# NOTA DE FUNDAMENTARE

**la proiectul hotărârii Comitetului executiv al Băncii Naționale a Moldovei pentru aprobarea Regulamentului privind reziliența operațională digitală a sectorului financiar**

| **1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ** |
|---|
| Autorul proiectului de act normativ este Banca Națională a Moldovei (BNM) |
| **2. Condițiile ce au impus elaborarea proiectului actului normativ** |
| 2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ |
| Proiectul a fost elaborat în temeiul art. 5 alin. (1) lit. d), m) și p), art. 11 alin. (1) și art. 27 alin. (1) lit. c) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 38² alin. (6) din Legea nr. 202/2017 privind activitatea băncilor, art. 32¹ alin. (3) și art. 32² alin. (3) din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică și pct. 95 (acțiunea 81) din anexa A aferentă Capitolului 9, cluster 2, din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025.<br>Proiectul pune în aplicare parțial Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar (DORA), în cadrul procesului de armonizare a legislației naționale cu legislația Uniunii Europene desfășurat potrivit Hotărârii Guvernului nr. 497/2026. |
| 2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative |
| Activitatea entităților financiare depinde în măsură tot mai mare de tehnologia informației și comunicațiilor (TIC). Incidentele cibernetice și operaționale pot întrerupe serviciile financiare și se pot propaga în sistemul financiar. Preambulul DORA (considerentele (1)-(3) și (8)-(12)) descrie aceleași probleme la nivelul Uniunii: dependența critică a serviciilor financiare de TIC, riscul ca incidentele locale să se propage în întregul sistem financiar și lipsa unui cadru cuprinzător privind riscurile TIC, cu lacune în raportarea incidentelor, în testarea rezilienței operaționale digitale și în monitorizarea riscurilor generate de părți terțe. În Uniune, DORA se aplică de la 17 ianuarie 2025.<br>Cadrul național actual este fragmentat. Regulamentul privind cerințele minime pentru gestionarea riscurilor aferente tehnologiei informației și comunicațiilor, securității informației și continuității activității, aprobat prin Hotărârea Comitetului executiv al Băncii Naționale a Moldovei (BNM) nr. 29/2025 (Regulamentul BNM nr. 29/2025), se aplică doar prestatorilor de servicii de plată (bănci, societăți de plată, societăți emitente de monedă electronică și furnizori de servicii poștale). Pentru asigurători, reasigurători și intermediarii în asigurări nu există cerințe TIC dedicate, ci doar cerințe generale privind managementul riscurilor, inclusiv al riscurilor operaționale (art. 38 din Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare).<br>Lipsesc testarea avansată bazată pe amenințări (TLPT), cerințele privind registrul acordurilor cu furnizorii terți de servicii TIC și dispozițiile contractuale minime, precum și o raportare unitară a incidentelor pentru toate entitățile supravegheate de BNM.<br>Legea nr. 48/2023 privind securitatea cibernetică, care transpune parțial Directiva (UE) 2022/2555 (NIS 2), stabilește cerințe pentru furnizorii de servicii identificați de autoritatea competentă. În raport cu Directiva NIS 2, DORA constituie regimul sectorial pentru entitățile financiare (art. 1 alin. (2) și considerentul (16)), iar proiectul pregătește acest regim la nivel național. |

**3. Obiectivele urmărite și soluțiile propuse**

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul urmărește ca, de la 1 ianuarie 2029, toate entitățile supravegheate de BNM care intră în domeniul de aplicare să aplice un cadru unitar de reziliență operațională digitală, aliniat la DORA, care preia și cerințele naționale din Regulamentul BNM nr. 29/2025. Regulamentul are nouă capitole:

Capitolul I: obiectul, domeniul de aplicare (bănci, societăți de plată, prestatori de servicii de informare cu privire la conturi, societăți emitente de monedă electronică, societăți de asigurare și de reasigurare, intermediari în asigurări și în reasigurări care nu sunt întreprinderi mici și mijlocii), definițiile și principiul proporționalității;

