REPUBLICA MOLDOVA
BANCA NAȚIONALĂ

РЕСПУБЛИКА МОЛДОВА
НАЦИОНАЛЬНЫЙ БАНК

H O T Ă R Â R E
pentru aprobarea Regulamentului privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii şi modificarea unor acte normative

nr. 29 din 12.02.2025

Monitorul Oficial nr.62-65/131 din 20.02.2025

* * *

În temeiul art.32[1] alin.(3), art.32[2] alin.(3) din Legea nr.114/2012 cu privire la serviciile de plată şi moneda electronică (Monitorul Oficial al Republicii Moldova, 2012, nr.193-197, art.661) şi art.38[2] alin.(6) din Legea nr.202/2017 privind la activitatea băncilor (Monitorul Oficial al Republicii Moldova, 2017, nr.434-439, art.727), Comitetul executiv al Băncii Naţionale a Moldovei

HOTĂRĂŞTE:

1. Se aprobă Regulamentul privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii, conform anexei.

2. Se abrogă Hotărârea Comitetului Executiv al Băncii Naţionale a Moldovei cu privire la aprobarea Regulamentului privind cerinţele minime pentru sistemele informaţionale şi de comunicare ale băncilor nr.47/2018 (Monitorul Oficial al Republicii Moldova, 2018, nr.113-120, art.491), înregistrat la Ministerul Justiţiei al Republicii Moldova cu nr.1307 din 28 martie 2018.

3. La pct.271 din Regulamentul privind cadrul de administrare a activităţii băncilor, aprobat prin Hotărârea Comitetului executiv al Băncii Naţionale a Moldovei nr.322/2018, textul „Regulamentul privind cerinţele minime pentru sistemele informaţionale şi de comunicare ale băncilor, aprobat prin Hotărârea Comitetului executiv al Băncii Naţionale a Moldovei nr.47/2018” se substituie cu textul „Regulamentul privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii”.

4. La pct.2 din Regulamentul privind externalizarea activităţilor şi operaţiunilor băncii, aprobat prin Hotărârea Comitetului executiv al Băncii Naţionale a Moldovei nr.46/2020, textul „Regulamentul privind cerinţele minime pentru sistemele informaţionale şi de comunicare ale băncilor, aprobat prin Hotărârea Comitetului executiv al Băncii Naţionale a Moldovei nr.47/2018” se substituie cu textul „Regulamentul privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii”.

5. Prestatorii de servicii de plată prevăzuţi la art.5 alin.(1) lit.a)-d) din Legea nr.114/2012 cu privire la serviciile de plată şi moneda electronică vor asigura conformarea cu prevederile pct.81 din Regulamentul indicat la pct.1 – în termen de 3 luni, cu prevederile pct.4-56, pct.62, pct.65-67, pct.76-80 şi pct.82 din Regulamentul indicat la pct.1 – în termen de 9 luni, cu prevederile pct.57, pct.58 subpct.58.1-58.11 din Regulamentul indicat la pct.1 – în termen de 12 luni, cu prevederile subpct.58.12–61, pct.63-64 şi pct.68-75 din Regulamentul indicat la pct.1 – în termen de 15 luni, de la data intrării în vigoare a prezentei hotărâri.

6. Prezenta hotărâre intră în vigoare la expirarea termenului de o lună de la data publicării în

Monitorul Oficial al Republicii Moldova.

PREŞEDINTELE COMITETULUI EXECUTIV Anca-Dana DRAGU

Nr.29. Chişinău, 12 februarie 2025.

Aprobat
prin Hotărârea Comitetului executiv
al Băncii Naţionale a Moldovei
nr.29 din 12 februarie 2025

REGULAMENT
privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii

Capitolul I
DISPOZIŢII GENERALE

Secţiunea 1
Domeniul de aplicare

1. Prezentul Regulament se aplică prestatorilor de servicii de plată (în continuare – *instituţii*) prevăzuţi la art.5 alin.(1) lit.a)-d) din Legea nr.114/2012 cu privire la serviciile de plată şi moneda electronică şi stabileşte cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor (în continuare – *TIC*), de securitate a informaţiei şi de continuitate a activităţii.

2. Scopul regulamentului este de a asigura că instituţiile dispun de un cadru intern adecvat de securitate a informaţiei şi de continuitate a activităţii, inclusiv pentru gestionarea riscurilor aferente TIC, aliniate la strategia generală de afaceri, iar procesele de guvernanţă internă sunt stabilite adecvat în raport cu sistemele TIC ale instituţiei şi protejează în mod corespunzător sistemele TIC ale acestora proporţional cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate.

Secţiunea a 2-a
Noţiuni principale

3. În sensul prezentului regulament se aplică următoarele definiţii:

3.1 Apetit la risc – nivelul absolut al riscurilor şi tipurile acestora, pe care o instituţie este dispusă să şi le asume în limita capacităţii sale de risc, conform modelului de afaceri în vederea realizării obiectivelor sale strategice;

3.2 Cadrul intern aferent TIC – totalitatea reglementărilor interne (primare şi secundare), a proceselor şi structurilor organizatorice TIC stabilite în cadrul instituţiei, care asigură gestionarea adecvată a riscurilor aferente TIC şi atingerea obiectivelor privind TIC ale instituţiei;

3.3 Cont privilegiat – cont de utilizator, într-un sistem informatic sau într-o reţea, care are privilegii sau drepturi de acces extinse faţă de conturile obişnuite;

3.4 Clasificarea informaţiilor – operaţiune de atribuire a unei categorii de confidenţialitate informaţiilor prin aplicarea marcajelor corespunzătoare acestora;

3.5 Declasificarea informaţiilor – operaţiune de diminuare a categoriei de confidenţialitate la care se atribuie unele informaţii cu excluderea acestora de sub incidenţa unor măsurile de securitate;

3.6 Funcţii critice – activităţi, servicii sau operaţiuni a căror întrerupere ar afecta în mod semnificativ performanţa financiară a instituţiei sau soliditatea ori continuitatea serviciilor şi activităţilor sale sau a cărei întrerupere, deficienţă sau eşuare în executare ar afecta în mod semnificativ respectarea în continuare, de către o instituţie a condiţiilor care au stat la baza acordării licenţei sau a

altor obligaţii care îi revin în temeiul legislaţiei aplicabile în domeniul financiar;

3.7 Incident – un eveniment unic sau o serie de evenimente neprevăzute care au apărut şi care au afectat disponibilitatea, confidenţialitatea, securitatea sistemelor/serviciilor, integritatea şi/sau autenticitatea datelor aferente TIC sau continuitatea prestării serviciilor;

3.8 Incident major – incident care are un impact negativ puternic asupra reţelelor, sistemelor, datelor TIC care sprijină funcţiile critice ale instituţiei sau a dus la indisponibilitatea sistemelor/serviciilor pentru o perioadă mai mare de 3 ore;

