MONITORUL OFICIAL AL ROMÂNIEI

Anul 189 (XXXIII) — Nr. 599

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Miercuri, 16 iunie 2021

SUMAR

ACTE ALE BĂNCII NAȚIONALE A ROMÂNIEI

BANCA NAȚIONALĂ A ROMÂNIEI

REGULAMENT
pentru modificarea Regulamentului Băncii Naționale a României nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate și cerințele de raportare aferente serviciilor de plată

Având în vedere:

— prevederile art. 218, 219, 223 și art. 244 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

— Ghidul EBA/GL/2019/04 privind administrarea riscurilor TIC și de securitate;

— Ghidul EBA/GL/2018/05 referitor la cerințele de raportare a datelor privind fraudele din articolul 96 alineatul (6) din Directiva privind serviciile de plată (PSD2),

în temeiul dispozițiilor art. 243 alin. (1) și ale art. 244 alin. (1) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, precum și ale art. 48 din Legea nr. 312/2004 privind Statutul Băncii Naționale a României,

Banca Națională a României emite prezentul regulament.

Art. I. — Regulamentul nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate și cerințele de raportare aferente serviciilor de plată, publicat în Monitorul Oficial al României, Partea I, nr. 115 din 14 februarie 2020, se modifică după cum urmează:

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

„(2) În sensul prezentului regulament, termenii și expresiile de mai jos au următoarele semnificații:

a) *active informaționale* — date sau alte informații, corporale sau necorporale, care trebuie protejate;

b) *activ TIC* — un activ de natură software sau hardware care se găsește în mediul de afaceri, inclusiv sisteme TIC;

c) *apărare în adâncime* — ansamblu de mai multe tipuri de controale care acoperă același risc, precum principiul celor patru ochi, autentificarea pe baza a doi factori, segmentarea rețelei și mecanisme multiple de tip firewall;

d) *apetit la risc* — nivelul și tipurile cumulate de risc pe care o instituție este dispusă să și le asume în limita capacității sale de risc, conform modelului său de afaceri, în vederea realizării obiectivelor sale strategice;

e) *autenticitate* — proprietatea unei surse de a fi ceea ce se pretinde a fi;

f) *conducere superioară:*

(i) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții de credit și sucursale ale instituțiilor de credit din state terțe, acest termen are înțelesul prevăzut la art. 3 alin. (1) pct. 3 din Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare;

(ii) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții de plată, acest termen se referă la persoanele prevăzute la art. 13 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

(iii) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții emitente de monedă electronică, acest termen se referă la persoanele prevăzute la art. 10 alin. (2) din Legea nr. 210/2019 privind activitatea de emitere de monedă electronică;

(iv) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. b) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, acest termen se referă la persoanele prevăzute la art. 13 alin. (2) sau art. 98 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, după caz;

(v) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, acest termen are semnificația conferită în temeiul legislației naționale aplicabile referitoare la organele de conducere;

g) *continuitate* — proprietatea proceselor, sarcinilor și activelor unei organizații, care sunt necesare pentru prestarea serviciilor aferente plăților, de a fi pe deplin accesibile și de a se desfășura, respectiv de a funcționa, la niveluri prestabilite acceptabile;

h) *disponibilitate* — proprietatea serviciilor aferente plăților de a fi accesibile și utilizabile de către utilizatorii serviciilor de plată;

i) *«Emiterea unui ordin de plată de către autorul fraudei»* — un tip de operațiune de plată neautorizată și se referă la situația în care un ordin de plată fals este emis de autorul fraudei după ce a obținut datele sensibile privind plățile ale plătitorului sau ale beneficiarului plății prin mijloace frauduloase;

j) *funcția de audit:*

(i) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții de credit și sucursale ale instituțiilor de credit din state terțe, funcția de audit are înțelesul prevăzut la art. 54—60 din Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare;

(ii) în cazul prestatorilor de servicii de plată, alții decât cei prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, funcția de audit trebuie să fie independentă de prestatorul de servicii de plată sau independentă în cadrul acestuia și poate fi o funcție de audit intern și/sau extern;

k) *incident TIC operațional sau de securitate* — un singur eveniment sau o serie de evenimente corelate neplanificate de prestatorul de servicii de plată, care are/au sau va/vor avea probabil un impact negativ asupra integrității, disponibilității, confidențialității, autenticității și/sau continuității serviciilor aferente plăților;

l) *integritate* — proprietatea de a proteja funcționarea precisă și caracterul complet al activelor (inclusiv în ceea ce privește datele);

m) *manipularea plătitorului* — acțiune a unei persoane care are ca scop determinarea plătitorului să emită un ordin de plată sau să dea instrucțiuni prestatorului său de servicii de plată să îl emită, cu bună-credință, către un cont de plată despre care crede că aparține beneficiarului legitim al plății;

n) *mediu informatic* — un subset al infrastructurii IT care este folosit pentru un scop bine determinat — de exemplu, mediu de dezvoltare, mediu de asamblare, mediu de test, mediu de producție;

o) *«Modificarea unui ordin de plată de către autorul fraudei»* — un tip de operațiune neautorizată și se referă la situația în care autorul fraudei interceptează și modifică un ordin de plată autorizat la un moment dat, în timpul comunicării electronice între dispozitivul plătitorului și prestatorul de servicii de plată [precum programe malware sau atacuri care le permit atacatorilor să intercepteze comunicarea dintre două gazde care comunică în mod autorizat (atacuri de tip «omul din mijloc»)] sau modifică instrucțiunea de plată în sistemul prestatorului de servicii de plată înainte de compensarea și decontarea ordinului de plată;

p) *operațiune de plată neautorizată* — operațiune de plată executată fără exprimarea consimțământului plătitorului în conformitate cu prevederile art. 147—149 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, inclusiv ca urmare a pierderii, furtului, deturnării datelor sensibile privind plățile sau a instrumentului de plată, indiferent dacă a putut fi detectată de către plătitor înaintea efectuării plății și indiferent dacă a fost cauzată de neglijența gravă a plătitorului;

q) *organ de conducere:*

(i) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții de credit și sucursale ale instituțiilor de credit din state terțe, acest termen are înțelesul prevăzut la art. 3 alin. (1) pct. 1 din Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare;

(ii) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. a) și b) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care sunt instituții de plată, instituții emitente de monedă electronică sau furnizori specializați în servicii de informare cu privire la conturi, acest termen se referă la persoanele prevăzute la lit. f) pct. (ii)—(iv), după caz;

(iii) în cazul prestatorilor de servicii de plată prevăzuți la art. 223 alin. (1) lit. e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, acest termen are semnificația conferită în temeiul legislației naționale aplicabile referitoare la organele de conducere;

r) *principiul «privilegiilor minime»* — prevede că personalul care are nevoie de acces la sistemele informatice și de comunicații trebuie să aibă accesul minim necesar pentru a-și îndeplini funcția. Acest principiu se aplică atât accesului fizic, cât și accesului logic la date și resurse TIC, precum și sistemelor și aplicațiilor care prelucrează date. Abilitatea de a citi, a crea, a actualiza și a șterge datele constituie controale de acces supuse principiului privilegiilor minime;

s) *proiect TIC* — orice proiect sau parte a acestuia în care sunt modificate, înlocuite, respinse sau implementate sisteme și servicii TIC. Proiectele TIC pot face parte din programe de transformare mai ample în sectorul TIC sau în cel de afaceri;

t) *risc TIC și de securitate* — se referă la riscurile operaționale și de securitate prevăzute la art. 218 alin. (1) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative. Acesta reprezintă înregistrări de pierderi din cauza încălcării confidențialității, pierderii integrității sistemelor și a datelor, caracterului necorespunzător sau indisponibilității sistemelor și datelor sau incapacității de a schimba tehnologia informației (TI) într-o perioadă de timp rezonabilă și la costuri rezonabile, atunci când cerințele de mediu sau de afaceri se schimbă. Riscul TIC și de securitate include riscuri de securitate care rezultă fie din procese interne inadecvate sau care nu și-au îndeplinit funcția în mod corespunzător, fie din evenimente externe, inclusiv din atacuri cibernetice sau din securitatea fizică inadecvată;

u) *serviciu aferent plăților* — orice activitate din categoria serviciilor de plată prevăzute la art. 7 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative și toate sarcinile tehnice de asistență necesare pentru prestarea serviciilor de plată;

v) *servicii TIC* — serviciile furnizate de sisteme TIC unuia sau mai multor utilizatori interni sau externi, precum: serviciile de introducere a datelor, de stocare a datelor, de prelucrare și de raportare a datelor, însă și serviciile de monitorizare și serviciile-suport ale afacerii și deciziilor;

w) *sisteme TIC* — tehnologia informației și comunicațiilor configurată în cadrul unui mecanism sau al unei rețele de interconectare care susține operațiunile unui prestator de servicii de plată;

x) *terț* — o organizație care a încheiat contracte în vederea desfășurării unor relații comerciale sau a altui tip de raport juridic, pentru a furniza unei entități un produs sau un serviciu;

y) *TIC* — tehnologia informației și comunicațiilor;

z) *RTO* — obiectivul perioadei de recuperare reprezintă intervalul maxim admis în care un sistem sau un serviciu TIC trebuie să fie restabilit după o întrerupere, înainte de a avea un impact negativ asupra proceselor aferente activității unei instituții;

aa) *RPO* — obiectivul momentului de recuperare reprezintă perioada maximă anterioară momentului în care un serviciu este restaurat după o întrerupere, în care se acceptă pierderea datelor;

bb) *exercițiu de testare a securității de tip «red team»* — înseamnă un exercițiu care imită tactica, tehnicile și procedurile actorilor de amenințări din viața reală percepute ca reprezentând o amenințare cibernetică autentică, care oferă un test controlat, personalizat, desfășurat ca o simulare a unei tentative de atac în vederea compromiterii sistemelor critice aferente activității unei instituții, pentru a oferi o evaluare cuprinzătoare a capacității securității sistemelor TIC și a instituției."

2. **Titlul II se modifică și va avea următorul cuprins:**

„TITLUL II
Gestionarea riscurilor TIC și de securitate

CAPITOLUL I
Dispoziții generale

Art. 3. — (1) Prestatorii de servicii de plată trebuie să prevadă într-un document formal măsuri de securitate adecvate pentru gestionarea riscurilor TIC și de securitate, legate de serviciile de plată pe care le oferă, cu respectarea dispozițiilor prevăzute în prezentul titlu.

(2) Nivelul de detaliu al descrierii măsurilor de securitate prevăzute la alin. (1) trebuie să fie proporțional cu dimensiunea, organizarea internă a prestatorului de servicii de plată, precum și cu natura, scopul, extinderea, complexitatea și gradul de risc asociat serviciilor de plată și produselor pe care prestatorul de servicii de plată le oferă sau intenționează să le ofere.

(3) Prestatorii de servicii de plată trebuie să fundamenteze în mod adecvat măsurile de securitate prevăzute la alin. (1) și să comunice documentația de fundamentare Băncii Naționale a României — Direcția monitorizare a infrastructurilor pieței financiare și a plăților, prin intermediul Rețelei de comunicații interbancare, anual, până cel târziu la data de 31 martie sau mai des la solicitarea acesteia.

(4) Modificările intervenite cu privire la documentația prevăzută la alin. (1) se transmit Băncii Naționale a României — Direcția monitorizare a infrastructurilor pieței financiare și a plăților, în termen de 10 zile de la adoptarea deciziei cu privire la modificări.

(5) Banca Națională a României (*BNR*) poate solicita prestatorilor de servicii de plată să pună la dispoziția acesteia orice alte date și informații pe care le consideră necesare în vederea evaluării adecvării la risc a măsurilor de securitate implementate de către prestatorii de servicii de plată. Prestatorii de servicii de plată au obligația de a pune la dispoziția BNR informațiile și documentele solicitate în termen de 10 zile de la primirea solicitării.

(6) Banca Națională a României poate prelungi, cu maximum 90 de zile, termenul de comunicare a documentației prevăzut la alin. (3), în situații fundamentate de către prestatorii de servicii de plată, care necesită alocarea cât mai eficientă a resurselor umane și materiale existente la nivelul acestora, pentru punerea în aplicare a planurilor lor generale de asigurare a continuității activității în condițiile unor stări de urgență decretate de către autorități, sau alte situații speciale.

(7) Prelungirea termenului prevăzut la alin. (6) se poate realiza în situația în care documentația pusă la dispoziția BNR, precum și istoricul acțiunilor întreprinse de prestatorii de servicii de plată probează față de BNR că îndeplinesc obligația de a deține, pe bază continuă, măsuri de securitate adecvate pentru gestionarea riscurilor TIC și de securitate.

(8) Prelungirea termenului prevăzut la alin. (3), conform alin. (6), nu scutește prestatorii de servicii de plată de la îndeplinirea obligației de a deține, pe bază continuă, măsuri de securitate adecvate pentru gestionarea riscului TIC și de securitate.

CAPITOLUL II
Guvernanța și strategia

SECȚIUNEA 1
Guvernanța

Art. 4. — (1) Organul de conducere trebuie să se asigure că prestatorul de servicii de plată dispune de un cadru adecvat de administrare a activității sale de prestare de servicii aferente plăților și de un cadru de control intern corespunzător riscurilor sale TIC și de securitate.

(2) Organul de conducere trebuie să stabilească roluri și responsabilități clare privind funcțiile TIC, administrarea riscurilor de securitate a informațiilor și continuitatea activității de prestare de servicii aferente plăților, inclusiv pentru organul de conducere și comitetele specializate ale prestatorului de servicii de plată, dacă este cazul.

Art. 5. — (1) Organul de conducere trebuie să se asigure că numărul și competențele membrilor personalului prestatorului de servicii de plată sunt corespunzătoare pentru a sprijini permanent nevoile acestuia operaționale TIC și proceselor sale de administrare a riscurilor TIC și de securitate, precum și pentru a asigura punerea în aplicare a strategiei sale TIC.

(2) Organul de conducere trebuie să se asigure că bugetul alocat este corespunzător pentru a îndeplini strategia TIC a prestatorului de servicii de plată.

Art. 6. — Organul de conducere este pe deplin răspunzător de stabilirea, aprobarea și supravegherea punerii în aplicare a strategiei TIC a prestatorului de servicii de plată în cadrul strategiei sale generale de afaceri, precum și de stabilirea unui cadru eficace de administrare a riscurilor TIC și de securitate.

SECȚIUNEA a 2-a
Strategia

Art. 7. — (1) Strategia TIC trebuie aliniată la strategia generală de afaceri a prestatorului de servicii de plată și trebuie să definească:

a) modul în care trebuie să evolueze TIC a prestatorului de servicii de plată pentru a sprijini și a participa în mod eficient la strategia sa de afaceri, inclusiv la evoluția structurii organizatorice, a modificărilor din sistemul TIC și a dependențelor-cheie de terți;

b) strategia planificată și evoluția arhitecturii TIC, inclusiv a dependențelor de terți;

c) obiective clare de securitate a informațiilor, punând accent pe sisteme și servicii TIC, pe personal și procese.

(2) Prestatorii de servicii de plată trebuie să instituie procese de monitorizare și măsurare a eficacității punerii în aplicare a strategiei lor TIC.

