Proiect

COMITETUL EXECUTIV
AL BĂNCII NAȚIONALE A MOLDOVEI

HOTĂRÂREA

nr. ___ din __ _____ 2023

Pentru aprobarea Regulamentului privind cerințe minime pentru gestiunea riscurilor TIC și de securitate a informației

În temeiul art. 5 alin. (1), art. 11 alin. (1), art. 27 alin. (1) lit. c) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr. 297-300, art. 544) și art. 2 alin. (11), art. 32^1, art.32^2 și art.94 alin.(1) lit. c) din Legea nr.114/2012 cu privire la serviciile de plată și moneda electronică (Monitorul Oficial al Republicii Moldova, 2012, nr.193-197, art.661), Comitetul executiv al Băncii Naționale a Moldovei

HOTĂRĂȘTE:

1. Se aprobă Regulamentul privind cerințe minime pentru gestiunea riscurilor TIC și de securitate a informației (se anexează).

2. Prezentul Regulament intră în vigoare la data publicării în Monitorul Oficial al Moldovei.

Anexă
la Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr.___ din _____2023

REGULAMENT
privind cerințe minime pentru gestiunea riscurilor TIC și de securitate a informației

Capitolul I. DISPOZIȚII GENERALE

Secțiunea 1. Domeniul de aplicare

1. Prezentul regulament se aplică prestatorilor de servicii de plată prevăzuți la art. 5 alin. (1) lit. a-c) *Legea nr. 114/2012 cu privire la serviciile și moneda electronică* (în continuare – instituții) și stabilește cerințe minime pentru gestiunea riscurilor Tehnologiei Informației și Comunicațiilor (în continuare – TIC) și de securitate a informației.
2. Scopul regulamentului este de a asigura că instituțiile dispun de un cadru intern adecvat pentru gestiunea riscurilor TIC și de securitate a informației aliniat la strategia generală de afaceri, iar procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele TIC ale băncii și protejează în mod adecvat sistemele TIC ale băncilor.

Secțiunea 2. Noțiuni principale

3. Termenii și expresiile utilizate în prezentul regulament au semnificațiile prevăzute *de Legea nr. 114/2012 cu privire la serviciile și moneda electronică* și în *Regulamentul privind cadrul de administrare a activității băncii, aprobat prin Hotărârea Comitetului Executiv al Băncii Naționale a Moldovei (în continuare – BNM) nr.146 din 07 iunie 2017, înregistrată la Ministerul Justiției cu nr. 1229 din 14 iunie 2017 (Monitorul Oficial al Republicii Moldova, 2017, nr. 201-213, art.1183 din 23.06.17)*.
4. Adițional, în sensul prezentului regulament se aplică următoarele definiții:

cadrul intern aferent TIC – totalitatea reglementărilor interne, a proceselor și structurilor organizatorice TIC stabilite în cadrul instituției, ce asigură gestionarea adecvată a riscurilor aferente TIC și atingerea obiectivelor privind TIC ale instituției;
profil de risc TIC – suma expunerilor unei instituții la riscuri reale și potențiale aferent TIC.
clasificarea informațiilor – operațiune de atribuire a unei categorii de confidențialitate informațiilor prin aplicarea marcajelor corespunzătoare acestora;
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;
declasificarea informațiilor – operațiune de excludere a informațiilor de sub incidența măsurilor de securitate.
incident – un eveniment sau o serie de evenimente neașteptate care pot apărea și care au afectat disponibilitatea, securitatea sistemelor/serviciilor critice, fie integritatea datelor aferente TIC critice sau continuitatea prestării serviciilor către clienți;
înregistrare de audit – o singură înregistrare în jurnalul de audit care descrie apariția unui singur eveniment auditabil;
jurnal de audit – secvență cronologică de înregistrări de audit, fiecare dintre acestea conținând dovezi privind rezultatul executării a unui proces sau a unei funcții din cadrul unui sistem;
Perioada Maximă de Întrerupere Tolerabilă (PMIT) – perioada maximă pentru care activitatea poate fi întreruptă, iar impactul asupra activității instituției va fi tolerabil;

