Proiect

BANCA NAȚIONALĂ A ROMÂNIEI

# REGULAMENT

Nr. _____din_____

pentru modificarea și completarea Regulamentului Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare

**2019**

Având în vedere prevederile art. 4 alin. (1), art. 24 alin. (1) și (2) , art. 101, art.104, art. 122, art. 148, art. 150 alin. (1) lit.b) și art.166 din *Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea nr. 227/2007*, cu modificările și completările ulterioare,

Recomandările Fondului Monetar Internațional și ale Băncii Mondiale, rezultate urmare evaluării respectării Principiilor Basel pentru o supraveghere bancară eficace, în cadrul programului de evaluare a sectorului financiar din România realizată în perioada 2017-2018,

în temeiul dispozițiilor art. 420 alin. (1) și alin. (3) și (4) din *Ordonanța de urgență a Guvernului nr. 99/2006, aprobată cu modificări și completări prin Legea nr. 227/2007*, cu modificările și completările ulterioare, ale art. 25 alin. (2) lit. a) și art. 48 din *Legea nr. 312/2004 privind Statutul Băncii Naționale a României*,

Banca Națională a României emite următorul regulament:

**Art. I. –** Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, publicat în Monitorul Oficial al României, Partea I, nr. 841 din 30.12.2013, cu modificările și completările ulterioare, se modifică și se completează după cum urmează:

1. **La articolul 3 alineatul (1), după punctul 4 se introduce un nou punct, punctul $4^1$, cu următorul cuprins:**

"**$4^1$. Tratarea riscurilor -** luarea măsurilor ce se impun pentru contracararea efectelor negative pe care materializarea respectivelor riscuri le poate induce și care poate afecta atingerea obiectivelor instituției de credit."

2. **La articolul 3 alineatul (1), punctul 19 se modifică și va avea următorul cuprins:**

"**19. Risc aferent tehnologiei informației și comunicațiilor** – subcategorie a riscului operațional care se referă la riscul existent sau potențial de afectare negativă a profiturilor și/sau capitalurilor instituțiilor de credit determinat de caracterul inadecvat al strategiei și politicilor TIC, de disfuncționalitățile manifestate la nivelul componentelor TIC, provocate de cauze interne sau externe, inclusiv utilizarea necorespunzătoare a TIC, ceea ce poate compromite disponibilitatea/accesibilitatea, integritatea, confidențialitatea și securitatea infrastructurii și a datelor;" [GL TIC – EBA/GL/2017/05, punctul 8, EBA/GL/2018/03 – *această definiție este*

*preferată celei din SREP propusă în proiectul de modificare a Reg. nr 5/2013 privind SREP, ICAAP ILAAP*)]

3. **La articolul 3 alineatul (1), după punctul 19 se introduc opt puncte noi, punctele $19^1$ – $19^8$, cu următorul cuprins:**

"**$19^1$. Sisteme TIC** - tehnologia informației și comunicațiilor (TIC) configurată în cadrul unui mecanism sau al unei rețele de interconectare care susține operațiunile unei instituții de credit; [GL TIC, punctul 8]

**$19^2$. Servicii asociate TIC** - serviciile furnizate de sisteme TIC unuia sau mai multor utilizatori interni sau externi. Printre exemple se numără serviciile de introducere a datelor, de stocare a datelor, de prelucrare și de raportare a datelor, însă și serviciile de monitorizare și de asistență comercială și decizională; [GL TIC, punctul 8]

**$19^3$. Funcția TIC** - funcția de administrare și valorificare a sistemelor și a serviciilor asociate TIC, care asigură și gestionarea riscurilor asociate activității proprii, inclusiv cele specifice TIC, contribuind astfel la realizarea funcției de administrare a riscurilor de la nivelul instituției de credit; [GL TIC, punctul 26, lit. a)]

**$19^4$. Risc de disponibilitate și continuitate TIC** - riscul ca performanța și disponibilitatea sistemelor și datelor TIC să fie afectate negativ, inclusiv imposibilitatea de a restabili la timp serviciile instituției de credit din cauza unei defecțiuni la componentele hardware sau software ale TIC; vulnerabilitățile de la nivelul gestionării sistemului TIC; sau orice alt eveniment, astfel cum se prezintă în Anexa nr. 5 la prezentul regulament; [GL TIC, punctul 8]

**$19^5$. Risc de securitate TIC** - riscul de acces neautorizat la sisteme și date TIC din interiorul sau din afara instituției de credit (de exemplu, atacuri cibernetice), astfel cum se prezintă în Anexa nr. 5 la prezentul regulament; [GL TIC, punctul 8]

**$19^6$. Risc de schimbare TIC** - riscul care apare ca urmare a incapacității instituției de credit de a gestiona cu promptitudine și în mod controlat schimbările asociate sistemului TIC, în special în cazul programelor de schimbare ample și complexe, astfel cum se prezintă în Anexa nr. 5 la prezentul regulament; [GL TIC, punctul 8]

**$19^7$. Riscul de integritate a datelor TIC** - riscul ca datele stocate și prelucrate prin sisteme TIC să fie incomplete, inexacte sau neconsecvente la nivelul diferitelor sisteme TIC, spre exemplu ca urmare a procedurilor de control TIC precare sau absente în diferitele faze ale ciclului de viață al datelor TIC (mai exact, proiectarea arhitecturii datelor, dezvoltarea modelului de date și/sau a dicționarelor de date, verificarea datelor introduse, controlarea și prelucrarea extragerilor,

transferurilor și prelucrării datelor, inclusiv a datelor generate), afectarea capacității unei instituții de credit de administrare, de a furniza servicii și de a prezenta informații financiare în mod corect și cu promptitudine, astfel cum se prezintă în Anexa nr. 5 la prezentul regulament; [GL TIC, punctul 8]

**19[8]. Risc de externalizare TIC** - riscul ca angajarea unei terțe părți sau a unei alte entități din cadrul grupului pentru a furniza sisteme TIC sau servicii conexe să afecteze negativ performanța și administrarea riscurilor în cadrul instituției de credit, astfel cum se prezintă în Anexa nr. 5 la prezentul regulament; [GL TIC, punctul 8]

**4. După articolul 15 se introduce un nou articol, articolul 15[1], cu următorul cuprins:**

„**Art. 15[1]**. – Toate instituțiile de credit trebuie să aibă membri independenți în componența organului de conducere în funcția sa de supraveghere, astfel: [recomandare FSAP CP14 EC 3]

a) în cazul instituțiilor de credit semnificative și al instituțiilor de credit listate, organul de conducere în funcția sa de supraveghere trebuie să fie format dintr-un număr suficient de membri independenți care să nu fie mai mic de 2/3 din numărul total al membrilor;

b) în cazul instituțiilor de credit, altele decât cele prevăzute la lit.a), organul de conducere în funcția sa de supraveghere trebuie să aibă cel puțin un membru independent."

**5. La articolul 15, după alineatul (8) se introduce un nou alineat, alineatul (9), cu următorul cuprins:**

"**(9)** Instituțiile de credit au obligația să notifice, în scris, Băncii Naționale a României, de îndată ce iau cunoștință, orice informație reală și importantă care ar putea afecta negativ adecvarea unui membru al organului de conducere." [recomandare FSAP CP14 AC 1]

**6. Articolul 44 se modifică și va avea următorul cuprins:**

" **Art. 44. - (1)** În sensul art. 39 lit.e), funcția de administrare a riscurilor trebuie să asigure că măsurarea și evaluarea internă a riscurilor unei instituții de credit acoperă o gamă corespunzătoare de scenarii și se bazează pe ipoteze suficient de conservatoare privind dependențele și corelațiile. Aceasta trebuie să includă o perspectivă calitativă la nivel de ansamblu al instituției de credit (inclusiv cu raționamentul experților) a relației dintre riscuri și profitabilitatea instituției de credit și a mediului extern de operare al acesteia. Funcția de administrare a riscurilor trebuie să informeze organul de conducere cu privire la ipotezele utilizate și la posibilele deficiențe ale modelelor de risc și ale analizei acestora. [modificare necesară pentru corelare cu alin.(2) și (3)]

**(2)** Organul de conducere al instituției de credit trebuie să înțeleagă: [recomandare FSAP CP15 EC 6, 8]

a) limitele și incertitudinile privind rezultatele modelelor pentru cuantificarea valorii riscurilor și riscului de model;

b) riscurile aferente produselor noi și inițiativelor majore de modificare (cum ar fi modificări ale sistemelor, proceselor, modelelor de afaceri și ale achizițiilor majore).