Capitolul II: gestionarea riscurilor TIC (guvernanță, ofițerul de securitate a informației, cadrul de gestionare a riscurilor, identificare, protecție și prevenire, detectare, răspuns și recuperare, copii de rezervă, centre de date, învățăminte și comunicare în situații de criză);

Capitolul III: gestionarea, clasificarea și raportarea incidentelor majore legate de TIC prin Platforma centrală de schimb de informații (PCSI), cu notificare inițială până la sfârșitul zilei lucrătoare, raport intermediar și raport final;

Capitolul IV: programul de testare, testele de penetrare obligatorii cel puțin o dată la 3 ani, TLPT pentru entitățile identificate de BNM și informarea anuală a BNM;

Capitolul V: gestionarea riscurilor generate de furnizorii terți de servicii TIC (strategie, registru de informații, evaluare prealabilă, dispoziții contractuale, strategii de ieșire);

Capitolele VI-IX: schimbul de informații, cooperarea cu Agenția pentru Securitate Cibernetică, sancțiunile și secretul profesional (prin trimitere la legile sectoriale) și protecția datelor.

Elementele noi față de cadrul actual sunt registrul de informații privind acordurile cu furnizorii terți de servicii TIC, programul de testare a rezilienței operaționale digitale, TLPT, clasificarea incidentelor și raportarea unitară a incidentelor majore, dispozițiile contractuale minime, strategiile de ieșire și, pentru bănci, analiza evenimentelor de securitate cu tehnici de inteligență artificială. Pentru asigurători, reasigurători și intermediarii în asigurări, toate cerințele sunt noi.

Principalele opțiuni de reglementare:

a) excepțiile prevăzute de DORA pentru microîntreprinderi sunt preluate, noțiunea fiind definită prin trimitere la Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii, iar cerințele preluate din Regulamentul BNM nr. 29/2025 se aplică și microîntreprinderilor;

b) cerințele privind centrele de date, conexiunile și echipamentele (pct. 70-75) se aplică băncilor, societăților de plată și societăților emitente de monedă electronică, cărora li se aplică și în prezent, dar nu și prestatorilor care oferă doar servicii de informare cu privire la conturi;

c) incidentul care a dus la indisponibilitatea totală a serviciilor TIC care sprijină funcții critice sau importante pentru mai mult de 3 ore, dacă funcția nu a putut fi asigurată prin soluții alternative, se consideră, în orice caz, major, în lipsa pragurilor stabilite la nivelul Uniunii prin standarde tehnice. Întreruperile repetate din aceeași cauză în 24 de ore se cumulează, iar indisponibilitatea planificată și anunțată nu se ia în calcul;

d) elementele esențiale din standardele tehnice ale Uniunii, precum termenele de raportare a incidentelor, sunt prevăzute direct în regulament;

e) sancțiunile și secretul profesional se aplică potrivit legilor sectoriale și Legii nr. 548/1995, la care regulamentul face trimitere;

f) Regulamentul BNM nr. 29/2025 rămâne aplicabil doar furnizorilor de servicii poștale. Pentru continuitatea informării anuale, băncile, societățile de plată și societățile emitente de monedă electronică transmit informațiile pentru anul 2028 potrivit pct. 135, până la 31 ianuarie 2029 (pct. 3 din hotărâre). Din cele 199 de prevederi ale sale, 164 sunt preluate în proiect și 10 parțial, iar celelalte 25 privesc domeniul de aplicare, competențe ale BNM stabilite prin lege, noțiuni folosite fără definiție sau detalii de organizare internă.

**Prevederi cu specific național.** Proiectul conține 35 de prevederi fără corespondent în DORA, dintre care 33 sunt preluate din Regulamentul BNM nr. 29/2025:

a) definițiile sistemelor și serviciilor TIC critice, momentului obiectiv pentru restabilire, perioadei maxime de întrerupere tolerabile și timpului obiectiv pentru restabilire (subpct. 3.25, 3.27, 3.38 și 3.43), folosite de cerințele privind continuitatea activității și copiile de rezervă;

b) funcția de ofițer de securitate a informației (pct. 9) și înregistrarea în PCSI a materialelor și a deciziilor organului de conducere în domeniul TIC (pct. 10);

