

**COMITETUL EXECUTIV
AL BĂNCII NAȚIONALE A MOLDOVEI**

HOTĂRÂREA

nr. ____ din _____ 20__

**Pentru completarea Regulamentului privind externalizarea activităților și
operațiunilor băncii, aprobat prin Hotărârea Consiliului de administrație al BNM
nr.241/2011**

În temeiul art.5 alin.(1) lit. d), art.11 alin.(1), art.27 alin.(1) lit. c), art.44 lit. a) din Legea nr.548/1995 cu privire la Banca Națională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr.297-300, art.544), cu modificările ulterioare, precum și al art.82 din Legea nr.202/2017 privind activitatea băncilor (Monitorul Oficial al Republicii Moldova, 2017, nr.434-439, art.727), cu modificările ulterioare, Comitetul executiv al Băncii Naționale a Moldovei

HOTĂRĂȘTE:

1. Regulamentul privind externalizarea activităților și operațiunilor băncii, aprobat prin Hotărârea Consiliului de administrație al BNM nr.241 din 3.11.2011, se completează cu Capitolul VII cu următorul cuprins:

**CAPITOLUL VII EXTERNALIZAREA TEHNOLOGIILOR INFORMAȚIONALE ȘI A
COMUNICAȚIILOR**

Secțiunea 1. Dispoziții generale

36. Prezentul capitol se aplică băncilor care intenționează să externalizeze Tehnologii Informaționale și Comunicații (în continuare TIC) și stabilește cerințe suplimentare celor prevăzute de prezentul regulament.
37. În cazul externalizării activităților TIC care reprezintă activități de importanță materială pentru bancă, aceasta urmează să obțină acordul prealabil al BNM în conformitate cu prezentul regulament.

Secțiunea 2. Administrarea riscurilor asociate externalizării TIC

38. Banca elaborează și aprobă o politică de externalizare TIC care urmează să definească principiile, responsabilitățile și procesele ce țin de externalizarea TIC care va conține cel puțin următoarele aspecte, fără a se limita la acestea:
- 1) responsabilitățile organelor de conducere, inclusiv nivelul de implicare și luare a deciziilor;
 - 2) responsabilitățile și nivelul de implicare a funcțiilor de control intern și a șefilor de subdiviziuni;
 - 3) cerințele cu privire la evaluarea riscurilor și verificările prelabile ale furnizorului în conformitate cu cerințele prezentului regulament;

- 4) cerințe cu privire la gestionarea conflictelor de interese;
 - 5) cerințe cu privire la asigurarea continuității activității și securității informațiilor, performanța și calitatea serviciilor/sistemelor TIC externalizate;
 - 6) cerințe cu privire la auditul, supravegherea și raportarea aferente procesului de externalizare TIC;
 - 7) cerințe cu privire la strategiile de reintegrare.
39. Politica de externalizare TIC va determina aspectele importante ale etapei precontractuale, constând în :
- 1) atribuirea clară a rolurilor și responsabilităților pentru gestiunea externalizării TIC;
 - 2) evaluarea importanței TIC ce urmează a fi externalizate, prin prisma dependenței de acestea a desfășurării și continuității proceselor critice, a activităților de bază ale băncii și a impactului asupra datelor cu caracter personal aferent clienților;
 - 3) pregătirea unei argumentări privind necesitatea externalizării TIC și criteriile ce vor fi utilizate la selectarea furnizorului;
 - 4) efectuarea unei verificări prealabile a furnizorului de servicii TIC pentru a se asigura că acesta are o reputație bună, expertiză, capacitate, resurse (ex. umane, tehnice, financiare) suficiente, structură organizațională adecvată, și, după caz, dispune de autorizațiile corespunzătoare pentru a presta acest tip de servicii pe toată perioada contractului;
 - 5) **ținerea evidenței documentate** a deliberărilor membrilor conducerii la luarea deciziei de aprobare a externalizării TIC;
 - 6) identificarea tuturor conflictelor de interese ce pot să apară urmare externalizării TIC, inclusiv în cazul externalizării în **cadrul** grupului din care face parte banca.
40. În procesul analizei riscurilor asociate externalizării TIC, banca evaluează cel puțin următoarele aspecte, fără a se limita la ele:
- 1) impactul potențial al oricărei întreruperi sau perturbări în prestarea de către furnizor a serviciilor TIC;
 - 2) viabilitatea externalizării TIC pe termen scurt și pe termen lung, inclusiv costurile financiare aferente;
 - 3) aspectele legale și reputaționale aferente procesul de externalizare TIC;
 - 4) impactul externalizării TIC asupra capacității băncii de a gestiona riscurile TIC și de securitate a informației, de a respecta cerințele legale și de reglementare;
 - 5) impactul externalizării TIC asupra capacității băncii de a efectua misiuni de audit, inclusiv a serviciilor externalizate;
 - 6) impactul externalizării TIC asupra riscului operațional;
 - 7) impactul potențial al externalizării TIC asupra calității serviciilor prestate clienților băncii;
 - 8) riscul de concentrare, inclusiv riscul de contractare a unui furnizor dominant sau care nu este ușor de substituit;

