor extern de servicii situat într-o țară terță cu risc ridicat (excluzând externalizarea către alte entități ale grupului situate în țări terțe cu risc ridicat) - % din sarcinile externalizate de combatere a spălării banilor și a finanțării terorismului pentru care există un acord scris printre sarcinile externalizate către un furnizor extern de servicii situat într-o țară terță cu risc ridicat. - Existența sarcinilor PCSBFT externalizate către un furnizor extern de servicii situat într-o țară terță cu risc ridicat care face parte din grup - Există un acord scris pentru toate sarcinile externalizate către un furnizor extern de servicii situat într-o țară terță cu risc ridicat care face parte din grup
	4. Funcția și resursele de conformitate PCSBFT	- Numărul de personal dedicat conformității PCSBFT - Numărul de ofițeri de conformitate numiți în ultimii 5 ani sau de la autorizarea entității, dacă autorizația a fost acordată în urmă cu mai puțin de 5 ani
	5. Instruire PCSBFT (angajați, funcționari, agenți și distribuitori)	% din personalul care a beneficiat de instruire privind combaterea spălării banilor în ultimul an calendaristic: - Specialist PCSBFT - personal non-specializat în combaterea spălării banilor/finanțării terorismului (personal care interacționează cu clienții , directori executivi) - agenți și distribuitori Numărul mediu de ore de instruire PCSBFT în ultimul an calendaristic la care au participat (per persoană) : - Personal specializat PCSBFT - personal non-specializat în combaterea spălării banilor (inclusiv conducerea, prima linie de apărare) Membrii consiliului de administrație / directorii neexecutivi % din personal sau stagiaari pentru care cel puțin o instruire a fost validată printr-un test
	6. Funcția de audit intern / expert extern	Datele la care obligațiile/controalele PCSBFT au fost evaluate ultima dată de către un audit intern sau un expert extern: - Evaluarea riscurilor la nivelul întregii afaceri - determinarea profilului de risc SBFT al clienților aflați într-o relație de afaceri - Măsuri de conștientizare și de formare a personalului legate de combaterea spălării banilor și a finanțării terorismului

		- Proceduri de identificare și verificare a identității clienților - Politici și proceduri pentru monitorizarea și analiza relațiilor de afaceri, inclusiv monitorizarea tranzacțiilor - Politici și proceduri pentru raportarea tranzacțiilor suspecte - Politici și proceduri de păstrare a evidențelor - Resurse dedicate PCSBFT Organizarea sistemului PCSBFT, guvernanta și raportarea către organele de conducere.
Evaluarea riscurilor SBFT	1. Evaluarea riscurilor la nivelul entității raportoare	- Data la care entitatea raportoare a evaluat ultima dată necesitatea actualizării Raportului de evaluare a riscului de SBFT - Conducerea superioară a aprobat ultima versiune a Raportului de evaluare a riscului de SBFT - Frecvența cu care entitatea raportoare evaluează necesitatea revizuirii Raportului de evaluare a riscului de SBFT
	2. Evaluarea și clasificarea riscurilor de ML/TF ale clienților	- Data la care entitatea raportoare a evaluat ultima dată necesitatea actualizării riscurilor de SBFT ale clienților - Numărul de clienți per categorie de risc SBFT (risc scăzut, risc mediu-scăzut, risc mediu-ridicat, risc ridicat)
Politici și proceduri PCSBFT	1. Cunoașterea clienților	- Numărul de clienți care sunt entități juridice/trusturi ai căror beneficiari efectivi nu au fost identificați - Numărul de clienți cu risc ridicat care sunt persoane juridice - Numărul de clienți cu risc ridicat care sunt entități juridice/trusturi al căror beneficiar efectiv a fost identificat, dar a căror identitate nu a fost verificată - Numărul de clienți fără documente/informații de identificare și verificare - Numărul de clienți cu documentație/informații incomplete de identificare și verificare - Numărul de clienți cu risc ridicat ale căror date sau informații privind diligența de verificare a clientului lipsesc sau sunt incomplete - Numărul de clienți fără profil de risc de SBFT (excluzând clienții cu care entitatea raportoare nu are o relație de afaceri) - Numărul de clienți pentru care nu s-au obținut informații privind scopul și natura preconizată a relației de afaceri (excluzând clienții cu care entitatea raportoare nu are o relație de afaceri) - Numărul de clienți pentru care nu s-au obținut informații privind natura activității clienților sau privind angajarea sau ocupația acestora (cu excepția clienților cu care entitatea raportoare nu are o relație de afaceri) - Numărul de clienți (excluzând persoanele fizice) pentru care datele de identificare ale beneficiarului efectiv sunt introduse în baza de date a instituției - Numărul de clienți, persoane fizice, pentru care toate datele de identificare (nume/data nașterii, naționalitate, cod fiscal) sunt introduse în baza de date a instituției
	2. Monitorizarea continuă a relațiilor de afaceri	- Numărul de clienți pentru care au fost necesare actualizări ale informațiilor despre clienți în ultimul an calendaristic, în conformitate cu politicile și procedurile entității raportoare - Numărul de clienți pentru care informațiile despre clienți au fost revizuite și actualizate în ultimul an calendaristic

	3. Monitorizarea tranzacțiilor	Entitatea obligată are implementat un sistem de monitorizare a tranzacțiilor Sistemul de monitorizare a tranzacțiilor : - Nu este automatizat; sau - Cel puțin parțial automatizat În cazul sistemului manual: numărul anual de tranzacții depășește numărul de tranzacții pe care entitatea raportoare le poate procesa manual Dacă sistemul este manual: Timpul mediu în zile pentru analiza tranzacției din momentul în care aceasta a avut loc Dacă sistemul este automatizat: Sistemul poate genera alerte în cazul unor neconcordanțe între informațiile prezentate de client referitoare la acesta și următoarele elemente: - Numărul de tranzacții - Valoarea tranzacțiilor agregate - valoarea tranzacțiilor individuale - contrapărți - țări În cazul sistemului automatizat: Numărul de alerte neanalizate la sfârșitul anului calendaristic În cazul unui sistem automatizat: Timpul mediu necesar pentru analizarea unei alerte în ultimul an calendaristic (numărul de zile dintre emiterea alertei și închiderea acesteia) În cazul unui sistem automatizat: Raportul dintre numărul de alerte și numărul de STRs
	4. Raportarea tranzacțiilor și activităților suspecte (STR și SAR)	Numărul mediu de zile dintre data identificării tranzacțiilor potențial suspecte (înainte de analiza tranzacției) și data la care tranzacția este raportată către SPCSB (după analiza tranzacției) în ultimul an calendaristic Numărul de STR-uri transmise către SPCSB înainte de finalizarea tranzacției în ultimul an calendaristic Numărul total de STR-uri transmise către SPCSB în ultimul an calendaristic
	5. Sancțiuni financiare specifice	Numărul mediu de ore dintre publicarea Sancțiunilor financiare ținute (TFS) de către autorități și implementarea acestor modificări în instrumentele de screening ale entității Numărul conincidențelor pozitive în raport cu cele fals pozitive identificate Valoarea mijloacelor bănești /activelor blocate (MDL)
	6. Respectarea cadrului normativ aplicabil transferurilor de fonduri	- Numărul de transferuri de ieșire pentru care s-au primit solicitări de la o contraparte din lanțul de transfer pentru informații lipsă, incomplete sau furnizate folosind caractere inadmisibile în ultimul an calendaristic - Numărul total de transferuri de ieșire în ultimul an calendaristic - % din transferurile de ieșire respinse sau returnate de contraparte din lanțul de transfer din cauza informațiilor lipsă, incomplete sau furnizate folosind caractere inadmisibile în ultimul an calendaristic - Numărul de contrapărți care au intrat în dificultate în mod repetat și au fost semnalate autorității de supraveghere în ultimul an calendaristic

		- Numărul total de contrapărți ale transferurilor de ieșire și de intrare în ultimul an calendaristic
	7. Păstrarea înregistrărilor	Numărul dosarelor/tranzacțiilor identificate pentru care nu s-a asigurat păstrarea datelor complete
Supravegherea grupului	Conformitatea PCSBFT a grupului	Numărul de deficiențe identificate de către supraveghetorii din cadrul grupului în domeniul PCSBFT în ultimul an calendaristic, asociat: - Cunoașterii clienților, inclusiv monitorizarea activităților/tranzacțiilor acestora; - Evaluarea riscurilor de SBFT; - păstrarea datelor; - Raportarea tranzacțiilor suspecte; - eficiența sistemului de control intern;

Anexa nr. 3

Evaluarea riscului de spălare a banilor și finanțarea a terorismului în cadrul entității prin metoda cantitativă

Entitatea raportoare ia în considerare la identificarea și evaluarea riscului de spălare a banilor și finanțare a terorismului mai mulți factori de risc relevanți activități care sunt asociați tipul clienților deserviți, produsele oferite sau jurisdicțiile și canalele de distribuție utilizate.

	Scăzut	Mediu	Sporit
1.	Clienți stabili cu o relație de afacere mai mare de 3 ani.	Clienți a căror relație de afacere este nestabilă și în schimbare, cu o durată mai mare de 1 an și mai mică de 3 ani.	Clienți noi - o relație de afacere mai mică de 1 an.
2.	Clienți rezidenți.	Clienți rezidenți noi cu o relație de afacere mai mică de 1 an.	Clienți nerezidenți.
3.	Clienți la care se cunoaște beneficiarul efectiv.	Clienți la care se cunoaște fondatorul, dar nu și beneficiarul efectiv.	Clienți la care nu se cunoaște beneficiarul efectiv sau există suspiciunea că aceștia sunt deținători nominali.
4.	Clienți care nu beneficiază de produse și servicii electronice sau e-banking (ca exemplu, transferuri între conturi, plata serviciilor comunale sau deschiderea conturilor prin internet).	Clienți care beneficiază de servicii electronice sau e-banking, dar efectuează rar operațiuni prin intermediul acestora.	Clienți care beneficiază de servicii electronice sau e-banking și efectuează permanent operațiuni prin intermediul acestora.
5.	Clienți care efectuează un număr și volum limitat (< 200 mii lei/lună) de tranzacții în numerar.	Clienți care efectuează un număr și volum moderat (> 200 mii lei/lună și < 500 mii lei/lună) de tranzacții în numerar.	Clienți care efectuează un număr și volum mare (> 500 mii lei/lună) de tranzacții în numerar.

6.	Clienți care efectuează un număr și volum limitat (< 500 mii lei/lună) de tranzacții prin virament.	Clienți care efectuează un număr și volum moderat (> 500 mii lei/lună și < 1 mil. lei/lună) de tranzacții prin virament.	Clienți care efectuează un număr și volum mare (> 1 mil. lei/lună) de tranzacții prin virament.
7.	Clienți a căror activitate nu se caracterizează printr-un grad de risc sporit.	Clienți a căror activitate nu se caracterizează printr-un grad de risc sporit, dar sunt în relație de afaceri de o perioadă mai mică de un an.	Clienți a căror activitate se caracterizează printr-un grad de risc sporit (clienți care efectuează transferuri în zone off-shore sau alte zone cu grad de risc sporit, clienți care nu prezintă documente confirmative, etc.).
8.	Entitatea are relații corespondente cu instituții rezidente. Relația de afaceri dintre acestea durează o perioadă mai mare de 5 ani.	Entitatea are relații corespondente cu instituții rezidente. Relația de afaceri dintre acestea durează de o perioadă mai mică de 5 ani.	Entitatea are relații corespondente cu instituții nerezidente.
9.	Clienți care remit sau primesc un număr și volum limitat (persoane fizice < 10 mii lei/lună; persoane juridice < 500 mii lei/lună) de mijloace bănești în/din străinătate.	Clienți care remit sau primesc un număr și volum moderat (persoane fizice > 10 mii lei/lună și < 20 mii lei/lună; persoane juridice > 500 mii lei/lună și < 3 mil. lei/lună) de mijloace bănești în/din străinătate.	Clienți care remit sau primesc un număr și volum mare (persoane fizice > 20 mii lei/lună; persoane juridice > 3 mil. lei/lună) de mijloace bănești în/din străinătate.
10.	Entitatea raportează un număr și volum limitat (< 1 mil. lei/lună) de tranzacții suspecte către Serviciul Prevenirea și Combaterea Spălării Banilor.	Entitatea raportează un număr și volum moderat (> 1 mil. lei/lună și < 3 mil. lei/lună) de tranzacții suspecte către Serviciul Prevenirea și Combaterea Spălării Banilor.	Entitatea raportează un număr și volum mare (> 3 mil. lei/lună) de tranzacții suspecte către Serviciul Prevenirea și Combaterea Spălării Banilor.
11.	Entitatea nu raportează către Serviciul Prevenirea și Combaterea Spălării Banilor tranzacții suspecte de finanțarea terorismului.	Entitatea raportează un număr limitat (< 5 tranzacții/ trimestru) de tranzacții suspecte de finanțarea terorismului către Serviciul Prevenirea și Combaterea Spălării Banilor.	Entitatea raportează un număr mare (> 5 tranzacții/ trimestru) de tranzacții suspecte de finanțarea terorismului către Serviciul Prevenirea și Combaterea Spălării Banilor.
12.	Clienții entității care nu efectuează tranzacții cu clienții așa numitelor „bănci” din zona transnistreană.	Clienții entității efectuează tranzacții în număr și volum limitat (< 500 mii lei/lună) cu clienții așa numitelor „bănci” din zona transnistreană.	Clienții entității efectuează tranzacții în număr și volum mare (> 500 mii lei/lună) cu clienții așa numitelor „bănci” din zona transnistreană.
13.	Clienții care efectuează tranzacții și față de care entitatea nu aplică măsuri de precauție sporită.	Clienții care efectuează tranzacții și față de care entitatea aplică un număr limitat (maxim 3 măsuri) de măsuri de precauție sporită.	Clienții care efectuează tranzacții și față de care entitatea aplică toate măsuri de precauție sporită.
14.	Politicile entității în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului au fost actualizate pe parcursul anului.	Există proiect de modificare a politicilor entității în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului în scopul actualizării acestora pe parcursul anului.	Politicile entității în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului nu au fost actualizate pe parcursul anului.

15.	Entitatea deține un sistem de monitorizare și raportare comprehensivă pentru toți clienții, inclusiv ale sucursalelor, diviziuni și sucursale separate.	Entitatea deține un sistem de monitorizare și raportare comprehensivă pentru toți clienții, dar nu acoperă toate sucursalele, diviziunile, acestea efectuează monitorizarea și raportează către entitate separat.	Entitatea nu deține un sistem robust de monitorizare și raportare, dar se bazează pe verificări manuale și raportări ocazionale de la sucursalele și diviziunile individuale.
16	Pe parcursul anului au fost organizate mai mult de 6 seminare pentru instruirea angajaților în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. Programul de instruire nu include și membrii de conducere a entității.	Pe parcursul anului au fost organizate 3 seminare pentru instruirea angajaților în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. Programul de instruire include doar membrii de conducere a entității cu atribuții în domeniul de p.c.s.b.f.t.	Pe parcursul anului au fost organizate mai puțin de 3 seminare pentru instruirea angajaților în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. Programul de instruire include toți membrii de conducere a entității.
17.	Angajații responsabili de întreprinderea acțiunilor de prevenire și combatere a spălării banilor și finanțării terorismului au experiență în domeniu mai mare de 5 ani.	Angajații responsabili de întreprinderea acțiunilor de prevenire și combatere a spălării banilor și finanțării terorismului au experiență mică în domeniu.	Angajații responsabili de întreprinderea acțiunilor de prevenire și combatere a spălării banilor și finanțării terorismului au experiență în domeniu mai mică de 2 ani.
18.	Pe parcursul anului în rezultatul controalelor efectuate de auditul intern nu a constat deficiențe sau deficiențele constatate sunt minore aferent conformării programului intern de p.c.s.b.f.t. și cerințelor legale de domeniu	Pe parcursul anului în rezultatul controalelor efectuate de auditul intern au fost constatate unele deficiențe de neconformare cu cerințele programului intern de p.c.s.b.f.t. și cerințelor legale de domeniu. Aceste au fost comunicate conducerii și au fost întreprinse măsuri de rigoare în vederea diminuării riscurilor constatate.	Pe parcursul anului în rezultatul controalelor efectuate de auditul intern au fost constatate mai multe deficiențe de neconformare cu cerințele programului intern de p.c.s.b.f.t. și cerințelor legale de domeniu. Aceste au fost comunicate conducerii și au fost întreprinse măsuri de rigoare în vederea diminuării riscurilor constatate.
19.	Pe parcursul anului nu au fost date recomandări pentru îmbunătățirea activității, precum și nu au fost aplicate sancțiuni de către organele de supraveghere în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.	Pe parcursul anului a fost recomandat de către organele de supraveghere în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului îmbunătățirea activității băncii în acest domeniu.	Pe parcursul anului au fost aplicate sancțiuni de către organele de supraveghere în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.
n.	...	...	...

Descrierea tabelului:

Tabelul propus poate înlesni procesul de evaluare a riscurilor, prin calcularea unui coeficient pentru fiecare celulă determinând în acest sens ponderea fiecărui factor enumerat (entitatea poate determina un număr nelimitat de „n” factori pentru a-i lua în considerare în cadrul evaluării riscurilor). Această pondere poate fi înregistrată ca și coeficient sau procent, iar important este ca suma pentru fiecare câmp/rând să fie egală cu 1 sau respectiv 100%. În final, se calculează, utilizând media aritmetică / geometrică,

coeficientul în fiecare coloană sau risc atribuit, iar ca urmare valoarea maximă obținută va indica un reper aferent ponderii majore a riscului de spălare a banilor și finanțare a terorismului în entitate. Un exemplu, care cuprinde 3 factori determinați pentru evaluarea riscului de spălare a banilor și finanțare a terorismului, poate fi vizualizat mai jos:

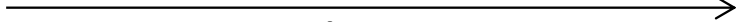
	Risc scăzut	Risc mediu	Risc sporit
1	30%	45%	25%
2	17%	80%	3%
3	80%	8%	12%
Total	42,3%	44,3%	13.3%

În baza datelor din tabel, concluzionăm că entitatea este expusă unui risc mediu de spălare a banilor și finanțare a terorismului.