Timpul Obiectiv pentru Restabilire (TOR) – perioada de timp în care activitățile sau resursele trebuie să fie restabilite în rezultatul unui incident major ce le-a afectat;
Momentul Obiectiv pentru Restabilire (MOR) – momentul în timp la care va fi restabilită informația conținută într-un sistem TIC ca urmare a unui incident de continuitate (ex. MOR de 24h înseamnă că informația din va fi restabilită la starea zilei de ieri, cu 24 ore în urmă);
resursă TIC – orice bun material sau nematerial al instituției necesar gestiunii informației, cum ar fi aplicații, echipamente de calcul și alte elemente de infrastructură;
risc TIC și de securitate - se referă la riscurile operaționale și de securitate prevăzute la art. 32^1 alin. (1) din *Legea nr. 114/2012 cu privire la serviciile și moneda electronică*. Acesta reprezintă înregistrări 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;
risc de disponibilitate și continuitate aferente TIC – riscul ca performanțele sau disponibilitatea sistemelor/serviciilor și datelor aferent TIC să fie afectate în mod negativ, inclusiv incapacitatea de a recupera în timp util procesele și serviciile instituției;
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;
risc de integritate a datelor aferent TIC – riscul ca datele stocate și/sau procesate de sistemele/serviciile aferent TIC să fie incomplete, inexacte sau incoerente la nivelul diferitor sisteme TIC;
risc asociat externalizărilor TIC – riscul ca angajarea unei terțe părți sau a unei alte entități a grupului (externalizare intragrup) pentru a furniza sisteme aferente TIC sau servicii conexe să afecteze negativ performanța și gestionarea riscurilor în cadrul instituției;
risc de conformitate aferent TIC – riscul de încălcare sau neconformare cu cadrul legal, acorduri, practici recomandate sau standarde etice aferent TIC;
risc aferent TIC semnificativ – risc aferent TIC ce poate avea un impact negativ asupra sistemelor sau serviciilor aferente TIC critice;
sisteme aferente TIC – sisteme TIC configurate și interconectate ca parte a unui mecanism sau a unei rețele care susțin efectuarea operațiunilor unei instituții;
servicii aferente TIC – servicii furnizate prin intermediul sistemelor TIC unuia sau mai multor utilizatori interni sau externi;
sisteme/servicii aferente TIC critice – sisteme/servicii TIC care sunt critice pentru 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;

Capitolul II. CERINȚE PRIVIND CADRUL INTERN ȘI GESTIUNEA RISCURILOR TIC

Secțiunea 1. Guvernanța, strategia, cadrul intern TIC și de securitate a informației

5. Instituția trebuie să dețină o strategie TIC și de securitate a informației ce se conformează și sprijină strategia generală de afaceri a instituției și care este aprobată și monitorizată adecvat de către organele de conducere ale instituției și care sunt pe deplin responsabile de punerea în aplicare a acesteia.

