Anexă
la Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr. ____ din _____ 2026

REGULAMENT PRIVIND REZILIENȚA OPERAȚIONALĂ DIGITALĂ A SECTORULUI FINANCIAR

Prezentul regulament pune în aplicare parțial (art. 1 alin. (1), art. 2 alin. (1)-(3), art. 3 pct. 1-19, 21-31, 35, 37, 38, 47-49, 51, 60 și 63-65, art. 4-9, art. 10 alin. (1)-(3), art. 11 alin. (1)-(8) și (10), art. 12 alin. (1)-(4), (6) și (7), art. 13-14, art. 17, art. 18 alin. (1) și (2), art. 19 alin. (1)-(6), art. 22-24, art. 25 alin. (1) și (3), art. 26 alin. (1)-(9), art. 27, art. 28 alin. (1)-(8), art. 29, art. 30 alin. (1)-(4), art. 45-47, art. 48 alin. (1), art. 49 alin. (1), art. 50-51 și art. 54-56) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011, publicat în Jurnalul Oficial al Uniunii Europene seria L, nr. 333 din 27 decembrie 2022, CELEX: 32022R2554.

Capitolul I
DISPOZIȚII GENERALE

Secțiunea 1
Obiectul reglementării

1. În scopul asigurării unui nivel comun ridicat de reziliență operațională digitală, prezentul regulament stabilește cerințe uniforme privind securitatea tehnologiei informației și comunicațiilor (TIC) care sprijină procesele operaționale ale entităților financiare, după cum urmează:

1.1. cerințe aplicabile în legătură cu următoarele:

a) gestiunea riscurilor TIC;

b) raportarea incidentelor majore legate de TIC și notificarea în mod voluntar a amenințărilor cibernetice semnificative;

c) raportarea de către entitățile financiare menționate la subpct. 2.1-2.4 a incidentelor majore operaționale sau de securitate legate de plăți;

d) testarea rezilienței operaționale digitale;

e) schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități;

f) măsuri pentru buna gestionare a riscurilor TIC generate de părți terțe;

1.2. cerințe aferente acordurilor contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare;

1.3. norme privind supravegherea și asigurarea conformității aferente tuturor aspectelor vizate de prezentul regulament.

Secțiunea a 2-a
Domeniul de aplicare

2. Prezentul regulament se aplică următoarelor entități (în continuare – entități financiare):

2.1. instituțiile de credit;

2.2. instituțiile de plată;

2.3. prestatorii de servicii de informare cu privire la conturi;

2.4. instituțiile emitente de monedă electronică;

2.5. societățile de asigurare și societățile de reasigurare;

2.6. intermediarii de asigurări și intermediarii de reasigurări, cu excepția celor care sunt microîntreprinderi, întreprinderi mici sau mijlocii în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii.

Prevederile pct. 70-75 nu se aplică entităților financiare menționate la subpct. 2.5 și 2.6 și prestatorilor de servicii de informare cu privire la conturi care prestează doar acest serviciu de plată.

Secțiunea a 3-a

Definiții

3. În sensul prezentului regulament se aplică următoarele definiții:

3.1. *activ informațional* – o colecție de informații, materială sau imaterială, care merită protejată;

3.2. *activ TIC* – un activ software sau hardware din rețelele și sistemele informatice utilizate de entitatea financiară;

3.3. *amenințare cibernetică* – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau întreruperi la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;

3.4. *amenințare cibernetică semnificativă* – o amenințare cibernetică ale cărei caracteristici tehnice indică faptul că ar putea cauza un incident major legat de TIC sau un incident major operațional sau de securitate legat de plăți;

3.5. *atac cibernetic* – un incident rău-intenționat legat de TIC, cauzat prin intermediul unei tentative comise de un factor perturbator care generează amenințări de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține acces neautorizat la un activ ori a utiliza în mod neautorizat un activ;

3.6. *autoritate publică* – orice entitate guvernamentală sau altă entitate a administrației publice, inclusiv băncile centrale naționale;

3.7. *date operative privind amenințările* – informații care au fost agregate, transformate, analizate, interpretate sau îmbogățite pentru a oferi contextul necesar procesului decizional și pentru a face posibilă o înțelegere adecvată și suficientă cu scopul de a atenua impactul unui incident legat de TIC sau al unei amenințări cibernetice, inclusiv detaliile tehnice ale unui atac cibernetic, persoanele responsabile de atac, modul de operare și motivațiile acestora;

3.8. *filială* – o întreprindere controlată de o societate-mamă, care deține puterea de a exercita sau exercită efectiv o influență dominantă sau un control asupra acesteia, iar societatea-mamă și filiala au o bază comună de gestionare asigurată de societatea-mamă;

3.9. *funcție critică sau importantă* – o funcție a cărei întrerupere ar afecta în mod semnificativ performanța financiară a unei entități financiare 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 entitatea financiară, a condițiilor și obligațiilor aferente autorizației sale sau a altor obligații care îi revin în temeiul dreptului aplicabil în domeniul serviciilor financiare. Funcțiile critice în sensul Legii nr. 232/2016 privind redresarea și rezoluția băncilor sunt considerate funcții critice sau importante;

3.10. *furnizor terț de servicii TIC* – o întreprindere care furnizează servicii TIC;

3.11. *furnizor terț de servicii TIC stabilit într-un stat terț* – un furnizor terț de servicii TIC care este o persoană juridică stabilită într-un stat terț și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;

3.12. *grup* – o societate-mamă și toate filialele acesteia;

3.13. *incident legat de TIC* – un eveniment unic sau o serie de evenimente conexe neplanificate de entitatea financiară care compromit securitatea rețelelor și a sistemelor informatice și care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;

3.14. *incident major legat de TIC* – un incident legat de TIC care are un impact negativ puternic asupra rețelelor și sistemelor informatice care sprijină funcțiile critice sau importante ale entității financiare;

3.15. *incident major operațional sau de securitate legat de plăți* – un incident operațional sau de securitate legat de plăți care are un efect negativ puternic asupra serviciilor legate de plăți furnizate;

3.16. *incident operațional sau de securitate legat de plăți* – un eveniment unic sau o serie de evenimente conexe neplanificate de entitățile financiare menționate la subpct. 2.1-2.4, legate sau nu de TIC, care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor legate de plăți sau asupra serviciilor legate de plăți furnizate de entitatea financiară;

3.17. *instituție de credit* – bancă în sensul art. 3 din Legea nr. 202/2017 privind activitatea băncilor;

3.18. *instituție de plată* – societate de plată în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;

3.19. *instituție emitentă de monedă electronică* – societate emitentă de monedă electronică în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;

3.20. *intermediar de asigurări* – intermediar în asigurări în sensul art. 4 din Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare;

3.21. *intermediar de reasigurări* – intermediar în reasigurări în sensul art. 4 din Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare;

3.22. *întreprindere mică* – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;

3.23. *întreprindere mijlocie* – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;

3.24. *microîntreprindere* – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;

3.25. *momentul obiectiv pentru restabilire (MOR)* – perioada minimă anterioară unui eveniment sau incident de continuitate pentru care entitatea financiară recuperează sau restabilește datele din surse alternative (de exemplu, un MOR de 24 de ore înseamnă că informația este restabilită la starea din ziua precedentă, cu 24 de ore anterior apariției incidentului);

3.26. *organ de conducere* – organele entității financiare numite în conformitate cu legislația aplicabilă, împuternicite să stabilească strategia, obiectivele și orientarea generală ale entității financiare, care supraveghează și monitorizează procesul decizional de conducere, precum și persoanele care conduc în mod efectiv activitatea entității financiare;

3.27. *perioada maximă de întrerupere tolerabilă (PMIT)* – perioada maximă pentru care activitatea poate fi întreruptă, iar impactul asupra activității entității financiare este tolerabil;

3.28. *prestator de servicii de informare cu privire la conturi* – în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;

3.29. *rețea* – sisteme de transmisie, indiferent dacă sunt bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, după caz,

echipamente de comutare sau de rutare și alte resurse, inclusiv elemente de rețea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv rețele de comunicații prin satelit, rețele fixe (cu comutare de circuite și cu comutare de pachete, inclusiv internet) și mobile, rețele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, indiferent de tipul de informație transmisă;

3.30. *reziliență operațională digitală* – capacitatea unei entități financiare de a construi, a asigura și a reevalua integritatea și fiabilitatea sa operațională, prin asigurarea, în mod direct sau indirect, utilizând servicii oferite de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC care sunt necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de entitatea financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora, inclusiv pe întreaga durată a perturbărilor;

3.31. *risc de concentrare a serviciilor TIC* – o expunere la unul sau mai mulți furnizori terți de servicii TIC relaționați care nu sunt ușor de înlocuit și 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 entități financiare de a oferi funcții critice sau importante ori ar putea genera alte tipuri de efecte negative pentru aceasta, inclusiv pierderi mari, sau poate pune în pericol stabilitatea financiară a țării;

3.32. *risc TIC* – orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, dacă se materializează, poate compromite securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiilor și a proceselor sau a furnizării serviciilor prin crearea de efecte negative în mediul digital sau fizic;

3.33. *risc TIC generat de părți terțe* – un risc TIC care poate apărea în cadrul unei entități financiare în legătură cu utilizarea, de către aceasta, a serviciilor TIC oferite de furnizori terți de servicii TIC sau de subcontractanți ai acestora din urmă, inclusiv prin acorduri de externalizare;

3.34. *securitatea rețelelor și a sistemelor informatice* – capacitatea unei rețele și a unui sistem informatic de a rezista, la un anumit nivel de încredere, oricărui eveniment care poate compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

3.35. *servicii TIC* – servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi în mod continuu, inclusiv hardware ca serviciu și servicii hardware, care includ furnizarea de asistență tehnică prin actualizări de software sau firmware din partea furnizorului de hardware, cu excepția serviciilor de telefonie analogică tradiționale;

3.36. *sistem informatic* – orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale, precum și datele digitale stocate, prelucrate, recuperate sau transmise de acestea și de rețele în vederea operării, utilizării, protejării și întreținerii datelor respective;