Anexa nr. 4

Evaluarea riscului de spălare a banilor și finanțarea a terorismului în cadrul entității prin metoda calitativă

Entitatea raportoare utilizează la identificarea și evaluarea riscului de spălare a banilor și finanțare a terorismului o matrice de risc, care reflectă probabilitatea de apariție a riscului și impactul acestuia, determinat în corespundere de factorii de risc relevanți activității, având în vedere tipul clienților deserviți, produsele oferite sau jurisdicțiile și canalele de distribuție utilizate.

Probabilitatea 	Foarte probabil	Mediu 2	Sporit 3	Extrem 5
	Probabil	Scăzut 1	Mediu 2	Sporit 3
	Puțin probabil	Scăzut 1	Scăzut 1	Mediu 2
		Minor	Moderat	Major
		Impact 		

Descrierea tabelului:

După identificarea factorilor de risc și prin utilizarea matricei de mai sus poate fi calculat nivelul riscului de spălare a banilor și finanțare a terorismului (Probabilitatea x impact = nivelul riscului). Gradul probabilității se referă la riscurile potențiale de spălare a banilor și finanțare a terorismului care pot să apară în activitatea entității și pot fi definite într-un număr necesar pentru evaluarea adecvată a riscurilor. Cu toate că modelul ilustrat evidențiază 3 nivele ale probabilității (foarte probabil, probabil și puțin probabil), fiecare entității își poate defini un număr diferit de nivele ale probabilității riscurilor adaptat la activitatea acesteia (ca exemplu, un alt model poate fi: nu se aplică, se aplică rar, puțin probabil, probabil, probabilitate înaltă și garantat).

Descrierea celor 3 nivele de probabilitate utilizate este următoarea:

- a) foarte probabil - riscul are o probabilitate înaltă de a se materializa pe baza experiențelor anterioare și probabil va apărea de câteva ori pe an;
- b) probabil - riscul se poate materializa pe baza experiențelor anterioare și are probabilitate că va apărea o dată pe an;
- c) puțin probabil - riscul este puțin probabil să se materializeze pe baza experiențelor anterioare.

În condiții similare entitatea poate defini și gradul impactului asupra activității sale. Modelul ilustrat evidențiază 3 nivele ale impactului (major, moderat și minor), însă fiecare entitate își poate defini un număr diferit de nivele ale impactului riscurilor adaptat la activitatea sa (ca exemplu, un alt model poate fi: nu se aplică, se aplică nesemnificativ, scăzut, moderat, sporit și extrem).

Este esențial de evidențiat faptul că gradul impactului se referă la consecințele pierderilor apărute și ale gravității prejudiciilor rezultate în cazul dacă riscurile se materializează. Acestea se pot materializa în funcție de activitatea fiecărei entități și pot fi evidențiate prin riscul actual de pierderi, riscul reputațional, riscul cauzării de daune, riscul de sancționare etc.

Descrierea celor 3 nivele ale impactului utilizat este următoarea:

- a) major – evenimentul ar avea consecințe serioase prin cauzarea de pierderi majore sau ar influența acte teroriste grave și spălare de bani;
- b) moderat – evenimentul ar avea un impact moderat și consecințe medii asupra activității;
- c) minor – evenimentul ar avea un impact nesemnificativ sau redus asupra activității.

Caracterizarea riscurilor probabile ilustrate în matricea din tabelul de mai sus este următoarea:

- a) extrem (5) – este sigur că riscul se va materializa și va avea consecințe foarte grave pentru activitatea entității, cum ar fi: sancțiuni foarte mari din partea organului de supraveghere, pierderea clienților, pierderea personalului, pierderi financiare mari și un impact major asupra activității entității;
- b) sporit (3) – există probabilitate ridicată ca riscul să se materializeze și să aibă consecințe majore pentru activitatea entității, cum ar fi: sancțiuni mari din partea organului de supraveghere, pierderea un număr însemnat de clienți, pierderea

- personalului care dețin funcții cheie, pierderi financiare majore și un impact semnificativ asupra activității entității;
- c) mediu (2) – există probabilitate redusă ca riscul să se materializeze având consecințe nesemnificative asupra activității entității, cum ar fi: sancțiuni mici (de exemplu, atenționare/ prescripție dată entității sau administratorului; prescripție publică dată entității) din partea organului de supraveghere, pierderea unui număr neînsemnat de clienți și personal cheie, pierderi financiare neînsemnate;
- d) scăzut (1) – în cazul materializării riscului dat nu există temeri semnificative privind activitatea entității.

În baza celor menționate, evaluarea riscului de spălare a banilor și finanțare a terorismului în entitate poate fi efectuată utilizând exemplul de mai jos:

Grup de risc/factorii:	Clienți/Servicii		
	Probabilitatea	Impactul	Nivelul riscului
Clienți noi	Probabil	Moderat	2
Clienți care efectuează operațiuni semnificative în numerar	Probabil	Major	3
Clienți care efectuează operațiuni semnificative în virament	Foarte Probabil	Major	5
Clienți ONG	Probabil	Major	3
Clienți care nu beneficiază de servicii e-banking	Probabil	Minor	1
Servicii de administrare a activelor	Probabil	Major	3
Clienți - instituții corespondente cu relații de afaceri mai mare de 5 ani	Probabil	Minor	1
n	...	...	...
Risc total (calcularea mediei geometrice asupra factorilor și riscurilor potențiale)			2

Anexa nr. 2
la Hotărârea Comitetului Executiv
al Băncii Naționale a Moldovei
nr.din

RECOMANDĂRI

cu privire la monitorizarea tranzacțiilor și activităților clienților în vederea prevenirii și combaterii spălării banilor și finanțării terorismului

I. Prevederi generale

1. Recomandările cu privire la monitorizarea tranzacțiilor și activităților clienților în vederea prevenirii și combaterii spălării banilor și finanțării terorismului (în continuare – Recomandări) au ca scop de a oferi entităților rapoarte supravegheate de Banca Națională a Moldovei (în continuare - entități) îndrumări metodologice în procesul creării unor politici, proceduri și mecanisme interne eficiente privind monitorizarea tranzacțiilor și relațiilor de afaceri cu clienții, determinarea scopului și naturii relației de afaceri cu aceștia, interpretarea caracterului ordinar al activității clienților, precum și monitorizarea tranzacțiilor complexe pentru prevenirea și combaterea spălării banilor și finanțării terorismului.

2. Recomandările, de asemenea, sunt elaborate pentru a exemplifica modul în care entitatea își poate organiza sistemul de control intern pentru a instrui angajații, a organiza procesul de auditare independent, a cunoaște angajații săi, dar și pentru a investiga și raporta activitățile și tranzacțiile suspecte de spălare a banilor și finanțare a terorismului.

3. Recomandările sunt elaborate ținând cont de Recomandările 40 ale Grupului de Acțiune Financiară Internațională (FATF-GAFI), documentele Grupului Wolfsberg aferente monitorizării tranzacțiilor și alte documente internaționale aferente domeniului dat.

4. Termenii și expresiile utilizate în prezentele Recomandări au semnificațiile prevăzute în Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și actele normative subordonate acestei legi emise de către Banca Națională a Moldovei și Serviciul Prevenirea și Combaterea Spălării Banilor. De asemenea, în sensul prezentelor Recomandări se utilizează următorii termeni și expresii:

verificarea plăților în timp real – procesul de analiză și determinare a caracterului plăților înaintea executării lor, pentru prevenirea efectuării acestora cu încălcarea sancțiunilor, interdicțiilor sau altor restricții aplicate în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

verificarea clientului – verificarea identității clientului și a beneficiarului efectiv al acestuia (numele persoanei fizice/denumirea persoanei juridice și alte date referitoare la client și beneficiarul efectiv) în baze de date publice sau private (Registrul de stat al persoanelor juridice sau, după caz, într-un alt registru public sau privat, sau altă sursă sigură și independentă, de exemplu; referința birourilor/agențiilor istoriei de credit), precum și în listele publicate în Monitorul Oficial sau furnizate de autoritățile competente cu privire la persoanele sau entitățile implicate în activități teroriste, extremiste, de proliferare a armelor de distrugere în masă, de finanțare a acestora sau alte activități ilicite în privința

căroră sînt aplicate sancțiuni financiare specifice, interdicții sau alte restricții în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

monitorizare a tranzacțiilor – procesul de verificare automată, manuală sau mixtă a tranzacțiilor executate, cu scopul determinării caracterului ordinar sau neordinar al acestora. Procesul este aplicat atît unei singure tranzacții cît și unui lanț de tranzacții, iar în cazul în care tranzacția neordinară este suspectă, aceasta urmează a fi raportată Serviciului Prevenire și Combaterea Spălării Banilor (în continuare SPCSB) conform legislației;

5. Sistemul entității de monitorizare a tranzacțiilor și determinare a tranzacțiilor complexe, neordinare și suspecte va asigura identificarea, evaluarea și minimizarea riscurilor și vulnerabilităților aferente activității de prevenire și combatere a spălării banilor și finanțării terorismului.

II. Monitorizarea tranzacțiilor și a relațiilor de afaceri

6. Procesele și soluțiile informatice ale entității se recomandă să permită identificarea tranzacțiilor, modelelor de tranzacții și activitățile complexe și neordinare. Deoarece acestea nu vor fi suspecte în toate cazurile, entitatea analizează tranzacțiile, modelele acestora și activitățile pentru a determina caracterul ordinar sau suspect al acestora. Prin urmare, monitorizarea activităților și tranzacțiilor este o măsură continuă aplicată în vederea asigurării îndeplinirii cerințelor de prevenire și combatere a spălării banilor și finanțării terorismului.

7. Scopul monitorizării tranzacțiilor este alertarea entității asupra activităților care sunt neordinare sau potențial suspecte și necesită examinare suplimentară. În consecință aplicarea metodelor de verificare a plăților în timp real și monitorizarea tranzacțiilor va susține efortul entității în acest sens.

8. Politicile și procedurile interne ale entității se recomandă să cuprindă o listă de criterii și indici de suspiciune sau „semnale de avertismente”, care vor asista personalul implicat în activitățile de monitorizare a tranzacțiilor și clienților la identificarea suspiciunilor de spălare a banilor și finanțării terorismului. Entitatea, la elaborarea acestei liste, poate utiliza la fel lista suplimentară a „semnalelor de avertismente” referitoare la spălarea banilor și finanțarea terorismului înscrise în Anexă.

9. Un sistem de monitorizare a tranzacțiilor este eficient atunci când entitatea elaborează și pune în aplicare la diferite nivele monitorizarea activităților în dependență de factorii de risc implicați, cum ar fi: activitățile și operațiunile efectuate de în cadrul subdiviziunilor, baza de date a clienților și localitatea unde operează sau canalele de distribuție utilizate, etc.

10. Profilul de risc poate fi diferit în dependență de activitățile propuse, produsele sau serviciile oferite. Aplicarea monitorizării tranzacțiilor în dependență de profilul de risc implicat trebuie să reflecte riscurile asociate în ariile specifice și să conducă la micșorarea acestora.

11. Componentele principale în cadrul unui sistem eficient de monitorizare a tranzacțiilor sunt:

- a) verificarea ex-ante a clienților și verificări pre-tranzacție;
- b) verificarea clienților și verificarea tranzacțiilor în timp real;

c) analiza continuă a tranzacțiilor efectuate pentru a constata activitățile și tranzacțiile neordinare și suspecte sau revizuri post-tranzacție.

12. Entitățile raportoare care nu dispun de acces integral la informațiile și datele cu privire la tranzacțiile ori activitatea clientului vor lua în considerare neprocesarea tranzacțiilor respective sau în cazul în care dețin un acces limitat la acestea, inclusiv în cazul în care volumul, complexitatea ori viteza de derulare a tranzacțiilor nu justifică utilizarea unor sisteme automatizate sau mixte de monitorizare, pot aplica proceduri manuale de monitorizare și control, cu condiția ca acestea să fie proporționale și adecvate politicilor interne, modelului de afaceri și profilului de risc al entității. Acestea vor include revizuri periodice, verificări ale documentelor tranzacționale și după caz, verificări pre-tranzacție în vederea detectării tranzacțiilor și activităților neordinare sau suspecte.

Verificarea clienților și tranzacțiilor în timp real presupune examinarea ordinelor de plată sau solicitărilor de efectuare a plăților parvenite înaintea executării lor, avînd ca scop identificarea persoanelor implicate în activități teroriste sau asupra cărora sunt aplicate sancțiuni, interdicții sau alte restricții în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. Această activitate urmează a fi aplicată atît înaintea începerii relației de afaceri cît și pe parcursul derulării relației de afaceri. Sistemul de monitorizare a entității raportoare va permite analiza continuă a tranzacțiilor, iar revizuirile post-tranzacție sunt efectuate în vederea investigării tranzacțiilor realizate în scopul identificării unor tranzacții sau activități neordinare sau suspecte.

13. Pentru îmbunătățirea calității verificării tranzacțiilor este necesară respectarea următoarelor:

a) utilizarea listelor persoanelor implicate în activități teroriste, de proliferare a armelor de distrugere în masă, a persoanelor asupra cărora au fost aplicate sancțiuni, interdicții sau alte restricții;

b) aplicarea măsurilor de verificare în momentul inițierii unei plăți sau pe parcursul derulării relației de afaceri, în cazul reînnoirii listei publicate sau furnizate imediat sau în decurs de 1 zi lucrătoare din data actualizării listei;

c) în calitate de intermediar al tranzacțiilor efectuate, prestatorul plătitor asigură verificarea în timp real a informației despre emitentul ordinului de plată sau inițiatorul plății și beneficiarul acestuia;

d) pentru a minimiza numărul mare de „rezultate pozitive false”¹ și în vederea maximizării eficacității și eficienței operaționale, este esențial preluarea din listele menționate la lit.a) a informațiilor relevante, precum ar fi: numele complet al persoanei fizice, data de naștere, alți indici unici de identificare;

e) revizuirea și actualizarea periodică a informațiilor și datelor cu privire la client și tranzacțiile acestuia, în funcție de modificările operate în listele menționate la lit. a), precum și asigurarea unei actualizări automatizate a datelor cu privire la client în funcție de profilul de risc atribuit acestuia.¹⁴ În scopul identificării persoanelor implicate în

¹ Rezultat pozitiv fals - este o eroare în raportarea datelor în care un rezultat al testului indică în mod incorect prezența unei condiții. În cazul de față este vorba despre identificarea în cadrul unei plăți a potrivirii numelui persoanei fizice/denumirii persoanei juridice care efectuează plata sau în/din adresa căreia se efectuează plata cu cei din lista persoanelor desemnate.

activități teroriste sau de proliferare a armelor de distrugere în masă sau asupra cărora sunt aplicate sancțiuni, interdicții sau alte restricții, entitatea poate utiliza suplimentar următoarele surse de date și informații:

- a) Lista consolidată Consiliului de Securitate al Organizației Națiunilor Unite cu privire la persoanele, grupurile și entitățile implicate în activități teroriste;
- b) Lista Consiliului de Securitate al Organizației Națiunilor Unite cu privire la persoanele, grupurile și entitățile implicate în activități de proliferare a armelor de distrugere în masă
- c) Lista Uniunii Europene cu privire la persoanele, grupurile și entitățile implicate în activități teroriste;
- d) Lista suplimentară a Serviciului de Informații și Securitate cu privire la persoanele, grupurile și entitățile implicate în activități teroriste;
- d) Lista consolidată a Oficiului de Control al Activelor Străine din cadrul Departamentului Trezoreriei de Stat al SUA (OFAC) privind sancțiunile financiare aplicate persoanelor, grupurilor de persoane și entităților;
- e) Informațiile și rapoartele emise de organizația non profit - Proiectul Wisconsin privind controlul armelor nucleare;
- f) Alte informații și rapoarte difuzate de organizațiile internaționale specializate (FATF-GAFI, Wolfsberg, OCDE, etc);
- g) informații remise de autoritățile de supraveghere în vederea respectării de către entitățile raportoare a cerințelor de aplicare a sancțiunilor financiare specifice în conformitate cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.

15. Procesul de monitorizare a tranzacțiilor descris în reglementările interne ale entității cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului urmează să fie corelate cu riscurile modelului de afacere a entității, produsele și serviciile furnizate și natura clientelei deservite.

16. Entitatea utilizează abordarea bazată pe risc a clientelei la efectuarea monitorizării tranzacțiilor acestora. Astfel, procesul dat trebuie să reflecte evaluarea riscului în entitate pe sfere de activitate, produse și servicii oferite, iar atenția sporită se va oferi activității, tranzacției și/sau clientului ce implică un grad de risc sporit.

17. Monitorizarea eficientă a tranzacțiilor și activităților presupune existența:

- a) unui sistem automatizat de monitorizare a tranzacțiilor, inclusiv verificarea restricțiilor și sancțiunilor financiare specifice aplicate;
- b) unui sistem de generare a alertelor în caz de neconcordanță între date;
- c) procedeele care descriu activitatea de monitorizare;
- d) procedurilor de revizuire și stabilire periodică a limitelor;
- e) procedurilor de revizuire determinate de anumite evenimente, cum ar fi, aprobarea unor noi tipologii și metode de spălare a banilor și finanțare a terorismului, în baza informației parvenită din partea autorităților competente.

18. Efectuarea unei monitorizări eficiente a tranzacțiilor necesită automatizarea parțială sau integrală a procesului de monitorizare. Gradul automatizării poate varia de la o entitate la alta și va depinde de mărimea, natura și complexitatea activității acesteia. Sistemele automatizate de monitorizare bazate pe reguli sunt capabile să identifice

activități neordinare datorită setării corespunzătoare a diferitor parametri determinați de entitate. Aceste reguli pot fi individualizate clienților treptat în dependență de modificările în activitatea entității și a metodelor de spălare a banilor și finanțare a terorismului.