6. Strategia TIC și de securitate a informației trebuie să definească modul în care trebuie să evolueze TIC al instituției, evoluția structurii organizatorice, modificările din sistemul TIC, dependențele cheie de terțe părți, evoluția arhitecturii TIC, obiective clare de securitate a informațiilor, sisteme și servicii TIC, personal și procese, comunicare în cazul unor incidente TIC sau de securitate a informației.
7. Instituția trebuie să stabilească planuri de acțiuni care să conțină măsuri ce trebuie de luat în vederea atingerii obiectivelor strategiei TIC și de securitate a informației. Planurile urmează a fi comunicate personalului relevant și revizuite periodic la intervale regulate de timp, cel puțin cu o periodicitate anuală, pentru a asigura adecvarea acestora.
8. Instituția urmează să instituie procese de monitorizare și măsurare a eficacității punerii în aplicare a strategiei TIC și de securitate a informației.
9. Instituția trebuie să asigure 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.
10. Instituția va asigura ca membrii organelor de conducere să urmeze periodic instruiri specifice aferent 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 menține actualizate cunoștințele și competențele respective.
11. Instituția trebuie să asigure că tot personalul TIC și de securitate a informației, inclusiv persoanele ce dețin funcții cheie, beneficiază cel puțin anual de formare profesională adecvată și proporțională responsabilităților.
12. Instituția trebuie să se asigure că bugetul alocat este suficient pentru a pune în aplicare strategia TIC și de securitate a informației.
13. Instituția trebuie să asigure 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 ce sunt comunicate în mod clar, stabilite și integrate în organizarea internă și procesele relevante, inclusiv roluri privind colectarea și agregarea informațiilor despre riscuri și raportarea acestora către organele de conducere.
14. Instituția trebuie să asigure o segregare a funcțiilor de administrare, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare.
15. Instituția trebuie să se asigure că are stabilit cadrul intern aferent TIC și securității informației ce protejează în mod adecvat sistemele și serviciile sale TIC proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și susține implementarea strategiei TIC și de securitate a informației.
16. Instituția trebuie să elaboreze și să pună în aplicare o procedură clară de denumire a reglementărilor interne și a nivelelor de aprobare, în funcție de importanța și aria de aplicare a acestora.
17. Instituția trebuie să asigure revizuirea tuturor reglementărilor interne aferente domeniului TIC odată la 3 ani.
18. Instituția trebuie să asigure o structură organizatorică adecvată din punct de vedere a responsabilităților aferente TIC și securității informației, proporțională cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate.
19. Instituția trebuie să asigure o gestionare adecvată a riscurilor aferente TIC și securității informației prin identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al instituției pentru cel puțin următoarele categorii de riscuri aferente TIC și securității informației:
    a) riscuri de disponibilitate și continuitate aferente TIC;
    b) riscuri de securitate aferente TIC;
    c) riscuri de schimbare aferente TIC;
    d) riscuri de integritate a datelor aferente TIC;
    e) riscuri asociate părților terțe și externalizărilor TIC;

f) riscuri de conformitate aferente TIC;
g) riscuri de concentrare a serviciilor TIC.

20. Instituția trebuie să atribuie gestiunea riscurilor aferent TIC și de securitate a informației unor funcții de control, separate de procesele operaționale TIC, ce vor fi responsabile de monitorizarea respectării cadrului intern aferent TIC și securității informației cu o raportare directă către organele de conducere.
21. Instituția trebuie să asigure derularea procesului de gestiune a riscurilor pentru toate resursele TIC critice cel puțin odată la 3 ani.
22. Instituția trebuie să asigure pentru procesele de gestionare a riscurilor aferente TIC și de securitate a informației, resurse financiare, umane și tehnice suficiente, cât și alte resurse necesare ce vor fi cantitativ cât și calitativ corespunzătoare cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de instituție.
23. Instituția trebuie să asigure că funcția de ofițer de securitate este subordonată direct președintelui organelor de conducere.
24. Instituția trebuie să asigure că organizarea funcției de audit intern în ceea ce privește auditarea 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 trebuie să aibă 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 cadrul intern TIC și de securitate a informației, precum și cu reglementările aplicabile.
25. Instituția trebuie să asigure auditarea într-un interval de 3 ani a tuturor sistemelor și serviciilor TIC critice. Cel puțin următoarele sisteme urmează a fi auditate, dacă sunt implementate de instituție: SAPI, Instrumente de plată cu acces la distanță, SWIFT, corebanking, sisteme de gestiune a bazelor de date, Active Directory (AD), Privileged Acces Management (PAM), Firewall, VPN, sisteme de gestiune electronică a documentelor.
26. Instituția trebuie să asigure implementarea unui proces de remediere în timp util a constatărilor de audit intern proporțional cu natura, amploarea și complexitatea amenințărilor, vulnerabilităților și riscurilor TIC identificate pentru modelul de afaceri și activitățile desfășurate de instituție.