**(3)** Organul de conducere în funcția sa de supraveghere se asigură că incertitudinile aferente măsurării riscurilor sunt recunoscute. [recomandare FSAP CP15 EC 1]"

7. **După articolul 56 se introduce un nou articol, articolul 56[1], cu următorul cuprins:**

„**Art. 56[1]** - Instituțiile de credit se asigură că funcția de audit intern este informată în timp util cu privire la orice modificări semnificative aduse strategiei, politicilor sau proceselor privind administrarea riscurilor. [recomandare FSAP CP26 EC 5]"

8. **La Titlul II Capitolul I, se introduce o nouă secțiune, Secțiunea 5[1] care va avea următoarea denumire: "Secțiunea 5[1]. Identificarea, evaluarea și administrarea, riscurilor asociate TIC"**
9. **După articolul 64 se introduc 34 noi articole, articolele 64[1] – 64[34], cu următorul cuprins:**

„**Art.64[1] –** În administrarea riscurilor TIC, instituțiile de credit trebuie să clasifice riscurile TIC. În acest sens instituțiile de credit pot utiliza propriile clasificări, la realizarea cărora trebuie să aibă în vedere, dacă este cazul, cel puțin subcategoriile de risc TIC și scenariile de risc prezentate în Anexa nr. 5 la prezentul regulament, care evidențiază riscurile TIC care pot genera pierderi cu un grad ridicat de severitate. [GL TIC, punctul 18]

**Art.64[2] –** Instituțiile de credit trebuie să includă în mod corespunzător sistemele TIC și administrarea riscurilor aferente acestora, în cadrul de guvernanță și în cel aferent controlului intern, ținând cont de prevederile legislației în vigoare din acest domeniu , în măsura în care sunt aplicabile, având în vedere specificitatea sistemelor și riscurilor asociate TIC. [GL TIC, punctele 20 și 21]

**Art.64[3] –** Instituțiile de credit trebuie:

**a)** să stabilească o strategie TIC administrată în mod corespunzător și în conformitate cu strategia de afaceri a instituției de credit;

**b)** să se asigure că organizarea și structura organizatorică sunt adecvate în raport cu sistemele TIC

ale instituției de credit;

**c)** să implementeze un cadru aferent controlului intern și gestionării riscurilor TIC care protejează în mod corespunzător sistemele TIC ale instituției de credit, prin luarea în considerare a riscurilor TIC în cadrul de administrare a riscurilor de la nivelul instituției de credit. [GL TIC, punctul 22]

**Art.64[4] –** Pentru scopurile art. 64[3] lit. a), instituțiile de credit au în vedere prevederile de la art. 64[5].-64[7].

**Art.64[5] –** Organul de conducere al instituției de credit trebuie:

**a)** să stabilească și să aprobe strategia TIC, în concordanță cu strategia și modelul de afaceri al instituției de credit, precum și planurile de implementare și să monitorizeze implementarea acesteia;

**b)** să supravegheze și să asigure actualizarea sistemelor TIC și planificarea sau implementarea unor schimbări importante și complexe care să susțină modelul de afaceri al instituției de credit; [GL TIC, punctul 25]

**Art.64[6] –** Instituțiile de credit trebuie să stabilească un cadru adecvat pentru realizarea și dezvoltarea strategiei TIC, proporțional cu natura, amploarea și complexitatea activităților sale în aria TIC, luând în considerare cel puțin următoarele:

**a)** conducerea superioară responsabilă cu coordonarea liniilor de activitate trebuie să fie implicată în mod corespunzător în stabilirea priorităților TIC strategice ale instituției de credit și conducerea superioară responsabilă cu coordonarea funcției TIC trebuie să aibă cunoștință despre dezvoltarea, proiectarea și lansarea de strategii și inițiative economice majore pentru a asigura alinierea permanentă a sistemelor TIC, a serviciilor TIC și a funcției TIC, la strategia de afaceri a instituției de credit;

**b)** sistemele TIC trebuie actualizate în mod eficace;

**c)** strategia TIC este documentată și susținută de planuri de implementare concrete, în special în ceea ce privește reperele și planificările de resurse importante, inclusiv resurse financiare și umane, pentru a asigura faptul că acestea sunt realiste și permit punerea în practică a strategiei TIC;

**d)** instituția de credit actualizează periodic strategia sa TIC, în special atunci când schimbă strategia de afaceri, pentru a asigura alinierea permanentă dintre sistemele TIC și obiectivele, planurile și activitățile economice pe termen mediu și lung; [GL TIC, punctul 26]

**Art.64[7] – (1)** În cazul în care strategia TIC a instituției de credit impune implementarea unor schimbări importante și complexe ale sistemelor TIC, sau schimbări cu implicații semnificative pentru modelul de afaceri al instituției de credit, instituția de credit trebuie să stabilească un cadru de

control adecvat pentru dimensiunea sa, activitățile sale TIC și pentru nivelul de schimbare al activităților pentru a susține implementarea eficace a strategiei TIC.

**(2)** În sensul alin. (1), instituția de credit trebuie să se asigure că respectivul cadru de control:

**a)** include procese interne (de exemplu, monitorizarea și raportarea progreselor și a bugetului) și structuri relevante (de exemplu, un birou de gestionare a proiectelor (BGP), un grup coordonator TIC sau un grup echivalent) pentru a susține în mod eficace implementarea programelor strategice TIC;

**b)** definește și alocă rolurile și responsabilitățile pentru implementarea programelor strategice TIC, acordându-se o atenție deosebită experienței părților interesate cheie în organizarea, coordonarea și monitorizarea schimbărilor TIC importante și complexe și gestionării impacturilor mai ample la nivel organizațional și uman (de exemplu, gestionarea rezistenței la schimbare, formare, comunicare;

**c)** angajează funcțiile de control și de audit intern să se asigure că au fost identificate, evaluate și diminuate în mod eficace riscurile asociate implementării strategiei TIC și că acel cadru de guvernanță instituit pentru implementarea strategiei TIC este eficace; și

**d)** cuprinde un proces de planificare și de revizuire a planificării care oferă flexibilitate pentru a răspunde aspectelor importante identificate (de exemplu, probleme sau întârzieri ivite la nivelul implementării) sau evoluțiilor externe (de exemplu, schimbări importante produse în mediul economic, probleme tehnologice sau inovații), astfel încât să asigure o adaptare oportună a planului strategic de implementare. [GL TIC, punctul 27]

**Art.64[8] –** Pentru scopurile art. 64[3] lit. b), instituțiile de credit au în vedere prevederile de la art. 64[9]-64[10].

**Art.64[9] – (1)** Instituția de credit trebuie să dețină o structură organizatorică adecvată, robustă și transparentă, cu responsabilități clare privind sistemele TIC și administrarea riscurilor asociate TIC, care să includă organul de conducere, comitetele sale relevante, precum și persoanele cu responsabilități cheie pentru aria TIC (de exemplu, responsabilul pentru informații – CIO, directorul general operațiuni – COO sau un rol echivalent etc.).