19. Entitatea poate utiliza sisteme TI inteligente pentru a actualiza profilul clientului în dependență de tranzacțiile efectuate. Acestea pot identifica modele de tranzacții prin examinarea corespondenței între conturi sau plăți, compara activitatea de tranzacționare cu metodele stabilite de spălare a banilor și finanțare a terorismului și stabili ratingul tranzacțiilor în dependență de nivelul suspiciunii.

20. În scopul facilitării identificării „semnalelor de avertisment” și a tranzacțiilor suspecte, la utilizarea anumitor limite valorice ale tranzacțiilor stabilite pentru soluțiile automatizate, entitățile pot seta următoarele limite:

- a) tranzacții efectuate în numerar și prin virament în sume de până la 200 mii lei;
- b) tranzacții efectuate în numerar și prin virament în sume de la 200 mii lei până la 500 mii lei;
- c) tranzacții efectuate în numerar și prin virament în sume de la 500 mii lei până la 1 mil. lei;
- d) tranzacții efectuate în numerar și prin virament în sume mai mari de 1 mil. lei.

21. Entitatea identifică expunerea la risc pentru operațiunile și activitățile supuse unui risc de spălare a banilor și finanțare a terorismului și determină relevanța și aplicabilitatea sistemului său pentru micșorarea riscului implicat. Sistemul automatizat de monitorizare a tranzacțiilor poate suplimenta dar nu și schimba lucrul și raționamentele angajaților la detectarea activităților neordinare sau suspecte. Prin urmare, entitatea trebuie să se asigure că implementarea unui astfel de sistem nu va conduce la micșorarea responsabilității angajaților aferent identificării activităților de spălare de bani și finanțare a terorismului.

22. Sistemul automatizat de monitorizare a tranzacțiilor bazat pe risc în cadrul entității este necesar să asigure cel puțin următoarele:

- a) compararea tranzacțiilor clienților sau a conturilor utilizate într-o anumită perioadă de timp cu tranzacțiile similare efectuate anterior în cadrul entității care sunt considerate rezonabile și adecvate;
- b) compararea datelor clienților sau a unor tranzacții specifice cu modelele de stabilire a ratingului riscului;
- c) emiterea alertelor în cazul identificării tranzacțiilor complexe, neordinare și/sau suspecte;
- d) înregistrarea alertelor corespunzătoare, pentru a fi gestionate adecvat în cadrul monitorizării acestora;
- e) posibilitatea ajustării acestuia la recomandările emise de auditul intern/extern și/sau organul de supraveghere;
- f) furnizarea informației agregate și a datelor statistice.

23. Eficiența sistemului automatizat de monitorizare a tranzacțiilor este influențat semnificativ de disponibilitatea informației care poate fi utilizată și tehnica de stabilire a regulilor sau parametrilor de funcționare. Entitatea în acest scop efectuează îmbunătățiri la necesitate la sistemul de monitorizare a tranzacțiilor luând în considerare modificările în

activitatea operațională și dezvoltările metodelor/tipologiilor de spălare a banilor și finanțare a terorismului. Toate îmbunătățirile sistemului trebuie să fie corespunzător documentate și aprobate de către conducerea entității.

24. În scopul monitorizării tranzacțiilor și activității clienților, entitatea, de asemenea, poate implementa un sistem care generează rapoarte, bazat pe tehnicile de eșantionare a clienților sau tranzacțiilor.

25. Eficiența monitorizării în condițiile pct.24 presupune elaborarea periodică a unor rapoarte și stabilirea unor proceduri adecvate de control pentru a asigura că tranzacțiile clienților sunt cuprinse în procesul de monitorizare a entității în funcție de gradul de risc implicat. Rapoartele periodice de monitorizare ale tranzacțiilor trebuie cel puțin să cuprindă următoarele tipuri de operațiuni: depunerile/eliberările în numerar a mijloacelor bănești, încasările/transferurile de mijloace bănești efectuate prin virament, plățile/transferurile efectuate cu utilizarea dispozitivelor de comunicație electronice, digitale sau informatice (de ex. terminale mobile), tranzacțiile cu instituțiile financiare corespondente și alți clienți cu grad de risc sporit.

26. Sistemul de monitorizare a tranzacțiilor va include proceduri pentru evaluarea nu numai a tranzacțiilor curente ale clientului dar și stabilirea modelului sau tipului de tranzacții și a fluxurilor acestora. Tranzacțiile curente vor fi comparate cu tranzacțiile de același tip anterioare și profilul de risc al clientului. Suplimentar, se vor consulta metodele și tipologiile identificate de spălare a banilor și finanțare a terorismului elaborate de către autoritățile naționale și internaționale.

27. Revizuirea și actualizarea cadrului de monitorizare a tranzacțiilor, în contextul modificării sau nu a riscului implicat, presupune consultarea următoarelor surse de informație:

- a) publicațiile FATF-GAFI și ale altor autorități competente;
- b) recomandări și publicații ale organelor de drept;
- c) informații de la organele de supraveghere și SPCSB;
- d) publicațiile mass-mediei cu referire la prevenirea și combaterea spălării banilor și finanțării terorismului;
- e) experiența operațională obținută în cadrul activității de monitorizare desfășurată de entitate.

28. O premisă pentru stabilirea și funcționarea unui sistem eficient de monitorizare a tranzacțiilor este suportul și angajamentul conducerii entității. Prin urmare, acordarea resurselor suficiente pentru menținerea și operarea sistemului sunt esențiale. Persoanele responsabile în entități primesc și analizează informația rezultată în urma procesului de monitorizare a tranzacțiilor și iau decizii privind acțiunile necesare a fi întreprinse pentru minimizarea riscului de spălare a banilor și finanțare a terorismului.

29. Un element important în cadrul sistemului de monitorizare al entității este monitorizarea continuă a relației de afaceri. Aceasta presupune revizuirea tuturor datelor și informațiilor disponibile aferente clientului în vederea actualizării acestora în scopul cunoașterii activității clientului și cele aferente tranzacțiilor preconizate de a fi efectuate.

30. Entitatea poate întreprinde următoarele măsuri aferente monitorizării continue a relației de afaceri:

- a) actualizarea informației privind cunoașterea clientului prezentată în cadrul stabilirii relației de afaceri;
- b) verificarea corespunderii activității clientului, produselor și serviciilor oferite cu segmentul de piață pe care acesta activează;
- c) obținerea informației privind modificarea actelor de constituire, structurii de proprietate și conducere a clientului, inclusiv cu privire la beneficiarii efectivi a acestuia;
- d) urmărirea realizării scopului și obiectivului propus de client atât la inițierea relației de afaceri cât și pe parcursul acesteia.

III. Natura relației de afaceri

31. Stabilirea naturii relației de afaceri este un proces aplicat de către entitate pentru a înțelege scopul și obiectivele propuse de a fi atinse de către persoană fizică sau juridică la inițierea relației de afaceri.

32. Entitatea determină natura relației de afaceri cu clienții săi prin obținerea datelor despre activitatea curentă sau propusă a lor. În acest sens, prin consultarea și analiza actelor de constituire, analiza tranzacțiilor efectuate prin conturi după stabilirea relației de afaceri, a informației declarate de client privind genurile de activitate desfășurate, precum și verificarea veridicității informației oferite, entitatea determină activitatea sau activitățile de bază desfășurate de către client.

33. Circumstanțele care indică existența unei relații de afaceri sunt, cel puțin următoarele:

- a) deschiderea unui cont de plată;
- b) deținerea unui card de plată;
- c) procurarea prin intermediul entității a unor instrumente financiare;
- d) furnizarea unor servicii de o anumită durată;
- e) încheierea oricărui alt acord ce facilitează existența unei relații de afaceri.

34. În dependență de riscul implicat, informația care este relevantă și necesară pentru determinarea naturii relației de afaceri poate include unele sau toate elementele menționate mai jos:

- a) detalii referitoare la activitatea clientului sau angajatorului;
- b) sursa mijloacelor bănești preconizate a fi utilizate în cadrul relației de afaceri, precum și destinația acestora;
- c) copii valide ale ultimilor rapoarte financiare (cu excepția cazului stabilirii relației de afaceri sau deschiderii contului persoanei juridice nou constituite și persoanei fizice întreprinzător individual sau care practică alt tip de activitate) și a conturilor supuse auditului extern, după caz;
- d) nivelul și natura activității preconizate să fie desfășurată în cadrul relației de afaceri.

IV. Caracterul ordinar al activității

35. Caracterul activității unui client poate fi determinată prin efectuarea unei evaluări asupra afacerii specifice a acestuia ținând cont de anumiți factori caracteristici. Pentru majoritatea afacerilor, este evident atunci când activitățile desfășurate sunt activități ordinare, dar totuși există situații când activitatea ordinară nu poate fi identificată complet.

36. În cazul în care entitatea nu este convinsă dacă activitatea desfășurată de client este ordinară sau nu, atunci entitatea analizează dacă activitatea este:

- a) normală sau nu poate fi confundată cu o altă afacere și este caracteristică sistemului, proceselor, promovării și competitivității pe segmentul de piață unde activează;
- b) frecventă;
- c) periodică;
- d) implicată în tranzacții cu un volum mare de mijloace bănești;
- e) o sursă de venit pentru afacere și proprietarii acesteia;
- f) consumatoare de resurse;
- g) în măsură de a oferi clienților un serviciu sau produs.

37. La determinarea caracterului activității entitatea ia în considerare și măsura în care fiecare factor descrie activitatea afacerii. Prin urmare, trebuie considerați toți factorii, fiecare în parte nefiind definitiv. Consolidat ei vor indica dacă activitatea desfășurată este ordinară sau nu.

38. Diverse aspecte ale afacerii sau operațiunii pot ajuta la efectuarea analizei necesare, iar factorii descriși pot îmbunătăți calitatea evaluării. Un aspect esențial în analiza efectuată este mărimea financiară a activității. Pentru evaluarea acestui factor, este important analiza mijloacelor bănești implicate în activitatea economică pe o anumită perioadă de timp. Astfel, prin calcularea unor indicatori medii ce caracterizează valoarea tranzacțiilor și veniturile încasate în urma acestora pot oferi cu exactitate caracterul activității afacerii.

39. Resursele alocate pentru activitate sunt proporționale volumului produselor și serviciilor oferite. Resursele pot semnifica timpul personalului, echipamentele utilizate, materia primă și materialele, clădiri, terenuri și alte cheltuieli de capital și/sau orice alte cheltuieli. Evaluarea acestora într-o perioadă de timp va permite aprecierea gradului de dezvoltare a afacerii și implicit probabilitatea continuității acesteia și stabilirea caracterului ordinar al activității.

V. Tranzacții complexe

40. Entitatea va înțelege natura și scopul tranzacțiilor pentru a determina dacă acestea corespund structurii și sensului economic planificat. În cazul când entitatea nu poate determina compatibilitatea tranzacțiilor, aceasta trebuie să obțină informație suplimentară pentru confirmarea sensului economic al acestora. În cazul în care clientul refuză prezentarea documentelor justificative, entitatea nu va efectua tranzacțiile și va raporta astfel de circumstanțe SPCSB, conform legislației.

41. Entitatea în dependență de mărimea, complexitatea și structura activității sale definește caracteristicile tranzacțiilor financiare cu structuri complexe care impun acesteia riscuri sporite și nu garantează veridicitatea scopului tranzacțiilor cu sensul economic aferent. Un șir de tranzacții pot avea caracteristici complexe dar să fie total transparente. Însă lipsa transparenței poate conduce la neînțelegerea structurii tranzacțiilor efectuate și ca urmare duce la creșterea riscurilor în activitatea entității.

42. În general tranzacțiile complexe prezintă o serie de operațiuni în care sunt implicate diferite tipuri de tranzacții sau este un flux de tranzacții cu o structură și grad de dificultate mare fără a avea un scop economic clar. Tranzacțiile pe care entitatea le poate

lua în considerare la determinarea caracterului complex reprezintă, fără a se limita la acestea:

a) tranzacții cu utilizarea instrumentelor financiare – cecuri, cambii, certificate de depozit, acțiuni și obligațiuni, inclusiv cele la purtător, contracte forward, contracte swap, instrumente ale ratei dobânzii, futures, etc.

b) tranzacții de creditare cu instituirea garanțiilor aferente – credite ordinare, linii de credit, factoring, credite ipotecare, eliberarea garanțiilor și cauțiunilor, leasing, acreditive, etc;

c) tranzacții de investire și administrare fiduciară a bunurilor – fonduri de pensii, societăți de asigurări, fonduri de investiții, consultații și asistență investițională, etc;

d) tranzacții efectuate în cadrul activităților profesionale independente - agenți imobiliari, notari, contabili, auditori, etc;

e) tranzacții ale participanților profesioniști la piața valorilor mobiliare – în sensul prevederilor Legii nr.171 din 11 iulie 2012 privind piața de capital;

f) tranzacții de cumpărare – vânzare a metalelor și pietrelor prețioase și jocurile de noroc.

g) tranzacții care vizează criptoactive ori cu privire la utilizarea serviciilor de criptoactive, în funcție de amploarea și complexitatea acestora.

h) tranzacții care implică schimb de mijloace bănești în diferite valute urmate într-un timp scurt de transferuri în străinătate sau retrageri în numerar;

i) tranzacții multiple din diferite conturi de plăți pentru colectarea și mobilizarea mijloacelor bănești către un singur cont;

j) tranzacții multiple din diferite conturi de plăți pentru facilitarea procurării în străinătate a unui produs sau serviciu obscur, etc.

44. Pentru minimizarea riscurilor, precum și pentru gestionarea acestora corespunzător, la efectuarea tranzacțiilor complexe entitatea aplică următoarele, fără a se limita la acestea:

a) instruirea permanentă a angajaților aferent tranzacțiilor complexe;

b) aplică sisteme și modele adecvate pentru urmărirea performanței și gestionarea riscurilor;

c) elaborează proceduri de administrare și control intern;

d) alocarea resurselor tehnologice, materiale și umane corespunzătoare în analiza tranzacțiilor și activităților ce necesită o atenție sporită.

VI. Recomandări privind politicile, controalele interne și procedurile entității

Secțiunea 1 Instruirea internă

45. Un program de instruire eficient în cadrul entității va explica actele normative în vigoare aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului, dar și politicile și procedurile interne utilizate pentru diminuarea riscurilor identificate.

46. Instruirea va include atât cursuri formale de instruire, cât și comunicări în curs care servesc la educarea angajaților și la menținerea gradului de conștientizare continuă a acestora în ceea ce privește cerințele de prevenire și combatere a spălării banilor și finanțare a terorismului, cum ar fi e-mailuri, buletine de știri, întâlniri periodice cu echipa, site-uri intranet și alte mijloace care facilitează schimbul de informații.

47. Un factor important în proiectarea unui program eficient de instruire este identificarea audienței țintă. În acest context, angajații care au tangență cu aplicarea cerințelor de prevenire și combatere a spălării banilor și finanțării terorismului care activează în diferite subdiviziuni ale entității trebuie să primească instruirii în mod continuu:

- a) Personalul din prima linie – sunt angajații care necesită cel mai mult înțelegerea practică a importanței eforturilor de prevenire și combatere a spălării banilor și finanțării terorismului și ce măsuri urmează a fi întreprinse pentru a fi vigilenți împotriva activităților și tranzacțiilor ce impun risc de spălarea banilor și finanțare a terorismului. Este important instruirea asupra tuturor produselor și serviciilor oferite de entitate (depozite, credite, operațiuni în numerar, transferuri, schimb valutar, etc.) și riscul impus de către acestea;
- b) Personalul operațional – personalul care nu se află în relație directă cu clienții dar care analizează și evaluează anumite tipuri de tranzacții sau activități, cum ar fi: operațiuni de finanțare a comerțului, operațiuni cu hârtii de valoare, operațiuni de management și consultanță, subscrieri (underwriter) de împrumuturi, etc;
- c) Personalul responsabil de conformitate – este angajatul/angajații desemnați pentru coordonarea și monitorizarea implementării eficiente a programului de prevenire și combatere a spălării banilor și finanțării terorismului entității. Având în vedere responsabilitatea activităților acestora entitățile vor instrui mai avansat personalul implicat pentru a rămâne la curent cu cerințele noi și tipologiile identificate de spălarea banilor și finanțarea terorismului;
- d) Personalul de testare independent (auditul intern) – este personalul care asigură testarea independentă a conformării entităților la cerințele de prevenire și combatere a spălării banilor și finanțării terorismului. Acești angajați trebuie periodic să fie instruiți cu privire la cerințele de reglementare, modificările în reglementare, metodele de spălare a banilor și impactul acestora asupra entității;
- e) Managementul entității - Consiliul și organul executiv au nevoie de un grad mai mic de instruire în comparație cu alte categorii de personal. Instruirea specializată pentru conducerea organizației ar trebui să abordeze importanța cerințelor de reglementare în domeniu, sancțiunile pentru neconformitate, răspunderea personală și riscurile unice ale organizației.

48. Următorul factor în proiectarea unui program eficient de formare în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului este identificarea subiectelor de învățat. Acestea vor varia în dependență de entitate și produsele și serviciile oferite. La identificarea subiectelor mai multe elemente urmează a fi luate în considerare, precum:

- a) Istoricul general referitor la controalele efectuate în vederea respectării domeniului de prevenire și combatere a spălării banilor și finanțării terorismului; inclusiv

- explicarea noțiunii de spălare a banilor și finanțare a terorismului și consecințele acestui fenomen;
- b) Cadrul juridic al domeniului și actele normative aplicabile entității și angajaților acesteia;
 - c) Modificarea cadrului normativ care reglementează regimul de sancționare pentru încălcările aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului;
 - d) Politicile și procedurile interne de identificare și verificare a clienților și beneficiarilor efectivi, inclusiv măsurile de precauție sporită privind clienții și monitorizarea tranzacțiilor în mod continuu;
 - e) Evaluarea internă a riscurilor de spălare a banilor și finanțare a terorismului și planurile de minimizare a riscurilor identificate;
 - f) Cerințe legale de păstrare a datelor;
 - g) Cerințe de identificare a tranzacțiilor suspecte și de raportare către autoritatea competentă;
 - h) Modalitatea de interacțiune cu clienții, inclusiv în cazul examinării situațiilor de risc sau tranzacțiilor suspecte;
 - i) Obligațiile și responsabilitatea angajaților;
 - j) Păstrarea confidențialității în chestiunile legate de prevenirea și combaterea spălării banilor și finanțării terorismului;
 - k) Tendințele și problemele emergente legate de activitatea criminală, finanțarea terorismului, tipologiile identificate și cerințele de reglementare;
 - l) Schemele de spălare a banilor identificate (de preferință cazuri care au avut loc la entitate), inclusiv modul în care a fost detectată pentru prima, impactul acesteia asupra entității și rezoluția sa finală.