Secțiunea 2: Securitatea informației

27. Instituția trebuie să elaboreze o politică de securitate a informației ce 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 asigurarea securității informației și securității cibernetice 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 tuturor angajaților instituției și terților părți ce interacționează cu instituția pe bază contractuală.
28. Instituția va elabora un regulament aprobat de organul de conducere a instituției care va reglementa clasificarea, declasificarea informațiilor în cadrul instituției și va 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.
29. Instituția trebuie să elaboreze proceduri privind controlul accesului logic la sistemele informatice sau serviciile TIC ale instituției și să monitorizeze implementarea acestora. Aceste proceduri vor fi revizuite periodic, cel puțin o dată la 3 ani, și vor conține minim următoarele principii și măsuri de control:
    a) instituția trebuie să acorde utilizatorilor drepturi minime de acces, strict necesare pentru executarea sarcinilor;

b) instituția trebuie să se asigure că acțiunile din cadrul sistemelor informatice și serviciilor TIC critice pot fi atribuite unor utilizatori concreți, iar utilizarea conturilor generice sau partajate urmează a fi limitată pe cât de posibil;
c) instituția urmează să implementeze măsuri de control aferent conturilor privilegiate prin limitarea strictă a utilizării lor și monitorizarea permanentă prin înregistrarea tuturor acțiunilor efectuate de conturile respective într-un sistem de gestiune centralizată a evenimentelor;
d) toate activitățile cel puțin aferent utilizatorilor privilegiați urmează a fi înregistrare în sisteme de gestiune centralizată a evenimentelor;
e) drepturile de acces ale utilizatorilor trebuie acordate, retrase sau modificate în conformitate cu procesele automatizate predefinite în cadrul instituției ce implică obligatoriu proprietarul resursei informaționale. Pe parcursul concediilor de maternitate sau suspendării contractului, conturile utilizatorilor trebuie dezactivate, iar în caz de încetare a contractului de muncă, contul trebuie dezactivat și drepturile de acces retrase imediat. În cazul concediilor anuale, implicit conturile utilizatorilor urmează a fi dezactivate, cu excepția cazurilor aprobate de ofițerul de securitate;
f) drepturile de acces trebuie 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;
g) instituția trebuie să aplice 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 utilizatorii de rând și autentificare cu doi factori pentru conturile privilegiate aferent sistemelor critice precum și în cazul accesului de la distanță;
h) instituția trebuie să implementeze mecanisme automatizate de izolare a resurselor informaționale ce au fost afectate de incidente de securitate sau au fost țința unor atacuri cibernetice.

30. Instituția trebuie să elaboreze și să pună 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 urmează a 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.
31. Instituția trebuie să elaboreze 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:
a) instituția trebuie să identifice vulnerabilitățile aferent aplicațiilor software, sistemelor și echipamentelor de rețea, prin efectuarea scanărilor periodice, și să implementeze în timp util măsuri de control de diminuare a impactului sau a probabilității exploatării vulnerabilităților identificate, riscurilor implicate sau să aplice măsuri de control compensatorii;
b) instituția trebuie să implementeze 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;
c) instituția trebuie să își stabilească configurări de securitate de referință pentru toate echipamentele de rețea critice;
d) instituția trebuie să implementeze 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;
e) instituția trebuie să implementeze 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;

f) instituția trebuie să implementeze mecanisme de monitorizare a informațiilor ce părăsesc perimetrul rețelei interne. Urmează a fi monitorizate cel puțin: conexiunea la rețeaua internet, informațiile transmise la imprimante, informațiile copiate pe dispozitive externe, informațiile transmise prin email.
g) instituția trebuie să implementeze mecanisme de verificare a integrității aplicațiilor software critice instalate pe serverele instituției.
h) instituția trebuie să implementeze 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 trebuie să gestioneze modificările care sunt necesare și trebuie introduse cât mai curând posibil, urmând proceduri care să asigure o protecție adecvată.

