TABEL DE CONCORDANȚĂ

1. Actul Uniunii Europene	Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011, publicat în Jurnalul Oficial al Uniunii Europene seria L, nr. 333 din 27 decembrie 2022, CELEX: 32022R2554.
2. Proiectul actului normativ național	Proiectul hotărârii Comitetului executiv al Băncii Naționale a Moldovei pentru aprobarea Regulamentului privind reziliența operațională digitală a sectorului financiar.
3. Gradul general de aplicare prin măsuri naționale	Pus în aplicare parțial
4. Autoritatea responsabilă/grupul de lucru/persoana responsabilă	Banca Națională a Moldovei Ciubotaru Victor, șef direcție, Direcția Managementul Continuității Activității, Securității Informației și Supraveghere în TI
5. Data întocmirii/actualizării	23.11.2026

6. Prevederile Regulamentului/Deciziei UE	**7. Tehnica aplicată (cod)**	**8. Prevederile proiectului**	**9. Prevederile actului/actelor normativ(e) național(e)**	**10. Calificativul de compatibilitate**	**11. Observații/justificări**
CAPITOLUL I Dispoziții generale **Articolul 1. Obiectul** (1) Pentru a atinge un nivel comun ridicat de reziliență operațională digitală, prezentul regulament stabilește cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care sprijină procesele operaționale ale entităților financiare, după cum urmează: (a) cerințe aplicabile entităților financiare în legătură cu: (i) gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC); (ii) raportarea incidentelor majore legate de TIC și notificarea, în mod voluntar, a amenințărilor cibernetice semnificative către autoritățile competente; (iii) raportarea de către entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d) către autoritățile competente a incidentelor operaționale sau de securitate majore legate de plăți; (iv) testarea rezilienței operaționale digitale; (v) schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități; (vi) măsuri pentru buna gestionare a riscurilor TIC generate de părți terțe; (b) cerințe în legătură cu acordurile contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare;	PF	1. În scopul asigurării unui nivel comun ridicat de reziliență operațională digitală, prezentul regulament stabilește cerințe uniforme privind securitatea tehnologiei informației și comunicațiilor (TIC) care sprijină procesele operaționale ale entităților financiare, după cum urmează: 1.1. cerințe aplicabile în legătură cu următoarele: a) gestiunea riscurilor TIC; b) raportarea incidentelor majore legate de TIC și notificarea în mod voluntar a amenințărilor cibernetice semnificative; c) raportarea de către entitățile financiare menționate la subpct. 2.1-2.4 a incidentelor majore operaționale sau de securitate legate de plăți; d) testarea rezilienței operaționale digitale; e) schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități; f) măsuri pentru buna gestionare a riscurilor TIC generate de părți terțe; 1.2. cerințe aferente acordurilor contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare; 1.3. norme privind supravegherea și asigurarea conformității aferente tuturor aspectelor vizate de prezentul regulament.	-	compatibil	Lit. (c) privește cadrul de supraveghere a furnizorilor terți esențiali la nivelul Uniunii, care nu necesită măsuri naționale (art. 31-44). Lit. (d) este redată la subpct. 1.3, în limitele competențelor BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) reguli privind instituirea și desfășurarea cadrului de supraveghere pentru furnizorii terți esențiali de servicii TIC, atunci când furnizează servicii entităților financiare; (d) reguli privind cooperarea între autoritățile competente și norme privind supravegherea și asigurarea conformității de către autoritățile competente în legătură cu toate aspectele vizate de prezentul regulament.					
(2) În ceea ce privește entitățile financiare identificate drept entități esențiale sau importante în temeiul normelor naționale care transpun articolul 3 din Directiva (UE) 2022/2555, prezentul regulament este considerat un act juridic sectorial al Uniunii în sensul articolului 4 din directiva respectivă.	PF	-	**Legea nr. 48/2023 privind securitatea cibernetică, art. 3 alin. (5):** (5) În cazul în care legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele critice, stabilite de către Guvern, prevăd implementarea unor măsuri de securitate sau îndeplinirea obligațiilor de notificare a incidentelor cibernetice cu impact semnificativ, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, se consideră că prevederile legilor respective au caracter special în raport cu prevederile prezentei legi.	prevederi UE neacoperite de măsuri naționale	Legea nr. 48/2023, care transpune art. 4 din Directiva (UE) 2022/2555, recunoaște caracterul special al obligațiilor sectoriale de securitate și de notificare a incidentelor numai dacă acestea sunt prevăzute de legi (art. 3 alin. (5)). Pentru entitățile financiare identificate ca furnizori de servicii, efectul alineatului necesită completarea legilor sectoriale sau a Legii nr. 48/2023, care urmează a fi propusă printr-o inițiativă legislativă ulterioară.
(3) Prezentul regulament nu aduce atingere responsabilității statelor membre în ceea ce privește funcțiile esențiale ale statului cu privire la siguranța publică, apărarea și securitatea națională, în conformitate cu dreptul Uniunii.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind competențele statelor membre în domeniul securității naționale, care nu necesită măsuri de punere în aplicare.
Articolul 2. Domeniul de aplicare (1) Fără a aduce atingere alineatelor (3) și (4), prezentul regulament se aplică următoarelor entități: (a) instituțiile de credit; (b) instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366;	PF	2. Prezentul regulament se aplică următoarelor entități (în continuare – entități financiare): 2.1. instituțiile de credit; 2.2. instituțiile de plată; 2.3. prestatorii de servicii de informare cu privire la conturi; 2.4. instituțiile emitente de monedă electronică;	-	parțial compatibil	Sunt preluate lit. (a)-(d), (n) și (o), adică entitățile supravegheate de BNM (subpct. 2.1-2.6), iar alineatul al doilea al pct. 2 limitează cerințele naționale de la pct. 70-75 la bănci, societăți de

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) prestatorii de servicii de informare cu privire la conturi; (d) instituțiile emitente de monedă electronică, inclusiv instituțiile emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE; (e) firmele de investiții; (f) prestatorii de servicii de criptoactive autorizați în temeiul unui regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 (denumit în continuare „Regulamentul privind piețele criptoactivelor”) și emitenții de tokenuri raportate la active; (g) depozitarii centrali de titluri de valoare; (h) contrapărțile centrale; (i) locurile de tranzacționare; (j) registrele centrale de tranzacții; (k) administratorii de fonduri de investiții alternative; (l) societățile de administrare; (m) furnizorii de servicii de raportare a datelor; (n) întreprinderile de asigurare și de reasigurare; (o) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare; (p) instituțiile pentru furnizarea de pensii ocupaționale; (q) agențiile de rating de credit; (r) administratorii de indici de referință critici; (s) furnizorii de servicii de finanțare participativă; (t) registrele centrale de securitizări; (u) furnizorii terți de servicii TIC.		2.5. societățile de asigurare și societățile de reasigurare; 2.6. intermediarii de asigurări și intermediarii de reasigurări, cu excepția celor care sunt microîntreprinderi, întreprinderi mici sau mijlocii în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii. Prevederile pct. 70-75 nu se aplică entităților financiare menționate la subpct. 2.5 și 2.6 și prestatorilor de servicii de informare cu privire la conturi care prestează doar acest serviciu de plată.			plată și societăți emitente de monedă electronică. Lit. (e)-(m) și (p)-(t) vizează entități care nu se află în supravegherea BNM și urmează a fi acoperite prin actele normative aplicabile acestora. Lit. (f) se acoperă după adoptarea legii privind piața criptoactivelor. Lit. (u) privește cadrul de supraveghere de la nivelul Uniunii (art. 31-44). Legislația națională nu prevede instituții de plată sau instituții emitente de monedă electronică exceptate.
(2) În sensul prezentului regulament, entitățile menționate la alineatul (1) literele (a)-(t) sunt denumite colectiv „entități financiare”.	PF	2. Prezentul regulament se aplică următoarelor entități (în continuare – entități financiare):	-	compatibil	-
(3) Prezentul regulament nu se aplică următoarelor entități: (a) administratorii de fonduri de investiții alternative, astfel cum sunt menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE;	PF	2.5. societățile de asigurare și societățile de reasigurare; 2.6. intermediarii de asigurări și intermediarii de reasigurări, cu excepția celor care sunt microîntreprinderi, întreprinderi mici sau mijlocii în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii.	-	parțial compatibil	Lit. (e) este preluată la subpct. 2.6. Lit. (b) nu se preia, deoarece legislația națională nu prevede regimul întreprinderilor de asigurare de mici

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(b) întreprinderile de asigurare și de reasigurare, astfel cum sunt menționate la articolul 4 din Directiva 2009/138/CE; (c) instituțiile pentru furnizarea de pensii ocupaționale care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total; (d) persoanele fizice sau juridice exceptate în temeiul articolelor 2 și 3 din Directiva 2014/65/UE; (e) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care sunt microîntreprinderi sau întreprinderi mici sau mijlocii; (f) oficiile poștale care efectuează operațiuni de virament, astfel cum sunt menționate la articolul 2 alineatul (5) punctul 3 din Directiva 2013/36/UE.					dimensiuni de la art. 4 din Directiva 2009/138/CE, toate societățile de asigurare și de reasigurare intrând în domeniul de aplicare (subpct. 2.5). Lit. (a), (c), (d) și (f) vizează entități din afara domeniului de aplicare.
(4) Statele membre pot exclude din domeniul de aplicare al prezentului regulament entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE care sunt situate pe teritoriile lor. În cazul în care un stat membru face uz de această opțiune, acesta informează Comisia cu privire la aceasta, precum și cu privire la orice modificare ulterioară. Comisia pune aceste informații la dispoziția publicului pe site-ul său sau prin alte mijloace ușor accesibile.	N/A	-	-	prevederi UE neaplicabile	Opțiune a statelor membre, fără corespondent în legislația națională. Legislația națională nu prevede instituții de credit exceptate în sensul art. 2 alin. (5) din Directiva 2013/36/UE.
Articolul 3. Definiții În sensul prezentului regulament, se aplică următoarele definiții:	PF	3. În sensul prezentului regulament se aplică următoarele definiții:	-	compatibil	-
1. „reziliență operațională digitală” înseamnă capacitatea unei entități financiare de a construi, a asigura și a reevalua integritatea și fiabilitatea sa operațională, prin asigurarea, în mod direct sau indirect, utilizând servicii oferite de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC care sunt necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de o entitate financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora, inclusiv pe întreaga durată a perturbărilor;	PF	3.30. reziliență operațională digitală – capacitatea unei entități financiare de a construi, a asigura și a reevalua integritatea și fiabilitatea sa operațională, prin asigurarea, în mod direct sau indirect, utilizând servicii oferite de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC care sunt necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de entitatea financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora, inclusiv pe întreaga durată a perturbărilor;	-	compatibil	-
2. „rețea și sistem informatic” înseamnă rețea și sistem informatic astfel cum sunt definite la articolul 6 punctul 1 din Directiva (UE) 2022/2555;	PF	3.29. rețea – sisteme de transmisie, indiferent dacă sunt bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, după caz, echipamente de comutare sau de rutare	-	compatibil	Definiția trimite la art. 6 pct. 1 din Directiva (UE) 2022/2555, transpus prin noțiunea „rețea și