Art. 8. — (1) Prestatorii de servicii de plată trebuie să stabilească seturi de planuri de acțiune care să conțină măsurile ce trebuie luate în vederea atingerii obiectivului strategiei TIC.

(2) Planurile de acțiune menționate la alin. (1) trebuie să fie:

a) comunicate tuturor membrilor relevanți ai personalului (inclusiv contractanților și furnizorilor terți, dacă este cazul și dacă este relevant);

b) revizuite periodic, pentru a se asigura relevanța și adecvarea acestora.

SECȚIUNEA a 3-a
Externalizarea unor funcții operaționale aferente serviciilor de plată

Art. 9. — (1) În cazul în care au fost externalizate funcții operaționale aferente serviciilor de plată și/sau servicii TIC și sisteme TIC ale oricărei activități de prestare de servicii aferente plăților, inclusiv către entitățile din grup, sau atunci când se folosesc furnizori terți, prestatorii de servicii de plată trebuie să asigure eficacitatea măsurilor de securitate prevăzute în prezentul titlu.

(2) Pentru îndeplinirea obligațiilor prevăzute la alin. (1) prestatorii de servicii de plată trebuie să se asigure că în contractele și acordurile privind nivelul de calitate al serviciilor, atât în circumstanțe normale, cât și în caz de întrerupere a serviciului potrivit art. 51[1], cu furnizori de servicii de externalizare, entități din grup sau furnizori terți către care au externalizat funcțiile respective sunt incluse următoarele:

a) obiective și măsuri corespunzătoare și proporționale de securitate a informațiilor, inclusiv cerințe precum cerințe minime de securitate cibernetică, specificații ale ciclului de viață al datelor instituțiilor financiare, orice cerințe privind criptarea datelor, securitatea rețelei și procesele de monitorizare a securității și amplasarea centrelor de date;

b) proceduri de gestionare a incidentelor operaționale și de securitate, inclusiv escaladarea și raportarea.

(3) Prestatorii de servicii de plată trebuie să monitorizeze și să se asigure că furnizorii către care au externalizat funcții operaționale îndeplinesc obiectivele de securitate, măsurile de securitate și obiectivele de performanță stabilite în acord cu alin. (2).

(4) Prestatorii de servicii de plată rămân pe deplin responsabili pentru evaluarea eficacității măsurilor de securitate ale funcțiilor operaționale externalizate aferente serviciilor de plată și/sau serviciilor TIC și sistemelor TIC ale oricărei activități de prestare de servicii aferente plăților.

CAPITOLUL III
Cadrul de gestionare a riscurilor TIC și de securitate

SECȚIUNEA 1
Organizarea și obiectivele

Art. 10. — (1) Prestatorii de servicii de plată trebuie să își identifice și să își administreze adecvat riscurile TIC și de securitate.

(2) Funcția (funcțiile) TIC responsabilă (responsabile) de sistemele TIC, procesele și operațiunile de securitate trebuie să dispună de procese și controale corespunzătoare pentru a se asigura că toate riscurile sunt identificate, analizate, măsurate, monitorizate, administrate, raportate și menținute în limitele apetitului la risc al prestatorului de servicii de plată și că proiectele și sistemele pe care le livrează și activitățile pe care le prestează sunt în conformitate cu cerințele externe și interne.

Art. 11. — (1) Prestatorii de servicii de plată trebuie să atribuie responsabilitatea administrării și supravegherii riscurilor TIC și de securitate unei funcții de control, prin aplicarea în mod corespunzător a prevederilor secțiunii a 4-a, capitolul I al titlului II din Regulamentul nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare.

(2) Prestatorii de servicii de plată trebuie să asigure independența și obiectivitatea acestei funcții de control, separând-o în mod corespunzător de procesele operațiunilor TIC.

(3) Prestatorii de servicii de plată trebuie să se asigure că funcția de control menționată la alin. (1):

a) este direct răspunzătoare în fața organului de conducere și este responsabilă de monitorizarea și controlul respectării cadrului de administrare a riscurilor TIC și de securitate;

b) trebuie să asigure că riscurile TIC și de securitate sunt identificate, măsurate, evaluate, administrate, monitorizate și raportate;

c) nu este responsabilă de niciun audit intern.

Art. 12. — Funcția de audit intern stabilită prin aplicarea în mod corespunzător a prevederilor relevante din cadrul secțiunii a 4-a, capitolul I al titlului II din Regulamentul nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare, trebuie să aibă capacitatea, urmând o abordare bazată pe riscuri, de a revizui independent și de a oferi asigurări obiective cu privire la conformarea tuturor unităților și activităților TIC și de securitate ale prestatorului de servicii de plată cu politicile și procedurile acestuia și cu cerințele externe.

Art. 13. — (1) Prestatorii de servicii de plată trebuie să stabilească un cadru de gestionare a riscurilor TIC și de securitate potrivit prevederilor art. 218 alin. (1) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, denumit în continuare *cadru de gestionare a riscurilor*.

(2) Cadrul de gestionare a riscurilor prevăzut la alin. (1) trebuie integrat în întregime în procesele generale de gestionare a riscurilor ale prestatorilor de servicii de plată și în concordanță cu aceste procese.

Art. 14. — Prestatorii de servicii de plată trebuie să definească și să desemneze rolurile și responsabilitățile-cheie, precum și liniile de raportare relevante, necesare pentru punerea în aplicare a măsurilor de securitate și pentru gestionarea riscurilor TIC și de securitate.

Art. 15. — (1) Cadrul de gestionare al riscurilor TIC elaborat de către prestatorii de servicii de plată potrivit art. 13 trebuie să includă stabilirea de procese pentru:

a) determinarea apetitului la risc, în cazul riscurilor TIC și de securitate, în conformitate cu apetitul la risc al prestatorului de servicii de plată;

b) identificarea, măsurarea, monitorizarea și gestionarea gamei de riscuri TIC și de securitate, care decurg din activitatea de prestare de servicii aferente plăților desfășurată de prestatorul de servicii de plată și la care acesta este expus, inclusiv măsurile de asigurare a continuității activității de prestare de servicii aferente plăților prevăzute în cap. VII al prezentului titlu;

c) definirea măsurilor de diminuare a riscurilor TIC și de securitate, inclusiv a controalelor aferente acestora;

d) monitorizarea eficacității măsurilor stabilite potrivit lit. c), precum și a numărului de incidente TIC operaționale sau de securitate raportate la nivel intern, inclusiv a celor majore raportate în conformitate cu titlul III, care afectează activitățile legate de TIC, precum și acționarea în sensul corectării acestor măsuri, dacă este cazul;

e) raportarea către organul de conducere cu privire la riscurile TIC și de securitate și cu privire la controalele aferente acestora;

f) identificarea și evaluarea posibilității de apariție a riscurilor TIC și de securitate în urma modificărilor majore ale sistemelor sau serviciilor TIC, ale proceselor sau procedurilor TIC și/sau după orice incident major operațional sau de securitate.

(2) Cadrul de gestionare a riscurilor TIC și de securitate trebuie să fie documentat în mod corespunzător și îmbunătățit pe bază continuă cu experiența dobândită și documentată pe parcursul punerii în aplicare și monitorizării acestuia.

(3) Cadrul de administrare a riscurilor TIC și de securitate trebuie aprobat și revizuit, cel puțin o dată pe an, de către organul de conducere.

SECȚIUNEA a 2-a

Identificarea funcțiilor, a proceselor și a activelor

Art. 16. — Prestatorii de servicii de plată trebuie să identifice, să stabilească și să mențină o diagramă funcțională actualizată a funcțiilor activității lor de prestare de servicii aferente plăților, a rolurilor și a proceselor-suport, pentru a identifica importanța fiecăreia dintre ele, interdependențele acestora, raportat la riscurile TIC și de securitate.

Art. 17. — Prestatorii de servicii de plată trebuie să identifice, să stabilească și să mențină o diagramă funcțională actualizată a activelor informaționale care susțin funcțiile activității lor de prestare de servicii aferente plăților și procesele-suport, cum ar fi sistemele TIC cu personalul, contractanții, terții și dependențele de alte sisteme și procese interne și externe, în vederea gestionării, cel puțin, a activelor informaționale care sprijină procesele și funcțiile critice ale activității lor de prestare a serviciilor aferente plăților.

SECȚIUNEA a 3-a

Clasificarea și evaluarea riscurilor

Art. 18. — (1) Prestatorii de servicii de plată trebuie să clasifice funcțiile activității lor de prestare de servicii aferente plăților, procesele-suport și activele informaționale identificate potrivit art. 16 și 17, în funcție de nivelul critic al acestora.

(2) Prestatorii de servicii de plată trebuie să realizeze clasificarea potrivit alin. (1) prin definirea nivelului critic cu luarea în considerare, cel puțin, a cerințelor de confidențialitate, integritate și disponibilitate.

(3) Prestatorii de servicii de plată trebuie să atribuie răspunderi și responsabilități clare pentru activele informaționale.

(4) Prestatorii de servicii de plată trebuie să revizuiască caracterul adecvat al clasificării activelor informaționale și al documentației relevante, atunci când efectuează o evaluare a riscurilor.

Art. 19. — (1) Prestatorii de servicii de plată trebuie să efectueze o evaluare a riscurilor TIC și de securitate prin identificarea acestor riscuri cu impact asupra funcțiilor activității lor de prestare de servicii aferente plăților, proceselor-suport și activelor informaționale, identificate și clasificate în funcție de nivelul critic al acestora potrivit art. 18.

(2) Prestatorii de servicii de plată trebuie să efectueze și să documenteze evaluările riscurilor cel puțin anual.

(3) Evaluarea riscurilor prevăzută la alin. (1) și (2) trebuie să fie efectuată și din perspectiva gestionării oricăror modificări majore ale infrastructurii, proceselor sau procedurilor care afectează funcțiile activității lor de prestare de servicii aferente plăților, procesele-suport sau activele informaționale.

(4) Prestatorii de servicii de plată trebuie să se asigure că monitorizează permanent amenințările și vulnerabilitățile relevante pentru procesele activității lor de prestare de servicii aferente plăților, funcțiile-suport și activele informaționale și să revizuiască în mod regulat scenariile de risc cu impact asupra lor.

SECȚIUNEA a 4-a

Diminuarea riscului

Art. 20. — (1) Pe baza evaluării riscurilor efectuată potrivit art. 19, prestatorii de servicii de plată trebuie să stabilească ce măsuri sunt necesare și dacă sunt necesare modificări ale proceselor activității lor de prestare de servicii aferente plăților, ale măsurilor de control, ale sistemelor și serviciilor TIC existente pentru diminuarea la un nivel acceptabil a riscurilor TIC și de securitate identificate.

(2) Prestatorii de servicii de plată trebuie să ia în considerare durata necesară pentru punerea în aplicare a modificărilor prevăzute la alin. (1) și pentru luarea măsurilor provizorii adecvate în vederea diminuării riscurilor TIC și de securitate, astfel încât acestea să nu depășească apetitul la riscurile TIC și de securitate al prestatorului de servicii de plată.

Art. 21. — Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare măsuri pentru diminuarea riscurilor TIC și de securitate identificate și pentru a proteja activele informaționale, în funcție de clasificarea lor.

SECȚIUNEA a 5-a

Raportarea

Art. 22. — (1) Prestatorii de servicii de plată trebuie să raporteze în mod clar și la timp organului de conducere rezultatele evaluării riscurilor TIC și de securitate.

(2) Raportarea realizată potrivit alin. (1) nu aduce atingere obligației prestatorilor de servicii de plată de a furniza Băncii Naționale a României o evaluare actualizată și detaliată a riscurilor, astfel cum se prevede la art. 218 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.

Art. 22[1]. — Prestatorii de servicii de plată vor remite anual, până la data de 31 martie, pentru anul anterior, prin intermediul Rețelei de comunicații interbancare, următoarele informații:

a) scenariile de test avute în vedere potrivit art. 43 și rezultatele testărilor prevăzute la art. 46;

b) extrase din rapoartele auditorilor, care să conțină concluziile acestora cu privire la reziliența cadrului de administrare a activității de prestare de servicii aferente plăților, sistemelor și proceselor aferente riscurilor TIC și de securitate;

c) modificările semnificative aduse cadrului de administrare a activității de prestare de servicii aferente plăților, sistemelor și proceselor aferente riscurilor TIC și de securitate, inclusiv a locațiilor sediilor secundare ce asigură continuitatea activității de procesare a plăților, decontărilor și a instrumentelor de plată.

SECȚIUNEA a 6-a

Auditul

Art. 23. — (1) Prestatorii de servicii de plată trebuie să se asigure că cadrul de administrare a activității de prestare de servicii aferente plăților, sistemele și procesele aferente riscurilor TIC și de securitate sunt auditate periodic de către auditori cu suficiente cunoștințe, competențe și experiență în riscurile TIC și de securitate și în plăți, pentru a oferi organului de conducere asigurări independente cu privire la eficacitatea acestora.

(2) Prestatorii de servicii de plată trebuie să se asigure că auditarea efectuată potrivit alin. (1) este realizată de auditori independenți din punct de vedere operațional de prestatorul de servicii de plată, indiferent dacă își desfășoară activitatea în cadrul sau separat de acesta.

(3) Frecvența și obiectul auditurilor realizate potrivit alin. (1) trebuie să fie proporționale cu riscurile TIC și de securitate relevante.

(4) Organul de conducere al unui prestator de servicii de plată trebuie să aprobe planul de audit care stă la baza auditurilor realizate potrivit alin. (1), inclusiv orice audituri TIC și orice modificări semnificative ale acestuia.

(5) Planul de audit și execuția sa, inclusiv frecvența auditului, trebuie să reflecte și să fie proporționale cu riscurile TIC și de securitate asociate activității de prestare de servicii aferente plăților a prestatorului de servicii de plată și trebuie actualizat cel puțin anual.

Art. 24. — Prestatorii de servicii de plată trebuie să instituie un proces formal de monitorizare la nivel intern care să includă dispoziții pentru verificarea și remedierea la timp a constatărilor critice rezultate din auditul TIC.

CAPITOLUL IV
Măsurile de securitate preventive

SECȚIUNEA 1

Dispoziții generale

Art. 25. — Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare măsuri de securitate preventive împotriva riscurilor TIC și de securitate identificate.

Art. 26. — Prestatorii de servicii de plată trebuie să elaboreze și să implementeze măsurile de securitate preventive potrivit art. 25, prin utilizarea unei abordări de tipul «apărare în adâncime», instituind controale pe mai multe niveluri, care vizează persoane, procese și tehnologia, fiecare nivel servind drept mecanism de siguranță pentru nivelurile anterioare.

SECȚIUNEA a 2-a

Politica în domeniul securității informațiilor

Art. 27. — (1) Prestatorii de servicii de plată trebuie să dezvolte și să documenteze o politică în domeniul securității informațiilor care trebuie să definească principiile generale și normele de protejare a confidențialității, integrității și disponibilității datelor și informațiilor prestatorilor de servicii de plată și ale clienților lor.

(2) Politica prevăzută la alin. (1) trebuie să fie inclusă în documentul privind politica de securitate în materia prestării serviciilor de plată, care este adoptat în conformitate cu art. 29 alin. (1) lit. m) din Regulamentul nr. 4/2019 privind instituțiile de plată și furnizorii specializați în servicii de informare cu privire la conturi.