**(2)** Instituția de credit trebuie să identifice și să se asigure că persoanele responsabile pentru TIC au acces direct sau indirect corespunzător la organul de conducere pentru a asigura raportarea, discutarea și deciderea la nivel corespunzător asupra informațiilor sau problemelor importante legate de TIC la nivelul organului de conducere, și că organul de conducere cunoaște și abordează riscurile asociate TIC. [GL TIC, punctul 28]

**Art.64[10] –** Instituția de credit trebuie să se asigure că politica și strategia de externalizare a TIC au în vedere, după caz, impactul externalizării TIC asupra activității și a modelului de afaceri al instituției de credit. [GL TIC, punctul 29]

**Art.64[11] –** Pentru scopurile art. 64[3] lit. c), instituțiile de credit au în vedere prevederile de la art. 64[12]-64[14].

**Art.64[12] – (1)** Cadrul aferent controlului intern și cadrul de administrare a riscurilor trebuie să trateze în mod corespunzător sistemele TIC ale instituției de credit, proporțional cu dimensiunea și activitățile acesteia, precum și cu profilul de risc TIC prevăzut la art. 64[18].

**(3)** Apetitul la risc și adecvarea capitalului intern trebuie să cuprindă riscurile TIC în categoria mai amplă a riscului operațional pentru definirea strategiei generale privind riscurile și stabilirea capitalului intern.

**(4)** Riscurile TIC trebuie tratate de cadrul privind administrarea riscurilor și în cadrul de control intern stabilite la nivelul instituției de credit. [GL TIC, punctul 30]

**Art.64[13] –** Atunci când stabilesc apetitul la risc și profilul de risc TIC, instituțiile de credit trebuie să țină cont atât de scenariul de bază preconizat, cât și scenariile aferente unor condiții de criză, incluse în simulările de criză specifice instituției de credit. [GL TIC, punctul 31]

**Art.64[14] –** În aplicarea art. 64[12] alin. (3), instituțiile de credit trebuie să asigure că funcțiile independente de control și de audit intern, astfel cum sunt prevăzute la art. 34[8] alin. (1), asigură un nivel suficient de independență între funcția TIC și funcțiile de control și de audit în situația în care aceste funcții se pot combina, proporțional cu dimensiunea și profilul de risc TIC al instituției de credit. [GL TIC, punctul 32]

**Art.64[15] –** Instituțiile de credit trebuie să identifice, evalueze, monitorizeze, administreze și să diminueze în mod corespunzător riscurile asociate TIC, în cadrul de administrare a riscului operațional. [GL TIC, punctul 35]

**Art.64[16] –** În vederea stabilirii profilului de risc TIC, instituțiile de credit trebuie să identifice mai întâi riscurile inerente semnificative aferente TIC la care sunt sau ar putea fi expuse, să le evalueze și să stabilească un cadru de administrare adecvat, proceduri și măsuri de control pentru diminuarea acestor riscuri. [GL TIC, punctul 36]

**Art.64[17] –** Instituțiile de credit trebuie să:

**a)** definească un cadru de raportare internă către organul de conducere, conducerea superioară și alte

structuri relevante privind riscurile TIC, care să detalieze, printre altele, riscurile TIC semnificative, expunerile, natura incidentelor și pierderile aferente (pierderile aferente riscurilor TIC vor fi raportate inclusiv în baza de date a pierderilor operaționale), măsurile întreprinse. Nivelul de adresabilitate, frecvența, conținutul raportării trebuie aprobate în mod formal de organul de conducere;

**b)** realizeze, prin intermediul funcției TIC, autoevaluări ale riscurilor TIC și ale procedurilor de control al riscurilor;

**c)** efectueze audituri interne și/sau externe privind riscurile TIC, iar rezultatele acestora trebuie raportate comitetului de audit. [GL TIC, punctul 37]

**Art.64[18] –** Atunci când își stabilește profilul de risc TIC, instituția de credit trebuie să evalueze următoarele aspecte:

**a)** eventualul impact al unei întreruperi semnificative a propriilor sisteme TIC asupra sistemului financiar național sau internațional;

**b)** nivelul expunerii la riscul de securitate TIC sau la riscurile de disponibilitate și continuitate TIC din cauza dependențelor de Internet, a adoptării la un nivel semnificativ a soluțiilor TIC inovatoare sau a altor canale de distribuție, ce ar putea să crească riscul ca instituția de credit să fie ținta atacurilor cibernetice;

**c)** nivelul expunerii la riscurile de securitate TIC, riscurile de disponibilitate și continuitate TIC, riscurile de integritate a datelor sau riscurile de schimbare TIC din cauza complexității (de exemplu, ca urmare a fuziunilor sau a achizițiilor) sau a depășirii morale a sistemelor sale TIC;

**d)** eventualul impact negativ asupra stabilității sau funcționării ordonate a sistemelor TIC și care pot genera riscuri TIC semnificative de disponibilitate și continuitate, de securitate, de schimbare sau de integritate a datelor, în cazul în care instituția de credit implementează schimbări semnificative aduse sistemelor TIC și/sau funcției TIC (de exemplu, ca urmare a fuziunilor, a achizițiilor, a cesionării sau a înlocuirii sistemelor sale TIC de bază);

**e)** posibilitatea apariției unor riscuri semnificative de externalizare TIC, în cazul în care instituția de credit a externalizat servicii sau sisteme TIC în cadrul sau în afara grupului;

**f)** creșterea potențială a expunerii la toate tipurile de risc TIC, în cazul în care instituția de credit implementează măsuri agresive de reducere a costurilor TIC, care ar putea determina reducerea investițiilor și resurselor TIC, precum și a expertizei IT necesare;

**g)** creșterea potențială semnificativă a riscurilor de disponibilitate și continuitate TIC și a riscurilor de securitate TIC ca urmare a localizării operațiunilor/centrelor de date TIC importante în regiuni sau țări care sunt susceptibile de a expune instituția de credit unor calamități naturale, instabilității politice sau conflictelor de muncă, perturbărilor civile etc.; [GL TIC, punctul 39]

**Art.64[19] – (1)** Instituțiile de credit trebuie să realizeze anual o analiză a sistemelor și a serviciilor TIC în vederea identificării celor care sunt critice pentru funcționarea, disponibilitatea, continuitatea și securitatea adecvată a activităților esențiale ale instituțiilor de credit. Această analiză trebuie să conțină inclusiv descrierea metodologiei și proceselor aplicate de instituția de credit pentru identificarea sistemelor și serviciilor TIC critice.

**(2)** Pentru a fi considerate critice, sistemele și serviciile TIC trebuie să îndeplinească cel puțin una dintre următoarele condiții:

**a)** susțin operațiunile economice de bază și canalele de distribuție ale instituției de credit (de exemplu, ATM-uri, Internet și mobile banking);

**b)** susțin procesele de guvernanță și liniile principale de afaceri, inclusiv administrarea riscurilor;

**c)** intră sub incidența cerințelor legale și de reglementare care impun cerințe mai stricte privind disponibilitatea, reziliența, confidențialitatea sau securitatea etc.;

**d)** prelucrează sau stochează date confidențiale sau sensibile a căror accesare neautorizată ar putea produce un impact semnificativ asupra reputației instituției de credit, a rezultatelor financiare sau a solidității și continuității activității sale (de exemplu, baze de date cu informații sensibile despre clienți); și/sau

**e)** asigură funcționalități de bază care sunt critice pentru funcționarea adecvată a instituției de credit (de exemplu, servicii de telecomunicații și de conectivitate, servicii de securitate TIC și cibernetică). Metodologia prevăzută la alin. (1) trebuie să precizeze aceste funcționalități.