- 9) riscul asociat subcontractării și externalizării în lanț de către furnizor, în cazul externalizării activităților ce nu sunt de importanță materială;
 - 10) riscul agregat ce rezultă din externalizarea a mai multor funcții ale băncii către același furnizor;
 - 11) dacă furnizorul de servicii TIC este supus supravegherii din partea autorităților competente;
 - 12) în cazul furnizorilor cu sisteme de tip cloud, riscurile asociate tipului de cloud utilizat (public/privat/hibrid/comunicate) și locației fizice a stocării/procesării datelor;
 - 13) riscul de portabilitate a tehnologiilor utilizate de către furnizorul de servicii TIC;
 - 14) posibilitatea de a extinde sau a reduce volumul externalizării TIC fără a revizui aranjamentele contractuale;
 - 15) capacitatea băncii de a transfera externalizarea TIC către un alt furnizor, inclusiv costurile, timpul necesar, dificultățile ce pot apărea;
 - 16) capacitatea băncii de a reintegra serviciile/sistemele TIC externalizate în cadrul activităților băncii.
41. În cazul externalizării TIC în afara țării, banca urmează să identifice riscul de țară aferent furnizorului de servicii TIC. La identificarea riscului de țară aferent furnizorului de servicii TIC, banca va evalua cel puțin următoarele aspecte, fără a se limita la ele:
- 1) complexitatea reglementărilor aferente prestării serviciilor TIC, protecției datelor cu caracter personal și insolvabilității;
 - 2) riscul de instabilitate politică care ar putea să aibă impact asupra capacității furnizorului să ofere servicii;
 - 3) riscul climateric și al mediului unde este amplasat echipamentul furnizorului;
 - 4) probleme culturale și/sau lingvistice cu privire la așteptările băncii față de serviciile TIC;
 - 5) fusul orar în care este amplasat furnizorul și disponibilitatea personalului său de a remedia incidentele în timp util.

Secțiunea 3. Contractul de externalizare TIC

42. În cazul externalizării TIC, banca întocmește un proiect al contractului de externalizare cu furnizorul ce conține cel puțin următoarele aspecte, fără a se limita la ele:
- 1) perioada de valabilitate a contractului, inclusiv perioadele de notificare prealabilă privind modificările ce pot surveni;
 - 2) locațiile ce vor fi folosite de furnizor pentru a presta servicii TIC și locațiile de stocare a datelor, inclusiv obligativitatea furnizorului de a notifica banca dacă intenționează să schimbe locațiile respective;
 - 3) obligația furnizorului de a coopera cu BNM, alte organe de control abilitate sau cu oricare altă entitate sau persoană delegată de bancă;
 - 4) dreptul băncii de a supraveghea în mod continuu performanța serviciilor TIC prestate de către furnizor;