3.9 Înregistrare de audit – o singură înregistrare în jurnalul de audit care descrie apariţia unui singur eveniment auditabil din cadrul sistemului informaţional al instituţiei;

3.10 Jurnal de audit – secvenţă cronologică de înregistrări de audit, fiecare dintre acestea conţinând dovezi privind rezultatul executării unui proces sau a unei funcţii din cadrul unui sistem;

3.11 Gestionar al resursei TIC – subdiviziunea sau persoana responsabilă de gestiunea eficientă a resursei TIC din cadrul instituţiei;

3.12 Moment obiectiv pentru restabilire (MOR) – perioada minimă anterioară unui eveniment sau incident de continuitate pentru care instituţia recuperează sau restabileşte datele din surse alternative (ex. MOR de 24h înseamnă că informaţia va fi restabilită la starea din ziua precedentă, cu 24 de ore anterior apariţiei incidentului);

3.13 Perioadă maximă de întrerupere tolerabilă (PMIT) – perioada maximă pentru care activitatea poate fi întreruptă, iar impactul asupra activităţii instituţiei va fi tolerabil;

3.14 Profil de risc TIC – expunerea totală a unei instituţii la riscuri reale şi potenţiale aferente TIC;

3.15 Proprietar al resursei TIC – subdiviziunea sau persoană determinată ca fiind cea mai potrivită subdiviziune sau persoană de a controla resursa TIC, având în vedere importanţa acesteia în activitatea subdiviziunii sau persoanei respective;

3.16 Resursă TIC – orice bun material sau nematerial al instituţiei necesar gestiunii informaţiei, cum ar fi aplicaţii, echipamente de calcul şi alte elemente de infrastructură;

3.17 Risc TIC şi de securitate – reprezintă riscul înregistrării de pierderi din cauza încălcării confidenţialităţii, pierderii integrităţii sistemelor şi a datelor, caracterului necorespunzător sau indisponibilităţii sistemelor şi datelor sau incapacităţii de a schimba tehnologia informaţiei (TI) într-o perioadă de timp rezonabilă şi la costuri rezonabile, atunci când cerinţele de mediu sau de afaceri se schimbă. Riscul TIC şi de securitate include riscuri de securitate care rezultă fie din procese interne inadecvate sau care nu şi-au îndeplinit funcţia în mod corespunzător, fie din evenimente externe, inclusiv din atacuri cibernetice, sau din securitatea fizică inadecvată. Riscul TIC şi de securitate include cel puţin următoarele subcomponente:

3.17.1 Risc de disponibilitate şi continuitate aferente TIC – riscul ca performanţele sau disponibilitatea sistemelor/serviciilor şi datelor aferente TIC să fie afectate, inclusiv incapacitatea de a recupera în timp util procesele şi serviciile instituţiei;

3.17.2 Risc de schimbare aferent TIC – riscul care este un rezultat al incapacităţii instituţiei de a gestiona în timp util şi în mod controlat schimbările asociate sistemelor şi serviciilor aferente TIC;

3.17.3 Risc de integritate a datelor aferent TIC – riscul ca datele stocate şi/sau procesate de sistemele/serviciile aferente TIC să fie incomplete, inexacte sau incoerente la nivelul diferitelor sisteme TIC;

3.17.4 Risc asociat părţilor terţe şi externalizărilor TIC – riscul ca angajarea unei terţe părţi sau a unei alte entităţi a grupului (externalizare intra grup) pentru a furniza sisteme aferente TIC sau servicii conexe să afecteze performanţa şi gestionarea riscurilor în cadrul instituţiei;

3.17.5 Risc de conformitate aferent TIC – riscul de încălcare sau neconformare cu cadrul normativ, acorduri, practici recomandate sau standarde etice aferente TIC;

3.17.6 Risc aferent TIC semnificativ – risc aferent TIC care poate avea un impact negativ asupra sistemelor sau serviciilor aferente TIC critice;

3.17.7 Risc de concentrare a serviciilor TIC – o expunere la furnizori terţi de servicii TIC individuali sau multipli relaţionaţi, care creează un grad de dependenţă faţă de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficienţă a acestor furnizori poate pune în

pericol capacitatea unei instituţii de a oferi funcţii critice;

3.18 Sisteme aferente TIC – sisteme TIC configurate şi interconectate ca parte a unui mecanism sau a unei reţele care susţin efectuarea operaţiunilor unei instituţii;

3.19 Sistem informaţional – sistem de gestionare a informaţiei din cadrul unei instituţii, împreună cu resursele organizaţionale asociate, cum ar fi resurse informaţionale, resurse umane, structuri organizatorice;

3.20 Servicii aferente TIC – servicii furnizate prin intermediul sistemelor TIC unuia sau mai multor utilizatori interni sau externi;

3.21 Sisteme/servicii aferente TIC critice – sisteme/servicii TIC care sunt critice pentru instituţie din perspectiva continuităţii şi disponibilităţii acestora sau a securităţii informaţiei prelucrate şi/sau stocate şi sunt esenţiale pentru funcţionarea adecvată a proceselor de guvernanţă, responsabilităţilor/rolurilor corporative critice (inclusiv gestionarea riscurilor), proceselor de activitate şi operaţiunilor instituţiei;

3.22 Timp obiectiv pentru restabilire (TOR) – perioada maximă în care instituţia trebuie să îşi recupereze operaţiunile, serviciile sau sistemele critice în urma unui eveniment sau incident major. Se referă la durata de timp dintre momentul în care apare incidentul şi momentul în care operaţiunile afectate trebuie să fie restabilite la un nivel funcţional suficient pentru a permite desfăşurarea activităţii de prestare a serviciilor;

3.23 Toleranţă la risc – nivelul maxim al riscului acceptat de către instituţie care se încadrează în limitele reale din cadrul apetitului la risc asumat de către instituţie.

Capitolul II
CERINŢE PRIVIND CADRUL INTERN ŞI GESTIONAREA RISCURILOR AFERENTE TIC ŞI DE SECURITATE A INFORMAŢIEI

Secţiunea 1
Guvernanţa, cadrul intern TIC şi de securitate a informaţiei

4. Instituţia va deţine o strategie TIC şi de securitate a informaţiei care se conformează şi sprijină strategia generală de afaceri a instituţiei şi care este aprobată ca parte a strategiei generale de afaceri sau ca document separat şi este monitorizată adecvat de către organul de conducere al instituţiei, responsabil pe deplin de punerea în aplicare a acesteia.

5. Strategia TIC şi de securitate a informaţiei va defini următoarele:

5.1 modul în care va evolua TIC a instituţiei, pentru a sprijini şi a participa în mod eficient la strategia generală de afaceri, inclusiv la evoluţia structurii organizatorice, a modificărilor din sistemele TIC şi a dependenţelor cheie de furnizori terţi;

5.2 evoluţia arhitecturii TIC;

5.3 obiectivele clare de securitate a informaţiilor, punând accent pe sistemele şi serviciile TIC, pe personalul şi procesele instituţiei.