**(3)** – Instituțiile de credit transmit anual BNR, în cadrul procesului intern de evaluare a adecvării capitalului la riscuri, analiza de la alin.(1). [GL TIC, punctul 41]

**Art.64[20] –** Instituțiile de credit trebuie să identifice riscurile TIC semnificative care pot avea un impact semnificativ asupra sistemelor și serviciilor TIC critice ale instituției de credit. [GL TIC, punctul 42]

**Art.64[21] –** Atunci când evaluează impactul riscurilor TIC asupra sistemelor și serviciilor TIC critice, instituțiile de credit trebuie să surprindă :

**a)** impactul financiar, inclusiv pierderea de fonduri sau active, eventuale obligații de acordare de compensări, cheltuieli de judecată și de remediere, daune contractuale, venituri pierdute;

**b)** eventualitatea întreruperii activității, având în vedere inclusiv importanța serviciilor financiare afectate; numărul de clienți și/sau sucursale și angajați care ar putea fi afectați;

**c)** un eventual impact asupra instituției de credit sub aspectul reputației în funcție de importanța serviciului bancar sau a activității operaționale afectate (de exemplu, furtul de date despre clienți); profilul/vizibilitatea sistemelor și serviciilor TIC afectate (de exemplu, sisteme bancare mobile sau online, puncte de vânzare, bancomate sau sisteme de plată);

**d)** impactul neconformării cu cadrul de reglementare;

**e)** impactul strategic asupra instituției de credit, spre exemplu dacă produsul strategic sau planurile economice sunt compromise sau furate. [GL TIC, punctul 43]

**Art.64[22] – (1)** Instituțiile de credit trebuie să clasifice riscurile TIC semnificative identificate, cel puțin în următoarele categorii de riscuri TIC, în cazul în care nu dispun de o metodologie de clasificare mai granulară și mai adecvată la profilul lor de risc TIC conform art. 64[1]:

**a)** Risc de disponibilitate și continuitate TIC;

**b)** Risc de securitate TIC;

**c)** Risc de schimbare TIC;

**d)** Riscul de integritate a datelor TIC;

**e)** Risc de externalizare TIC;

**(2)** În sensul alin. (1), instituțiile de credit trebuie să stabilească, documenteze și să justifice nivelul pragurilor de semnificație privind categoriile de riscuri TIC. [GL TIC, punctul 44]

**Art.64[23] –** Pentru identificarea, monitorizarea, evaluarea și diminuarea riscurilor TIC semnificative identificate, instituțiile de credit trebuie să dispună, proporțional cu natura, amploarea și complexitatea activităților desfășurate, de următoarele:

**a)** politici și procese de administrare a riscurilor TIC, precum și nivelul de toleranță la risc;

**b)** un cadru solid de administrare al activității;

**c)** o funcție eficace de audit intern, care să acopere guvernanța TIC, precum și sistemele și procesele instituției de credit;

**d)** proceduri de control a riscurilor TIC specifice riscului TIC semnificativ identificat. [GL TIC, punctul 45 și 46]

**Art.64[24] – (1)** În sensul art. 64[23] lit.a), politicile și procesele de administrare a riscurilor TIC și nivelurile de toleranță trebuie formalizate, sens în care pot fi incluse în cadrul de administrare a riscului operațional sau într-un document separat și trebuie să țină cont de următoarele:

**a)** politica de administrare a riscurilor trebuie aprobată de către organul de conducere și trebuie să cuprindă descrierea apetitului la riscul TIC al instituției de credit și a principalelor obiective de administrare a riscurilor TIC urmărite, precum și toleranța la riscul TIC;

**b)** politica relevantă de administrare a riscurilor TIC trebuie comunicată tuturor părților interesate relevante;

**c)** descrierea proceselor și procedurilor implementate pentru identificarea și monitorizarea riscurilor TIC semnificative (de exemplu, autoevaluarea riscurilor (RCSA), analize pe baza de scenarii de risc); și

**d)** descrierea sistemului de raportare pentru administrarea riscurilor TIC. Instituția de credit trebuie să implementeze un sistem de raportare pentru administrarea riscurilor TIC care să asigure furnizarea de informații prompte organelor cu funcție de conducere și structurii de conducere și care să permită acestor organe și/sau acestei structuri să evalueze și să monitorizeze dacă planurile și măsurile de diminuare a riscurilor TIC ale instituției de credit sunt în concordanță cu apetitul la risc și/sau nivelurile de toleranță aprobate, precum și să monitorizeze schimbările produse la nivelul riscurilor TIC semnificative. [GL TIC, punctul 49]

**Art.64[25] – (1)** Instituțiile de credit trebuie să definească în mod clar rolurile și responsabilitățile privind administrarea riscurilor TIC și să le încorporeze și integreze în cadrul intern pentru administrarea și supravegherea riscurilor TIC semnificative identificate.

**(2)** În sensul alin. (1), instituția de credit trebuie să asigure următoarele:

**a)** existența unor roluri și responsabilități clare pentru identificarea, evaluarea, monitorizarea, diminuarea, raportarea și supravegherea riscurilor TIC semnificative;

**b)** comunicarea în mod clar a responsabilităților și rolurilor privind riscurile TIC;

**c)** alocarea și integrarea responsabilităților și rolurilor în toate segmentele și procesele relevante ale instituției de credit, inclusiv rolurile și responsabilitățile privind colectarea și agregarea informațiilor

despre riscuri și raportarea acestora către organele cu funcție de conducere și/sau structura de conducere.

**d)** desfășurarea activităților de administrare a riscurilor TIC cu resurse umane și tehnice suficiente și corespunzătoare calitativ;

**e)** alocarea de fonduri bugetare suficiente și/sau alte resurse necesare pentru punerea în aplicare a planurilor de diminuare a riscurilor aplicabile;

**f)** organul de conducere desfășoară acțiuni de monitorizare cu privire la constatări importante ale funcțiilor de control independente referitoare la riscurile TIC, ținând cont de o posibilă delegare a unora dintre atribuții către un comitet, dacă acesta există; și

**g)** să înregistreze excepțiile de la procedurile și politicile TIC aplicabile și să se asigure că acestea fac obiectul unei analize documentate și a unei raportări din partea unei funcții de control independente, cu axarea pe riscurile aferente acestor excepții. [GL TIC, punctul 50]

**Art.64[26]** – Instituțiile de credit trebuie să asigure faptul că funcția de audit intern este eficace în ceea ce privește auditarea cadrului de control al riscurilor TIC, având în vedere următoarele aspecte :

**a)** cadrul de control al riscurilor TIC este auditat la calitatea, profunzimea și frecvența impusă și proporțional cu dimensiunea, activitățile și profilul de risc TIC al instituției de credit;

**b)** planul de audit include acțiuni de audit privind riscurile TIC semnificative identificate de către instituția de credit;

**c)** constatările importante ale auditului cu privire la TIC, inclusiv acțiunile convenite, sunt raportate organului de conducere;

**d)** constatările auditului cu privire la TIC, inclusiv acțiunile de remediere convenite, sunt urmărite și se analizează periodic rapoartele privind progresele înregistrate de către conducerea superioară și comitetul de audit. [GL TIC, punctul 51]

**Art.64[27]** – În cazul riscurilor TIC semnificative identificate cf. art. $64^{22}$, instituțiile de credit trebuie să stabilească proceduri de control specifice pentru abordarea acestor riscuri. [GL TIC, punctul 52]

**Art.64[28]** – În sensul art. $64^{22}$ lit.a), instituțiile de credit trebuie să stabilească un cadru adecvat pentru identificarea, înțelegerea, măsurarea, monitorizarea și diminuarea riscurilor de disponibilitate și continuitate TIC, care să cuprindă cel puțin următoarele elemente:

**a)** identificarea proceselor TIC critice și a sistemelor TIC de susținere relevante, care trebuie să facă parte din planurile de recuperare în caz de dezastru și de continuitate a afacerii, bazat pe:

(i) analiza cuprinzătoare a dependențelor dintre procesele critice ale afacerii și sistemele TIC care le susțin;

(ii) stabilirea obiectivelor de recuperare pentru sistemele TIC respective (determinate de liniile de business și/sau de cadrul de reglementare, în termeni de Recovery Time Objective - RTO, Recovery Point Objective - RPO etc.);

(iii) planificarea corespunzătoare a continuității afacerii în situații de criză/urgență pentru a asigura disponibilitatea, continuitatea și recuperarea sistemelor și serviciilor TIC critice și reducerea la minim a întreruperii operațiunilor instituției de credit, în limitele acceptabile.

