

REGULAMENT
privind cerințele minime pentru gestionarea riscurilor aferente tehnologiei
informației și comunicațiilor, securității informației și continuității activității

Publicat în Monitorul Oficial al Republicii Moldova nr. 62-65 din 20.02.2025, art. 131

APROBAT
prin Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr. 29 din 12 februarie 2025
În vigoare: din **20 martie 2025**

Prestatorii de servicii de plată vor asigura conformarea cu prevederile
pct. 81 din Regulament, care intră în vigoare în termen de 3 luni,
pct. 4-56, pct. 62, pct. 65-67, pct. 76-80 și pct. 82 – în termen de 9 luni,
pct. 57, pct. 58 subpct. 58.1-58.11 – în termen de 12 luni,
subpct. 58.12-61, pct. 63-64 și pct. 68-75 – în termen de 15 luni.

Capitolul I
DISPOZIȚII GENERALE

Secțiunea 1
Domeniul de aplicare

1. Prezentul Regulament se aplică prestatorilor de servicii de plată (în continuare – instituții) prevăzuți la art. 5 alin. (1) lit. a)-d) din *Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică* și stabilește cerințele minime pentru gestionarea riscurilor aferente tehnologiei informației și comunicațiilor (în continuare – TIC), de securitate a informației și de continuitate a activității.
2. Scopul regulamentului este de a asigura că instituțiile dispun de un cadru intern adecvat de securitate a informației și de continuitate a activității, inclusiv pentru gestionarea riscurilor aferente TIC, aliniate la strategia generală de afaceri, iar procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele TIC ale instituției și protejează în mod corespunzător sistemele TIC ale acestora proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate.

Secțiunea a 2-a
Noțiuni principale

3. În sensul prezentului regulament se aplică următoarele definiții:
 - 3.1 **Apetit la risc** – nivelul absolut al riscurilor și tipurile acestora, pe care o instituție este dispusă să și le asume în limita capacității sale de risc, conform modelului de afaceri în vederea realizării obiectivelor sale strategice;

- 3.2 **Cadrul intern aferent TIC** – totalitatea reglementărilor interne (primare și secundare), a proceselor și structurilor organizatorice TIC stabilite în cadrul instituției, care asigură gestionarea adecvată a riscurilor aferente TIC și atingerea obiectivelor privind TIC ale instituției;
- 3.3 **Cont privilegiat** – cont de utilizator, într-un sistem informatic sau într-o rețea, care are privilegii sau drepturi de acces extinse față de conturile obișnuite;
- 3.4 **Clasificarea informațiilor** – operațiune de atribuire a unei categorii de confidențialitate informațiilor prin aplicarea marcajelor corespunzătoare acestora;
- 3.5 **Declasificarea informațiilor** – operațiune de diminuare a categoriei de confidențialitate la care se atribuie unele informații cu excluderea acestora de sub incidența unor măsurile de securitate;
- 3.6 **Funcții critice** - activități, servicii sau operațiuni a căror întrerupere ar afecta în mod semnificativ performanța financiară a instituției sau soliditatea ori continuitatea serviciilor și activităților sale sau a cărei întrerupere, deficiență sau eșuare în executare ar afecta în mod semnificativ respectarea în continuare, de către o instituție a condițiilor care au stat la baza acordării licenței sau a altor obligații care îi revin în temeiul legislației aplicabile în domeniul financiar;
- 3.7 **Incident** – un eveniment unic sau o serie de evenimente neprevăzute care au apărut și care au afectat disponibilitatea, confidențialitatea, securitatea sistemelor/serviciilor, integritatea și/sau autenticitatea datelor aferente TIC sau continuitatea prestării serviciilor;
- 3.8 **Incident major** – incident care are un impact negativ puternic asupra rețelelor, sistemelor, datelor TIC care sprijină funcțiile critice ale instituției 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 apariția unui singur eveniment auditabil din cadrul sistemului informațional al instituției;
- 3.10 **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;
- 3.11 **Gestionar al resursei TIC** – subdiviziunea sau persoana responsabilă de gestiunea eficientă a resursei TIC din cadrul instituției;
- 3.12 **Momentul obiectiv pentru restabilire (MOR)** – perioada minimă anterioară unui eveniment sau incident de continuitate pentru care instituția recuperează sau restabilește datele din surse alternative (ex. MOR de 24h înseamnă că informația va fi restabilită la starea din ziua precedentă, cu 24 de ore anterior apariției incidentului);
- 3.13 **Perioada maximă de întrerupere tolerabilă (PMIT)** – perioada maximă pentru care activitatea poate fi întreruptă, iar impactul asupra activității instituției va fi tolerabil;
- 3.14 **Profil de risc TIC** – expunerea totală a unei instituții la riscuri reale și potențiale aferente TIC;
- 3.15 **Proprietar al resursei TIC** – subdiviziunea sau persoana determinată ca fiind cea mai potrivită subdiviziune sau persoană de a controla resursa

TIC, având în vedere importanța acesteia în activitatea subdiviziunii sau persoanei respective;