32. Instituția trebuie să implementeze măsuri de securitate aferent 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 aferent resurselor informaționale ale instituției.
33. Instituția trebuie să introducă în toate acordurile sale cu părți terțe, furnizori de servicii TIC, clauze privind asigurarea confidențialității, integrității și disponibilității informațiilor ce constituie secret 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 rezoluție.
34. Instituția trebuie să elaboreze și să pună 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:
    a) testele includ scanări ale vulnerabilităților și teste de penetrare corespunzătoare nivelului riscurilor identificate de instituție și importanței sistemelor sau serviciilor TIC;
    b) testele de penetrare aferent sistemelor și serviciilor TIC critice, vor fi efectuate pe bază continuă, cel puțin cu o periodicitate de 3 ani, sau mai des la solicitarea Băncii Naționale a Moldovei;
    c) 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;
    d) testele de penetrare urmează a fi efectuate de experți independenți 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);
    e) instituția trebuie să efectueze 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 internet.
35. Instituția trebuie să stabilească un program anual de formare profesională, care să includă instruiri periodice de conștientizare cu privire la riscurile de securitate a informației pentru toți angajații în conformitate cu reglementările interne.

Secțiunea 3: Operațiunile TIC

36. Instituția trebuie să mențină 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 trebuie să fie suficient de detaliat pentru a permite identificarea imediată a resursei, amplasamentul acesteia, proprietarul și gestionarul.

37. Instituția trebuie să utilizeze sisteme și servicii TIC actualizate ce sunt proporționale cu natura, amploarea și complexitatea modelului de afaceri și activităților desfășurate de instituție, 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.
38. Instituția trebuie să definească și să pună 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.
39. Instituția trebuie să elaboreze și să pună 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 trebuie să fie testate periodic la intervale regulate de timp, cel puțin cu o periodicitate anuală.
40. Instituția trebuie să se asigure că, copiile de rezervă aferent 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 sediului de bază.
41. Instituția trebuie să asigure mecanisme de verificare a integrității copiilor de rezervă.
42. Instituția trebuie să asigure 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 4: Incidentele TIC

43. Instituția trebuie să instituie și să pună 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 și operaționale pentru a permite instituției să continue sau să reia rapid procesele critice în cazul unor întreruperi.
44. Instituția trebuie să stabilească criterii clare de clasificare a incidentelor după prioritatea de soluționare și impact, să stabilească roluri și responsabilități de soluționare și să elaboreze proceduri de analiză a cauzelor ce au provocat incidentele și a lecțiilor învățate cu implementarea unor măsuri de control adiționale sau ajustarea măsurilor existente.
45. Instituția trebuie să stabilească proceduri eficiente de comunicare internă și externă, notificare și escaladare a incidentelor care să prevadă ca incidentele majore să fie comunicate imediat organelor 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 care urmează încă a fi implementate pentru a preveni astfel de incidente pe viitor.

Secțiunea 5: Gestionarea proiectelor TIC

46. Instituția trebuie să stabilească procese și elaboreze 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 trebuie să asigure că în cadrul documentației pentru fiecare proiect TIC, de securitate a informației și continuitate a activității sunt definite cel puțin următoarele informații:
    a) scopul și obiectivele proiectului;
    b) rolurile și responsabilitățile;
    c) evaluarea riscurilor asociate proiectului, în conformitate cu prevederile pct.19;
    d) planul, calendarul și etapele proiectului;
    e) principalele obiective intermediare;

f) cerințele de gestionare a modificărilor;
g) cerințele de securitate a informației care sunt elaborate de către o funcție independentă de cea de gestiune a proiectului.

48. Instituția, aferent portofoliul lor de proiecte TIC, de securitate a informației și continuitate a activității, trebuie să monitorizeze și să diminueze 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 trebuie să se asigure că proprietarii tuturor proceselor 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 trebuie să stabilească proceduri de raportare ad-hoc și la intervale regulate de timp, către organele de conducere, a informațiilor privind evoluția și riscurile asociate proiectelor TIC de securitate a informației și continuitate a activității în funcției de importanța și dimensiunea acestora.