- 5) nivelurile convenite de performanță și calitate a serviciilor TIC ce urmează a fi prestate de furnizor care trebuie să conțină valori precise atât calitative, cât și cantitative pentru o monitorizare adecvată;
 - 6) obligativitatea furnizorului, dacă este cazul, de a încheia un contract de asigurare obligatorie aferentă unor riscuri specifice.
43. Contractul încheiat cu furnizorul trebuie să conțină cel puțin următoarele aspecte cu privire la securitatea informației și continuitatea activității, fără a se limita la ele:
- 1) obligativitatea furnizorului de a se conforma cu reglementările TIC și standardele de securitate a informației și continuitate a activității aplicabile băncii;
 - 2) cerințe specifice de securitate și continuitate înaintate de bancă pentru serviciile/sistemele TIC externalizate ce stochează sau conțin date cu caracter personal;
 - 3) cerințe cu privire la asigurarea în orice moment a accesibilității, disponibilității, integrității și confidențialității datelor băncii în cadrul sistemului informațional al furnizorului;
 - 4) obligativitatea furnizorului de a nu stoca datele băncii în baze de date comune cu datele altor clienți pentru care se prestează servicii de externalizare TIC;
 - 5) cerințe față de furnizor cu privire la timpul de restabilire a serviciilor/sistemelor TIC prestate în cazul incidentelor;
 - 6) obligativitatea furnizorului de a dezvolta planuri de restabilire aferente serviciilor/sistemelor TIC prestate băncii;
 - 7) obligativitatea furnizorului de a efectua anual testele de continuitate a serviciilor/sistemelor TIC cu raportarea rezultatelor către bancă.
44. Contractul încheiat cu furnizorul urmează să conțină cel puțin următoarele aspecte cu privire la dreptul băncii de acces la sisteme/servicii TIC și la informație, fără a se limita la ele:
- 1) dreptul băncii de a recepționa de la furnizorul de servicii TIC rapoarte privind indicatori de performanță și calitate;
 - 2) obligativitatea furnizorului de servicii TIC de a permite autorităților de supraveghere sau oricărei alte entități, sau persoane delegate de bancă, accesul complet la toate încăperile, echipamentele și sistemele utilizate pentru a presta serviciile TIC, accesul la datele și informațiile aferente procesului de prestare a serviciilor TIC, inclusiv situațiile financiare ale furnizorului;
 - 3) dreptul băncii de a cere și de a primi de la furnizor, în timp optim, toate datele aferente procesului de prestare a serviciilor TIC, inclusiv jurnale de audit și copii de rezervă aferente sistemelor/serviciilor TIC ca urmare a unor investigații, misiuni de audit sau în cazul întreruperii relației cu furnizorul din orice motive;
 - 4) dreptul băncii la auditul serviciilor/sistemelor TIC externalizate, inclusiv cu utilizarea în acest scop a evaluărilor și a rapoartelor de audit efectuate de către terțe părți, precum și la examinarea rapoartelor de audit intern ale furnizorului. Unde este relevant, banca se va asigura de posibilitatea efectuării testelor de penetrare a serviciilor/sistemelor TIC prestate băncii de către furnizor.

45. Pentru a se asigura că gestionează eficient riscurile în cazul încetării relației cu furnizorul, banca se asigură că, contractul conține cel puțin următoarele aspecte cu privire la dreptul de încetare a relației cu furnizorul, fără a se limita la ele:

- 1) posibilitatea de încetare a relației cu furnizorul cel puțin în următoarele cazuri:
 - a) neconformarea furnizorului cu prevederile legale aferente domeniului TIC, securității informației, continuității activității sau a datelor cu caracter personal;
 - b) identificarea unor impedimente capabile să afecteze performanța sau calitatea prestării serviciilor TIC de către furnizor;
 - c) existența vulnerabilităților ce pot afecta securitatea informației și a datelor cu caracter personal ale clienților băncii;
 - d) la indicația Băncii Naționale a Moldovei.
- 2) prevederea unei perioade de tranziție în cazul încetării relației cu furnizorul sau al transferului către alt furnizor, cu obligativitatea furnizorului de a acorda suport băncii;
- 3) obligativitatea furnizorului de a crea mecanisme ce vor permite identificarea și ștergerea tuturor datelor ce țin de bancă, inclusiv cele aferente procesului de prestare băncii de către furnizor a serviciilor TIC.

