23.04.2018

Regulament privind cerințe minime pentru Sistemele Informaționale și de Comunicare ale băncilor, aprobat prin HCE al BNM nr.47 din 14 martie 2018

Aprobat
prin Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr.47 din 14 martie 2018

REGULAMENT
privind cerințe minime pentru Sistemele Informaționale
și de Comunicare ale băncilor

Capitolul I
DISPOZIȚII GENERALE

Secțiunea 1. Domeniul de aplicare

1. Prezentul regulament se aplică băncilor din Republica Moldova și sucursalelor băncilor străine deschise pe teritoriul Republicii Moldova și stabilește cerințe 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 că cadrul intern de gestionare a riscurilor TIC și control intern protejează în mod adecvat sistemele TIC ale băncilor.

Secțiunea 2. 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, înregistrată la Ministerul Justiției cu nr. 1229 din 14 iunie 2017 (Monitorul Oficial al Republicii Moldova, 2017, nr. 201-213, art.1183 din 23.06.17)
4. Adițional, în sensul prezentului regulament se aplică următoarele definiții:
sisteme aferente TIC – TIC configurate și interconectate ca parte a unui mecanism sau a unei rețele care susțin efectuarea operațiunilor unei bănci;
servicii aferente TIC – servicii furnizate prin intermediul sistemelor TIC unuia sau mai multor utilizatori interni sau externi;
sisteme/servicii aferente TIC critice – sisteme/servicii TIC care sunt critice pentru bancă din perspectiva continuității și disponibilității acestora sau a securității informației prelucrate și/sau stocate și sunt esențiale pentru funcționarea adecvată a proceselor de guvernanță, responsabilităților/rolurilor corporative critice (inclusiv gestionarea riscurilor), proceselor de activitate și operațiunilor băncii;
risc de disponibilitate și continuitate aferente TIC – riscul ca performanțele sau disponibilitatea sistemelor/serviciilor și datelor aferent TIC să fie afectate în mod negativ, inclusiv incapacitatea de a recupera în timp util procesele și serviciile băncii;
risc de securitate aferent TIC – riscul accesului neautorizat la sistemele/serviciile și datele aferente TIC din interiorul sau din afara băncii;
risc de schimbare aferent TIC – riscul care este un rezultat al incapacității băncii de a gestiona în timp util și în mod controlat schimbările asociate sistemelor și serviciilor aferente TIC;
risc de integritate a datelor aferent TIC – riscul ca datele stocate și/sau procesate de sistemele/serviciile aferent TIC să fie incomplete, inexacte sau incoerente la nivelul diferitor sisteme TIC;

risc asociat externalizărilor TIC – riscul ca angajarea unei terțe părți sau a unei alte entități a grupului (externalizare intragrup) pentru a furniza sisteme aferente TIC sau servicii conexe să afecteze negativ performanța și gestionarea riscurilor în cadrul băncii;
risc de conformitate aferent TIC – riscul de încălcare sau neconformare cu cadrul legal, acorduri, practici recomandate sau standarde etice aferent TIC;
risc aferent TIC semnificativ – risc aferent TIC ce poate avea un impact negativ asupra sistemelor sau serviciilor aferente TIC critice;
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 a unui proces sau a unei funcții din cadrul unui sistem;
cadrul intern aferent TIC – totalitatea reglementărilor interne, a proceselor și structurilor organizatorice TIC stabilite în cadrul băncii, ce asigură gestionarea adecvată a riscurilor aferente TIC și atingerea obiectivelor privind TIC ale băncii;
profil de risc TIC - suma expunerilor unei bănci la riscuri reale și potențiale aferent TIC;

Capitolul II. CERINȚE PRIVIND CADRUL INTERN ȘI EVALUAREA RISCURILOR TIC

Secțiunea 1. Guvernanța, Strategia și cadrul intern TIC

5. Banca trebuie să dețină o strategie TIC ce se conformează și sprijină strategia generală de afaceri a băncii și care este aprobată și monitorizată adecvat de către organele de conducere ale băncii.
6. Banca trebuie să se asigure că are stabilit cadrul intern aferent TIC ce protejează în mod adecvat sistemele și serviciile sale TIC proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și susține implementarea strategiei aferent TIC iar apetitul și toleranța la risc cuprind și riscurile aferente TIC în categoria riscului operațional.
7. Banca trebuie să asigure o structură organizatorică adecvată din punct de vedere a responsabilităților aferente TIC, proporțională cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate.
8. Banca trebuie să asigure gestionarea adecvată a riscurilor aferente TIC identificate ca fiind semnificative și pot avea un impact negativ asupra sistemelor și serviciilor aferente TIC critice prin stabilirea unor proceduri de control specifice.
9. Banca trebuie să asigure că are definite roluri și responsabilități de gestionare a riscurilor aferente TIC ce sunt comunicate în mod clar, stabilite și integrate în organizarea internă și procesele relevante, inclusiv roluri privind colectarea și agregarea informațiilor despre riscuri și raportarea acestora către organele de conducere.
10. Banca trebuie să asigure pentru procesele de gestionare a riscurilor aferente TIC, resurse financiare, umane și tehnice suficiente, cât și alte resurse necesare ce vor fi cantitativ cât și calitativ corespunzătoare cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă.
11. Banca trebuie să asigure că organizarea funcției de audit intern în ceea ce privește auditarea cadrului intern aferent TIC este proporțională cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și profilului de risc TIC al băncii.
12. Banca trebuie să asigure că există implementate măsuri de control adecvate pentru a trata, dacă este cazul, cel puțin următoarele categorii de riscuri aferente TIC:
a) riscuri de disponibilitate și continuitate aferente TIC;
b) riscuri de securitate aferente TIC;
c) riscuri de schimbare aferente TIC;
d) riscuri de integritate a datelor aferente TIC;
e) riscuri asociate externalizărilor TIC;
f) riscuri de conformitate aferente TIC.

