Proiect

COMITETUL EXECUTIV
AL BĂNCII NAȚIONALE A MOLDOVEI

H O T Ă R Â R E A Nr.___
din „__” _____ 20___

Pentru aprobarea Regulamentului privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor

În temeiul art.5 alin.(1) lit d), art.11 alin.(1), art.27 alin.(1) lit.c) și art.44 lit.a) din Legea nr.548-XIII din 21 iulie 1995 cu privire la Banca Națională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr.297-300, art.544), cu modificările și completările ulterioare, precum și art.25 alin (2) f) și g), art.28 alin (2) lit i) și art.40 din Legea instituțiilor financiare nr.550-XIII din 21 iulie 1995 (republicată în Monitorul Oficial al Republicii Moldova, 2011, nr.78-81, art.199), cu modificările și completările ulterioare, Comitetul executiv al Băncii Naționale a Moldovei

HOTĂRĂȘTE:

1. Se aprobă Regulamentul privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor conform anexei.

2. Prezenta hotărâre intră în vigoare la data de 31 decembrie 2017.

Anexa
la Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr.___ din ____ _____ 20___

REGULAMENT
privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor

Titlul I. DISPOZIȚII GENERALE

Capitolul I. Domeniul de aplicare

1. Prezentul regulament se aplică băncilor din Republica Moldova și filialelor băncilor străine deschise pe teritoriul Republicii Moldova și stabilește cerințele minime pentru sistemele informaționale și de comunicare ale băncilor.

2. Scopul regulamentului este de a asigura că băncile dispun de o strategie adecvată aferentă tehnologiei informației și comunicațiilor (în continuare TIC) aliniată la strategia generală de afaceri, că procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele TIC ale băncii și cadrul intern de gestiune a riscurilor aferente TIC și control intern protejează în mod adecvat sistemele TIC ale băncilor.

Capitolul II. Noțiuni principale

3. Termenii și expresiile utilizate în prezentul regulament au semnificațiile prevăzute în Regulamentul privind cadrul de administrare a activității băncii, aprobat prin Hotărârea Comitetului executiv al Băncii Naționale a Moldovei nr.146 din 07 iunie 2017.

4. Adițional, în sensul prezentului regulament, se aplică următoarele definiții:

tehnologia informației și comunicațiilor - ansamblu sistematizat de metode, cunoștințe, procese tehnice și mijloace utilizate în vederea gestiunii informației;

sisteme TIC – tehnologii ale informațiilor și comunicațiilor interconectate ce funcționează ca parte a unui sistem sau a unei rețele și sprijină efectuarea operațiunilor unei bănci;

sisteme TIC critice – sisteme TIC care în cazul în care sunt indisponibile au impact asupra derulării proceselor critice de activitate și operațiunilor băncii;

servicii TIC – servicii furnizate de sistemele TIC unuia sau mai multor utilizatori interni sau externi;

riscul de disponibilitate și continuitate aferent TIC – riscul ca performanțele sau disponibilitatea sistemelor și datelor TIC să fie afectate în mod negativ, inclusiv incapacitatea de a recupera în timp util procesele și serviciile băncii;

riscul de securitate aferent TIC – riscul accesului neautorizat la sistemele și datele aferente TIC din interiorul sau din afara băncii;

riscul de schimbare aferent TIC – riscul care este un rezultat al incapacității băncii de a gestiona în timp util și în mod controlat schimbările în sistemele și serviciile aferent TIC;

riscul de integritate a datelor – riscul ca datele stocate și procesate de sistemele aferent TIC să fie incomplete, inexacte sau incoerente;

riscul asociat externalizărilor TIC – riscul ca angajarea unei terțe părți sau a unei alte entități a grupului (externalizare intragrup) pentru a furniza sisteme TIC sau servicii conexe să aibă un impact negativ asupra performanței băncii și asupra gestionării riscurilor;

înregistrare de audit - o singură înregistrare în jurnalul de audit care descrie apariția unui singur eveniment auditabil;

jurnal de audit - secvență cronologică de înregistrări de audit, fiecare dintre acestea conținând dovezi privind rezultatul executării unui proces sau a unei funcții din cadrul unui sistem;

cadrul intern aferent TIC – totalitatea reglementărilor interne, a proceselor și structurilor organizatorice aferente TIC stabilite în cadrul băncii, ce asigură minimizarea riscurilor aferente TIC și atingerea obiectivelor privind TIC ale băncii.

Titlul II. CERINȚE PRIVIND CADRUL INTERN ȘI EVALUAREA RISCURILOR TIC

Capitolul I. Guvernanța, strategia și cadrul intern aferent TIC

5. Banca trebuie să dețină o strategie aferentă TIC, aliniată la strategia generală de afaceri a băncii, aprobată și monitorizată adecvat de către organele de conducere ale băncii.