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		și alte resurse, inclusiv elemente de rețea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv rețele de comunicații prin satelit, rețele fixe (cu comutare de circuite și cu comutare de pachete, inclusiv internet) și mobile, rețele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, indiferent de tipul de informație transmisă; 3.36. sistem informatic – orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale, precum și datele digitale stocate, prelucrate, recuperate sau transmise de acestea și de rețele în vederea operării, utilizării, protejării și întreținerii datelor respective;			sistem informatic" din art. 2 al Legii nr. 48/2023. Proiectul definește distinct „rețea" (subpct. 3.29) și „sistem informatic" (subpct. 3.36), cu toate elementele noțiunii.
3. „sistem TIC moștenit" înseamnă un sistem TIC ajuns la sfârșitul ciclului său de viață care nu este adecvat pentru a fi modernizat sau reparat, din motive tehnologice sau comerciale, sau pentru care furnizorul său ori un furnizor terț de servicii TIC nu mai oferă asistență, dar care încă este în uz și sprijină funcțiile entității financiare;	PF	3.37. sistem TIC moștenit – un sistem TIC ajuns la sfârșitul ciclului său de viață care nu este adecvat pentru a fi modernizat sau reparat, din motive tehnologice sau comerciale, sau pentru care furnizorul său ori un furnizor terț de servicii TIC nu mai oferă asistență, dar care încă este în uz și sprijină funcțiile entității financiare;	-	compatibil	-
4. „securitatea rețelelor și a sistemelor informatice" înseamnă securitatea rețelelor și a sistemelor informatice astfel cum sunt definite la articolul 6 punctul 2 din Directiva (UE) 2022/2555;	PF	3.34. securitatea rețelelor și a sistemelor informatice – capacitatea unei rețele și a unui sistem informatic de a rezista, la un anumit nivel de încredere, oricărui eveniment care poate compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;	**Legea nr. 48/2023 privind securitatea cibernetică, art. 2:** securitatea rețelelor și sistemelor informatice – capacitate a rețelelor și sistemelor informatice de a rezista, la un anumit nivel de încredere, oricărei acțiuni care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și/sau de sistemele informatice respective sau accesibile prin intermediul acestora;	compatibil	Definiția trimite la art. 6 pct. 2 din Directiva (UE) 2022/2555, al cărui conținut este redat. Noțiunea corespunde celei din art. 2 al Legii nr. 48/2023.
5. „risc TIC" înseamnă orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, dacă se materializează, poate compromite	PF	3.32. risc TIC – orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, dacă se materializează, poate compromite	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiilor și a proceselor sau a furnizării serviciilor prin crearea de efecte negative în mediul digital sau fizic;		securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiilor și a proceselor sau a furnizării serviciilor prin crearea de efecte negative în mediul digital sau fizic;			
6. „activ informațional” înseamnă o colecție de informații, materială sau imaterială, care merită protejată;	PF	3.1. activ informațional – o colecție de informații, materială sau imaterială, care merită protejată;	-	compatibil	-
7. „activ TIC” înseamnă un activ software sau hardware din rețelele și sistemele informatice utilizate de entitatea financiară;	PF	3.2. activ TIC – un activ software sau hardware din rețelele și sistemele informatice utilizate de entitatea financiară;	-	compatibil	-
8. „incident legat de TIC” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitatea financiară care compromit securitatea rețelelor și a sistemelor informatice și care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;	PF	3.13. incident legat de TIC – un eveniment unic sau o serie de evenimente conexe neplanificate de entitatea financiară care compromit securitatea rețelelor și a sistemelor informatice și care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;	-	compatibil	-
9. „incident operațional sau de securitate legat de plăți” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d), legate sau nu de TIC, care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor legate de plăți sau asupra serviciilor legate de plăți furnizate de entitatea financiară;	PF	3.16. incident operațional sau de securitate legat de plăți – un eveniment unic sau o serie de evenimente conexe neplanificate de entitățile financiare menționate la subpct. 2.1-2.4, legate sau nu de TIC, care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor legate de plăți sau asupra serviciilor legate de plăți furnizate de entitatea financiară;	-	compatibil	-
10. „incident major legat de TIC” înseamnă un incident legat de TIC care are un impact negativ puternic asupra rețelelor și sistemelor informatice care sprijină funcțiile critice sau importante ale entității financiare;	PF	3.14. incident major legat de TIC – un incident legat de TIC care are un impact negativ puternic asupra rețelelor și sistemelor informatice care sprijină funcțiile critice sau importante ale entității financiare;	-	compatibil	-
11. „incident major operațional sau de securitate legat de plăți” înseamnă un incident operațional sau de securitate legat de plăți care are un efect negativ puternic asupra serviciilor legate de plăți furnizate;	PF	3.15. incident major operațional sau de securitate legat de plăți – un incident operațional sau de securitate legat de plăți care are un efect negativ puternic asupra serviciilor legate de plăți furnizate;	-	compatibil	-
12. „amenințare cibernetică” înseamnă amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;	PF	3.3. amenințare cibernetică – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau întreruperi la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;	**Legea nr. 48/2023 privind securitatea cibernetică, art. 2:** amenințare cibernetică – circumstanță, eveniment sau acțiune potențială, care ar putea cauza daune, perturba sau avea un alt fel de impact negativ	compatibil	Definiția trimite la art. 2 pct. 8 din Regulamentul (UE) 2019/881, al cărui conținut este redat. Noțiunea corespunde celei din art. 2 al Legii nr. 48/2023.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			asupra rețelelor și sistemelor informatice, asupra utilizatorilor unor astfel de sisteme sau asupra altor persoane;		
13. „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ale cărei caracteristici tehnice indică faptul că ar putea avea ca rezultat un incident major legat de TIC sau un incident major operațional sau de securitate legat de plăți;	PF	3.4. amenințare cibernetică semnificativă – o amenințare cibernetică ale cărei caracteristici tehnice indică faptul că ar putea cauza un incident major legat de TIC sau un incident major operațional sau de securitate legat de plăți;	-	compatibil	-
14. „atac cibernetic” înseamnă un incident rău-intenționat legat de TIC, cauzat prin intermediul unei tentative comise de un factor perturbator care generează amenințări de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține acces neautorizat la un activ ori a utiliza în mod neautorizat un activ;	PF	3.5. atac cibernetic – un incident rău-intenționat legat de TIC, cauzat prin intermediul unei tentative comise de un factor perturbator care generează amenințări de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține acces neautorizat la un activ ori a utiliza în mod neautorizat un activ;	-	compatibil	-
15. „date operative privind amenințările” înseamnă informații care au fost agregate, transformate, analizate, interpretate sau îmbogățite pentru a oferi contextul necesar procesului decizional și pentru a face posibilă o înțelegere adecvată și suficientă cu scopul de a atenua impactul unui incident legat de TIC sau al unei amenințări cibernetice, inclusiv detaliile tehnice ale unui atac cibernetic, persoanele responsabile de atac, modul de operare și motivațiile acestora;	PF	3.7. date operative privind amenințările – informații care au fost agregate, transformate, analizate, interpretate sau îmbogățite pentru a oferi contextul necesar procesului decizional și pentru a face posibilă o înțelegere adecvată și suficientă cu scopul de a atenua impactul unui incident legat de TIC sau al unei amenințări cibernetice, inclusiv detaliile tehnice ale unui atac cibernetic, persoanele responsabile de atac, modul de operare și motivațiile acestora;	-	compatibil	-
16. „vulnerabilitate” înseamnă un punct slab, o sensibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat;	PF	3.44. vulnerabilitate – un punct slab, o sensibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat;	-	compatibil	-
17. „teste de penetrare bazate pe amenințări (TLPT)” înseamnă un cadru care imită tacticile, tehnicile și procedurile utilizate de actorii din viața reală care generează amenințări, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură o testare controlată, personalizată, bazată pe date operative (de tipul „echipa roșie”) a sistemelor critice de producție în timp real ale entității financiare;	PF	3.42. teste de penetrare bazate pe amenințări (TLPT) – un cadru care imită tacticile, tehnicile și procedurile utilizate de actorii din viața reală care generează amenințări, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură o testare controlată, personalizată, bazată pe date operative (de tipul „echipa roșie”) a sistemelor critice de producție în timp real ale entității financiare;	-	compatibil	-
18. „risc TIC generat de părți terțe” înseamnă un risc TIC care poate apărea pentru o entitate financiară în legătură cu utilizarea, de către aceasta, a serviciilor TIC oferite de furnizori terți de servicii TIC sau de subcontractanți ai acestora din urmă, inclusiv prin acorduri de externalizare;	PF	3.33. risc TIC generat de părți terțe – un risc TIC care poate apărea în cadrul unei entități financiare în legătură cu utilizarea, de către aceasta, a serviciilor TIC oferite de furnizori terți de servicii TIC sau de subcontractanți ai acestora din urmă, inclusiv prin acorduri de externalizare;	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
19. „furnizor terț de servicii TIC" înseamnă o întreprindere care furnizează servicii TIC;	PF	3.10. furnizor terț de servicii TIC – o întreprindere care furnizează servicii TIC;	-	compatibil	-
20. „furnizor de servicii TIC intragrup" înseamnă o întreprindere care face parte dintr-un grup financiar și care oferă servicii predominant TIC exclusiv entităților financiare din același grup ori entităților financiare care țin de același sistem instituțional de protecție, inclusiv societăților-mamă ale acestora, filialelor și sucursalelor sau altor entități care sunt în proprietate comună ori sub control comun;	N/A	-	-	prevederi UE neaplicabile	Noțiunea este folosită doar la art. 31 alin. (8), care privește cadrul de supraveghere de la nivelul Uniunii.
21. „servicii TIC" înseamnă servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi în mod continuu, inclusiv hardware ca serviciu și servicii hardware, care includ furnizarea de asistență tehnică prin actualizări de software sau firmware din partea furnizorului de hardware, cu excepția serviciilor de telefonie analogică tradiționale;	PF	3.35. servicii TIC – servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi în mod continuu, inclusiv hardware ca serviciu și servicii hardware, care includ furnizarea de asistență tehnică prin actualizări de software sau firmware din partea furnizorului de hardware, cu excepția serviciilor de telefonie analogică tradiționale;	-	compatibil	-
22. „funcție critică sau importantă" înseamnă o funcție a cărei întrerupere ar afecta în mod semnificativ performanța financiară a unei entități financiare sau soliditatea ori continuitatea serviciilor și activităților sale sau a cărei întrerupere, deficiență sau eșuare în executare ar afecta în mod semnificativ respectarea în continuare, de către o entitate financiară, a condițiilor și obligațiilor aferente autorizației sale sau a altor obligații care îi revin în temeiul dreptului aplicabil în domeniul serviciilor financiare;	PF	3.9. funcție critică sau importantă – o funcție a cărei întrerupere ar afecta în mod semnificativ performanța financiară a unei entități financiare sau soliditatea ori continuitatea serviciilor și activităților sale sau a cărei întrerupere, deficiență sau eșuare în executare ar afecta în mod semnificativ respectarea în continuare, de către entitatea financiară, a condițiilor și obligațiilor aferente autorizației sale sau a altor obligații care îi revin în temeiul dreptului aplicabil în domeniul serviciilor financiare. Funcțiile critice în sensul Legii nr. 232/2016 privind redresarea și rezoluția băncilor sunt considerate funcții critice sau importante;	-	compatibil	Fraza a doua (funcțiile critice în sensul Legii nr. 232/2016) este o precizare națională, care nu restrânge noțiunea.
23. „furnizor terț esențial de servicii TIC" înseamnă un furnizor terț de servicii TIC desemnat drept esențial în conformitate cu articolul 31;	N/A	-	-	prevederi UE neaplicabile	Noțiunea privește desemnarea furnizorilor terți esențiali la nivelul Uniunii (art. 31), pentru care în Republica Moldova nu există un mecanism. Riscul de concentrare (art. 3 pct. 29) este definit fără această noțiune, la subpct. 3.31.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
24. „furnizor terț de servicii TIC stabilit într-o țară terță” înseamnă un furnizor terț de servicii TIC care este o persoană juridică stabilită într-o țară terță și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;	PF	3.11. furnizor terț de servicii TIC stabilit într-un stat terț – un furnizor terț de servicii TIC care este o persoană juridică stabilită într-un stat terț și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;	-	compatibil	„Țară terță” este redată prin „stat terț”, definit la subpct. 3.40.
25. „filială” înseamnă o filială în sensul articolului 2 punctul 10 și al articolului 22 din Directiva 2013/34/UE;	PF	3.8. filială – o întreprindere controlată de o societate-mamă, care deține puterea de a exercita sau exercită efectiv o influență dominantă sau un control asupra acesteia, iar societatea-mamă și filiala au o bază comună de gestionare asigurată de societatea-mamă;	-	compatibil	Definiția trimite la art. 2 pct. 10 din Directiva 2013/34/UE. Proiectul redă noțiunea prin elementele controlului.
26. „grup” înseamnă un grup în sensul articolului 2 punctul 11 din Directiva 2013/34/UE;	PF	3.12. grup – o societate-mamă și toate filialele acesteia;	-	compatibil	Definiția trimite la art. 2 pct. 11 din Directiva 2013/34/UE, al cărui conținut este redat.
27. „societate-mamă” înseamnă o societate-mamă în sensul articolului 2 punctul 9 și al articolului 22 din Directiva 2013/34/UE;	PF	3.39. societate-mamă – o întreprindere care controlează una sau mai multe filiale;	-	compatibil	Definiția trimite la art. 2 pct. 9 din Directiva 2013/34/UE, al cărui conținut este redat.
28. „subcontractant TIC stabilit într-o țară terță” înseamnă un subcontractant TIC care este o persoană juridică stabilită într-o țară terță și care a încheiat un acord contractual fie cu un furnizor terț de servicii TIC, fie cu un furnizor terț de servicii TIC stabilit într-o țară terță;	PF	3.41. subcontractant TIC stabilit într-un stat terț – un subcontractant TIC care este o persoană juridică stabilită într-un stat terț și care a încheiat un acord contractual fie cu un furnizor terț de servicii TIC, fie cu un furnizor terț de servicii TIC stabilit într-un stat terț;	-	compatibil	„Țară terță” este redată prin „stat terț”, definit la subpct. 3.40.
29. „risc de concentrare a serviciilor TIC” înseamnă o expunere la furnizori terți esențiali de servicii TIC individuali sau multipli relaționați, care creează un grad de dependență față de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestor furnizori poate pune în pericol capacitatea unei entități financiare de a oferi funcții critice sau importante ori ar putea genera alte tipuri de efecte negative pentru aceasta, inclusiv pierderi mari sau poate pune în pericol stabilitatea financiară a Uniunii în ansamblu;	PF	3.31. risc de concentrare a serviciilor TIC – o expunere la unul sau mai mulți furnizori terți de servicii TIC relaționați care nu sunt ușor de înlocuit și care creează un grad de dependență față de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestor furnizori poate pune în pericol capacitatea unei entități financiare de a oferi funcții critice sau importante ori ar putea genera alte tipuri de efecte negative pentru aceasta, inclusiv pierderi mari, sau poate pune în pericol stabilitatea financiară a țării;	-	parțial compatibil	În lipsa desemnării furnizorilor terți esențiali (art. 31), expunerea se raportează la furnizorii care nu sunt ușor de înlocuit, criteriul de la pct. 153. Stabilitatea financiară a Uniunii este redată prin stabilitatea financiară a țării.
30. „organ de conducere” înseamnă un organ de conducere astfel cum este definit la articolul 4 alineatul (1) punctul 36 din Directiva 2014/65/UE, la articolul 3 alineatul (1) punctul 7 din Directiva 2013/36/UE, la articolul 2 alineatul (1) litera (s) din Directiva 2009/65/CE a Parlamentului European și al Consiliului, la articolul 2 alineatul (1) punctul 45 din Regulamentul (UE) nr. 909/2014, la articolul 3	PF	3.26. organ de conducere – organele entității financiare numite în conformitate cu legislația aplicabilă, împuternicite să stabilească strategia, obiectivele și orientarea generală ale entității financiare, care supraveghează și monitorizează procesul decizional de conducere, precum și persoanele care conduc în mod efectiv activitatea entității financiare;	-	compatibil	Definiția trimite la actele sectoriale ale Uniunii. Proiectul redă elementele acestora.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
alineatul (1) punctul 20 din Regulamentul (UE) 2016/1011 și în dispozițiile relevante din Regulamentul privind piețele criptoactivelor, sau persoanele echivalente care conduc efectiv entitatea sau dețin funcții-cheie în conformitate cu dreptul Uniunii sau cu dreptul intern relevant;					
31. „instituție de credit" înseamnă o instituție de credit astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului;	PF	3.17. instituție de credit – bancă în sensul art. 3 din Legea nr. 202/2017 privind activitatea băncilor;	**Legea nr. 202/2017 privind activitatea băncilor, art. 3:** bancă – persoană juridică a cărei activitate constă în atragerea de depozite sau de alte fonduri rambursabile de la public și în acordarea de credite în cont propriu;	compatibil	Noțiunea UE este pusă în corespondență cu noțiunea națională „bancă" (art. 54 alin. (4) din Legea nr. 100/2017). Definiția băncii din Legea nr. 202/2017 reproduce art. 4 alin. (1) pct. 1 din Regulamentul (UE) nr. 575/2013.
32. „instituție de credit exceptată în temeiul Directivei 2013/36/UE" înseamnă o entitate astfel cum este menționată la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE;	N/A	-	-	prevederi UE neaplicabile	Noțiune legată de opțiunea de la art. 2 alin. (4). Legislația națională nu prevede instituții de credit exceptate.
33. „firmă de investiții" înseamnă o firmă de investiții astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Directiva 2014/65/UE;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
34. „firmă de investiții mică și neinterconectată" înseamnă o firmă de investiții care îndeplinește condițiile prevăzute la articolul 12 alineatul (1) din Regulamentul (UE) 2019/2033 al Parlamentului European și al Consiliului;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
35. „instituție de plată" înseamnă o instituție de plată astfel cum este definită la articolul 4 punctul 4 din Directiva (UE) 2015/2366;	PF	3.18. instituție de plată – societate de plată în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;	**Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 3:** societate de plată – societate comercială, alta decît banca, furnizorul de servicii poștale sau societatea emitentă de monedă electronică, ce deține licență, în conformitate cu prezenta lege,	compatibil	Noțiunea UE este pusă în corespondență cu noțiunea națională „societate de plată".

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			pentru prestarea serviciilor de plată;		
36. „instituție de plată exceptată în temeiul Directivei (UE) 2015/2366" înseamnă o instituție de plată exceptată în temeiul articolului 32 alineatul (1) din Directiva (UE) 2015/2366;	N/A	-	-	prevederi UE neaplicabile	Legislația națională nu prevede instituții de plată exceptate.
37. „prestator de servicii de informare cu privire la conturi" înseamnă un prestator de servicii de informare cu privire la conturi astfel cum este menționat la articolul 33 alineatul (1) din Directiva (UE) 2015/2366;	PF	3.28. prestator de servicii de informare cu privire la conturi – în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;	**Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 3:** prestator de servicii de informare cu privire la conturi – prestator de servicii de plată care desfășoară activitățile indicate la art. 4 alin. (1) pct. 9);	compatibil	-
38. „instituție emitentă de monedă electronică" înseamnă o instituție emitentă de monedă electronică astfel cum este definită la articolul 2 punctul 1 din Directiva 2009/110/CE;	PF	3.19. instituție emitentă de monedă electronică – societate emitentă de monedă electronică în sensul art. 3 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică;	**Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 3:** societate emitentă de monedă electronică – societate comercială, alta decît banca, ce deține licență, în conformitate cu prezenta lege, pentru emiterea monedei electronice;	compatibil	Noțiunea UE este pusă în corespondență cu noțiunea națională „societate emitentă de monedă electronică".
39. „instituție emitentă de monedă electronică exceptată în temeiul Directivei 2009/110/CE" înseamnă o instituție emitentă de monedă electronică care beneficiază de o exceptare astfel cum se menționează la articolul 9 alineatul (1) din Directiva 2009/110/CE;	N/A	-	-	prevederi UE neaplicabile	Legislația națională nu prevede instituții emitente de monedă electronică exceptate (a se vedea art. 16 alin. (1)).
40. „contraparte centrală" înseamnă o contraparte centrală astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
41. „registru central de tranzacții" înseamnă un registru central de tranzacții astfel cum este definit la articolul 2 punctul 2 din Regulamentul (UE) nr. 648/2012;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
42. „depozitar central de titluri de valoare” înseamnă un depozitar central de titluri de valoare astfel cum este definit la articolul 2 alineatul (1) punctul 1 din Regulamentul (UE) nr. 909/2014;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
43. „loc de tranzacționare” înseamnă un loc de tranzacționare astfel cum este definit la articolul 4 alineatul (1) punctul 24 din Directiva 2014/65/UE;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
44. „administrator de fonduri de investiții alternative” înseamnă un administrator de fonduri de investiții alternative astfel cum este definit la articolul 4 alineatul (1) litera (b) din Directiva 2011/61/UE;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
45. „societate de administrare” înseamnă o societate de administrare astfel cum este definită la articolul 2 alineatul (1) litera (b) din Directiva 2009/65/CE;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
46. „furnizor de servicii de raportare a datelor” înseamnă un furnizor de servicii de raportare a datelor în sensul Regulamentului (UE) nr. 600/2014, astfel cum se menționează la articolul 2 alineatul (1) punctele 34-36;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
47. „întreprindere de asigurare” înseamnă o întreprindere de asigurare astfel cum este definită la articolul 13 punctul 1 din Directiva 2009/138/CE;	PF	2.5. societățile de asigurare și societățile de reasigurare;	**Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 4:** societate de asigurare sau asigurător – persoană juridică care desfășoară activitate de asigurare în baza unei licențe pentru desfășurarea activității de asigurare, acordată de	compatibil	Noțiunea este redată prin „societățile de asigurare” (subpct. 2.5), în sensul Legii nr. 92/2022.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			autoritatea de supraveghere. Noțiunea de societate de asigurare care nu conține sintagma „dintr-un stat terț” se aplică societăților de asigurare cu sediul central în Republica Moldova;		
48. „întreprindere de reasigurare” înseamnă o întreprindere de reasigurare astfel cum este definită la articolul 13 punctul 4 din Directiva 2009/138/CE;	PF	Subpct. 2.5 (transcris la art. 3 pct. 47).	**Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 4:** societate de reasigurare sau reasigurător – persoană juridică care desfășoară activitate de reasigurare în baza unei licențe pentru desfășurarea activității de reasigurare, acordată de autoritatea de supraveghere. Noțiunea de societate de reasigurare care nu conține sintagma „dintr-un stat terț” se aplică societăților de reasigurare cu sediul central în Republica Moldova;	compatibil	Noțiunea este redată prin „societățile de reasigurare” (subpct. 2.5), în sensul Legii nr. 92/2022.
49. „intermediar de asigurări” înseamnă un intermediar de asigurări astfel cum este definit la articolul 2 alineatul (1) punctul 3 din Directiva (UE) 2016/97 a Parlamentului European și a Consiliului;	PF	3.20. intermediar de asigurări – intermediar în asigurări în sensul art. 4 din Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare;	**Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 4:** intermediar în asigurări – persoană fizică sau juridică care desfășoară activitate de intermediere în asigurări în schimbul unei remunerații și care are calitatea de broker de asigurare, agent de asigurare sau agent bancassurance;	compatibil	-
50. „intermediar de asigurări auxiliare” înseamnă un intermediar de asigurări auxiliare astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva (UE) 2016/97;	N/A	-	-	prevederi UE neaplicabile	Categoria intermediarilor de asigurări auxiliare nu există în legislația națională (Legea nr. 92/2022).
51. „intermediar de reasigurări” înseamnă un intermediar de reasigurări astfel cum este definit la articolul 2 alineatul (1) punctul 5 din Directiva (UE) 2016/97;	PF	3.21. intermediar de reasigurări – intermediar în reasigurări în sensul art. 4 din Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare;	**Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 4:**	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			intermediar în reasigurări – broker de reasigurare care desfășoară activitate de intermediere în reasigurări în schimbul unei remunerații;		
52. „instituție pentru furnizarea de pensii ocupaționale” înseamnă o instituție pentru furnizarea de pensii ocupaționale astfel cum este definită la articolul 6 punctul 1 din Directiva (UE) 2016/2341;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
53. „instituție mică pentru furnizarea de pensii ocupaționale” înseamnă o instituție pentru furnizarea de pensii ocupaționale care gestionează scheme de pensii care împreună au mai puțin de 100 de membri în total;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
54. „agenție de rating de credit” înseamnă o agenție de rating de credit astfel cum este definită la articolul 3 alineatul (1) litera (b) din Regulamentul (CE) nr. 1060/2009;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
55. „furnizor de servicii de criptoactive” înseamnă un furnizor de servicii de criptoactive astfel cum este definit în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități. Se acoperă după adoptarea legii privind piața criptoactivelor.
56. „emitent de tokenuri raportate la active” înseamnă un emitent de tokenuri raportate la active astfel cum sunt definite în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități. Se acoperă după adoptarea