- 3.16 **Resursă TIC** – orice bun material sau nematerial al instituției necesar gestiunii informației, cum ar fi aplicații, echipamente de calcul și alte elemente de infrastructură;
- 3.17 **Risc TIC și de securitate** – reprezintă riscul înregistrării de pierderi din cauza încălcării confidențialității, pierderii integrității sistemelor și a datelor, caracterului necorespunzător sau indisponibilității sistemelor și datelor sau incapacității de a schimba tehnologia informației (TI) într-o perioadă de timp rezonabilă și la costuri rezonabile, atunci când cerințele de mediu sau de afaceri se schimbă. Riscul TIC și de securitate include riscuri de securitate care rezultă fie din procese interne inadecvate sau care nu și-au îndeplinit funcția în mod corespunzător, fie din evenimente externe, inclusiv din atacuri cibernetice sau din securitatea fizică inadecvată. Riscul TIC și de securitate include cel puțin următoarele subcomponente:
 - 3.17.1 **Risc de disponibilitate și continuitate aferente TIC** – riscul ca performanțele sau disponibilitatea sistemelor/serviciilor și datelor aferente TIC să fie afectate, inclusiv incapacitatea de a recupera în timp util procesele și serviciile instituției;
 - 3.17.2 **Risc de schimbare aferent TIC** – riscul care este un rezultat al incapacității instituției de a gestiona în timp util și în mod controlat schimbările asociate sistemelor și serviciilor aferente TIC;
 - 3.17.3 **Risc de integritate a datelor aferent TIC** – riscul ca datele stocate și/sau procesate de sistemele/serviciile aferente TIC să fie incomplete, inexacte sau incoerente la nivelul diferitelor sisteme TIC;
 - 3.17.4 **Risc asociat părților terțe și externalizărilor TIC** – riscul ca angajarea unei terțe părți sau a unei alte entități a grupului (externalizare intra grup) pentru a furniza sisteme aferente TIC sau servicii conexe să afecteze performanța și gestionarea riscurilor în cadrul instituției;
 - 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 terți de servicii TIC individuali sau multipli relaționați, care creează un grad de dependență față de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestor furnizori poate pune în pericol capacitatea unei instituții de a oferi funcții critice;
- 3.18 **Sisteme aferente TIC** – sisteme TIC configurate și interconectate ca parte a unui mecanism sau a unei rețele care susțin efectuarea operațiunilor unei instituții;

- 3.19 Sistem informațional** - sistem de gestionare a informației din cadrul unei instituții, împreună cu resursele organizaționale asociate, cum ar fi resurse informaționale, resurse umane, structuri organizatorice;
- 3.20 Servicii aferente TIC** – servicii furnizate prin intermediul sistemelor TIC unui sau mai multor utilizatori interni sau externi;
- 3.21 Sisteme/servicii aferente TIC critice** – sisteme/servicii TIC care sunt critice pentru instituție 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 instituției;
- 3.22 Timpul obiectiv pentru restabilire (TOR)** – perioada maximă în care instituția trebuie să își recupereze operațiunile, serviciile sau sistemele critice în urma unui eveniment sau incident major. Se referă la durata de timp dintre momentul în care apare incidentul și momentul în care operațiunile afectate trebuie să fie restabilite la un nivel funcțional suficient pentru a permite desfășurarea activității de prestare a serviciilor;
- 3.23 Toleranța la risc** - nivelul maxim al riscului acceptat de către instituție care se încadrează în limitele reale din cadrul apetitului la risc asumat de către instituție.

Capitolul II

CERINȚE PRIVIND CADRUL INTERN ȘI GESTIONAREA RISCURILOR AFERENTE TIC ȘI DE SECURITATE A INFORMAȚIEI

Secțiunea 1

Guvernanța, cadrul intern TIC și de securitate a informației

- 4. Instituția va deține o strategie TIC și de securitate a informației care se conformează și sprijină strategia generală de afaceri a instituției și care este aprobată ca parte a strategiei generale de afaceri sau ca document separat și este monitorizată adecvat de către organul de conducere al instituției, responsabil pe deplin de punerea în aplicare a acesteia.
- 5. Strategia TIC și de securitate a informației va defini următoarele:
 - 5.1 modul în care va evolua TIC a instituției, pentru a sprijini și a participa în mod eficient la strategia generală de afaceri, inclusiv la evoluția structurii organizatorice, a modificărilor din sistemele TIC și a dependențelor cheie de furnizori terți;
 - 5.2 evoluția arhitecturii TIC;
 - 5.3 obiective clare de securitate a informațiilor, punând accent pe sisteme și servicii TIC, pe personalul și procesele instituției.
- 6. Instituția va stabili planuri de acțiuni care să conțină măsuri ce vor fi luate în considerare la atingerea obiectivelor strategiei TIC și de securitate a informației. Planurile vor fi comunicate tuturor membrilor relevanți ai personalului și revizuite periodic la intervale regulate de timp, cel puțin cu o periodicitate anuală, pentru a asigura adecvarea acestora.