49. În scopul instruirii continue a angajaților entitatea va desfășura pentru angajații existenți cel puțin o sesiune anuală de instruire, în timp ce angajații noi, vor beneficia de mai multe instruirii, inclusiv cu privire la funcția lor profesională, dar și într-o perioadă rezonabilă de timp după angajare sau transferul la un nou loc de muncă. Pot apărea situații care necesită sesiuni imediate de instruire, de exemplu, după o examinare sau un audit care descoperă deficiențe grave de control în domeniul combaterii spălării banilor, apariția unei știri despre implicarea entității în activități riscante, schimbările în software sau sistemele și procedurile interne.

50. Instructorii la elaborarea programului de instruire vor avea în vedere problemele aferente domeniului în cadrul entității; audiența la care se adresează; dezvoltarea curriculumului care să răspundă scopului cursului, obiectivelor și rezultatelor dorite; stabilirea calendarului de formare; materialele de curs necesare a fi prezentate; desfășurarea testărilor și evaluarea cunoștințelor acumulate, etc.

Secțiunea a 2-a

Evaluarea conformității de către auditul independent

51. Entitatea la aplicarea cerințelor politicilor interne în materie de auditare independentă a conformării entității prevederilor de prevenire și combatere a spălării

banilor și finanțării terorismului (auditul independent) vor ține cont de riscurile identificate pentru stabilirea frecvenței aplicării controalelor. Rezultatele obținute se prezintă managementului entității, iar recomandările elaborate trebuie urmărite să fie implementate de către personalul responsabil în termenul limită stabilit.

52. În cadrul auditărilor desfășurate, controalele aplicate trebuie să fie cuprinzătoare având în vedere volumul activității și riscurile la care este expusă entitatea. Elementele importante a fi considerate în cadrul controalelor, cu excepția celor obligatorii prevăzute de către actele normative în vigoare, sunt:

- 1) Evaluarea riscurilor de spălare a banilor și finanțare a terorismului desfășurată și a planului de măsuri aprobat în scopul minimizării riscurilor identificate;
- 2) Efectuarea testării tranzacțiilor, în special, a celor cu risc înalt, complexe, semnificative și neordinare;
- 3) Examinarea măsurilor de precauție sporite aplicate clienților/tranzacțiilor cu grad de risc sporit, inclusiv față de Persoanele Expuse Politic, instituții corespondente, elaborarea și utilizarea tehnologiilor informaționale inovatoare, tranzacții cu jurisdicții cu un grad de risc sporit, tranzacțiile în numerar, etc.;
- 4) Examinarea integrității și exactității sistemelor informatice utilizate de entitate, inclusiv capacitatea aplicației de monitorizare a tranzacțiilor pentru a identifica activitatea neordinară a clienților prin:
 - a) Revizuirea politicilor, procedurilor și proceselor de monitorizare a activităților suspecte;
 - b) Revizuirea proceselor de asigurare a integrității, acurateței și oportunității datelor furnizate de sistemele sursă de procesare a tranzacțiilor;
 - c) Evaluarea metodologiei de stabilire și analiză a activității preconizate sau a criteriilor de filtrare;
 - d) Evaluarea caracterului adecvat al rapoartelor de monitorizare;
 - e) Compararea tipologiilor de monitorizare a tranzacțiilor cu evaluarea riscurilor de spălare a banilor și finanțare a terorismului pentru rezonabilitate, etc.;
- 5) Revizuirea managementului/gestiunii cazurilor de identificare a tranzacțiilor suspecte, indicii și criteriile de suspiciune utilizați și a sistemelor de raportare a tranzacțiilor suspecte;
- 6) Examinarea aplicării eficiente a cerințelor privind informațiile care însoțesc transferurile de fonduri naționale și internaționale;
- 7) Evaluarea caracterului adecvat al sistemului de control intern, inclusiv a desemnării persoanei responsabile, petrecerii instruirilor și acuratețea materialelor și a programului de instruire, etc.;
- 8) Examinarea aspectele oricăror funcții de conformitate aferente domeniului care au fost externalizate terțelor părți, inclusiv calificările personalului, contractul, performanța și reputația companiei;
- 9) Evaluarea eficacității politicii entității de revizuire a conturilor care generează multiple dosare de raportare a tranzacțiilor suspecte, inclusiv procese aplicate de închidere a contului;
- 10) Evaluarea adecvării proceselor de păstrare a datelor;

- 11) Urmărirea aplicării măsurilor restrictive internaționale, inclusiv față de persoanele, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă, etc;
- 12) Urmărirea deficiențelor identificate anterior și asigurarea înlăturării prompte a acestora;
- 13) Examinarea dacă managementul entității a fost receptiv la constatările anterioare ale auditului și măsurile întreprinse în scopul neadmiterii acestora pe viitor.

Secțiunea a 3-a Cunoașterea angajatului

53. Entitatea va elabora programul intern privind cunoaște-ți angajatul având în vedere că scopul acestuia este de a permite entității să înțeleagă situația fiecărui angajat, conflictele de interese și susceptibilitatea ca acesta să fie complice în spălarea banilor și/sau finanțarea terorismului. Politicile, procedurile și controalele interne, inclusiv, fișele de post, codul de conduită și etică, nivelurile de autorizare, responsabilitatea, monitorizarea, controlul dual și alte elemente constitutive trebuie ferm să descurajeze implicarea angajaților în activități cu caracter criminal.

54. Analiza preliminară a angajaților potențiali și actuali este esențială pentru păstrarea în afară a angajaților nedoriti și identificarea celor care urmează să fie eliminați. Contextul de screening poate fi un instrument eficient de gestionare a riscurilor, oferind managementului o asigurare că informațiile furnizate de angajat sunt adevărate și că acesta nu are trecut criminal. Folosite în mod eficient, controalele de fond asupra angajaților pot descuraja furtul și delapidării de fonduri și previne litigiile de muncă.

55. Avantajele unei evaluări corespunzătoare a potențialilor angajați și a celor existenți sunt: obținerea unui avantaj competitiv, creșterea productivității, creșterea moralei, reducerea riscului de perturbare a afacerii, luarea deciziilor bune de angajare, asigurarea unui mediu de lucru sigur, protejarea activelor organizației, etc.

56. Programului de cunoaștere a angajatului va conține:

1) Formularul de aplicare la angajare – asigură uniformitatea, deplinătatea informațiilor obținute și prezintă spațiu pentru candidat de a semna anumite declarații necesare pe proprie răspundere. Formularele trebuie să includă, cel puțin, următoarele informații:

- a) Informații curente ale solicitantului: numele, prenumele și informațiile de contact;
- b) Adresa de reședință, inclusiv istoricul acesteia, necesară pentru a verifica istoricul ocupării forței de muncă;
- c) Numărul de identificare de stat (IDNP).
- d) Data nașterii, pentru a permite angajatorului să efectueze o verificare a autobiografiei;
- e) Istoricul locurilor de muncă (indicând numele, adresa și numărul de telefon al angajatorului, funcția, subdiviziunea și funcțiile deținute, salariul, numele și titlul supervisorului, datele de început și sfârșit, motivul plecării și permisiunea de a contacta angajatorul);

- f) Antecedente penale - este necesar asigurarea unui spațiu suficient subiectului pentru a explica informații complete despre incident(e) și dispoziția (dispozițiile);
 - g) Istoricul studiilor - (indicând denumirea, adresa și numerele de telefon ale instituțiilor de învățământ, datele de început și de sfârșit, durata majoră sau cursul de studiu și statutul de finalizare);
 - h) Informații privind licențe, certificări sau alte înregistrări obținute.
- 2) Revizuirea formularului de aplicare – următorul pas la evaluarea solicitantului este examinarea cererii prezentate pentru revizuirea corespunderii cu cerințele minime ale funcției și ale informațiilor din formular și cu capacitatea solicitantului de a respecta aceste cerințe minime.
- 3) Interviuul – este, de obicei, prima oportunitate pentru angajator de a se întâlni față în față cu solicitantii. Un interviu bine planificat și executat poate realiza trei obiective:
- a) Să transmită solicitantului informații critice pentru a descuraja solicitanții necorespunzători și pentru a încuraja onestitatea;
 - b) Permite transferul informațiilor lipsă de la solicitant către angajator. De asemenea, angajatorul are posibilitatea de a pune întrebări suplimentare dacă angajatorul suspectează că candidatul a încercat să omită sau să mintă despre informații nefavorabile;
 - c) Permite o evaluare a candidatului și oferă angajatorului o șansă de a evalua aptitudinile, calificările și prerogativele solicitantului în persoană.
- 4) Procesul de verificare a candidatului - scopul acestei secțiuni este validarea informațiilor prezentate anterior în proces de angajare și corespunderea acestuia funcției vacante.

Secțiunea a 4-a

Desfășurarea investigațiilor și raportarea tranzacțiilor suspecte

57. Măsurile de precauție aplicate adecvat de către entitate vor asigura colectarea informațiilor referitoare la client sau tranzacțiile acestuia și vor oferi entității capacitatea promptă de a identifica tranzacțiile și/sau activitățile suspecte. Astfel, angajații entității prin utilizarea regulilor și mecanismelor stabilite vor putea la timp să urmărească activitățile care nu pot fi atribuite ca fiind cu un caracter economic evident al clientului, inclusiv în comparație cu sursa mijloacelor bănești implicate sau a venitului clientului, sau cu activitățile obișnuite ale acestuia, și respectiv, vor investiga discrepanțele existente.

58. Investigațiile pot fi inițiate de la o monitorizare pro-activă a activității potențial suspecte, la fel ca măsurile reactive luate pentru a aborda constatările autorităților de supraveghere, referințele sau alte recomandări. Printre inițiativele de investigare se numără:

- a) Recomandări din partea autorităților de supraveghere - astfel de eforturi pot duce la crearea unei noi monitorizări continue sau pot fi revizuiți unice pentru a aborda întrebări sau observații specifice. Cel mai important este ca investigațiile inițiate ca rezultat al constatărilor autorităților de supraveghere să fie clar

documentate și concepute astfel încât să se asigure că toate aspectele constatărilor sunt abordate în termenul solicitat;

- b) Reguli de monitorizare a tranzacțiilor destinate detectării unei activități suspecte potențiale – metodele comune pentru monitorizarea tranzacțiilor includ crearea de reguli interne personalizate de monitorizare a tranzacțiilor sau angajarea unui furnizor terț să asiste la elaborarea și implementarea unor reguli automatizate;
- c) Recomandări din partea angajaților din prima linie cu privire la activitatea potențial suspectă - în funcție de mărimea entității, pot exista procese de raportare manuală prin e-mail sau prin telefon, sau printr-un sistem de raportare internă care direcționează raportările la echipele de investigare corespunzătoare (ca exemplu, când se identifică o structurare a tranzacțiilor, se prezintă bancnote care conțin un miros ce indică asupra unor substanțe interzise sau răspunsurile inconsecvente ale clientului la întrebările legate de sursa depozitelor mari de numerar);
- d) Informațiile obținute din linii telefonice interne - cunoscute sub numele de linii telefonice de etică, conformitate sau de avertizare în caz de nereguli, acestea permit angajaților să raporteze o gamă largă de activități, inclusiv fraudă angajaților, hărțuirea și discriminarea, încălcări ale codului de conduită, furt de proprietate a companiei și cadouri inadecvate;
- e) Informații negative publicate în sursele media – importanța acestora este redată de relevanța știrii vis-a-vis de un client al entității, modul în care un produs este utilizat pe piață, o locație geografică pe care o deservește entitatea sau implicarea într-un eveniment de spălare de bani sau finanțare a terorismului;
- f) Primirea unei citații sau a unui mandat de percheziție din partea autorităților competente – entitatea trebuie să îndeplinească în mod legal cerințele solicitate și să stabilească dacă activitatea clientului identificat necesită depunerea unui raport de tranzacție suspectă.

59. Există câțiva pași importanți pentru desfășurarea unei investigații financiare eficiente în ceea ce privește potențialele activități suspecte, inclusiv:

- a) examinarea tranzacțiilor interne, a informațiilor obținute de la client, și alte documente interne relevante;
- b) identificarea și revizuirea informațiilor externe pentru a înțelege activitatea clientului, entitățile afiliate și sursele media relevante;
- c) contactarea angajaților din prima linie responsabili pentru relația cu clientul și monitorizarea contului acestuia;
- d) generarea unui raport scris care să documenteze constatări relevante.

60. Obiectivul principal al investigatorului financiar este de a urmări circulația mijloacelor bănești, fie printr-o bancă, broker-dealer, alți prestatori de servicii financiare, furnizor de servicii privind activele virtuale, cazinouri sau altă instituție financiară. Instituțiile financiare au un șir de informații la îndemână, deoarece furnizează clienților săi diferite produse și servicii cum sunt încasări în conturi, plăți naționale și internaționale, eliberări în numerar, emit cecuri și alte instrumente de plată, acordă împrumuturi, efectuează operațiuni de schimb valutar, etc., pentru analiza cuprinzătoare a activității și

tranzacțiilor clientului și a forma o opinie asupra riscului de spălare a banilor și finanțare a terorismului pe care acesta îl impune instituției.

61. O investigație eficientă presupune ca informațiile utilizate să fie obținute atât din cadrul entității, cât și din surse externe, să fie fiabile și verificabile. Internetul este din ce în ce mai mult utilizat ca sursă de informații în cadrul investigațiilor interne. O abordare focalizată pe căutarea unor surse sigure și de încredere poate oferi informații utile de la terțe părți și un context suplimentar la dosarele deținute de către entitate. Combinată cu o analiza documentelor interne și a înregistrărilor existente, sursele sigure de internet pot contribui la furnizarea unei imagini complete asupra faptului dacă sunt necesari pași suplimentari pentru a atenua posibilele riscuri de spălare a banilor și finanțării terorismului asociate cu clientul.

62. Pot fi considerate surse web fiabile pentru realizarea cercetării de către entitate paginile web independente menținute de organizații internaționale (de exemplu, FATF-GAFI, Wolfsberg, OCDE și OFAC) și de autoritățile de supraveghere la nivel național (de exemplu, autorități de reglementare, agenți de înregistrare corporativă), precum și în unele situații pot fi utilizate și conținutul articolelor din media specializată (de exemplu, cea care furnizează informații valoroase privind statutul de reglementare/supraveghere, sancțiuni, amenzi, activități comerciale permise, etc.), necesare obiectului anchetei.

63. Decizia de a raporta tranzacția/activitatea ca una suspectă implică deseori cântărirea factorilor agravanți și atenuanți care decurg din cercetarea efectuată în timpul procesului de investigație. Entitatea ar trebui să dispună de proceduri clare care să documenteze factorii care sunt luați în considerare atunci când se stabilește dacă o tranzacție/activitate este suspectă și urmează a fi raportată. Decizia finală ar trebui să fie documentată și susținută de raționamentul utilizat pentru determinare suspiciunii și să fie coordonat cu ofițerul de conformitate sau altei persoane investite cu atribuții de executare a Legii cu privire la prevenirea și combaterea spălării banilor și finanțarea terorismului, inclusiv celei cu funcții de conducere de rang superior din cadrul entității.

64. Entitatea, pentru a determina operațiunile care par a fi legate între ele, dar sunt efectuate sub limitele de identificare sau raportare, poate utiliza următoarea caracteristică a acestora:

- a) perioada efectuării tranzacțiilor în numerar nu depășește 1 zi;
- b) perioada efectuării tranzacțiilor în virament nu depășește 3 zile;
- c) perioada efectuării operațiunii complexe (consultanță, management activelor, comerț cu hârtii de valoare, etc) nu depășește 5 zile.

65. În scopul identificării tranzacțiilor care par a fi legate între ele, entitățile obligate iau în considerare cel puțin următoarele criterii:

1) În ceea ce privește elementele referitoare la originea și destinația identică sau similară, se iau în considerare tranzacțiile efectuate sau primite de aceeași persoană fizică sau juridică;

2) În ceea ce privește elementele referitoare la originea și destinația identică sau similară, pe baza informațiilor de care dispune entitatea raportoare, se iau în considerare următoarele situații:

- a) clienții sunt membri ai aceleiași familii;
- b) clienții sunt parteneri de afaceri;

c) clienții acționează în mod concertat;
 d) clienții sunt filiale sau beneficiari efectivi ai aceleiași întreprinderi-mamă;
 e) este utilizată aceeași infrastructură digitală;
 f) sunt utilizați intermediari sau prestatori de servicii comuni care facilitează efectuarea tranzacțiilor.

3) În ceea ce privește elementul referitor la scopul identic sau similar, pe baza informațiilor de care dispune entitatea raportoare, se iau în considerare tranzacțiile aferente aceleiași achiziții.

4) În ceea ce privește elementul referitor la alte caracteristici relevante, se iau în considerare următoarele:

a) pe baza informațiilor de care dispune entitatea obligată, tranzacțiile prezintă caracteristici comune;

b) tranzacții cu o origine și o destinație identice sau similare, efectuate la sedii diferite sau prin intermediul unei rețele de agenți ori distribuitori;

c) tranzacții cu o origine identică sau similară, efectuate în cadrul unui program de fidelitate;

d) finalizarea unei tranzacții este condiționată de finalizarea prealabilă a uneia sau a mai multor tranzacții, toate acestea fiind gestionate de aceeași entitate obligată.