Secțiunea 6: Achiziția și dezvoltarea de sisteme TIC

51. Instituția, aplicând o abordare bazată pe riscuri, trebuie să stabilească procese și să elaboreze proceduri privind achiziția, dezvoltarea ți menținerea sistemelor și serviciilor TIC și de securitate a informației.
52. Instituția trebuie să se asigure că, înainte de orice achiziție sau dezvoltare a sistemelor TIC și de securitate a informației, cerințele funcționale și nefuncționale, inclusiv cerințele de securitate a informațiilor, sunt clar definite și aprobate de către organele de conducere relevante.
53. Instituția trebuie să implementeze 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 trebuie să elaboreze 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 trebuie să asigure efectuarea testării, inclusiv din punct de vedere a securității informației, a tuturor dezvoltărilor 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 operaționale sau de securitate majore, proporțional cu natura, amploarea și complexitatea riscurilor inerente.

Secțiunea 7: Continuitatea activității

56. Instituția trebuie să elaboreze o politică de asigurare a continuității activității ce 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 tuturor angajaților instituției și terțelor părți ce interacționează cu instituția pe bază contractuală.
57. Instituția trebuie să elaboreze un regulament ce va fi aprobat de organele de conducere și va stabili cadrul metodologic intern aferent continuității activității eficient și capabil de a sigura protecția angajaților, vizitatorilor și reprezentanților terțelor părți contra amenințărilor majore posibile, precum și pentru a asigura continuitatea proceselor critice ale instituției în situații de incident major. Regulamentul va conține descrierea cel puțin a următoarelor etape ale procesului de gestiune a continuității activității:

a) inventarierea tuturor proceselor de activitate și identificarea celor ce sunt critice din punct de vedere a derulării continue în timp;
b) evaluarea impactului pe care îl pot avea întreruperile în procesele identificate asupra activității instituției;
c) stabilirea indicatorilor de continuitate aferent proceselor prin indicarea Perioadei Maxime de Întrerupere Tolerabile pentru procesele de activitate (PMIT);
d) 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;
e) stabilirea cerințelor de disponibilitate pentru toate resursele critice TIC prin indicarea Timpului Obiectiv pentru Restabilire (TOR) și Momentului Obiectiv pentru Restabilire (MOR);
f) 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;
g) stabilirea strategiilor de continuitate pentru a continua desfășurarea proceselor critice în timp în condițiile în care riscurile identificate se realizează. Urmează a fi considerate cel puțin 2 strategii de continuitate: restabilirea resurselor critice sau aplicarea procedurilor alternative de lucru;
h) gruparea 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;
i) elaborarea planului de continuitate a 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;
j) stabilirea unei strategii de comunicare pe plan intern și extern în cazurile de incidente majore sau dezastre ce au afectat continuitatea activității instituției;
k) instruirea tuturor angajaților 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 metodologice la planificarea, implementarea, monitorizarea și îmbunătățirea procesului în limita responsabilităților atribuite;
l) 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 organele de conducere. Testarea PCA va aborda în mod obligatoriu:
   - testarea măsurilor de asigurare a continuității sistemelor și infrastructurii TIC;
   - testarea măsurilor de asigurare a continuității la nivel de roluri și personal;
   - testarea măsurilor implementate aferent serviciilor și sistemelor de infrastructură non-TIC (ex. electricitate, anti-incendiar, alarmă, climatizare, etc);
   - testarea cunoașterii prevederilor PCA de către angajații responsabili de continuitatea activității;
   - testarea reluării activității a tuturor proceselor și resurselor critice în cadrul locației de rezervă.
m) revizuirea la intervale regulate de timp, cel puțin o dată la 2 ani, a PCA precum și a anexelor acestuia pentru a asigura o îmbunătățire continuă a procesului de gestiune a continuității activității instituției.

58. Instituția urmează să elaboreze adițional la PCA cel puțin următoarele planuri:
a) 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;

b) planul de asigurare a continuității TIC, ce are ca scop de a asigura disponibilitatea sistemelor și serviciilor TIC în scopul exercitării fără întreruperi a procesele critice ale instituției;
c) planul de comunicare în situații excepționale.