(3) Politica în domeniul securității informațiilor trebuie să fie în concordanță cu obiectivele de securitate a informațiilor ale prestatorilor de servicii de plată stabilite potrivit art. 7 alin. (1) lit. c) și trebuie să se bazeze pe rezultatele relevante ale procesului de evaluare a riscurilor TIC și de securitate ale activității lor de prestare de servicii aferente plăților.

(4) Politica în domeniul securității informațiilor realizată potrivit alin. (1) trebuie aprobată de organul de conducere.

(5) Politica în domeniul securității informațiilor trebuie:

a) să conțină o descriere a rolurilor și responsabilităților principale de gestionare a securității informațiilor;

b) să stabilească cerințele referitoare la securitatea informațiilor pentru personal și contractanți, procese și tehnologie, inclusiv cu privire la faptul că personalul și contractanții de la toate nivelurile trebuie să fie responsabili în asigurarea securității informațiilor prestatorilor de servicii de plată;

c) să asigure confidențialitatea, integritatea și disponibilitatea activelor fizice și logice critice, ale resurselor și ale datelor sensibile privind plățile, aferente prestatorilor de servicii de plată, fie că sunt în stare de repaus, în tranzit sau în folosință;

d) să fie comunicată tuturor membrilor personalului și contractanților prestatorilor de servicii de plată.

(6) Dacă datele sensibile privind plățile includ date cu caracter personal, astfel de măsuri trebuie puse în aplicare în conformitate cu prevederile art. 217 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.

Art. 28. — (1) Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare măsuri de securitate pentru diminuarea riscurilor TIC și de securitate la care sunt expuși, pe baza politicii în domeniul securității informațiilor.

(2) Măsurile de securitate prevăzute la alin. (1) trebuie să includă:

a) organizarea și administrarea activității;

b) securitatea logică;

c) securitatea fizică;

d) securitatea operațiunilor TIC;

e) monitorizarea securității;

f) revizuirea, evaluarea și testarea securității informațiilor;

g) formarea profesională și conștientizarea cu privire la securitatea informațiilor.

SECȚIUNEA a 3-a

Securitatea logică

Art. 29. — (1) Prestatorii de servicii de plată trebuie să definească, să documenteze, să pună în aplicare și să impună proceduri de control al accesului logic pentru gestionarea identității și a accesului.

(2) Procedurile prevăzute la alin. (1) trebuie să fie monitorizate permanent, să includă controale pentru monitorizarea anomaliilor și să fie revizuite cel puțin anual.

Art. 30. — (1) Procedurile prevăzute la art. 29 trebuie să pună în aplicare cel puțin următoarele elemente:

a) necesitatea de a cunoaște, potrivit căreia prestatorii de servicii de plată trebuie să gestioneze drepturile de acces la activele informaționale și la sistemele lor suport pe baza principiului «necesității de a cunoaște», inclusiv în ceea ce privește accesul de la distanță;

b) privilegiile minime și separarea sarcinilor, potrivit cărora prestatorii de servicii de plată trebuie să acorde utilizatorilor drepturile minime de acces strict necesare pentru executarea sarcinilor lor (principiul «privilegiilor minime»), și anume pentru a proteja împotriva accesului nejustificat al utilizatorilor la un set mare de date sau pentru a împiedica alocarea unor combinații de drepturi de acces care pot fi utilizate pentru a eluda controalele (principiul «separării sarcinilor»);

c) cerința operațională legitimă, potrivit căreia prestatorii de servicii de plată trebuie să instituie controale eficiente care să asigure că accesul la sistemele TIC este permis doar persoanelor cu o cerință operațională legitimă;

d) răspunderea utilizatorului: potrivit căreia prestatorii de servicii de plată trebuie să limiteze pe cât posibil utilizarea de conturi de utilizator generice și partajate și trebuie să se asigure că utilizatorii pot fi identificați pentru acțiunile întreprinse în sistemele TIC;

e) drepturile de acces privilegiat, potrivit cărora prestatorii de servicii de plată trebuie să instituie controale stricte privind accesul privilegiat la sisteme TIC, prin limitarea strictă și prin

supravegherea îndeaproape a conturilor utilizatorilor cu drepturi sporite de acces la sistem, inclusiv a conturilor de administrator;

f) comunicarea în condiții de siguranță și reducerea riscurilor, potrivit cărora prestatorii de servicii de plată trebuie să acorde accesul administrativ de la distanță la sistemele TIC critice numai pe baza principiului necesității de a cunoaște și atunci când se utilizează soluții de autentificare puternice, din categoria celor specificate la lit. j);

g) înregistrarea activităților utilizatorilor, potrivit căreia prestatorii de servicii de plată trebuie să se asigure că toate activitățile utilizatorilor cu drepturi sporite de acces la sistem trebuie cel puțin înregistrate și monitorizate și că jurnalele de acces sunt securizate pentru a împiedica modificarea sau ștergerea neautorizată a acestora. Prestatorii de servicii de plată trebuie să utilizeze aceste informații pentru facilitarea identificării și investigării activităților atipice, detectate în cadrul activității de prestare de servicii aferente plăților;

h) gestionarea accesului, potrivit căreia prestatorii de servicii de plată trebuie să acorde, să retragă sau să modifice drepturile de acces în conformitate cu termenele prevăzute în cadrul procedurilor interne, fără întârzieri nejustificate, și cu fluxurile de lucru de aprobare care îl implică pe proprietarul informațiilor accesate (proprietarul activelor informaționale). În caz de încetare a contractului de muncă al utilizatorilor, drepturile de acces trebuie retrase cel mai târziu până la încetarea raporturilor de muncă;

i) recertificarea accesului, potrivit căreia drepturile de acces prevăzute la lit. a) trebuie revizuite periodic, însă cel puțin anual pentru a se asigura că utilizatorii nu dețin privilegii excesive și că drepturile de acces sunt retrase atunci când nu mai sunt necesare;

j) metodele de autentificare, potrivit cărora prestatorii de servicii de plată trebuie să aplice metode de autentificare suficient de solide care să asigure respectarea adecvată și eficientă a politicilor și procedurilor de control al accesului. Metodele de autentificare trebuie să fie proporționale cu nivelul critic al sistemelor TIC, al informațiilor sau al procesului care sunt accesate. Acestea trebuie să conțină cel puțin parole complexe sau metode de autentificare mai sigure (cum ar fi autentificarea cu doi factori), în funcție de riscul relevant.

(2) Prestatorii de servicii de plată trebuie să păstreze jurnalele prevăzute la alin. (1) lit. g) pe o perioadă de timp proporțională cu nivelul critic al funcțiilor activității lor de prestare de servicii aferente plăților, proceselor de asistență și activelor informaționale, identificate în conformitate cu prevederile secțiunii a 3-a din capitolul III, fără a aduce atingere legislației naționale aplicabile referitoare la cerințele de păstrare a datelor.

(3) În înțelesul prezentului articol, termenul *utilizator* include și *utilizatori tehnici*.

Art. 31. — Prestatorii de servicii de plată trebuie să se asigure că autorizarea accesului electronic la date și sisteme TIC, prin intermediul unor aplicații, este limitată la minimul necesar pentru prestarea serviciului de plată relevant.

Art. 32. — (1) Prestatorii de servicii de plată trebuie să se asigure că funcționarea produselor, a instrumentelor și a procedurilor referitoare la procesele de control al accesului sunt eficiente din perspectiva protejării respectivelor procese împotriva compromiterii sau eludării acestora.

(2) Obligația prestatorilor de servicii de plată prevăzută la alin. (1) include înregistrarea, transmiterea, revocarea și retragerea produselor, instrumentelor și procedurilor corespunzătoare.

SECȚIUNEA a 4-a

Securitatea fizică

Art. 33. — Prestatorii de servicii de plată trebuie să definească, să documenteze și să pună în aplicare măsuri de securitate fizică corespunzătoare pentru a-și proteja sediile, centrele de date și zonele sensibile, în special a celor destinate pentru gestionarea datelor sensibile privind plățile ale utilizatorilor de servicii de plată, precum și a sistemelor TIC utilizate pentru prestarea serviciilor de plată, împotriva accesului neautorizat și al pericolelor de mediu.

Art. 34. — (1) Accesul fizic la sistemele TIC trebuie să fie permis numai persoanelor care sunt autorizate.

(2) Autorizarea prevăzută la alin. (1) trebuie atribuită în conformitate cu sarcinile și responsabilitățile personalului, limitată la persoanele care sunt instruite și monitorizate în mod corespunzător.

(3) Accesul fizic trebuie revizuit periodic pentru a se asigura că drepturile de acces sunt revocate imediat ce nu mai sunt necesare.

Art. 35. — Prestatorii de servicii de plată trebuie să instituie măsuri adecvate de protecție împotriva pericolelor de mediu, care trebuie să fie proporționale cu importanța clădirilor și nivelul critic al operațiunilor sau al sistemelor TIC din aceste clădiri, utilizate pentru prestarea serviciilor de plată.

SECȚIUNEA a 5-a

Securitatea operațiunilor TIC

Art. 35[1]. — (1) Prestatorii de servicii de plată trebuie să pună în aplicare proceduri care să împiedice apariția de probleme de securitate în sistemele și prestarea serviciilor TIC și trebuie să minimizeze impactul acestora asupra prestării de servicii TIC.

(2) Procedurile stabilite potrivit alin. (1) trebuie să cuprindă următoarele măsuri:

a) identificarea posibilelor vulnerabilități, care trebuie evaluate și remediate prin asigurarea actualizării programelor software și firmware, inclusiv a programelor software furnizate de prestatorii de servicii de plată utilizatorilor lor interni și externi, prin instalarea de patch-uri de securitate critice sau prin punerea în aplicare de controale compensatoare;

b) implementarea de configurații securizate de referință pentru toate componentele rețelei;

c) implementarea segmentării rețelei, a unor sisteme de prevenire a pierderii datelor și criptarea traficului din rețea, în conformitate cu clasificarea datelor, respectiv critice sau sensibile privind plățile;

d) implementarea protecției punctelor finale de acces, inclusiv a serverelor, a stațiilor de lucru și a dispozitivelor mobile;

e) evaluarea dacă punctele finale de acces respectă standardele de securitate definite de prestatorii de servicii de plată, înainte de a li se acorda accesul la rețeaua prestatorului de servicii de plată sau a entităților către care au fost externalizate servicii operaționale;

f) asigurarea existenței și funcționării corespunzătoare a unor mecanisme de verificare a integrității programelor și aplicațiilor software, a firmware-ului și a datelor;

g) asigurarea că direcționarea, colectarea, prelucrarea, stocarea și/sau arhivarea și vizualizarea datelor sensibile privind plățile ale utilizatorului de servicii de plată sunt adecvate, relevante și limitate la ceea ce este necesar pentru prestarea serviciilor de plată;

h) criptarea datelor în stare de repaus, precum și a celor transmise prin intermediul unui canal de comunicare se realizează în conformitate cu clasificarea datelor, respectiv critice sau sensibile privind plățile.

Art. 35[2]. — (1) Prestatorii de servicii de plată trebuie să stabilească pe bază continuă dacă modificările la nivelul mediului operațional existent influențează măsurile de securitate existente sau dacă impun adoptarea de măsuri suplimentare pentru diminuarea în mod corespunzător a riscurilor asociate.

(2) Modificările prevăzute la alin. (1) trebuie să facă parte din procesul formal de gestionare a modificărilor al prestatorilor de servicii de plată, proces care trebuie să asigure planificarea, testarea, documentarea, autorizarea și aplicarea corespunzătoare a modificărilor.

SECȚIUNEA a 6-a

Monitorizarea securității

SUBSECȚIUNEA 1

Monitorizarea continuă și detecția

Art. 36. — (1) Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare politici și proceduri pentru monitorizarea continuă a funcțiilor activității de prestare de servicii aferente plăților, proceselor de asistență, precum și a activelor informaționale și TIC, activității lor de prestare de servicii aferente plăților, pentru a detecta activitățile anormale care pot afecta securitatea informațiilor prestatorilor de servicii de plată și pentru a răspunde în mod corespunzător acestor evenimente.

(2) În cadrul monitorizării continue prevăzute la alin. (1), prestatorii de servicii de plată trebuie să implementeze mecanisme corespunzătoare și eficiente de detectare și raportare a intruziunilor logice sau fizice, precum și a încălcărilor confidențialității, integrității și disponibilității activelor informaționale utilizate în prestarea serviciilor de plată.

(3) Prestatorii de servicii de plată trebuie să aloce și să dețină resurse corespunzătoare pentru îndeplinirea obligațiilor prevăzute la alin. (1) și (2).

Art. 37. — Politicile și procedurile de monitorizare continuă și detectare prevăzute la art. 36 trebuie să acopere:

a) factorii interni și externi relevanți, inclusiv funcțiile administrative privind TIC și cele ale activității lor de prestare de servicii aferente plăților;

b) operațiunile pentru detectarea utilizării abuzive a accesului de către terți sau de către alte entități și a utilizării abuzive a accesului intern;

c) amenințările interne și externe potențiale.

SUBSECȚIUNEA a 2-a

Cadrul amenințărilor și cunoașterea situației

Art. 38. — (1) Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare procese și structuri organizatorice, pentru a identifica și monitoriza constant amenințările de securitate care ar putea afecta semnificativ capacitatea acestora de a presta servicii de plată.

(2) Prestatorii de servicii de plată trebuie să monitorizeze activ evoluțiile tehnologice, pentru a se asigura că au în vedere riscurile TIC și de securitate.

(3) Prestatorii de servicii de plată trebuie să pună în aplicare măsuri de detecție pentru a identifica eventualele scurgeri de informații, coduri dăunătoare și alte amenințări la adresa securității și vulnerabilitățile cunoscute în mod public ale echipamentelor, aplicațiilor și sistemelor TIC și să verifice existența unor noi actualizări de securitate corespunzătoare.

(4) Presatorul de servicii de plată trebuie să utilizeze procesul de monitorizare a securității prevăzut la alin. (1) în scopul susținerii înțelegerii naturii incidentelor operaționale sau de securitate, al identificării tendințelor în materie de securitate și al sprijinirii investigațiilor organizației.

Art. 39. — (1) Prestatorii de servicii de plată trebuie să analizeze incidentele operaționale sau de securitate care au fost identificate sau care au avut loc în cadrul și/sau în afara prestatorului de servicii de plată.

(2) Prestatorii de servicii de plată trebuie să ia în considerare experiența dobândită ca urmare a analizei realizate potrivit alin. (1) și să actualizeze în consecință măsurile de securitate prevăzute potrivit dispozițiilor prezentului titlu.

SECȚIUNEA a 7-a

Revizuirea, evaluarea și testarea măsurilor de securitate a informațiilor

Art. 40. — (1) Prestatorii de servicii de plată trebuie să realizeze o varietate de revizuiri, evaluări și testări ale securității informațiilor pentru a asigura identificarea eficientă a vulnerabilităților din sistemele și serviciile lor TIC.