5) În ceea ce privește elementul referitor la o anumită perioadă, prevăzut în definiția tranzacțiilor legate, se iau în considerare tranzacțiile efectuate într-un interval de timp scurt, determinat în funcție de natura activității, inclusiv de riscurile și complexitatea acesteia, precum și de dimensiunea entității obligate.

66. Pe baza investigației interne efectuate, entitatea ar trebui să facă o determinare independentă cu privire la închiderea contului clientului său. Unii dintre factorii pe care entitatea ar trebui să îi ia în considerare sunt:

- a) Baza legală pentru închiderea unui cont;
- b) Politicile și procedurile stabilite de entitate pentru închiderea unui cont, care pot include recomandarea automată de închidere ca urmare a unui număr specificat de raportări a tranzacțiilor suspecte;
- c) Gravitatea comportamentului de bază a clientului manifestat prin lipsa feedback-ului și atenției cuvenite față de solicitările entității;
- d) Riscul de reputație pentru instituție prin menținerea contului deschis;
- e) Corespondența cu autoritățile competente de aplicare a legislației aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului.

Anexă

la Recomandările cu privire la monitorizarea tranzacțiilor și activităților clienților în vederea prevenirii și combaterii spălării banilor și finanțării terorismului

„Semnale de avertisment” referitoare la spălarea banilor și finanțarea terorismului

I. Circumstanțe neobișnuite aferente clienților

- 1) Clientul are o comportament neobișnuit sau excesiv de preocupat;
- 2) Clientul discută cerințele de păstrare a datelor sau de raportare de către entitatea raportoare cu intenția aparentă de a le evita;
- 3) Clientul exercită presiuni asupra unui angajat într-un efort de a descuraja înregistrarea/ păstrarea datelor sau raportarea necesară;
- 4) Clientul este reticent în a efectua o tranzacție după ce i s-a comunicat că aceasta va fi raportată;
- 5) Clientul, care exercită funcții publice, deschide cont în numele unui membru al familiei și efectuează depuneri semnificative care nu sunt relevante cu sursele declarate de venituri oficiale ale familiei;
- 6) Clientul, care este student, transferă sau schimbă în mod neobișnuit sume mari de bani;
- 7) Contul indică o dinamică sporită a mișcărilor de fonduri dar păstrează o balanță zilnică scăzută la început/ sfârșit de zi;
- 8) Tranzacțiile implică companii off-shore ale căror denumiri sunt similare cu denumirile unor instituții financiare bine-cunoscute;
- 9) Tranzacțiile sunt efectuate în jurisdicții (țări/ insule) necunoscute;
- 10) Agentul, notarul sau consultatul financiar acționează în numele altei persoane fără documente confirmative, cum ar fi procura notarială, declarație de trust, etc;
- 11) Clientul prezintă informații care generează suspiciuni sau acesta refuză să prezinte documente originale în procesul de verificare;
- 12) Clientul nu dorește să prezinte informații personale la deschiderea contului;
- 13) Clientul încearcă să deschidă un cont fără a prezenta documente de identificare, de referință sau adrese locale complete;
- 14) Clientul indică o adresă permanente care se află în afara ariei de deservire a instituției;
- 15) Clientul indică date de contact (numere de telefoane) la care nu poate fi contactat, acestea fiind deconectate;
- 16) Clientul nu dorește să recepționeze extrase ale contului său ori alte e-mailuri expediate;
- 17) Clientul prezintă un interes sporit asupra procedurilor instituției financiare de furnizare a informațiilor despre identificarea clienții săi;
- 18) Un client- persoană juridică nu dorește să furnizeze informații complete despre natura și scopul afacerii sale, scopul operațiunilor din cont și alte detalii despre companie sau să furnizeze situații financiare sau documente despre o entitate de afaceri asociată;
- 19) Clientul nu oferă detalii privind istoricul angajărilor sau situația curentă în cazul cererii pentru împrumut;
- 20) Adresa IP a clientului nu corespunde informațiilor de identificare furnizate la momentul înregistrării online.

II. Operațiuni neobișnuite cu numerar

- 1) Clientul depune frecvent în numerar bancnote contrafăcute, deteriorate, și/sau nu-i pasă de numărul bancnotelor depuse, etc;

- 2) Clientul este însoțit de o altă persoană care se deservesc la ghișee diferite pentru a efectua operațiuni în valută în sume de până la limita de raportare;
- 3) Clientul efectuează depuneri semnificative în numerar în bancnote de valoare mică;
- 4) Clientul deschide mai multe conturi din numele unei singure sau mai multor persoane apoi efectuează depuneri în numerar în sume de până la limita de raportare;
- 5) Clientul efectuează retrageri de numerar din unul din conturile sale și depune numerarul în alt cont al cărui titular este, fără un scop sau explicație economică evidentă;
- 6) Clientul efectuează tranzacții neobișnuite în numerar utilizând în acest sens și safeurile individuale în lipsa unui raționament economic;
- 7) Clientul efectuează frecvent depuneri sau retrageri al unor sume semnificative în valută fără vreun anumit scop economic sau pentru o companie care nu obișnuiește să opereze cu sume semnificative în numerar;
- 8) Clientul efectuează operațiuni semnificative în numerar la diferite sucursale în aceeași zi sau coordonează astfel de operațiuni din numele său;
- 9) Clientul depune numerar în mai multe conturi în sume de până la limita de raportare apoi centralizează fondurile într-un cont unic pentru a le transfera peste hotare ulterior;
- 10) Clientul intenționează să retragă o parte din suma depusă în numerar care depășește pragul de raportare după ce acesta a aflat despre faptul că operațiunea urmează a fi raportată;
- 11) Clientul efectuează mai multe depuneri în numerar până la limita de raportare prin bancomate (ATM);
- 12) Clientul efectuează frecvent depuneri semnificative de numerar împachetate cu benzi speciale;
- 13) Clientul procură frecvent instrumente monetare în numerar în sume de până la limita de raportare;
- 14) Clientul efectuează o serie neobișnuită de operațiuni de schimb valutar, fără un scop economic vizibil;
- 15) O persoană care nu este client efectuează depuneri în numerar în contul unui client care ulterior se retrag în diferite locații geografice.

III. Operațiuni de credit neobișnuite și transferuri electronice neordinare

- 1) O tranzacție este făcută să apară mai complicată decât trebuie să fie, prin utilizarea unor termeni impresionanți, dar lipsiți de sens, cum ar fi rata de emisie, note bancare primare, angajament stand-by, arbitraj sau contracte de hedging;
- 2) Clientul solicită împrumuturi fie pentru companii rezidente în jurisdicții cu risc înalt fie garantate de obligațiile băncilor din jurisdicții cu risc înalt;
- 3) Clientul achită pe neașteptate o parte semnificativă din împrumut fără a explica sursa mijloacelor bănești;
- 4) Clientul procură certificate de depozite și le utilizează ca documente confirmative pentru un împrumut;
- 5) Clientul garantează un împrumut cu depuneri în numerar;
- 6) Clientul utilizează garanții în numerar cu proveniență din jurisdicții cu risc înalt pentru obținerea unui împrumut;

- 7) Împrumutul contractat de către client este transferat pe neașteptate în jurisdicții cu risc înalt;
- 8) Transferurile electronice sunt efectuate sau primite de la aceeași persoană din sau către aceleași conturi;
- 9) Netitularii de conturi efectuează transferuri electronice de fonduri care implică numeroase instrumente monetare a căror sume se situează sub limita de raportare;
- 10) Transferul electronic este însoțit de instrucțiuni de convertire a fondurilor la ghișeu și transmiterea lor către un netitular de cont;
- 11) Creșterea numărului de transferuri electronice internaționale dintr-un cont în care nu obișnuia să efectueze astfel de transferuri sau în cazul când activitatea economică a clientului nu implică astfel de tranzacții.

IV. Alte activități neobișnuite ale clienților

- 1) Clienții persoane juridice prezintă situații financiare care diferă esențial de alte situații financiare ale altor persoane juridice cu activitate similară;
- 2) Clientul păstrează un număr excesiv de conturi pentru tipul de activitate despre care se presupune că este efectuată;
- 3) Conturile persoanelor juridice- corporative indică o activitate neesențială, neregulată și periodică;
- 4) O tranzacție este efectuată în circumstanțe în care angajatul entității ar putea avea temei de a refuza acordarea unui împrumut din motivul garanțiilor dubioase;
- 5) Numeroase plăți sau transferuri semnificative între companii-fantomă (fictive) fără un scop economic legitim;
- 6) Companiile care efectuează operațiuni între ele se află la aceeași adresă sau indică date de înregistrare similare sau implică alte inconsistențe cu referire la activitatea acestora;
- 7) Clientul solicită plata unor încasări către o parte terță neafiliată;
- 8) Un număr semnificativ de scrisori de garanție (letter of credit) ale căror beneficiari sau destinații ale plăților sunt modificate în mod nejustificat înaintea realizării plăților sau clientul modifică locația plății indicată inițial;
- 9) Scrisoarea de garanție nu corespunde activității clientului;
- 10) Scrisoarea de garanție este emisă pentru produse care au puțină cerere în țara importatorului;
- 11) Scrisoarea de garanție este emisă pentru bunuri care sunt rare sau nu sunt produse în țara exportatorului;
- 12) Scrisorile de garanție sunt recepționate din țările care prezintă un risc înalt de spălare a banilor;
- 13) Prețul bunurilor și serviciilor sunt supra-/ subevaluate;
- 14) Structura tranzacției pare să fie mult prea complexă și are intenția de a voala scopul și natura tranzacției;
- 15) Mărfurile sunt expediate prin una sau mai multe jurisdicții fără un scop economic și logistic clar;
- 16) Volumul mărfurilor expediate nu corespunde cu volumul obișnuit specific activității economice a importatorului sau a exportatorului;

- 17) Clientul realizează un număr semnificativ de operațiuni/ tranzacții prin Internet sau telefon;
- 18) Clientul achiziționează un număr de cartele preplătite de tip open-end pentru sume semnificative, incompatibile cu activitatea economică desfășurată;
- 19) Operațiunile de retrageri din conturi nu corespund activității obișnuite desfășurate de către titularul de cont sau include transferuri către jurisdicții internaționale cu un grad de risc înalt;
- 20) Clientul utilizează contul personal în scopuri economice (desfășurarea activității economice).

V. Activitatea neobișnuită a angajatului

- 1) Angajatul denaturează calitățile, profilul sau capacitatea financiară și resursele unui client în rapoartele scrise solicitate de către entitate;
- 2) Angajatul duce un stil de viață extravagant pe care nu și l-ar putea primi având în vedere veniturile sale;
- 3) Angajatul, în mod frecvent nu ține cont de controalele/ acordurile stabilite sau ignoră reglementările/ politicile interne;
- 4) Angajatul utilizează resursele companiei pentru a favoriza interese personale;
- 5) Angajatul este prezent la momentul efectuării tranzacțiilor în care sunt implicați beneficiari efectivi sau părți ale tranzacției ale căror identitate este secretă;
- 6) Angajatul refuză să beneficieze de zilele de concediu.

VI. Indicatori „semnale de avertisment” în actele de corupție

- 1) Experiență slabă sau nerelevantă în ceea ce privește serviciile care urmează să fie furnizate;
- 2) Reputație compromisă (implicare în acte de corupție, etc);
- 3) Funcționar public responsabil sau persoana care deține o funcție de decizie pentru atribuirea unui contract de achiziție în care s-au constatat probleme sau deficiențe rezultante sau de implementare;
- 4) Tranzacție sau un Intermediar sugerat de un funcționar public, în special, pentru acțiune comună în cadrul unei activități sau operațiune;
- 5) Relații comerciale, personale sau familiale apropiate cu un funcționar public care are autoritate discreționară în privința unei afacerii sau tranzacție;
- 6) Partea la o tranzacție sau un contract face obiecții fără motive/neargumentate față de măsurile de precauție, de reprezentare sau oferirea garanțiilor incluse în acord;
- 7) Partea nu locuiește sau nu are o prezență semnificativă în țara în care urmează să fie furnizat serviciul;
- 8) Utilizarea unei companii fictive/fantome sau a unei alte structuri corporatiste netransparente/opace;
- 9) Necesită plata unui comision sau a unei părți semnificative a acestuia, înainte sau imediat după atribuirea contractului;
- 10) Cereri pentru clauze contractuale neobișnuite;

- 11) Cereri pentru activități repetate, executate de aceleași sau alte persoane (de exemplu, construcții, reparații, schimbări de mobilier, etc) în lipsa unui scop economic evident;
- 12) Solicitări de plată în numerar, plăți în avans, plată către o persoană fizică sau juridică care nu este persoana/entitatea contractantă sau plata într-o țară care nu este sediul principal al întreprinderii contractante sau țara în care se desfășoară serviciile;
- 13) Anticipă plăți care nu pot fi justificate din punct de vedere comercial în raport cu rolul întreprins;
- 14) Ajustarea cererii de remunerare în timpul angajamentului, în special în imediata apropiere de atribuirea contractului;
- 15) Contabilitate vagă sau nedocumentată;
- 16) Dependență mare de numerar.

VII. Indicatori „semnale de avertisment” în spălarea banilor pe bază de comerț (contrabanda)

- 1) Se constată discrepanțe semnificative între descrierea mărfii pe foaia de transport și factură;
- 2) Se constată discrepanțe semnificative între descrierea mărfurilor pe foaia de transport (sau factură) și bunurile efective expediate;
- 3) Se constată discrepanțe semnificative între valoarea mărfii raportată pe factură și valoarea justă de piață a mărfii;
- 4) Mărimea încărcăturii pare incompatibilă cu scara activităților comerciale regulate ale exportatorului sau importatorului;
- 5) Tipul mărfurilor expediate este desemnat drept cu „risc ridicat” pentru activitățile de spălare a banilor;
- 6) Tipul mărfurilor expediate pare incompatibil cu activitățile de afaceri regulate ale exportatorului sau importatorului;
- 7) Expedierea de mărfuri/bunuri nu are sens economic;
- 8) Mărfurile sunt expediate către (sau din) o jurisdicție desemnată drept cu „risc ridicat” pentru activitățile de spălare a banilor;
- 9) Mărfurile sunt transbordate prin una sau mai multe jurisdicții fără nici un motiv economic aparent;
- 10) Metoda de plată pare incompatibilă cu caracteristicile de risc ale tranzacției;
- 11) Tranzacția implică primirea de numerar (sau alte plăți) de la entități terțe care nu au legătură evidentă cu tranzacția;
- 12) Tranzacția implică utilizarea de scrisori de garanții în mod repetat modificate sau extinse;
- 13) Tranzacția implică utilizarea companiilor intermediare sau fictive/fantome.

VIII. Activități neobișnuite suspecte de trafic de ființe umane

- 1) Transferurile electronice multiple, în general efectuate sub pragul de raportare, expediate de la diverse locații către un beneficiar comun;

- 2) Transferuri multiple efectuate la diferite sucursale ale unei instituții financiare către sau din jurisdicții (locații) în aceeași zi sau în zile consecutive;
- 3) Fluxuri de bani care nu se potrivesc cazurilor comune de remitențe:
 - a) Transferurile transmise din țări cu populații cu migrație înaltă sunt direcționate către beneficiari aflați în orașe/jurisdicții limitrofe;
 - b) Beneficiarii care primesc transferuri din țările cu populații cu migrație mare care nu sunt resortisanți ai acestor țări.
- 4) Depuneri neobișnuite în valută în instituțiile financiare, urmate de transferuri către țările cu populații cu migrație înaltă într-o manieră incompatibilă cu activitatea preconizată a clienților. Acestea pot include creșteri bruște ale depunerilor în numerar, fluctuația rapidă a fondurilor și volumul mare de depozite în numerar cu surse necunoscute de fonduri;
- 5) Contul unui client pare să funcționeze ca un cont de tranzit, în care depozitele în numerar (adesea păstrate sub pragul de raportare) apar în orașe / state în care clientul nu locuiește sau nu desfășoară activități comerciale. În mod frecvent, în cazul conturilor de tranzit, fondurile sunt retrase rapid (în aceeași zi) după efectuarea depozitelor;
- 6) Schimbul frecvent de bancnote de valoare mică cu bancnote de valoare mai mare ale unui client care nu se regăsește în mod obișnuit în circuit cu utilizare largă a numerarului. Acest tip de activitate poate să apară ca încasări pentru contrabandiști pentru transferurile în vrac în numerar;
- 7) Atunci când conturile clienților sunt închise din cauza unei activități suspecte, noii clienți pot începe să tranzacționeze în numele acelor clienți ale căror conturi au fost închise; acest lucru se poate face ca un mijloc de a continua activitățile ilicite. În acest caz, conturile noi reflectă adesea o activitate similară cu cea a conturilor închise în care tranzacțiile se pot întâmpla frecvent, sunt semnificative și implică persoane care primesc / trimit fonduri de la / către conturile anterior închise din cauza unei activități suspecte;
- 8) Stil de viață inexplicabil / nejustificat în comparație cu sfera de activitate; profiturile / depozitele semnificativ mai mari decât cele ale colegilor din profesii / sfere de activitate similare;
- 9) Influxurile sunt în mare parte primite în numerar, în cazul în care încasările financiare substanțiale sunt incompatibile cu activitatea economică desfășurată de către client; utilizarea pe scară largă a mijloacelor bănești pentru achiziționarea de active și efectuarea tranzacțiilor;
- 10) Un client- persoană juridică nu prezintă documente privind cheltuielile pentru statele de personal (de ex. salarii, plățile pentru statele de personal, contribuțiile sociale), cheltuielile pentru statele de personal lipsesc sau sunt extrem de mici ținând cont de operațiunile clientului- persoană juridică, forța de muncă și activitatea desfășurată;
- 11) Deducțiile salariale sunt semnificative. Din experiența și observațiile băncii, clientul, desfășurând o activitate economică, deduce sume semnificative pentru achitarea salariilor angajaților său asumându-și și alte cheltuieli (cazare, cheltuieli pentru

- masa) însă angajații sunt remunerați cu o parte mica din salariul lor. Acestea pot avea loc înainte sau după achitarea salariilor;
- 12) Transferuri electronice au loc în afara țării, fără scopuri comerciale evidente, către țările cu risc sporit de trafic de ființe umane sau către țări care nu corespund specificului activității preconizate a clientului;
 - 13) Consumatori multipli, aparent fără legături între ei, efectuează transferuri electronice aceluiași beneficiar. Acești expeditori electronici pot utiliza, de asemenea, informații similare ce însoțesc tranzacțiile, incluzând, dar fără a se limita la, o adresă și un număr de telefon comun. Atunci când sunt interogați în măsura în care circumstanțele o permit, expeditorii electronici pot să nu aibă o legătură aparentă cu destinatarul fondurilor sau nu cunosc scopul transferurilor;
 - 14) Tranzacțiile efectuate de către persoanele fizice însoțite de o persoană-terță (ex. sub pretextul necesității unui interpret) pentru a realiza transferul fondurilor (care par a fi salarii lor sau poate să dețină în posesia sa documente de identitate a clientului) către alte țări;
 - 15) Plăți frecvente către servicii online pentru publicitate, inclusiv taxe mici de postare către companii de anunțuri online, precum și companii de publicitate mai scumpe și mai performante;
 - 16) Tranzacții frecvente, neconforme cu activitatea preconizată și / sau linia de afaceri, efectuate de un client- persoană juridică în eforturi aparente de a furniza susținere persoanelor (de exemplu, plata pentru locuințe, cazare, închirieri regulate de vehicule, achiziții de cantități mari de alimente);
 - 17) Plățile către agenții de recrutare sau de angajare a studenților care nu sunt licențiate/ înregistrate sau care au înregistrat încălcări ale codului muncii;
 - 18) Semnatarii/ custodele sunt identici în conturi persoanelor juridice și/ sau conturi persoanelor fizice aparent independente; informații comune (de exemplu, adresa, numărul de telefon, informațiile despre angajare) folosite pentru a deschide mai multe conturi în nume diferite;
 - 19) Conturile angajaților străini sau studenților în care angajatorul sau agenția de ocupare a forței de muncă servește drept custode.