Secțiunea 4. Controlul activităților externalizate

46. Pentru a se asigura că gestionează eficient riscurile asociate reintegrării serviciilor/sistemelor TIC externalizate, la întreruperea relației cu furnizorul de servicii TIC, banca urmează:

- 1) să elaboreze o strategie de reintegrare a serviciilor/sistemelor TIC externalizate care va asigura continuitatea activităților băncii, conformarea cu cerințele cadrului de reglementare și evitarea impactului asupra calității deservirii clienților în cazul întreruperii relației cu furnizorul;
- 2) să se asigure că strategia de reintegrare conține cel puțin următoarele:
 - a) obiectivele strategiei;
 - b) analiza de impact și analiza de riscuri aferent externalizării TIC;
 - c) identificarea resurselor tehnico-organizatorice, umane și financiare, inclusiv a perioadei necesare implementării strategiei;
 - d) alocarea rolurilor și responsabilităților pentru gestiunea strategiei;
 - e) criteriile de succes a procesului de reintegrare;
 - f) indicatorii de performanță și calitate a serviciilor externalizate ce urmează a fi monitorizați de către bancă și care vor declanșa aplicarea strategiei;
- 3) să revizuiască anual strategia de reintegrare a serviciilor/sistemelor TIC externalizate pentru a asigura viabilitatea ei.

47. Pentru a asigura continuitatea activității în cazuri excepționale, pentru activități de importanță materială, banca se va conforma cel puțin cu următoarele aspecte, fără a se limita la ele:

- 1) să aloce suficiente resurse tehnice pentru a asigura în orice moment la sediul băncii continuitatea serviciilor/sistemelor TIC externalizate și reziliența operațională în cazul unui incident major/situație excepțională la furnizor sau declanșarea de către autoritatea de supraveghere a procedurii de rezoluție sau lichidare a băncii;

- 2) să dețină resurse umane ce posedă cunoștințe suficiente pentru a asigura la necesitate reintegrarea/substituirea/continuitatea în timp optim a serviciilor/sistemelor TIC externalizate;
- 3) să dezvolte planuri de continuitate a activităților externalizate care să permită, în timp optim, reluarea integrală la sediul băncii a oricărui serviciu/sistem TIC externalizat;
- 4) să organizeze anual în comun cu furnizorul testarea planurilor de continuitate a serviciilor/sistemelor TIC externalizate cu restabilirea la sediul băncii.

48. Pentru a asigura o supraveghere eficientă a externalizării TIC banca urmează să:

- 1) aloce suficiente resurse tehnice, financiare, inclusiv umane, ce dețin suficiente cunoștințe pentru a asigura o monitorizare eficientă a serviciilor/sistemelor TIC externalizate;
- 2) monitorizeze în mod continuu performanța și calitatea serviciilor TIC prestate de furnizor pentru a se asigura că acestea corespund cu cerințele stabilite în contract. Evaluarea performanței poate fi efectuată prin intermediul următoarelor surse, fără a se limita la acestea: rapoartele privind livrarea serviciului prestat de furnizor, indicatori de performanță, de calitate, de continuitate, revizuirii independente, certificări, rapoarte privind testele de continuitate;
- 3) revizuiască periodic și să raporteze organelor de conducere a băncii despre schimbările profilului de risc aferent serviciilor externalizate.

2. Cererea și documentele înaintate de către bancă pentru obținerea aprobării prealabile a Băncii Naționale a Moldovei privind externalizarea activităților TIC, în cazul acesta reprezintă activități de importanță materială pentru bancă, nesoluționate până la data intrării în vigoare a prezentei hotărâri, se examinează și se soluționează în conformitate cu prevederile regulamentului menționat la pct.1, cu condiția completării acestora în termen de 15 zile lucrătoare de la data intrării în vigoare a prezentei hotărâri.

Cererea și documentele se examinează de către Banca Națională a Moldovei în termen de 30 de zile de la data completării de către bancă a setului de documente și informații. În cazul în care cererea și documentele nu sunt completate în termenul indicat, acestea se restituie băncii.

3. Banca, care a externalizat activități TIC până la data intrării în vigoare a prezentei hotărâri, asigură conformitatea cu prevederile expuse la pct.1 în termen de 12 luni de la data intrării în vigoare a prezentei hotărâri.