7. Instituția va institui procese de monitorizare și măsurare a eficacității punerii în aplicare a strategiei TIC și de securitate a informației.
8. Organul de conducere al instituției va asigura că numărul și competența personalului instituției sunt corespunzătoare pentru a pune în aplicare strategia TIC și de securitate a informației, precum și pentru a sprijini permanent necesitățile operaționale TIC ale instituției.
9. Instituția va asigura că membrii organului de conducere urmează periodic instruirii specifice aferente evaluării riscurilor TIC și de securitate a informației cu scopul de a dobândi cunoștințe și competențe suficiente pentru a înțelege impactul acestora asupra activităților și operațiunilor instituției, precum și pentru a actualiza cunoștințele și competențele respective.
10. Instituția va asigura că tot personalul TIC și de securitate a informației, inclusiv persoanele ce dețin funcții-cheie, beneficiază cel puțin anual sau mai des, dacă este necesar, de formare profesională adecvată și proporțională responsabilităților.
11. Instituția se va asigura că bugetul alocat este suficient pentru a pune în aplicare strategia TIC și de securitate a informației.
12. Instituția va asigura că are definite roluri și responsabilități privind funcțiile TIC, gestiunea riscurilor TIC și de securitate a informațiilor, continuitatea activității, inclusiv în cadrul organului de conducere și comitetele sale. Rolurile și responsabilitățile 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 organul de conducere.
13. Instituția va asigura o segregare a funcției de administrare a riscurilor, a funcției de conformitate și a funcției de audit intern, în conformitate cu cele trei linii ale modelului de apărare descrise în cele mai bune practici în domeniu.
14. Instituția se va asigura că are stabilit cadrul intern aferent TIC și securității informației care protejează în mod adecvat sistemele și serviciile sale TIC proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și va susține implementarea strategiei TIC și de securitate a informației.
15. Instituția va elabora și va pune în aplicare o procedură clară de clasificare a reglementărilor interne primare (statutul, strategiile, codurile, politicile, regulamentele și alte acte normative interne) și secundare (instrucțiuni, proceduri, ghiduri, manuale sau alte documente) în domeniul TIC și a nivelurilor de aprobare, în funcție de importanța și aria de aplicare a acestora.
16. Instituția va asigura revizuirea tuturor reglementărilor interne aferente domeniului TIC cel puțin o dată la 3 ani.
17. Instituția va asigura o structură organizatorică adecvată din punctul de vedere al responsabilităților aferente TIC și securității informației, proporțională cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate.
18. Instituția va dispune de un cadru de gestionare a riscurilor aferente TIC și securității informației, care să conțină procese și proceduri pentru a asigura identificarea, analizarea, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele toleranței la risc pentru cel puțin următoarele categorii de riscuri aferente TIC și securității informației:

- 18.1 riscuri de disponibilitate și continuitate;
 - 18.2 riscuri de securitate;
 - 18.3 riscuri de schimbare;
 - 18.4 riscuri de integritate a datelor;
 - 18.5 riscuri asociate părților terțe și externalizărilor TIC;
 - 18.6 riscuri de conformitate;
 - 18.7 riscuri de concentrare a serviciilor TIC.
19. Instituția va atribui gestionarea riscurilor aferent TIC și de securitate a informației unei funcții separate de procesele operaționale TIC.
 20. Instituția va asigura derularea procesului de revizuire a riscurilor descris la pct. 18 pentru toate resursele TIC critice cel puțin o dată la 3 ani.
 21. Instituția va asigura pentru procesele de gestionare a riscurilor aferente TIC și de securitate a informației, resurse financiare, umane și tehnice suficiente, precum și alte resurse necesare care vor fi atât cantitativ, cât și calitativ corespunzătoare cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de instituție.
 22. Instituția va institui o funcție de Ofițer de securitate a informației, responsabil de elaborarea, coordonarea implementării și monitorizarea respectării a cadrului intern aferent securității informației. Ofițerul de securitate a informației, va fi subordonat direct președintelui organului executiv sau administratorului instituției. În funcție de natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de instituție, funcția de Ofițer de securitate a informației poate fi cumulată cu funcția de la pct.19.
 23. Instituția va asigura că organizarea funcției de audit intern în ceea ce privește efectuarea auditului cadrului intern aferent TIC și de securitate a informației este proporțională cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri, activităților desfășurate și profilului de risc TIC al instituției. Auditul intern va avea capacitatea, urmând o abordare bazată pe riscuri, să revizuiască independent și să ofere asigurări cu privire la conformarea tuturor proceselor și activităților TIC și de securitate a informației cu reglementările aplicabile.
 24. Instituția va asigura efectuarea auditului de către un audit intern și/sau extern într-un interval de cel mult 3 ani a tuturor sistemelor și serviciilor TIC critice. Auditul se va efectua cel puțin pentru următoarele sisteme, dacă sunt implementate de instituție: Sistemul automatizat de plăți interne (SAPI), instrumente de plată cu acces la distanță, SWIFT, sistemele de bază (corebanking), sisteme de gestiune a bazelor de date, Active Directory (AD), procesul de gestiune al identităților și accesului, inclusiv privilegiat, Firewall, VPN, sisteme de gestiune electronică a documentelor și mesagerie/comunicare internă și externă.
 25. Instituția va asigura implementarea unui proces de remediere în timp util a recomandărilor de audit intern/extern proporțional cu natura, amploarea și complexitatea amenințărilor, vulnerabilităților și riscurilor TIC identificate pentru modelul de afaceri și activitățile desfășurate de instituție.