IX. Indicatori „semnale de avertisment” utilizați pentru a detecta posibilele cazuri de evaziune fiscală și/sau spălare de bani care implică fraude de identitate

Geografice - Adresă/Locație:

- 1) Utilizarea adresei pentru facilitarea fraudei de identitate;
- 2) Utilizarea adresei unei persoane suspectate în evaziune fiscală;
- 3) Utilizarea acelorași adrese și conturi de plăți de către mai multe persoane și corporații;
- 4) Depunerea dărilor de seamă privind venitul obținut de către clienți în diferite regiuni ale țării;
- 5) Utilizarea adreselor de cutie poștală sau utilizarea adreselor inexistente, de exemplu, adresa de reședință, adresa angajatorului etc.; sau codul poștal indicat de client sau angajator nu este în concordanță cu adresa dată;
- 6) Afacerea nu este situată acolo unde locuiește persoana;

- 7) Restituiri de taxe la aceeași adresă;
- 8) Restituiri de taxe trimise mai degrabă la oficii/cutii poștale decât la o adresă reală;
- 9) Restituirile de taxe expediate prin poștă la alte adrese decât cele enumerate în declarația fiscală ca reședință a contribuabilului;
- 10) Restituirile de taxe expediate revin la adresa agentului/consultantului/contabilului pregător al documentelor.

Analiză financiară:

- 1) Valoarea rambursării sau reducerilor;
- 2) Revendicări și deduceri neobișnuite, sau revendicări similare efectuate în același mod sau format;
- 3) Venitul pare nerezonabil pentru client: de exemplu, în comparație cu raportarea din primul an, taxa deductibilă neobișnuit de mare pentru veniturile raportate;
- 4) Depuneri excesive a căror origine nu este justificată;
- 5) Achiziționarea mijloacelor de transport de lux;
- 6) Facturare subevaluată în sectorul imobiliar;
- 7) Analiza tranzacțiilor/activităților suspecte indică utilizarea mai multor conturi de plăți care primesc depuneri mari din diferite surse;
- 8) Sumele de reținere fiscală sunt mult mai mari decât ar fi adecvate pentru suma veniturilor obținute;
- 9) Venit insuficient pentru a începe o afacere;
- 10) Tranzacții care implică paradisuri fiscale.

Documentație și relația de afaceri:

- 1) Similarități în tipărire, scris de mână, adrese, semnături, formate, sume de rambursare;
- 2) Declarații fiscale aparent fără legătură toate împachetate la fel;
- 3) Utilizarea acelorași capse/clame pe hârtie sau introducerea în spații similare pe declarații și/sau ordinea atașamentelor e aceeași;
- 4) Semnăturile pe declarațiile duplicate apar diferite;
- 5) Chitanțele de orice fel par să fi fost scrise sau modificate de către client sau de către o persoană care pregătește declarație pe impozit;
- 6) Formularele de deducere a surselor de impozit pe venit pentru diferiți angajatori aparent pregătite de aceeași persoană (de exemplu, scris de mână, sau cu aceeași mașină de scris sau cu o imprimantă pentru calculator);
- 7) Nu există numărul de identificare a angajatorului pe formularele de impozit pe venit sau numele angajatorului este ciudat/straniu;
- 8) Companiile care nu raportează venituri, dar au efectuat tranzacții raportate de terți;
- 9) Utilizarea persoanelor nominale/interpuse și folosirea companiilor fictive/fantome pentru ascunderea beneficiarului real.

Caracteristici individuale, identitate, comportament și asocierea:

- 1) Statutul de rezidență al persoanelor suspectate;
- 2) Asocierea cu anumiți agenți fiscali;

- 3) Istoricul conformității persoanelor suspectate;
- 4) Grup de clienți din același grup de vârstă;
- 5) Numerele de identificare fiscală din același interval: de exemplu cele care încep cu aceleași primele 3 cifre;
- 6) Nume de familie similare pe un grup de declarații, de ex. Anderson/Sanderson/Henderson;
- 7) Grup de clienți cu angajatori diferiți, dar în aceeași profesie;
- 8) Recomandări multiple de la același angajator;
- 9) Persoana suspectată, eventual, prea tânără sau prea bătrână pentru a începe o afacere;
- 10) Contactarea solicitantului înregistrării și acesta susține că nu știe nimic despre afacere;
- 11) Contribuabilii care nu pot recunoaște sau explica în mod corespunzător operațiunile asociate acestora;
- 12) Pierderea repetată a unui card de identitate (de mai multe ori pe an);
- 13) Contribuabilii care nu pot recunoaște dreptul de proprietate asupra conturilor de plăți relevante.

Sincronizare:

- 1) Număr multiplu de declarații depuse simultan sau datate la și în jurul aceleiași date.

Alte:

- 1) Un anumit nivel de detectare poate fi derivat din cererile de informații făcute în circumstanțe neobișnuite, de ex. abordări ilegale referitoare la o problemă legată de taxe sau loterii;
- 2) Numărul de identitate înserat pe declarațiile fiscale nu se potrivește cel din baza de date;
- 3) Multiple declarații sunt depuse cu variații ale acelorași numere de identificare.

Metodele și schemele comune folosite pentru comiterea fraudei fiscale și a spălării banilor care implică fraude de identitate:

- 1) Crearea sau preluarea identității unei persoane în scopul depunerii unor cereri false pentru restituiri și rabaturi (de exemplu, depunerea de declarații fiscale individuale de impozit pe venit false, folosirea informațiilor și documentelor false pentru a obține rambursări de impozit pe venit și TVA);
- 2) Utilizarea identităților false și furate pentru înființarea de întreprinderi pentru comite fraude cu impozitul pe venit și TVA;
- 3) Crearea unei identități pe baza unui pașaport furat sau utilizat fraudulos sau pe baza unei alte surse majore de identificare, care este folosită pentru obținerea unui număr național de identificare, care la rândul său este folosit pentru cererile de asistență socială, pentru înregistrarea fiscală sau de afaceri, deschiderea conturilor de plăți, imprimarea facturilor, etc;

- 4) Furtul corespondenței de la autoritatea fiscală și utilizarea acestor detalii pentru a obține un loc de muncă sau pentru a solicita în mod fals rambursări pentru cheltuielile efectuate, după ce au fost modificate datele de contact;
- 5) Crearea de companii fictive/fantome care nu desfășoară operațiuni reale, ci doar simulează tranzacții pentru a genera o rambursare de TVA;
- 6) Fraudă de tip carusel, în care managerul unei companii fictive/fantome utilizează o identitate falsă sau o identitate furată;
- 7) Crearea de companii fictive/fantome care nu desfășoară operațiuni reale, dar pun în circulație bancnote deteriorate/greșite/false obținute cu identitate și documente false;
- 8) Folosirea frauduloasă a documentației furnizorilor cu care nu s-a desfășurat nici o activitate, în scopul reducerii ratei impozitului pe venit aplicabile sau generării unor pierderi fictive;
- 9) Depunerea unor sume mari de numerar transferate ulterior în alte conturi ale persoanelor juridice în mai multe țări;
- 10) Utilizarea identităților imigranților care s-au întors în țările lor de origine de către rude sau alte persoane pentru a continua să primească plăți pentru beneficii;
- 11) Nominalizarea unui cont de plăți care nu este în numele solicitantului;
- 12) Profitarea de persoanele vulnerabile pentru a obține detalii despre parola privată, accesul ilegal la sisteme și manipularea pentru obținerea avantajelor personale frauduloase;
- 13) Hoții care încearcă să obțină acces la informațiile de identificare păstrate la depozitari majori de date cu caracter personal (de exemplu, agenții guvernamentale, bănci). Acest acces poate lua forma intruziunii computerului (hacking), compromiterea angajaților cu acces autorizat la date (corupție) sau înșelăciune;
- 14) Utilizarea computerelor și a altor mijloace de înșelăciune pentru a obține informații de identificare direct de la individ (de exemplu, "phishing", "spyware" și "skimming");
- 15) Utilizarea Internetului pentru a obține informații despre companiile care efectuează vânzări pe Internet, în scopul transferării banilor din conturile acelor companii către conturile personale deschise prin utilizarea unei identități false.

X. Activități neobișnuite suspecte de finanțare a terorismului

Indicatori comportamentali:

- 1) Părțile implicate în efectuarea tranzacțiilor (inițiatorul, beneficiarul, etc.) sunt din țări suspecte și cu risc înalt în finanțarea terorismului;
- 2) Utilizarea corporațiilor false sau companiilor-fantomă (fictive);
- 3) Includerea persoanelor din listele de sancțiuni ale Consiliului de Securitate al ONU;
- 4) Surse media informează că titularul contului este afiliat organizațiilor teroriste sau este angajat în activități teroriste;
- 5) Beneficiarul efectiv al contului nu este identificat conform tuturor cerințelor;
- 6) Utilizarea persoanelor nominalizate, trusturilor, membrii familiilor sau conturile persoanelor-terțe;

- 7) Utilizarea datelor de identificare false;
- 8) Abuzuri ale organizațiilor non-profit.

Indicatori legați de tranzacții financiare:

- 1) Utilizarea fondurilor de către organizațiile non-profit nu coincide cu scopul inițial stabilit pentru aceste fonduri;
- 2) Tranzacțiile nu sunt justificate din punct de vedere economic ținând cont de activitatea economică sau profesia titularului contului;
- 3) O serie de transferuri complexe de fonduri de la o persoană către o altă persoană ce denotă camuflarea sursei fondurilor și scopul utilizării fondurilor;
- 4) Tranzacțiile nu corespund cu activitatea obișnuită derulată în cont;
- 5) Depuneri au fost efectuate în sume sub limita de raportare pentru a nu trezi suspiciuni;
- 6) Operațiunile multiple de depuneri de numerar sau retrageri care conțin referințe suspecte;
- 7) Activitate intense prin bancomate au loc în țara de reședință și internațional;
- 8) Tranzacțiile nu au sensuri economice justificate;
- 9) Activitate neobișnuită cu numerar în conturile deschise în bănci străine;
- 10) Multiple depuneri în numerar în sume mici urmate de transferuri electronice semnificative în altă țară;
- 11) Utilizarea multiplelor conturi în bănci străine.

Anexa nr.3
la Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr.din

RECOMANDĂRI

cu privire la stabilirea relațiilor transfrontaliere în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului

I. Prevederi generale

II.

1. Recomandările cu privire la stabilirea relațiilor transfrontaliere în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (în continuare – Recomandări) au ca scop oferirea unor îndrumări metodologice băncilor licențiate și prestatorilor de servicii de plată nebancari (în continuare - entități) privind aplicarea legislației în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului în procesul de încheiere a unei relații de afaceri cu o instituție corespondentă din străinătate.

2. Recomandările au ca obiect:

- a) descrierea riscurilor în cadrul relațiilor transfrontaliere;
- b) descrierea măsurilor privind cunoașterea clientului – instituție corespondentă;
- c) abordarea bazată pe risc în contextul relației de corespondență;
- d) descrierea modalităților de determinare a băncilor fictive și altor persoane juridice fictive ce prestează servicii de plată;

3. Recomandările sunt elaborate ținând cont de cele 40 Recomandări ale Grupului de Acțiune Financiară Internațională (FATF-GAFI), documentele Grupului Wolfsberg aferente relațiilor de corespondență bancară, documentele BASEL privind cunoașterea clienților și alte documente internaționale aferente domeniului dat.

4. Prezentele Recomandări nu se aplică în relație cu băncile centrale, trezoreriile centrale și autoritățile monetare din țările membre FATF-GAFI, băncile comerciale de dezvoltare regională sau internațională, cum ar fi, BERD, Fondul Monetar Internațional, Banca Mondială, etc., cel puțin în măsura în care relația cu aceste instituții implică furnizarea de servicii și produse, care sunt în conformitate cu atribuțiile și activitățile statutare ale acestora.

5. Termenii și expresiile utilizate în prezentele Recomandări au semnificațiile prevăzute în Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și actele normative emise pentru implementarea acestei legi. De asemenea, în sensul prezentelor Recomandări se utilizează următorii termeni și expresii:

instituție corespondentă – banca sau prestatorul de servicii de plată nebanca din străinătate sau orice altă persoană juridică din străinătate care prestează servicii de plată;

relație transfrontalieră (corespondentă) - furnizarea de către entitate a serviciilor și produselor sale instituției corespondente prin deschiderea unui cont de plăți sau în lipsa acestuia și oferirea altor servicii conexe, cu scopul de a gestiona lichidități, de acordare după necesitate a împrumuturilor sau efectuarea altor investiții, de a livra numerar în valută străină cu înregistrarea echivalentului în conturile corespondente deschise în alte instituții corespondente, precum și efectuarea plăților în numele clienților.

6. Respectarea recomandărilor aferent stabilirii relațiilor transfrontaliere va facilita identificarea, evaluarea și minimizarea riscurilor și vulnerabilităților aferente activității entității în relația cu instituțiile corespondente.

II. Riscuri în cadrul relațiilor transfrontaliere

Secțiunea 1 Categorii de risc

7. Relațiile transfrontaliere construite între bănci și instituțiile corespondente într-o perioadă îndelungată de timp creează un mecanism de o eficiență înaltă, care are o importanță fundamentală pentru economia globală. Acest mecanism facilitează mișcarea banilor de la o persoană sau entitate la alta și de la o țară la alta precum și asigură efectuarea operațiunilor de schimb valutar. Pentru ca această infrastructură de plăți internaționale să continue să funcționeze eficient și în același timp să asigure desfășurarea eficientă a proceselor de combatere a spălării banilor și finanțării terorismului, fiecare entitate implicată trebuie să fie responsabilă pentru efectuarea măsurilor de cunoaștere a clienților săi, precum și să monitorizeze tranzacțiile în conformitate cu reglementările aplicate, luând în considerare standardele internaționale relevante.

8. Relațiile corespondente reprezintă o afacere de volum mare, sensibilă în timp, care implică fluxuri substanțiale de bani printr-o serie de bănci sau persoane juridice ce prestează servicii de plată care nu au nici o legătură între ele și de obicei sunt situate în diferite țări. În multe cazuri, o singură parte implicată nu are o imagine completă asupra întregului flux tranzacțional. O entitate procesează tranzacții inițiate de către corespondentul său, în favoarea unei părți pe care nu o cunoaște și nu are relații directe, nefiind clienții săi, și asupra cărora, prin urmare, entitatea nu a aplicat măsuri de cunoaștere. Aceste caracteristici pot face conturile corespondentului vulnerabile la potențiale abuzuri de spălare a banilor și finanțare a terorismului și îngreunează detectarea și prevenirea activităților ilegale.

9. Fiecare relație corespondentă se recomandă să fie revizuită în funcție de performanțe, iar instituțiile implicate trebuie să implementeze adecvat legislația țării privind prevenirea și combaterea spălării banilor și finanțării terorismului. Revizuirea relațiilor transfrontaliere, presupune acordarea unei atenții deosebite factorilor care pot constitui un risc sporit privind spălarea banilor sau finanțarea terorismului, fie individual sau în combinație. Astfel de factori au fost identificați în standardele internaționale și accentul principal a fost pus pe 2 categorii de riscuri:

- a) riscul de țară (jurisdicție);
- b) riscul clientului.

10. Riscul de țară/jurisdicție trebuie evaluat prin prisma respectării relațiilor corespondente, pentru a determina potențialul risc de spălare a banilor sau finanțare a terorismului datorită unor criterii aferente statului/teritoriului. Printre criteriile care ar determina dacă o țară/jurisdicție prezintă un risc sporit de spălare a banilor și/sau finanțare a terorismului sunt:

- a) sancțiunile, embargouri, interdicțiile sau alte restricții aplicate în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;
- b) nivelul înalt al criminalității și corupției;
- c) lipsa sau existența unui cadru legal inadecvat în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;
- d) acordarea suportului activităților de terorism și organizațiilor teroriste;
- e) existența țării în lista jurisdicțiilor ce nu implementează standarde internaționale de transparență.