c) planificarea performanței și a capacității sistemelor și gestiunea proiectelor TIC, de securitate a informației și de continuitate a activității (pct. 24-29);

d) măsurile tehnice de securitate, adică scanarea periodică a vulnerabilităților, configurările de securitate de referință, segmentarea rețelei interne, protecția echipamentelor conectate la rețea, monitorizarea informațiilor care părăsesc rețeaua internă (pct. 44-48) și sistemele de operare cu suport din partea producătorului (pct. 77);

e) instruirea personalului privind continuitatea activității (pct. 55) și punerea în aplicare, în coordonare cu BNM, a planurilor de continuitate de către entitățile desemnate (pct. 61 și 62);

f) schema copiilor de rezervă, retenția informației și a jurnalelor de audit, actualitatea datelor contabile și copia de rezervă lunară păstrată offline sau imutabil (pct. 64, 68, 69 și 76);

g) cerințele minime pentru centrele de date, conexiuni și echipamente (pct. 70-75);

h) monitorizarea și gestionarea problemelor (pct. 95);

i) raportarea incidentelor majore prin PCSI (pct. 106), care nu provine din Regulamentul BNM nr. 29/2025;

j) informarea anuală a BNM privind testele, scanările și evaluările efectuate (pct. 135);

k) analiza evenimentelor de securitate cu tehnici de inteligență artificială, ca nivel suplimentar de control, de către bănci (subpct. 49.1-49.5), care nu provine din Regulamentul BNM nr. 29/2025.

Aceste prevederi sunt incluse din trei motive. În primul rând, ele se aplică deja prestatorilor de servicii de plată prin Regulamentul BNM nr. 29/2025, iar renunțarea la ele ar coborî nivelul actual al cerințelor. În al doilea rând, ele detaliază cerințele generale din capitolele II-IV ale DORA (gestionarea riscurilor TIC, gestionarea incidentelor și testarea), pe care Uniunea le detaliază prin standarde tehnice care nu se preiau ca atare. În al treilea rând, ele reflectă specificul național: PCSI ca platformă de raportare și punerea în aplicare a planurilor de continuitate în coordonare cu BNM. Cerința de la lit. k) a fost introdusă după consultarea publică. Volumul evenimentelor colectate potrivit pct. 43 depășește capacitatea de analiză manuală, iar regulile de corelare definite explicit nu surprind atacurile desfășurate lent, cu credențiale valide sau prin evenimente care, luate separat, par legitime. Cerința detaliază art. 10 din DORA și se aplică doar băncilor, având în vedere volumul evenimentelor și expunerea lor. Prelucrarea are loc în infrastructura băncii sau a grupului, ca evenimentele, care conțin date cu caracter personal și informații despre vulnerabilități, să rămână sub controlul băncii. Prevederile nu contravin DORA. La aderare, ele se reexaminează în raport cu DORA și cu standardele tehnice ale Uniunii, care vor deveni direct

aplicabile.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Au fost analizate următoarele opțiuni alternative:

a) lipsa intervenției, respinsă deoarece asigurătorii, reasigurătorii și intermediarii ar rămâne fără cerințe TIC dedicate, ar lipsi TLPT, registrul de informații și dispozițiile contractuale minime, iar cadrul național s-ar îndepărta de cel al Uniunii înainte de aderare;

b) completarea Regulamentului BNM nr. 29/2025, respinsă deoarece ar menține fragmentarea, regulamentul aplicându-se doar prestatorilor de servicii de plată, iar structura lui nu urmează DORA, ceea ce ar îngreuna punerea în aplicare și ajustarea la aderare;

c) preluarea integrală a standardelor tehnice de reglementare și de punere în aplicare ale Uniunii, respinsă din cauza volumului lor și a trimiterilor la mecanisme ale Uniunii, elementele esențiale fiind prevăzute direct în regulament;

d) cadrul simplificat de gestionare a riscurilor TIC de la art. 16 din DORA, nepreluat deoarece legislația națională nu prevede instituții de plată sau instituții emitente de monedă electronică exceptate;

e) termene de conformare diferențiate, de 12 luni pentru prestatorii de servicii de plată și de 18 luni pentru asigurători, reasigurători și intermediari. S-a preferat o dată unică de intrare în vigoare, 1 ianuarie 2029, care oferă tuturor entităților timp de pregătire și permite restrângerea Regulamentului BNM nr. 29/2025 la aceeași dată, astfel încât cerințele se aplică fără întrerupere.