Secțiunea a 2-a Securitatea informației

26. Instituția va elabora o politică de securitate a informației care va fi aprobată de organul de conducere al instituției și va stabili contextul organizațional de nivel general care să asigure atingerea obiectivelor cu privire la securitatea informației și securitatea cibernetică în cadrul instituției. Politica va conține: scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare și o descriere a rolurilor și responsabilităților privind gestionarea securității informației. Politica de securitate a informației se va aplica și va fi comunicată personalului instituției și terțelor părți ce interacționează cu instituția pe bază contractuală.
27. Instituția va elabora un regulament ce va fi aprobat de organul de conducere al instituției, în care se va reglementa clasificarea, deklasificarea informațiilor în cadrul instituției și se vor stabili măsuri de securitate aferente fiecărei categorii de informații. Instituția va asigura implementarea unor măsuri ce vor permite aplicarea marcajelor de confidențialitate pe toată informația ce circulă în cadrul instituției.
28. Instituția va elabora proceduri privind controlul accesului logic la sistemele informatice sau serviciile TIC ale instituției, va monitoriza implementarea acestora și se va asigura că acestea vor conține minimum următoarele principii și măsuri de control:
 - 28.1 instituția va acorda utilizatorilor drepturi minime de acces, strict necesare pentru executarea sarcinilor;
 - 28.2 instituția va asigura că acțiunile din cadrul sistemelor informatice și serviciilor TIC critice pot fi atribuite unor utilizatori concreți, iar utilizarea conturilor generice sau partajate va fi limitată și documentată cu argumentele de rigoare;
 - 28.3 instituția va implementa măsuri de control aferente conturilor privilegiate prin limitarea strictă a utilizării lor și monitorizarea permanentă prin înregistrarea tuturor acțiunilor și activităților efectuate în conturile respective într-un sistem de gestiune centralizat a evenimentelor;
 - 28.4 drepturile de acces ale utilizatorilor vor fi acordate, retrase sau modificate în conformitate cu responsabilitățile predefinite în cadrul proceselor automatizate în instituție ce implică obligatoriu proprietarul resursei informaționale. 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 și drepturile de acces vor fi retrase imediat. În cazul concediilor anuale, implicit conturile utilizatorilor vor fi dezactivate, cu excepția cazurilor aprobate de ofițerul de securitate a informației;
 - 28.5 drepturile de acces la resursele TIC vor fi revizuite periodic, la intervale regulate de timp, cel puțin o dată pe an, pentru a se asigura că utilizatorii nu dețin drepturi excesive sau care excedă necesitățile de serviciu;

- 28.6 instituția va aplica metode sofisticate de autentificare, proporționale cu nivelul de importanță al sistemelor informatice, serviciilor TIC sau al informației care se accesează, utilizând cel puțin parole complexe pentru conturile obișnuite și autentificare cu doi factori pentru conturile privilegiate aferente sistemelor critice, precum și în cazul accesării tuturor conturilor de la distanță;
 - 28.7 instituția va implementa mecanisme automatizate de izolare a resurselor informaționale ce au fost afectate de incidente de securitate sau au fost ținta unor atacuri cibernetice.
29. Instituția va elabora și va pune în aplicare măsuri de securitate fizică pentru a proteja centrele de date și zonele importante împotriva accesului neautorizat sau împotriva altor riscuri specifice. Accesul fizic la sistemele TIC și de securitate a informației va fi acordat doar persoanelor autorizate, cu o monitorizare corespunzătoare, și o revizuire periodică, la intervale regulate de timp, cel puțin o dată pe an, a drepturilor de acces.
30. Instituția va elabora proceduri de control pentru asigurarea securității informației și integrității datelor aferente sistemelor și serviciilor TIC și să monitorizeze implementarea acestora. Aceste proceduri vor fi revizuite periodic, la intervale regulate de timp, cel puțin o dată pe an, și vor conține minim următoarele principii și măsuri de control:
- 30.1. instituția va identifica vulnerabilitățile aferente aplicațiilor software, sistemelor, echipamentelor de rețea și stațiilor de lucru critice, prin efectuarea scanărilor periodice, și va implementa în timp util măsuri de control de diminuare a impactului sau a probabilității exploatarei vulnerabilităților identificate, riscurilor implicate sau va aplica măsuri de control compensatorii;
 - 30.2. instituția va implementa mecanisme de detectare rapidă a activităților anormale, a incidentelor TIC și de securitate a informațiilor, în special a atacurilor cibernetice prin implementarea sistemelor de prevenire și detecție a intruziunilor;
 - 30.3. instituția își va stabili configurări de securitate de referință pentru toate echipamentele de rețea critice;
 - 30.4. instituția va implementa segmentarea rețelei interne pe zone, în funcție de echipamentele conectate și informația accesibilă, cu aplicarea măsurilor de criptare a traficului pentru zonele ce conțin sisteme sau servicii critice;
 - 30.5. instituția va implementa măsuri de control și protecție a serverelor, stațiilor de lucru, dispozitivelor mobile și altor echipamente ce sunt conectate la rețeaua acesteia sau gestionează informații din cadrul instituției;
 - 30.6. instituția va implementa mecanisme de monitorizare a informațiilor ce părăsesc perimetrul rețelei interne. Vor fi monitorizate cel puțin: conexiunea la rețeaua internet, informațiile imprimare, informațiile copiate pe dispozitive externe, informațiile transmise prin email;
 - 30.7. instituția va implementa mecanisme de verificare a integrității aplicațiilor software critice instalate pe serverele instituției;
 - 30.8. instituția va implementa măsuri de control eficiente aferente modificărilor și schimbărilor sistemelor și serviciilor TIC la nivelul

componentelor hardware, software și firmware, prin asigurarea unor mecanisme de planificare, înregistrare, testare, evaluare, aprobare, punere în aplicare și verificare. În cazul unor situații de urgență instituțiile vor gestiona modificările necesare pe care le vor introduce cât mai curând posibil, urmând proceduri care să asigure o protecție adecvată.