6. Instituţia va stabili planuri de acţiuni care să conţină măsuri ce vor fi luate în considerare la atingerea obiectivelor strategiei TIC şi de securitate a informaţiei. Planurile vor fi comunicate tuturor membrilor relevanţi ai personalului şi revizuite periodic la intervale regulate de timp, cel puţin cu o periodicitate anuală, pentru a asigura adecvarea acestora.

7. Instituţia va institui procese de monitorizare şi măsurare a eficacităţii punerii în aplicare a strategiei TIC şi de securitate a informaţiei.

8. Organul de conducere al instituţiei va asigura că numărul şi competenţa personalului instituţiei sunt corespunzătoare pentru a pune în aplicare strategia TIC şi de securitate a informaţiei, precum şi pentru a sprijini permanent necesităţile operaţionale TIC ale instituţiei.

9. Instituţia va asigura că membrii organului de conducere urmează periodic instruiri specifice aferente evaluării riscurilor TIC şi de securitate a informaţiei cu scopul de a dobândi cunoştinţe şi competenţe suficiente pentru a înţelege impactul acestora asupra activităţilor şi operaţiunilor instituţiei, precum şi pentru a actualiza cunoştinţele şi competenţele respective.

10. Instituţia va asigura că tot personalul TIC şi de securitate a informaţiei, inclusiv persoanele ce deţin funcţii-cheie, beneficiază cel puţin anual sau mai des, dacă este necesar, de formare profesională adecvată şi proporţională responsabilităţilor.

11. Instituţia se va asigura că bugetul alocat este suficient pentru a pune în aplicare strategia TIC şi de securitate a informaţiei.

12. Instituţia va asigura că are definite roluri şi responsabilităţi privind funcţiile TIC, gestiunea riscurilor TIC şi de securitate a informaţiilor, continuitatea activităţii, inclusiv în cadrul organului de conducere şi comitetele sale. Rolurile şi responsabilităţile sunt comunicate în mod clar, stabilite şi integrate în organizarea internă şi procesele relevante, inclusiv roluri privind colectarea şi agregarea informaţiilor despre riscuri şi raportarea acestora către organul de conducere.

13. Instituţia va asigura o segregare a funcţiei de administrare a riscurilor, a funcţiei de conformitate şi a funcţiei de audit intern, în conformitate cu cele trei linii ale modelului de apărare descrise în cele mai bune practici în domeniu.

14. Instituţia se va asigura că are stabilit cadrul intern aferent TIC şi securităţii informaţiei care protejează în mod adecvat sistemele şi serviciile sale TIC proporţional cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate şi va susţine implementarea strategiei TIC şi de securitate a informaţiei.

15. Instituţia va elabora şi va pune în aplicare o procedură clară de clasificare a reglementărilor interne primare (statutul, strategiile, codurile, politicile, regulamentele şi alte acte normative interne) şi secundare (instrucţiuni, proceduri, ghiduri, manuale sau alte documente) în domeniul TIC şi a nivelurilor de aprobare, în funcţie de importanţa şi aria de aplicare a acestora.

16. Instituţia va asigura revizuirea tuturor reglementărilor interne aferente domeniului TIC cel puţin o dată la 3 ani.

17. Instituţia va asigura o structură organizatorică adecvată din punctul de vedere al responsabilităţilor aferente TIC şi securităţii informaţiei, proporţională cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate.

18. Instituţia va dispune de un cadru de gestionare a riscurilor aferente TIC şi securităţii informaţiei, care să conţină procese şi proceduri pentru a asigura identificarea, analizarea, evaluarea, diminuarea, monitorizarea, raportarea şi menţinerea riscurilor în limitele toleranţei la risc pentru cel puţin următoarele categorii de riscuri aferente TIC şi securităţii informaţiei:

18.1 riscuri de disponibilitate şi continuitate;

18.2 riscuri de securitate;

18.3 riscuri de schimbare;

18.4 riscuri de integritate a datelor;

18.5 riscuri asociate părţilor terţe şi externalizărilor TIC;

18.6 riscuri de conformitate;

18.7 riscuri de concentrare a serviciilor TIC.

19. Instituţia va atribui gestionarea riscurilor aferent TIC şi de securitate a informaţiei unei funcţii separate de procesele operaţionale TIC.

20. Instituţia va asigura derularea procesului de revizuire a riscurilor descris la pct.18 pentru toate resursele TIC critice cel puţin o dată la 3 ani.

21. Instituţia va asigura pentru procesele de gestionare a riscurilor aferente TIC şi de securitate a informaţiei, resurse financiare, umane şi tehnice suficiente, precum şi alte resurse necesare care vor fi atât cantitativ, cât şi calitativ corespunzătoare cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate de instituţie.

22. Instituţia va institui o funcţie de Ofiţer de securitate a informaţiei, responsabil de elaborarea, coordonarea implementării şi monitorizarea respectării a cadrului intern aferent securităţii informaţiei. Ofiţerul de securitate a informaţiei, va fi subordonat direct preşedintelui organului executiv sau administratorului instituţiei. În funcţie de natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate de instituţie, funcţia de Ofiţer de securitate a informaţiei poate fi cumulată cu funcţia de la pct.19.

23. Instituţia va asigura că organizarea funcţiei de audit intern în ceea ce priveşte efectuarea auditului cadrului intern aferent TIC şi de securitate a informaţiei este proporţională cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri, activităţilor desfăşurate şi profilului de risc TIC al instituţiei. Auditul intern va avea capacitatea, urmând o abordare bazată pe riscuri, să revizuiască independent şi să ofere asigurări cu privire la conformarea tuturor proceselor şi activităţilor TIC şi de securitate a informaţiei cu reglementările aplicabile.

24. Instituţia va asigura efectuarea auditului de către un auditul intern şi/sau extern într-un interval de cel mult 3 ani a tuturor sistemelor şi serviciilor TIC critice. Auditul se va efectua cel puţin pentru următoarele sisteme, dacă sunt implementate de instituţie: Sistemul automatizat de plăţi interne (SAPI), instrumente de plată cu acces la distanţă, SWIFT, sistemele de bază (corebanking), sisteme de gestiune a bazelor de date, Active Directory (AD), procesul de gestiune al identităţilor şi accesului, inclusiv privilegiat, Firewall, VPN, sisteme de gestiune electronică a documentelor şi mesagerie/comunicare internă şi externă.

25. Instituţia va asigura implementarea unui proces de remediere în timp util a recomandărilor de audit intern/extern proporţional cu natura, amploarea şi complexitatea ameninţărilor, vulnerabilităţilor şi riscurilor TIC identificate pentru modelul de afaceri şi activităţile desfăşurate de instituţie.