**b)** politicile și standardele privind recuperarea în caz de dezastru și continuitatea activității, precum și procedurile de control operațional care includ:

(i) măsuri pentru a evita ca un singur scenariu, incident sau dezastru să aibă impact atât asupra sistemelor TIC de producție, cât și asupra celor destinate recuperării în caz de dezastru ;

(ii) proceduri de backup și de recuperare a sistemului TIC pentru aplicațiile informatice și datele critice, care să asigure stocarea copiilor de siguranță într-o locație diferită, sigură, aflată la o distanță suficient de mare, astfel încât un incident sau un dezastru să nu poată distruge sau corupe, aceste date critice din ambele locații;

(iii) soluții de monitorizare pentru detectarea promptă a incidentelor legate de disponibilitatea și continuitatea TIC;

(iv) un proces documentat de administrare și escaladare a incidentelor, care să ofere și îndrumări cu privire la diferitele roluri și responsabilități de administrare și escaladare a incidentelor, membrii comitetului (comitetelor) de criză și lanțul de comandă în caz de urgență;

(v) măsuri fizice pentru a proteja infrastructura TIC critică (de exemplu centrele de date) a instituției de credit de riscurile de mediu (de exemplu inundații, cutremure sau alte dezastre naturale) și a asigura un mediu de funcționare adecvat pentru sistemele TIC;

(vi) procese, roluri și responsabilități pentru a asigura faptul că sistemele și serviciile TIC externalizate sunt acoperite de soluții și planuri de recuperare și continuitate a activității adecvate;

(vii) soluții de planificare și monitorizare a performanței și capacității TIC pentru sistemele și serviciile TIC critice, cu cerințe stabilite privind disponibilitatea, pentru a depista cu promptitudine limitările importante la nivel de performanță și capacitate;

(viii) soluții pentru a proteja activitățile sau serviciile critice, cu acces la Internet (de exemplu serviciile tip e-banking), dacă este necesar și adecvat, împotriva blocării accesului și a altor atacuri cibernetice provenite prin Internet, care vizează împiedicarea sau perturbarea accesului la aceste activități și servicii.

**c)** testarea soluțiilor de disponibilitate și continuitate TIC în contextul unei serii de scenarii realiste, inclusiv atacuri cibernetice, teste privind eficiența sistemelor și echipamentelor de rezervă (failover) și teste de restaurare de pe copiile de siguranță în cazul aplicațiilor și al datelor critice care:

(i) sunt planificate, formalizate și documentate, iar rezultatele testelor sunt utilizate pentru a crește eficacitatea soluțiilor de disponibilitate și continuitate TIC;

(ii) includ atât părți interesate și funcții din cadrul organizației cu responsabilități în sistemul de administrare a liniilor de activitate, inclusiv continuitatea activității, cât și echipele de intervenție în caz de incidente sau criză, precum și părți interesate externe relevante;

(iii) organul de conducere este implicat în mod corespunzător (de exemplu, în cadrul echipelor de gestionare a crizelor) și este informat cu privire la rezultatele testelor. [GL TIC, punctul 54]

**Art.64[29] –** În sensul 64[22] lit.b), instituțiile de credit trebuie să stabilească un cadru adecvat pentru identificarea, înțelegerea, măsurarea, monitorizarea și diminuarea riscurilor de securitate TIC semnificative, care să cuprindă cel puțin următoarele elemente:

**a)** roluri și responsabilități definite clar cu privire la:

(i) persoana (persoanele) și/sau comitetele responsabile și/sau răspunzătoare pentru administrarea curentă a securității TIC și elaborarea de politici generale de securitate TIC, avându-se în vedere asigurarea independenței acestora;

(ii) proiectarea, implementarea, administrarea și monitorizarea controalelor privind securitatea TIC;

(iii) protecția sistemelor și serviciilor TIC critice (implementarea unui proces de evaluare a vulnerabilităților, gestionarea patch-urilor, protecția end point (de exemplu viruși de tip malware), instrumente de prevenirea și detectarea intruziunilor etc.);

(iv) clasificarea, gestionarea și monitorizarea incidentelor de securitate TIC externe sau interne; inclusiv intervenția în caz de incidente și relansarea și recuperarea sistemelor și serviciilor TIC;

(v) evaluările periodice și proactive ale amenințărilor de securitate, în vederea menținerii de controale adecvate cu privire la securitatea cibernetică.

**b)** o politică de securitate TIC care respectă standarde, bune practici și principii de securitate TIC recunoscute la nivel internațional (de exemplu, „principiul celui mai mic privilegiu", adică pentru gestionarea drepturilor de acces se va aplica limitarea accesului la nivelul minim care va permite funcționarea normală, și principiul „apărării în profunzime", adică proiectarea arhitecturii de securitate prin aplicarea unor mecanisme de securitate pe mai multe nivele, care cresc nivelul de securitate al sistemului în ansamblu);

**c)** un proces pentru i) identificarea sistemelor și serviciilor TIC și a cerințelor de securitate corespunzătoare, care să ia în considerare eventualele riscuri de fraudă și/sau posibile utilizări inadecvate și/sau abuzuri privind date confidențiale, ii) elaborarea unor principii documentate privind securitatea TIC, aplicabile și respectate pentru aceste sisteme, servicii și date TIC identificate, în concordanță cu toleranța la risc a instituției de credit și iii) monitorizarea implementării corecte a acestora;

**d)** un proces documentat de administrare și escaladare a incidentelor legate de securitate, care să ofere îndrumări cu privire la diferitele roluri și responsabilități de administrare și escaladare a incidentelor, membrii comitetului (comitetelor) de criză și lanțul de comandă în cazuri de urgență de securitate;

**e)** funcția de înregistrare în fișiere de jurnalizare (fișiere log) a acțiunilor/activității în sistemele TIC a utilizatorilor și a administratorilor de sistem pentru a permite monitorizarea eficace, detectarea și intervenția promptă în cazul unei activități anormale și/sau neautorizate, precum și desfășurarea de investigații cu privire la incidentele de securitate. Instituția de credit trebuie să instituie politici de jurnalizare în sistem prin care să se stabilească care sunt categoriile adecvate de fișiere de jurnalizare, precum și perioada de păstrare a acestora;

**f)** campanii sau inițiative de sensibilizare și informare pentru a informa toate nivelurile din cadrul instituției de credit cu privire la utilizarea sigură și protecția sistemelor TIC ale instituției de credit, precum și la principalele riscuri de securitate TIC (și alte riscuri) pe care trebuie să le cunoască acestea, în special cu privire la amenințările cibernetice existente și cele evolutive (de exemplu, viruși informatici, posibile abuzuri sau atacuri interne sau externe, atacuri cibernetice) și rolul acestora în reducerea breșelor de securitate;

**g)** măsuri de securitate fizice adecvate (de exemplu, CCTV, uși securizate, sistem de alarmare) pentru prevenirea accesului fizic neautorizat la sisteme TIC critice și sensibile (de exemplu, centrele de date);

**h)** măsuri pentru protejarea sistemelor TIC de atacurile de pe Internet (de exemplu, atacuri cibernetice) sau de pe alte rețele externe (de exemplu, legături de comunicații tradiționale sau legături cu parteneri de încredere). [GL TIC, punctul 55]

**Art.64[30] –** Pentru scopurile art. 64[29] lit. h), instituțiile de credit trebuie să dispună de următoarele:

**a)** un proces și soluții pentru menținerea unui inventar complet și actualizat al tuturor punctelor exterioare de conectare la rețea prin care terții ar putea să spargă sistemele TIC interne.