11. Entitatea ține cont de sediul instituției corespondente, precum și de țara al cărei rezident este beneficiarul instituției corespondente. În anumite circumstanțe specifice, riscul de țară poate include, de asemenea, o evaluare a principalelor piețe geografice acoperite de către instituția corespondentă.

12. Riscul clientului este legat fie de organizare și structura instituției corespondente, fie de natura și scopul afacerii acesteia. Unii factorii care ar putea constitui un risc sporit de spălare a banilor și finanțare a terorismului pot fi:

- a) instituția corespondentă este rezident al zonei/țării offshore și/sau desfășoară activitatea într-o zonă/țară offshore;
- b) instituția corespondentă are proprietar sau este controlată de o persoană expusă politic;
- c) instituția corespondentă oferă servicii clienților săi ce se caracterizează printr-un grad de risc sporit;
- d) instituția corespondentă este o instituție financiară nebanară, cum ar fi, oficiu de schimb valutar sau organizatorul sistemului de remitere de bani;
- e) instituția corespondentă efectuează tranzacții ce comportă un grad de risc sporit și cad sub incidența indicilor și criteriilor de suspiciune;
- f) instituția corespondentă oferă clienților săi serviciul „conturi corespondente de transfer” (payable through accounts);
- g) instituția corespondentă este o instituție financiară care oferă relații corespondente pentru alte instituții financiare (corespondenți „nested” sau „downstream”).

13. Entitatea folosește criteriile menționate mai sus pentru a-și dezvolta propriul său model de risc aferent identificării instituției corespondente pentru a-și spori măsurile aplicate de cunoaștere, control și monitorizare. Entitatea trebuie să documenteze metodele utilizate și controlul întreprins.

Secțiunea a 2-a

Abordarea bazată pe risc în contextul relației de corespondență

14. Entitatea, la stabilirea relațiilor cu instituțiile corespondente va considera următorii factori de risc relevanți pentru înțelegerea riscului de spălare a banilor și finanțare a terorismului implicat:

1. riscul inerent care rezultă din natura serviciilor furnizate, în particular:

- a) scopul serviciilor furnizate instituției respondente (ca exemplu: servicii de schimb valutar, comerț cu valori mobiliare pe piețe reglementate sau plăți în cadrul unui grup de instituții respondente din aceeași jurisdicție - pot indica asupra unui risc scăzut);
- b) dacă serviciile de corespondență vor fi utilizate prin intermediul instituțiilor financiare ce furnizează servicii de corespondență altor instituții corespondente (corespondenți „nested”), sau prin intermediul unei instituții respondente afiliate, sau prin intermediul unei a treia persoană și riscul diferit pe care aceste instituții îl impun;
- c) dacă serviciile de corespondență vor fi utilizate prin intermediul conturilor corespondente de transfer (payable through accounts), sau prin intermediul unei instituții respondente afiliate, sau prin intermediul unei a treia persoană și riscul diferit pe care aceste instituții îl impun;

2. caracteristicile sau informația despre instituția respondentă, în particular:

- a) activitățile principale de afaceri ale instituției respondente, inclusiv piețele țintă și tipul clienților deserviți;
- b) managementul și proprietarii (inclusiv beneficiarii efectivi) instituției respondente și dacă aceștia reprezintă anumit risc specific de spălare a banilor și finanțare a terorismului (de exemplu: Persoană Expusă Politic);
- c) politicile și procedurile instituției respondente de prevenire și combatere a spălării banilor și finanțare a terorismului, inclusiv descrierea măsurilor aplicate pentru cunoașterea clienților și abilitatea de a obține informații suplimentare despre natura tranzacțiilor efectuate de aceștia;
- d) dacă au fost aplicate față de instituția respondentă de către oricare instanță sau autoritate de supraveghere a sancțiunilor civile, administrative sau penale, data sancțiunii, gradul de severitate și dacă încălcările constatate au fost remediate.

3. zona geografică în care instituția respondentă operează, în particular:

- a) jurisdicția în care instituția respondentă este localizată (și compania mamă în cazul în care instituția respondentă este o subsidiară);
- b) jurisdicția în care subsidiarele și filialele grupului sunt localizate, după disponibilitate utilizând structura grupului existentă în sistemul Identificatorului Unic al Companiei, la fel și jurisdicția în care utilizatorii terți ai relațiilor de corespondență pot fi localizați;
- c) calitatea și eficiența reglementărilor și supravegherii în jurisdicția în care instituția respondentă este localizată (în special, reglementările cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului) și compania mamă, în cazul unei subsidiare a instituției respondente.

15. Se recomandă ca entitatea să ia o imagine holistică a indicatorilor enumerați mai sus și a altor informații disponibile în scopul determinării în primul rând a riscului inerent al fiecărei relații cu o instituție corespondentă, iar apoi să ia în considerare factorii de reducere a riscurilor identificați pentru a evalua riscul rezidual și gradul de gestionare al acestuia. În general, factorii care ar putea reduce riscurile de spălare a banilor și finanțare

a terorismului ar include aplicarea eficace a politicilor și procedurilor de gestionare a riscurilor în relații de corespondență, inclusiv prin adaptarea serviciilor/produselor oferite sau limitarea activității.

Secțiunea a 3-ea **Respondenții instituțiilor corespondente (corespondenți „nested”)**

16. Corespondenți „nested” se referă la utilizarea relației de corespondență de către un număr de instituții respondente prin intermediul unor instituții corespondente direct pentru efectuarea tranzacțiilor și obținerea accesului la alte servicii financiare. Acordarea serviciilor de către o instituție corespondentă altor instituții financiare respondente reprezintă o parte integrantă și în general legitimă a relațiilor de corespondență. Prin intermediul unor astfel de relații, instituțiile financiare mai mici dintr-o regiune obțin acces la sistemul financiar internațional sau facilitează tranzacțiile cu o instituție financiară cu care nu are stabilită o relație de corespondență.

17. Furnizarea accesului la instituții financiare străine terțe, care nu sunt clientul instituției corespondente, și care nu este neapărat cunoscută, poate face obscur transparența financiară și poate crește riscurile de spălare a banilor și finanțare a terorismului. Din acest considerent, entitățile ar trebui să evalueze riscul asociat clienților instituții corespondente care au relații cu alte instituții respondente. Nivelul de risc pentru fiecare instituție corespondentă în parte poate varia în funcție de natura relației dintre instituția corespondentă și alte instituții respondente, inclusiv mărimea și localizarea geografică, produsele și serviciile oferite, piețele și clienții deserviți și gradul de transparență oferit de instituția respondentă.

18. Pentru a evalua riscul de spălare a banilor și finanțare a terorismului asociat relațiilor de corespondență „nested”, se recomandă ca entitatea să înțeleagă scopul unei astfel de relații utilizând următorii factori de risc:

- a) numărul și tipul instituțiilor financiare pentru care astfel de relații respondente „nested” sunt oferite;
- b) dacă instituțiile respondente sunt localizate în aceeași jurisdicție cu instituția corespondentă sau în altă țară;
- c) dacă jurisdicția în care instituțiile respondente și zona geografică pe care acestea le deserveșc dispun de reglementări adecvate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului în conformitate cu informația disponibilă public;
- d) tipul serviciilor oferite de instituția corespondentă pentru respondenții săi;
- e) durata relației de afaceri între instituția corespondentă și respondenții săi (o relație de lungă durată permite instituției corespondente să înțeleagă bine riscul de spălare a banilor și finanțare a terorismului asociat relației cu instituția respondentă, în comparație cu o relație nouă creată);
- f) adecvarea programului instituției corespondente de cunoaștere a clienților în scopul evaluării măsurilor de prevenire și combatere a spălării banilor și finanțării terorismului aplicate de către instituția respondentă.

III. Cunoașterea clientului

19. Cunoașterea clientului - instituția corespondentă presupune aplicarea de către entitate a procesului de abordare bazată pe risc pentru identificarea instituției corespondente și a riscurilor potențiale pe care aceasta le poate genera pe parcursul desfășurării relației de afaceri. Principalii indicatori de risc descriși în capitolul II se recomandă a fi luați în considerație atât la începutul relațiilor, cât și pe durata continuă a relației de afaceri, pentru a stabili măsurile standarde sau sporite de cunoaștere ce vor fi întreprinse.

20. Clienții entității - instituțiile corespondente trebuie să fie supuse măsurilor corespunzătoare de cunoaștere în vederea asigurării faptului că entitatea va desfășura activitatea adecvat ținând cont de profilul de risc al clientului. La stabilirea relației de afaceri, pentru cunoașterea instituției corespondente, entitatea poate utiliza cel puțin „Chestionarul privind cunoașterea clientului – instituție corespondentă” (vezi Anexa nr.1 la Recomandări) și „Informațiile și documentele privind cunoașterea instituției corespondente” (vezi Anexa nr.2 la Recomandări) sau alte formate a chestionarelor la discreția acestora. Dacă instituția corespondentă activează într-un mediu supus supravegherii și reglementării adecvate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, entitatea se poate baza pe informația disponibilă publică necesară cunoașterii partenerului său.

21. Instituțiile internaționale de specialitate, cum ar fi, FATF-GAFI, Grupul Wolfsberg, Comitetul Basel pentru Supravegherea Bancară, etc., prin aprobarea documentelor și recomandărilor aferente, au enumerat un șir de măsuri care pot fi aplicate de către entitățile care stabilesc relații transfrontaliere.

22. În cadrul relațiilor corespondente, datorită volumului și vitezei tranzacțiilor, iar în unele cazuri datorită lipsei informațiilor specifice sau complete privind clienții corespondenți și beneficiarii efectivi ai tranzacției, monitorizarea tranzacțiilor instituției este mai dificilă decât pentru alte afaceri ce implică relații directe cu clienții. Astfel, pentru îmbunătățirea procesului de monitorizare continuă a tranzacțiilor prin conturile corespondente, poate fi utilizată regula ce presupune stabilirea limitelor valorice pentru tranzacții, iar depășirea acestor limite duce la o examinare minuțioasă a scopului și naturii tranzacțiilor, oferind posibilitatea identificării potențialelor tranzacții neordinare și suspecte.

23. Rezultatul monitorizării tranzacțiilor se observă când entitatea aplică sistemul său astfel încât instituția corespondentă ce prezintă un risc sporit să fie supusă monitorizării în primul rând.

24. Responsabilitatea primară pentru măsurile de cunoaștere privind acceptarea clienților și monitorizarea continuă a relațiilor corespondente, trebuie să se afle sub controlul unei subdiviziuni sau persoane identificate în mod clar. Acest lucru oferă posibilitatea definirii anumitor parametri și reguli aferent tranzacțiilor efectuate, precum și instituie posibilitatea introducerii unor restricții asupra diverselor tipuri de tranzacții și/sau asupra unor sume sau volume și/sau privind implicarea în tranzacții cu anumite țări pentru o perioadă determinată /nedeterminată de timp, cu scopul de a se conforma activității și legislației aferente.

25. Monitorizarea tranzacțiilor este un proces dificil, iar utilizarea indicilor de suspiciune facilitează cunoașterea posibilelor tranzacții suspecte. În acest sens, pentru transferurile în sume deosebit de mari și / sau în volume/ frecvențe deosebit de mari pot fi considerați următorii indici:

- a) tranzacțiile implică țările cu un grad de risc sporit, vulnerabile la spălarea banilor și finanțării terorismului;
- b) tranzacțiile implică băncile fictive sau persoanele juridice fictive ce prestează servicii de plată;
- d) tranzacțiile includ frecvent sume care sunt mai mici decât limitele interne proprii de monitorizare sau limitele stabilite de legislația aferentă;
- e) tranzacțiile implică conturi care operează în mod semnificativ în afara limitelor, bazate fie pe informațiile colectate în baza măsurilor de cunoaștere, fie în baza comportamentului anterior privind activitatea preconizată;
- f) tranzacțiile se efectuează prin mai multe țări diferite sau prin mai multe instituții financiare înainte sau după implicarea entității, fără nici un scop evident, altul decât cel de a ascunde natura, sursa, proprietatea sau controlul asupra mijloacelor bănești;
- g) tranzacțiile au următoarele caracteristici sau caracteristici combinate, așa ca, transferurile repetate de la un anumit inițiator către un anumit beneficiar, și/sau transferurile electronice individuale efectuate într-o perioadă scurtă de timp, cum ar fi transferurile zilnice, de două ori pe zi sau în fiecare altă zi.
- h) alți factori de risc.

26. Entitatea promovează o politică generală în relațiile corespondente de susținere a sistemului de plăți internaționale și a comerțului internațional fără a prejudicia interesul comercial al clienților și instituției corespondente. Totuși, entitatea va evita stabilirea relațiilor corespondente ce prezintă un risc sporit și /sau sunt interzise, cum ar fi relațiile cu:

- a) băncile fictive sau persoanele juridice fictive ce prestează servicii de plată;
- b) instituțiile financiare neautorizate sau nereglementate;
- c) instituțiile corespondente care în momentul aplicării măsurilor de cunoaștere produc incertitudini semnificative;
- d) instituțiile corespondente care nu dispun de măsuri privind prevenirea și combaterea spălării banilor și finanțării terorismului sau măsurile sunt considerate inadecvate și/sau insuficiente, fapt care în consecință nu permite realizarea adecvată a prevederilor legislației naționale în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

27. În cadrul monitorizării continue a tranzacțiilor, dacă există îndoieli apărute ca urmare a analizei alertelor privind tranzacțiile suspecte generate, instituția corespondentă ar putea solicita informații suplimentare privind tranzacțiile instituției respondente. În astfel de situații, persoana responsabilă din cadrul entității trebuie să fie informată regulat despre riscul relației de corespondență și rezultatele monitorizării.

28. Înainte de a decide retragerea dintr-o relație corespondentă, entitatea poate lua în considerare aplicarea măsurilor suplimentare, cum ar fi: limitarea serviciilor furnizate, monitorizarea în timp real și testarea prin eșantion a tranzacțiilor sau vizitele la fața locului.

IV. Determinarea băncii fictive sau persoanei juridice fictive ce prestează servicii de plată

29. O entitate sau persoană juridică ce prestează servicii de plată și este considerată fictivă impune un risc sporit de spălare a banilor și finanțare a terorismului.

30. Administrația unei astfel de bănci sau persoane juridice fictive ce prestează servicii de plată se poate afla în altă țară decât cea unde își desfășoară activitatea și deseori poate avea oficii într-o societate asociată sau în reședințe private. De obicei, o entitate sau persoană juridică ce prestează servicii de plată poate păstra legătura doar cu un agent privat de înregistrare a persoanei juridice, care nu cunoaște nimic referitor la activitatea și operațiunile zilnice ale acesteia, și furnizează, la cerere numai informație privind adresa de înregistrare a băncii sau persoanei juridice ce prestează servicii de plată. Structuri cu particularitățile enumerate se găsesc de obicei în zonele / țărilor offshore sau alte jurisdicții netransparente.

31. O entitate sau persoană juridică fictivă ce prestează servicii de plată nu este afiliată unui grup financiar reglementat. Totodată, administrarea instituției poate fi situată în altă țară. Respectiv, o autoritate de supraveghere nu are capacitatea de a verifica aceasta instituție, prin organizarea de inspecții pe teren sau purtarea discuțiilor cu conducerea instituției, în conformitate cu practicile internaționale. La fel, se cunoaște că băncile sau persoanele juridice fictive ce prestează servicii de plată adeseori au fost implicate în activități ilegale sau tranzacții financiare suspecte. În această ordine de idei, băncile sau persoanele juridice fictive ce prestează servicii de plată impun bariere serioase la efectuarea unei supravegheri adecvate, și nu există condiții speciale care ar putea fi implementate pentru obținerea unei supravegheri legale efective.

32. Pentru o cunoaștere adecvată a instituțiilor corespondente și determinarea băncii sau persoanei juridice fictive ce prestează servicii de plată, în scopul neadmiterii stabilirii relației de afaceri sau efectuării de tranzacții, entitatea atrage atenția la următoarele particularități de bază caracteristice acestor instituții:

- a) lipsa activității la o adresa fixă;
- b) desfășurarea activității / tranzacțiilor în altă țară decât cea în care a fost licențiată;
- c) lipsa personalului angajat;
- d) lipsa totală/parțială a evidenței contabile;
- e) lipsa supravegherii din partea autorităților de supraveghere a entităților vizate.
- f) lipsa licenței de activitate.

V. Informația ce acompaniază mesajul la transferurile de fonduri

33. Entitatea va stabili în politicile și procedurile interne prioritățile pentru informațiile care urmează a fi transmise ca parte a instrucțiunii de plată atunci când acționează ca entitate inițitoare/intermediară a plății/transferului. Informațiile completate sunt importante dat fiind scopul utilizării acestora, de exemplu, informația despre numele și adresa plătitorului sunt utilizate la monitorizarea în timp real și post factum a plăților/transferurilor, iar informația despre țara plătitorului/beneficiarului este importantă

în contextul înțelegerii riscului de spălare a banilor și finanțare a terorismului implicat și existența sancțiunilor.

34. Entitatea va urmări realizarea următoarelor standarde care vizează informația ce acompaniază mesajul la transferurile de fonduri:

a) entitatea nu ar trebui să omită, să șteargă sau să modifice informațiile din mesaje sau ordinele de plată în scopul de a evita detectarea acestor informații de către orice altă instituție financiară în procesul de plată;

b) entitatea nu ar trebui să utilizeze niciun mesaj special de plată pentru a evita detectarea de informații de către orice altă instituție financiară în procesul de plată;

c) entitatea ar trebui să coopereze cât mai deplin posibil cu alte instituții financiare în procesul de plată atunci când li se solicită să furnizeze informații despre părțile implicate;

d) entitatea ar trebui să încurajeze și alte instituții corespondente să respecte aceste standarde.