(2) În desfășurarea activităților prevăzute la alin. (1) prestatorii de servicii de plată trebuie:

a) să realizeze cel puțin analiza deficiențelor pe baza standardelor de securitate a informațiilor, revizuiri ale conformității, audituri interne și externe ale sistemelor informatice sau revizuiri ale securității fizice;

b) să țină seama de bunele practici, cum ar fi: revizuiri ale codului-sursă, evaluări ale vulnerabilităților, teste de penetrare și exerciții de testare a securității de tip «red team».

Art. 41. — Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare un cadru de testare al măsurilor de securitate a informațiilor stabilite de aceștia în aplicarea prezentului titlu, care să valideze robustețea și eficiența măsurilor de securitate a informațiilor și să se asigure că acest cadru de testare este adaptat pentru a lua în considerare noile amenințări și vulnerabilități, identificate prin intermediul procesului de monitorizare a amenințărilor și de evaluare a riscurilor TIC și de securitate.

Art. 42. — (1) Cadrul de testare prevăzut la art. 41 trebuie să asigure că testele:

a) sunt efectuate ca parte a procesului formal de gestionare a modificărilor, care trebuie prevăzut de către prestatorii de servicii de plată, pentru a asigura robustețea și eficiența măsurilor de securitate a informațiilor;

b) sunt efectuate de verificatori independenți, care au cunoștințe, competențe și expertize suficiente în testarea măsurilor de securitate a informațiilor aferente serviciilor de plată și care nu sunt implicați în dezvoltarea măsurilor de securitate a informațiilor aferente serviciilor de plată sau a sistemelor care urmează să fie testate;

c) includ scanări ale vulnerabilităților și teste de penetrare (inclusiv teste de penetrare bazate pe amenințări) corespunzătoare nivelului de risc identificat în cadrul sistemelor și proceselor aferente activității de prestare de servicii de plată;

d) cuprind examinarea măsurilor de securitate relevante.

(2) Măsurile de securitate relevante prevăzute la alin. (1) lit. d) se referă la:

a) terminalele de plată și dispozitivele utilizate pentru prestarea serviciilor de plată;

b) terminalele de plată și dispozitivele utilizate pentru autentificarea utilizatorului de servicii de plată;

c) dispozitivele, programele și aplicațiile software furnizate de prestatorul de servicii de plată utilizatorului de servicii de plată pentru a genera/primi un cod de autentificare.

Art. 43. — Prestatorii de servicii de plată trebuie să se asigure că testele măsurilor de securitate prevăzute la art. 42 includ scenariile atacurilor potențiale cunoscute și relevante, pe baza amenințărilor la adresa securității constatate și a modificărilor efectuate.

Art. 44. — (1) Prestatorii de servicii de plată trebuie să efectueze testele prevăzute la art. 42 pe bază continuă și în mod repetat, cu privire la măsurile de securitate aferente serviciilor de plată oferite de aceștia.

(2) Prestatorii de servicii de plată trebuie să efectueze, cel puțin anual, testarea sistemelor TIC, care au fost identificate drept critice pentru prestarea serviciilor de plată potrivit art. 18 alin. (1).

(3) Testele realizate potrivit alin. (2) trebuie să facă parte din evaluarea detaliată a riscurilor de securitate asociate serviciilor de plată pe care aceștia le prestează, în conformitate cu art. 218 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.

(4) Sistemele care nu sunt critice trebuie testate regulat de către prestatorii de servicii de plată printr-o abordare bazată pe riscuri, dar cel puțin la fiecare trei ani.

Art. 45. — Prestatorii de servicii de plată trebuie să se asigure că testele măsurilor de securitate se efectuează în următoarele situații:

a) în eventualitatea unor modificări ale infrastructurii, proceselor și procedurilor;

b) în situația în care aceste modificări sunt efectuate ca urmare a unor incidente operaționale sau de securitate majore;

c) în cazul lansării de aplicații critice cu acces la internet, noi sau modificate substanțial.

Art. 46. — Prestatorii de servicii de plată trebuie să monitorizeze și să evalueze rezultatele testelor de securitate efectuate și să își actualizeze măsurile de securitate în mod corespunzător și fără întârzieri nejustificate în ceea ce privește sistemele TIC critice, identificate conform dispozițiilor art. 18 alin. (1).

SECȚIUNEA a 8-a

Programe de formare și de cunoaștere în materie de securitate

Art. 47. — (1) Prestatorii de servicii de plată trebuie să stabilească un program de formare profesională care trebuie:

a) să includă programe periodice de conștientizare cu privire la securitate pentru toți membrii personalului și contractanți, pentru a se asigura că aceștia sunt instruiți pentru a-și îndeplini sarcinile și responsabilitățile, în conformitate cu procedurile și politicile de securitate relevante, în vederea prevenirii și diminuării factorilor de risc precum eroarea umană, furtul, frauda, utilizarea abuzivă sau pierderea și pentru a aborda adecvat riscurile TIC și de securitate asociate securității informațiilor;

b) să asigure instruirea tuturor membrilor personalului și contractanților cel puțin anual și, dacă este necesar, mai frecvent, la inițiativa prestatorului de servicii de plată ori la solicitarea Băncii Naționale a României.

(2) Prestatorii de servicii de plată trebuie să se asigure că toți membrii personalului, inclusiv persoanele care îndeplinesc rolurile-cheie și responsabilitățile-cheie asociate acestora, identificate conform dispozițiilor art. 16, sunt instruiți anual sau mai frecvent, dacă este necesar, prin programe de formare profesională adecvată cu privire la riscurile TIC și de securitate, inclusiv cu privire la securitatea informațiilor.

(3) Tematica programelor prevăzute la alin. (1) trebuie să conțină inclusiv dispoziții cu privire la modalitatea în care membrii personalului prestatorului de servicii de plată sunt obligați să raporteze toate incidentele sau activitățile neobișnuite.

CAPITOLUL V
Gestionarea operațiunilor TIC

SECȚIUNEA 1

Dispoziții generale

Art. 47[1]. — (1) Prestatorii de servicii de plată trebuie să își gestioneze, în ceea ce privește prestarea de servicii de plată, operațiunile TIC pe bază de procese și proceduri documentate, care să fie incluse în politica de securitate prin aplicarea în mod corespunzător a prevederilor art. 29 alin. (1) lit. m) din Regulamentul nr. 4/2019 privind instituțiile de plată și furnizorii specializați în servicii de informare cu privire la conturi.

(2) Setul de documente prevăzut la alin. (1) trebuie:

a) să fie aprobat de organul de conducere și să fie pus în aplicare de către prestatorii de servicii de plată în mod corespunzător;

b) să definească modul în care prestatorii de servicii de plată operează, monitorizează și își verifică sistemele și serviciile TIC, inclusiv documentarea operațiunilor TIC critice;

c) să permită prestatorilor de servicii de plată să își actualizeze inventarul activelor TIC.

Art. 47[2]. — (1) Prestatorii de servicii de plată trebuie să se asigure că performanța operațiunilor TIC este în concordanță cu cerințele lor de afaceri.

(2) Prestatorii de servicii de plată trebuie să mențină și să își îmbunătățească, atunci când este posibil, eficiența operațiunilor TIC, cel puțin cu privire la necesitatea de a analiza modul în care pot fi minimizate eventualele erori ce decurg din executarea sarcinilor manuale.

Art. 47[3]. — Prestatorii de servicii de plată trebuie să pună în aplicare proceduri privind înregistrarea și monitorizarea în cazul operațiunilor TIC critice, pentru a permite detectarea, analiza și corectarea erorilor.

Art. 47[4]. — (1) Prestatorii de servicii de plată trebuie să mențină un inventar actualizat al activelor, inclusiv al sistemelor TIC, dispozitivelor de rețea și al bazelor de date.

(2) Inventarul activelor TIC realizat potrivit prevederilor alin. (1) trebuie să conțină configurația activelor TIC, legăturile și interdependențele dintre diferitele active TIC, pentru a permite un proces adecvat de gestionare a configurațiilor și modificărilor.

(3) Inventarul activelor TIC trebuie să fie suficient de detaliat pentru a permite identificarea imediată a unui activ TIC, a amplasamentului acestuia, a nivelului de securitate și a proprietarului.

(4) Interdependențele dintre active trebuie documentate, pentru a ajuta prestatorii de servicii de plată să intervină în caz de incidente de securitate sau operaționale, inclusiv în caz de atacuri cibernetice.

Art. 47[5]. — (1) Prestatorii de servicii de plată trebuie să monitorizeze și să gestioneze ciclurile de viață ale activelor TIC, inclusiv cele dedicate utilizatorilor de servicii de plată, pentru a se asigura că acestea îndeplinesc și susțin în continuare cerințele de afaceri și de administrare a riscurilor TIC și de securitate.

(2) Prestatorii de servicii de plată trebuie să monitorizeze dacă furnizorii lor interni sau externi și dezvoltatorii oferă asistență pentru activele lor TIC și dacă sunt instalate toate patch-urile și actualizările relevante pe bază de procese documentate.

(3) Riscurile care decurg din activele TIC învechite sau pentru care nu se mai oferă suport trebuie evaluate și diminuate.

Art. 47[6]. — Prestatorii de servicii de plată trebuie să pună în aplicare procese de planificare și monitorizare a performanței și capacității, pentru a împiedica, a detecta și a răspunde prompt problemelor importante legate de performanța sistemelor TIC și de deficiențe ale capacității TIC.

Art. 47[7]. — (1) Prestatorii de servicii de plată trebuie să definească și să implementeze proceduri pentru realizarea de copii de rezervă și de restaurare a datelor și a sistemelor TIC, pentru a se asigura că acestea pot fi recuperate, conform cerințelor.

(2) Domeniul de aplicare și frecvența operațiunilor de realizare a copiilor de rezervă prevăzute la alin. (1) trebuie stabilite în conformitate cu cerințele de redresare a activității de prestare de servicii aferente plăților și cu nivelul critic al datelor și al sistemelor TIC și trebuie analizate în funcție de evaluarea riscurilor.

(3) Testarea procedurilor de realizare a copiilor de rezervă și de restaurare trebuie efectuată periodic.

(4) Prestatorii de servicii de plată trebuie să asigure că este efectuată stocarea în siguranță a copiilor de rezervă ale datelor și ale sistemelor TIC realizate potrivit alin. (1), la o distanță suficient de mare față de amplasamentul principal, pentru a nu fi expuse acelorași riscuri.

SECȚIUNEA a 2-a

Gestionarea și raportarea problemelor și incidentelor TIC operaționale sau de securitate

Art. 47[8]. — (1) Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare un proces de gestionare a problemelor și incidentelor, pentru a monitoriza și înregistra incidentele TIC operaționale sau de securitate și pentru a permite prestatorilor de servicii de plată să continue sau să reia rapid procesele și funcțiile critice activității lor de prestare de servicii aferente plăților, atunci când se produc întreruperi.

(2) Prestatorii de servicii de plată trebuie să stabilească praguri și criterii corespunzătoare pentru clasificarea unui eveniment drept incident TIC operațional sau de securitate, precum și indicatori de alertă timpurie pentru a permite detectarea anticipată a incidentelor TIC operaționale sau de securitate.

(3) Criteriile și pragurile stabilite potrivit alin. (2) nu trebuie să aducă atingere clasificării incidentelor majore, în conformitate cu cerințele titlului III.

Art. 47[9]. — (1) Prestatorii de servicii de plată trebuie să stabilească proceduri și procese corespunzătoare și structuri organizatorice pentru a asigura monitorizarea, gestionarea și urmărirea în mod integrat și consecvent a incidentelor TIC operaționale sau de securitate, în vederea identificării și eliminării principalelor cauze care au condus la apariția acestora și pentru a evita reapariția unor astfel de incidente, în scopul diminuării impactului evenimentelor defavorabile și pentru a permite redresarea la timp.

(2) Procesul de gestionare a problemelor și incidentelor prevăzut la alin. (1) trebuie să stabilească:

a) proceduri de identificare, urmărire, înregistrare, categorisire și clasificare a incidentelor, potrivit unei reguli de prioritate, în funcție de nivelul critic al activității de prestare de servicii aferente plăților;

b) rolurile și responsabilitățile pentru diferite scenarii de incidente (de exemplu, erori, defecțiuni, atacuri cibernetice);

c) proceduri de gestionare a problemelor pentru a identifica, analiza și soluționa principala cauză a unuia sau a mai multor incidente — un prestator de servicii de plată trebuie să analizeze incidentele TIC operaționale sau de securitate care ar putea afecta prestatorul de servicii de plată, care au fost identificate sau care au avut loc în cadrul și/sau în afara organizației și trebuie să ia în considerare lecțiile-cheie învățate din aceste analize și să actualizeze în consecință măsurile de securitate;

d) planuri eficiente de comunicare internă, inclusiv proceduri de notificare și escaladare a incidentelor — care să acopere și reclamațiile clienților legate de securitate, care trebuie să asigure următoarele cerințe:

(i) incidentele și plângerile clienților legate de securitate cu un posibil impact negativ ridicat asupra sistemelor și serviciilor TIC se raportează conducerii superioare și conducerii care coordonează domeniul TIC;

(ii) organul de conducere trebuie informat ad-hoc în caz de incidente semnificative, identificate în baza unor criterii stabilite intern la nivelul prestatorului de servicii de plată, cel puțin cu privire la impactul, măsurile luate și controalele suplimentare care urmează să fie definite ca urmare a incidentelor;

e) proceduri de intervenție în caz de incidente, pentru reducerea impactului acestora și pentru a asigura că serviciul devine, în timp util, operațional și sigur;

f) planuri specifice de comunicare externă pentru procese și funcții critice asociate activității de prestare a serviciilor aferente plăților pentru a asigura îndeplinirea următoarelor cerințe:

(i) asigurarea colaborării cu părțile interesate relevante, pentru a interveni în mod eficient în caz de incidente și a se redresa în urma acestora;

(ii) furnizarea către părțile externe, inclusiv clienților, altor participanți în piață și Băncii Naționale a României de informații în timp util, în mod corespunzător și în conformitate cu titlul III.

Art. 47[10]. — Prestatorii de servicii de plată trebuie să se asigure de faptul că măsurile prevăzute în acord cu art. 47[9] definesc în mod clar toate responsabilitățile pentru raportarea incidentelor operaționale sau de securitate majore și aferente proceselor puse în aplicare pentru îndeplinirea cerințelor prevăzute de titlul III.

CAPITOLUL VI
Gestionarea proiectelor și modificărilor TIC

SECȚIUNEA 1
Gestionarea proiectelor TIC

Art. 47[11]. — Prestatorii de servicii de plată trebuie să pună în aplicare un program și/sau un proces de guvernanță a proiectelor care să definească rolurile, responsabilitățile și răspunderile, pentru a susține în mod eficient punerea în aplicare a strategiei TIC.

Art. 47[12]. — Prestatorii de servicii de plată trebuie să monitorizeze și să diminueze în mod corespunzător riscurile ce decurg din portofoliul lor de proiecte TIC (gestionarea programului), ținând seama și de riscurile care pot rezulta din interdependențele dintre diferite proiecte și din dependențele mai multor proiecte de aceleași resurse și/sau competențe.

Art. 47[13]. — Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare o politică de gestionare a proiectelor TIC, care să includă cel puțin:

a) obiectivele proiectului;

b) rolurile și responsabilitățile;

c) evaluarea riscurilor asociate proiectului;

d) planul, calendarul și etapele proiectului;

e) principalele obiective intermediare;

f) cerințele de gestionare a modificărilor.