3.37. *sistem TIC moștenit* – un sistem TIC ajuns la sfârșitul ciclului său de viață care nu este adecvat pentru a fi modernizat sau reparat, din motive tehnologice sau comerciale, sau pentru care furnizorul său ori un furnizor terț de servicii TIC nu mai oferă asistență, dar care încă este în uz și sprijină funcțiile entității financiare;

3.38. *sisteme și servicii TIC critice* – sistemele și serviciile TIC care sunt critice pentru entitatea financiară din perspectiva continuității și disponibilității lor sau a

securității informației prelucrate sau stocate și sunt esențiale pentru funcționarea adecvată a proceselor de guvernanță, a rolurilor corporative critice, inclusiv gestionarea riscurilor, a proceselor de activitate și a operațiunilor entității financiare;

3.39. *societate-mamă* – o întreprindere care controlează una sau mai multe filiale;

3.40. *stat terț* – stat care nu este Republica Moldova sau stat membru al Uniunii Europene ori al Spațiului Economic European;

3.41. *subcontractant TIC stabilit într-un stat terț* – un subcontractant TIC care este o persoană juridică stabilită într-un stat terț și care a încheiat un acord contractual fie cu un furnizor terț de servicii TIC, fie cu un furnizor terț de servicii TIC stabilit într-un stat terț;

3.42. *teste de penetrare bazate pe amenințări (TLPT)* – un cadru care imită tacticile, tehnicile și procedurile utilizate de actorii din viața reală care generează amenințări, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură o testare controlată, personalizată, bazată pe date operative (de tipul „echipa roșie") a sistemelor critice de producție în timp real ale entității financiare;

3.43. *timpul obiectiv pentru restabilire (TOR)* – perioada maximă în care entitatea financiară trebuie să își recupereze operațiunile, serviciile sau sistemele critice în urma unui eveniment sau incident major, adică 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.

3.44. *vulnerabilitate* – un punct slab, o sensibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat;

Secțiunea a 4-a
Principiul proporționalității

4. Entitățile financiare pun în aplicare normele prevăzute la capitolul II în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.

5. În plus, entitățile financiare aplică capitolele III, IV și V proporțional cu dimensiunea și profilul lor general de risc și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, astfel cum se prevede în mod specific în normele relevante din capitolele respective.

6. Banca Națională a Moldovei (în continuare – BNM) ia în considerare aplicarea principiului proporționalității de către entitățile financiare atunci când revizuiește coerența cadrului de gestionare a riscurilor TIC pe baza rapoartelor prezentate la cerere, în temeiul pct. 17.

Capitolul II
GESTIONAREA RISCURILOR TIC

Secțiunea 1
Guvernanță și organizare

7. Entitățile financiare dispun de un cadru intern de guvernanță și control care asigură o gestionare eficace și prudentă a riscurilor TIC, în conformitate cu pct. 16, cu scopul de a obține un nivel ridicat de reziliență operațională digitală.

8. Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor dispozițiilor legate de cadrul de gestionare a riscurilor TIC. În acest scop, organul de conducere:

8.1. poartă responsabilitatea finală pentru gestionarea riscurilor TIC ale entității financiare;

8.2. stabilește politici menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor;

8.3. stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții;

8.4. poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală, astfel cum este menționată la pct. 20, inclusiv pentru determinarea nivelului adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum este menționată la subpct. 20.2;

8.5. aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC ale entității financiare, menționate la pct. 51 și, respectiv, pct. 53, care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare;

8.6. aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare, precum și modificările semnificative aduse acestora;

8.7. alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante menționate la pct. 87, precum și competențe TIC pentru toți membrii personalului;

8.8. aprobă și verifică periodic politica entității financiare cu privire la acordurile privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC;

8.9. instituie, la nivel corporativ, canale de raportare care să îi permită să fie informat în mod corespunzător cu privire la:

a) acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC;

b) orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC;

c) impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC cu impactul acestora, precum și măsurile de răspuns, de recuperare și corective aplicate.

9. Entitățile financiare instituie funcția de ofițer de securitate a informației, responsabil de elaborarea, coordonarea implementării și monitorizarea respectării cadrului intern aferent securității informației. Ofițerul de securitate a informației este subordonat direct președintelui organului executiv sau administratorului entității financiare. În funcție de natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate, funcția de ofițer de securitate a informației poate fi cumulată cu funcția de control prevăzută la pct. 16, dacă ofițerul de securitate a informației nu are responsabilități de operare a sistemelor TIC, iar activitatea sa este evaluată de funcția de audit intern. Cumulul nu se admite în cazul instituțiilor de credit identificate ca societăți de importanță sistemică în sensul Legii nr. 202/2017 privind activitatea băncilor.

10. Entitățile financiare asigură, 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 lucrătoare, a deciziilor luate de organul de conducere

aferente domeniului TIC. Integritatea tuturor documentelor din cadrul PCSI se confirmă printr-o semnătură electronică calificată.

11. Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol pentru a monitoriza acordurile încheiate cu furnizorii terți de servicii TIC cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.

12. Membrii organului de conducere al entității financiare își actualizează în mod activ cunoștințele și competențele pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, proporționale cu nivelul riscurilor TIC gestionate.

Secțiunea a 2-a

Cadrul de gestionare a riscurilor TIC

13. Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, ca parte a sistemului lor general de gestionare a riscurilor, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală.

14. Cadrul de gestionare a riscurilor TIC include cel puțin strategii, politici, proceduri, precum și procese și instrumente TIC care sunt necesare pentru a proteja în mod corespunzător și adecvat toate activele informaționale și toate activele TIC, inclusiv software pentru calculatoare, hardware și servere, precum și pentru a proteja toate componentele și infrastructurile fizice relevante, cum sunt sediile, centrele de date și zonele desemnate sensibile, pentru a asigura că toate activele informaționale și toate activele TIC sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.

15. În conformitate cu cadrul lor de gestionare a riscurilor TIC, entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea unor strategii, politici, proceduri, procese și instrumente TIC adecvate. Acestea furnizează BNM, la cerere, informații complete și actualizate cu privire la riscurile TIC și la cadrul lor de gestionare a riscurilor TIC.

16. Entitățile financiare, altele decât microîntreprinderile, atribuie responsabilitatea pentru gestionarea și supravegherea riscurilor TIC unei funcții de control și asigură independența acestei funcții de control la un nivel adecvat, pentru a evita conflictele de interese. Entitățile financiare asigură în mod adecvat separarea și independența funcțiilor de gestionare a riscurilor TIC, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare sau cu un model intern de gestionare și control al riscurilor.

17. Cadrul de gestionare a riscurilor TIC se documentează și se revizuiește cel puțin o dată pe an, sau periodic în cazul microîntreprinderilor, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testarea relevantă a rezilienței operaționale digitale sau din procesele de audit relevante. Profilul de risc aferent TIC se documentează și se revizuiește cel puțin o dată pe an, precum și în cazul unor modificări majore ale proceselor, sistemelor, serviciilor sau echipamentelor TIC critice. Cadrul este îmbunătățit în permanență, pe baza experienței acumulate în urma punerii în aplicare și a monitorizării. Entitățile financiare prezintă BNM, la cererea acesteia, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.

18. Cadrul de gestionare a riscurilor TIC al entităților financiare, altele decât microîntreprinderile, este supus auditului intern de către auditori în mod regulat, în conformitate cu planul de audit al entităților financiare. Auditorii respectivi dețin

suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC, precum și o independență adecvată. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entităților financiare.

18.1. Entitățile financiare asigură efectuarea auditului, de către auditul intern și/sau extern, într-un interval de cel mult 3 ani, a tuturor sistemelor și serviciilor TIC critice. Auditul se efectuează cel puțin pentru următoarele sisteme, dacă sunt implementate de entitatea financiară: 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 a identităților și accesului, inclusiv privilegiat, sisteme de tip firewall, rețele private virtuale (VPN), sisteme de gestiune electronică a documentelor și mesagerie/comunicare internă și externă. Pentru sistemele și serviciile TIC critice operate de un furnizor terț de servicii TIC sau la nivelul grupului, auditul se poate baza pe rapoarte de asigurare independente care acoperă sistemele și controalele respective în perioada examinată, iar componentele aflate sub controlul entității financiare se auditează potrivit primei fraze.

19. Pe baza concluziilor evaluării de audit intern, entitățile financiare stabilesc un proces formal de urmărire, care include reguli pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC. Procesul stabilește, pentru fiecare constatare, acțiunile de remediere, persoana responsabilă și termenul, iar întârzierile se raportează organului de conducere.

20. Cadrul de gestionare a riscurilor TIC include o strategie privind reziliența operațională digitală, care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia privind reziliența operațională digitală include metode de abordare a riscurilor TIC și de realizare a obiectivelor TIC specifice, prin:

20.1. explicarea modului în care cadrul de gestionare a riscurilor TIC sprijină strategia de afaceri și obiectivele entității financiare;

20.2. stabilirea nivelului de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul pentru risc al entității financiare, și analizarea toleranței la impact pentru perturbările TIC;

20.3. stabilirea unor obiective clare privind securitatea informațiilor, inclusiv indicatori-cheie de performanță și indicatori-cheie de risc;

20.4. explicarea arhitecturii TIC de referință și a oricăror modificări necesare pentru atingerea obiectivelor specifice de activitate;

20.5. prezentarea diferitelor mecanisme instituite pentru a detecta incidentele legate de TIC, a preveni impactul acestora și a asigura protecție împotriva acestora;

20.6. evidențierea situației actuale a rezilienței operaționale digitale pe baza numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive;

20.7. implementarea testării rezilienței operaționale digitale, în conformitate cu capitolul IV din prezentul regulament;

20.8. conturarea unei strategii de comunicare în cazul producerii unor incidente legate de TIC cu privire la care este necesară informarea.