31. Instituția va implementa măsuri de securitate aferente datelor, indiferent dacă sunt în repaus, în uz sau în tranzit și mecanisme de monitorizare a evenimentelor de securitate, accesărilor neautorizate logice sau fizice, precum și a încălcărilor confidențialității, integrității și disponibilității aferente resurselor informaționale ale instituției.
32. Instituția va introduce în toate acordurile sale cu părți terțe, furnizori de servicii TIC, clauze privind asigurarea confidențialității, integrității și disponibilității informațiilor ce constituie secret bancar sau profesional, date cu caracter personal sau alte informații a căror divulgare ar putea avea un impact negativ asupra instituției, precum și obligația furnizorilor de a coopera pe deplin cu autoritățile de supraveghere și, după caz, de rezoluție.
33. Instituția va elabora și va pune în aplicare un cadru de evaluare, revizuire și testare a securității informației, care să valideze eficiența și eficacitatea măsurilor de control implementate respectând cel puțin următoarele condiții:
 - 33.1. scanări ale vulnerabilităților și teste de penetrare corespunzătoare nivelului riscurilor identificate de instituție și importanței sistemelor sau serviciilor TIC;
 - 33.2. testele de penetrare aferente sistemelor și serviciilor TIC critice, vor fi efectuate pe bază continuă, cu o periodicitate de cel puțin o dată la 3 ani, sau mai des la solicitarea Băncii Naționale a Moldovei;
 - 33.3. testele de penetrare vor fi efectuate conform unor scenarii prestabilite validate de către instituție și vor fi realizate pe sistemele de producție în timp real care sprijină activitățile instituției;
 - 33.4. testele de penetrare urmează a fi efectuate de experți care au competențe, cunoștințe suficiente și relevante domeniului, confirmate prin deținerea certificărilor internaționale (ex. CEPT, CPT, CEH, OSCP, OPST, CPENT, GPEN, GWART, LPT, PTC sau alte certificări recunoscute la nivel internațional);
 - 33.5. instituția va efectua testări de securitate în cazul modificărilor majore la nivel de infrastructură, la nivel de procese, ca urmare a unor incidente operaționale sau de securitate majore sau lansării de sisteme informaționale noi/modificate substanțial, accesibile din internet.
34. Instituția va stabili un program de formare profesională, care să includă instruiți periodice, dar cel puțin anual, de conștientizare cu privire la riscurile de securitate a informației pentru tot personalul în conformitate cu reglementările interne și pentru contractanți în cazul în care instituția consideră că este necesar.

Secțiunea a 3-a Operațiunile TIC

35. Instituția va menține un inventar actualizat al resurselor TIC și de securitate a informației critice, care să conțină configurările, legăturile logice, fizice,

interconexiunile și interdependențele de alte resurse din cadrul instituției, precum și furnizorii terți de servicii TIC. Inventarul va fi suficient de detaliat pentru a permite identificarea imediată a resursei, amplasamentul acesteia, proprietarul și gestionarul resursei TIC.

36. Instituția va utiliza sisteme și servicii TIC actualizate ce sunt proporționale cu natura, amploarea și complexitatea modelului de afaceri și activităților desfășurate de instituție, ce sunt fiabile și dispun de o capacitate suficientă pentru a prelucra cu precizie datele și pentru a face față nevoilor suplimentare de prelucrare a informațiilor în condiții de criză.
37. Instituția va defini și va pune în aplicare procese de planificare și monitorizare a performanței și capacității sistemelor, serviciilor și echipamentului TIC și de securitate a informației pentru a împiedica, detecta și a răspunde prompt la eventuale incidente legate de performanță.
38. Instituția va elabora și va pune în aplicare măsuri privind crearea copiilor de rezervă și de restaurare a datelor și sistemelor/serviciilor TIC critice și de securitate a informației, pentru a se asigura că acestea pot fi restabilite conform cerințelor instituției. Procedurile respective vor fi testate periodic la intervale regulate de timp, cel puțin cu o periodicitate anuală.
39. Instituția se va asigura că, copiile de rezervă aferente sistemelor și serviciilor TIC critice sunt păstrate în siguranță, în formă criptată, într-o altă locație și că nu sunt expuse acelorași riscuri ca și cele din cadrul centrului de date principal.
40. Instituția va asigura mecanisme de verificare a integrității copiilor de rezervă.
41. Instituția va asigura că evenimentele de securitate relevante unor eventuale investigații de pe toate resursele TIC critice sunt colectate în cadrul unor soluții specializate pentru colectarea și asigurarea integrității și disponibilității acestora.

Secțiunea a 4-a **Gestionarea incidentelor și problemelor**

42. Instituția va institui și va pune în aplicare un proces de monitorizare, gestionare și înregistrare a incidentelor, cu păstrarea detaliată a tuturor probelor privind incidentele TIC, de securitate a informației, de continuitate a activității pentru a permite instituției să continue sau să reia rapid procesele critice în cazul unor întreruperi.
43. Instituția va stabili criterii clare de clasificare a incidentelor după prioritatea de soluționare și impact, va defini roluri și responsabilități de soluționare și va elabora proceduri de analiză a cauzelor ce au provocat incidentele și a lecțiilor învățate cu implementarea unor măsuri de control adiționale sau ajustarea măsurilor existente.
44. Instituția va stabili proceduri eficiente de comunicare internă și externă, notificare și escaladare a incidentelor care să prevadă ca incidentele majore să fie comunicate imediat organului de conducere, iar ulterior la intervale regulate de timp, cel puțin o dată la 6 luni, să fie comunicate toate incidentele, inclusiv incidentele evitate dar cu un posibil impact negativ ridicat asupra sistemelor și serviciilor TIC, comunicând-se măsurile de remediere luate imediat și cele care urmează a fi implementate pentru a preveni astfel de incidente pe viitor.
45. Instituția va institui și va pune în aplicare un proces de monitorizare și gestionare a problemelor. În sensul prezentului punct, prin problemă se înțelege

cauza principală care stă la baza unor incidente care se repetă de mai multe ori într-un interval de timp.