Secţiunea a 2-a
Securitatea informaţiei

26. Instituţia va elabora o politică de securitate a informaţiei care va fi aprobată de organul de conducere al instituţiei şi va stabili contextul organizaţional de nivel general care să asigure atingerea obiectivelor cu privire la securitatea informaţiei şi securitatea cibernetică în cadrul instituţiei. Politica va conţine: scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare şi o descriere a rolurilor şi responsabilităţilor privind gestionarea securităţii informaţiei. Politica de securitate a informaţiei se va aplica şi va fi comunicată personalului instituţiei şi terţelor părţi ce interacţionează cu instituţia pe bază contractuală.

27. Instituţia va elabora un regulament ce va fi aprobat de organul de conducere al instituţiei, în care se va reglementa clasificarea, declasificarea informaţiilor în cadrul instituţiei şi se vor stabili măsuri de securitate aferente fiecărei categorii de informaţii. Instituţia va asigura implementarea unor măsuri ce vor permite aplicarea marcajelor de confidenţialitate pe toată informaţia ce circulă în cadrul instituţiei.

28. Instituţia va elabora proceduri privind controlul accesului logic la sistemele informatice sau serviciile TIC ale instituţiei, va monitoriza implementarea acestora şi se va asigura că acestea vor conţine minimum următoarele principii şi măsuri de control:

28.1. instituţia va acorda utilizatorilor drepturi minime de acces, strict necesare pentru executarea sarcinilor;

28.2. instituţia va asigura că acţiunile din cadrul sistemelor informatice şi serviciilor TIC critice pot fi atribuite unor utilizatori concreţi, iar utilizarea conturilor generice sau partajate va fi limitată şi documentată cu argumentele de rigoare;

28.3. instituţia va implementa măsuri de control aferente conturilor privilegiate prin limitarea strictă a utilizării lor şi monitorizarea permanentă prin înregistrarea tuturor acţiunilor şi activităţilor efectuate în conturile respective într-un sistem de gestiune centralizat al evenimentelor;

28.4. drepturile de acces ale utilizatorilor vor fi acordate, retrase sau modificate în conformitate cu responsabilităţile predefinite în cadrul proceselor automatizate în instituţie ce implică obligatoriu proprietarul resursei informaţionale. Pe parcursul concediilor sociale prevăzute de Codul muncii al Republicii Moldova nr.154/2003 sau suspendării contractului individual de muncă, sau în cazul neutilizării conturilor pentru o perioadă mai mare de 60 de zile conturile utilizatorilor vor fi dezactivate, iar în caz de încetare a contractului de muncă, contul va fi dezactivat şi drepturile de acces vor fi retrase imediat. În cazul concediilor anuale, implicit conturile utilizatorilor vor fi dezactivate, cu excepţia cazurilor aprobate de ofiţerul de securitate a informaţiei;

28.5. drepturile de acces la resursele TIC vor fi revizuite periodic, la intervale regulate de timp, cel puţin o dată pe an, pentru a se asigura că utilizatorii nu deţin drepturi excesive sau care excedă

necesităţile de serviciu;

28.6. instituţia va aplica metode sofisticate de autentificare, proporţionale cu nivelul de importanţă al sistemelor informatice, serviciilor TIC sau al informaţiei care se accesează, utilizând cel puţin parole complexe pentru conturile obişnuite şi autentificare cu doi factori pentru conturile privilegiate aferente sistemelor critice, precum şi în cazul accesării tuturor conturilor de la distanţă;

28.7. instituţia va implementa mecanisme automatizate de izolare a resurselor informaţionale ce au fost afectate de incidente de securitate sau au fost ţinta unor atacuri cibernetice.

29. Instituţia va elabora şi va pune în aplicare măsuri de securitate fizică pentru a proteja centrele de date şi zonele importante împotriva accesului neautorizat sau împotriva altor riscuri specifice. Accesul fizic la sistemele TIC şi de securitate a informaţiei va fi acordat doar persoanelor autorizate, cu o monitorizare corespunzătoare şi o revizuire periodică, la intervale regulate de timp, cel puţin o dată pe an, a drepturilor de acces.

30. Instituţia va elabora proceduri de control pentru asigurarea securităţii informaţiei şi integrităţii datelor aferente sistemelor şi serviciilor TIC şi să monitorizeze implementarea acestora. Aceste proceduri vor fi revizuite periodic, la intervale regulate de timp, cel puţin o dată pe an, şi vor conţine minimum următoarele principii şi măsuri de control:

30.1. instituţia va identifica vulnerabilităţile aferente aplicaţiilor software, sistemelor, echipamentelor de reţea şi staţiilor de lucru critice, prin efectuarea scanărilor periodice, şi va implementa în timp util măsuri de control de diminuare a impactului sau a probabilităţii exploatării vulnerabilităţilor identificate, riscurilor implicate sau va aplica măsuri de control compensatorii;

30.2. instituţia va implementa mecanisme de detectare rapidă a activităţilor anormale, a incidentelor TIC şi de securitate a informaţiilor, în special a atacurilor cibernetice prin implementarea sistemelor de prevenire şi detecţie a intruziunilor;

30.3. instituţia îşi va stabili configurări de securitate de referinţă pentru toate echipamentele de reţea critice;

30.4. instituţia va implementa segmentarea reţelei interne pe zone, în funcţie de echipamentele conectate şi informaţia accesibilă, cu aplicarea măsurilor de criptare a traficului pentru zonele ce conţin sisteme sau servicii critice;

30.5. instituţia va implementa măsuri de control şi protecţie a serverelor, staţiilor de lucru, dispozitivelor mobile şi altor echipamente ce sunt conectate la reţeaua acesteia sau gestionează informaţii din cadrul instituţiei;

30.6. instituţia va implementa mecanisme de monitorizare a informaţiilor ce părăsesc perimetrul reţelei interne. Vor fi monitorizate cel puţin: conexiunea la reţeaua internet, informaţiile imprimate, informaţiile copiate pe dispozitive externe, informaţiile transmise prin e-mail;

30.7. instituţia va implementa mecanisme de verificare a integrităţii aplicaţiilor software critice instalate pe serverele instituţiei;

30.8. instituţia va implementa măsuri de control eficiente aferente modificărilor şi schimbărilor sistemelor şi serviciilor TIC la nivelul componentelor hardware, software şi firmware, prin asigurarea unor mecanisme de planificare, înregistrare, testare, evaluare, aprobare, punere în aplicare şi verificare. În cazul unor situaţii de urgenţă instituţiile vor gestiona modificările necesare pe care le vor introduce cât mai curând posibil, urmând proceduri care să asigure o protecţie adecvată.