21. Entitățile financiare pot defini, în contextul strategiei privind reziliența operațională digitală menționate la pct. 20, o strategie TIC cuprinzătoare privind existența mai multor furnizori, la nivel de grup sau de entitate, care să prezinte principalele dependențe față de furnizorii terți de servicii TIC și să explice raționamentul care stă la baza mixului de achiziții de la furnizori terți de servicii TIC.

22. Entitățile financiare pot externaliza, în conformitate cu legislația în vigoare, sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe. În cazul unei astfel de externalizări, entitatea financiară

rămâne pe deplin responsabilă de verificarea conformității cu cerințele de gestionare a riscurilor TIC.

Secțiunea a 3-a

Sisteme, proceduri și instrumente TIC

23. Pentru a aborda și a gestiona riscurile TIC, entitățile financiare utilizează și mențin sisteme, procese și instrumente TIC actualizate care sunt:

23.1. adecvate magnitudinii operațiunilor care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității;

23.2. fiabile;

23.3. dotate cu suficientă capacitate de a prelucra cu precizie datele necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii;

23.4. reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.

24. Entitățile financiare definesc și pun în aplicare procese de planificare și monitorizare a performanței și capacității sistemelor, serviciilor și echipamentului TIC și de securitate a informației pentru a împiedica, a detecta și a răspunde prompt la eventuale incidente legate de performanță.

25. Entitățile financiare stabilesc procese și elaborează proceduri privind gestiunea proiectelor TIC, de securitate a informației și de 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.

26. Entitățile financiare asigură că documentația fiecărui proiect TIC, de securitate a informației și de continuitate a activității definește cel puțin următoarele informații:

26.1. scopul și obiectivele proiectului;

26.2. rolurile și responsabilitățile;

26.3. evaluarea riscurilor asociate proiectului, în conformitate cu prevederile pct. 36;

26.4. planul, calendarul și etapele proiectului;

26.5. principalele obiective intermediare;

26.6. cerințele de gestionare a modificărilor;

26.7. cerințele de securitate a informației care sunt analizate și aprobate de către o funcție independentă de cea de gestiune a proiectului.

27. Entitățile financiare, aferent portofoliului de proiecte TIC, de securitate a informației și de continuitate a activității, monitorizează și diminuează 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.

28. Entitățile financiare se asigură 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.

29. Entitățile financiare stabilesc proceduri de raportare ad-hoc și la intervale regulate de timp, cel puțin o dată la 6 luni, către organul de conducere, a informațiilor privind evoluția și riscurile asociate proiectelor TIC, de securitate a informației și de continuitate a activității, în funcție de importanța și dimensiunea acestora.

Secțiunea a 4-a

Identificare

30. Ca parte a cadrului de gestionare a riscurilor TIC menționat la pct. 14, entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC, activele informaționale și activele TIC care sprijină funcțiile respective, precum și rolurile și dependențele lor în legătură cu riscurile TIC. Entitățile financiare revizuiesc după caz, dar cel puțin anual, caracterul adecvat al acestei clasificări și al oricărei documentări relevante.

31. Entitățile financiare identifică în mod constant toate sursele de riscuri TIC, în special expunerea la riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. Entitățile financiare revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc care au un impact asupra lor.

32. Entitățile financiare, altele decât microîntreprinderile, efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic și proceselor sau procedurilor care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.

33. Entitățile financiare identifică toate activele informaționale și activele TIC, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC. Inventarul este suficient de detaliat pentru a permite identificarea imediată a resursei, a amplasamentului acesteia, a proprietarului și a gestionarului resursei TIC.

34. Entitățile financiare identifică și documentează toate procesele care depind de furnizori terți de servicii TIC și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.

35. În scopul aplicării pct. 30, 33 și 34, entitățile financiare mențin inventarele relevante și le actualizează periodic și de fiecare dată când are loc orice modificare majoră, astfel cum este menționată la pct. 32.

36. Entitățile financiare, altele decât microîntreprinderile, efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC moștenite și, în orice caz, înainte și după conectarea unor tehnologii, aplicații sau sisteme. Evaluările riscurilor TIC prevăzute la pct. 31, 32 și la prezentul punct vizează cel puțin următoarele categorii de riscuri aferente TIC și securității informației:

36.1. riscuri de disponibilitate și continuitate;

36.2. riscuri de securitate;

36.3. riscuri de schimbare;

36.4. riscuri de integritate a datelor;

36.5. riscuri asociate părților terțe și externalizărilor TIC;

36.6. riscuri de conformitate;

36.7. riscuri de concentrare a serviciilor TIC.

Secțiunea a 5-a

Protecție și prevenire

37. În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare monitorizează și controlează în mod continuu securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.

38. Entitățile financiare stabilesc, achiziționează și pun în aplicare politici, proceduri, procese și instrumente în domeniul securității TIC care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.

39. În vederea realizării obiectivelor menționate la pct. 38, entitățile financiare utilizează soluții și procese TIC care sunt adecvate în conformitate cu principiul proporționalității. Respectivele soluții și procese TIC:

39.1. asigură clasificarea, declasificarea informațiilor și permit aplicarea marcajelor de confidențialitate pe toată informația ce circulă în cadrul entității financiare;

39.2. asigură securitatea mijloacelor de transfer al datelor;

39.3. reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de defecțiuni tehnice care pot împiedica derularea activităților;

39.4. previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor;

39.5. asigură protecția datelor împotriva riscurilor aferente gestionării datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane.

40. Ca parte a cadrului de gestionare a riscurilor TIC menționat la pct. 14, entitățile financiare:

40.1. elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz. Politica conține cel puțin: scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare și o descriere a rolurilor și responsabilităților privind gestionarea securității informației;

40.2. stabilesc, urmând o abordare bazată pe riscuri, o structură de gestionare solidă a rețelei și a infrastructurii care utilizează tehnici, metode, procese și proceduri adecvate ce pot include punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice;

40.3. pun în aplicare politici care limitează accesul fizic sau logic la activele informaționale și activele TIC la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora, asigurându-se că acestea conțin cel puțin următoarele principii și măsuri de control:

a) utilizatorilor li se acordă drepturi minime de acces, strict necesare pentru executarea sarcinilor;

b) acțiunile din cadrul sistemelor informatice și serviciilor TIC critice pot fi atribuite unor utilizatori concreți, iar utilizarea conturilor generice sau partajate este limitată și documentată cu argumentele de rigoare;

c) se implementează măsuri de control aferente conturilor privilegiate prin limitarea strictă a utilizării lor și prin monitorizarea permanentă, cu înregistrarea tuturor acțiunilor și activităților efectuate în conturile respective într-un sistem centralizat de gestiune a evenimentelor;

d) drepturile de acces ale utilizatorilor sunt acordate, retrase sau modificate în conformitate cu responsabilitățile predefinite, în cadrul unor procese automatizate sau semiautomatizate, documentate, ale entității financiare, care implică obligatoriu proprietarul resursei informaționale. Pe durata concediilor sociale prevăzute de Codul muncii al Republicii Moldova nr. 154/2003 sau a suspendării contractului individual de

muncă, precum și în cazul neutilizării conturilor pentru o perioadă mai mare de 60 de zile, conturile utilizatorilor sunt dezactivate, iar în caz de încetare a contractului de muncă, contul este dezactivat și drepturile de acces sunt retrase imediat. În cazul concediilor anuale, conturile privilegiate și drepturile de acces de la distanță ale utilizatorilor se dezactivează implicit, cu excepția cazurilor aprobate de ofițerul de securitate a informației, iar pentru celelalte conturi entitatea financiară stabilește măsurile aplicabile pe baza evaluării riscurilor;

e) drepturile de acces la resursele TIC sunt 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;

f) se implementează mecanisme de izolare rapidă a resurselor informaționale care au fost afectate de incidente de securitate sau au fost ținta unor atacuri cibernetice. Gradul de automatizare a izolării se stabilește pe baza evaluării riscurilor, ținând cont de caracterul critic al resursei și de cerințele de continuitate. Pentru stațiile de lucru și resursele necritice izolarea poate fi automată, iar pentru sistemele TIC critice decizia de izolare se ia conform procedurilor de răspuns la incidente, cu confirmarea persoanelor responsabile;

g) se aplică metode de autentificare proporționale cu importanța sistemelor informatice, a serviciilor TIC sau a informațiilor accesate, utilizând cel puțin parole complexe pentru conturile obișnuite și autentificarea cu cel puțin doi factori pentru conturile privilegiate aferente sistemelor TIC critice, precum și pentru toate accesările de la distanță;

40.4. pun în aplicare politici și proceduri pentru mecanisme solide de autentificare, bazate pe standarde relevante și sisteme de control specifice, precum și măsuri de protecție a cheilor criptografice, prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor TIC;

40.5. pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrilor sistemelor sau de securitate, care sunt stabilite având o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat;

40.6. dispun de politici documentate, adecvate și cuprinzătoare pentru corecții și actualizări;

40.7. stabilesc, pe baza unei abordări bazate pe riscuri, procese și proceduri privind achiziția, dezvoltarea și mentenanța sistemelor TIC, care asigură că, înainte de orice achiziție sau dezvoltare, cerințele funcționale și nefuncționale, inclusiv cerințele minime de securitate a informației, sunt clar definite și aprobate de organul de conducere sau de persoana ori funcția desemnată de acesta, în funcție de nivelul de risc;

40.8. aplică măsuri de control împotriva modificării neintenționate sau a manipulării intenționate a sistemelor TIC pe durata dezvoltării și a implementării în mediul de producție și asigură separarea responsabilităților de dezvoltare, testare și implementare;

40.9. aplică o metodologie de testare și aprobare a sistemelor TIC noi sau modificate, care asigură că acestea funcționează conform proiectării și că mediile de testare reflectă în mod corespunzător mediul de producție.

41. În scopul aplicării subpct. 40.2, entitățile financiare stabilesc o infrastructură de conectare a rețelei într-un mod care permite întreruperea sau segmentarea instantanee a acesteia, pentru a reduce la minimum și a preveni contagiunea, în special în cazul proceselor financiare interconectate.