Secțiunea a 5-a **Gestionarea proiectelor**

46. Instituția va stabili procese și va elabora proceduri privind gestiunea proiectelor TIC de securitate a informației și continuitate a activității care să definească rolurile și responsabilitățile pe domeniu, necesare în scopul de a susține atingerea obiectivelor strategiei TIC și de securitate a informației.
47. Instituția va asigura în cadrul documentației pentru fiecare proiect TIC, de securitate a informației și continuitate a activității că sunt definite cel puțin următoarele informații:
 - 47.1. scopul și obiectivele proiectului;
 - 47.2. rolurile și responsabilitățile;
 - 47.3. evaluarea riscurilor asociate proiectului, în conformitate cu prevederile pct. 18;
 - 47.4. planul, calendarul și etapele proiectului;
 - 47.5. principalele obiective intermediare;
 - 47.6. cerințele de gestionare a modificărilor;
 - 47.7. cerințele de securitate a informației care sunt analizate și aprobate de către o funcție independentă de cea de gestiune a proiectului.
48. Instituția, aferent portofoliului de proiecte TIC, de securitate a informației și continuitate a activității, va monitoriza și va diminua în mod corespunzător riscurile care pot rezulta din interdependențele dintre diferite proiecte precum și din dependențele mai multor proiecte de aceleași resurse și/sau competențe.
49. Instituția se va asigura că proprietarii tuturor resurselor afectate de un proiect TIC sunt reprezentați în echipa de proiect și că echipa de proiect deține cunoștințele necesare și suficiente pentru a asigura implementarea sigură și cu succes a proiectului.
50. Instituția va stabili proceduri de raportare ad-hoc și la intervale regulate de timp, cel puțin odată la 6 luni, către organul de conducere, a informațiilor privind evoluția și riscurile asociate proiectelor TIC de securitate a informației și continuitate a activității în funcție de importanța și dimensiunea acestora.

Secțiunea a 6-a **Achiziția și dezvoltarea de sisteme TIC**

51. Instituția, aplicând o abordare bazată pe riscuri, va stabili procese și va elabora proceduri privind achiziția, dezvoltarea și menținerea sistemelor și serviciilor TIC și de securitate a informației.
52. Instituția se va asigura că, înainte de orice achiziție sau dezvoltare a sistemelor TIC și de securitate a informației, cerințele funcționale și nefuncționale, inclusiv cerințele minime de securitate a informațiilor, sunt clar definite și aprobate de către organul de conducere relevant.
53. Instituția va implementa măsuri de control pentru diminuarea riscurilor de modificare neintenționată sau de manipulare intenționată a sistemelor TIC și de

securitate a informației pe durata dezvoltării și implementării în mediul de producție.

54. Instituția va elabora o metodologie de testare și aprobare a sistemelor TIC și de securitate a informației, care să asigure că noile sisteme funcționează așa cum au fost proiectate și că mediile de testare utilizate reflectă în mod corespunzător mediul de producție.
55. Instituția va asigura efectuarea testării, inclusiv din punctul de vedere al securității informației, a măsurilor de dezvoltare importante și a modificărilor de infrastructură, a proceselor sau procedurilor, care să cuprindă și situația în care aceste modificări sunt efectuate ca urmare a unor incidente majore, proporțional cu natura, amploarea și complexitatea riscurilor inerente.
56. Instituția va asigura segregarea responsabilităților aferent domeniului de dezvoltare, testare și implementare.

Secțiunea a 7-a **Continuitatea activității**

57. Instituția va elabora o politică de asigurare a continuității activității care va fi aprobată de organul de conducere al instituției și va stabili contextul organizațional de nivel general care să asigure atingerea obiectivelor cu privire la continuitatea activității instituției. Politica va conține scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare și o descriere a rolurilor și responsabilităților privind gestionarea continuității activității în cadrul instituției. Politica de continuitate a activității se va aplica și va fi comunicată personalului instituției și după caz, terțelor părți ce interacționează cu instituția pe bază contractuală.
58. Instituția va elabora un regulament care va fi aprobat de organul de conducere și care va stabili cadrul intern aferent continuității activității proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri, eficient și capabil de a asigura protecția personalului instituției, vizitatorilor și reprezentanților terțelor părți contra amenințărilor majore posibile, precum și continuitatea proceselor critice ale instituției în situații de incident major. Regulamentul va conține descrierea corespunzătoare cel puțin a următoarelor procese de gestiune a continuității activității:
 - 58.1. inventarierea tuturor proceselor de activitate și 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 activității instituției;
 - 58.3. stabilirea indicatorilor de continuitate aferenți proceselor prin specificarea PMIT pentru procesele de activitate;
 - 58.4. identificarea proceselor critice în timp și stabilirea resurselor necesare pentru derularea normală a acestora, în particular: resurse de personal, sisteme și resurse TIC, încăperi, alte resurse;
 - 58.5. stabilirea indicatorilor de continuitate pentru toate resursele critice TIC prin indicarea TOR și 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 desfășurarea normală a proceselor;
- 58.7. stabilirea strategiilor de continuitate pentru desfășurarea proceselor critice în timp în condițiile în care riscurile au fost identificate. Urmează a fi considerate cel puțin 2 strategii de continuitate: restabilirea resurselor critice sau aplicarea procedurilor alternative de lucru;
 - 58.8. clasificarea proceselor critice în grupe de urgență în baza indicatorilor PMIT, pentru a stabili prioritățile acțiunilor de restabilire când sunt afectate sau întrerupte mai multe procese simultan;
 - 58.9. elaborarea planului de asigurare a continuității activității (în continuare – PCA) în baza rezultatelor obținute în cadrul etapelor descrise anterior prin care sunt stabilite măsurile necesare de întreprins pentru a asigura un nivel adecvat al continuității activității instituției;
 - 58.10. stabilirea unei strategii de comunicare pe plan intern și extern în cazurile de incidente majore sau dezastre ce au afectat continuitatea activității instituției;
 - 58.11. Instruirea personalului instituției pentru ca aceștia să conștientizeze importanța asigurării continuității activității instituției, să cunoască responsabilitățile individuale desemnate în cadrul acestui proces, să înțeleagă și să fie capabili să aplice cerințele actelor interne la planificarea, implementarea, monitorizarea și îmbunătățirea procesului în limita responsabilităților atribuite;
 - 58.12. testarea PCA, precum și a anexelor acestuia cu o periodicitate regulată, cel puțin o dată la 2 ani. Rezultatele testărilor vor fi adecvat documentate, cu păstrarea probelor comprehensive și raportate către organul de conducere. Testarea PCA va aborda în mod obligatoriu:
 - 58.12.1. testarea măsurilor de asigurare a continuității sistemelor și infrastructurii TIC;
 - 58.12.2. testarea măsurilor de asigurare a continuității la nivel de roluri și personal;
 - 58.12.3. testarea măsurilor implementate aferente serviciilor și sistemelor de infrastructură non-TIC (ex. electricitate, anti-incendiar, alarmă, climatizare, etc);
 - 58.12.4. testarea cunoașterii prevederilor PCA de către personalul responsabil de continuitatea activității;
 - 58.12.5. testarea reluării activității a tuturor proceselor și resurselor critice în cadrul locației de rezervă.
 - 58.13. revizuirea la intervale regulate de timp, cel puțin o dată la 3 ani, a PCA, precum și a anexelor acestuia pentru a asigura o îmbunătățire continuă a procesului de gestiune a continuității activității instituției.
59. Instituția va elabora adițional, sau în cadrul PCA cel puțin 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 și corespunzător instruite și calificate pentru a putea continua procesele critice ale instituției;
 - 59.2. planul de asigurare a continuității TIC, ce are ca scop de a asigura disponibilitatea sistemelor și serviciilor TIC în scopul exercitării