**4. Analiza impactului de reglementare**

4.1. Impactul asupra sectorului public

Proiectul nu presupune reforme structurale sau instituționale. BNM exercită supravegherea prin subdiviziunile existente și preia sarcini noi: examinarea notificărilor și a rapoartelor privind incidentele majore și a informațiilor anuale primite prin PCSI, desemnarea entităților care pun în aplicare planurile de continuitate, identificarea entităților obligate să efectueze TLPT și transmiterea informațiilor privind incidentele majore către Agenția pentru Securitate Cibernetică, care primește astfel informații despre incidentele din sectorul financiar.

4.2. Impactul financiar și argumentarea costurilor estimative

Proiectul nu are impact asupra bugetului public național.

4.3. Impactul asupra sectorului privat

Impactul a fost evaluat calitativ, în formă simplificată, potrivit art. 31 alin. (3) din Legea nr. 100/2017 cu privire la actele normative pentru entitățile aflate în aria de supraveghere a Băncii Naționale a Moldovei – 27 de entități, dintre care 10 bănci, 2 societăți de plată, 6 societăți emitente de monedă electronică și 9 societăți de asigurare:

a) pentru bănci, societăți de plată, prestatori de servicii de informare cu privire la conturi și societăți emitente de monedă electronică, costurile de conformare sunt incrementale, întrucât majoritatea cerințelor naționale se aplică deja prin Regulamentul BNM nr. 29/2025. Costurile noi țin de registrul de informații, programul de testare, clasificarea și raportarea incidentelor prin PCSI, revizuirea contractelor pentru dispozițiile minime și, pentru entitățile identificate, TLPT. Pentru bănci se adaugă soluția de analiză a evenimentelor de securitate cu tehnici de inteligență artificială (subpct. 49.1-49.5): licențierea sau dezvoltarea ei, infrastructura de prelucrare proprie sau a grupului și validarea anuală a modelelor. Băncile din

grupuri pot folosi soluția operată la nivelul grupului (subpct. 49.3);

b) pentru asigurători, reasigurători și intermediari, cerințele sunt noi. Costurile țin de instituirea cadrului de gestionare a riscurilor TIC (politici, proceduri, personal și instrumente), a programului de testare, a procesului de gestionare și raportare a incidentelor și a registrului de informații, precum și de revizuirea contractelor cu furnizorii terți de servicii TIC. Impactul este atenuat de intrarea în vigoare la 1 ianuarie 2029, de excepțiile pentru microîntreprinderi și de neaplicarea cerințelor privind centrele de date (pct. 70-75);

c) intermediarii în asigurări și în reasigurări care sunt întreprinderi mici și mijlocii nu intră în domeniul de aplicare, iar principiul proporționalității și excepțiile pentru microîntreprinderi limitează costurile entităților mici;

d) cerințele uniforme pentru toate entitățile supravegheate de BNM asigură condiții egale de concurență.

Costurile nu au putut fi estimate cantitativ, întrucât participanții la consultarea publică nu au furnizat date privind costurile proprii.

4.4. Impactul social

Nu este aplicabil.

4.4.1. Impactul asupra datelor cu caracter personal

BNM prelucrează date cu caracter personal numai în măsura necesară îndeplinirii sarcinilor de supraveghere prevăzute de regulament, în conformitate cu legislația privind protecția datelor cu caracter personal, și le păstrează cel mult 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită o perioadă mai lungă (pct. 170 și 171). Entitățile financiare asigură retenția jurnalelor de audit, care pot conține date cu caracter personal, pentru cel puțin 12 luni, perioadă extinsă până la cel mult 24 de luni în funcție de ultima perioadă supusă controlului BNM (pct. 68). Informațiile confidențiale primite de BNM sunt protejate prin secretul profesional (pct. 169).