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
					legii privind piața criptoactivelor.
57. „administrator de indici de referință critici” înseamnă un administrator de indici de referință critici astfel cum sunt definiți la articolul 3 alineatul (1) punctul 25 din Regulamentul (UE) 2016/1011;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
58. „furnizor de servicii de finanțare participativă” înseamnă un furnizor de servicii de finanțare participativă astfel cum este definit la articolul 2 alineatul (1) litera (e) din Regulamentul (UE) 2020/1503 al Parlamentului European și al Consiliului;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
59. „registru central de securitizări” înseamnă un registru central de securitizări astfel cum este definit la articolul 2 punctul 23 din Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.
60. „microîntreprindere” înseamnă o entitate financiară, alta decât un loc de tranzacționare, o contraparte centrală, un registru central de tranzacții sau un depozitar central de titluri de valoare, care are mai puțin de 10 angajați și o cifră de afaceri anuală și/sau un bilanț anual total care nu depășește 2 milioane EUR;	PF	3.24. microîntreprindere – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;	**Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii, art. 5 alin. (1) lit. a):** (1) În funcție de numărul mediu anual de salariați, de cifra anuală de afaceri sau de totalul activelor pe care le dețin, întreprinderile mici și mijlocii se clasifică în următoarele categorii: a) microîntreprindere – are cel mult 9 salariați și realizează o cifră de afaceri anuală netă ce nu depășește 2 milioane de euro, echivalent în lei moldovenești, sau deține active totale ce nu depășesc 2 milioane de euro, echivalent în lei moldovenești;	compatibil	Criteriile de la art. 5 alin. (1) lit. a) din Legea nr. 179/2016 (cel mult 9 salariați, cifra de afaceri anuală netă sau activele totale de cel mult 2 milioane de euro) corespund definiției. Locurile de tranzacționare, contrapărțile centrale, registrele centrale de tranzacții și depozitarii centrali nu intră în domeniul de aplicare.
61. „supraveghetor principal” înseamnă autoritatea europeană de supraveghere desemnată în	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
conformitate cu articolul 31 alineatul (1) litera (b) din prezentul regulament;					Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.
62. „Comitetul comun” înseamnă comitetul menționat la articolul 54 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010;	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
63. „întreprindere mică” înseamnă o entitate financiară care are cel puțin 10 angajați, dar mai puțin de 50 de angajați, și o cifră de afaceri anuală și/sau un bilanț anual total care depășește 2 milioane EUR, dar nu depășește 10 milioane EUR;	PF	3.22. întreprindere mică – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;	**Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii, art. 5 alin. (1) lit. b):** (1) În funcție de numărul mediu anual de salariați, de cifra anuală de afaceri sau de totalul activelor pe care le dețin, întreprinderile mici și mijlocii se clasifică în următoarele categorii: b) întreprindere mică – are cel puțin 10 și cel mult 49 de salariați și realizează o cifră de afaceri anuală netă ce nu depășește 10 milioane de euro, echivalent în lei moldovenești, sau deține active totale ce nu depășesc 10 milioane de euro, echivalent în lei moldovenești;	compatibil	-
64. „întreprindere mijlocie” înseamnă o entitate financiară care nu este o întreprindere mică și care are mai puțin de 250 de angajați și o cifră de afaceri anuală care nu depășește 50 de milioane EUR și/sau un bilanț anual care nu depășește 43 de milioane EUR;	PF	3.23. întreprindere mijlocie – în sensul art. 5 din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;	**Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii, art. 5 alin. (1) lit. c):** (1) În funcție de numărul mediu anual de salariați, de cifra anuală de afaceri sau de totalul activelor pe care le dețin, întreprinderile mici și mijlocii se clasifică în următoarele categorii: c) întreprindere mijlocie – are minim 50 și cel mult 249 de salariați și realizează o cifră de	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			afaceri anuală netă ce nu depășește 25 de milioane de euro, echivalent în lei moldovenești, sau deține active totale ce nu depășesc 21,5 milioane de euro, echivalent în lei moldovenești.		
65. „autoritate publică” înseamnă orice entitate guvernamentală sau altă entitate a administrației publice, inclusiv băncile centrale naționale.	PF	3.6. autoritate publică – orice entitate guvernamentală sau altă entitate a administrației publice, inclusiv băncile centrale naționale;	-	compatibil	Noțiunea este folosită la pct. 163.
Articolul 4. Principiul proporționalității (1) Entitățile financiare pun în aplicare normele prevăzute la capitolul II în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.	PF	4. Entitățile financiare pun în aplicare normele prevăzute la capitolul II în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.	-	compatibil	-
(2) În plus, entitățile financiare aplică capitolele III și IV și capitolul V secțiunea I proporțional cu dimensiunea și profilul lor general de risc și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, astfel cum se prevede în mod specific în normele relevante din capitolele respective.	PF	5. În plus, entitățile financiare aplică capitolele III, IV și V proporțional cu dimensiunea și profilul lor general de risc și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, astfel cum se prevede în mod specific în normele relevante din capitolele respective.	-	compatibil	Capitolele III, IV și V ale proiectului corespund capitolelor III și IV și secțiunii I a capitolului V din Regulamentul (UE) 2022/2554.
(3) Autoritățile competente iau în considerare aplicarea principiului proporționalității de către entitățile financiare atunci când revizuiesc coerența cadrului de gestionare a riscurilor TIC pe baza rapoartelor prezentate la cererea autorităților competente în temeiul articolului 6 alineatul (5) și al articolului 16 alineatul (2).	PF+CN	6. Banca Națională a Moldovei (în continuare – BNM) ia în considerare aplicarea principiului proporționalității de către entitățile financiare atunci când revizuiește coerența cadrului de gestionare a riscurilor TIC pe baza rapoartelor prezentate la cerere, în temeiul pct. 17.	-	compatibil	Autoritatea competentă este redată prin BNM. Trimiterea la art. 16 alin. (2) nu se preia, întrucât legislația națională nu prevede entitățile cărora li se aplică cadrul simplificat.
CAPITOLUL II Gestionarea riscurilor TIC **Secțiunea I** **Articolul 5. Guvernanță și organizare** (1) Entitățile financiare dispun de un cadru intern de guvernanță și control care asigură o gestionare eficace și prudentă a riscurilor TIC, în conformitate cu articolul 6 alineatul (4), cu scopul de a obține un nivel ridicat de reziliență operațională digitală.	PF	7. Entitățile financiare dispun de un cadru intern de guvernanță și control care asigură o gestionare eficace și prudentă a riscurilor TIC, în conformitate cu pct. 16, cu scopul de a obține un nivel ridicat de reziliență operațională digitală.	-	compatibil	-
(2) Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor dispozițiilor legate de	PF	8. Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
cadrul de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1). În scopul aplicării primului paragraf, organul de conducere: (a) poartă responsabilitatea finală pentru gestionarea riscurilor TIC ale entității financiare; (b) stabilește politici menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor; (c) stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții; (d) poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală, astfel cum este menționată la articolul 6 alineatul (8), inclusiv pentru determinarea nivelul adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum este menționată la articolul 6 alineatul (8) litera (b); (e) aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC ale entității financiare, menționate la articolul 11 alineatul (1) și, respectiv, alineatul (3), care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare; (f) aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare, precum și modificările semnificative aduse acestora; (g) alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante menționate la articolul 13 alineatul (6), precum și competențe TIC pentru toți membrii personalului;		dispozițiilor legate de cadrul de gestionare a riscurilor TIC. În acest scop, organul de conducere: 8.1. poartă responsabilitatea finală pentru gestionarea riscurilor TIC ale entității financiare; 8.2. stabilește politici menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor; 8.3. stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții; 8.4. poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală, astfel cum este menționată la pct. 20, inclusiv pentru determinarea nivelului adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum este menționată la subpct. 20.2; 8.5. aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC ale entității financiare, menționate la pct. 51 și, respectiv, pct. 53, care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare; 8.6. aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare, precum și modificările semnificative aduse acestora; 8.7. alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante menționate la pct. 87, precum și competențe TIC pentru toți membrii personalului; 8.8. aprobă și verifică periodic politica entității financiare cu privire la acordurile privind utilizarea			