31. Instituţia va implementa măsuri de securitate aferente datelor, indiferent dacă sunt în repaus, în uz sau în tranzit şi mecanisme de monitorizare a evenimentelor de securitate, accesărilor neautorizate logice sau fizice, precum şi a încălcărilor confidenţialităţii, integrităţii şi disponibilităţii aferente resurselor informaţionale ale instituţiei.

32. Instituţia va introduce în toate acordurile sale cu părţi terţe, furnizori de servicii TIC, clauze privind asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor ce constituie secret bancar sau profesional, date cu caracter personal sau alte informaţii a căror divulgare ar putea avea un impact negativ asupra instituţiei, precum şi obligaţia furnizorilor de a coopera pe deplin cu autorităţile de supraveghere şi, după caz, de rezoluţie.

33. Instituţia va elabora şi va pune în aplicare un cadru de evaluare, revizuire şi testare a securităţii

informaţiei, care să valideze eficienţa şi eficacitatea măsurilor de control implementate respectând cel puţin următoarele condiţii:

33.1. scanări ale vulnerabilităţilor şi teste de penetrare corespunzătoare nivelului riscurilor identificate de instituţie şi importanţei sistemelor sau serviciilor TIC;

33.2. testele de penetrare aferente sistemelor şi serviciilor TIC critice vor fi efectuate pe bază continuă, cu o periodicitate de cel puţin o dată la 3 ani, sau mai des la solicitarea Băncii Naţionale a Moldovei;

33.3. testele de penetrare vor fi efectuate conform unor scenarii prestabilite validate de către instituţie şi vor fi realizate pe sistemele de producţie în timp real care sprijină activităţile instituţiei;

33.4. testele de penetrare urmează a fi efectuate de experţi care au competenţe, cunoştinţe suficiente şi relevante domeniului, confirmate prin deţinerea certificărilor internaţionale (ex. CEPT, CPT, CEH, OSCP, OPST, CPENT, GPEN, GWART, LPT, PTC sau alte certificări recunoscute la nivel internaţional);

33.5. instituţia va efectua testări de securitate în cazul modificărilor majore la nivel de infrastructură, la nivel de procese, ca urmare a unor incidente operaţionale sau de securitate majore sau lansării de sisteme informaţionale noi/modificate substanţial, accesibile din internet.

34. Instituţia va stabili un program de formare profesională, care să includă instruiri periodice, dar cel puţin anual, de conştientizare cu privire la riscurile de securitate a informaţiei pentru tot personalul în conformitate cu reglementările interne şi pentru contractanţi în cazul în care instituţia consideră că este necesar.

Secţiunea a 3-a
Operaţiunile TIC

35. Instituţia va menţine un inventar actualizat al resurselor TIC şi de securitate a informaţiei critice, care să conţină configurările, legăturile logice, fizice, interconexiunile şi interdependenţele de alte resurse din cadrul instituţiei, precum şi furnizorii terţi de servicii TIC. Inventarul va fi suficient de detaliat pentru a permite identificarea imediată a resursei, amplasamentul acesteia, proprietarul şi gestionarul resursei TIC.

36. Instituţia va utiliza sisteme şi servicii TIC actualizate ce sunt proporţionale cu natura, amploarea şi complexitatea modelului de afaceri şi activităţilor desfăşurate de instituţie, ce sunt fiabile şi dispun de o capacitate suficientă pentru a prelucra cu precizie datele şi pentru a face faţă nevoilor suplimentare de prelucrare a informaţiilor în condiţii de criză.

37. Instituţia va defini şi va pune în aplicare procese de planificare şi monitorizare a performanţei şi capacităţii sistemelor, serviciilor şi echipamentului TIC şi de securitate a informaţiei pentru a împiedica, detecta şi a răspunde prompt la eventuale incidente legate de performanţă.

38. Instituţia va elabora şi va pune în aplicare măsuri privind crearea copiilor de rezervă şi de restaurare a datelor şi sistemelor/serviciilor TIC critice şi de securitate a informaţiei, pentru a se asigura că acestea pot fi restabilite conform cerinţelor instituţiei. Procedurile respective vor fi testate periodic la intervale regulate de timp, cel puţin cu o periodicitate anuală.

39. Instituţia se va asigura că copiile de rezervă aferente sistemelor şi serviciilor TIC critice sunt păstrate în siguranţă, în formă criptată, într-o altă locaţie şi că nu sunt expuse aceloraşi riscuri ca şi cele din cadrul centrului de date principal.

40. Instituţia va asigura mecanisme de verificare a integrităţii copiilor de rezervă.

41. Instituţia va asigura că evenimentele de securitate relevante unor eventuale investigaţii de pe toate resursele TIC critice sunt colectate în cadrul unor soluţii specializate pentru colectarea şi asigurarea integrităţii şi disponibilităţii acestora.

Secţiunea a 4-a
Gestionarea incidentelor şi problemelor

42. Instituţia va institui şi va pune în aplicare un proces de monitorizare, gestionare şi înregistrare a incidentelor, cu păstrarea detaliată a tuturor probelor privind incidentele TIC, de securitate a informaţiei,

de continuitate a activităţii pentru a permite instituţiei să continue sau să reia rapid procesele critice în cazul unor întreruperi.

43. Instituţia va stabili criterii clare de clasificare a incidentelor după prioritatea de soluţionare şi impact, va defini roluri şi responsabilităţi de soluţionare şi va elabora proceduri de analiză a cauzelor ce au provocat incidentele şi a lecţiilor învăţate cu implementarea unor măsuri de control adiţionale sau ajustarea măsurilor existente.

44. Instituţia va stabili proceduri eficiente de comunicare internă şi externă, notificare şi escaladare a incidentelor care să prevadă ca incidentele majore să fie comunicate imediat organului de conducere, iar ulterior la intervale regulate de timp, cel puţin o dată la 6 luni, să fie comunicate toate incidentele, inclusiv incidentele evitate dar cu un posibil impact negativ ridicat asupra sistemelor şi serviciilor TIC, comunicând-se măsurile de remediere luate imediat şi cele care urmează a fi implementate pentru a preveni astfel de incidente pe viitor.

45. Instituţia va institui şi va pune în aplicare un proces de monitorizare şi gestionare a problemelor. În sensul prezentului punct, prin problemă se înţelege cauza principală care stă la baza unor incidente care se repetă de mai multe ori într-un interval de timp.

Secţiunea a 5-a
Gestionarea proiectelor

46. Instituţia va stabili procese şi va elabora proceduri privind gestiunea proiectelor TIC de securitate a informaţiei şi continuitate a activităţii care să definească rolurile şi responsabilităţile pe domeniu, necesare în scopul de a susţine atingerea obiectivelor strategiei TIC şi de securitate a informaţiei.