Secțiunea 2. Integritatea, disponibilitatea informației și continuitatea TIC

13. Banca va asigura, inclusiv și în cazul externalizării sistemelor/serviciilor aferente TIC critice, integritatea și disponibilitatea informației precum și o perioadă de retenție de minim 12 luni a informației conținute în:
a) copiile de rezervă ale bazelor de date aferente sistemelor/serviciilor aferente TIC critice;
b) jurnalele de audit pentru sistemele/serviciile aferente TIC critice;
c) mesajele transmise/primite prin intermediul serviciului de poștă electronică oficială a băncii.
14. În rezultatul evaluării efectuate conform pct.18, Banca Națională a Moldovei (în continuare BNM) poate impune perioade mai mari de retenție, în funcție de mărimea, importanța sistemică, natura, extinderea și complexitatea activităților desfășurate de bănci.
15. Banca va asigura că are implementat un proces de gestiune a continuității activității cu planuri pentru situații

neprevăzute precum și cu planuri de redresare pentru toate funcțiile și resursele sale critice, proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate ce să asigure continuitatea atât în perioade normale cât și în perioade de criză.
16. Banca va efectua testări anuale de disponibilitate și continuitate pentru sistemele/serviciile TIC critice, cu un grad de complexitate adecvat riscurilor aferente TIC la care este supusă.

Capitolul III. EVALUAREA RISCURILOR

17. Banca trebuie să își evalueze profilul de risc aferent TIC cel puțin anual sau dacă au fost operate modificări majore în procesele, sistemele, serviciile sau echipamentele critice aferente TIC. Urmare a evaluării profilului de risc, după caz, banca va revizui cadrul intern corespunzător cât și măsurile de control aplicabile.
18. BNM evaluează cadrul intern aferent TIC în fiecare bancă, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă și cu profilul/apetitul de risc în cadrul controalelor pe teren, controalelor din oficiu și prin dispunerea efectuării auditelor conform art.87 a Legii nr.202 din 6 octombrie 2017 privind activitatea băncilor.
19. Dacă urmare a evaluării efectuate conform pct.18, se constată că cadrul intern aferent TIC nu este adecvat în raport cu profilul/apetitul de risc, cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă, BNM poate impune cerințe concrete față de cadrul intern aferent TIC.
20. Banca este obligată să notifice BNM, cel târziu în ziua următoare lucrătoare a producerii, despre incidentele ce au afectat disponibilitatea sau securitatea sistemelor/serviciilor, fie integritatea datelor aferente TIC critice. Cel mult în 4 zile lucrătoare din ziua producerii incidentului, banca va transmite în adresa BNM informația suplimentară cu privire la circumstanțele incidentului produs, procesele/sistemele/serviciile afectate, impactul estimat și măsurile de remediere întreprinse sau care urmează a fi întreprinse de bancă.
21. Băncile vor transmite, în termen de o lună de la încheierea anului de gestiune, BNM informații cu privire la următoarele:
a) lista sistemelor/serviciilor aferente TIC critice cu indicarea periodicității de efectuare și de retenție a copiilor de rezervă ale bazelor de date pentru fiecare sistem/serviciu aferent TIC critic;
b) rezultatele testărilor de continuitate sistemelor/serviciilor aferente TIC critice;
c) raport privind gestionarea riscurilor aferente TIC identificate ca fiind semnificative;
d) raport privind gestionarea incidentelor produse pe parcursul anului aferent sistemelor/serviciilor critice ale băncii.
22. Notificarea BNM și/sau transmiterea informațiilor, conform pct. 20 și 21, se efectuează prin intermediul unei scrisori oficiale și/sau la adresa de poștă electronică supraveghereTIC@bnm.md [1].

Referința spre Registrul de stat al actelor juridice: https://www.legis.md/cautare/getResults?doc_id=104887&lang=ro [2]

Vezi și

Tag-uri
Regulament privind cerințe minime pentru Sistemele Informaționale și de Comunicare ale băncilor [3]
nr. 47 [4]
14 martie 2018 [5]
14.03.2018 [6]
47 [7]

---

martie 2018 [6] http://bnm.md/ro/search?hashtags[0]=14.03.2018 [7] http://bnm.md/ro/search?hashtags[0]=47