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(h) aprobă și verifică periodic politica entității financiare cu privire la acordurile privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC; (i) instituie, la nivel corporativ, canale de raportare care să îi permită să fie informat în mod corespunzător cu privire la: (i) acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC; (ii) orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC; (iii) impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC și impactul acestora, precum și cu privire la măsurile de răspuns, de recuperare și corective.		serviciilor TIC furnizate de furnizori terți de servicii TIC; 8.9. instituie, la nivel corporativ, canale de raportare care să îi permită să fie informat în mod corespunzător cu privire la: a) acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC; b) orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC; c) impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC cu impactul acestora, precum și măsurile de răspuns, de recuperare și corective aplicate.			
(3) Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol pentru a monitoriza acordurile încheiate cu furnizorii terți de servicii TIC cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.	PF	11. Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol pentru a monitoriza acordurile încheiate cu furnizorii terți de servicii TIC cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.	-	compatibil	-
(4) Membrii organului de conducere al entității financiare își actualizează în mod activ cunoștințele și competențele pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, pe măsura riscurilor TIC gestionate.	PF	12. Membrii organului de conducere al entității financiare își actualizează în mod activ cunoștințele și competențele pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, proporționale cu nivelul riscurilor TIC gestionate.	-	compatibil	-
Secțiunea II **Articolul 6. Cadrul de gestionare a riscurilor TIC** (1) Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, ca parte a sistemului lor general de gestionare a riscurilor, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală.	PF	13. Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, ca parte a sistemului lor general de gestionare a riscurilor, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală.	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(2) Cadrul de gestionare a riscurilor TIC include cel puțin strategii, politici, proceduri, precum și protocoale și instrumente TIC care sunt necesare pentru a proteja în mod corespunzător și adecvat toate activele informaționale și toate activele TIC, inclusiv software pentru calculatoare, hardware și servere, precum și pentru a proteja toate componentele și infrastructurile fizice relevante, precum sediile, centrele de date și zonele desemnate sensibile, pentru a asigura că toate activele informaționale și toate activele TIC sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.	PF	14. Cadrul de gestionare a riscurilor TIC include cel puțin strategii, politici, proceduri, precum și procese și instrumente TIC care sunt necesare pentru a proteja în mod corespunzător și adecvat toate activele informaționale și toate activele TIC, inclusiv software pentru calculatoare, hardware și servere, precum și pentru a proteja toate componentele și infrastructurile fizice relevante, cum sunt sediile, centrele de date și zonele desemnate sensibile, pentru a asigura că toate activele informaționale și toate activele TIC sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.	-	compatibil	-
(3) În conformitate cu cadrul lor de gestionare a riscurilor TIC, entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea unor strategii, politici, proceduri, protocoale și instrumente TIC adecvate. Acestea furnizează autorităților competente, la cererea acestora, informații complete și actualizate cu privire la riscurile TIC și la cadrul lor de gestionare a riscurilor TIC.	PF+CN	15. În conformitate cu cadrul lor de gestionare a riscurilor TIC, entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea unor strategii, politici, proceduri, procese și instrumente TIC adecvate. Acestea furnizează BNM, la cerere, informații complete și actualizate cu privire la riscurile TIC și la cadrul lor de gestionare a riscurilor TIC.	-	compatibil	Autoritatea competentă este redată prin BNM.
(4) Entitățile financiare, altele decât microîntreprinderile, atribuie responsabilitatea pentru gestionarea și supravegherea riscurilor TIC unei funcții de control și asigură independența acestei funcții de control la un nivel adecvat, pentru a evita conflictele de interese. Entitățile financiare asigură în mod adecvat separarea și independența a funcțiilor de gestionare a riscurilor TIC, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare sau cu un model intern de gestionare și control al riscurilor.	PF	16. Entitățile financiare, altele decât microîntreprinderile, atribuie responsabilitatea pentru gestionarea și supravegherea riscurilor TIC unei funcții de control și asigură independența acestei funcții de control la un nivel adecvat, pentru a evita conflictele de interese. Entitățile financiare asigură în mod adecvat separarea și independența funcțiilor de gestionare a riscurilor TIC, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare sau cu un model intern de gestionare și control al riscurilor.	-	compatibil	-
(5) Cadrul de gestionare a riscurilor TIC se documentează și se revizuiește cel puțin o dată pe an, sau periodic în cazul microîntreprinderilor, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testarea relevantă a rezilienței operaționale digitale sau din procesele de audit relevante. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport	PF+CN	17. Cadrul de gestionare a riscurilor TIC se documentează și se revizuiește cel puțin o dată pe an, sau periodic în cazul microîntreprinderilor, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testarea relevantă a rezilienței operaționale digitale sau din procesele de audit relevante. Profilul de risc aferent TIC se documentează și se revizuiește cel puțin o dată pe an, precum și în cazul unor modificări majore ale proceselor, sistemelor, serviciilor sau	-	compatibil	Fraza a doua (revizuirea profilului de risc TIC de către toate entitățile financiare, anual și la modificări majore) este o completare națională, preluată din Regulamentul BNM nr. 29/2025 (pct. 77). Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
privind revizuirea cadrului de gestionare a riscurilor TIC.		echipamentelor TIC critice. Cadrul este îmbunătățit în permanență, pe baza experienței acumulate în urma punerii în aplicare și a monitorizării. Entitățile financiare prezintă BNM, la cererea acesteia, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.			
(6) Cadrul de gestionare a riscurilor TIC al entităților financiare, altele decât microîntreprinderile, este supus auditului intern de către auditori în mod regulat, în conformitate cu planul de audit al entităților financiare. Auditorii respectivi dețin suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC, precum și o independență adecvată. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entităților financiare.	PF	18. Cadrul de gestionare a riscurilor TIC al entităților financiare, altele decât microîntreprinderile, este supus auditului intern de către auditori în mod regulat, în conformitate cu planul de audit al entităților financiare. Auditorii respectivi dețin suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC, precum și o independență adecvată. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entităților financiare. 18.1. Entitățile financiare asigură efectuarea auditului, de către auditul intern și/sau extern, într-un interval de cel mult 3 ani, a tuturor sistemelor și serviciilor TIC critice. Auditul se efectuează cel puțin pentru următoarele sisteme, dacă sunt implementate de entitatea financiară: Sistemul automatizat de plăți interne (SAPI), instrumente de plată cu acces la distanță, SWIFT, sistemele de bază (corebanking), sisteme de gestiune a bazelor de date, Active Directory (AD), procesul de gestiune a identităților și accesului, inclusiv privilegiat, sisteme de tip firewall, rețele private virtuale (VPN), sisteme de gestiune electronică a documentelor și mesagerie/comunicare internă și externă. Pentru sistemele și serviciile TIC critice operate de un furnizor terț de servicii TIC sau la nivelul grupului, auditul se poate baza pe rapoarte de asigurare independente care acoperă sistemele și controalele respective în perioada examinată, iar componentele aflate sub controlul entității financiare se auditează potrivit primei fraze.	-	compatibil	Subpct. 18.1 este o prevedere cu specific național, preluată din Regulamentul BNM nr. 29/2025 (pct. 24). Fraza a treia de la subpct. 18.1 (rapoartele de asigurare independente) este o precizare națională.
(7) Pe baza concluziilor evaluării de audit intern, entitățile financiare stabilesc un proces formal de urmărire, care include reguli pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC.	PF	19. Pe baza concluziilor evaluării de audit intern, entitățile financiare stabilesc un proces formal de urmărire, care include reguli pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC. Procesul stabilește, pentru fiecare constatare, acțiunile de	-	compatibil	Fraza a doua (elementele procesului de urmărire) este o completare națională.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		remediere, persoana responsabilă și termenul, iar întârzierile se raportează organului de conducere.			
(8) Cadrul de gestionare a riscurilor TIC include o strategie privind reziliența operațională digitală, care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia privind reziliența operațională digitală include metode de abordare a riscurilor TIC și de realizare a obiectivelor TIC specifice, prin: (a) explicarea modului în care cadrul de gestionare a riscurilor TIC sprijină strategia de afaceri și obiectivele entității financiare; (b) stabilirea nivelului de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul pentru risc al entității financiare, și analizarea toleranței la impact pentru perturbările TIC; (c) stabilirea unor obiective clare privind securitatea informațiilor, inclusiv indicatori-cheie de performanță și indicatori-cheie de risc; (d) explicarea arhitecturii TIC de referință și a oricăror modificări necesare pentru atingerea obiectivelor specifice de activitate; (e) prezentarea diferitelor mecanisme instituite pentru a detecta incidentele legate de TIC, a preveni impactul acestora și a asigura protecție împotriva acestora; (f) evidențierea situației actuale a rezilienței operaționale digitale pe baza numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive; (g) implementarea testării rezilienței operaționale digitale, în conformitate cu capitolul IV din prezentul regulament; (h) conturarea unei strategii de comunicare în cazul producerii unor incidente legate de TIC cu privire la care este necesară informarea în conformitate cu articolul 14.	PF	20. Cadrul de gestionare a riscurilor TIC include o strategie privind reziliența operațională digitală, care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia privind reziliența operațională digitală include metode de abordare a riscurilor TIC și de realizare a obiectivelor TIC specifice, prin: 20.1. explicarea modului în care cadrul de gestionare a riscurilor TIC sprijină strategia de afaceri și obiectivele entității financiare; 20.2. stabilirea nivelului de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul pentru risc al entității financiare, și analizarea toleranței la impact pentru perturbările TIC; 20.3. stabilirea unor obiective clare privind securitatea informațiilor, inclusiv indicatori-cheie de performanță și indicatori-cheie de risc; 20.4. explicarea arhitecturii TIC de referință și a oricăror modificări necesare pentru atingerea obiectivelor specifice de activitate; 20.5. prezentarea diferitelor mecanisme instituite pentru a detecta incidentele legate de TIC, a preveni impactul acestora și a asigura protecție împotriva acestora; 20.6. evidențierea situației actuale a rezilienței operaționale digitale pe baza numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive; 20.7. implementarea testării rezilienței operaționale digitale, în conformitate cu capitolul IV din prezentul regulament; 20.8. conturarea unei strategii de comunicare în cazul producerii unor incidente legate de TIC cu privire la care este necesară informarea.	-	compatibil	-
(9) Entitățile financiare pot defini, în contextul strategiei privind reziliența operațională digitală menționate la alineatul (8), o strategie TIC cuprinzătoare privind existența mai multor furnizori, la nivel de grup sau de entitate, care să prezinte principalele dependențe față de furnizorii terți de servicii TIC și să explice raționamentul care stă la	PF	21. Entitățile financiare pot defini, în contextul strategiei privind reziliența operațională digitală menționate la pct. 20, o strategie TIC cuprinzătoare privind existența mai multor furnizori, la nivel de grup sau de entitate, care să prezinte principalele dependențe față de furnizorii terți de servicii TIC și	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
baza mixului de achiziții de la furnizori terți de servicii TIC.		să explice raționamentul care stă la baza mixului de achiziții de la furnizori terți de servicii TIC.			
(10) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cea națională, sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de verificarea conformității cu cerințele de gestionare a riscurilor TIC.	PF	22. Entitățile financiare pot externaliza, în conformitate cu legislația în vigoare, sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de verificarea conformității cu cerințele de gestionare a riscurilor TIC.	-	compatibil	-
Articolul 7. Sisteme, protocoale și instrumente TIC Pentru a aborda și a gestiona riscurile TIC, entitățile financiare utilizează și mențin sisteme, protocoale și instrumente TIC actualizate care sunt: (a) adecvate magnitudinii operațiunilor care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității astfel cum este menționat la articolul 4; (b) fiabile; (c) dotate cu suficientă capacitate de a prelucra cu precizie datele necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii; (d) reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.	PF	23. Pentru a aborda și a gestiona riscurile TIC, entitățile financiare utilizează și mențin sisteme, procese și instrumente TIC actualizate care sunt: 23.1. adecvate magnitudinii operațiunilor care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității; 23.2. fiabile; 23.3. dotate cu suficientă capacitate de a prelucra cu precizie datele necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii; 23.4. reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.	-	compatibil	-
Articolul 8. Identificare (1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC, activele informaționale și activele TIC care sprijină funcțiile respective, precum și rolurile și dependențele lor în legătură cu riscurile TIC. Entitățile financiare revizuiesc după caz, dar cel puțin anual, caracterul adecvat al acestei clasificări și al oricărei documentări relevante.	PF	30. Ca parte a cadrului de gestionare a riscurilor TIC menționat la pct. 14, entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC, activele informaționale și activele TIC care sprijină funcțiile respective, precum și rolurile și dependențele lor în legătură cu riscurile TIC. Entitățile financiare revizuiesc după caz, dar cel puțin anual, caracterul adecvat al acestei clasificări și al oricărei documentări relevante.	-	compatibil	-
(2) Entitățile financiare identifică în mod constant toate sursele de riscuri TIC, în special expunerea la	PF	31. Entitățile financiare identifică în mod constant toate sursele de riscuri TIC, în special expunerea la	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. Entitățile financiare revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc care au un impact asupra lor.		riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. Entitățile financiare revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc care au un impact asupra lor.			
(3) Entitățile financiare, altele decât microîntreprinderile, efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic și proceselor sau procedurilor care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.	PF	32. Entitățile financiare, altele decât microîntreprinderile, efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic și proceselor sau procedurilor care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.	-	compatibil	-
(4) Entitățile financiare identifică toate activele informaționale și activele TIC, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC.	PF	33. Entitățile financiare identifică toate activele informaționale și activele TIC, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC. Inventarul este suficient de detaliat pentru a permite identificarea imediată a resursei, a amplasamentului acesteia, a proprietarului și a gestionarului resursei TIC.	-	compatibil	Ultima frază (detalierea inventarului) este o completare națională, preluată din Regulamentul BNM nr. 29/2025.
(5) Entitățile financiare identifică și documentează toate procesele care depind de furnizori terți de servicii TIC și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.	PF	34. Entitățile financiare identifică și documentează toate procesele care depind de furnizori terți de servicii TIC și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.	-	compatibil	-
(6) În scopul aplicării alineatelor (1), (4) și (5), entitățile financiare mențin inventarele relevante și le actualizează periodic și de fiecare dată când are loc orice modificare majoră, astfel cum este menționată la alineatul (3).	PF	35. În scopul aplicării pct. 30, 33 și 34, entitățile financiare mențin inventarele relevante și le actualizează periodic și de fiecare dată când are loc orice modificare majoră, astfel cum este menționată la pct. 32.	-	compatibil	-
(7) Entitățile financiare, altele decât microîntreprinderile, efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC moștenite și, în orice caz, înainte și după conectarea tehnologiilor, aplicațiilor sau sistemelor.	PF	36. Entitățile financiare, altele decât microîntreprinderile, efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC moștenite și, în orice caz, înainte și după conectarea unor tehnologii, aplicații sau sisteme. Evaluările riscurilor TIC prevăzute la pct. 31, 32 și la prezentul punct vizează	-	compatibil	Fraza a doua și subpct. 36.1-36.7 sunt prevederi cu specific național, preluate din Regulamentul BNM nr. 29/2025 (pct. 18).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		cel puțin următoarele categorii de riscuri aferente TIC și securității informației: 36.1. riscuri de disponibilitate și continuitate; 36.2. riscuri de securitate; 36.3. riscuri de schimbare; 36.4. riscuri de integritate a datelor; 36.5. riscuri asociate părților terțe și externalizărilor TIC; 36.6. riscuri de conformitate; 36.7. riscuri de concentrare a serviciilor TIC.			
Articolul 9. Protecție și prevenire (1) În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare monitorizează și controlează în mod continuu securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.	PF	37. În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare monitorizează și controlează în mod continuu securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.	-	compatibil	-
(2) Entitățile financiare concep, achiziționează și pun în aplicare politici, proceduri, protocoale și instrumente în domeniul securității TIC care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.	PF	38. Entitățile financiare stabilesc, achiziționează și pun în aplicare politici, proceduri, procese și instrumente în domeniul securității TIC care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.	-	compatibil	-
(3) În vederea realizării obiectivelor menționate la alineatul (2), entitățile financiare utilizează soluții și procese TIC care sunt adecvate în conformitate cu articolul 4. Respectivele soluții și procese TIC: (a) asigură securitatea mijloacelor de transfer al datelor; (b) reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de defecțiuni tehnice care pot împiedica derularea activităților; (c) previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor;	PF	39. În vederea realizării obiectivelor menționate la pct. 38, entitățile financiare utilizează soluții și procese TIC care sunt adecvate în conformitate cu principiul proporționalității. Respectivele soluții și procese TIC: 39.1. asigură clasificarea, declasificarea informațiilor și permit aplicarea marcajelor de confidențialitate pe toată informația ce circulă în cadrul entității financiare; 39.2. asigură securitatea mijloacelor de transfer al datelor; 39.3. reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de	-	compatibil	Subpct. 39.1 este o prevedere cu specific național, preluată din Regulamentul BNM nr. 29/2025 (pct. 27).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(d) asigură protecția datelor împotriva riscurilor care decurg din gestionarea datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane.		defecțiuni tehnice care pot împiedica derularea activităților; 39.4. previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor; 39.5. asigură protecția datelor împotriva riscurilor aferente gestionării datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane.			
(4) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare: (a) elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz; (b) stabilesc, urmând o abordare bazată pe riscuri, o structură de gestionare solidă a rețelei și a infrastructurii care utilizează tehnici, metode și protocoale adecvate ce pot include punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice; (c) pun în aplicare politici care limitează accesul fizic sau logic la activele informaționale și activele TIC la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora; (d) pun în aplicare politici și protocoale pentru mecanisme solide de autentificare, bazate pe standarde relevante și sisteme de control specifice, precum și măsuri de protecție a cheilor criptografice, prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor TIC; (e) pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrii sistemelor sau de securitate, care sunt	PF	40. Ca parte a cadrului de gestionare a riscurilor TIC menționat la pct. 14, entitățile financiare: 40.1. elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz. Politica conține cel puțin: scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare și o descriere a rolurilor și responsabilităților privind gestionarea securității informației; 40.2. stabilesc, urmând o abordare bazată pe riscuri, o structură de gestionare solidă a rețelei și a infrastructurii care utilizează tehnici, metode, procese și proceduri adecvate ce pot include punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice; 40.3. pun în aplicare politici care limitează accesul fizic sau logic la activele informaționale și activele TIC la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora, asigurându-se că acestea conțin cel puțin următoarele principii și măsuri de control: a) utilizatorilor li se acordă drepturi minime de acces, strict necesare pentru executarea sarcinilor; b) acțiunile din cadrul sistemelor informatice și serviciilor TIC critice pot fi atribuite unor utilizatori concreți, iar utilizarea conturilor generice sau partajate este limitată și documentată cu argumentele de rigoare;	-	compatibil	Fraza a doua de la subpct. 40.1, lit. a)-g) de la subpct. 40.3, subpct. 40.7-40.9 și fraza a doua de la pct. 42 sunt prevederi cu specific național, preluate din Regulamentul BNM nr. 29/2025 (pct. 26, 28 și 51-56, subpct. 30.8).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
fondate pe o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat; (f) dispun de politici documentate adecvate și cuprinzătoare pentru corecții și actualizări. În scopul aplicării literei (b) de la primul paragraf, entitățile financiare concep infrastructura de conectare a rețelei într-un mod care permite întreruperea sau segmentarea instantanee a acesteia, pentru a reduce la minimum și a preveni contagiunea, în special în cazul proceselor financiare interconectate. În scopul aplicării literei (e) de la primul paragraf, procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de protocoale specifice.		c) se implementează măsuri de control aferente conturilor privilegiate prin limitarea strictă a utilizării lor și prin monitorizarea permanentă, cu înregistrarea tuturor acțiunilor și activităților efectuate în conturile respective într-un sistem centralizat de gestiune a evenimentelor; d) drepturile de acces ale utilizatorilor sunt acordate, retrase sau modificate în conformitate cu responsabilitățile predefinite, în cadrul unor procese automatizate sau semiautomatizate, documentate, ale entității financiare, care implică obligatoriu proprietarul resursei informaționale. Pe durata concediilor sociale prevăzute de Codul muncii al Republicii Moldova nr. 154/2003 sau a suspendării contractului individual de muncă, precum și în cazul neutilizării conturilor pentru o perioadă mai mare de 60 de zile, conturile utilizatorilor sunt dezactivate, iar în caz de încetare a contractului de muncă, contul este dezactivat și drepturile de acces sunt retrase imediat. În cazul concediilor anuale, conturile privilegiate și drepturile de acces de la distanță ale utilizatorilor se dezactivează implicit, cu excepția cazurilor aprobate de ofițerul de securitate a informației, iar pentru celelalte conturi entitatea financiară stabilește măsurile aplicabile pe baza evaluării riscurilor; e) drepturile de acces la resursele TIC sunt revizuite periodic, la intervale regulate de timp, cel puțin o dată pe an, pentru a se asigura că utilizatorii nu dețin drepturi excesive sau care excedă necesitățile de serviciu; f) se implementează mecanisme de izolare rapidă a resurselor informaționale care au fost afectate de incidente de securitate sau au fost ținta unor atacuri cibernetice. Gradul de automatizare a izolării se stabilește pe baza evaluării riscurilor, ținând cont de caracterul critic al resursei și de cerințele de continuitate. Pentru stațiile de lucru și resursele necritice izolarea poate fi automată, iar pentru sistemele TIC critice decizia de izolare se ia conform procedurilor de răspuns la incidente, cu confirmarea persoanelor responsabile; g) se aplică metode de autentificare proporționale cu importanța sistemelor informatice, a serviciilor			

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		TIC sau a informațiilor accesate, utilizând cel puțin parole complexe pentru conturile obișnuite și autentificarea cu cel puțin doi factori pentru conturile privilegiate aferente sistemelor TIC critice, precum și pentru toate accesările de la distanță; 40.4. pun în aplicare politici și proceduri pentru mecanisme solide de autentificare, bazate pe standarde relevante și sisteme de control specifice, precum și măsuri de protecție a cheilor criptografice, prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor TIC; 40.5. pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrilor sistemelor sau de securitate, care sunt stabilite având o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat; 40.6. dispun de politici documentate, adecvate și cuprinzătoare pentru corecții și actualizări; 40.7. stabilesc, pe baza unei abordări bazate pe riscuri, procese și proceduri privind achiziția, dezvoltarea și mentenanța sistemelor TIC, care asigură că, înainte de orice achiziție sau dezvoltare, cerințele funcționale și nefuncționale, inclusiv cerințele minime de securitate a informației, sunt clar definite și aprobate de organul de conducere sau de persoana ori funcția desemnată de acesta, în funcție de nivelul de risc; 40.8. aplică măsuri de control împotriva modificării neintenționate sau a manipulării intenționate a sistemelor TIC pe durata dezvoltării și a implementării în mediul de producție și asigură separarea responsabilităților de dezvoltare, testare și implementare; 40.9. aplică o metodologie de testare și aprobare a sistemelor TIC noi sau modificate, care asigură că acestea funcționează conform proiectării și că			