**b)** măsuri de securitate gestionate și monitorizate îndeaproape (de exemplu, sisteme de tip firewall, servere proxy, sisteme de retransmitere a mesajelor, sisteme de scanare antivirus și a conținutului) pentru a securiza traficul care intră și care iese din rețea și conexiunile la rețea din exterior prin care terții ar putea să pătrundă în sistemele TIC interne;

**c)** procese și soluții pentru securizarea site-urilor și aplicațiilor care pot fi atacate în mod direct de pe Internet și/sau din exterior și care pot constitui drept puncte de intrare în sistemele TIC interne;

**d)** teste periodice de penetrare a sistemelor TIC de securitate pentru a evalua eficacitatea măsurilor și proceselor de securitate TIC interne și cibernetice implementate. Aceste teste trebuie efectuate de către personal și/sau experți externi având expertiza necesară, iar rezultatele testelor documentate și concluziile raportate conducerii superioare. Instituția de credit trebuie să identifice în urma acestor teste, punctele care necesită îmbunătățiri suplimentare la nivelul procedurilor de control și al proceselor de securitate și/sau să obțină asigurarea cu privire la eficacitatea acestora. [GL TIC, punctul 55, lit h]

**Art.64[31] –** În sensul art. 64[22] lit.c), instituțiile de credit trebuie să stabilească un cadru adecvat pentru identificarea, înțelegerea, măsurarea și diminuarea riscului de schimbare TIC, care să cuprindă riscurile asociate dezvoltării, testării și aprobării schimbărilor/modificărilor produse la nivelul sistemelor TIC, inclusiv cele asociate dezvoltării sau schimbării/modificării software-ului, înainte ca acestea să fie transmise către utilizare în cadrul instituției de credit și să asigure o administrare adecvată a ciclului de viață TIC. Acest cadru trebuie să prevadă cel puțin următoarele :

**a)** procese documentate pentru administrarea și controlarea schimbărilor aduse sistemelor (de exemplu, configurare și gestionarea patch-ului) și datelor TIC (de exemplu, rezolvarea erorilor de tip

bug sau corecțiile de date), asigurarea implicării adecvate a gestionării riscurilor TIC în cazul schimbărilor TIC importante care ar putea avea un impact semnificativ asupra profilului de risc și a expunerii instituției de credit;

**b)** specificații privind separarea necesară a sarcinilor în diferitele etape ale proceselor de schimbare TIC implementate (de exemplu, proiectarea și dezvoltarea de soluții, testarea și aprobarea de software nou și/sau schimbări, migrarea și implementarea în mediul de producție și rezolvarea erorilor de tip bug), cu axare pe soluțiile implementate și separarea sarcinilor pentru administrarea și controlarea schimbărilor aduse sistemelor de producție și datelor TIC de către personalul TIC (de exemplu, dezvoltatori, administratori de sistem TIC, administratori de baze de date) sau orice altă parte (de exemplu, utilizatori economici, furnizori de date);

**c)** medii de testare care reflectă în mod corespunzător mediul de producție;

**d)** un inventar al activelor care folosesc aplicațiile și sistemele TIC existente, din mediul de desfășurare a activității, precum și din mediul de testare și dezvoltare, pentru ca schimbările necesare (de exemplu, actualizări sau îmbunătățiri ale versiunilor, aplicarea de coduri patch în sisteme, schimbări de configurații) să fie gestionate, implementate și monitorizate în mod corespunzător în cazul sistemelor TIC în cauză;

**e)** un proces pentru monitorizarea și administrarea ciclului de viață al sistemelor TIC utilizate pentru a asigura faptul că acestea respectă și susțin în continuare cerințele efective de administrare a activității și a riscurilor asociate și pentru a obține certitudinea că soluțiile și sistemele TIC utilizate sunt susținute în continuare de către furnizorii acestora; și că acesta este însoțit de proceduri adecvate pentru ciclul de viață al procesului de dezvoltare a software-ului;

**f)** un sistem de verificare a codului sursă al software-ului și proceduri adecvate de prevenire a schimbărilor neautorizate asupra codului sursă al software-ului elaborat la nivel intern;

**g)** un proces pentru realizarea unei verificări de securitate și vulnerabilitate asupra sistemelor TIC și programelor software noi sau modificate semnificativ înainte de a le lansa în mediul de desfășurare a activității și a le expune unor posibile atacuri cibernetice;

**h)** un proces și soluții pentru prevenirea divulgării neautorizate sau neintenționate a datelor confidențiale odată cu înlocuirea, arhivarea, eliminarea sau distrugerea sistemelor TIC;

**i)** un proces independent de analiză și validare pentru reducerea riscurilor de eroare umană atunci când se aduc schimbări la nivelul sistemelor TIC, care ar putea avea un efect negativ important

asupra disponibilității, continuității sau securității instituției de credit (de exemplu, schimbări importante aduse configurației firewall), sau la nivelul securității instituției de credit (de exemplu, schimbări aduse aplicațiilor de tip firewall). [GL TIC, punctul 56]

**Art.64[32] – (1)** În sensul art. 64[22] lit.d), instituțiile de credit trebuie să stabilească un cadru adecvat pentru identificarea, înțelegerea, măsurarea și diminuarea riscului de integritate a datelor TIC, proporțional cu natura, amploarea și complexitatea activităților, precum și cu profilul de risc TIC al instituției de credit.

**(2)** Cadrul instituției de credit trebuie să aibă în vedere riscurile asociate păstrării integrității datelor stocate și prelucrate prin sistemele TIC și trebuie să prevadă cel puțin următoarele :

**a)** o politică ce definește rolurile și responsabilitățile de gestionare a integrității datelor din sistemele TIC (de exemplu, roluri/responsabilități cu privire la arhitectura datelor („data arhitect"), la procesarea și utilizarea datelor ("data officer"), la custodia, depozitarea și transportul datelor („data custodian"), la proprietatea datelor („data owner"), la gestionarea și caracterul potrivit al elementelor datelor, atât din punct de vedere al conținutului, cât și al metadatelor („data steward") etc.) și care oferă îndrumări cu privire la datele care sunt critice din perspectiva integrității datelor și care trebuie supuse unor proceduri de control TIC specifice (de exemplu, proceduri automatizate de control pentru validarea datelor introduse, proceduri de control al transferului de date, reconcilieri etc.) sau analize (de exemplu, o verificare a compatibilității cu arhitectura datelor) în diferitele faze ale ciclului de viață al datelor TIC;

**b)** o arhitectură documentată a datelor, un model și/sau dicționar de date, care se validează de către responsabilii IT desemnați, pentru a susține consecvența necesară a datelor între sistemele TIC și pentru a asigura faptul că arhitectura datelor, modelul și/sau dicționarul de date rămân în concordanță cu cerințele economice și de administrare a riscurilor;

**c)** o politică privind permisiunea utilizării și siguranța în utilizare a aplicațiilor informatice dezvoltate de utilizatori finali (End-User Computing - EUC), în special în ceea ce privește identificarea, înregistrarea și documentarea acestor soluții informatice și nivelurile de securitate necesare pentru a preveni modificări neautorizate, atât la nivelul soluției în sine, cât și la nivelul datelor aferente stocate;

**d)** procese documentate de abordare a excepțiilor pentru rezolvarea problemelor de integritate a datelor TIC identificate în funcție de importanța și sensibilitatea acestora [GL TIC, punctul 57]

**Art.64[33] –** Instituțiile de credit trebuie să efectueze și să formalizeze o analiză a riscurilor TIC asupra capacităților sale de raportare a riscurilor și de agregare a datelor, prevăzute la art. 67[7]. [GL TIC, punctul 58]

**Art.64[34] – (1)** Pentru scopurile art. 64[22] lit.e)**,** instituțiile de credit trebuie să stabilească o strategie privind riscurile semnificative determinate de externalizarea TIC în conformitate cu cerințele Titlului II, Capitolul V, aplicabilă în mod corespunzător în cazul externalizării TIC, inclusiv în cazul externalizării intra-grup care furnizează servicii TIC în cadrul grupului. [GL TIC, punctul 59]