42. În scopul aplicării subpct. 40.5, procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de proceduri specifice. Procesul include proceduri pentru gestionarea modificărilor în situații de urgență, care asigură un nivel adecvat de protecție.

Secțiunea a 6-a
Detectare

43. Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu pct. 92-94, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative. Toate mecanismele de detectare sunt testate cu regularitate, în conformitate cu pct. 117. Evenimentele de securitate relevante pentru eventuale investigații, generate de toate sistemele și serviciile TIC critice, sunt colectate în soluții specializate care le asigură integritatea și disponibilitatea. Mecanismele de detectare includ sisteme de prevenire și detectare a intruziunilor.

44. Entitățile financiare identifică vulnerabilitățile aferente aplicațiilor software, sistemelor, echipamentelor de rețea și stațiilor de lucru critice, prin efectuarea scanărilor periodice, și implementează în timp util măsuri de control de diminuare a impactului sau a probabilității exploatării vulnerabilităților identificate și a riscurilor implicate sau aplică măsuri de control compensatorii.

45. Entitățile financiare își stabilesc configurări de securitate de referință pentru toate echipamentele de rețea critice.

46. Entitățile financiare implementează 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.

47. Entitățile financiare implementează măsuri de control și protecție a serverelor, stațiilor de lucru, dispozitivelor mobile și altor echipamente ce sunt conectate la rețeaua acestora sau gestionează informații din cadrul entității financiare. Entitățile financiare implementează mecanisme de verificare a integrității aplicațiilor software critice instalate pe servere.

48. Entitățile financiare implementează mecanisme de monitorizare a informațiilor ce părăsesc perimetrul rețelei interne. Sunt monitorizate cel puțin informațiile transmise prin conexiunea la rețeaua internet, informațiile imprimate, informațiile copiate pe dispozitive externe și informațiile transmise prin e-mail.

49. Mecanismele de monitorizare și detectare permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare și inițiere a proceselor de răspuns la incidentele legate de TIC, inclusiv mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC.

49.1. Instituțiile de credit utilizează, ca nivel suplimentar de control al mecanismelor de monitorizare și detectare, soluții de analiză a evenimentelor de securitate bazate pe tehnici de inteligență artificială, cum sunt modelele de învățare automată, care identifică tipare și anomalii fără a se limita la reguli de detectare definite explicit. Soluțiile analizează, fără a afecta funcționarea sistemelor monitorizate, cel puțin evenimentele de securitate colectate potrivit pct. 43 de la sistemele și serviciile TIC critice și asigură:

a) corelarea automată a evenimentelor provenite din surse multiple, inclusiv din sistemele de gestionare a identităților și a accesului, din infrastructura de rețea și din sistemele de securitate;

b) identificarea comportamentelor anormale și a tiparelor suspecte, inclusiv a legăturilor dintre evenimente care, analizate separat, nu generează alerte;

c) clasificarea și prioritizarea alertelor în funcție de riscul estimat, cu indicarea evenimentelor care au stat la baza fiecărei alerte;

d) păstrarea rezultatelor analizei și a alertelor generate pe perioada prevăzută la pct. 68, pentru trasabilitate și pentru evaluarea eficacității detectării.

49.2. Prelucrarea evenimentelor de securitate de către soluțiile prevăzute la subpct. 49.1, inclusiv executarea modelelor, are loc în infrastructura TIC proprie a instituției de credit, aflată sub controlul său direct, sau, în cazul prevăzut la subpct. 49.3, în infrastructura TIC proprie a grupului din care face parte. În scopul acestei analize, evenimentele de securitate, informațiile extrase din ele și rezultatele prelucrării nu se transmit către servicii de prelucrare sau de inferență furnizate în afara acestei infrastructuri. Soluțiile pot primi din surse externe actualizări ale modelelor și ale regulilor de detectare, fără transmiterea către acestea a datelor prelucrate.

49.3. Instituția de credit care face parte dintr-un grup poate utiliza soluția prevăzută la subpct. 49.1 operată de societatea-mamă sau de o altă entitate din grup, dacă sunt îndeplinite cumulativ următoarele condiții:

a) infrastructura TIC în care are loc prelucrarea se află sub controlul direct al grupului și este amplasată pe teritoriul Republicii Moldova sau al unui stat membru al Uniunii Europene ori al Spațiului Economic European;

b) acordul cu entitatea din grup care operează soluția respectă cerințele capitolului V, inclusiv drepturile de acces, de inspecție și de audit ale instituției de credit și ale BNM prevăzute la subpct. 161.5;

c) instituția de credit are acces permanent la alertele și la rezultatele analizei care o privesc, precum și la evenimentele care au stat la baza acestora;

d) soluția îndeplinește cerințele prevăzute la subpct. 49.1.

49.4. Instituțiile de credit validează modelele înainte de utilizarea lor în mediul de producție și le reevaluează cel puțin o dată pe an și după orice modificare semnificativă, ca parte a testării mecanismelor de detectare prevăzute la pct. 43. Validarea și reevaluarea verifică cel puțin capacitatea de identificare a activităților anormale, ponderea alertelor fals pozitive și fals negative, rezistența modelelor la manipularea datelor de intrare și riscurile de securitate asociate utilizării lor. În cazul prevăzut la subpct. 49.3, validarea și reevaluarea pot fi efectuate la nivelul grupului, iar rezultatele lor se pun la dispoziția instituției de credit.

49.5. Soluțiile prevăzute la subpct. 49.1 completează celelalte mecanisme de monitorizare și detectare, fără a le înlocui, și nu înlocuiesc analiza alertelor de către personalul cu atribuții de monitorizare și de răspuns la incidente (pct. 50 și subpct. 94.3). Acțiunile de răspuns cu impact semnificativ asupra sistemelor TIC nu se aplică numai pe baza rezultatelor acestor soluții, fără confirmarea persoanelor responsabile, cu excepția mecanismelor automate de răspuns aprobate în prealabil potrivit subpct. 40.3 lit. f).

50. Entitățile financiare alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.

Secțiunea a 7-a

Răspuns și recuperare

51. Ca parte a cadrului de gestionare a riscurilor TIC și pe baza cerințelor de identificare, entitățile financiare instituie o politică cuprinzătoare de continuitate a activității TIC, care poate fi adoptată sub forma unei politici specifice dedicate sau ca parte integrantă a politicii generale de continuitate a activității entității financiare. Politica conține cel puțin scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare

și o descriere a rolurilor și responsabilităților privind gestionarea continuității activității în cadrul entității financiare.

52. Entitățile financiare pun în aplicare politica de continuitate a activității TIC prin regulamente, măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate care vizează:

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

52.2. evaluarea impactului pe care îl pot avea întreruperile în procesele identificate asupra activității entității financiare;

52.3. stabilirea indicatorilor de continuitate aferenți proceselor prin specificarea PMIT pentru procesele de activitate;

52.4. 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;

52.5. stabilirea indicatorilor de continuitate pentru toate sistemele și serviciile TIC critice prin indicarea TOR și MOR;

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

52.7. stabilirea strategiilor de continuitate pentru desfășurarea proceselor critice în timp în condițiile în care riscurile au fost identificate. Se iau în considerare cel puțin două strategii de continuitate: restabilirea resurselor critice sau aplicarea procedurilor alternative de lucru;

52.8. 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;

52.9. asigurarea continuității funcțiilor critice sau importante ale entității financiare în baza rezultatelor obținute conform subpct. 52.1-52.8;

52.10. un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare;

52.11. activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare a impactului, adecvate pentru fiecare tip de incident legat de TIC și previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate și stabilite;

52.12. estimarea efectelor, a daunelor și a pierderilor preliminare;

52.13. stabilirea unor măsuri de comunicare și de gestionare a crizelor care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante și raportarea către BNM, în conformitate cu pct. 98-103.

53. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC asociate, care, în cazul altor entități financiare decât microîntreprinderile, sunt supuse unor evaluări de audit intern independente.

54. Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, în special în ceea ce privește funcțiile critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC.

55. Entitățile financiare asigură instruirea personalului entității financiare pentru ca aceștia să conștientizeze importanța asigurării continuității activității entității financiare, 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.

56. Ca parte a politicii generale de continuitate a activității, entitățile financiare efectuează o analiză a impactului asupra activității (BIA) al expunerilor lor la perturbări grave ale activității. În conformitate cu BIA, entitățile financiare evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii, după caz. BIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora. Entitățile financiare se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu BIA, în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice.

Pe baza BIA, entitățile financiare identifică sistemele și serviciile TIC critice din perspectiva continuității și disponibilității, cărora li se aplică subpct. 52.5 și pct. 64, 74 lit. d), 75 și 76. Pentru sistemele și serviciile TIC critice doar din perspectiva securității informației, copiile de rezervă se stabilesc pe baza evaluării riscurilor.

57. Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare:

57.1. testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC în legătură cu sistemele TIC care sprijină toate funcțiile cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC care sprijină funcții critice sau importante. Rezultatele testărilor sunt documentate adecvat, cu păstrarea probelor comprehensive, și sunt raportate organului de conducere. Testarea vizează cel puțin continuitatea sistemelor și a infrastructurii TIC, a rolurilor și a personalului, a infrastructurii non-TIC (alimentarea cu energie electrică, protecția împotriva incendiilor, sistemele de alarmă și de climatizare), cunoașterea planurilor de către personalul responsabil și, după caz, reluarea proceselor critice în locația de rezervă. Testarea rolurilor și a personalului, a infrastructurii non-TIC și a reluării proceselor critice în locația de rezervă poate fi eșalonată, cu condiția ca fiecare element să fie testat cel puțin o dată la 2 ani. Testarea efectuată potrivit pct. 61 sau 62 se consideră parte a testării anuale pentru sistemele, serviciile și procesele pe care le acoperă;

57.2. testează planurile de comunicare în situații de criză instituite;

57.3. cu excepția microîntreprinderilor, includ în planurile de testare prevăzute la subpct. 57.1 scenarii de atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la pct. 63-79;

57.4. își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC, ținând seama de rezultatele testelor efectuate în conformitate cu subpct. 57.1 și 57.2, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.