proceselor critice ale instituției în conformitate cu cerințele TOR și MOR stabilite;

59.3. planul de comunicare în situații excepționale.

60. Instituția va pune în aplicare, fără întârziere, planurile specifice incidentelor de continuitate identificate, în scopul restabilirii în timp util a proceselor operaționale critice și pentru a preveni sau a limita impactul asupra activității.
61. În relația cu părți terțe, prestatori de servicii TIC, instituția se va asigura că poate să înceteze relațiile contractuale fără întreruperea activităților critice sau a continuității și calității furnizării serviciilor. La încetarea contractului inclusiv din inițiativa furnizorului, instituția va asigura existența unor strategii de ieșire cu stabilirea unei perioade de tranziție 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 Națională a Moldovei (în continuare BNM), pe parcursul lunii octombrie/noiembrie, pe parcursul unei zile lucrătoare instituția va pune în aplicare Planul de asigurare a continuității 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, instituția pe parcursul unei zile lucrătoare va pune în aplicare PCA pentru procesele și resursele critice, cu rularea acestora din cadrul centrului de date de rezervă, precum și cu relocarea personalului critic la o locație de rezervă.
64. Instituția va evalua eficacitatea punerii în aplicare a planurilor de continuitate și va identifica măsuri de îmbunătățire a calității și rapidității deciziilor luate, reacției la incidente, pentru a consolida gradul de pregătire a instituției de a face față întreruperilor în activitate.

Secțiunea a 8-a

Integritatea, disponibilitatea informației și continuitatea TIC

65. Instituția va asigura, inclusiv în cazul externalizării sistemelor/serviciilor aferente TIC critice, integritatea și disponibilitatea informației precum și o perioadă de retenție de minim 12 luni, fie de la ultima perioadă supusă controlului de către BNM, dar nu mai mult de 24 de luni.

Se va asigura retenția informației conținute în:

- 65.1. jurnalele de audit ce conțin înregistrări de audit relevante pentru cel puțin următoarele sisteme/servicii, dacă sunt implementate de instituție: SAPI, Instrumente de plată cu acces la distanță, 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 rețea, sisteme de gestiune electronică a documentelor;
 - 65.2. mesajele transmise/primate prin intermediul serviciului de poștă electronică oficială a instituției;
 - 65.3. sistemele de monitorizare video a zonelor critice aferente centrului de date principal și centrului de date de rezervă.
66. Instituția 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 retenției pentru ultimii 2 ani;
 - 66.2. copie de tip full la finele fiecărei luni cu asigurarea retenției pentru ultimele 6 luni;
 - 66.3. copie de tip diferențial la finele fiecărei zile cu asigurarea retenției pentru ultimele 30 zile.
67. Instituția va asigura în cadrul Platformei centrale de schimb de informații (în continuare – PCSI), înregistrarea, stocarea și gestiunea materialelor preliminare aferente ședințelor organului de conducere ce țin de domeniul TIC precum și 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 instituției va asigura că informația stocată în cadrul sistemelor TIC ce conțin date contabile este actuală și se bazează pe tranzacții reale.
69. Instituția va asigura redundanța conexiunilor de date de la doi prestatori de servicii pentru cel puțin 30% din punctele de prezență (sucursale) și pentru cel puțin 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 populației la aceste ATM-uri și puncte de prezență.
70. Instituția va asigura că dispune de un centru de date de rezervă capabil să preia activitatea tuturor proceselor critice în cazul indisponibilității centrului de date principal.
71. Instituția va asigura conexiunea la rețeaua internet pentru centrul de date principal și centrul de date de rezervă prin intermediul a cel puțin 2 prestatori de servicii.
72. Instituția va asigura că centrul de date principal și centrul de date de rezervă dispun de următoarele sisteme și echipamente:
- 72.1. sistem de aer condiționat redundant sau contract de suport pentru reparația sistemului cu timp de punere în funcțiune de maximum 6 ore;
 - 72.2. generator de curent electric capabil să asigure necesitățile echipamentelor;
 - 72.3. sistem de monitorizare video ce acoperă toate zonele;
 - 72.4. sistem de detectare a umidității și scurgere a apei;
 - 72.5. sistem de acces fizic în încăpere cu mai mulți factori sau biometric;
 - 72.6. sistem de stingere automatizată a incendiilor;
 - 72.7. sistem de monitorizare a temperaturii.
73. Instituția va asigura redundanța următoarelor echipamente și servicii din centru de date principal:
- 73.1. echipamentelor de rețea ce asigură conexiunea la internet a centrului de date central și a centrului de date de rezervă;
 - 73.2. echipamentelor de rețea ce asigură legătura între nodurile informaționale principale ale instituției;
 - 73.3. echipamentelor firewall;
 - 73.4. echipamentelor pe care rulează bazele de date aferente sistemelor și serviciilor TIC critice;