**(2)** În sensul alin. (1), instituțiile de credit trebuie să stabilească un cadru adecvat pentru identificarea, înțelegerea, măsurarea și diminuarea riscului determinat de externalizare TIC și, în mod specific, proceduri de control și un mediu de control pentru diminuarea riscurilor asociate serviciilor TIC semnificative externalizate, care să fie proporționale cu dimensiunea, activitățile și profilul de risc TIC al instituției de credit și care includ cel puțin:

**a)** o evaluare a impactului externalizării TIC asupra gestionării riscurilor de către instituția de credit în legătură cu utilizarea furnizorilor de servicii (de exemplu, furnizori de servicii de tip cloud) și a serviciilor acestora în cadrul procesului de achiziții care este documentat și luat în considerare de către conducerea superioară sau de către organul de conducere pentru decizia de a externaliza serviciile sau nu. Instituția de credit trebuie să analizeze politicile de administrare a riscurilor TIC, precum și procedurile de control și mediul de control TIC ale furnizorului de servicii, pentru a verifica dacă acesta îndeplinește obiectivele de administrare internă a riscurilor și apetitul la risc la nivelul instituției de credit. Această analiză trebuie actualizată periodic în perioada de externalizare contractuală, ținând cont de caracteristicile serviciilor externalizate;

**b)** o monitorizare a riscurilor TIC asociate serviciilor externalizate în perioada de externalizare contractuală în cadrul acțiunii de administrare a riscurilor instituției de credit, care stă la baza raportării privind administrarea riscului TIC a instituției de credit (de exemplu, raportarea privind continuitatea activității, raportarea privind securitatea);

**c)** o monitorizare și o comparație a nivelurilor serviciilor primite cu nivelurile serviciilor convenite prin contract, care trebuie să constituie parte integrantă din contractul de externalizare sau acordul privind nivelul serviciilor (Service Level Agreement - SLA); și

**d)** personal, resurse și competențe adecvate pentru monitorizarea și administrarea riscurilor TIC generate de serviciile externalizate.” [GL TIC, punctul 60]

**10. La articolul 98, alineatul (2) se modifică și va avea următorul cuprins:**

„**(2)** În sensul alin. (1), expunerile (incluzând expunerile intragrup, unde este cazul) sunt identificate, monitorizate și administrate la nivel de regiune și individual pentru fiecare țară – în plus față de monitorizarea pe debitorul final/contrapartida finală.”

**11. După articolul 101 se introduc două noi articole, articolul 101[1] și articolul 101[2], cu următorul cuprins:**

„**Art.101[1] –** Politicile menționate la art.98 alin.(1) trebuie să cuprindă cel puțin: [recomandare FSAP, Basel Core Principle 21 – CP21]

a) țările și/sau regiunile față de care înregistrarea de expuneri este considerată acceptabilă din punctul de vedere al riscului asumat;

b) un sistem de clasificare a gradului de risc aferent țărilor și/sau regiunilor față de care se vor înregistra expuneri și a riscului de transfer și acordarea unui rating corespunzător, care să presupună cel puțin metodele de măsurare și evaluare a riscului de țară prin componentele de risc economic și risc politic, precum și a riscului de transfer; [recomandare FSAP CP21]

c) tipurile de entități din cadrul țărilor și/sau regiunilor față de care înregistrarea de expuneri este considerată acceptabilă din punctul de vedere al riscului asumat;

d) tipurile de operațiuni și scadențele inițiale maxime considerate acceptabile din punctul de vedere al riscului asumat pentru fiecare țară și/sau regiune și al riscului de transfer;

e) limitele expunerilor față de entități individuale din cadrul fiecărei țări și/sau regiuni, precum și limitele expunerilor agregate la nivelul fiecărei țări și/sau regiuni, în scopul diversificării expunerilor;

f) caracteristicile garanțiilor aferente expunerilor având scopul de a reduce riscul de nerambursare, cuprinzând cel puțin: tipurile de garanții, nivelul minim al garanției raportat la valoarea inițială a expunerii, perioada de valabilitate a garanției corelată cu scadența expunerii;

g) modalitățile de recuperare a creanțelor și de executare a garanțiilor în caz de nerambursare, precum și frecvența de evaluare a cadrului legal aferent țării și/sau regiunii față de care se înregistrează expunerea, inclusiv din perspectiva cadrului legal aplicabil garanțiilor, în scopul asigurării că garanțiile constituite produc efecte juridice, au fost îndeplinite formalitățile de perfectare și/sau opozabilitate față de terți cu privire la aceste garanții și acestea pot fi puse în executare;

h) planuri pentru situații neprevăzute, care să se refere inclusiv la situațiile în care este necesară diversificarea expunerilor, sau în care debitorul se schimbă ca urmare a proceselor de transformare care pot include, fără a se limita, procese de divizare și fuziune,

i) strategia de lichidare a expunerilor în situații de criză sau în situații în care debitorul se schimbă ca urmare a proceselor de transformare care pot include, fără a se limita, procese de divizare și fuziune;

j) mecanismul de identificare a expunerilor din perspectiva cuantificării riscului de țară și riscului de transfer, inclusiv în situații în care: (i) ultimul deținător al debitorului este dificil de identificat datorită structurii netransparente a acționariatului, (ii) structura acționariatului debitorului suportă modificări sau (iii) debitorul se schimbă ca urmare a proceselor de transformare care pot include, fără a se limita, procese de divizare și fuziune; [recomandare FSAP CP21]

k) mecanismul de control și de supraveghere al riscului de țară și riscului de transfer, prin stabilirea nivelului de aprobare a expunerilor, precum și a frecvenței de revizuire a acestui nivel și a limitelor de expunere de către organul de conducere al instituției de credit.

**Art.101[2] – (1)** Instituțiile de credit trebuie să deruleze periodic, dar cel puțin anual, simulări de criză care să ia în considerare scenarii nefavorabile cu privire la impactul riscului de țară și riscul de transfer, în scopul administrării riscului de credit. [recomandare FSAP CP21]

**(2)** Rezultatele simulării de criză efectuate conform alin.(1) trebuie aduse la cunoștința organului de conducere al instituției de credit și trebuie avute în vedere la elaborarea/revizuirea politicilor și proceselor menționate la art.98 alin.(1). [recomandare FSAP CP21]”

**12. La articolul 102 alineatul (3), literele a) și b) se modifică și vor avea următorul cuprins:**

„a) orice entitate asupra căreia instituția de credit exercită controlul, inclusiv vehicule investiționale cu scop special („*special purpose vehicles*”);

b) orice entitate în care instituția de credit deține participații, inclusiv vehicule investiționale cu scop special („*special purpose vehicles*”); [recomandare FSAP CP20]”

**13. La articolul 102 alineatul (3), după litera f) se introduce o nouă literă, litera f[1]), cu următorul cuprins:**

„f[1]) orice entitate care deține participații la capitalul entităților menționate la lit.a) – f); [recomandare FSAP CP20]”

**14. La articolul 102 alineatul (3), după litera g) se introduce o nouă literă, litera h), cu următorul cuprins:**

„h) membrii organului de conducere și persoanele care dețin funcții cheie în entitățile de la lit.a) – f'), împreună cu entitățile și persoanele aferente prevăzute la lit.g) pct.(i) și (ii). [recomandare FSAP CP20]

**15. La articolul 102, după alineatul (4), se introduce un nou alineat, alineatul (5), cu următorul cuprins:**

„**(5)** În aplicarea alin.(3), Banca Națională a României poate stabili că o anumită persoană și/sau entitate reprezintă parte afiliată instituției de credit. [recomandare FSAP – CP20 Ess.1]"