59. Instituția trebuie, fără întârziere, să pună în aplicare 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.
60. În relația cu părți terțe, prestatori de servicii TIC, instituția se va asigura că poate să rezilieze acordurile contractuale fără întreruperea activităților critice sau a continuității și calității furnizării serviciilor. La încetarea contractului 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.
61. Anual, în coordonare prealabilă cu BNM pe parcursul lunii noiembrie, instituția trebuie pe parcursul unei zile lucrătoare să pună în aplicare Planul de asigurare a continuității TIC cu asigurarea continuității din cadrul centrului de date de rezervă, a unor sisteme sau servicii critice agreate de BNM.
62. O dată la 2 ani, în coordonare prealabilă cu BNM pe parcursul lunii noiembrie, instituția trebuie pe parcursul unei zile lucrătoare să pună în aplicare PCA cu asigurarea continuității tuturor proceselor și a resurselor critice în cadrul centrului de date de rezervă, precum și cu relocarea personalului critic la o locație de rezervă.
63. Instituția urmează să evalueze eficacitatea punerii în aplicare a planurilor de continuitate și să identifice măsuri de îmbunătățire a calității și rapidității deciziilor luate, promptitudinii reacției la incidente și pentru a consolida gradul de pregătire a instituției de a face față întreruperilor în activitate.

Secțiunea 8: Integritatea, disponibilitatea informației și continuitatea TIC

64. Instituția va asigura, inclusiv și în cazul externalizării sistemelor/serviciilor aferente TIC critice, integritatea și disponibilitatea informației precum și o perioadă de retenție de minim 12 luni a informației conținute în:
    a) jurnalele de audit ce conțin evenimente de securitate relevante pentru cel puțin următoarele sisteme/serviciile, dacă sunt implementate de instituție: SAPI, Instrumente de plată cu acces la distanță, SWIFT, Corebanking, sisteme de gestiune a bazelor de date, Active Directory (AD), Privileged Acces Management (PAM), Firewall, VPN, echipamente critice de rețea, sisteme de gestiune electronică a documentelor;
    b) mesajele transmise/primite prin intermediul serviciului de poștă electronică oficială a instituției;
    c) sistemele de monitorizarea video a zonelor critice aferent centrului de date principal și sediului de rezervă.
65. Instituția va asigura copii de rezervă ale bazelor de date aferente sistemelor/serviciilor TIC critice efectuate după următoarea schemă:
    a) copie de tip full la finele fiecărui an pentru ultimii 2 ani;
    b) copie de tip full la finele fiecărei luni pentru ultimele 6 luni;
    c) copie de tip diferențial la finele fiecărei zile pentru ultimele 30 zile.
66. Instituția, începând cu 01.01.2025 în cadrul Platformei Centrale de Schimb de Informații (PCSI) va asigura înregistrarea, stocarea și gestiunea materialelor preliminare aferente ședințelor organelor de conducere ale băncilor precum și înregistrarea în decurs de 5 zile a deciziilor luate de organele de conducere ale băncilor. Integritatea tuturor documentelor în cadrul sistemului urmează a fi confirmată printr-o semnătură electronică calificată.
67. Organele de conducere ale instituției sunt responsabile pentru asigurarea faptului că informația stocată în cadrul sistemelor TIC ce conțin date contabile este actuală și se bazează pe tranzacții reale.