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		mediile de testare reflectă în mod corespunzător mediul de producție. 41. În scopul aplicării subpct. 40.2, entitățile financiare stabilesc o infrastructură de conectare a rețelei într-un mod care permite întreruperea sau segmentarea instantanee a acesteia, pentru a reduce la minimum și a preveni contagiunea, în special în cazul proceselor financiare interconectate. 42. În scopul aplicării subpct. 40.5, procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de proceduri specifice. Procesul include proceduri pentru gestionarea modificărilor în situații de urgență, care asigură un nivel adecvat de protecție.			
Articolul 10. Detectare (1) Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu articolul 17, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative. Toate mecanismele de detectare menționate la primul paragraf sunt testate cu regularitate în conformitate cu articolul 25.	PF	43. Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu pct. 92-94, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative. Toate mecanismele de detectare sunt testate cu regularitate, în conformitate cu pct. 117. Evenimentele de securitate relevante pentru eventuale investigații, generate de toate sistemele și serviciile TIC critice, sunt colectate în soluții specializate care le asigură integritatea și disponibilitatea. Mecanismele de detectare includ sisteme de prevenire și detectare a intruziunilor.	-	compatibil	Fraza a treia (colectarea centralizată a evenimentelor de securitate) este o completare națională, preluată din Regulamentul BNM nr. 29/2025 (pct. 41). Fraza a patra (sistemele de prevenire și detectare a intruziunilor) este o completare națională, preluată din Regulamentul BNM nr. 29/2025 (subpct. 30.2).
(2) Mecanismele de detectare menționate la alineatul (1) permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare și inițiere a proceselor de răspuns la incidentele legate de TIC, inclusiv mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC.	PF	49. Mecanismele de monitorizare și detectare permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare și inițiere a proceselor de răspuns la incidentele legate de TIC, inclusiv mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC. 49.1. Instituțiile de credit utilizează, ca nivel suplimentar de control al mecanismelor de monitorizare și detectare, soluții de analiză a evenimentelor de securitate bazate pe tehnici de inteligență artificială, cum sunt modelele de învățare automată, care identifică tipare și anomalii fără a se	-	compatibil	Subpct. 49.1-49.5 (analiza evenimentelor de securitate cu tehnici de inteligență artificială, pentru instituțiile de credit) sunt o prevedere cu specific național.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		limita la reguli de detectare definite explicit. Soluțiile analizează, fără a afecta funcționarea sistemelor monitorizate, cel puțin evenimentele de securitate colectate potrivit pct. 43 de la sistemele și serviciile TIC critice și asigură: a) corelarea automată a evenimentelor provenite din surse multiple, inclusiv din sistemele de gestionare a identităților și a accesului, din infrastructura de rețea și din sistemele de securitate; b) identificarea comportamentelor anormale și a tiparelor suspecte, inclusiv a legăturilor dintre evenimente care, analizate separat, nu generează alerte; c) clasificarea și prioritizarea alertelor în funcție de riscul estimat, cu indicarea evenimentelor care au stat la baza fiecărei alerte; d) păstrarea rezultatelor analizei și a alertelor generate pe perioada prevăzută la pct. 68, pentru trasabilitate și pentru evaluarea eficacității detectării. 49.2. Prelucrarea evenimentelor de securitate de către soluțiile prevăzute la subpct. 49.1, inclusiv executarea modelelor, are loc în infrastructura TIC proprie a instituției de credit, aflată sub controlul său direct, sau, în cazul prevăzut la subpct. 49.3, în infrastructura TIC proprie a grupului din care face parte. În scopul acestei analize, evenimentele de securitate, informațiile extrase din ele și rezultatele prelucrării nu se transmit către servicii de prelucrare sau de inferență furnizate în afara acestei infrastructuri. Soluțiile pot primi din surse externe actualizări ale modelelor și ale regulilor de detectare, fără transmiterea către acestea a datelor prelucrate. 49.3. Instituția de credit care face parte dintr-un grup poate utiliza soluția prevăzută la subpct. 49.1 operată de societatea-mamă sau de o altă entitate din grup, dacă sunt îndeplinite cumulativ următoarele condiții: a) infrastructura TIC în care are loc prelucrarea se află sub controlul direct al grupului și este amplasată pe teritoriul Republicii Moldova sau al			

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		unui stat membru al Uniunii Europene ori al Spațiului Economic European; b) acordul cu entitatea din grup care operează soluția respectă cerințele capitolului V, inclusiv drepturile de acces, de inspecție și de audit ale instituției de credit și ale BNM prevăzute la subpct. 161.5; c) instituția de credit are acces permanent la alertele și la rezultatele analizei care o privesc, precum și la evenimentele care au stat la baza acestora; d) soluția îndeplinește cerințele prevăzute la subpct. 49.1. 49.4. Instituțiile de credit validează modelele înainte de utilizarea lor în mediul de producție și le reevaluează cel puțin o dată pe an și după orice modificare semnificativă, ca parte a testării mecanismelor de detectare prevăzute la pct. 43. Validarea și reevaluarea verifică cel puțin capacitatea de identificare a activităților anormale, ponderea alertelor fals pozitive și fals negative, rezistența modelelor la manipularea datelor de intrare și riscurile de securitate asociate utilizării lor. În cazul prevăzut la subpct. 49.3, validarea și reevaluarea pot fi efectuate la nivelul grupului, iar rezultatele lor se pun la dispoziția instituției de credit. 49.5. Soluțiile prevăzute la subpct. 49.1 completează celelalte mecanisme de monitorizare și detectare, fără a le înlocui, și nu înlocuiesc analiza alertelor de către personalul cu atribuții de monitorizare și de răspuns la incidente (pct. 50 și subpct. 94.3). Acțiunile de răspuns cu impact semnificativ asupra sistemelor TIC nu se aplică numai pe baza rezultatelor acestor soluții, fără confirmarea persoanelor responsabile, cu excepția mecanismelor automate de răspuns aprobate în prealabil potrivit subpct. 40.3 lit. f).			
(3) Entitățile financiare alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.	PF	50. Entitățile financiare alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(4) Furnizorii de servicii de raportare a datelor dispun, în plus, de sisteme care pot verifica în mod eficace integralitatea rapoartelor de tranzacționare, pot identifica omisiunile și erorile evidente și pot solicita retransmiterea rapoartelor respective.	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează furnizorii de servicii de raportare a datelor, care nu se află în supravegherea BNM.
Articolul 11. Răspuns și recuperare (1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1) și pe baza cerințelor de identificare prevăzute la articolul 8, entitățile financiare instituie o politică cuprinzătoare de continuitate a activității TIC, care poate fi adoptată sub forma unei politici specifice dedicate, ca parte integrantă a politicii generale de continuitate a activității a entității financiare.	PF	51. Ca parte a cadrului de gestionare a riscurilor TIC și pe baza cerințelor de identificare, entitățile financiare instituie o politică cuprinzătoare de continuitate a activității TIC, care poate fi adoptată sub forma unei politici specifice dedicate sau ca parte integrantă a politicii generale de continuitate a activității entității financiare. Politica conține cel puțin scopul, obiectivele, domeniul de aplicare, principiile generale de aplicare și o descriere a rolurilor și responsabilităților privind gestionarea continuității activității în cadrul entității financiare.	-	compatibil	Fraza a doua este o completare națională, preluată din Regulamentul BNM nr. 29/2025.
(2) Entitățile financiare pun în aplicare politica de continuitate a activității TIC prin măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate care vizează: (a) asigurarea continuității funcțiilor critice sau importante ale entității financiare; (b) un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare; (c) activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare adecvate pentru fiecare tip de incident legat de TIC și previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate, stabilite în conformitate cu articolul 12; (d) estimarea efectelor, a daunelor și a pierderilor preliminare; (e) stabilirea unor măsuri de comunicare și de gestionare a crizelor care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante, în conformitate cu articolul 14, și raportarea către autoritățile competente, în conformitate cu articolul 19.	PF	52. Entitățile financiare pun în aplicare politica de continuitate a activității TIC prin regulamente, măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate care vizează: 52.1. inventarierea tuturor proceselor de activitate și identificarea celor ce sunt critice din punctul de vedere al derulării continue în timp; 52.2. evaluarea impactului pe care îl pot avea întreruperile în procesele identificate asupra activității entității financiare; 52.3. stabilirea indicatorilor de continuitate aferenți proceselor prin specificarea PMIT pentru procesele de activitate; 52.4. identificarea proceselor critice în timp și stabilirea resurselor necesare pentru derularea normală a acestora, în particular: resurse de personal, sisteme și resurse TIC, încăperi, alte resurse; 52.5. stabilirea indicatorilor de continuitate pentru toate sistemele și serviciile TIC critice prin indicarea TOR și MOR; 52.6. analiza riscurilor de continuitate ce pot duce la întreruperea proceselor critice. Implicit se analizează riscurile de bază ce presupun indisponibilitatea resurselor necesare pentru desfășurarea normală a proceselor;	-	compatibil	Subpct. 52.1-52.8 și completarea de la subpct. 52.9 sunt prevederi cu specific național, preluate din Regulamentul BNM nr. 29/2025 (pct. 58).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		52.7. stabilirea strategiilor de continuitate pentru desfășurarea proceselor critice în timp în condițiile în care riscurile au fost identificate. Se iau în considerare cel puțin două strategii de continuitate: restabilirea resurselor critice sau aplicarea procedurilor alternative de lucru; 52.8. clasificarea proceselor critice în grupe de urgență în baza indicatorilor PMIT, pentru a stabili prioritățile acțiunilor de restabilire când sunt afectate sau întrerupte mai multe procese simultan; 52.9. asigurarea continuității funcțiilor critice sau importante ale entității financiare în baza rezultatelor obținute conform subpct. 52.1-52.8; 52.10. un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare; 52.11. activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare a impactului, adecvate pentru fiecare tip de incident legat de TIC și previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate și stabilite; 52.12. estimarea efectelor, a daunelor și a pierderilor preliminare; 52.13. stabilirea unor măsuri de comunicare și de gestionare a crizelor care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante și raportarea către BNM, în conformitate cu pct. 98-103.			
(3) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC asociate care, în cazul altor entități financiare decât microîntreprinderile, sunt supuse unor evaluări de audit intern independente.	PF	53. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC asociate, care, în cazul altor entități financiare decât microîntreprinderile, sunt supuse unor evaluări de audit intern independente.	-	compatibil	-
(4) Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, în special în ceea ce privește funcțiile	PF	54. Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, în special în ceea ce privește funcțiile	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC.		critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC.			
(5) Ca parte a politicii generale de continuitate a activității, entitățile financiare efectuează o analiză a impactului asupra activității (AIA) al expunerilor lor la perturbări grave ale activității. În conformitate cu AIA, entitățile financiare evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii, după caz. AIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora. Entitățile financiare se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu AIA, în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice.	PF	56. Ca parte a politicii generale de continuitate a activității, entitățile financiare efectuează o analiză a impactului asupra activității (BIA) al expunerilor lor la perturbări grave ale activității. În conformitate cu BIA, entitățile financiare evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii, după caz. BIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora. Entitățile financiare se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu BIA, în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice. Pe baza BIA, entitățile financiare identifică sistemele și serviciile TIC critice din perspectiva continuității și disponibilității, cărora li se aplică subpct. 52.5 și pct. 64, 74 lit. d), 75 și 76. Pentru sistemele și serviciile TIC critice doar din perspectiva securității informației, copiile de rezervă se stabilesc pe baza evaluării riscurilor.	-	compatibil	Alineatul al doilea (sistemele critice din perspectiva continuității și disponibilității, cărora li se aplică cerințele naționale de continuitate) este o precizare națională.
(6) Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare: (a) testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC în legătură cu sistemele TIC care sprijină toate funcțiile cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC care sprijină funcții critice sau importante; (b) testează planurile de comunicare în situații de criză instituite în conformitate cu articolul 14. În scopul aplicării literei (a) de la primul paragraf, entitățile financiare altele decât microîntreprinderile includ în planurile de testare scenarii de atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la articolul 12.	PF	57. Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare: 57.1. testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC în legătură cu sistemele TIC care sprijină toate funcțiile cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC care sprijină funcții critice sau importante. Rezultatele testărilor sunt documentate adecvat, cu păstrarea probelor comprehensive, și sunt raportate organului de conducere. Testarea vizează cel puțin continuitatea sistemelor și a infrastructurii TIC, a rolurilor și a personalului, a infrastructurii non-TIC (alimentarea cu energie electrică, protecția împotriva incendiilor, sistemele de alarmă și de climatizare), cunoașterea planurilor de către personalul responsabil și, după	-	compatibil	Frazele a doua și a treia de la subpct. 57.1 (documentarea testelor și conținutul minim al testării) sunt completări naționale, preluate din Regulamentul BNM nr. 29/2025 (pct. 58.12). Frazele a patra și a cincea de la subpct. 57.1 (eșalonarea elementelor naționale, cel puțin o dată la 2 ani, și recunoașterea testărilor de la pct. 61 și 62) sunt precizări naționale.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Entitățile financiare își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC, ținând seama de rezultatele testelor efectuate în conformitate cu primul paragraf, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.		caz, reluarea proceselor critice în locația de rezervă. Testarea rolurilor și a personalului, a infrastructurii non-TIC și a reluării proceselor critice în locația de rezervă poate fi eșalonată, cu condiția ca fiecare element să fie testat cel puțin o dată la 2 ani. Testarea efectuată potrivit pct. 61 sau 62 se consideră parte a testării anuale pentru sistemele, serviciile și procesele pe care le acoperă; 57.2. testează planurile de comunicare în situații de criză instituite; 57.3. cu excepția microîntreprinderilor, includ în planurile de testare prevăzute la subpct. 57.1 scenarii de atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la pct. 63-79; 57.4. își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC, ținând seama de rezultatele testelor efectuate în conformitate cu subpct. 57.1 și 57.2, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.			
(7) Entitățile financiare altele decât microîntreprinderile au o funcție de gestionare a crizelor, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză, în conformitate cu articolul 14.	PF	58. Entitățile financiare, altele decât microîntreprinderile, au o funcție de gestionare a crizelor, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză.	-	compatibil	-
(8) Entitățile financiare păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor perturbatoare atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.	PF	59. Entitățile financiare păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor de continuitate atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.	-	compatibil	-
(9) Depozitarii centrali de titluri de valoare furnizează autorităților competente copii ale rezultatelor testelor privind continuitatea activității TIC sau ale unor exerciții similare.	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
					normative aplicabile acestor entități.
(10) Entitățile financiare, altele decât microîntreprinderile, raportează autorităților competente, la cererea acestora, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.	PF+CN	60. Entitățile financiare, altele decât microîntreprinderile, raportează către BNM, la cererea acesteia, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.	-	compatibil	Autoritatea competentă este redată prin BNM.
(11) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES elaborează, prin intermediul Comitetului comun, până la 17 iulie 2024, orientări comune privind estimarea costurilor și pierderilor anuale agregate menționate la alineatul (10).	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
Articolul 12. Politici și proceduri privind copiile de rezervă și proceduri și metode de restaurare și recuperare (1) Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează și documentează: (a) politici și proceduri privind copiile de rezervă care precizează sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau al nivelului de confidențialitate al datelor; (b) proceduri și metode de restaurare și recuperare.	PF	63. Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează și documentează: 63.1. politici și proceduri privind copiile de rezervă care precizează sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau al nivelului de confidențialitate al datelor; 63.2. proceduri și metode de restaurare și recuperare.	-	compatibil	-
(2) Entitățile financiare instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. Periodic se efectuează testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare.	PF	65. Entitățile financiare instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. Testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare se efectuează periodic, cel puțin o dată pe an. Entitățile	-	compatibil	Frecvența anuală a testării și verificarea integrității copiilor de rezervă sunt completări naționale, preluate din Regulamentul BNM nr. 29/2025 (pct. 38 și 40).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
		financiare dispun de mecanisme de verificare a integrității copiilor de rezervă.			
(3) Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz. În cazul contrapărților centrale, planurile de recuperare permit recuperarea tuturor tranzacțiilor în momentul perturbării, pentru a permite contrapărții centrale să continue să opereze în condiții de siguranță și să finalizeze decontarea la data stabilită. În plus, furnizorii de servicii de raportare a datelor mențin resurse adecvate și dispun de instalații pentru copii de rezervă și de restaurare, cu scopul de a-și oferi și a-și menține serviciile viabile în orice moment.	PF	66. Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz.	-	parțial compatibil	Frazele privind contrapărțile centrale și furnizorii de servicii de raportare a datelor vizează entități care nu se află în supravegherea BNM.
(4) Entitățile financiare, altele decât microîntreprinderile, mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale. Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc.	PF	67. Entitățile financiare, altele decât microîntreprinderile, mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale. Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc, fără a aduce atingere pct. 70-75.	-	compatibil	-
(5) Depozitarii centrali de titluri de valoare mențin cel puțin o unitate de prelucrare secundară, dotată cu resurse adecvate, capacități, funcții și resurse umane pentru a acoperi nevoile operaționale. Unitatea de prelucrare secundară: (a) este situată la o distanță geografică față de unitatea de prelucrare principală pentru a se asigura că are un profil de risc distinct și pentru a preveni afectarea acesteia de către evenimentul care a afectat unitatea de prelucrare principală; (b) este capabilă să asigure continuitatea funcțiilor critice sau importante în mod identic cu unitatea de prelucrare principală sau să furnizeze serviciile la nivelul necesar pentru a se asigura că entitatea financiară își desfășoară operațiunile critice în conformitate cu obiectivele de recuperare;	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în aplicare prin actele normative aplicabile acestor entități.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) este imediat accesibilă personalului entității financiare pentru a asigura continuitatea funcțiilor critice sau importante în cazul în care unitatea de prelucrare principală a devenit indisponibilă.					
(6) Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.	PF	78. Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.	-	compatibil	-
(7) În cazul recuperării în urma unui incident legat de TIC, entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat. Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.	PF	79. În cazul recuperării în urma unui incident legat de TIC, entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat. Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.	-	compatibil	-
Articolul 13. Învățăminte și perspective de dezvoltare (1) Entitățile financiare dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale.	PF	80. Entitățile financiare dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale.	-	compatibil	-
(2) Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC după ce un incident major legat de TIC le perturbă activitățile de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC menționate la articolul 11. Entitățile financiare, altele decât microîntreprinderile, comunică autorităților competente, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la primul paragraf.	PF+CN	81. Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC după ce un incident major legat de TIC le perturbă activitățile de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC. 82. Entitățile financiare, altele decât microîntreprinderile, comunică către BNM, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la pct. 81. 83. Verificările ulterioare incidentelor legate de TIC menționate la pct. 81 stabilesc dacă procedurile	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Verificările ulterioare incidentelor legate de TIC menționate la primul paragraf stabilesc dacă procedurile instituite au fost urmate și dacă măsurile luate au fost eficace, inclusiv în ceea ce privește următoarele: (a) promptitudinea reacției la alertele de securitate și determinarea impactului și a gravității incidentelor legate de TIC; (b) calitatea și rapiditatea efectuării unei analize judiciare, acolo unde se consideră necesar; (c) eficacitatea activării nivelurilor succesive de intervenție (incident escalation) în caz de incidente în cadrul entității financiare; (d) eficacitatea comunicării interne și externe.		instituite au fost urmate și dacă măsurile luate au fost eficace, inclusiv în ceea ce privește următoarele: 83.1. promptitudinea reacției la alertele de securitate și determinarea impactului și a gravității incidentelor legate de TIC; 83.2. calitatea și rapiditatea efectuării unei analize judiciare, acolo unde se consideră necesar; 83.3. eficacitatea activării nivelurilor succesive de intervenție (incident escalation) în caz de incidente în cadrul entității financiare; 83.4. eficacitatea comunicării interne și externe.			
(3) Învățămintele desprinse în urma testării rezilienței operaționale digitale, efectuată în conformitate cu articolele 26 și 27, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1).	PF	84. Învățămintele desprinse în urma testării rezilienței operaționale digitale, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC.	-	compatibil	-
(4) Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală menționate la articolul 6 alineatul (8). Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC, în special în legătură cu funcțiile critice sau importante, și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.	PF	85. Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală menționate la pct. 20. Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC, în special în legătură cu funcțiile critice sau importante, și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.	-	compatibil	-
(5) Personalul de nivel superior din domeniul TIC raportează cel puțin o dată pe an către organul de	PF	86. Personalul cu funcție-cheie pe domeniul TIC raportează cel puțin o dată pe an către organul de	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
conducere cu privire la rezultatele menționate la alineatul (3) și propune recomandări.		conducere cu privire la rezultatele menționate la pct. 84 și propune recomandări.			
(6) Entitățile financiare elaborează programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale ca module obligatorii în cadrul programelor lor de formare a personalului. Respectivele programe și cursuri de formare se aplică tuturor angajaților și personalului de conducere de nivel superior și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante, în conformitate cu articolul 30 alineatul (2) litera (i).	PF	87. Entitățile financiare elaborează programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale ca module obligatorii în cadrul programelor lor de formare a personalului. Respectivele programe și cursuri de formare se aplică tuturor angajaților, inclusiv personalului cu funcții-cheie și membrilor organelor de conducere, și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante, în conformitate cu subpct. 160.9. Instruirile de conștientizare cu privire la riscurile de securitate a informației se desfășoară cel puțin o dată pe an.	-	compatibil	Ultima frază (instruirea anuală) este o completare națională, preluată din Regulamentul BNM nr. 29/2025 (pct. 10 și 34).
(7) Entitățile financiare altele decât microîntreprinderile monitorizează evoluțiile tehnologice relevante în mod continuu, inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.	PF	88. Entitățile financiare, altele decât microîntreprinderile, monitorizează evoluțiile tehnologice relevante în mod continuu, inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.	-	compatibil	-
Articolul 14. Comunicare (1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.	PF	89. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.	-	compatibil	-
(2) Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare politici de comunicare pentru personalul intern și pentru părțile interesate externe. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea riscurilor TIC, în special personalul responsabil pentru	PF	90. Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare politici de comunicare pentru personalul intern și pentru părțile interesate externe. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea riscurilor TIC, în special personalul responsabil	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
răspuns și recuperare, și personalul care trebuie să fie informat.		pentru răspuns și recuperare, și personalul care trebuie să fie informat.			
(3) Cel puțin o persoană din entitatea financiară este însărcinată cu punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media.	PF	91. Cel puțin o persoană din entitatea financiară este responsabilă de punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media.	-	compatibil	-
Articolul 15. Armonizarea suplimentară a instrumentelor, metodelor, proceselor și politicilor de gestionare a riscurilor TIC AES elaborează, prin intermediul Comitetului comun, în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), proiecte comune de standarde tehnice de reglementare în următoarele scopuri: (a) pentru a aduce precizări suplimentare privind elementele necesare a fi incluse în politicile, procedurile, protocoalele și instrumentele de securitate TIC menționate la articolul 9 alineatul (2), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor, al menținerii disponibilității, autenticității, integrității și confidențialității datelor, inclusiv tehnici criptografice, și al garantării unei transmiteri exacte și rapide a datelor fără perturbări majore și fără întârzieri nejustificate; (b) pentru a aduce precizări suplimentare privind componentele controalelor drepturilor de gestionare a accesului menționate la articolul 9 alineatul (4) litera (c) și politica privind resursele umane aferentă, precizând drepturile de acces, procedurile de acordare și de revocare a drepturilor, monitorizarea comportamentului anormal în ceea ce privește riscurile TIC prin intermediul unor indicatori adecvați, inclusiv pentru modelele de utilizare a rețelei, orele, activitatea IT și dispozitivele necunoscute; (c) pentru a aduce precizări suplimentare privind mecanismele menționate la articolul 10 alineatul (1) care permit detectarea rapidă a activităților anormale și criteriile menționate la articolul 10 alineatul (2) care declanșează procesele de detectare și de răspuns la incidentele legate de TIC;	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(d) pentru a aduce precizări suplimentare privind componentele politicii de continuitate a activității TIC, menționată la articolul 11 alineatul (1); (e) pentru a aduce precizări suplimentare privind testarea planurilor de continuitate a activității TIC menționate la articolul 11 alineatul (6), pentru a asigura faptul că o astfel de testare ține seama în mod corespunzător de scenariile în care calitatea furnizării unei funcții critice sau importante se deteriorează până la un nivel inacceptabil sau eșuează, precum și că ia în considerare în mod corespunzător impactul potențial al insolvenței sau al altor disfuncționalități ale oricărui furnizor terț de servicii TIC relevant și, dacă este cazul, riscurile politice din jurisdicțiile furnizorilor respectivi; (f) pentru a aduce precizări suplimentare privind componentele planurilor de răspuns și de recuperare în domeniul TIC menționate la articolul 11 alineatul (3); (g) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (5). Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, ținând seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Articolul 16. Cadrul simplificat de gestionare a riscurilor TIC (1) Articolele 5-15 din prezentul regulament nu se aplică firmelor de investiții mici și neinterconectate,	N/A	-	-	prevederi UE neaplicabile	Cadrul simplificat se aplică doar entităților exceptate: instituții de plată exceptate în