**16. La articolul 105, alineatul (1) se modifică și va avea următorul cuprins:**

„**Art. 105 – (1)** Orice operațiune care conduce la înregistrarea, scoaterea în afara bilanțului sau modificarea unei expuneri față de o parte afiliată, care depășește un prag prevăzut de normele interne ale instituției de credit, precum și orice operațiune de acest tip care prezintă în alt fel un risc deosebit vor fi efectuate numai cu aprobarea prealabilă a organului de conducere al instituției de credit. [CP 20 Ess.3] [recomandare FSAP]"

**17. La articolul 105, după alineatul (2), se introduce un nou alineat, alineatul (3), cu următorul cuprins:**

„**(3)** În scopurile alin.(2), excluderea unui membru al organului de conducere din procesul de aprobare și administrare a tranzacțiilor cu părțile afiliate presupune cel puțin: [recomandare FSAP CP20]

a) aducerea, de către respectivul membru, la cunoștința celorlalți membri ai organului de conducere a existenței conflictului de interese și completarea unei declarații pe propria răspundere cu detalii privind natura conflictului; }"

b) abținerea de la participarea la reuniunile cu scop de prezentare, analiză și luare a deciziei privind tranzacțiile cu părțile afiliate;

c) organizarea reuniunilor în care prezența membrului organului de conducere este solicitată de către ceilalți membri ai organului de conducere în scopul furnizării de informații cu privire la natura conflictului de interese, în altă zi decât cea în care au loc reuniunile cu scop de prezentare, analiză și luare a deciziei privind tranzacțiile cu părțile afiliate;

d) abținerea de a fi prezent în vecinătatea locului desfășurării reuniunilor menționate la lit.b);

e) evidențierea în dreptul locului destinat semnăturii, în cadrul documentelor de decizie, a sintagmei „conflict de interese”;

f) abținerea de la contactarea personalului implicat în procesul de aprobare și administrare a tranzacțiilor cu părțile afiliate, în legătură cu respectivele tranzacții.

**18. După articolul 111 se introduce un nou articol, articolul 111[1], cu următorul cuprins:**

„**Art.111[1]** - În cadrul politicilor și procedurilor menționate la art.111, instituțiile de credit trebuie să stabilească praguri aferente nivelurilor acceptabile ale riscului de concentrare pentru a reflecta apetitul la risc, profilul de risc și nivelul de capital ale instituțiilor de credit, care să fie comunicate periodic către și însușite de către personalul relevant. Respectivele politici și proceduri trebuie să prevadă că toate concentrările semnificative sunt revizuite periodic și raportate organului de conducere.” [recomandare FSAP CP19 Essential. criterion 3]

**19. Articolul 157 se modifică și va avea următorul cuprins:**

„**Art. 157 – (1)** Instituțiile de credit trebuie să informeze Banca Națională a României – Direcția supraveghere periodic, dar cel puțin anual, precum și imediat ce apar evoluții ce pot avea un impact semnificativ asupra riscului operațional la care acestea sunt expuse. [recomandare FSAP CP25]”

**(2)** Instituțiile de credit trebuie să furnizeze Băncii Naționale a României – Direcția supraveghere, bianual, informații privind acțiunile întreprinse ca urmare a apariției evenimentelor de risc operațional, eventualele deficiențe identificate în cadrul de control intern care au dus la apariția respectivelor evenimente, departamentele implicate din cadrul băncii, precum și măsurile întreprinse în vederea prevenirii apariției viitoare a unor astfel de deficiențe. [recomandare FSAP CP25]”

**20. La articolul 131, alineatele (2) și (3) se modifică și vor avea următorul cuprins:**

„**(2)** Pentru scopurile alin.(1), instituțiile de credit trebuie să dispună de capacitatea necesară pentru a calcula modificările potențiale ale valorii lor economice și a câștigurilor, ca urmare a schimbării nivelurilor ratelor dobânzii, precum și nivelul general al riscului de rată a dobânzii din afara portofoliului de tranzacționare la nivel individual, subconsolidat și consolidat

**(3)** Instituțiile de credit trebuie să elaboreze și să utilizeze propriile metodologii de calcul ale modificărilor potențiale ale valorii lor economice și a câștigurilor, ca urmare a schimbării nivelurilor ratelor dobânzii, în conformitate cu profilul de risc și politicile de administrare a riscului aferente acestora.” [recomandare FSAP CP23; EBA Guidelines on management of interest rate risk arising

from non-trading activities (EBA/GL/2018/02)]

**21. Articolul 132 se modifică și va avea următorul cuprins:**

**„Art. 132 – (1)** Instituțiile de credit calculează și raportează Băncii Naționale a României – Direcția supraveghere modificarea valorii lor economice ca urmare a aplicării unor schimbări bruște și neașteptate a ratelor dobânzii de +/- 200 de puncte de bază, în ambele direcții, indiferent de monedă. Calcularea modificării valorii economice se efectuează cel puțin trimestrial, iar raportarea se efectuează trimestrial pe bază individuală și semestrial pe bază subconsolidată și consolidată în conformitate cu actele normative emise de Banca Națională a României în aplicarea acestui articol."

**(2)** Instituțiile de credit calculează și raportează Băncii Naționale a României – Direcția supraveghere modificarea valorii lor economice ca urmare a aplicării unor schimbări bruște și neașteptate a ratelor dobânzii conform a șase scenarii de șoc standardizate pentru detectarea valorilor extreme, respectiv un șoc paralel în sus, un șoc paralel în jos, un șoc cu variație bruscă (rate scurte în jos și rate lungi în sus), un șoc cu evoluție constantă (rate scurte în sus și rate lungi în jos), un șoc cu rate scurte în sus, un șoc cu rate scurte în jos. Calcularea modificării valorii economice se efectuează cel puțin trimestrial. Dacă în cel puțin unul din cele 6 scenarii, scăderea valorii economice rezultate în urma calculării este mai mare decât 15% din fondurile proprii de nivel 1, instituia de credit trebuie să informeze imediat Banca Națională a României. În orice alte situații, instituțiile de credit includ rezultatul calculelor în cadrul raportului anual referitor la procesul intern de evaluare a adecvării capitalului la riscuri prevăzut la art. 674.

**(3)** Pentru scopurile alin. (1), instituțiile de credit trebuie să aplice fie metodologia standardizată în conformitate cu Anexa nr.1, fie o metodologie internă.

**(4)** În cazurile în care metodologia aplicată de o instituție de credit în baza alin (3) este considerată, de către Banca Națională a României – Direcția supraveghere, inadecvată din perspectiva profilului de risc al instituției de credit, Banca Națională a României poate solicita instituției de credit, dar fără a se limita la aceasta, modificarea metodologiei.

**(5)** Instituțiile de credit trebuie să asigure că metodologiile interne utilizate pentru administrarea riscului de rată a dobânzii din activități în afara portofoliului de tranzacționare este validat de către o funcție independentă de unitățile de lucru care prezintă relevanță din perspectiva asumării de riscuri.

**(6)** - Pentru scopurile art. 166 alin. (5), în cazul în care valoarea economică a unei instituții de credit scade cu mai mult de 20% din fondurile proprii ca urmare a aplicării șocului prevăzut la alin.(1), instituția de credit va discuta cu Banca Națională a României - Direcția supraveghere măsurile

necesare pentru diminuarea unui astfel de declin potențial, măsuri care pot include, printre altele, următoarele:

a) îmbunătățirea activității de administrare a riscului;

b) modificarea limitelor interne;

c) reducerea profilului de risc;

d) creșterea cerinței de capital reglementat.” [recomandare FSAP CP23; EBA Guidelines on management of interest rate risk arising from non-trading activities (EBA/GL/2018/02)].

**Art. II. -** Prezentul regulament se publică în Monitorul Oficial al României, Partea I.

Președintele Consiliului de Administrație al

Băncii Naționale a României

MUGUR CONSTANTIN ISĂRESCU