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

4.6. Alte impacturi și informații relevante

Proiectul contribuie la stabilitatea financiară și la încrederea în serviciile financiare digitale prin reducerea probabilității și a impactului incidentelor TIC, raportarea unică prin PCSI, supravegherea unitară a riscurilor TIC și alinierea la standardele Uniunii.

**5. Compatibilitatea proiectului actului normativ cu legislația UE**

Proiectul pune în aplicare parțial Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011, publicat în Jurnalul Oficial al Uniunii Europene seria L, nr. 333 din 27 decembrie 2022, CELEX: 32022R2554. Potrivit art. 58 din DORA, Comisia Europeană efectuează o reexaminare până la 17 ianuarie 2028 și prezintă un raport Parlamentului European și Consiliului, însoțit, dacă este cazul, de o propunere legislativă.

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

a) Obiectivele DORA: un nivel comun ridicat de reziliență operațională digitală a entităților

financiare, prin cerințe uniforme privind gestionarea riscurilor TIC, raportarea incidentelor majore legate de TIC, testarea rezilienței operaționale digitale, schimbul de informații și gestionarea riscurilor generate de furnizorii terți de servicii TIC.

b) Gradul de punere în aplicare este parțial. Tabelul de concordanță, întocmit potrivit modelului 2 din anexa nr. 2 la Hotărârea Guvernului nr. 497/2026, cuprinde 245 de rânduri: 161 compatibile, 10 parțial compatibile, 22 neacoperite de măsuri naționale, 52 neaplicabile și nicio prevedere incompatibilă. Prevederile neacoperite vizează entități care nu se află în supravegherea BNM (firme de investiții, contrapărți centrale, depozitari centrali, locuri de tranzacționare și altele), precum și relația cu Directiva NIS 2 (art. 1 alin. (2)), care necesită o normă de lege. Prevederile neaplicabile privesc cadrul de supraveghere a furnizorilor terți esențiali la nivelul Uniunii (art. 31-44), mandatele autorităților europene de supraveghere și ale Comisiei Europene, opțiunile statelor membre și modificările altor acte ale Uniunii. Prevederile parțial compatibile privesc domeniul de aplicare limitat la entitățile supravegheate de BNM, desemnarea furnizorilor terți esențiali, cooperarea cu alte autorități, declarațiile publice ca sancțiune pentru asigurători și mecanismul de la art. 55 alin. (4).

c) Cele 35 de prevederi cu specific național, care nu sunt prevăzute expres în DORA, sunt descrise și argumentate la pct. 3.1.

Pentru punerea în aplicare totală, prevederile neacoperite care vizează alte entități financiare urmează a fi puse în aplicare prin actele autorităților competente, relația cu Directiva NIS 2 necesită completarea Legii nr. 48/2023 sau a legilor sectoriale, iar prevederile neaplicabile, care țin de mecanismele Uniunii, devin aplicabile direct la aderare. DORA nu a fost pus în aplicare anterior în legislația națională, proiectul constituind prima punere în aplicare. Tabelul de concordanță a fost actualizat după consultarea publică și se actualizează după expertize.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Pentru Regulamentul (UE) 2022/2554, proiectul stabilește măsurile naționale de aplicare: BNM ca autoritate competentă pentru entitățile financiare pe care le supraveghează, raportarea incidentelor și a informațiilor anuale prin PCSI, cooperarea cu Agenția pentru Securitate Cibernetică, precum și sancțiunile și secretul profesional, prin trimitere la legile sectoriale și la Legea nr. 548/1995. Aceste măsuri sunt necesare pentru ca cerințele să poată fi aplicate și supravegheate înainte de aderare, în lipsa arhitecturii de supraveghere a Uniunii, adică a autorităților europene de supraveghere și a cadrului de supraveghere a furnizorilor terți esențiali.