47. Instituţia va asigura în cadrul documentaţiei pentru fiecare proiect TIC, de securitate a informaţiei şi continuitate a activităţii că sunt definite cel puţin următoarele informaţii:

47.1. scopul şi obiectivele proiectului;

47.2. rolurile şi responsabilităţile;

47.3. evaluarea riscurilor asociate proiectului, în conformitate cu prevederile pct.18;

47.4. planul, calendarul şi etapele proiectului;

47.5. principalele obiective intermediare;

47.6. cerinţele de gestionare a modificărilor;

47.7. cerinţele de securitate a informaţiei care sunt analizate şi aprobate de către o funcţie independentă de cea de gestiune a proiectului.

48. Instituţia, aferent portofoliului de proiecte TIC, de securitate a informaţiei şi continuitate a activităţii, va monitoriza şi va diminua în mod corespunzător riscurile care pot rezulta din interdependenţele dintre diferite proiecte precum şi din dependenţele mai multor proiecte de aceleaşi resurse şi/sau competenţe.

49. Instituţia se va asigura că proprietarii tuturor resurselor afectate de un proiect TIC sunt reprezentaţi în echipa de proiect şi că echipa de proiect deţine cunoştinţele necesare şi suficiente pentru a asigura implementarea sigură şi cu succes a proiectului.

50. Instituţia va stabili proceduri de raportare ad-hoc şi la intervale regulate de timp, cel puţin o dată la 6 luni, către organul de conducere, a informaţiilor privind evoluţia şi riscurile asociate proiectelor TIC de securitate a informaţiei şi continuitate a activităţii în funcţie de importanţa şi dimensiunea acestora.

Secţiunea a 6-a
Achiziţia şi dezvoltarea de sisteme TIC

51. Instituţia, aplicând o abordare bazată pe riscuri, va stabili procese şi va elabora proceduri privind achiziţia, dezvoltarea şi menţinerea sistemelor şi serviciilor TIC şi de securitate a informaţiei.

52. Instituţia se va asigura că, înainte de orice achiziţie sau dezvoltare a sistemelor TIC şi de securitate a informaţiei, cerinţele funcţionale şi nefuncţionale, inclusiv cerinţele minime de securitate a informaţiilor, sunt clar definite şi aprobate de către organul de conducere relevant.

53. Instituţia va implementa măsuri de control pentru diminuarea riscurilor de modificare

neintenţionată sau de manipulare intenţionată a sistemelor TIC şi de securitate a informaţiei pe durata dezvoltării şi implementării în mediul de producţie.

54. Instituţia va elabora o metodologie de testare şi aprobare a sistemelor TIC şi de securitate a informaţiei, care să asigure că noile sisteme funcţionează aşa cum au fost proiectate şi că mediile de testare utilizate reflectă în mod corespunzător mediul de producţie.

55. Instituţia va asigura efectuarea testării, inclusiv din punctul de vedere al securităţii informaţiei, a măsurilor de dezvoltare importante şi a modificărilor de infrastructură, a proceselor sau procedurilor, care să cuprindă şi situaţia în care aceste modificări sunt efectuate ca urmare a unor incidente majore, proporţional cu natura, amploarea şi complexitatea riscurilor inerente.

56. Instituţia va asigura segregarea responsabilităţilor aferent domeniului de dezvoltare, testare şi implementare.

Secţiunea a 7-a
Continuitatea activităţii

57. Instituţia va elabora o politică de asigurare a continuităţii activităţii care va fi aprobată de organul de conducere al instituţiei şi va stabili contextul organizaţional de nivel general care să asigure atingerea obiectivelor cu privire la continuitatea activităţii instituţiei. Politica va conţine scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare şi o descriere a rolurilor şi responsabilităţilor privind gestionarea continuităţii activităţii în cadrul instituţiei. Politica de continuitate a activităţii se va aplica şi va fi comunicată personalului instituţiei şi, după caz, terţelor părţi ce interacţionează cu instituţia pe bază contractuală.

58. Instituţia va elabora un regulament care va fi aprobat de organul de conducere şi care va stabili cadrul intern aferent continuităţii activităţii proporţional cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri, eficient şi capabil de a asigura protecţia personalului instituţiei vizitatorilor şi reprezentanţilor terţelor părţi contra ameninţărilor majore posibile, precum şi continuitatea proceselor critice ale instituţiei în situaţii de incident major. Regulamentul va conţine descrierea corespunzătoare cel puţin a următoarelor procese de gestiune a continuităţii activităţii:

58.1. inventarierea tuturor proceselor de activitate şi identificarea celor ce sunt critice din punctul de vedere al derulării continue în timp;

58.2. evaluarea impactului pe care îl pot avea întreruperile în procesele identificate asupra activităţii instituţiei;

58.3. stabilirea indicatorilor de continuitate aferenţi proceselor prin specificarea PMIT pentru procesele de activitate;

58.4. identificarea proceselor critice în timp şi stabilirea resurselor necesare pentru derularea normală a acestora, în particular: resurse de personal, sisteme şi resurse TIC, încăperi, alte resurse;

58.5. stabilirea indicatorilor de continuitate pentru toate resursele critice TIC prin indicarea TOR şi MOR;

58.6. analiza riscurilor de continuitate ce pot duce la întreruperea proceselor critice. Implicit se vor analiza riscurile de bază ce presupun indisponibilitatea resurselor necesare pentru desfăşurarea normală a proceselor;

58.7. stabilirea strategiilor de continuitate pentru desfăşurarea proceselor critice în timp în condiţiile în care riscurile au fost identificate. Urmează a fi considerate cel puţin 2 strategii de continuitate: restabilirea resurselor critice sau aplicarea procedurilor alternative de lucru;

58.8. clasificarea proceselor critice în grupe de urgenţă în baza indicatorilor PMIT, pentru a stabili priorităţile acţiunilor de restabilire când sunt afectate sau întrerupte mai multe procese simultan;

58.9. elaborarea planului de asigurare a continuităţii activităţii (în continuare – PCA) în baza rezultatelor obţinute în cadrul etapelor descrise anterior prin care sunt stabilite măsurile necesare de întreprins pentru a asigura un nivel adecvat al continuităţii activităţii instituţiei;

58.10. stabilirea unei strategii de comunicare pe plan intern şi extern în cazurile de incidente majore sau dezastre ce au afectat continuitatea activităţii instituţiei;

58.11. instruirea personalului instituţiei pentru ca acesta să conştientizeze importanţa asigurării

continuităţii activităţii instituţiei, să cunoască responsabilităţile individuale desemnate în cadrul acestui proces, să înţeleagă şi să fie capabili să aplice cerinţele actelor interne la planificarea, implementarea, monitorizarea şi îmbunătăţirea procesului în limita responsabilităţilor atribuite;

58.12. testarea PCA, precum şi a anexelor acestuia cu o periodicitate regulată, cel puţin o dată la 2 ani. Rezultatele testărilor vor fi adecvat documentate, cu păstrarea probelor comprehensive şi raportate către organul de conducere. Testarea PCA va aborda în mod obligatoriu:

58.12.1. testarea măsurilor de asigurare a continuităţii sistemelor şi infrastructurii TIC;

58.12.2. testarea măsurilor de asigurare a continuităţii la nivel de roluri şi personal;

58.12.3. testarea măsurilor implementate aferente serviciilor şi sistemelor de infrastructură non-TIC (ex. electricitate, antiincendiar, alarmă, climatizare etc.);

58.12.4. testarea cunoaşterii prevederilor PCA de către personalul responsabil de continuitatea activităţii;

58.12.5. testarea reluării activităţii a tuturor proceselor şi resurselor critice în cadrul locaţiei de rezervă.