58. Entitățile financiare, altele decât microîntreprinderile, au o funcție de gestionare a crizelor, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză.

59. Entitățile financiare păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor de continuitate atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.

60. Entitățile financiare, altele decât microîntreprinderile, raportează către BNM, la cererea acesteia, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.

61. Entitățile financiare desemnate de BNM pun în aplicare anual, într-o zi lucrătoare din luna octombrie sau noiembrie, în coordonare prealabilă cu BNM, planul de continuitate a activității TIC din centrul de date de rezervă, pentru sistemele sau serviciile critice convenite cu BNM. BNM desemnează entitățile financiare ținând seama de criteriile prevăzute la subpct. 130.1 și 130.2 și comunică desemnarea, împreună cu sistemele sau serviciile convenite, cu cel puțin 6 luni înainte de luna testării.

62. Entitățile financiare desemnate de BNM pun în aplicare o dată la 3 ani, într-o zi lucrătoare din luna noiembrie, în coordonare prealabilă cu BNM, planul de continuitate a activității pentru procesele și resursele critice, cu rularea acestora din centrul de date de rezervă și cu relocarea personalului critic într-o locație de rezervă. În anul în care se efectuează testarea prevăzută la prezentul punct, aceasta ține loc și de testarea prevăzută la pct. 61.

Secțiunea a 8-a

Politici și proceduri privind copiile de rezervă și proceduri și metode de restaurare și recuperare

63. Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează și documentează:

63.1. politici și proceduri privind copiile de rezervă care precizează sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau al nivelului de confidențialitate al datelor;

63.2. proceduri și metode de restaurare și recuperare.

64. Entitățile financiare asigură crearea copiilor de rezervă ale bazelor de date aferente sistemelor și serviciilor TIC critice după următoarea schemă sau după o altă schemă care asigură cel puțin aceleași puncte de restaurare și aceleași perioade de retenție:

a) copie de tip full la finele fiecărui an cu asigurarea retenției pentru ultimii 2 ani;

b) copie de tip full la finele fiecărei luni cu asigurarea retenției pentru ultimele 6 luni;

c) copie de tip diferențial la finele fiecărei zile cu asigurarea retenției pentru ultimele 30 de zile.

65. Entitățile financiare instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. Testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare se efectuează periodic, cel puțin o dată pe an. Entitățile financiare dispun de mecanisme de verificare a integrității copiilor de rezervă.

66. Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz.

67. Entitățile financiare, altele decât microîntreprinderile, mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale. Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc, fără a aduce atingere pct. 70-75.

Secțiunea a 9-a

Retenția datelor și a jurnalelor de audit

68. Entitățile financiare asigură, inclusiv în cazul externalizării sistemelor și serviciilor TIC critice, integritatea și disponibilitatea informației, precum și o perioadă de retenție de cel puțin 12 luni sau, dacă aceasta este mai lungă, perioada scursă de la ultima perioadă supusă controlului de către BNM, dar nu mai mult de 24 de luni. Se asigură retenția informației conținute în:

a) jurnalele de audit ce conțin înregistrări de audit relevante pentru cel puțin următoarele sisteme/servicii, dacă sunt implementate de entitatea financiară: SAPI, instrumente de plată cu acces la distanță, SWIFT, sistem de bază (corebanking), sisteme de gestiune a bazelor de date, Active Directory (AD), sisteme de gestionare a accesului privilegiat (Privileged Access Management, PAM), sisteme de tip firewall, VPN, echipamente critice de rețea, sisteme de gestiune electronică a documentelor;

b) mesajele transmise/primite prin intermediul serviciului de poștă electronică oficială a entității financiare;

c) sistemele de monitorizare video a zonelor critice aferente centrului de date principal și centrului de date de rezervă.

69. Organul de conducere al entității financiare asigură că informația stocată în cadrul sistemelor TIC ce conțin date contabile este actuală și se bazează pe tranzacții reale.

Secțiunea a 10-a

Cerințe minime pentru centrele de date și conexiuni

70. Entitățile financiare asigură 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. Decizia se fundamentează pe o analiză de riscuri care urmărește accesibilitatea unei părți cât mai largi a populației la aceste ATM-uri și puncte de prezență.

71. Entitățile financiare dispun de un centru de date de rezervă capabil să preia activitatea tuturor proceselor critice în cazul indisponibilității centrului de date principal.

72. Entitățile financiare asigură conexiunea la rețeaua internet pentru centrul de date principal și centrul de date de rezervă prin intermediul a cel puțin doi prestatori de servicii.

Secțiunea a 11-a

Cerințe tehnice pentru echipamente și sisteme de suport

73. Entitățile financiare asigură 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 maximum 6 ore;

b) generator de curent electric capabil să asigure necesitățile echipamentelor;

c) sistem de monitorizare video 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.

74. Entitățile financiare asigură redundanța următoarelor echipamente și servicii din centrul de date principal:

a) echipamentelor de rețea ce asigură conexiunea la internet a centrului de date principal și a centrului de date de rezervă;

b) echipamentelor de rețea ce asigură legătura între nodurile informaționale principale ale entității financiare;

c) echipamentelor firewall;

d) echipamentelor pe care rulează bazele de date aferente sistemelor și serviciilor TIC critice;

e) 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 entitatea financiară;

f) serviciilor DNS externe ale entității financiare, cu localizarea obligatorie a unuia pe teritoriul Republicii Moldova.

75. Entitățile financiare asigură replicarea bazelor de date ce conțin date financiare critice în centrul de date de rezervă.

76. Entitățile financiare asigură lunar păstrarea în regim offline sau în regim imutabil, protejat tehnic împotriva modificării, ștergerii și criptării neautorizate, inclusiv de către conturile privilegiate, în formă criptată, a cel puțin unei copii de rezervă de tip full a datelor pentru toate sistemele lor critice, într-o locație diferită de centrul de date principal și de centrul de date de rezervă. În cazul sistemelor și serviciilor TIC critice externalizate, cerințele prevăzute la pct. 64 și la prezentul punct pot fi îndeplinite prin măsuri echivalente ale furnizorului terț de servicii TIC, prevăzute în acordul contractual și verificate potrivit pct. 145.

77. Entitățile financiare asigură 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 fac sistemele TIC moștenite, care rulează într-o rețea izolată și pentru care se aplică măsuri compensatorii de securitate. Lista sistemelor exceptate se aprobă de organul de conducere al entității financiare.

Secțiunea a 12-a

Obiective și verificări de recuperare

78. Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.

79. În cazul recuperării în urma unui incident legat de TIC, entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat. Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.

Secțiunea a 13-a

Învățăminte și perspective de dezvoltare

80. Entitățile financiare dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale.

81. Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC după ce un incident major legat de TIC le perturbă activitățile de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC.

82. Entitățile financiare, altele decât microîntreprinderile, comunică către BNM, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la pct. 81.

83. Verificările ulterioare incidentelor legate de TIC menționate la pct. 81 stabilesc dacă procedurile instituite au fost urmate și dacă măsurile luate au fost eficace, inclusiv în ceea ce privește următoarele:

83.1. promptitudinea reacției la alertele de securitate și determinarea impactului și a gravității incidentelor legate de TIC;

83.2. calitatea și rapiditatea efectuării unei analize judiciare, acolo unde se consideră necesar;

83.3. eficacitatea activării nivelurilor succesive de intervenție (incident escalation) în caz de incidente în cadrul entității financiare;

83.4. eficacitatea comunicării interne și externe.

84. Învățămintele desprinse în urma testării rezilienței operaționale digitale, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC.

85. Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală menționate la pct. 20. Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC, în special în legătură cu funcțiile critice sau importante, și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.

86. Personalul cu funcție-cheie pe domeniul TIC raportează cel puțin o dată pe an către organul de conducere cu privire la rezultatele menționate la pct. 84 și propune recomandări.

87. Entitățile financiare elaborează programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale ca module obligatorii în cadrul programelor lor de formare a personalului. Respectivele programe și cursuri de formare se aplică tuturor angajaților, inclusiv personalului cu funcții-cheie și membrilor organelor de conducere, și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante, în conformitate cu subpct. 160.9. Instruirile de conștientizare cu privire la riscurile de securitate a informației se desfășoară cel puțin o dată pe an.

88. Entitățile financiare, altele decât microîntreprinderile, monitorizează evoluțiile tehnologice relevante în mod continuu, inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.

Secțiunea a 14-a

Comunicare în situații de criză

89. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.

90. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare politici de comunicare pentru personalul intern și pentru părțile interesate externe. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea riscurilor TIC, în special personalul responsabil pentru răspuns și recuperare, și personalul care trebuie să fie informat.

91. Cel puțin o persoană din entitatea financiară este responsabilă de punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media.

Capitolul III
GESTIONAREA, CLASIFICAREA ȘI RAPORTAREA INCIDENTELOR LEGATE DE TIC

Secțiunea 1
Procesul de gestionare a incidentelor legate de TIC

92. Entitățile financiare definesc, instituie și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC.

92.1. Entitățile financiare stabilesc proceduri eficiente de comunicare internă și externă, de notificare și de 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, comunicându-se măsurile de remediere luate imediat și cele care urmează a fi implementate pentru a preveni astfel de incidente pe viitor.

93. Entitățile financiare înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative. Entitățile financiare instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea cauzelor lor principale, astfel încât să se prevină apariția unor astfel de incidente. Entitățile financiare păstrează probele aferente incidentelor legate de TIC necesare investigațiilor și analizelor criminalistice.

94. Procesul de gestionare a incidentelor legate de TIC menționat la pct. 92:

94.1. instituie indicatori de avertizare timpurie;

94.2. stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite la pct. 96;

94.3. alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC;

94.4. stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media și pentru notificarea clienților, proceduri interne de activare a nivelurilor succesive de intervenție, inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz;

94.5. asigură că cel puțin incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la cel puțin incidentele

majore legate de TIC, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a unor astfel de incidente legate de TIC;

94.6. stabilește proceduri de răspuns la incidentele legate de TIC în vederea atenuării efectelor și a asigurării faptului că serviciile devin operaționale și sigure în timp util.