**6. Avizarea și consultarea publică a proiectului actului normativ**

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, proiectul hotărârii a fost supus consultării publice în perioada 22.10.2026 – 08.11.2026, prin plasarea pe pagina web a BNM (www.bnm.md), în compartimentul „Legislație”, rubrica „Transparența decizională”. Au răspuns 14 participanți: Asociația Băncilor din Moldova, opt bănci, un asigurător, doi prestatori de servicii de plată, o societate comercială și o persoană fizică. Obiecțiile și propunerile, cu argumentarea autorului, sunt reflectate în sinteză, iar cele acceptate au fost incluse în proiect. Întrucât completarea pct. 49 cu subpct. 49.1-49.5 introduce aspecte noi, proiectul completat se supune repetat avizării și consultării publice în perioada 23.11.2026-30.11.2026, potrivit art. 32 alin. (7) din Legea nr. 100/2017.

**7. Concluziile expertizelor**

Proiectul de hotărâre, însoțit de tabelul de concordanță, se va expedia Centrului de Armonizare a Legislației în vederea efectuării expertizei de compatibilitate cu legislația Uniunii Europene,

conform prevederilor art. 34 alin. (1) și art. 35 din Legea nr. 100/2017. Totodată, în temeiul art. 11 alin. (3³) din Legea nr. 548/1995 se va solicita o opinie cu caracter consultativ din partea Ministerului Justiției. Conform art. 36 alin. (5) din Legea nr. 100/2017, proiectul hotărârii a fost supus expertizei anticorupție în cadrul Băncii Naționale a Moldovei, în urma căreia factori și riscuri de corupție nu au fost identificate.

**8. Modul de încorporare a actului în cadrul normativ existent**

Cadrul normativ aferent prezentei hotărâri va fi ajustat corespunzător, ca urmare a aprobării acesteia. Pentru a evita dubla notificare a incidentelor către BNM și către Agenția pentru Securitate Cibernetică, este necesară completarea Legii nr. 48/2023 privind securitatea cibernetică sau a legilor sectoriale, întrucât, potrivit art. 3 alin. (5) din Legea nr. 48/2023, caracterul special al obligațiilor sectoriale de notificare îl pot stabili doar legile. Până la modificare, BNM transmite Agenției informațiile privind incidentele majore (pct. 105) și îi propune un acord de cooperare privind rapoartele transmise prin PCSI. Terminologia actelor normative ale BNM privind externalizarea se corelează cu regulamentul la revizuirea acestora.

**9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ**

Implementarea este asigurată de Direcția Managementul Continuității Activității, Securității Informației și Supraveghere în TI, în cooperare cu subdiviziunile responsabile de supravegherea entităților financiare. Până la 1 ianuarie 2029:

a) până la 30 iunie 2028, BNM aprobă formularele PCSI pentru notificările și rapoartele privind incidentele, pentru informarea anuală și pentru registrul de informații, aliniate, în limitele regulamentului, la Regulamentele de punere în aplicare (UE) 2025/302 și 2024/2956, cu o perioadă de testare până la data aplicării, precum și procedurile interne de examinare;

b) BNM convine cu Agenția pentru Securitate Cibernetică modul de transmitere a informațiilor privind incidentele majore (pct. 105) și, după caz, mecanismele de schimb de practici eficace între subsectoarele financiare (pct. 167);

c) entitățile financiare analizează decalajele față de cerințe și actualizează cadrul de gestionare a riscurilor TIC, contractele cu furnizorii terți de servicii TIC și registrul de informații;

d) BNM publică clarificări sub formă de întrebări și răspunsuri, o matrice a aplicabilității cerințelor pe categorii de entități și materiale de implementare, inclusiv pentru desfășurarea TLPT, și organizează sesiuni de informare cu entitățile financiare, pe categorii.

După intrarea în vigoare, BNM desemnează entitățile care pun în aplicare planurile de continuitate (pct. 61 și 62), cu cel puțin 6 luni înainte de luna testării, și identifică entitățile obligate să efectueze TLPT (pct. 130), cu cel puțin 12 luni înainte de termenul primului test. Performanța actului se măsoară anual, pe baza informațiilor transmise de entitățile financiare (pct. 135) și a incidentelor majore raportate prin PCSI. După 2 ani de aplicare, BNM evaluează ex post aplicarea regulamentului, inclusiv a prevederilor cu specific național, în consultare cu sectorul financiar.

Anexă: tabelul de concordanță.

**Guvernator**