Art. 47[14]. — Politica de gestionare a proiectelor TIC realizată potrivit art. 47[13] trebuie să asigure că cerințele de securitate a informațiilor sunt analizate și aprobate de către o funcție independentă de funcția care le-a elaborat.

Art. 47[15]. — Prestatorii de servicii de plată trebuie să se asigure că toate domeniile afectate de un proiect TIC sunt reprezentate în echipa de proiect și că echipa de proiect deține cunoștințele necesare pentru a asigura implementarea sigură și cu succes a proiectului.

Art. 47[16]. — (1) Elaborarea și evoluția proiectelor TIC și riscurile lor asociate trebuie raportate organului de conducere, individual sau agregat, în funcție de importanța și de dimensiunea proiectelor TIC, în mod regulat și ad-hoc, după caz.

(2) Prestatorii de servicii de plată trebuie să includă riscul asociat proiectului în cadrul lor de administrare a riscurilor.

SECȚIUNEA a 2-a
Achiziția și dezvoltarea de sisteme TIC

Art. 47[17]. — (1) Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare un proces care să reglementeze achiziția, dezvoltarea și întreținerea sistemelor TIC.

(2) Procesul prevăzut la alin. (1) trebuie conceput folosind o abordare bazată pe riscuri.

Art. 47[18]. — Prestatorii de servicii de plată trebuie să se asigure că, înainte de orice achiziție sau dezvoltare a sistemelor TIC, cerințele funcționale și nefuncționale, inclusiv cerințele de securitate a informațiilor, sunt clar definite și aprobate de către conducerea relevantă.

Art. 47[19]. — Prestatorii de servicii de plată trebuie să instituite măsuri pentru diminuarea riscurilor de modificare neintenționată sau de manipulare intenționată a sistemelor TIC pe durata dezvoltării și implementării în mediul de producție.

Art. 47[20]. — (1) Prestatorii de servicii de plată trebuie să dețină o metodologie pentru testarea și aprobarea sistemelor TIC înainte de prima lor utilizare.

(2) Metodologia prevăzută la alin. (1) trebuie să țină seama de nivelul critic al activelor și proceselor activității de prestare a serviciilor aferente plăților.

(3) Testarea prevăzută la alin. (1) trebuie să asigure faptul că noile sisteme TIC funcționează așa cum au fost proiectate.

(4) Prestatorii de servicii de plată trebuie să utilizeze medii de testare care să reflecte în mod corespunzător mediul de producție.

Art. 47[21]. — Prestatorii de servicii de plată trebuie să testeze sistemele TIC, serviciile TIC și măsurile de securitate a informațiilor, pentru a identifica eventualele puncte slabe, încălcări și incidente TIC operaționale sau de securitate.

Art. 47[22]. — (1) Prestatorii de servicii de plată trebuie să implementeze medii TIC separate pentru a asigura separarea adecvată a sarcinilor și pentru a atenua impactul modificărilor neverificate asupra sistemelor de producție.

(2) Atunci când realizează separarea mediilor conform alin. (1) prestatorii de servicii de plată trebuie asigure inclusiv separarea mediilor de producție de alte medii care nu au legătură cu producția, inclusiv cele de dezvoltare și testare.

(3) Prestatorii de servicii de plată trebuie să asigure integritatea și confidențialitatea datelor de producție în mediile care nu au legătură cu producția. Accesul la datele din mediul de producție este limitat la utilizatorii autorizați.

Art. 47[23]. — (1) Prestatorii de servicii de plată trebuie să pună în aplicare măsuri pentru protejarea integrității codurilor-sursă ale sistemelor TIC dezvoltate intern.

(2) Prestatorii de servicii de plată trebuie să documenteze în mod amănunțit dezvoltarea, implementarea, operarea și/sau configurarea sistemelor TIC, pentru a reduce orice dependență inutilă de experții în domeniu.

(3) Documentația prevăzută la alin. (2) aferentă sistemului TIC trebuie să conțină cel puțin documentația de utilizare, documentația tehnică a sistemului și procedurile de operare, dacă este cazul, inclusiv când nu sunt procese automate.

Art. 47[24]. — (1) Procesele de achiziție și dezvoltare a sistemelor TIC ale unui prestator de servicii de plată trebuie să se aplice și sistemelor TIC dezvoltate sau gestionate de către utilizatorii finali ai liniilor de afaceri din afara organizației TIC (de exemplu, în aplicațiile informatice ale utilizatorilor finali), folosind o abordare bazată pe riscuri.

(2) Prestatorul de servicii de plată trebuie să țină o evidență a aplicațiilor prevăzute la alin. (1) care sprijină procesele și funcțiile critice ale activității de prestare a serviciilor aferente plăților.

SECȚIUNEA a 3-a

Gestionarea modificărilor TIC

Art. 48. — (1) Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare un proces de gestionare a modificărilor TIC pentru a se asigura că toate modificările aduse sistemelor TIC sunt planificate, înregistrate, testate, evaluate, aprobate, implementate și verificate în mod controlat.

(2) Prestatorii de servicii de plată trebuie să gestioneze modificările prevăzute la alin. (1) care sunt necesare și trebuie introduse cât mai curând posibil în timpul situațiilor de urgență, urmând proceduri care să asigure o protecție adecvată.

(3) Prestatorii de servicii de plată trebuie să stabilească dacă modificările la nivelul mediului operațional existent influențează măsurile de securitate prevăzute la art. 25 sau dacă impun adoptarea de măsuri suplimentare pentru atenuarea riscurilor implicate.

(4) Modificările prevăzute la alin. (1) trebuie să fie în conformitate cu procesul formal de gestionare a modificărilor pentru prestatorii de servicii de plată.

CAPITOLUL VII
Gestionarea continuității activității de prestare a serviciilor aferente plăților

SECȚIUNEA 1

Dispoziții generale

Art. 49. — Prestatorii de servicii de plată trebuie să instituie un proces solid de gestionare a continuității activității de prestare a serviciilor aferente plăților pentru a-și maximiza capacitatea de a presta servicii de plată în mod continuu și pentru a limita pierderile în caz de întrerupere gravă a activității de prestare a serviciilor aferente plăților, prin aplicarea în mod corespunzător a prevederilor art. 61—64 din Regulamentul nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare.

SECȚIUNEA a 2-a

Analiza impactului asupra activității de prestare a serviciilor aferente plăților

Art. 50. — (1) Prestatorii de servicii de plată trebuie să realizeze o analiză de impact cu privire la expunerea activității de prestare a serviciilor aferente plăților la întreruperea gravă a acesteia, ca parte a bunei gestionări a continuității activității de prestare a serviciilor aferente plăților.

(2) În cadrul analizei prevăzute la alin. (1) prestatorii de servicii de plată trebuie să evalueze, cantitativ și calitativ, impactul potențial al întreruperii grave a activității de prestare a serviciilor aferente plăților, inclusiv asupra confidențialității, integrității și disponibilității, folosind date interne și/sau externe, inclusiv date de la furnizorii terți, relevante pentru un proces aferent activității de prestare a serviciilor aferente plăților, sau date disponibile public care pot fi relevante pentru analiza de impact asupra activității de prestare a serviciilor aferente plăților și analize pe bază de scenariu.

(3) Analiza de impact asupra activității de prestare a serviciilor aferente plăților realizată conform alin. (1) trebuie să țină seama și de nivelul critic al funcțiilor activității de prestare a serviciilor aferente plăților, al proceselor-suport, al terților și al activelor informaționale identificate și clasificate, precum și de interdependențele acestora, în conformitate cu prevederile art. 16—18.

Art. 50[1]. — Prestatorii de servicii de plată trebuie să se asigure că sistemele și serviciile lor TIC sunt concepute și în concordanță cu analiza lor de impact asupra activității de prestare a serviciilor aferente plăților, inclusiv din perspectiva redundanței anumitor componente critice, pentru a preveni întreruperile cauzate de evenimente cu impact asupra componentelor respective.

SECȚIUNEA a 3-a

Planificarea continuității activității de prestare a serviciilor aferente plăților pe bază de scenariu

Art. 51. — (1) În baza analizei de impact efectuate potrivit prevederilor art. 50, prestatorii de servicii de plată trebuie să implementeze:

a) planuri de continuitate a activității de prestare a serviciilor aferente plăților pentru a se asigura că pot răspunde în mod corespunzător la urgențe și că pot menține activitățile lor operaționale critice;

b) măsuri de atenuare care trebuie adoptate în cazul încetării prestării serviciilor de plată și în cazul rezilierii contractelor existente, pentru evitarea efectelor negative asupra sistemelor de plăți și asupra utilizatorilor de servicii de plată și pentru a asigura executarea operațiunilor de plată în așteptare.

(2) Prestatorii de servicii de plată trebuie să se asigure că planul de continuitate prevăzut la alin. (1) este documentat și aprobat de organele lor de conducere.

(3) Planurile trebuie să țină seama în mod special de riscurile care ar putea afecta în mod negativ sistemele și serviciile TIC.

(4) Prestatorii de servicii de plată trebuie să se asigure că planurile de continuitate a activității de prestare a serviciilor aferente plăților sprijină obiectivele de a proteja și, dacă este cazul, de a restabili confidențialitatea, integritatea și disponibilitatea funcțiilor activității de prestare a serviciilor aferente plăților, a proceselor-suport și a activelor informaționale.

(5) Prestatorii de servicii de plată trebuie să se coordoneze și să coopereze cu părțile relevante de la nivel intern și extern care sunt interesate, după caz, pe parcursul elaborării planurilor de continuitate a activității de prestare a serviciilor aferente plăților.

Art. 51[1]. — (1) Prestatorii de servicii de plată trebuie să pună în aplicare planuri de asigurare a continuității activității de prestare a serviciilor aferente plăților pentru a se asigura că acestea pot reacționa în mod corespunzător la eventuale scenarii de intrare în dificultate și că sunt capabile să își redreseze operațiunile critice ale activității lor de prestare a serviciilor aferente plăților în urma unor întreruperi, conform obiectivului timp de recuperare (*RTO*) și obiectivului punct de recuperare (*RPO*).

(2) Prestatorii de servicii de plată trebuie să stabilească ordinea de prioritate pentru acțiunile specifice din cadrul planului de continuitate a activității de prestare a serviciilor aferente plăților, declanșate ca urmare a unei întreruperi grave a activității de prestare a serviciilor aferente plăților, folosind o abordare bazată pe riscuri, care se poate fundamenta pe evaluările riscurilor efectuate potrivit cap. III al prezentului titlu.

(3) Planurile de asigurare a continuității activității de prestare a serviciilor aferente plăților prevăzute la alin. (1) trebuie să faciliteze cel puțin prelucrarea operațiunilor critice, în timp ce continuă eforturile de remediere.

Art. 52. — (1) Prestatorii de servicii de plată trebuie să ia în considerare o serie de scenarii diferite în planul lor de asigurare a continuității activității de prestare a serviciilor aferente plăților, inclusiv cele extreme, dar plauzibile, la care ar putea fi expuși, inclusiv un scenariu de atac cibernetic, și trebuie să evalueze impactul potențial al unor astfel de scenarii.

(2) Pe baza scenariilor prevăzute la alin. (1), prestatorii de servicii de plată trebuie să descrie modul în care sunt asigurate continuitatea sistemelor și serviciilor TIC și securitatea informațiilor acestora.

SECȚIUNEA a 4-a

Planurile de intervenție și de redresare

Art. 53. — (1) În baza analizei de impact asupra activității de prestare a serviciilor aferente plăților efectuate potrivit prevederilor art. 50 și a scenariilor plauzibile identificate potrivit prevederilor art. 52, prestatorii de servicii de plată trebuie să elaboreze planuri de intervenție și de redresare.

(2) Planurile de intervenție și redresare prevăzute la alin. (1) trebuie:

a) să precizeze condițiile în care poate fi declanșată activarea planurilor și măsurile care trebuie luate pentru a asigura disponibilitatea, continuitatea și redresarea cel puțin a sistemelor și serviciilor TIC critice ale prestatorilor de servicii de plată;

b) să vizeze atingerea obiectivelor de redresare a operațiunilor prestatorilor de servicii de plată;

c) să țină seama atât de opțiunile de redresare pe termen scurt, cât și de cele pe termen lung;

d) să se concentreze pe redresarea operațiunilor funcțiilor critice aferente activității de prestare a serviciilor aferente plăților, proceselor-suport, sistemelor și activelor informaționale, precum și ale interdependențelor dintre acestea pentru a evita efectele negative asupra funcționării prestatorilor de servicii de plată și asupra sistemului financiar, inclusiv asupra sistemelor de plată și asupra utilizatorilor serviciilor de plată, și pentru a asigura executarea operațiunilor de plată în așteptare;

e) să fie documentate și puse la dispoziția unităților operaționale și funcțiilor-suport și ușor accesibile în caz de urgență;

f) să fie actualizate în conformitate cu experiența dobândită din incidente și teste, cu noile riscuri și amenințări identificate, precum și cu prioritățile și obiectivele de redresare modificate;

g) să aibă în vedere și opțiuni alternative, în cazul în care este posibil ca redresarea să nu fie fezabilă pe termen scurt, din cauza costurilor, riscurilor, logisticii sau a situațiilor neprevăzute.

(3) În cadrul planurilor de intervenție și de redresare, prestatorul de servicii de plată trebuie să aibă în vedere și punerea în aplicare a măsurilor de asigurare a continuității pentru a atenua incapacitățile furnizorilor terți, măsuri extrem de importante pentru asigurarea continuității serviciilor TIC ale prestatorului de servicii de plată în concordanță cu dispozițiile Ghidului ABE privind externalizarea EBA/GL/2019/02 referitoare la planurile de continuitate a activității.

SECȚIUNEA a 5-a

Testarea planurilor

Art. 54. — (1) Prestatorii de servicii de plată trebuie să testeze planurile de asigurare a continuității activității de prestare a serviciilor aferente plăților.

(2) Prestatorii de servicii de plată trebuie să se asigure că planurile de asigurare a continuității funcțiilor critice ale activității lor de prestare a serviciilor aferente plăților, ale proceselor-suport, ale activelor informaționale și ale interdependențelor dintre acestea, inclusiv cele furnizate de terți, unde este cazul, sunt testate cel puțin anual potrivit art. 56.

Art. 55. — (1) Prestatorii de servicii de plată trebuie să actualizeze planurile de continuitate a activității de prestare a serviciilor aferente plăților cel puțin anual, pe baza rezultatelor testelor prevăzute la art. 54 alin. (2), a informațiilor privind amenințările curente, a schimbului de informații și a experienței dobândite din evenimentele anterioare.

(2) Orice modificări ale obiectivelor de redresare a activității de prestare a serviciilor aferente plăților (inclusiv ale RTO și RPO) și/sau modificări ale funcțiilor activității lor de prestare a serviciilor aferente plăților, ale proceselor-suport și ale activelor informaționale, dacă este cazul, trebuie să fie luate în considerare, inclusiv ca o bază pentru actualizarea planurilor de asigurare a continuității activității de prestare a serviciilor aferente plăților.