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
instituțiilor de plată exceptate în temeiul Directivei (UE) 2015/2366; instituțiilor exceptate în temeiul Directivei 2013/36/UE în cazul cărora statele membre au decis să nu aplice opțiunea menționată la articolul 2 alineatul (4) din prezentul regulament; instituțiilor emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE; și nici instituțiilor mici pentru furnizarea de pensii ocupaționale. Fără a aduce atingere primului paragraf, entitățile menționate la primul paragraf: (a) instituie și mențin un cadru solid și documentat de gestionare a riscurilor TIC care detaliază mecanismele și măsurile care vizează o gestionare rapidă, eficientă și cuprinzătoare a riscurilor TIC, inclusiv pentru protecția componentelor și infrastructurilor fizice relevante; (b) monitorizează în permanență securitatea și funcționarea tuturor sistemelor TIC; (c) reduc la minimum impactul riscurilor TIC prin utilizarea unor sisteme, protocoale și instrumente TIC solide, reziliente și actualizate care sunt adecvate pentru a sprijini desfășurarea activităților lor și furnizarea serviciilor și protejează în mod adecvat disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor din rețele și sistemele informatice; (d) permit identificarea și detectarea rapidă a surselor de riscuri TIC și a anomaliilor din rețele și sistemele informatice, precum și gestionarea rapidă a incidentelor legate de TIC; (e) identifică principalele dependențe față de furnizorii terți de servicii TIC; (f) asigură continuitatea funcțiilor critice sau importante, prin planuri de continuitate a activității și măsuri de răspuns și de recuperare, care includ, cel puțin, măsuri privind copii de rezervă și restaurarea; (g) testează cu regularitate planurile și măsurile menționate la litera (f), precum și eficacitatea controalelor puse în aplicare în conformitate cu literele (a) și (c); (h) implementează, după caz, concluziile operaționale relevante rezultate din testele menționate la litera (g) și din analiza ulterioară incidentului în procesul de					temeiul Directivei (UE) 2015/2366, instituții emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE, instituții exceptate în temeiul Directivei 2013/36/UE, firme de investiții mici și neinterconectate și instituții mici pentru furnizarea de pensii ocupaționale. Legea nr. 114/2012 nu prevede regimuri de exceptare: societățile de plată și societățile emitente de monedă electronică sunt licențiate și aplică cadrul complet. Celelalte categorii nu intră în domeniul de aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
evaluare a riscurilor TIC și elaborează, în funcție de nevoi și de profilul de risc TIC, programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale destinate personalului și conducerii.					
(2) Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a) se documentează și se revizuiește periodic, precum și în momentul producerii unor incidente majore legate de TIC, în conformitate cu instrucțiunile de supraveghere. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.	N/A	-	-	prevederi UE neaplicabile	Cadrul simplificat nu are destinatari în legislația națională (vezi alin. (1)).
(3) AES elaborează, prin intermediul Comitetului comun, în consultare cu ENISA, proiecte comune de standarde tehnice de reglementare în următoarele scopuri: (a) pentru a aduce precizări suplimentare privind elementele care trebuie incluse în cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a); (b) pentru a aduce precizări suplimentare privind elementele legate de sistemele, protocoalele și instrumentele destinate reducerii la minimum a impactului riscurilor TIC menționate la alineatul (1) al doilea paragraf litera (c), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor și al menținerii disponibilității, autenticității, integrității și confidențialității datelor; (c) pentru a aduce precizări suplimentare privind componentele planurilor de continuitate a activității TIC menționate la alineatul (1) al doilea paragraf litera (f); (d) pentru a aduce precizări suplimentare privind normele referitoare la testarea planurilor de continuitate a activității și pentru a asigura eficacitatea controalelor menționate la alineatul (1) al doilea paragraf litera (g), precum și pentru a garanta faptul că o astfel de testare ține seama în mod	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
corespunzător de scenariile în care calitatea furnizării unei funcții critice sau importante se deteriorează până la un nivel inacceptabil sau eșuează; (e) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la alineatul (2). Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
CAPITOLUL III Gestionarea, clasificarea și raportarea incidentelor legate de TIC **Articolul 17. Procesul de gestionare a incidentelor legate de TIC** (1) Entitățile financiare definesc, instituie și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC.	PF	92. Entitățile financiare definesc, instituie și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC. 92.1. Entitățile financiare stabilesc proceduri eficiente de comunicare internă și externă, de notificare și de escaladare a incidentelor, care să prevadă ca incidentele majore să fie comunicate imediat organului de conducere, iar ulterior, la intervale regulate de timp, cel puțin o dată la 6 luni, să fie comunicate toate incidentele, inclusiv incidentele evitate, dar cu un posibil impact negativ ridicat asupra sistemelor și serviciilor TIC, comunicându-se măsurile de remediere luate imediat și cele care urmează a fi implementate pentru a preveni astfel de incidente pe viitor.	-	compatibil	Subpct. 92.1 este o prevedere cu specific național, preluată din Regulamentul BNM nr. 29/2025 (pct. 44).
(2) Entitățile financiare înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative. Entitățile financiare instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea cauzelor lor	PF	93. Entitățile financiare înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative. Entitățile financiare instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea	-	compatibil	Fraza a treia (păstrarea probelor) este o completare națională, preluată din Regulamentul BNM nr. 29/2025 (pct. 42).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
principale, astfel încât să se prevină apariția unor astfel de incidente.		cauzelor lor principale, astfel încât să se prevină apariția unor astfel de incidente. Entitățile financiare păstrează probele aferente incidentelor legate de TIC necesare investigațiilor și analizelor criminalistice.			
(3) Procesul de gestionare a incidentelor legate de TIC menționat la alineatul (1): (a) instituie indicatori de avertizare timpurie; (b) stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite la articolul 18 alineatul (1); (c) alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC; (d) stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media, în conformitate cu articolul 14, și pentru notificarea clienților, proceduri interne de activare a nivelurilor succesive de intervenție (escalation), inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz; (e) asigură că cel puțin incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la cel puțin incidentele majore legate de TIC, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a unor astfel de incidente legate de TIC; (f) stabilește proceduri de răspuns la incidentele legate de TIC în vederea atenuării efectelor și a asigurării faptului că serviciile devin operaționale și sigure în timp util.	PF	94. Procesul de gestionare a incidentelor legate de TIC menționat la pct. 92: 94.1. instituie indicatori de avertizare timpurie; 94.2. stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite la pct. 96; 94.3. alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC; 94.4. stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media și pentru notificarea clienților, proceduri interne de activare a nivelurilor succesive de intervenție, inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz; 94.5. asigură că cel puțin incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la cel puțin incidentele majore legate de TIC, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a unor astfel de incidente legate de TIC; 94.6. stabilește proceduri de răspuns la incidentele legate de TIC în vederea atenuării efectelor și a asigurării faptului că serviciile devin operaționale și sigure în timp util.	-	compatibil	-
Articolul 18. Clasificarea incidentelor legate de TIC și a amenințărilor cibernetice (1) Entitățile financiare clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii:	PF	96. Entitățile financiare clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii: 96.1. numărul și/sau relevanța clienților sau a contrapărților financiare afectate și, după caz, cuantumul și numărul tranzacțiilor afectate de	-	compatibil	Criteriul de la lit. (c) („mai mult de două state membre”) este adaptat la contextul național („și alte state”). Alineatul al doilea (pragul de 3 ore de indisponibilitate