6. Banca trebuie să se asigure că, cadrul intern aferent TIC, externalizării TIC și procesului de gestiune a riscurilor TIC este adecvat, proporțional cu mărimea, natura și complexitatea activităților băncii și susține implementarea strategiei aferente TIC.

7. Banca trebuie să asigure o structură organizatorică aferentă TIC, adecvată din punctul de vedere al responsabilităților, în funcție de mărimea, natura și complexitatea activităților aferente TIC ale băncii.

8. Banca trebuie să definească și să aprobe în reglementările interne și la un nivel adecvat profilul de risc, apetitul și toleranța pentru riscurile aferente TIC identificate.

9. Banca trebuie să definească roluri și responsabilități de gestionare a riscurilor TIC și să asigure integrarea acestora în organizarea internă pentru a gestiona și monitoriza adecvat riscurile identificate aferente TIC.

10. Banca trebuie să asigure pentru implementarea proceselor de gestionare adecvată a riscurilor aferente TIC resurse financiare, umane și tehnice suficiente, precum și alte resurse necesare ce vor fi cantitativ și calitativ corespunzătoare.

11. Banca trebuie să evalueze profilul de risc aferent TIC cel puțin anual sau mai des, dacă au fost operate modificări majore în procesele, serviciile sau echipamentele critice aferente TIC.

12. Urmare a evaluării profilului de risc, după caz, banca va revizui cadrul intern corespunzător.

13. Banca trebuie să asigure că evaluarea de către auditul intern a cadrului intern, precum și a măsurilor de control aplicabile riscurilor aferente TIC corespunde mărimii, naturii și complexității activităților băncii.

14. Banca trebuie să asigure că există implementate măsuri de control adecvate pentru a trata, dacă este cazul, cel puțin următoarele riscuri:

a) riscurile de disponibilitate și continuitate aferente TIC;

b) riscurile de securitate aferente TIC;

c) riscurile de schimbare aferente TIC;

d) riscurile de integritate a datelor aferente TIC;

e) riscurile asociate externalizărilor TIC;

f) riscurile de conformitate aferente TIC.

Titlul III. CERINȚE PRIVIND INTEGRITATEA ȘI CONTINUITATEA INFORMAȚIEI

15. Banca va asigura o perioadă de retenție de minimum 12 luni pentru:

a) copiile de rezervă ale bazelor de date aferente sistemelor TIC;

b) jurnalele de audit pentru sistemele TIC critice;

c) mesajele transmise/primite prin intermediul serviciului de poștă electronică al băncii.

16. Ca rezultat al evaluării efectuate, conform pct.18, Banca Națională a Moldovei poate impune perioade mai mari de retenție, în funcție de mărimea, natura și complexitatea activităților băncii.

17. Banca va efectua testări anuale de continuitate pentru sistemele TIC critice, cu un grad de complexitate adecvat riscurilor aferente TIC la care este supusă.

Titlul X. DISPOZIȚII FINALE

18. Banca Națională a Moldovei evaluează cadrul! intern aferent TIC în fiecare bancă, în raport cu profilul/apetitul de risc definit, cu mărimea, natura și complexitatea activităților băncii:

a) în ! decursul controalelor pe teren;

b) controalelor din oficiu;

c) auditelor în cadrul băncilor în scop de supraveghere.

19. În cazul în care, urmare a evaluării efectuate conform pct.18, se constată că, cadrul intern aferent TIC nu este adecvat în raport cu profilul/apetitul de risc definit, cu mărimea, natura și complexitatea activităților băncii, Banca Națională a Moldovei poate impune cerințe concrete față de cadrul intern aferent TIC.

20. Banca este obligată să notifice, prin intermediul unei scrisori oficiale sau la adresa electronică pusă la dispoziție de Banca Națională a Moldovei, cel târziu în ziua următoare a producerii, despre incidentele majore ce au afectat disponibilitatea, securitatea sau integritatea sistemelor TIC critice. În decurs de 4 zile lucrătoare din ziua producerii incidentului, banca va transmite pe adresa BNM, prin intermediul unei scrisori oficiale sau al poștei electronice, informația suplimentară cu privire la circumstanțele incidentului produs, procesele/sistemele afectate, impactul estimat și măsurile de remediere întreprinse / care urmează a fi întreprinse de bancă.

21. Băncile vor transmite, prin intermediul unei scrisori oficiale, anual, în termen de 1 lună de la încheierea anului de raportare, Băncii Naționale a Moldovei informații cu privire la următoarele:

a) lista sistemelor TIC critice cu indicarea periodicității de efectuare și de retenție a copiilor de rezervă ale bazelor de date pentru fiecare sistem TIC critic;

b) rezultatele testărilor de continuitate aferente sistemelor TIC critice.