Art. 56. — (1) Testarea planurilor de asigurare a continuității activității de prestare de servicii aferente plăților prevăzută la art. 54 trebuie să demonstreze capacitatea acestora de a susține viabilitatea activității de prestare de servicii aferente plăților a prestatorilor de servicii de plată până la restabilirea operațiunilor lor critice.

(2) Testarea planurilor de asigurare a continuității activității de prestare de servicii aferente plăților prevăzută la alin. (1) trebuie:

a) să includă un set adecvat de scenarii, extreme, dar plauzibile, inclusiv cele avute în vedere la elaborarea planurilor de asigurare a continuității activității de prestare de servicii aferente plăților prevăzute la art. 52, precum și testarea serviciilor prestate de terți, unde este cazul;

b) să includă transferarea funcțiilor critice ale activității de prestare de servicii aferente plăților, ale proceselor-suport și ale activelor informaționale în mediul de redresare în caz de dezastru și demonstrarea faptului că pot fi gestionate astfel o perioadă suficient de reprezentativă și că funcționarea normală poate fi restabilită ulterior;

c) să fie concepute pentru a verifica ipotezele pe care se bazează planurile de asigurare a continuității activității de prestare de servicii aferente plăților, inclusiv mecanismele de guvernanță și planurile de comunicare în situații de criză; și

d) să includă proceduri pentru verificarea capacității personalului și a contractanților, a sistemelor și serviciilor TIC de a răspunde în mod corespunzător la scenariile prevăzute la art. 52.

Art. 57. — Prestatorii de servicii de plată trebuie să documenteze rezultatele testelor și să analizeze, abordeze și să raporteze organului de conducere toate deficiențele identificate în urma testelor.

SECȚIUNEA a 6-a

Comunicările în situații de criză

Art. 58. — Prestatorii de servicii de plată trebuie să se asigure că atât în cazul unei întreruperi a activității lor de prestare de servicii aferente plăților sau al unei situații de urgență, cât și pe parcursul punerii în aplicare a planurilor de asigurare a continuității activității de prestare de servicii aferente plăților au prevăzut măsuri eficiente de comunicare în situații de criză, astfel încât toate părțile interesate interne și externe relevante, inclusiv furnizori de servicii de externalizare, entități din grup sau furnizori terți, precum și Banca Națională a României, sunt informate în timp util și în mod corespunzător.

CAPITOLUL VIII

Gestionarea relației cu utilizatorul serviciilor de plată

Art. 59. — Prestatorii de servicii de plată trebuie să stabilească și să pună în aplicare procese de creștere a gradului de conștientizare al utilizatorilor de servicii de plată cu privire la riscurile de securitate aferente serviciilor de plată prestate acestora, acordând asistență și îndrumare utilizatorilor de servicii de plată.

Art. 60. — Asistența și îndrumarea acordate utilizatorilor de servicii de plată potrivit art. 59 trebuie să fie actualizate în funcție de noile amenințări și vulnerabilități, iar prestatorii de servicii de plată trebuie să informeze utilizatorii de servicii de plată cu privire la aceste modificări.

Art. 61. — În cazul în care funcționalitatea produsului o permite, prestatorii de servicii de plată trebuie să le permită utilizatorilor de servicii de plată să dezactiveze anumite funcționalități de plată aferente serviciilor de plată furnizate de către prestatorul de servicii de plată către utilizatorul de servicii de plată.

Art. 62. — În cazul în care, în conformitate cu art. 163 alin. (1) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, un prestator de servicii de plată a acceptat limitele de cheltuieli ale plătitorului în ceea ce privește operațiunile de plată efectuate prin intermediul anumitor instrumente de plată, prestatorul de servicii de plată trebuie să ofere plătitorului opțiunea de a ajusta aceste limite până la limita maximă admisă.

Art. 63. — Prestatorii de servicii de plată trebuie să acorde utilizatorilor de servicii de plată opțiunea de a primi alerte referitoare la încercările inițiate și/sau eșuate de inițiere a operațiunilor de plată, permițându-le să detecteze utilizarea frauduloasă sau premeditată a conturilor lor de plăți.

Art. 64. — Prestatorii de servicii de plată trebuie să își informeze utilizatorii de servicii de plată despre actualizările procedurilor de securitate care afectează utilizatorii de servicii de plată în ceea ce privește prestarea serviciilor de plată.

Art. 65. — (1) Prestatorii de servicii de plată trebuie să acorde asistență utilizatorilor de servicii de plată în orice solicitări, cereri de sprijin și notificări de anomalii sau aspecte referitoare la probleme de securitate legate de serviciile de plată.

(2) Prestatorii de servicii de plată trebuie să informeze utilizatorii de servicii de plată în mod corespunzător cu privire la modalitatea în care se poate obține asistența prevăzută la alin. (1).”

3. **Articolul 70 se modifică și va avea următorul cuprins:**

„Art. 70. — Prestatorii de servicii de plată trebuie să efectueze evaluarea menționată la art. 66—68 pe bază continuă, pe întreaga durată a existenței incidentului pentru a identifica orice posibilă schimbare a încadrării incidentului, respectiv prin încadrarea incidentului din incident minor în major sau prin încadrarea incidentului din major în minor.”

4. **La articolul 80, alineatul (1) se modifică și va avea următorul cuprins:**

„Art. 80. — (1) În rapoartele lor inițiale, prestatorii de servicii de plată trebuie să includă informațiile prevăzute în formularul «A — Raport inițial» cuprins în anexa nr. 3, prezentând unele caracteristici de bază ale incidentului și consecințele estimate ale acestuia pe baza informațiilor disponibile imediat după detectarea sau reîncadrarea acestuia potrivit art. 70.”

5. **La articolul 91, alineatul (3) se modifică și va avea următorul cuprins:**

„(3) În situația prevăzută la alin. (1), prestatorii de servicii de plată trebuie să indice reîncadrarea incidentului drept minor, să transmită formularul «C — Raport final» cuprins în anexa nr. 3 și să explice motivele acestei încadrări.”

6. **Articolul 103 se modifică și va avea următorul cuprins:**

„Art. 103. — (1) Prestatorii de servicii de plată trebuie să transmită Băncii Naționale a României, prin intermediul Sistemului Informatic de Raportare către Banca Națională a României (*SIRBNR*), datele statistice prevăzute la art. 99, potrivit dispozițiilor cuprinse în cadrul cap. VI din prezentul titlu.

(2) Transmiterea datelor se realizează în format XML, în conformitate cu dispozițiile art. 101 alin. (2) și (3) și cu regulile de sistem stabilite și puse la dispoziția entităților raportoare — prin intermediul SIRBNR — de Banca Națională a României.”

7. **Articolul 105 se modifică și va avea următorul cuprins:**

„Art. 105. — (1) Prestatorii de servicii de plată trebuie să transmită Băncii Naționale a României datele statistice prevăzute la art. 99, prin exprimarea acestora în lei.

(2) Prestatorii de servicii de plată trebuie să raporteze Băncii Naționale a României datele statistice la nivel agregat, incluzând datele aferente activității de prestare de servicii de plată în mod direct în alte state membre și activității desfășurate prin intermediul agenților.

(3) Prestatorii de servicii de plată prevăzuți la art. 223 alin. (1) lit. c), cu excepția furnizorilor specializați în servicii de informare cu privire la conturi, și lit. d) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, din alte state membre, care desfășoară activitate de prestare de servicii de plată pe teritoriul României prin intermediul sucursalelor, raportează Băncii Naționale a României datele statistice prevăzute la art. 99, aferente activității desfășurate de acestea în România, separat de raportarea datelor efectuată de către prestatorul de servicii de plată în statul membru de origine.

(4) Prestatorii de servicii de plată prevăzuți la art. 223 alin. (1) lit. c), cu excepția agenților și a furnizorilor specializați în servicii de informare cu privire la conturi, din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care desfășoară activitate de prestare de servicii de plată pe teritoriul României prin intermediul agenților, nu raportează informațiile și datele statistice către Banca Națională a României.

(5) Fără a aduce atingere alin. (1), în cazul operațiunilor de plată și al operațiunilor de plată frauduloase denominate în monedă străină, prestatorii de servicii de plată determină valorile, inițial, prin aplicarea cursului de schimb pentru moneda respectivă raportat la euro, iar rezultatul în euro este convertit în lei, utilizându-se cursurile de schimb publicate pe website-ul Băncii Centrale Europene. Pentru operațiunile de plată, inclusiv frauduloase, denominate în alte monede decât cele pentru care sunt disponibile cursuri de schimb pe website-ul Băncii Centrale Europene, prestatorii de servicii de plată trebuie să utilizeze cursul de schimb publicat pe website-ul Băncii Naționale a României.

(6) Valorile cursurilor de schimb utilizate pentru conversiile prevăzute la alin. (5) sunt cele aplicate acestor operațiuni sau rata de schimb medie de referință a Băncii Centrale Europene sau a Băncii Naționale a României, după caz, pentru perioada de raportare respectivă.”

8. **Articolul 106 se abrogă.**

9. **Articolul 113 se modifică și va avea următorul cuprins:**

„Art. 113. — Prestatorul de servicii de plată care oferă servicii de emitere de carduri de plată utilizatorilor de servicii de plată în calitate de plătitori trebuie să raporteze, în calitate de emitent, toate operațiunile de plată și operațiunile de plată frauduloase în care s-a folosit un card de plată sau un dispozitiv similar, care au fost inițiate și executate, în conformitate cu formularul «C — Defalcarea datelor pentru operațiunile de plată cu cardul care trebuie raportate de prestatorul de servicii emitent» din anexa nr. 5. Datele aferente categoriilor «Tranzacții inițiate de comerciant» și «Altele» se vor raporta pentru operațiunile de plată inițiate și executate ulterior datei de 01.07.2020.”

10. **Articolul 114 se modifică și va avea următorul cuprins:**

„Art. 114. — Prestatorii de servicii de plată care oferă servicii de acceptare de operațiuni de plată utilizatorilor de servicii de plată în calitate de beneficiari trebuie să raporteze toate operațiunile de plată și operațiunile de plată frauduloase de tip acceptare de operațiuni de plată în care s-a folosit un card de plată sau un dispozitiv similar, care au fost inițiate și executate, în conformitate cu formularul «D — Defalcarea datelor pentru operațiunile de plată cu cardul sau un dispozitiv similar care vor fi raportate de către prestatorul de servicii de plată care acceptă la plată aceste operațiuni de plată (cu o relație contractuală cu utilizatorul serviciului de plată)» din anexa nr. 5. Datele aferente indicatorilor «Tranzacții inițiate de comerciant» și «Altele» se vor raporta pentru operațiunile de plată inițiate și executate ulterior datei de 1.07.2020.”

11. **La articolul 115 alineatul (1), litera d) se modifică și va avea următorul cuprins:**

„d) motivul neaplicării autentificării stricte a clienților, prin indicarea derogărilor de la autentificarea strictă a clienților, prevăzute la cap. 3 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare, sau una din categoriile «Tranzacții inițiate de comerciant» sau «Altele», după caz;”

12. **La articolul 115 alineatul (1), litera f) se modifică și va avea următorul cuprins:**

„f) funcția cardului pentru operațiunile de plată raportate în conformitate cu secțiunile «C — Defalcarea datelor pentru

operațiunile de plată cu cardul care trebuie raportate de prestatorul de servicii de plată emitent» și «D — Defalcarea datelor pentru operațiunile de plată cu cardul sau un dispozitiv similar care vor fi raportate de către prestatorul de servicii de plată care acceptă la plată aceste operațiuni de plată (cu o relație contractuală cu utilizatorul serviciului de plată)» și".

13. **Articolul 117 se modifică și va avea următorul cuprins:**

„Art. 117. — Prestatorii de servicii de plată, care emit instrumente de plată de tipul cardurilor, trebuie să raporteze toate operațiunile de plată și operațiunile de plată frauduloase de tip retragere de numerar efectuate la bancomate (inclusiv prin intermediul aplicațiilor), la ghișeele bancare și la comercianți, utilizând cardurile emise de către aceștia, în conformitate cu formularul «E — Defalcarea datelor pentru retragerile de numerar folosind carduri care vor fi raportate de prestatorul de servicii de plată emitent al cardului» din anexa nr. 5."

14. **La articolul 118, alineatul (1) se modifică și va avea următorul cuprins:**

„Art. 118. — (1) Prestatorii de servicii de plată care nu administrează contul de plăți al utilizatorului de servicii de plată, dar care emit instrumente de plată de tipul cardurilor și execută operațiuni de plăți pe baza acestor carduri trebuie să raporteze datele referitoare la volumul și valoarea aferente acestor operațiuni și ale operațiunilor de plată frauduloase efectuate cu aceste carduri, potrivit formularului «C — Defalcarea datelor pentru operațiunile de plată cu cardul care trebuie raportate de prestatorul de servicii de plată emitent» din anexa nr. 5."

15. **La articolul 119, alineatul (1) se modifică și va avea următorul cuprins:**

„Art. 119. — (1) Prestatorii de servicii de plată care oferă servicii de plată cu monedă electronică trebuie să raporteze operațiunile de plată și operațiunile de plată frauduloasă cu monedă electronică, astfel cum aceasta este definită la art. 4 alin. (1) lit. f) din Legea nr. 210/2019 privind activitatea de emitere de monedă electronică, în conformitate cu formularul «F — Defalcarea datelor pentru operațiunile efectuate cu monedă electronică» din anexa nr. 5. Datele aferente categoriilor «Tranzacții inițiate de comerciant» și «Altele» se vor raporta pentru operațiunile de plată inițiate și executate ulterior datei de 1.07.2020."

16. **La articolul 119 alineatul (3), litera d) se modifică și va avea următorul cuprins:**

„d) motivul neaplicării autentificării stricte a clienților, prin indicarea derogărilor de la autentificarea strictă a clienților, prezentate în capitolul III din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare sau una din categoriile «Tranzacții inițiate de comerciant» sau «Altele», după caz; și".

17. **La anexa nr. 4, punctul 1.6 se modifică și va avea următorul cuprins:**

„1.6. Operațiunile de plată și operațiunile frauduloase de plată în care moneda electronică este transferată de un prestator de servicii de emitere de monedă electronică în contul unui beneficiar al plății, inclusiv în cazurile în care prestatorul de servicii de plată al plătitorului este același cu prestatorul de servicii de plată al beneficiarului, vor fi raportate de prestatorul de servicii de emitere de monedă electronică utilizând formularul «F — Defalcarea datelor pentru operațiunile efectuate în monedă electronică» din anexa nr. 5 la regulament. În cazurile în care prestatorii de servicii de plată sunt diferiți, plata va fi raportată numai de prestatorul de servicii de plată al plătitorului, pentru a evita dubla raportare."

18. **La anexa nr. 4, punctul 2.5 se modifică și va avea următorul cuprins:**

„2.5 În scopul de a evita raportarea dublă, prestatorul de servicii de plată al plătitorului va transmite datele în calitatea sa de emitent (sau inițiator). Prin excepție, datele referitoare la plățile cu cardul vor fi raportate atât de prestatorul de servicii de plată emitent, cât și de prestatorul de servicii de plată care acceptă operațiunea de plată. Cele două perspective trebuie raportate separat, cu defalcări diferite, conform formularelor corespunzătoare prevăzute în anexa nr. 5 la regulament."