68. Instituția va asigura redundanța conexiunilor de date de la doi prestatori de servicii pentru cel puțin 30% din punctele de prezență (filiale/sucursale) și pentru cel puțin 30% din ATM-uri.
69. Instituția va asigura că dispune de un centru de date de rezervă capabil să preia activitatea proceselor critice în cazul indisponibilității centrului de date principal.
70. Instituția va asigura conexiunea la rețeaua internet pentru sediul central și centrul de rezervă prin cel puțin 2 prestatori de servicii.
71. Instituția va asigura că centrul de date principal și centrul de date de rezervă dispun de următoarele sisteme și echipamente:
    a) sistem de aer condiționat redundant sau contract de suport pentru reparația sistemului cu timp de punere în funcțiune de maxim 6 ore;
    b) generator de curent electric capabil să asigure necesitățile echipamentelor;
    c) sistem de video monitorizare ce acoperă toate zonele;
    d) sistem de detectare a umidității și scurgere a apei;
    e) sistem de acces fizic în încăpere cu mai mulți factori sau biometric;
    f) sistem de stingere automatizată a incendiilor;
    g) sistem de monitorizare a temperaturii;
72. Instituția va asigura redundanța următoarelor echipamente și servicii:
    a) echipamentelor de rețea ce asigură conexiunea cu internet a sediului central și a sediului de rezervă;
    b) echipamentelor de rețea ce asigură legătura între nodurile informaționale principale ale instituției;
    c) echipamentelor firewall;
    d) echipamentelor pe care rulează bazele de date aferent sistemelor și serviciilor TIC critice;
    e) echipamentelor pe care rulează sistemul de Corebanking, SWIFT, Instrumente de plată cu acces la distanță;
    f) serviciilor DNS externe ale instituției, cu localizarea obligatorie pe teritoriul RM a serviciului de rezervă;
73. Instituția va asigura replicarea bazelor de date ce conțin date financiare critice în sediul de rezervă.
74. 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 rezervă.
75. 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 organele de conducere ale instituției.

Capitolul III. EVALUAREA RISCURILOR

76. Instituția trebuie să își evalueze profilul de risc aferent TIC cel puțin anual sau dacă au fost operate modificări majore în procesele, sistemele, serviciile sau echipamentele critice aferente TIC. Urmare a evaluării profilului de risc, după caz, instituția va revizui cadrul intern corespunzător cât și măsurile de control aplicabile.
77. Instituția, în cazul în care a externalizate funcții operaționale și/sau servicii TIC și sisteme TIC ale oricărei activități de prestare de servicii către furnizori terți, inclusiv către entitățile din grup, trebuie să asigure eficacitatea măsurilor prevăzute în prezentul Regulament. Instituția rămâne pe deplin responsabil 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.

78. BNM, în cadrul controalelor pe teren, controalelor din oficiu și prin dispunerea efectuării misiunilor de audit, evaluează cadrul intern aferent TIC a fiecărei instituții, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate și cu profilul/apetitul de risc a instituției.
79. Dacă 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, sancțiuni sau măsuri sancționatorii.
80. Instituția este obligată să notifice BNM prin intermediul PCSI sau în cazul indisponibilității acestuia la adresa de email SupraveghereTIC@bnm.md despre incidentele majore respectând următoarele condiții:
   a) 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;
   b) un raport intermediar, în termen de cel mult în 3 zile din ziua producerii incidentului, ce 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;
   c) un raport final, semnat de membru al organului de conducere a instituției, în termen de cel mult 20 zile, pentru incidentele ce au dus la indisponibilitatea sistemele/serviciilor critice pentru o durată mai lungă de 1 oră, sau la solicitarea BNM. Raportul va conține analiza cauzelor principale ce au dus la producerea incidentului, 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.
81. 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, BNM informații cu privire la următoarele:
   a) rezultatele testelor de penetrare efectuate din extern;
   b) rezultatele scanărilor de vulnerabilități efectuate pentru toate resursele critice, conform situației la data de 31 decembrie;
   c) raport privind gestionarea incidentelor produse pe parcursul anului aferent sistemelor/serviciilor critice ale instituției;
   d) 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;
   e) raportul de evaluare a instituției în conformitate cu standardul PCI-DSS, în cazul când instituția este supusă unei astfel de evaluări anuale;
   f) rezultatele testărilor de continuitate sistemelor/serviciilor aferente TIC critice;
   g) raport privind gestionarea riscurilor aferente TIC identificate ca fiind semnificative.