95. Entitățile financiare instituie și pun 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 2-a

Clasificarea incidentelor legate de TIC și a amenințărilor cibernetice

96. Entitățile financiare clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii:

96.1. numărul și/sau relevanța clienților sau a contrapărților financiare afectate și, după caz, cuantumul și numărul tranzacțiilor afectate de incidentul legat de TIC, precum și eventualul impact al incidentului legat de TIC asupra reputației;

96.2. durata incidentului legat de TIC, inclusiv perioada de indisponibilitate a serviciului;

96.3. întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC, în special în cazul în care acesta afectează și alte state;

96.4. pierderile de date pe care le implică incidentul legat de TIC, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor;

96.5. caracterul critic al serviciilor afectate, inclusiv al tranzacțiilor și operațiunilor entității financiare;

96.6. impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC, în termeni atât absoluți, cât și relativi.

Se consideră major, în orice caz, incidentul legat de TIC care a dus la indisponibilitatea totală a serviciilor TIC care sprijină funcții critice sau importante pentru o perioadă mai mare de 3 ore, dacă funcția nu a putut fi asigurată prin soluții alternative. Întreruperile repetate din aceeași cauză produse în 24 de ore se cumulează, iar indisponibilitatea planificată și anunțată în prealabil nu se ia în calcul în limitele intervalului anunțat.

97. Entitățile financiare clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.

Secțiunea a 3-a

Raportarea incidentelor majore legate de TIC și notificarea voluntară a amenințărilor cibernetice semnificative

98. Entitățile financiare raportează incidentele majore legate de TIC către BNM în conformitate cu pct. 103.

99. Notificarea inițială se efectuează pe baza informațiilor disponibile la momentul clasificării incidentului, iar rapoartele se elaborează după colectarea și analizarea tuturor informațiilor relevante și se transmit BNM. În cazul în care o imposibilitate tehnică împiedică transmiterea notificării inițiale prin PCSI, entitățile financiare informează BNM cu privire la aceasta prin mijloace alternative.

Notificarea inițială și rapoartele includ toate informațiile necesare BNM pentru a determina semnificația incidentului major legat de TIC și a evalua posibilele efecte.

100. Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative către BNM atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți. BNM poate furniza astfel de informații și altor autorități relevante.

101. În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia, fără întârzieri nejustificate, de îndată ce află despre incidentul major legat de TIC, cu privire la incidentul respectiv și la măsurile care au fost luate pentru a atenua efectele negative ale unui astfel de incident.

102. În cazul unei amenințări cibernetice semnificative, entitățile financiare își informează, după caz, clienții care ar putea fi afectați cu privire la eventualele măsuri de protecție adecvate pe care aceștia din urmă ar putea dori să le ia.

103. Entitățile financiare transmit BNM, prin intermediul PCSI, următoarele:

103.1. o notificare inițială fără întârziere după clasificarea incidentului ca incident major legat de TIC, dar nu mai târziu de sfârșitul zilei lucrătoare sau, în cazul unui incident clasificat ca major cu mai puțin de 2 ore înainte de încheierea zilei lucrătoare, nu mai târziu de 4 ore de la începutul următoarei zile lucrătoare. Clasificarea se efectuează fără întârziere, dar nu mai târziu de 24 de ore de la detectarea incidentului, cu excepția incidentului care întrunește criteriile prevăzute la pct. 96 ulterior acestui termen, care se clasifică de îndată ce criteriile sunt întrunite;

103.2. un raport intermediar, de îndată ce starea incidentului inițial s-a schimbat în mod semnificativ sau gestionarea incidentului major legat de TIC s-a schimbat pe baza noilor informații disponibile, dar nu mai târziu de 3 zile lucrătoare de la notificarea inițială menționată la subpct. 103.1, urmat, după caz, de notificări actualizate de fiecare dată când este disponibilă o actualizare relevantă a stării, precum și la cererea specifică a BNM;

103.3. un raport final, semnat de un membru al organului de conducere, atunci când analiza cauzelor principale a fost finalizată, indiferent dacă măsurile de atenuare au fost sau nu deja puse în aplicare, și atunci când cifrele efective ale impactului sunt disponibile pentru a înlocui estimările, dar nu mai târziu de 20 de zile lucrătoare de la data notificării inițiale.

În cazul în care activitatea normală a fost reluată înainte de expirarea termenului pentru notificarea inițială, notificarea inițială și raportul intermediar pot fi transmise împreună.

104. Entitățile financiare pot externaliza, în conformitate cu legislația națională, obligațiile de raportare prevăzute la pct. 98-103 către un furnizor terț de servicii. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de îndeplinirea cerințelor legate de raportarea incidentului.

105. La primirea notificării inițiale și a fiecărui raport menționat la pct. 103, BNM furnizează, în timp util și în condițiile legii, detalii privind incidentul major legat de TIC către Agenția pentru Securitate Cibernetică, în calitate de autoritate competentă potrivit Legii nr. 48/2023 privind securitatea cibernetică (în continuare – ASC).

Secțiunea a 4-a

Centralizarea raportării incidentelor majore legate de TIC

106. Raportarea incidentelor majore legate de TIC de către entitățile financiare se efectuează prin intermediul PCSI.

107. BNM, la primirea notificării inițiale și a fiecărui raport menționate la pct. 103, confirmă primirea și poate furniza entității financiare, acolo unde este posibil, în timp util, feedback relevant și proporțional sau îndrumări la nivel înalt, în special prin punerea la

dispoziție a oricăror informații și date operative relevante anonimizate cu privire la amenințări similare și poate discuta măsurile de remediere aplicate la nivelul entității financiare și modalități de reducere la minimum și de atenuare a impactului negativ la nivelul sectorului financiar. Fără a aduce atingere feedbackului privind supravegherea primit, entitățile financiare rămân pe deplin responsabile de gestionarea incidentelor legate de TIC raportate în temeiul pct. 98 și de consecințele acestora.

108. BNM elaborează rapoarte anuale, în mod anonim și agregat, cu privire la incidentele majore legate de TIC, menționând cel puțin numărul acestora, natura acestora și impactul lor asupra operațiunilor entităților financiare sau ale clienților, măsurile de remediere luate și costurile suportate.

109. BNM emite avertismente și elaborează statistici la nivel înalt pentru a sprijini evaluările privind amenințările și vulnerabilitățile din perspectiva TIC.

110. Cerințele prevăzute în prezentul capitol se aplică, de asemenea, incidentelor operaționale sau de securitate legate de plăți și incidentelor operaționale sau de securitate majore legate de plăți, atunci când acestea vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică.

Capitolul IV
TESTAREA REZILIENȚEI OPERAȚIONALE DIGITALE

Secțiunea 1

Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

111. În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare, altele decât microîntreprinderile, stabilesc, mențin și revizuiesc, ținând seama de criteriile principiului proporționalității, un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC.

112. Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu pct. 117-131.

113. Atunci când desfășoară programul de testare a rezilienței operaționale digitale menționat la pct. 111, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de criteriile principiului proporționalității și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.

114. Entitățile financiare, altele decât microîntreprinderile, se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe. Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.

115. Entitățile financiare, altele decât microîntreprinderile, stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile identificate pe parcursul desfășurării testelor și stabilesc metodologii de validare internă pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.

116. Entitățile financiare, altele decât microîntreprinderile, se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante.

Secțiunea a 2-a

Testarea instrumentelor și sistemelor TIC

117. Programul de testare a rezilienței operaționale digitale asigură, în conformitate cu criteriile principiului proporționalității, efectuarea de teste adecvate, precum evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă acolo unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end). Testele de penetrare se efectuează în mod obligatoriu, cel puțin o dată la 3 ani sau mai des, la solicitarea BNM, asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante, pe baza unor scenarii validate de entitatea financiară, de către experți care dețin cel puțin una dintre certificările prevăzute la subpct. 132.6, fără a aduce atingere testărilor avansate prin TLPT prevăzute la pct. 119. Entitățile financiare efectuează testări de securitate și în cazul modificărilor majore ale infrastructurii sau ale proceselor, după incidentele operaționale sau de securitate majore și la lansarea sistemelor informatice noi sau modificate substanțial, accesibile din internet.

118. Microîntreprinderile efectuează testele menționate la pct. 117 combinând o abordare bazată pe riscuri cu o planificare strategică a testării TIC și luând în considerare în mod corespunzător necesitatea de a menține o abordare echilibrată între amploarea resurselor și timpul care urmează să fie alocat testării TIC, pe de o parte, și urgența, tipul de risc, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor relevant, inclusiv capacitatea entității financiare de a-și asuma riscuri calculate, pe de altă parte.

Secțiunea a 3-a

Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT

119. Entitățile financiare, altele decât microîntreprinderile, identificate de BNM în conformitate cu pct. 130 efectuează, cel puțin o dată la 3 ani, testări avansate prin intermediul TLPT. Pe baza profilului de risc al entității financiare și ținând seama de circumstanțele operaționale, BNM poate să solicite entității financiare, dacă este necesar, să reducă sau să mărească această frecvență.

120. Fiecare test de penetrare bazat pe amenințări acoperă unele sau toate funcțiile critice sau importante ale unei entități financiare și este realizat pe sistemele de producție în timp real care sprijină astfel de funcții.

121. Entitățile financiare identifică toate sistemele, procesele și tehnologiile TIC subiacente relevante care sprijină funcțiile critice sau importante și serviciile TIC, inclusiv pe cele care sprijină funcțiile critice sau importante care au fost externalizate sau contractate unor furnizori terți de servicii TIC.

122. Entitățile financiare evaluează ce funcții critice sau importante trebuie să fie acoperite de TLPT. Rezultatul acestei evaluări determină sfera de aplicare exactă a TLPT și este validat de BNM.