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(a) numărul și/sau relevanța clienților sau a contrapărților financiare afectate și, după caz, cuantumul și numărul tranzacțiilor afectate de incidentul legat de TIC, precum și eventualul impact al incidentului legat de TIC asupra reputației; (b) durata incidentului legat de TIC, inclusiv perioada de indisponibilitate a serviciului; (c) întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC, în special în cazul în care acesta afectează mai mult de două state membre; (d) pierderile de date pe care le implică incidentul legat de TIC, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor; (e) caracterul critic al serviciilor afectate, inclusiv al tranzacțiilor și operațiunilor entității financiare; (f) impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC, în termeni atât absoluți, cât și relativi.		incidentul legat de TIC, precum și eventualul impact al incidentului legat de TIC asupra reputației; 96.2. durata incidentului legat de TIC, inclusiv perioada de indisponibilitate a serviciului; 96.3. întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC, în special în cazul în care acesta afectează și alte state; 96.4. pierderile de date pe care le implică incidentul legat de TIC, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor; 96.5. caracterul critic al serviciilor afectate, inclusiv al tranzacțiilor și operațiunilor entității financiare; 96.6. impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC, în termeni atât absoluți, cât și relativi. Se consideră major, în orice caz, incidentul legat de TIC care a dus la indisponibilitatea totală a serviciilor TIC care sprijină funcții critice sau importante pentru o perioadă mai mare de 3 ore, dacă funcția nu a putut fi asigurată prin soluții alternative. Întreruperile repetate din aceeași cauză produse în 24 de ore se cumulează, iar indisponibilitatea planificată și anunțată în prealabil nu se ia în calcul în limitele intervalului anunțat.			totală, fără soluții alternative) este o prevedere cu specific național, preluată din Regulamentul BNM nr. 29/2025 (pct. 3.8), în lipsa pragurilor stabilite prin standarde tehnice (alin. (3)).
(2) Entitățile financiare clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.	PF	97. Entitățile financiare clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.	-	compatibil	-
(3) AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, proiecte comune de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind următoarele: (a) criteriile menționate la alineatul (1), inclusiv pragurile de semnificație pentru determinarea incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți care fac obiectul obligației de raportare prevăzute la articolul 19 alineatul (1);	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(b) criteriile care trebuie aplicate de autoritățile competente în scopul evaluării relevanței incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți, pentru autoritățile competente relevante ale altor state membre, precum și detaliile rapoartelor referitoare la incidentele majore legate de TIC sau, după caz, incidentele majore operaționale sau de securitate legate de plăți care trebuie să fie comunicate altor autorități competente în temeiul articolului 19 alineatele (6) și (7); (c) criteriile prevăzute la alineatul (2) de la prezentul articol, inclusiv pragurile înalte de semnificație pentru determinarea amenințărilor cibernetice semnificative.					
(4) Atunci când elaborează proiectele comune de standarde tehnice de reglementare menționate la alineatul (3) de la prezentul articol, AES țin seama de criteriile stabilite la articolul 4 alineatul (2), precum și de standardele internaționale și de orientările și specificațiile elaborate și publicate de ENISA, inclusiv, după caz, de specificațiile pentru alte sectoare economice. În scopul aplicării criteriilor prevăzute la articolul 4 alineatul (2), AES iau în considerare în mod corespunzător necesitatea ca microîntreprinderile și întreprinderile mici și mijlocii să mobilizeze resurse și capacități suficiente pentru a se asigura că incidentele legate de TIC sunt gestionate rapid. AES transmit Comisiei aceste proiecte comune de standarde tehnice de reglementare până la 17 ianuarie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (3), în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
Articolul 19. Raportarea incidentelor majore legate de TIC și notificarea voluntară a amenințărilor cibernetice semnificative (1) Entitățile financiare raportează incidentele majore legate de TIC autorității competente relevante menționate la articolul 46 în conformitate cu alineatul (4) de la prezentul articol.	PF+CN	98. Entitățile financiare raportează incidentele majore legate de TIC către BNM în conformitate cu pct. 103. 99. Notificarea inițială se efectuează pe baza informațiilor disponibile la momentul clasificării incidentului, iar rapoartele se elaborează după colectarea și analizarea tuturor informațiilor relevante și se transmit BNM. În cazul în care o	-	compatibil	Autoritatea competentă este redată prin BNM. Paragrafele privind autoritatea competentă unică, instituțiile de credit semnificative și opțiunea statelor membre de notificare a

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
În cazul în care o entitate financiară face obiectul supravegherii de către mai mult de o autoritate națională competentă astfel cum este menționată la articolul 46, statele membre desemnează o autoritate competentă unică drept autoritate competentă relevantă responsabilă cu îndeplinirea funcțiilor și a sarcinilor prevăzute la prezentul articol. Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, prezintă un raport referitor la incidentele majore legate de TIC autorității naționale competente relevante desemnate în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat raportul respectiv către BCE. În sensul primului paragraf, după colectarea și analizarea tuturor informațiilor relevante, entitățile financiare efectuează notificarea inițială și elaborează rapoartele menționate la alineatul (4) de la prezentul articol, utilizând modelele menționate la articolul 20, și le transmit autorității competente. În cazul în care o imposibilitate tehnică împiedică transmiterea notificării inițiale utilizând modelul, entitățile financiare informează autoritatea competentă cu privire la aceasta prin mijloace alternative. Notificarea inițială și rapoartele menționate la alineatul (4) includ toate informațiile necesare autorității competente pentru a determina semnificația incidentului major legat de TIC și a evalua posibilele efecte transfrontaliere. Fără a aduce atingere raportării prevăzute la primul paragraf de către entitățile financiare către autoritatea competentă relevantă, statele membre pot stabili în plus ca unele entități financiare sau toate aceste entități să transmită, de asemenea, notificarea inițială și fiecare raport menționat la alineatul (4) de la prezentul articol, folosind modelele menționate la articolul 20, autorităților competente sau echipelor de intervenție în caz de incidente de securitate informatică (echipe CSIRT) desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.		imposibilitate tehnică împiedică transmiterea notificării inițiale prin PCSI, entitățile financiare informează BNM cu privire la aceasta prin mijloace alternative. Notificarea inițială și rapoartele includ toate informațiile necesare BNM pentru a determina semnificația incidentului major legat de TIC și a evalua posibilele efecte.			echipelor CSIRT nu necesită măsuri naționale. Notificarea și rapoartele se transmit prin PCSI, iar modelele de la art. 20 nu se preiau. Prima frază a pct. 99 precizează, potrivit Regulamentului delegat (UE) 2025/301, că notificarea inițială se face pe baza informațiilor disponibile la clasificare.
(2) Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative către	PF+CN	100. Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
autoritatea competentă relevantă atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți. Autoritatea competentă relevantă poate furniza astfel de informații și altor autorități relevante, menționate la alineatul (6). Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea națională competentă relevantă, desemnată în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat notificarea către BCE. Statele membre pot stabili că entitățile financiare care fac în mod voluntar o notificare în conformitate cu primul paragraf pot transmite, de asemenea, notificarea respectivă către echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.		către BNM atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți. BNM poate furniza astfel de informații și altor autorități relevante.			Paragrafele privind instituțiile de credit semnificative și opțiunea statelor membre privind echipele CSIRT nu necesită măsuri naționale.
(3) În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia, fără întârzieri nejustificate, de îndată ce află despre incidentul major legat de TIC, cu privire la incidentul respectiv și la măsurile care au fost luate pentru a atenua efectele negative ale unui astfel de incident. În cazul unei amenințări cibernetice semnificative, entitățile financiare își informează, după caz, clienții care ar putea fi afectați cu privire la eventualele măsuri de protecție adecvate pe care aceștia din urmă ar putea dori să le ia.	PF	101. În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia, fără întârzieri nejustificate, de îndată ce află despre incidentul major legat de TIC, cu privire la incidentul respectiv și la măsurile care au fost luate pentru a atenua efectele negative ale unui astfel de incident. 102. În cazul unei amenințări cibernetice semnificative, entitățile financiare își informează, după caz, clienții care ar putea fi afectați cu privire la eventualele măsuri de protecție adecvate pe care aceștia din urmă ar putea dori să le ia.	-	compatibil	-
(4) Până la termenele care urmează să fie stabilite în conformitate cu articolul 20 primul paragraf litera (a) punctul (ii), entitățile financiare transmit autorității competente relevante următoarele: (a) o notificare inițială; (b) un raport intermediar după notificarea inițială menționată la litera (a) de îndată ce starea incidentului inițial s-a schimbat în mod semnificativ sau gestionarea incidentului major legat de TIC s-a schimbat pe baza noilor informații disponibile, urmat, după caz, de notificări actualizate de fiecare dată	PF+CN	103. Entitățile financiare transmit BNM, prin intermediul PCSI, următoarele: 103.1. o notificare inițială fără întârziere după clasificarea incidentului ca incident major legat de TIC, dar nu mai târziu de sfârșitul zilei lucrătoare sau, în cazul unui incident clasificat ca major cu mai puțin de 2 ore înainte de încheierea zilei lucrătoare, nu mai târziu de 4 ore de la începutul următoarei zile lucrătoare. Clasificarea se efectuează fără întârziere, dar nu mai târziu de 24 de ore de la detectarea incidentului, cu excepția incidentului	-	compatibil	Termenele sunt stabilite direct în proiect (subpct. 103.1-103.3), pornind de la Regulamentul BNM nr. 29/2025 (pct. 81), în locul standardelor tehnice de la art. 20. Transmiterea se face prin PCSI.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
când este disponibilă o actualizare relevantă a stării, precum și la cererea specifică a autorității competente; (c) un raport final, atunci când analiza cauzelor principale a fost finalizată, indiferent dacă măsurile de atenuare au fost sau nu deja puse în aplicare, precum și atunci când cifrele efective ale impactului sunt disponibile pentru a înlocui estimările.		care întrunește criteriile prevăzute la pct. 96 ulterior acestui termen, care se clasifică de îndată ce criteriile sunt întrunite; 103.2. un raport intermediar, de îndată ce starea incidentului inițial s-a schimbat în mod semnificativ sau gestionarea incidentului major legat de TIC s-a schimbat pe baza noilor informații disponibile, dar nu mai târziu de 3 zile lucrătoare de la notificarea inițială menționată la subpct. 103.1, urmat, după caz, de notificări actualizate de fiecare dată când este disponibilă o actualizare relevantă a stării, precum și la cererea specifică a BNM; 103.3. un raport final, semnat de un membru al organului de conducere, atunci când analiza cauzelor principale a fost finalizată, indiferent dacă măsurile de atenuare au fost sau nu deja puse în aplicare, și atunci când cifrele efective ale impactului sunt disponibile pentru a înlocui estimările, dar nu mai târziu de 20 de zile lucrătoare de la data notificării inițiale. În cazul în care activitatea normală a fost reluată înainte de expirarea termenului pentru notificarea inițială, notificarea inițială și raportul intermediar pot fi transmise împreună.			
(5) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cu cea națională, obligațiile de raportare prevăzute la prezentul articol către un furnizor terț de servicii. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de îndeplinirea cerințelor legate de raportarea incidentului.	PF	104. Entitățile financiare pot externaliza, în conformitate cu legislația națională, obligațiile de raportare prevăzute la pct. 98-103 către un furnizor terț de servicii. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de îndeplinirea cerințelor legate de raportarea incidentului.	-	compatibil	-
(6) La primirea notificării inițiale și a fiecărui raport menționat la alineatul (4), autoritatea competentă furnizează, în timp util, detalii privind incidentul major legat de TIC următorilor destinatari, pe baza, după caz, a competențelor lor respective: (a) ABE, ESMA sau EIOPA; (b) BCE, în cazul entităților financiare menționate la articolul 2 alineatul (1) literele (a), (b) și (d); (c) autoritățile competente, punctele unice de contact sau echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555;	PF+CN	105. La primirea notificării inițiale și a fiecărui raport menționat la pct. 103, BNM furnizează, în timp util și în condițiile legii, detalii privind incidentul major legat de TIC către Agenția pentru Securitate Cibernetică, în calitate de autoritate competentă potrivit Legii nr. 48/2023 privind securitatea cibernetică (în continuare – ASC).	**Legea nr. 48/2023 privind securitatea cibernetică, art. 7 alin. (2):** (2) Autoritatea competentă exercită inclusiv funcția de echipă de răspuns la incidentele cibernetice la nivel național și cea de punct național unic de contact.	parțial compatibil	Lit. (a) și (b) vizează instituții ale Uniunii. Lit. (c) este redată prin transmiterea către ASC, care, potrivit art. 7 alin. (2) din Legea nr. 48/2023, este și echipa națională de răspuns la incidentele cibernetice și punctul național unic de contact. Transmiterea se face în condițiile legii: art. 36 din Legea nr.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(d) autoritățile de rezoluție, astfel cum sunt menționate la articolul 3 din Directiva 2014/59/UE, și Comitetul unic de rezoluție (SRB) în ceea ce privește entitățile menționate la articolul 7 alineatul (2) din Regulamentul (UE) nr. 806/2014 al Parlamentului European și al Consiliului, precum și în ceea ce privește entitățile și grupurile menționate la articolul 7 alineatul (4) litera (b) și alineatul (5) din Regulamentul (UE) nr. 806/2014 dacă aceste detalii se referă la incidente care prezintă un risc pentru asigurarea funcțiilor critice în sensul articolului 2 alineatul (1) punctul 35 din Directiva 2014/59/UE; și (e) alte autorități publice relevante în temeiul dreptului intern.					548/1995, art. 126 și 129 din Legea nr. 202/2017, art. 103 din Legea nr. 114/2012 și art. 120 din Legea nr. 92/2022 limitează comunicarea informațiilor confidențiale. Lit. (d) și (e) (autoritățile de rezoluție și alte autorități publice relevante) nu sunt reflectate.
(7) După primirea informațiilor în conformitate cu alineatul (6), ABE, ESMA sau EIOPA și BCE, în consultare cu ENISA și în cooperare cu autoritatea competentă relevantă, evaluează dacă incidentul major legat de TIC este relevant pentru autoritățile competente din alte state membre. În urma acestei evaluări, ABE, ESMA sau EIOPA notifică în consecință, cât mai curând posibil, autoritățile competente relevante din alte state membre. BCE notifică membrilor Sistemului European al Băncilor Centrale aspectele relevante pentru sistemul de plată. Pe baza notificării respective, autoritățile competente iau, după caz, toate măsurile necesare pentru protejarea stabilității imediate a sistemului financiar.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
(8) Notificarea care trebuie efectuată de ESMA în temeiul alineatului (7) de la prezentul articol nu aduce atingere responsabilității autorității competente de a transmite de urgență detaliile incidentului major legat de TIC autorității relevante din statul membru gazdă, în cazul în care un depozitar central de titluri de valoare desfășoară o activitate transfrontalieră semnificativă în statul membru gazdă, în cazul în care incidentul major legat de TIC este susceptibil să genereze consecințe grave pentru piețele financiare din statul membru gazdă și în cazul în care există acorduri de cooperare între autoritățile competente în ceea ce privește supravegherea entităților financiare.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
Articolul 20. Armonizarea conținutului rapoartelor și a modelelor de rapoarte	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
AES, prin intermediul Comitetului comun și în consultare cu ENISA și BCE, elaborează: (a) proiecte comune de standarde tehnice de reglementare având ca scop următoarele: (i) stabilirea conținutului rapoartelor în cazul incidentelor majore legate de TIC, cu scopul de a reflecta criteriile prevăzute la articolul 18 alineatul (1) și de a include elemente suplimentare, precum detalii pentru a stabili dacă rapoartele sunt relevante pentru alte state membre și dacă incidentele constituie incidente majore operaționale sau de securitate legate de plăți; (ii) stabilirea termenelor pentru notificarea inițială și pentru fiecare raport menționat la articolul 19 alineatul (4); (iii) stabilirea conținutului notificării privind amenințările cibernetice semnificative. Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, în special pentru a se asigura că, în sensul literei (a) punctul (ii) de la prezentul paragraf, existența unor termene diferite poate reflecta, după caz, particularitățile sectoarelor financiare, fără a aduce atingere menținerii unei abordări coerente a raportării incidentelor legate de TIC în temeiul prezentului regulament și al Directivei (UE) 2022/2555. AES furnizează, după caz, justificări atunci când se abat de la abordările adoptate în contextul directivei respective; (b) proiecte comune de standarde tehnice de punere în aplicare având ca scop stabilirea formularelor, modelelor și procedurilor standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC și notificarea de către acestea a unei amenințări cibernetice semnificative. AES transmit Comisiei proiectele comune de standarde tehnice de reglementare menționate la primul paragraf litera (a) și proiectele comune de standarde tehnice de punere în aplicare menționate la primul paragraf litera (b), până la 17 iulie 2024.					măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat. Formularele de raportare sunt cele din PCSI.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare comune menționate la primul paragraf litera (a), în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010. Se conferă Comisiei competența de a adopta standardele tehnice de punere în aplicare comune menționate la primul paragraf litera (b), în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Articolul 21. Centralizarea raportării incidentelor majore legate de TIC (1) AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, un raport comun de evaluare a fezabilității centralizării suplimentare a raportării incidentelor prin crearea unei platforme unice la nivelul UE pentru raportarea incidentelor majore legate de TIC de către entitățile financiare. Raportul comun analizează modalitățile de facilitare a fluxului raportării incidentelor legate de TIC, de reducere a costurilor asociate și de susținere a analizelor tematice în vederea consolidării convergenței în materie de supraveghere. (2) Raportul comun menționat la alineatul (1) cuprinde cel puțin următoarele elemente: (a) condițiile prealabile pentru instituirea unei platforme unice la nivelul UE; (b) beneficiile, limitările și riscurile, inclusiv riscurile asociate concentrării ridicate a informațiilor sensibile; (c) capacitatea necesară pentru a asigura interoperabilitatea cu alte sisteme de raportare relevante; (d) elemente ale gestionării operaționale; (e) condițiile de participare; (f) modalitățile tehnice de accesare a platformei unice la nivelul UE de către entitățile financiare și autoritățile naționale competente; (g) o evaluare preliminară a costurilor suportate cu instituirea platformei operaționale care sprijină platforma unică la nivelul UE, inclusiv expertiza necesară.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare. La nivel național, raportarea incidentelor majore se centralizează prin PCSI (pct. 106).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(3) AES transmit raportul menționat la alineatul (1) Parlamentului European, Consiliului și Comisiei până la 17 ianuarie 2025.					
Articolul 22. Feedback privind supravegherea (1) Fără a aduce atingere contribuției, consultanței sau soluțiilor tehnice și urmăririi ulterioare care pot fi oferite, după caz, în conformitate cu dreptul intern, de către echipele CSIRT în temeiul Directivei (UE) 2022/2555, autoritatea competentă, la primirea notificării inițiale și a fiecărui raport menționate la articolul 19 alineatul (4), confirmă primirea și poate furniza autorității financiare, acolo unde este posibil, în timp util, feedback relevant și proporțional sau îndrumări la nivel înalt, în special prin punerea la dispoziție a oricăror informații și date operative relevante anonimizate cu privire la amenințări similare și poate discuta măsurile de remediere aplicate la nivelul entității financiare și modalități de reducere la minimum și de atenuare a impactului negativ la nivelul sectorului financiar. Fără a aduce atingere feedbackului privind supravegherea primit, entitățile financiare rămân pe deplin responsabile de gestionarea incidentelor legate de TIC raportate în temeiul articolului 19 alineatul (1) și de consecințele acestora.	PF+CN	107. BNM, la primirea notificării inițiale și a fiecărui raport menționate la pct. 103, confirmă primirea și poate furniza entității financiare, acolo unde este posibil, în timp util, feedback relevant și proporțional sau îndrumări la nivel înalt, în special prin punerea la dispoziție a oricăror informații și date operative relevante anonimizate cu privire la amenințări similare și poate discuta măsurile de remediere aplicate la nivelul entității financiare și modalități de reducere la minimum și de atenuare a impactului negativ la nivelul sectorului financiar. Fără a aduce atingere feedbackului privind supravegherea primit, entitățile financiare rămân pe deplin responsabile de gestionarea incidentelor legate de TIC raportate în temeiul pct. 98 și de consecințele acestora.	-	compatibil	Autoritatea competentă este redată prin BNM. Contribuția echipelor CSIRT în temeiul Directivei (UE) 2022/2555 nu necesită măsuri în proiect.
(2) Prin intermediul Comitetului comun, AES raportează anual, în mod anonim și agregat, cu privire la incidentele majore legate de TIC, ale căror detalii sunt furnizate de autoritățile competente în conformitate cu articolul 19 alineatul (6), menționând cel puțin numărul incidentelor majore legate de TIC, natura acestora și impactul lor asupra operațiunilor entităților financiare sau ale clienților, măsurile de remediere luate și costurile suportate. AES emit avertismente și elaborează statistici la nivel înalt pentru a sprijini evaluările privind amenințările și vulnerabilitățile din perspectiva TIC.	CN	108. BNM elaborează rapoarte anuale, în mod anonim și agregat, cu privire la incidentele majore legate de TIC, menționând cel puțin numărul acestora, natura acestora și impactul lor asupra operațiunilor entităților financiare sau ale clienților, măsurile de remediere luate și costurile suportate. 109. BNM emite avertismente și elaborează statistici la nivel înalt pentru a sprijini evaluările privind amenințările și vulnerabilitățile din perspectiva TIC.	-	compatibil	Sarcinile AES sunt preluate, la nivel național, de BNM (rapoarte anuale anonime și agregate, avertismente și statistici).
Articolul 23. Incidente operaționale sau de securitate legate de plăți care vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică Cerințele prevăzute în prezentul capitol se aplică, de asemenea, incidentelor operaționale sau de	PF	110. Cerințele prevăzute în prezentul capitol se aplică, de asemenea, incidentelor operaționale sau de securitate legate de plăți și incidentelor operaționale sau de securitate majore legate de plăți, atunci când acestea vizează instituții de credit, instituții de plată, prestatori de servicii de informare	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
securitate legate de plăți și incidentelor operaționale sau de securitate majore legate de plăți, atunci când acestea vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică.		cu privire la conturi și instituții emitente de monedă electronică.			
CAPITOLUL IV Testarea rezilienței operaționale digitale **Articolul 24. Cerințe generale pentru efectuarea testării rezilienței operaționale digitale** (1) În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare, altele decât microîntreprinderile, stabilesc, mențin și revizuiesc, ținând seama de criteriile prevăzute la articolul 4 alineatul (2), un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC menționat la articolul 6.	PF	111. În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare, altele decât microîntreprinderile, stabilesc, mențin și revizuiesc, ținând seama de criteriile principiului proporționalității, un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC.	-	compatibil	-
(2) Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu articolele 25 și 26.	PF	112. Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu pct. 117-131.	-	compatibil	-
(3) Atunci când desfășoară programul de testare a rezilienței operaționale digitale menționat la alineatul (1) de la prezentul articol, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de criteriile prevăzute la articolul 4 alineatul (2) și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.	PF	113. Atunci când desfășoară programul de testare a rezilienței operaționale digitale menționat la pct. 111, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de criteriile principiului proporționalității și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.	-	compatibil	-
(4) Entitățile financiare, altele decât microîntreprinderile, se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe. Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.	PF	114. Entitățile financiare, altele decât microîntreprinderile, se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe. Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(5) Entitățile financiare, altele decât întreprinderile, stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile identificate pe parcursul desfășurării testelor și stabilesc metodologii de validare internă pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.	PF	115. Entitățile financiare, altele decât microîntreprinderile, stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile identificate pe parcursul desfășurării testelor și stabilesc metodologii de validare internă pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.	-	compatibil	Versiunea în limba română a Regulamentului (UE) 2022/2554 are „altele decât întreprinderile”, eroare evidentă: alin. (1), (3), (4) și (6) ale art. 24 au „altele decât microîntreprinderile”, sens preluat în proiect.
(6) Entitățile financiare, altele decât microîntreprinderile, se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante.	PF	116. Entitățile financiare, altele decât microîntreprinderile, se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante.	-	compatibil	-
Articolul 25. Testarea instrumentelor și sistemelor TIC (1) Programul de testare a rezilienței operaționale digitale menționat la articolul 24 asigură, în conformitate cu criteriile prevăzute la articolul 4 alineatul (2), efectuarea de teste adecvate, precum evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă acolo unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end) sau teste de penetrare.	PF	117. Programul de testare a rezilienței operaționale digitale asigură, în conformitate cu criteriile principiului proporționalității, efectuarea de teste adecvate, precum evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă acolo unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end). Testele de penetrare se efectuează în mod obligatoriu, cel puțin o dată la 3 ani sau mai des, la solicitarea BNM, asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante, pe baza unor scenarii validate de entitatea financiară, de către experți care dețin cel puțin una dintre certificările prevăzute la subpct. 132.6, fără a aduce atingere testărilor avansate prin TLPT prevăzute la pct. 119. Entitățile financiare efectuează testări de securitate și în cazul modificărilor majore ale infrastructurii sau ale proceselor, după incidentele operaționale sau de securitate majore și la lansarea sistemelor informatice noi sau modificate substanțial, accesibile din internet.	-	compatibil	Frazele a doua și a treia (testele de penetrare obligatorii, cu frecvența, scenariile și certificările testerilor, și testarea de securitate la modificări) sunt completări naționale, preluate din Regulamentul BNM nr. 29/2025 (pct. 33 și 55).
(2) Depozitarii centrali de titluri de valoare și contrapărțile centrale efectuează evaluări ale vulnerabilității înainte de utilizarea sau reutilizarea unor aplicații și componente de infrastructură noi sau	PF	-	-	prevederi UE neacoperite de măsuri naționale	Vizează entități care nu se află în supravegherea BNM. Prevederea urmează a fi pusă în