19. **La anexa nr. 4, punctul 3.1 se modifică și va avea următorul cuprins:**

„3.1. Pentru operațiunile de plată care nu se bazează pe card și pentru operațiunile de plată la distanță pe bază de card, «operațiunile de plată naționale» se referă la operațiunile de plată inițiate de un plătitor sau de un/printr-un beneficiar al plății, în care prestatorul de servicii de plată al plătitorului/emitent și prestatorul de servicii de plată al beneficiarului/acceptant se află în România."

20. **La anexa nr. 4, punctul 3.2 se modifică și va avea următorul cuprins:**

„3.2. Pentru operațiunile de plată pe bază de card care nu sunt efectuate la distanță, «operațiunile de plată naționale» se referă la operațiunile de plată în care prestatorul de servicii de plată emitent, prestatorul de servicii de plată acceptant și punctul de vânzare sau bancomatul folosit se află în România."

21. **La anexa nr. 4, punctul 3.3 se modifică și va avea următorul cuprins:**

„3.3. Pentru sucursalele din România ale prestatorilor de servicii de plată operațiunile de plată naționale se referă la operațiunile de plată în care atât prestatorii de servicii de plată ai plătitorilor, cât și cei ai beneficiarilor plăților se află în România."

22. **La anexa nr. 4, punctul 3.4 se modifică și va avea următorul cuprins:**

„3.4. Pentru operațiunile de plată care nu se bazează pe card și pentru operațiunile de plată cu cardul la distanță, «operațiunea de plată transfrontalieră în cadrul SEE» se referă la o operațiune de plată inițiată de un plătitor sau de un/printr-un beneficiar al plății, în care prestatorul de servicii de plată al plătitorului/emitent și prestatorul de servicii de plată al beneficiarului plății/acceptant se află în state membre diferite, dintre care unul este situat în România."

23. **La anexa nr. 4, punctul 3.5 se modifică și va avea următorul cuprins:**

„3.5. Pentru operațiunile de plată pe bază de card care nu sunt efectuate la distanță, «operațiunile de plată transfrontaliere în cadrul SEE» se referă la operațiunile de plată în care:

a) prestatorul de servicii de plată emitent și prestatorul de servicii de plată acceptant se află în state membre diferite, dintre care unul este situat în România; sau

b) prestatorul de servicii de plată emitent se află într-un alt stat membru decât punctul de vânzare sau bancomatul, dintre care unul este situat în România."

24. **La anexa nr. 4, punctul 3.6 se modifică și va avea următorul cuprins:**

„3.6. «Operațiunile de plată transfrontaliere în afara SEE» se referă la operațiunile de plată inițiate de un plătitor sau de un/printr-un beneficiar al plății, în care fie prestatorul de servicii de plată al plătitorului, fie cel al beneficiarului plății se află într-un stat terț, iar celălalt se află în România."

25. **Anexa nr. 5 se modifică și va avea cuprinsul din anexa care face parte integrantă din prezentul regulament.**

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

București, 21 mai 2021.
Nr. 2.

Formulare de raportare a datelor privind fraudele

A – Defalcarea datelor pentru operațiunile de transfer credit

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
1.	**Operațiuni de transfer credit**, din care:		
1.1	- Inițiate de prestatorii de servicii de inițiere a plății		
1.2	- Inițiate prin mijloace neelectronice		
1.3	- Inițiate prin mijloace electronice, din care:		
1.3.1	- Inițiate print-un canal de plată la distanță, din care:		
1.3.1.1	**Pentru care se aplică autentificarea strictă a clienților**		
	Din care operațiuni frauduloase de transfer credit în funcție de tipul fraudei		
1.3.1.1.1	- Emiterea unui ordin de plată de către autorul fraudei		
1.3.1.1.2	- Modificarea unui ordin de plată de către autorul fraudei		
1.3.1.1.3	- Manipularea plătitorului de către autorul fraudei pentru a emite un ordin de plată		
1.3.1.2	**Pentru care nu se aplică autentificarea strictă a clienților**		
	Din care operațiuni frauduloase de transfer credit în funcție de tipul fraudei		
1.3.1.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
1.3.1.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
1.3.1.2.3	- Manipularea plătitorului de către autorul fraudei pentru a emite un ordin de plată		
	Din care defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
1.3.1.2.4	- Valoare scăzută[*]		

[*] Art. 16 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

[1)] Anexa este reprodusă în facsimil.

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
1.3.1.2.5	- Plată către sine însuși**		
1.3.1.2.6	- Beneficiar agreat***		
1.3.1.2.7	- Operațiune recurentă****		
1.3.1.2.8	- Utilizarea de procese și protocoale de plată sigure în mediul întreprinderilor*****		
1.3.1.2.9	- Analiza de risc a operațiunilor******		
1.3.2	- Inițiate printr-un canal de plată neefectuată la distanță, din care:		
1.3.2.1	**Pentru care se aplică autentificarea strictă a clienților**		
	Din care operațiuni frauduloase de transfer credit în funcție de tipul fraudei		
1.3.2.1.1	- Emiterea unui ordin de plată de către autorul fraudei		
1.3.2.1.2	- Modificarea unui ordin de plată de către autorul fraudei		
1.3.2.1.3	- Manipularea plătitorului de către autorul fraudei pentru a emite un ordin de plată		
1.3.2.2	**Pentru care nu se aplică autentificarea strictă a clienților**		
	Din care operațiuni frauduloase de transfer credit în funcție de tipul fraudei		
1.3.2.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
1.3.2.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
1.3.2.2.3	- Manipularea plătitorului de către autorul fraudei pentru a emite un ordin de plată		
	Din care defalcate în funcție de motivul neaplicării autentificării stricte a clienților		

** Art. 15 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

*** Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

***** Art. 17 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

****** Art. 18 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

Cod poziție	Denumirea indicatorului		
		Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
1.3.2.2.4	- Plată către sine însuși**		
1.3.2.2.5	- Beneficiar agreat***		
1.3.2.2.6	- Operațiune recurentă****		
1.3.2.2.7	- Plată contactless cu valoare scăzută*******		
1.3.2.2.8	- Terminal neasistat pentru bilete de transport și taxe de parcare********		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	Total pierderi
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciului de plată (plătitor)	
Altele	

Reguli de validare
1 = 1.2 + 1.3; 1.1 nu echivalează cu 1, dar este o submulțime a lui 1
1.3 = 1.3.1 + 1.3.2
1.3.1 = 1.3.1.1 + 1.3.1.2
1.3.2 = 1.3.2.1 + 1.3.2.2

** Art. 15 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

*** Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* Art. 11 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******** Art. 12 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

valoarea operațiunii de plată frauduloase pentru 1.3.1.1 = 1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3
valoarea operațiunii de plată frauduloase pentru 1.3.1.2 = 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3
valoarea operațiunii de plată frauduloase pentru 1.3.2.1 = 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3
valoarea operațiunii de plată frauduloase pentru 1.3.2.2 = 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3
1.3.1.2 = 1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9
1.3.2.2 = 1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8

B - Defalcarea datelor pentru operațiunile executate prin debitare directă

Cod poziție	**Denumirea indicatorului**	**Operațiuni de plată**	**Operațiuni de plată frauduloase**
0	A	B	C
2.	**Debitare directă**, din care:		
2.1	- **Pentru care consimțământul a fost acordat prin mandat electronic**, din care:		
	Debite directe frauduloase în funcție de tipul fraudei:		
2.1.1.1	- Operațiuni de plată neautorizate		
2.1.1.2	- Manipularea plătitorului de către autorul fraudei pentru a-și da consimțământul pentru debitul direct		
2.2	**Pentru care consimțământul a fost acordat altfel decât prin mandat electronic,** din care:		
	Debite directe frauduloase în funcție de tipul fraudei:		
2.2.1.1	- Operațiuni de plată neautorizate		
2.2.1.2	- Manipularea plătitorului de către autorul fraudei pentru a-și da consimțământul pentru debitul direct		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	**Total pierderi**
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciului de plată (beneficiar)	
Altele	

Reguli de validare
2 = 2.1 + 2.2
valoarea operațiunii de plată frauduloase pentru 2.1 = 2.1.1.1 + 2.1.1.2
valoarea operațiunii de plată frauduloase pentru 2.2 = 2.2.1.1 + 2.2.1.2

C- Defalcarea datelor pentru operațiunile de plată cu cardul care trebuie raportate de prestatorul de servicii de plată-**emitent**

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
3 .	**Plăți cu cardul (cu excepția cardurilor care au numai funcția de monedă electronică)**, din care:		
3.1	- Inițiate prin mijloace neelectronice		
3.2	- Inițiate prin mijloace electronice, din care:		
3.2.1	- Inițiate print-un canal de plată la distanță, din care:		
3.2.1.1	*Defalcate după funcția cardului:*		
3.2.1.1.1	- Plăți efectuate cu carduri cu funcție de debit		
3.2.1.1.2	- Plăți efectuate cu carduri cu funcție de credit sau debit amânat		
3.2.1.2	**Pentru care se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
3.2.1.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
3.2.1.2.1.1	- Card pierdut sau furat		
3.2.1.2.1.2	- Card neprimit		
3.2.1.2.1.3	- Card contrafăcut		
3.2.1.2.1.4	- Furtul datelor de pe card		
3.2.1.2.1.5	- Altele		
3.2.1.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
3.2.1.2.3	- Manipularea plătitorului să facă o plată cu cardul		
3.2.1.3	**Pentru care nu se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
3.2.1.3.1	- Emiterea unui ordin de plată de către autorul fraudei		

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
3.2.1.3.1.1	- Card pierdut sau furat		
3.2.1.3.1.2	- Card neprimit		
3.2.1.3.1.3	- Card contrafăcut		
3.2.1.3.1.4	- Furtul datelor de pe card		
3.2.1.3.1.5	- Altele		
3.2.1.3.2	- Modificarea unui ordin de plată de către autorul fraudei		
3.2.1.3.3	- Manipularea plătitorului să facă o plată cu cardul		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
3.2.1.3.4	- Valoare scăzută*		
3.2.1.3.5	- Beneficiar agreat***		
3.2.1.3.6	- Operațiune recurentă****		
3.2.1.3.7	- Utilizarea de procese și protocoale de plată sigure în mediul întreprinderilor*****		
3.2.1.3.8	- Analiza de risc a operațiunilor******		
3.2.1.3.9	- **Tranzacții inițiate de comerciant*******		

* Art. 16 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

*** Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

***** Art. 17 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

****** Art. 18 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* **Tranzacții de plată pe bază de card care îndeplinesc condițiile specificate de către Comisia Europeană în Q&A 2018 4131 și Q&A 2018 4031 sunt considerate ca fiind inițiate de către beneficiar și ca urmare nu se supun prevederilor referitoare la aplicarea autentificării stricte a clienților în conformitate cu art. 97 din Directiva (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare, transpus prin prevederile art. 220 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.**

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
3.2.1.3.10	- **Altele**		
3.2.2	- Inițiate printr-un canal de plată neefectuată la distanță, din care:		
	Defalcate după funcția cardului		
3.2.2.1.1	- Plăți efectuate cu carduri cu funcție de debit		
3.2.2.1.2	- Plăți efectuate cu carduri cu funcție de credit sau debit amânat		
3.2.2.2	**Pentru care se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
3.2.2.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
3.2.2.2.1.1	- Card pierdut sau furat		
3.2.2.2.1.2	- Card neprimit		
3.2.2.2.1.3	- Card contrafăcut		
3.2.2.2.1.4	- Altele		
3.2.2.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
3.2.2.2.3	- Manipularea plătitorului să facă o plată cu cardul		
3.2.2.3	**Pentru care nu se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
3.2.2.3.1	- Emiterea unui ordin de plată de către autorul fraudei		
3.2.2.3.1.1	- Card pierdut sau furat		
3.2.2.3.1.2	- Card neprimit		
3.2.2.3.1.3	- Card contrafăcut		
3.2.2.3.1.4	- Altele		
3.2.2.3.2	- Modificarea unui ordin de plată de către autorul fraudei		
3.2.2.3.3	- Manipularea plătitorului să facă o plată cu cardul		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
3.2.2.3.4	- Beneficiar agreat***		

*** Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
3.2.2.3.5	- Operațiune recurentă****		
3.2.2.3.6	- Plată contactless cu valoare scăzută*******		
3.2.2.3.7	- Terminal neasistat pentru bilete de transport și taxe de parcare********		
3.2.2.3.8	- **Altele**		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	**Total pierderi**
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciului de plată (plătitor)	
Altele	

Reguli de validare
3 = 3.1 + 3.2
3.2 = 3.2.1 + 3.2.2
3.2.1 = 3.2.1.1.1 + 3.2.1.1.2
3.2.1 = 3.2.1.2 + 3.2.1.3
3.2.2 = 3.2.2.1.1 + 3.2.2.1.2
3.2.2 = 3.2.2.2 + 3.2.2.3
valoarea operațiunii de plată frauduloase pentru 3.2.1.2 = 3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3
valoarea operațiunii de plată frauduloase pentru 3.2.1.3 = 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3
valoarea operațiunii de plată frauduloase pentru 3.2.2.2 = 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3
valoarea operațiunii de plată frauduloase pentru 3.2.2.3 = 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* Art. 11 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******** Art. 12 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

valoarea operațiunii de plată frauduloase pentru 3.2.1.2.1 = 3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5
valoarea operațiunii de plată frauduloase pentru 3.2.1.3.1 = 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5
valoarea operațiunii de plată frauduloase pentru 3.2.2.2.1 = 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4
valoarea operațiunii de plată frauduloase pentru 3.2.2.3.1 = 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4
3.2.1.3 = 3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8+ **3.2.1.3.9 + 3.2.1.3.10**
3.2.2.3 = 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7+ **3.2.2.3.8**

D - Defalcarea datelor privitoare la operațiunile de plată cu cardul care vor fi raportate de către prestatorul de servicii de plată **acceptant** (cu o relație contractuală cu utilizatorul serviciului de plată)

Cod poziție	**Denumirea indicatorului**		
		Operațiuni de plată	**Operațiuni de plată frauduloase**
0	A	B	C
4	**Plăți cu cardul acceptate (cu excepția cardurilor care au numai funcția de monedă electronică)**, din care:		
4.1	- Inițiate prin mijloace neelectronice		
4.2	- Inițiate prin mijloace electronice, din care:		
4.2.1	- Acceptate print-un canal la distanță, din care:		
4.2.1.1	*Defalcate după funcția cardului:*		
4.2.1.1.1	- Plăți efectuate cu carduri cu funcție de debit		
4.2.1.1.2	- Plăți efectuate cu carduri cu funcție de credit sau debit amânat		
4.2.1.2	**Pentru care se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
4.2.1.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
4.2.1.2.1.1	- Card pierdut sau furat		
4.2.1.2.1.2	- Card neprimit		
4.2.1.2.1.3	- Card contrafăcut		
4.2.1.2.1.4	- Furtul datelor de pe card		
4.2.1.2.1.5	- Altele		
4.2.1.2.2	- Modificarea unui ordin de plată de către autorul fraudei		