58.13. revizuirea la intervale regulate de timp, cel puţin o dată la 3 ani, a PCA, precum şi a anexelor acestuia pentru a asigura o îmbunătăţire continuă a procesului de gestiune a continuităţii activităţii instituţiei.

59. Instituţia va elabora adiţional sau în cadrul PCA cel puţin următoarele planuri:

59.1. planul de continuitate pentru resursele de personal, ce are ca scop de a asigura disponibilitatea resurselor de personal în număr necesar şi corespunzător instruite şi calificate pentru a putea continua procesele critice ale instituţiei;

59.2. planul de asigurare a continuităţii TIC, ce are ca scop de a asigura disponibilitatea sistemelor şi serviciilor TIC în scopul exercitării proceselor critice ale instituţiei în conformitate cu cerinţele TOR şi MOR stabilite;

59.3. planul de comunicare în situaţii excepţionale.

60. Instituţia va pune în aplicare, fără întârziere, planurile specifice incidentelor de continuitate identificate, în scopul restabilirii în timp util a proceselor operaţionale critice şi pentru a preveni sau a limita impactul asupra activităţii.

61. În relaţia cu părţi terţe, prestatori de servicii TIC, instituţia se va asigura că poate să înceteze relaţiile contractuale fără întreruperea activităţilor critice sau a continuităţii şi calităţii furnizării serviciilor. La încetarea contractului inclusiv din iniţiativa furnizorului, instituţia va asigura existenţa unor strategii de ieşire cu stabilirea unei perioade de tranziţie care să îi permită să treacă la un alt furnizor de servicii TIC sau să reintegreze activitatea la sediu.

62. Anual, în coordonare prealabilă cu Banca Naţională a Moldovei (în continuare – *BNM*), pe parcursul lunii octombrie/noiembrie, pe parcursul unei zile lucrătoare instituţia va pune în aplicare Planul de asigurare a continuităţii TIC din cadrul centrului de date de rezervă pentru anumite sisteme sau servicii critice agreate de BNM.

63. O dată la 3 ani, în coordonare prealabilă cu BNM, în luna noiembrie, instituţia pe parcursul unei zile lucrătoare va pune în aplicare PCA pentru procesele şi resursele critice, cu rularea acestora din cadrul centrului de date de rezervă, precum şi cu relocarea personalului critic la o locaţie de rezervă.

64. Instituţia va evalua eficacitatea punerii în aplicare a planurilor de continuitate şi va identifica măsuri de îmbunătăţire a calităţii şi rapidităţii deciziilor luate, reacţiei la incidente, pentru a consolida gradul de pregătire a instituţiei de a face faţă întreruperilor în activitate.

Secţiunea a 8-a
Integritatea, disponibilitatea informaţiei şi continuitatea TIC

65. Instituţia va asigura, inclusiv în cazul externalizării sistemelor/serviciilor aferente TIC critice, integritatea şi disponibilitatea informaţiei precum şi o perioadă de retenţie de minimum 12 luni, fie de la ultima perioadă supusă controlului de către BNM, dar nu mai mult de 24 de luni.

Se va asigura retenţia informaţiei conţinute în:

65.1. jurnalele de audit ce conţin înregistrări de audit relevante pentru cel puţin următoarele

sisteme/servicii, dacă sunt implementate de instituţie: SAPI, instrumente de plată cu acces la distanţă, SWIFT, sistem de bază (corebanking), sisteme de gestiune a bazelor de date, Active Directory (AD), Privileged Acces Management (PAM), Firewall, Virtual Private Network (VPN), echipamente critice de reţea, sisteme de gestiune electronică a documentelor;

65.2. mesajele transmise/primite prin intermediul serviciului de poştă electronică oficială a instituţiei;

65.3. sistemele de monitorizare video a zonelor critice aferente centrului de date principal şi centrului de date de rezervă.

66. Instituţia va asigura crearea copiilor de rezervă ale bazelor de date aferente sistemelor/serviciilor TIC critice efectuate după următoarea schemă:

66.1. copie de tip full la finele fiecărui an cu asigurarea retenţiei pentru ultimii 2 ani;

66.2. copie de tip full la finele fiecărei luni cu asigurarea retenţiei pentru ultimele 6 luni;

66.3. copie de tip diferenţial la finele fiecărei zile cu asigurarea retenţiei pentru ultimele 30 zile.

67. Instituţia va asigura în cadrul Platformei centrale de schimb de informaţii (în continuare – PCSI), înregistrarea, stocarea şi gestiunea materialelor preliminare aferente şedinţelor organului de conducere ce ţin de domeniul TIC precum şi înregistrarea, în termen de 10 zile, a deciziilor luate de organul de conducere aferente domeniului TIC. Integritatea tuturor documentelor în cadrul sistemului va fi confirmată printr-o semnătură electronică calificată.

68. Organul de conducere al instituţiei va asigura că informaţia stocată în cadrul sistemelor TIC ce conţin date contabile este actuală şi se bazează pe tranzacţii reale.

69. Instituţia va asigura redundanţa conexiunilor de date de la doi prestatori de servicii pentru cel puţin 30% din punctele de prezenţă (sucursale) şi pentru cel puţin 30% din ATM-uri. La baza deciziei date urmează a fi efectuată o analiză de riscuri ce va avea ca scop accesibilitatea unui număr cât mai larg al populaţiei la aceste ATM-uri şi puncte de prezenţă.

70. Instituţia va asigura că dispune de un centru de date de rezervă capabil să preia activitatea tuturor proceselor critice în cazul indisponibilităţii centrului de date principal.

71. Instituţia va asigura conexiunea la reţeaua internet pentru centrul de date principal şi centrul de date de rezervă prin intermediul a cel puţin 2 prestatori de servicii.

72. Instituţia va asigura că centrul de date principal şi centrul de date de rezervă dispun de următoarele sisteme şi echipamente:

72.1. sistem de aer condiţionat redundant sau contract de suport pentru reparaţia sistemului cu timp de punere în funcţiune de maximum 6 ore;

72.2. generator de curent electric capabil să asigure necesităţile echipamentelor;

72.3. sistem de monitorizare video ce acoperă toate zonele;

72.4. sistem de detectare a umidităţii şi scurgere a apei;

72.5. sistem de acces fizic în încăpere cu mai mulţi factori sau biometric;

72.6. sistem de stingere automatizată a incendiilor;

72.7. sistem de monitorizare a temperaturii.