- 73.5. echipamentelor pe care rulează sistemul de bază (corebanking), SWIFT, instrumente de plată cu acces la distanță în cazul în care sistemele respective sunt implementate în instituție;
 - 73.6. serviciilor DNS externe ale instituției, cu localizarea obligatorie a unuia pe teritoriul Republicii Moldova.
- 74. Instituția va asigura replicarea bazelor de date ce conțin date financiare critice în centrul de date de rezervă.
 - 75. Instituția va asigura lunar în regim offline, păstrarea în formă criptată a cel puțin o copie de rezervă de tip full a datelor pentru toate sistemele sale critice într-o locație diferită de centrul de date principal și centrul de date de rezervă.
 - 76. Instituția va asigura că toate ATM-urile, serverele, bazele de date și stațiile sau terminalele de lucru rulează pe sisteme de operare ce dispun de suport din partea producătorului. Excepție sunt sistemele de tip vechi/legacy ce vor rula într-o rețea izolată și aferent cărora se vor aplica măsuri compensatorii de securitate. Lista sistemelor exceptate urmează a fi aprobată de organul de conducere al instituției.

Capitolul III

EVALUAREA RISCURILOR TIC

- 77. Instituția își va evalua profilul de risc aferent TIC cel puțin 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, instituția va revizui cadrul intern corespunzător, precum și măsurile de control aplicabile.
- 78. Instituția, în cazul în care a externalizat funcții operaționale și/sau servicii TIC și sisteme TIC ale oricărei activități de prestare de servicii către furnizori terți, inclusiv către entitățile din grup, va asigura eficacitatea măsurilor prevăzute în prezentul Regulament. Instituția rămâne pe deplin responsabilă pentru evaluarea eficacității măsurilor de securitate ale funcțiilor operaționale externalizate aferente serviciilor de plată și/sau serviciilor TIC și sistemelor TIC ale oricărei activități de prestare de servicii.
- 79. BNM, în cadrul controalelor și prin dispunerea efectuării misiunilor de audit, evaluează cadrul intern aferent TIC al fiecărei instituții, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și cu profilul/apetitul de risc al instituției.
- 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 și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de instituție, BNM poate impune cerințe concrete față de cadrul intern aferent TIC, măsuri de supraveghere, măsuri de remediere, sancțiuni sau măsuri sancționatoare.

Capitolul IV

RAPORTAREA

- 81. Instituția este obligată să notifice BNM prin intermediul PCSI sau în cazul indisponibilității acestuia la adresa de email SupraveghereTIC@bnm.md despre incidentele produse, respectând următoarele condiții:

- 81.1. în cazul unui incident care a generat disfuncționalități sau care au afectat disponibilitatea, confidențialitatea, integritatea și/sau autenticitatea informațiilor fie a afectat continuitatea sistemelor/serviciilor ce susțin desfășurarea funcțiilor critice, se transmite o notificare inițială cu privire la incidentul produs, fără întârziere, dar nu mai târziu de sfârșitul zilei lucrătoare sau, în cazul unui incident care a avut loc cu mai puțin 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 disfuncționalități la nivelul funcțiilor semnificative, a afectat disponibilitatea, confidențialitatea, integritatea și/sau autenticitatea informațiilor, a afectat continuitatea serviciilor aferente plăților, prestatorii de servicii de plată, se transmite o notificare inițială 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 81.1 sau 81.2, care va conține informații suplimentare cu privire la circumstanțele incidentului produs, procesele/sistemele/serviciile afectate, impactul preliminar estimat și măsurile de remediere întreprinse până la acel moment de instituție;
 - 81.4. un raport final, semnat de un membru al organului de conducere al instituției, în termen de cel mult 20 de zile din ziua notificării inițiale prevăzute la pct.81.1 sau 81.2. Raportul va conține analiza cauzelor principale ce au dus la producerea incidentului, a impactului efectiv asupra activităților instituției sau a intereselor financiare ale clienților, măsurile întreprinse de instituție și care urmează a mai fi întreprinse pentru a preveni sau minimiza impactul de la producerea incidentelor de acest tip pe viitor.
82. Instituțiile vor transmite către BNM prin PCSI, sau în cazul indisponibilității acestuia la adresa de email SupraveghereTIC@bnm.md, în termen de o lună de la încheierea anului de gestiune, informații cu privire la următoarele:
- 82.1. rezultatele testelor de penetrare;
 - 82.2. rezultatele ultimelor scanări de vulnerabilități efectuate pentru toate resursele critice, conform situației 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 instituției în conformitate cu standardul PCI-DSS, în cazul când instituția 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.