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
4.2.1.2.3	- Manipularea plătitorului să facă o plată cu cardul		
4.2.1.3	**Pentru care nu se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
4.2.1.3.1	- Emiterea unui ordin de plată de către autorul fraudei		
4.2.1.3.1.1	- Card pierdut sau furat		
4.2.1.3.1.2	- Card neprimit		
4.2.1.3.1.3	- Card contrafăcut		
4.2.1.3.1.4	- Furtul datelor de pe card		
4.2.1.3.1.5	- Altele		
4.2.1.3.2	- Modificarea unui ordin de plată de către autorul fraudei		
4.2.1.3.3	- Manipularea plătitorului să facă o plată cu cardul		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
4.2.1.3.4	- Valoare scăzută*		
4.2.1.3.5	- Operațiune recurentă****		
4.2.1.3.6	- Analiza de risc a operațiunilor******		
4.2.1.3.7	- **Tranzacții inițiate de comerciant*******		
4.2.1.3.8	- **Altele**		
4.2.2	- Acceptate printr-un canal de plată neefectuată la distanță, din care:		

* Art. 16 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

****** Art. 18 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* **Tranzacții de plată pe bază de card care îndeplinesc condițiile specificate de către Comisia Europeană în Q&A 2018 4131 și Q&A 2018 4031 sunt considerate ca fiind inițiate de către beneficiar și ca urmare nu se supun prevederilor referitoare la aplicarea autentificării stricte a clienților în conformitate cu art. 97 din Directiva (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare, transpus prin prevederile art. 220 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.**

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
4.2.2.1	*Defalcate după funcția cardului*		
4.2.2.1.1	- Plăți efectuate cu carduri cu funcție de debit		
4.2.2.1.2	- Plăți efectuate cu carduri cu funcție de credit sau debit amânat		
4.2.2.2	**Pentru care se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
4.2.2.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
4.2.2.2.1.1	- Card pierdut sau furat		
4.2.2.2.1.2	- Card neprimit		
4.2.2.2.1.3	- Card contrafăcut		
4.2.2.2.1.4	- Altele		
4.2.2.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
4.2.2.2.3	- Manipularea plătitorului să facă o plată cu cardul		
4.2.2.3	**Pentru care nu se aplică autentificarea strictă a clienților**, din care:		
	Plăți cu cardul frauduloase în funcție de tipul fraudei:		
4.2.2.3.1	- Emiterea unui ordin de plată de către autorul fraudei		
4.2.2.3.1.1	- Card pierdut sau furat		
4.2.2.3.1.2	- Card neprimit		
4.2.2.3.1.3	- Card contrafăcut		
4.2.2.3.1.4	- Altele		
4.2.2.3.2	- Modificarea unui ordin de plată de către autorul fraudei		
4.2.2.3.3	- Manipularea plătitorului să facă o plată cu cardul		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
4.2.2.3.4	- Operațiune recurentă****		
4.2.2.3.5	- Plată contactless cu valoare scăzută*******		

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* Art. 11 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
4.2.2.3.6	- Terminal neasistat pentru bilete de transport și taxe de parcare********		
4.2.2.3.7	- **Altele**		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	**Total pierderi**
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciului de plată (beneficiar)	
Altele	

Reguli de validare
4 = 4.1 + 4.2
4.2 = 4.2.1 + 4.2.2
4.2.1 = 4.2.1.1.1 + 4.2.1.1.2
4.2.1 = 4.2.1.2 + 4.2.1.3
4.2.2 = 4.2.2.1.1 + 4.2.2.1.2
4.2.2 = 4.2.2.2 + 4.2.2.3
valoarea operațiunii de plată frauduloase pentru 4.2.1.2 = 4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3
valoarea operațiunii de plată frauduloase pentru 4.2.1.3 = 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3
valoarea operațiunii de plată frauduloase pentru 4.2.2.2 = 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3
valoarea operațiunii de plată frauduloase pentru 4.2.2.3 = 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3
valoarea operațiunii de plată frauduloase pentru 4.2.1.2.1 = 4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5
valoarea operațiunii de plată frauduloase pentru 4.2.1.3.1 = 4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5
valoarea operațiunii de plată frauduloase pentru 4.2.2.2.1 = 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4
valoarea operațiunii de plată frauduloase pentru 4.2.2.3.1 = 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4

******** Art. 12 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

4.2.1.3 = 4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 + **4.2.1.3.7** + **4.2.1.3.8**
4.2.2.3 = 4.2.2.3.4 + 4.2.2.3.5 + 4.2.2.3.6 + **4.2.2.3.7**

E - Defalcarea datelor privind retragerile de numerar folosind carduri care vor fi raportate de prestatorul de servicii de plată emitent al cardului

Cod poziție	**Denumirea indicatorului**		
		Operațiuni de plată	**Operațiuni de plată frauduloase**
0	A	B	C
5.	**Retrageri de numerar**, din care:		
	Defalcate după funcția cardului, din care:		
5.1	- **Retrageri de numerar** efectuate cu carduri cu funcție de debit		
5.2	- **Retrageri de numerar** efectuate cu carduri cu funcție de credit sau debit amânat		
	Retrageri de numerar *frauduloase efectuate cu cardul în funcție de tipul fraudei*, din care*:*		
5.**3**.1	- Emiterea unui ordin de plată (retragere de numerar) de către autorul fraudei		
5.**3**.1.1	- Card pierdut sau furat		
5.**3**.1.2	- Card neprimit		
5.**3**.1.3	- Card contrafăcut		
5.**3**.1.4	- Altele		
5.**3**.2	- Manipularea plătitorului să facă o retragere de numerar		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	**Total pierderi**
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciului de plată (titularul contului)	
Altele	

Reguli de validare
5 = 5.1 + 5.2
5 = 5.**3**.1 + 5.**3**.2
5.**3**.1 = 5.**3**.1.1 + 5.**3**.1.2 + 5.**3**.1.3 + 5.**3**.1.4

F – Defalcarea datelor pentru operațiunile efectuate în monedă electronică

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
6.	**Operațiuni de plată în monedă electronică**, din care:		
6.1	- **Printr-un canal de inițiere a plății la distanță**		
6.1.1	**Pentru care se aplică autentificarea strictă a clienților,** din care:		
	Operațiuni frauduloase de plată în monedă electronică în funcție de tipul fraudei:		
6.1.1.1	- Emiterea unui ordin de plată de către autorul fraudei		
6.1.1.2	- Modificarea unui ordin de plată de către autorul fraudei		
6.1.1.3	- Manipularea plătitorului de către autorul fraudei să emită un ordin de plată		
6.1.2	**Pentru care nu se aplică autentificarea strictă a clienților,** din care:		
	Operațiuni frauduloase de plată în monedă electronică în funcție de tipul fraudei		
6.1.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
6.1.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
6.1.2.3	- Manipularea plătitorului de către autorul fraudei să emită un ordin de plată		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		
6.1.2.4	- Valoare scăzută[*]		
6.1.2.5	- Beneficiar agreat[***]		
6.1.2.6	- Operațiune recurentă[****]		

[*] Art. 16 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

[***] Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

[****] Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
6.1.2.7	- Plată către sine însuși**		
6.1.2.8	- Utilizarea de procese și protocoale de plată sigure în mediul întreprinderilor*****		
6.1.2.9	- Analiza de risc a operațiunii******		
6.1.2.10	- **Tranzacții inițiate de comerciant*******		
6.1.2.11	- **Altele**		
6.2	**- Inițiate printr-un canal de plată neefectuată la distanță**, din care:		
6.2.1	**Pentru care se aplică autentificarea strictă a clienților**, din care:		
	Operațiuni frauduloase de plată în monedă electronică în funcție de tipul fraudei:		
6.2.1.1	- Emiterea unui ordin de plată de către autorul fraudei		
6.2.1.2	- Modificarea unui ordin de plată de către autorul fraudei		
6.2.1.3	- Manipularea plătitorului de către autorul fraudei să emită un ordin de plată		
6.2.2	**Pentru care nu se aplică autentificarea strictă a clienților**, din care:		
	Operațiuni frauduloase de plată în monedă electronică în funcție de tipul fraudei:		
6.2.2.1	- Emiterea unui ordin de plată de către autorul fraudei		
6.2.2.2	- Modificarea unui ordin de plată de către autorul fraudei		
6.2.2.3	- Manipularea plătitorului de către autorul fraudei să emită un ordin de plată		
	Defalcate în funcție de motivul neaplicării autentificării stricte a clienților		

** Art. 15 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

***** Art. 17 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

****** Art. 18 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* **Tranzacții de plată pe bază de card care îndeplinesc condițiile specificate de către Comisia Europeană în Q&A 2018 4131 și Q&A 2018 4031 sunt considerate ca fiind inițiate de către beneficiar și ca urmare nu se supun prevederilor referitoare la aplicarea autentificării stricte a clienților în conformitate cu art. 97 din Directiva (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare, transpus prin prevederile art. 220 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.**

Cod poziție	Denumirea indicatorului	Operațiuni de plată	Operațiuni de plată frauduloase
0	A	B	C
6.2.2.4	- Beneficiar agreat***		
6.2.2.5	- Operațiune recurentă****		
6.2.2.6	- Plată contactless cu valoare scăzută*******		
6.2.2.7	- Terminal neasistat pentru bilete de transport și taxe de parcare********		
6.2.2.8	- **Altele**		

Pierderi cauzate de fraudă în funcție de purtătorul responsabilității:	Total pierderi
Prestatorul de servicii de plată care emite raportul	
Utilizatorul serviciilor de plată	
Altele	

Reguli de validare
6 = 6.2 + 6.2
6.1 = 6.1.1 + 6.1.2
6.2 = 6.2.1 + 6.2.2
valoarea operațiunii de plată frauduloase pentru 6.1.1 = 6.1.1.1 + 6.1.1.2 + 6.1.1.3
valoarea operațiunii de plată frauduloase pentru 6.1.2 = 6.1.2.1 + 6.1.2.2 + 6.1.2.3
valoarea operațiunii de plată frauduloase pentru 6.2.1 = 6.2.1.1 + 6.2.1.2 + 6.2.1.3
valoarea operațiunii de plată frauduloase pentru 6.2.2 = 6.2.2.1 + 6.2.2.2 + 6.2.2.3

*** Art. 13 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

**** Art. 14 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******* Art. 11 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

******** Art. 12 din Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2.366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

6.1.2 = 6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 **+6.1.2.10 + 6.1.2.11**
6.2.2 = 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 **+6.2.2.8**

G - Defalcarea datelor pentru operațiunile de remitere de bani

Cod poziție	**Denumirea indicatorului**		
		Operațiuni de plată	**Operațiuni de plată frauduloase**
0	A	B	C
7.	**Remiteri de bani**		

H - Defalcarea datelor pentru operațiunile inițiate de prestatorii de servicii de inițiere a plății

Cod poziție	**Denumirea indicatorului**		
		Operațiuni de plată	**Operațiuni de plată frauduloase**
0	A	B	C
8.	**Operațiuni de plată inițiate de prestatori de servicii de inițiere a plății**, din care:		
8.1	- Inițiate printr-un canal de plată la distanță:		
8.1.1	- Pentru care se aplică autentificarea strictă a clienților		
8.1.2	- Pentru care nu se aplică autentificarea strictă a clienților		
8.2	- Inițiate printr-un canal de plată neefectuată la distanță		
8.2.1	- Pentru care se aplică autentificarea strictă a clienților		
8.2.2	- Pentru care nu se aplică autentificarea strictă a clienților		
8.3	- Defalcate după instrumentul de plată		
8.3.1	- Transferuri de credit		
8.3.2	- Altele		

Reguli de validare
8 = 8.1 + 8.2
8 = 8.3.1 + 8.3.2
8.1 = 8.1.1 + 8.1.2
8.2 = 8.2.1 + 8.2.2

ACTE ALE AUTORITĂȚII NAȚIONALE DE REGLEMENTARE ÎN DOMENIUL ENERGIEI

AUTORITATEA NAȚIONALĂ DE REGLEMENTARE ÎN DOMENIUL ENERGIEI

ORDIN
privind aprobarea tarifelor reglementate pentru prestarea serviciului de distribuție realizat de Societatea DELGAZ GRID — S.A.

Având în vedere dispozițiile art. 178 alin. (2) lit. a) și ale art. 179 alin. (4) și (6) din Legea energiei electrice și a gazelor naturale nr. 123/2012, cu modificările și completările ulterioare, precum și ale art. 61 din Metodologia de stabilire a tarifelor reglementate pentru serviciile de distribuție în sectorul gazelor naturale, aprobată prin Ordinul președintelui Autorității Naționale de Reglementare în Domeniul Energiei nr. 217/2018, cu modificările și completările ulterioare,

în temeiul dispozițiilor art. 10 alin. (1) lit. a) și m) din Ordonanța de urgență a Guvernului nr. 33/2007 privind organizarea și funcționarea Autorității Naționale de Reglementare în Domeniul Energiei, aprobată cu modificări și completări prin Legea nr. 160/2012, cu modificările și completările ulterioare,

președintele Autorității Naționale de Reglementare în Domeniul Energiei emite următorul ordin:

Art. 1. — (1) Se aprobă tarifele reglementate pentru prestarea serviciului de distribuție a gazelor naturale clienților care se încadrează în următoarele categorii de consum:

Categoria de clienți	Consum minim anual MWh	Consum maxim anual MWh	Tarife de distribuție lei/MWh
C.1.		≤ 280	30,26
C.2.	> 280	≤ 2.800	28,61
C.3.	> 2.800	≤ 28.000	26,23
C.4.	> 28.000	≤ 280.000	24,25
C.5.	> 280.000		22,90
C.7.	Tarif de tranzit		3,04

(2) Tarifele reglementate prevăzute la alin. (1) se aplică clienților serviciului de distribuție a gazelor naturale din localitățile pentru care Societatea DELGAZ GRID — S.A. deține licența de distribuție a gazelor naturale.

(3) Tarifele reglementate prevăzute la alin. (1) nu conțin acciza pentru gazul natural și T.V.A.

Art. 2. — Operatorul de distribuție licențiat duce la îndeplinire prevederile prezentului ordin, iar compartimentele de resort din cadrul Autorității Naționale de Reglementare în Domeniul Energiei urmăresc respectarea acestuia.

Art. 3. — La data intrării în vigoare a prezentului ordin se abrogă Ordinul președintelui Autorității Naționale de Reglementare în Domeniul Energiei nr. 124/2020 privind aprobarea tarifelor reglementate pentru prestarea serviciului de distribuție realizat de Societatea DELGAZ GRID — S.A., publicat în Monitorul Oficial al României, Partea I, nr. 550 din 25 iunie 2020.

Art. 4. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I, și intră în vigoare la data de 1 iulie 2021.

Președintele Autorității Naționale de Reglementare în Domeniul Energiei,
Dumitru Chiriță

București, 15 iunie 2021.
Nr. 43.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Adresa Biroului pentru relații cu publicul este:
Str. Parcului nr. 65, intrarea A, sectorul 1, București; 012329.
Tel. 021.401.00.73, fax 021.401.00.71 și 021.401.00.72,
e-mail: pierderiacte@ramo.ro, concursurifp@ramo.ro, convocariaga@ramo.ro

MONITORUL OFICIAL

5 948493 325390

Monitorul Oficial al României, Partea I, nr. 599/16.VI.2021 conține 32 de pagini. Prețul: 6,40 lei **ISSN** 1453—4495