73. Instituţia va asigura redundanţa următoarelor echipamente şi servicii din centru de date principal:

73.1. echipamentelor de reţea ce asigură conexiunea la internet a centrului de date central şi a centrului de date de rezervă;

73.2. echipamentelor de reţea ce asigură legătura între nodurile informaţionale principale ale instituţiei;

73.3. echipamentelor firewall;

73.4. echipamentelor pe care rulează bazele de date aferente sistemelor şi serviciilor TIC critice;

73.5. echipamentelor pe care rulează sistemul de bază (corebanking), SWIFT, instrumente de plată cu acces la distanţă în cazul în care sistemele respective sunt implementate în instituţie;

73.6. serviciilor DNS externe ale instituţiei, cu localizarea obligatorie a unuia pe teritoriul Republicii Moldova.

74. Instituţia va asigura replicarea bazelor de date ce conţin date financiare critice în centrul de

date de rezervă.

75. Instituţia va asigura lunar în regim offline, păstrarea în formă criptată a cel puţin o copie de rezervă de tip full a datelor pentru toate sistemele sale critice într-o locaţie diferită de centrul de date principal şi centrul de date de rezervă.

76. Instituţia va asigura că toate ATM-urile, serverele, bazele de date şi staţiile sau terminalele de lucru rulează pe sisteme de operare ce dispun de suport din partea producătorului. Excepţie sunt sistemele de tip vechi/legacy ce vor rula într-o reţea izolată şi aferent cărora se vor aplica măsuri compensatorii de securitate. Lista sistemelor exceptate urmează a fi aprobată de organul de conducere al instituţiei.

Capitolul III
EVALUAREA RISCURILOR TIC

77. Instituţia îşi va evalua profilul de risc aferent TIC cel puţin anual sau dacă au fost operate modificări majore în procesele, sistemele, serviciile sau echipamentele critice aferente TIC. Ca urmare a evaluării profilului de risc, după caz, instituţia va revizui cadrul intern corespunzător, precum şi măsurile de control aplicabile.

78. Instituţia, în cazul în care a externalizat funcţii operaţionale şi/sau servicii TIC şi sisteme TIC ale oricărei activităţi de prestare de servicii către furnizori terţi, inclusiv către entităţile din grup, va asigura eficacitatea măsurilor prevăzute în prezentul Regulament. Instituţia rămâne pe deplin responsabilă pentru evaluarea eficacităţii măsurilor de securitate ale funcţiilor operaţionale externalizate aferente serviciilor de plată şi/sau serviciilor TIC şi sistemelor TIC ale oricărei activităţi de prestare de servicii.

79. BNM, în cadrul controalelor şi prin dispunerea efectuării misiunilor de audit, evaluează cadrul intern aferent TIC al fiecărei instituţii, în raport cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate şi cu profilul/apetitul de risc al instituţiei.

80. În cazul în care, ca urmare a evaluării efectuate, se constată că cadrul intern aferent TIC nu este adecvat în raport cu profilul/apetitul de risc, cu natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităţilor desfăşurate de instituţie, BNM poate impune cerinţe concrete faţă de cadrul intern aferent TIC, măsuri de supraveghere, măsuri de remediere, sancţiuni sau măsuri sancţionatoare.

Capitolul IV
RAPORTAREA

81. Instituţia este obligată să notifice BNM prin intermediul PCSI sau în cazul indisponibilităţii acestuia la adresa de e-mail SupraveghereTIC@bnm.md despre incidentele produse, respectând următoarele condiţii:

81.1. în cazul unui incident care a generat disfuncţionalităţi sau care a afectat disponibilitatea, confidenţialitatea, integritatea şi/sau autenticitatea informaţiilor fie a afectat continuitatea sistemelor/serviciilor ce susţin desfăşurarea funcţiilor critice, se transmite o notificare iniţială cu privire la incidentul produs, fără întârziere, dar nu mai târziu de sfârşitul zilei lucrătoare sau, în cazul unui incident care a avut loc cu mai puţin de 2 ore înainte de încheierea zilei lucrătoare, nu mai târziu de 4 ore de la începutul următoarei zile lucrătoare;

81.2. în cazul unui incident care a generat disfuncţionalităţi la nivelul funcţiilor semnificative, a afectat disponibilitatea, confidenţialitatea, integritatea şi/sau autenticitatea informaţiilor, a afectat continuitatea serviciilor aferente plăţilor, prestatorii de servicii de plată, se transmite o notificare iniţială cu privire la incidentul produs, fără întârziere, dar nu mai târziu de următoarea zi lucrătoare după producerea incidentului;

81.3. un raport intermediar, în termen de cel mult 3 zile din ziua producerii incidentului prevăzut la subpct.81.1 sau subpct.81.2, care va conţine informaţii suplimentare cu privire la circumstanţele incidentului produs, procesele/sistemele/serviciile afectate, impactul preliminar estimat şi măsurile de remediere întreprinse până la acel moment de instituţie;

81.4. un raport final, semnat de un membru al organului de conducere al instituţiei, în termen de cel

mult 20 de zile din ziua notificării iniţiale prevăzute la subpct.81.1 sau subpct.81.2. Raportul va conţine analiza cauzelor principale ce au dus la producerea incidentului, a impactului efectiv asupra activităţilor instituţiei sau a intereselor financiare ale clienţilor, măsurile întreprinse de instituţie şi care urmează a mai fi întreprinse pentru a preveni sau minimiza impactul de la producerea incidentelor de acest tip pe viitor.

82. Instituţiile vor transmite către BNM prin PCSI, sau în cazul indisponibilităţii acestuia la adresa de e-mail SupraveghereTIC@bnm.md, în termen de o lună de la încheierea anului de gestiune, informaţii cu privire la următoarele:

82.1. rezultatele testelor de penetrare;

82.2. rezultatele ultimelor scanări de vulnerabilităţi efectuate pentru toate resursele critice, conform situaţiei din luna decembrie;

82.3. raportul de evaluare a sistemului SWIFT în conformitate cu Customer Security Controls Framework (CSCF), în cazul în care a fost efectuată o astfel de evaluare;

82.4. raportul de evaluare a instituţiei în conformitate cu standardul PCI-DSS, în cazul când instituţia este supusă unei astfel de evaluări anuale;

82.5. rezultatele testărilor de continuitate a sistemelor/serviciilor aferente TIC critice, în cazul în care acestea au avut loc fără participarea BNM;

82.6. raportul privind gestionarea riscurilor aferente TIC identificate ca fiind semnificative.