123. În cazul în care furnizorii terți de servicii TIC sunt incluși în sfera de aplicare a TLPT, entitatea financiară ia măsurile și garanțiile necesare pentru a asigura participarea acestor furnizori terți de servicii TIC la TLPT și rămâne în orice moment pe deplin responsabilă de asigurarea respectării prezentului regulament.

124. Fără a aduce atingere sferei de aplicare TLPT, în cazul în care se preconizează în mod rezonabil că participarea unui furnizor terț de servicii TIC la TLPT, astfel cum se menționează la pct. 123, va avea un impact negativ asupra calității sau securității serviciilor oferite de către furnizorul terț de servicii TIC către clienți care sunt entități ce nu intră în domeniul de aplicare al prezentului regulament, sau asupra confidențialității datelor legate de astfel de servicii, entitatea financiară și furnizorul terț de servicii TIC pot conveni în scris ca furnizorul terț de servicii TIC să încheie în mod direct acorduri contractuale cu o entitate externă de testare în scopul desfășurării, sub conducerea unei entități financiare desemnate unice, a unei TLPT grupate, în care să fie implicate mai multe entități financiare (testare grupată) pentru care furnizorul terț de servicii TIC oferă servicii TIC. Testarea grupată respectivă acoperă gama relevantă de servicii TIC care sprijină funcțiile critice sau importante contractate de către entitățile financiare respectivului furnizor terț de servicii TIC. Testarea grupată este considerată TLPT efectuată de entitățile financiare care participă la testarea grupată.

Numărul entităților financiare care participă la testarea grupată este calibrat în mod corespunzător, ținând seama de complexitatea și de tipurile serviciilor implicate.

125. Entitățile financiare efectuează, cu cooperarea furnizorilor terți de servicii TIC și a altor părți implicate, inclusiv a entităților de testare, dar excluzând BNM, controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la nivelul entității financiare, al contrapărților acesteia sau al sectorului financiar.

126. La sfârșitul testării, după ce s-a convenit cu privire la rapoarte și la planurile de remediere, entitatea financiară și, după caz, entitățile externe de testare furnizează BNM un rezumat al constatărilor relevante, planurile de remediere și documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele.

127. BNM furnizează entităților financiare menționate la pct. 2 o adeverință prin care se confirmă faptul că testul a fost efectuat în conformitate cu cerințele evidențiate în documentație. Fără a aduce atingere unei astfel de adeverințe, entitățile financiare rămân în orice moment pe deplin responsabile pentru impactul testelor menționate la pct. 124.

128. Entitățile financiare contractează entități de testare în scopul efectuării TLPT în conformitate cu pct. 132-134. Atunci când entitățile financiare utilizează entități interne de testare în scopul efectuării TLPT, acestea contractează entități externe de testare la fiecare trei teste.

129. Instituțiile de credit identificate ca societăți de importanță sistemică în sensul Legii nr. 202/2017 privind activitatea băncilor utilizează numai entități externe de testare în conformitate cu pct. 132.

130. BNM identifică entitățile financiare care sunt obligate să efectueze TLPT ținând seama de criteriile principiului proporționalității, pe baza unei evaluări a următoarelor elemente:

130.1. factorii legați de impact, în special măsura în care serviciile furnizate și activitățile întreprinse de entitatea financiară au impact asupra sectorului financiar;

130.2. posibile preocupări legate de stabilitatea financiară, inclusiv caracterul sistemic al entității financiare la nivel național;

130.3. profilul de risc TIC specific, nivelul de maturitate a entității financiare din perspectiva TIC sau caracteristicile tehnologice implicate.

La identificare și la stabilirea frecvenței TLPT, BNM poate lua în considerare TLPT efectuat la nivelul grupului din care face parte entitatea financiară, dacă acesta acoperă

funcțiile critice sau importante ale entității financiare, iar documentația prevăzută la pct. 126 este pusă la dispoziția BNM.

BNM comunică entității financiare identificarea și termenul primului TLPT cu cel puțin 12 luni înainte de expirarea acestui termen.

131. BNM este responsabilă de aspectele legate de TLPT în sectorul financiar la nivel național pentru entitățile financiare menționate la pct. 2 și îi sunt încredințate toate competențele și sarcinile în acest sens.

Secțiunea a 4-a

Cerințe pentru entitățile de testare în ceea ce privește efectuarea TLPT

132. Entitățile financiare utilizează, în scopul efectuării TLPT, numai entități de testare care:

132.1. sunt cele mai adecvate și de cea mai înaltă reputație;

132.2. dețin capacități tehnice și organizatorice și demonstrează expertiză specifică în ceea ce privește datele operative privind amenințările, testele de penetrare și testarea de tipul „echipa roșie”;

132.3. sunt certificate sau aderă la coduri de conduită ori la cadre etice formale;

132.4. oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu efectuarea TLPT, inclusiv protecția corespunzătoare a informațiilor confidențiale ale entității financiare și măsurile reparatorii pentru riscurile legate de activitățile entității financiare;

132.5. sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență;

132.6. dispun de testeri care dețin cel puțin una dintre următoarele certificări: CEPT, CPT, CEH, OSCP, OPST, CPENT, GPEN, GWAPT, LPT, PTC sau alte certificări recunoscute la nivel internațional.

133. În cazul utilizării entităților interne de testare, entitățile financiare se asigură că, în plus față de cerințele de la pct. 132, se respectă toate condițiile următoare:

133.1. utilizarea a fost aprobată de BNM;

133.2. BNM a verificat că entitatea financiară are suficiente resurse alocate și s-a asigurat că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului;

133.3. furnizorul de date operative privind amenințările este extern entității financiare.

134. Entitățile financiare se asigură că contractele încheiate cu entități externe de testare impun o gestionare solidă a rezultatelor TLPT și că orice prelucrare de date de către acestea, inclusiv orice generare, stocare, agregare, elaborare, raportare, comunicare sau distrugere, nu creează riscuri pentru entitatea financiară.

Secțiunea a 5-a

Raportarea anuală către BNM

135. Entitățile financiare transmit către BNM, prin PCSI sau, în cazul indisponibilității acesteia, la adresa de e-mail SupraveghereTIC@bnm.md, în termen de o lună de la încheierea anului de gestiune, informații cu privire la următoarele:

135.1. rezultatele testelor de penetrare efectuate în anul de gestiune sau, dacă în acel an nu au fost efectuate, data ultimului test și data planificată a următorului;

135.2. rezultatele ultimelor scanări de vulnerabilități efectuate pentru sistemele și serviciile TIC critice, conform situației din luna decembrie;

135.3. 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;

135.4. raportul de evaluare a entității financiare în conformitate cu standardul PCI-DSS, în cazul în care aceasta este supusă unei astfel de evaluări anuale;

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

135.6. raportul privind gestionarea riscurilor TIC identificate ca fiind semnificative.

Capitolul V
GESTIONAREA RISCURILOR TIC GENERATE DE PĂRȚI TERȚE

Secțiunea 1

Principii-cheie pentru o gestionare solidă a riscurilor TIC generate de părți terțe

136. Entitățile financiare gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC și în conformitate cu următoarele principii:

136.1. entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor care decurg din prezentul regulament și din dreptul aplicabil în domeniul serviciilor financiare;

136.2. gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare:

a) natura, amploarea, complexitatea și importanța dependențelor legate de TIC;

b) riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.

137. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare, altele decât microîntreprinderile, adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori menționată la pct. 21, după caz. Această strategie privind riscurile TIC generate de părți terțe include o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Pe baza unei evaluări a profilului general de risc al entității financiare și a amplorii și complexității serviciilor comerciale, organul de conducere examinează periodic riscurile identificate în ceea ce privește acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante.

138. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC.

139. Acordurile contractuale menționate la pct. 138 sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă.

140. Entitățile financiare raportează cel puțin o dată pe an către BNM cu privire la numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de

servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile TIC care sunt oferite. Raportarea se efectuează prin PCSI, în termenul prevăzut la pct. 135.

141. Entitățile financiare pun la dispoziția BNM, la cererea acesteia, registrul complet de informații sau, după caz, secțiuni specifice din acesta, împreună cu orice informații considerate necesare pentru a permite supravegherea eficace a entității financiare.

142. Entitățile financiare informează BNM, prin PCSI, cu cel puțin 30 de zile înainte de încheierea oricărui acord contractual planificat privind utilizarea unor servicii TIC care sprijină funcții critice sau importante, precum și fără întârziere atunci când o funcție a devenit critică sau importantă. Informarea nu constituie o procedură de aprobare a acordului. Notificarea acordului efectuată potrivit actelor normative ale BNM privind externalizarea ține loc de informare, dacă indică faptul că serviciul TIC sprijină o funcție critică sau importantă.

143. Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare:

143.1. evaluează dacă acordul contractual vizează utilizarea unor servicii TIC care sprijină o funcție critică sau importantă;

143.2. evaluează dacă sunt îndeplinite condițiile pentru contractare din perspectiva supravegherii;

143.3. identifică și evaluează toate riscurile relevante legate de acordul contractual, inclusiv posibilitatea ca un astfel de acord contractual să contribuie la consolidarea riscului de concentrare a serviciilor TIC;

143.4. efectuează toate diligențele necesare cu privire la potențialii furnizori terți de servicii TIC și se asigură, pe parcursul proceselor de selecție și evaluare, că furnizorul terț de servicii TIC este adecvat;

143.5. identifică și evaluează conflictele de interese pe care acordul contractual le poate cauza.

144. Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.

145. În exercitarea drepturilor de acces, de inspecție și de audit cu privire la furnizorul terț de servicii TIC, entitățile financiare stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit.

Pentru exercitarea acestor drepturi, entitățile financiare pot utiliza, pe baza evaluării riscurilor, audituri comune organizate împreună cu alte entități financiare care utilizează serviciile aceluiași furnizor terț de servicii TIC, certificări emise de terți și rapoarte de audit puse la dispoziție de furnizor, dacă domeniul acestora acoperă sistemele și controalele relevante, sunt actuale și sunt întocmite cu respectarea standardelor profesionale recunoscute. Utilizarea acestor metode nu limitează drepturile prevăzute la subpct. 161.5 și nu înlocuiește, în timp, auditul propriu sau auditul comun.