35. Entitatea va urmări realizarea standardelor menționate la pct.34 în următoarele cazuri:

a) la efectuarea tranzacțiilor transfrontaliere;

b) la efectuarea tranzacțiilor domestice, în măsura în care infrastructura domestică permite acest lucru;

c) la efectuarea tranzacțiilor în toate valutele;

d) la efectuarea tuturor tranzacțiilor, fără excepție de limite/praguri utilizate;

e) la efectuarea tranzacțiilor de către entitate inițitoare, intermediară și beneficiară a plății.

36. Entitatea la utilizarea infrastructurii de plată care limitează cantitatea de informații care poate fi inclusă în mesajul de plată, vor considera următoarele principii de completare a mesajului de plată:

a) numele titularului principal al contului ar trebui să fie completat integral înaintea furnizării informațiilor despre deținătorul secundar al contului, iar numele de familie trebuie să primească o prioritate față de prenumele clientului;

b) informațiile despre adresa clientului trebuie furnizate în cea mai mare măsură posibilă. Țara trebuie să primească o prioritate în acest sens, după care va urma orașul/regiunea/municipiul/strada/ numărul blocului și codul poștal. Transmiterea numelui și a adresei complete pentru titularul principal al contului ar trebui să aibă prioritate;

c) informațiile despre beneficiarul efectiv al clientului ar trebui să fie cuprinse în rubrica despre inițiatorul plății, iar în cazul existenței limitării din partea infrastructurii de plată, entitatea va acționa conform mecanismului descris în politicile interne;

d) în cazul în care sistemul / infrastructura de plată prevede utilizarea unui format structurat care contribuie la colectarea deplină de informații, entitatea inițitoare a plății va da prioritate acestui format.

Anexa nr.1

la Recomandările cu privire la stabilirea relațiilor transfrontaliere
în contextul legislației cu privire la prevenirea și combaterea
spălării banilor și finanțării terorismului

N/O	Chestionarul cunoaște-ți clientul – instituție corespondentă	Răspuns	
Date despre instituția corespondentă și structura de proprietate a acesteia			
1.	Denumirea deplină a instituției corespondente		
2.	Adresa juridică / Adresă de afaceri primară		
3.	Data înregistrării instituției		
4.	Tipul de proprietate și reprezentarea grafică a structurii de proprietate, dacă este disponibilă		
5.	Numele complet al beneficiarului efectiv și țara de reședință al acestuia		
6.	Instituția este constituită din acțiuni la purtător? Dacă da, care este mărimea cotei formată din acțiuni la purtător	Da	Nu
7.	Instituția sau oricare dintre sucursalele sale operează sub o licență offshore? Dacă Da, furnizați numele sucursalei.	Da	Nu
8.	Denumirea autorității de reglementare și supraveghere financiară primară		
9.	Furnizați Identificatorul unic al companiei (LEI), dacă este disponibil		
10.	Domeniile de activitate ale instituției.		
11.	Total active (mil.Euro)		
12.	Numărul de angajați		
13.	Instituția deține o bază semnificativă (10% sau mai mult) de clienți nerezidenți, inclusiv rezidenți ai zonelor off-shore. Dacă DA, furnizați detalii despre țară și cota deținută.	Da	Nu
14.	Dacă este cazul, furnizați informații suplimentare în legătură cu răspunsurile la întrebările secțiunii date.		
Produse și Servicii oferite de Instituție			
15.	Enumerați produsele și serviciile oferite de instituție		
16.	Instituția oferă servicii de corespondență? Dacă da, pentru ce categorii de instituții financiare (locale și/sau străine)?	Da	Nu
17.	Instituția permite altor instituții corespondente (locale și/sau străine) să stabilească relații interconectate (nested sau downstream relations)?	Da	Nu
18.	Instituția oferă produsul - Conturi corespondente de transfer	Da	Nu
19.	Deține instituția politici și proceduri pentru identificarea relațiilor corespondente interconectate?	Da	Nu
20.	Instituția oferă produsul - Relații bancare private (local și/sau internațional)	Da	Nu

21.	Instituția oferă produsul - Finanțarea comerțului	Da	Nu
22.	Instituția oferă produsul - Safeuri individuale	Da	Nu
23.	Instituția oferă produsul - Livrare de numerar în vrac	Da	Nu
24.	Instituția oferă produsul - Sisteme de depozitare a cecurilor la distanță	Da	Nu
25.	Instituția oferă produsul - Valută digitală/ virtuală	Da	Nu
26.	Instituția oferă produsul - Comerț cu valori mobiliare de valoare reduse	Da	Nu
27.	Instituția oferă produsul - Păstrarea corespondenței	Da	Nu
28.	Instituția oferă produsul - Remitențe peste hotare	Da	Nu
29.	Instituția oferă produsul - Servicii pentru clienții ocazionali (care nu dețin conturi)	Da	Nu
30.	Instituția oferă produsul - Alte produse și servicii ce implică un risc înalt Dacă da, enumerați-le.	Da	Nu
31.	Dacă este cazul, furnizați informații suplimentare în legătură cu răspunsurile la întrebările secțiunii date.		
Politici, Proceduri și Controale privind prevenirea și combaterea spălării banilor și finanțării terorismului			
32.	Sunt politicile și procedurile instituției corespondente privind prevenirea și combaterea spălării banilor și finanțării terorismului aprobate de către membrii consiliului instituției sau a altui organ de conducere superior?	Da	Nu
33.	Conțin politicile și procedurile, aprobate regulamentar, cerințe privind existența în cadrul instituției corespondente a unei persoane responsabile în domeniul dat, precum și responsabilitățile acestuia?	Da	Nu
34.	Conțin politicile și procedurile, aprobate regulamentar, cerințe scrise ce documentează procesele necesare pentru prevenirea, detectarea și raportarea tranzacțiilor suspecte?	Da	Nu
35.	Suplimentar la controlul efectuat de autoritățile de supraveghere și reglementare, are instituția corespondentă stabilită o funcție de audit internă sau o persoană terță independentă pentru a evalua sistematic politicile, procedurile și practicile privind prevenirea și combaterea spălării banilor și finanțării terorismului?	Da	Nu
36.	Deține instituția corespondentă politici care reglementează relațiile cu persoanele expuse politic în concordanță cu cele mai bune practici?	Da	Nu
37.	Dispune instituția corespondentă proceduri privind păstrarea înregistrărilor și informației aferente clienților și tranzacțiilor acestora? Dacă da, pentru ce perioadă?	Da	Nu

38.	Sunt politicile, procedurile și practicile instituției corespondente în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului aplicate tuturor filialelor și subdiviziunilor ei atât în țară cât și peste hotare?	Da	Nu
39.	Sunt politicile și procedurile actualizate cel puțin anual?	Da	Nu
40.	Deține instituția politici și proceduri care prevăd:		
a)	Interzicerea deschiderii și deținerii conturilor anonime sau sub nume fals?	Da	Nu
b)	Interzicerea deschiderii și deținerii conturilor pentru instituții financiare nelicențiate?	Da	Nu
c)	Interzicerea stabilirii relațiilor cu alte entități care prestează servicii instituțiilor nelicențiate?	Da	Nu
d)	Interzicerea conturilor/ relațiilor de afaceri cu firme-fantomă	Da	Nu
e)	Interzicerea stabilirii relațiilor de afaceri cu alte instituții care prestează servicii firmelor-fantomă	Da	Nu
f)	Terminarea relațiilor existente cu clienții săi, urmare determinării riscului de implicare a acestora în operațiuni de spălare a banilor și finanțare a terorismului?	Da	Nu
41.	Deține instituția politici, proceduri și procese adecvate în scopul completării depline a mesajelor care însoțesc transferurile de fonduri (pentru plătitor: numele, numărul de cont și adresa, numărul actului de identitate, IDNP sau datași locul nașterii; pentru beneficiar: numele și numărul de cont)?	Da	Nu
Evaluarea riscului			
42.	Practică instituția corespondentă o abordare bazată pe risc a clienților săi și tranzacțiilor efectuate de aceștia?	Da	Nu
43.	Dispune și aplică instituția corespondentă cerințe privind măsurile de precauție sporită față de categoriile de clienți și tranzacții cu grad de risc sporit efectuate prin intermediul instituției sau care sunt considerate că impun riscuri sporite datorită activităților ilicite?	Da	Nu
44.	Evaluează instituția riscul asociat următoarelor:		
a)	Clientului	Da	Nu
b)	Produsului/Serviciului	Da	Nu
c)	Canalului de distribuție	Da	Nu
d)	Zonei Geografice	Da	Nu
45.	A fost efectuată evaluarea riscului în domeniul PCSBFT la nivel de instituție în ultimele 12 luni?	Da	Nu
	Dacă NU, furnizați data ultimei evaluării riscului la nivel de instituție în domeniul PCSBFT?		
Regulile cunoaște-ți clientul, măsurile de precauție standard și sporite			
46.	Dispune instituția corespondentă de un sistem implementat aferent cunoașterii clienților persoane fizice și juridice?	Da	Nu

47.	Care din următoarele elemente acumulează și păstrează entitatea la aplicarea cerințelor de cunoaștere a clienților:		
a)	Structura proprietății	Da	Nu
b)	Identificarea clientului (nume, prenume, IDNP/IDNO, adresa domiciliu/reședință, etc.)	Da	Nu
c)	Identificarea beneficiarului efectiv (nume, prenume, IDNP, adresa domiciliu/reședință, etc.)	Da	Nu
d)	Identificarea administratorului/persoanei împuternicite de a gestiona activitatea clientului (nume, prenume, IDNP, adresa domiciliu/reședință etc.)	Da	Nu
e)	Natura și scopul activității	Da	Nu
f)	Scopul și natura relației / informație privind scopul preconizat de utilizare a contului	Da	Nu
g)	Natura activității/angajării /funcția publică deținută	Da	Nu
h)	Produsul și serviciul solicitat	Da	Nu
i)	Sursa fondurilor	Da	Nu
j)	Sursa averii	Da	Nu
47.	Dispune instituția corespondentă de un sistem implementat aferent verificării informației despre clienți și beneficiarii efectivi ai acestora?	Da	Nu
48.	Are instituția o abordare bazată pe risc pentru verificarea clienților din punct de vedere al surselor mass-media nefavorabile/știri negative? Dacă da, acest proces se inițiază la: stabilirea relației de afaceri/ reînnoirea datelor / alt eveniment declanșator	Da	Nu
49.	Care este metoda utilizată de instituție pentru verificarea surselor mass-media nefavorabile/știri negative		
a)	Automatizat	Da	Nu
b)	Manual	Da	Nu
c)	Combinat automatizat și manual	Da	Nu
50.	Aplică instituția corespondentă măsurile de precauție sporită față de clienții săi sau tranzacțiile acestora catalogate cu grad de risc sporit?	Da	Nu
51.	Din lista de mai jos, care categorii de clienți sau industrii se supun măsurilor de precauție sporite și/sau sunt interzise prin politicile entității?		
a)	Clienți fără cont	Da/Nu	Interzis
b)	Clienți din zone off-shore	Da/Nu	Interzis
c)	Instituții fantome/fictive	Da/Nu	Interzis
d)	Clienți care acordă servicii de transfer de bani sau de schimb valutar	Da/Nu	Interzis
e)	Persoane Expuse Politic/ membrii familiilor PEP/ persoane asociate PEP	Da/Nu	Interzis
f)	Instituții corespondente	Da/Nu	Interzis
g)	Arme, apărare, servicii militare	Da/Nu	Interzis

h)	Industria extractivă	Da/Nu	Interzis
i)	Metale și pietre prețioase	Da/Nu	Interzis
j)	Organizații de caritate nereglementate	Da/Nu	Interzis
k)	Organizații de caritate reglementate	Da/Nu	Interzis
l)	Organizații non-guvernamentale	Da/Nu	Interzis
m)	Monede virtuale	Da/Nu	Interzis
n)	Droguri/Marijuana	Da/Nu	Interzis
o)	Ambasade/Consulate	Da/Nu	Interzis
p)	Jocurile de noroc	Da/Nu	Interzis
q)	Prestatori de servicii de plată	Da/Nu	Interzis
r)	Altele (specificați)	Da/Nu	Interzis
Raportarea tranzacțiilor, prevenirea și detectarea tranzacțiilor suspecte			
52.	Deține instituția corespondentă politici și proceduri pentru identificarea și raportarea tranzacțiilor suspecte sau care depășesc limitele legale de raportare către autoritatea competentă?	Da	Nu
53.	Deține instituția corespondentă proceduri de identificare a tranzacțiilor structurate efectuate pentru evitarea cerințelor de raportare a sumelor mari în numerar?	Da	Nu
54.	Verifică instituția corespondentă tranzacțiile clienților săi care prezintă pentru instituție un risc sporit (cum ar fi, tranzacțiile cu persoane, entități sau țări care sunt catalogate cu grad de risc sporit)? Astfel de procedură se utilizează și până la efectuarea tranzacției?	Da	Nu
		Da	Nu
Monitorizarea tranzacțiilor și activităților			
55.	Deține instituția corespondentă un program de monitorizare a activităților neordinare sau suspecte? Prevede programul de monitorizare cerințe privind acumularea documentelor justificative la efectuarea tranzacțiilor?	Da	Nu
		Da	Nu
56.	Care este metoda utilizată de entitate pentru a monitoriza tranzacțiile și activitățile clientului?		
a)	Automatizat	Da	Nu
b)	Manual	Da	Nu
c)	Combinat automatizat și manual	Da	Nu
57.	Are instituția politici, proceduri sau alte metode de control concepute în mod rezonabil pentru a interzice și/sau a detecta acțiunile întreprinse pentru evitarea interdicțiilor de aplicare a sancțiunilor (cum ar fi: eliminarea sau repetarea și/sau mascarea, sancțiunilor aplicate?)	Da	Nu
58.	Își examinează instituția clienții, inclusiv beneficiarul efectiv, în momentul stabilirii relației de afaceri și efectuării tranzacțiilor, în mod regulat, în raport cu listele persoanelor și grupurilor	Da	Nu

	asupra cărora sunt aplicate sancțiuni sau alte restricții internaționale?		
59.	Care este metoda utilizată de instituție la monitorizarea categoriilor de persoane menționate la pct.58?		
a)	Manual	Da	Nu
b)	Automatizat	Da	Nu
c)	Combinat automatizat și manual	Da	Nu
60.	Selectează listele de sancțiuni utilizate de instituție în procesul său de verificare:		
a)	Lista consolidată de sancțiuni a Consiliului de Securitate al Organizației Națiunilor Unite	Da	Nu
b)	Lista consolidată a Oficiului de Control al activelor străine al Departamentului de Trezorerie al Statelor Unite (OFAC)	Da	Nu
c)	Lista consolidată a Uniunii Europene	Da	Nu
d)	Liste consolidată a statelor membre ale G7	Da	Nu
e)	Altele (specificați)		
Programul Anti Frauda și Corupției			
61.	Deține instituție politici și proceduri privind reglementarea, prevenirii și raportarea a actelor de corupției și fraudă?	Da	Nu
62.	Include acesta cerințe privind mecanismul de interacțiune cu persoane publice?	Da	Nu
63.	Include acesta interzicerea falsificării jurnalelor și registrelor, care documentează primirea cadourilor sau declararea fraudelor?	Da	Nu
64.	Implementează instituția măsuri de monitorizarea a eficienței programului său în domeniul combaterii fraudei și corupției?	Da	Nu
65.	Efectuează instituția o evaluare general a riscurilor de fraudă și corupție? Dacă DA, care este frecvența?	Da	Nu
66.	Funcția de audit a instituției sau altei părți terțe acoperă politicile și procedurile în domeniul combaterii corupției și fraudei?	Da	Nu
67.	Organizează instituția instruire/seminare în acest domeniul pentru angajații săi?	Da	Nu
68.	Dacă este cazul, furnizați informații suplimentare în legătură cu răspunsurile la întrebările secțiunii date.		
Altă informație			
69.	Desfășoară instituția corespondentă instruire în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului?	Da	Nu
70.	Păstrează instituția corespondentă înregistrările sesiunii de instruire ce include atât informație aferentă prezenței personalului cât și materialele folosite?	Da	Nu
71.	Dispune instituția corespondentă de politici menite să comunice personalului noile reglementari aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului?	Da	Nu

72.	Contractează instituția corespondentă serviciile unei părți terțe pentru aplicarea oricăror măsuri aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului? Dacă da, sunt instruiți personalul părții terțe aferent domeniului dat?	Da	Nu
		Da	Nu
73.	Au fost aplicate sancțiuni de către autoritățile de supraveghere sau alte autorități, în ultimii 3 ani, față de instituția corespondentă aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului? Dacă da, detaliați despre sancțiunile aplicate.	Da	Nu

Anexa nr.2
la Recomandările cu privire la stabilirea relațiilor transfrontaliere
în contextul legislației cu privire la prevenirea și combaterea
spălării banilor și finanțării terorismului

Informațiile și documentele privind cunoașterea instituției corespondente

1. „Chestionarul privind cunoașterea clientului – instituție corespondentă” (vezi Anexa nr.1);
2. Obținerea unei copii recente a politicilor și procedurilor privind prevenirea și combaterea spălării banilor și finanțării terorismului, dacă este necesar;
3. Biografiile succinte ale membrilor consiliului și executivului instituției corespondente, precum și speciemenle de semnături ale acestora;
4. Lista proprietarilor care dețin dreptul la vot de 10 la sută sau mai mult din numărul valorilor mobiliare emise și lista beneficiarilor efectivi;
5. Ultimul raport financiar anual al instituției corespondente;
6. Copia licenței instituției corespondente și amprenta ștampilei, după caz;
7. Copiile documentelor de constituire, cum ar fi, statutul instituției, contractul de constituire și certificatul de înregistrare;
8. Extrasul din Registrul de stat privind înregistrarea instituției corespondente.