146. În cazul în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată, entitatea financiară verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori,

dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.

147. Entitățile financiare se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe:

147.1. încălcarea semnificativă de către furnizorul terț de servicii TIC a actelor normative, a reglementărilor sau a clauzelor contractuale aplicabile;

147.2. circumstanțe identificate pe parcursul monitorizării riscurilor TIC generate de părți terțe care sunt considerate capabile să modifice îndeplinirea funcțiilor oferite prin acordul contractual, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC;

147.3. deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal;

147.4. în cazul în care BNM nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta.

148. Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire. Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate la pct. 147.

149. Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără:

149.1. perturbarea activităților lor comerciale;

149.2. limitarea respectării cerințelor în materie de reglementare;

149.3. afectarea continuității și calității serviciilor furnizate către clienți.

150. Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu criteriile stabilite la pct. 5, trebuie să fie testate în mod suficient și revizuite periodic.

151. Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lor către furnizori alternativi sau să le reintegreze în sistemul propriu.

152. Entitățile financiare instituie măsuri adecvate pentru situații neprevăzute astfel încât să păstreze continuitatea activității în cazul apariției situațiilor menționate la pct. 148.

Secțiunea a 2-a

Evaluarea preliminară a riscului de concentrare a serviciilor TIC

153. La identificarea și evaluarea riscurilor menționate la subpct. 143.3, entitățile financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații:

153.1. stabilirea unei relații contractuale cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau

153.2. instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați.

154. Entitățile financiare evaluează beneficiile și costurile soluțiilor alternative, cum ar fi utilizarea unor furnizori terți de servicii TIC diferiți, luând în considerare dacă și în ce mod soluțiile avute în vedere corespund nevoilor și obiectivelor operaționale stabilite în strategia lor privind reziliența operațională digitală.

155. În cazul în care acordurile contractuale privind utilizarea de servicii TIC care sprijină funcții critice sau importante includ posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare servicii TIC care sprijină o funcție critică sau importantă către alți furnizori terți de servicii TIC, entitățile financiare evaluează beneficiile și riscurile care pot apărea în legătură cu o astfel de subcontractare, în special în cazul unui subcontractant TIC stabilit într-un stat terț.

156. În cazul în care acordurile contractuale privesc servicii TIC care sprijină funcții critice sau importante, entitățile financiare iau în considerare în mod corespunzător dispozițiile din legislația privind insolvența care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC, precum și orice constrângere care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare.

157. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante sunt încheiate cu un furnizor terț de servicii TIC stabilit într-un stat terț, entitățile financiare iau în considerare, pe lângă aspectele menționate la pct. 156, conformitatea cu legislația privind protecția datelor cu caracter personal și asigurarea efectivă a respectării legii în statul terț respectiv.

158. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante prevăd subcontractarea, entitățile financiare evaluează dacă și în ce mod lanțurile de subcontractare potențial lungi sau complexe pot avea un impact asupra capacității lor de a monitoriza pe deplin funcțiile contractate și asupra capacității BNM de a supraveghea efectiv entitatea financiară din acest punct de vedere.

Secțiunea a 3-a

Dispoziții contractuale esențiale

159. Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris. Contractul complet include acordurile privind nivelul serviciilor și este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.

160. Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente:

160.1. o descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări;

160.2. locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC contractate sau subcontractate și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri;

160.3. dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal;

160.4. dispoziții privind asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară în caz de insolvență, de rezoluție sau de încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale;

160.5. descrieri la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora;

160.6. obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, atunci când survine un incident legat de TIC care este legat de serviciul TIC furnizat entității financiare;

160.7. obligația furnizorului terț de servicii TIC de a coopera pe deplin cu BNM și cu autoritățile de rezoluție ale entității financiare, inclusiv cu persoanele numite de acestea;

160.8. drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale, în conformitate cu așteptările BNM și ale autorităților de rezoluție;

160.9. condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale în conformitate cu pct. 87.

161. Acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante includ, în plus față de elementele menționate la pct. 160, cel puțin următoarele:

161.1. descrieri complete la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora, cu obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite monitorizarea eficace de către entitatea financiară a serviciilor TIC și adoptarea unor măsuri corective adecvate, fără întârzieri nejustificate, atunci când nu sunt asigurate nivelurile convenite ale serviciilor;

161.2. perioade de preaviz și obligații de raportare către entitatea financiară pentru furnizorul terț de servicii TIC, inclusiv notificarea oricărei evoluții care ar putea avea un impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC în sprijinul funcțiilor critice sau importante, în concordanță cu nivelurile convenite ale serviciului;

161.3. cerințe ca furnizorul terț de servicii TIC să pună în aplicare și să testeze planuri pentru situații neprevăzute și să dispună de măsuri, instrumente și politici în materie de securitate a TIC care să asigure un nivel adecvat de securitate în ceea ce privește furnizarea serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare;

161.4. obligația furnizorului terț de servicii TIC de a participa la TLPT ale entității financiare și de a coopera pe deplin în cadrul realizării acestora;

161.5. dreptul de a monitoriza, în permanență, performanța furnizorului terț de servicii TIC, care presupune următoarele:

a) drepturile nerestricționate de acces, de inspecție și de audit de către entitatea financiară sau o parte terță desemnată și de către BNM, precum și dreptul de a produce copii ale documentelor relevante la fața locului, dacă acestea sunt esențiale pentru operațiunile furnizorului terț de servicii TIC, drepturi a căror exercitare efectivă nu este împiedicată sau limitată de alte acorduri contractuale sau politici de punere în aplicare;

b) dreptul de a conveni asupra unor niveluri de asigurare alternative în cazul în care sunt afectate drepturile altor clienți;

c) obligația furnizorului terț de servicii TIC de a coopera pe deplin în timpul inspecțiilor și auditurilor la fața locului efectuate de BNM, de entitatea financiară sau de o parte terță desemnată; și

d) obligația de a transmite detalii privind domeniul de aplicare, procedurile care trebuie urmate și frecvența unor astfel de inspecții și audituri;

161.6. strategiile de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii:

a) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile TIC respective vizând să reducă riscul de perturbare în cadrul entității financiare sau să asigure rezoluția și restructurarea sa eficace;

b) care permite entității financiare să migreze către un alt furnizor terț de servicii TIC sau să treacă la soluții dezvoltate de aceasta pe plan intern, în conformitate cu complexitatea serviciului furnizat.

162. Prin derogare de la subpct. 161.5, furnizorul terț de servicii TIC și entitatea financiară care este o microîntreprindere pot conveni ca drepturile de acces, de inspecție și de audit ale entității financiare să poată fi delegate unui terț independent, numit de furnizorul terț de servicii TIC, și ca entitatea financiară să poată solicita în orice moment din partea terțului informații și asigurări cu privire la performanța furnizorului terț de servicii TIC.

163. La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard elaborate de autoritățile publice pentru servicii specifice.

Capitolul VI
ACORDURI PRIVIND SCHIMBUL DE INFORMAȚII

164. Entitățile financiare pot face schimb reciproc de informații și date operative privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative:

164.1. vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin creșterea gradului de conștientizare cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare;

164.2. au loc în cadrul unor comunități de încredere ale entităților financiare;

164.3. sunt puse în aplicare prin intermediul unor acorduri privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal și reglementările în domeniul concurenței.

165. În scopul aplicării subpct. 164.3, acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea BNM și calitatea în care aceasta poate fi asociată la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.

166. Entitățile financiare informează BNM cu privire la participarea lor la acordurile privind schimbul de informații menționate la pct. 164, în momentul validării sau, după caz, al încetării participării lor, odată ce aceasta începe să producă efecte.

Capitolul VII

EXERCIȚII, COMUNICARE ȘI COOPERARE TRANSSECTORIALE ÎN DOMENIUL FINANCIAR

167. BNM, în colaborare cu ASC, după caz, poate stabili mecanisme care să permită schimbul de practici eficace între subsectoarele financiare în vederea îmbunătățirii gradului de conștientizare a situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor.

BNM și ASC pot elabora exerciții de gestionare a crizelor și pentru situații neprevăzute care implică scenarii de atacuri cibernetice, cu scopul de a dezvolta canale de comunicare și de a permite treptat un răspuns coordonat eficace la nivel național în cazul unui incident transfrontalier major legat de TIC sau al unei amenințări conexe cu un impact sistemic asupra sectorului financiar. Exercițiile respective pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.

Capitolul VIII
SANCȚIUNI ADMINISTRATIVE ȘI MĂSURI DE REMEDIERE

168. Pentru încălcarea prevederilor prezentului regulament, BNM aplică măsurile de remediere și sancțiunile prevăzute de Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, Legea nr. 202/2017 privind activitatea băncilor, Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică și Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, după caz.

Capitolul IX
SECRETUL PROFESIONAL ȘI PROTECȚIA DATELOR

Secțiunea 1
Secretul profesional

169. Informațiile confidențiale primite, schimbate sau transmise în temeiul prezentului regulament fac obiectul condițiilor privind respectarea secretului profesional prevăzute de Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, Legea nr. 202/2017 privind activitatea băncilor, Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică și Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, după caz.

Secțiunea a 2-a
Protecția datelor

170. BNM este autorizată să prelucreze date cu caracter personal numai în cazul în care acest lucru este necesar în scopul îndeplinirii obligațiilor și sarcinilor care îi revin în temeiul prezentului regulament, în special în ceea ce privește investigarea, realizarea de inspecții, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, aprecierea și elaborarea de planuri de supraveghere. Datele cu caracter personal se prelucrează în conformitate cu legislația privind protecția datelor cu caracter personal.

171. Cu excepția cazului în care se prevede altfel în alte acte sectoriale, datele cu caracter personal menționate la pct. 170 se păstrează până la îndeplinirea atribuțiilor de supraveghere aplicabile și, în orice caz, pentru o perioadă maximă de 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită păstrarea acestor date pentru o perioadă mai lungă.