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
existente și servicii TIC care sprijină funcții critice sau importante ale entității financiare.					aplicare prin actele normative aplicabile acestor entități.
(3) Microîntreprinderile efectuează testele menționate la alineatul (1) combinând o abordare bazată pe riscuri cu o planificare strategică a testării TIC și luând în considerare în mod corespunzător necesitatea de a menține o abordare echilibrată între amploarea resurselor și timpul care urmează să fie alocat testării TIC prevăzute la prezentul articol, pe de o parte, și urgența, tipul de risc, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor relevant, inclusiv capacitatea entității financiare de a-și asuma riscuri calculate, pe de altă parte.	PF	118. Microîntreprinderile efectuează testele menționate la pct. 117 combinând o abordare bazată pe riscuri cu o planificare strategică a testării TIC și luând în considerare în mod corespunzător necesitatea de a menține o abordare echilibrată între amploarea resurselor și timpul care urmează să fie alocat testării TIC, pe de o parte, și urgența, tipul de risc, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor relevant, inclusiv capacitatea entității financiare de a-și asuma riscuri calculate, pe de altă parte.	-	compatibil	-
Articolul 26. Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT (1) Entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, care sunt identificate în conformitate cu alineatul (8) al treilea paragraf de la prezentul articol, efectuează, cel puțin o dată la trei ani, testări avansate prin intermediul TLPT. Pe baza profilului de risc al entității financiare și ținând seama de circumstanțele operaționale, autoritatea competentă poate să solicite entității financiare, dacă este necesar, să reducă sau să mărească această frecvență.	PF+CN	119. Entitățile financiare, altele decât microîntreprinderile, identificate de BNM în conformitate cu pct. 130 efectuează, cel puțin o dată la 3 ani, testări avansate prin intermediul TLPT. Pe baza profilului de risc al entității financiare și ținând seama de circumstanțele operaționale, BNM poate să solicite entității financiare, dacă este necesar, să reducă sau să mărească această frecvență.	-	compatibil	Autoritatea competentă este redată prin BNM. Entitățile obligate la TLPT sunt identificate de BNM potrivit pct. 130.
(2) Fiecare test de penetrare bazat pe amenințări acoperă unele sau toate funcțiile critice sau importante ale unei entități financiare și este realizat pe sistemele de producție în timp real care sprijină astfel de funcții. Entitățile financiare identifică toate sistemele, procesele și tehnologiile TIC subiacente relevante care sprijină funcțiile critice sau importante și serviciile TIC, inclusiv pe cele care sprijină funcțiile critice sau importante care au fost externalizate sau contractate unor furnizori terți de servicii TIC. Entitățile financiare evaluează ce funcții critice sau importante trebuie să fie acoperite de TLPT. Rezultatul acestei evaluări determină sfera de aplicare exactă a TLPT și este validat de autoritățile competente.	PF+CN	120. Fiecare test de penetrare bazat pe amenințări acoperă unele sau toate funcțiile critice sau importante ale unei entități financiare și este realizat pe sistemele de producție în timp real care sprijină astfel de funcții. 121. Entitățile financiare identifică toate sistemele, procesele și tehnologiile TIC subiacente relevante care sprijină funcțiile critice sau importante și serviciile TIC, inclusiv pe cele care sprijină funcțiile critice sau importante care au fost externalizate sau contractate unor furnizori terți de servicii TIC. 122. Entitățile financiare evaluează ce funcții critice sau importante trebuie să fie acoperite de TLPT. Rezultatul acestei evaluări determină sfera de aplicare exactă a TLPT și este validat de BNM.	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(3) În cazul în care furnizorii terți de servicii TIC sunt incluși în sfera de aplicare a TLPT, entitatea financiară ia măsurile și garanțiile necesare pentru a asigura participarea acestor furnizori terți de servicii TIC la TLPT și rămân în orice moment pe deplin responsabile de asigurarea respectării prezentului regulament.	PF	123. În cazul în care furnizorii terți de servicii TIC sunt incluși în sfera de aplicare a TLPT, entitatea financiară ia măsurile și garanțiile necesare pentru a asigura participarea acestor furnizori terți de servicii TIC la TLPT și rămâne în orice moment pe deplin responsabilă de asigurarea respectării prezentului regulament.	-	compatibil	-
(4) Fără a aduce atingere primului și celui de al doilea paragraf de la alineatul (2), în cazul în care se preconizează în mod rezonabil că participarea unui furnizor terț de servicii TIC la TLPT, astfel cum se menționează la alineatul (3), va avea un impact negativ asupra calității sau securității serviciilor oferite de către furnizorul terț de servicii TIC către clienți care sunt entități ce nu intră în domeniul de aplicare al prezentului regulament, sau asupra confidențialității datelor legate de astfel de servicii, entitatea financiară și furnizorul terț de servicii TIC pot conveni în scris ca furnizorul terț de servicii TIC să încheie în mod direct acorduri contractuale cu o entitate externă de testare în scopul desfășurării, sub conducerea unei entități financiare desemnate unice, a unei TLPT grupate, în care să fie implicate mai multe entități financiare (testare grupată) pentru care furnizorul terț de servicii TIC oferă servicii TIC. Testarea grupată respectivă acoperă gama relevantă de servicii TIC care sprijină funcțiile critice sau importante contractate de către entitățile financiare respectivului furnizor terț de servicii TIC. Testarea grupată este considerată TLPT efectuată de entitățile financiare care participă la testarea grupată. Numărul entităților financiare care participă la testarea grupată este calibrat în mod corespunzător, ținând seama de complexitatea și de tipurile serviciilor implicate.	PF	124. Fără a aduce atingere sferei de aplicare TLPT, în cazul în care se preconizează în mod rezonabil că participarea unui furnizor terț de servicii TIC la TLPT, astfel cum se menționează la pct. 123, va avea un impact negativ asupra calității sau securității serviciilor oferite de către furnizorul terț de servicii TIC către clienți care sunt entități ce nu intră în domeniul de aplicare al prezentului regulament, sau asupra confidențialității datelor legate de astfel de servicii, entitatea financiară și furnizorul terț de servicii TIC pot conveni în scris ca furnizorul terț de servicii TIC să încheie în mod direct acorduri contractuale cu o entitate externă de testare în scopul desfășurării, sub conducerea unei entități financiare desemnate unice, a unei TLPT grupate, în care să fie implicate mai multe entități financiare (testare grupată) pentru care furnizorul terț de servicii TIC oferă servicii TIC. Testarea grupată respectivă acoperă gama relevantă de servicii TIC care sprijină funcțiile critice sau importante contractate de către entitățile financiare respectivului furnizor terț de servicii TIC. Testarea grupată este considerată TLPT efectuată de entitățile financiare care participă la testarea grupată. Numărul entităților financiare care participă la testarea grupată este calibrat în mod corespunzător, ținând seama de complexitatea și de tipurile serviciilor implicate.	-	compatibil	-
(5) Entitățile financiare efectuează, cu cooperarea furnizorilor terți de servicii TIC și a altor părți implicate, inclusiv a entităților de testare, dar excluzând autoritățile competente, controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la	PF+CN	125. Entitățile financiare efectuează, cu cooperarea furnizorilor terți de servicii TIC și a altor părți implicate, inclusiv a entităților de testare, dar excluzând BNM, controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la nivelul	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
nivelul entității financiare înseși, al contrapărților acesteia sau al sectorului financiar.		entității financiare, al contrapărților acesteia sau al sectorului financiar.			
(6) La sfârșitul testării, după ce s-a convenit cu privire la rapoarte și la planurile de remediere, entitatea financiară și, după caz, entitățile externe de testare furnizează autorității desemnate în conformitate cu alineatul (9) sau (10) un rezumat al constatărilor relevante, planurile de remediere și documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele.	PF+CN	126. La sfârșitul testării, după ce s-a convenit cu privire la rapoarte și la planurile de remediere, entitatea financiară și, după caz, entitățile externe de testare furnizează BNM un rezumat al constatărilor relevante, planurile de remediere și documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele.	-	compatibil	Autoritatea competentă este redată prin BNM.
(7) Autoritățile furnizează entităților financiare o adeverință prin care se confirmă faptul că testul a fost efectuat în conformitate cu cerințele evidențiate în documentație, pentru a permite recunoașterea reciprocă între autoritățile competente a testelor de penetrare bazate pe amenințări. Entitatea financiară notifică autorității competente relevante adeverința, rezumatul constatărilor relevante și planurile de remediere. Fără a aduce atingere unei astfel de adeverințe, entitățile financiare rămân în orice moment pe deplin responsabile pentru impactul testelor menționate la alineatul (4).	PF+CN	127. BNM furnizează entităților financiare menționate la pct. 2 o adeverință prin care se confirmă faptul că testul a fost efectuat în conformitate cu cerințele evidențiate în documentație. Fără a aduce atingere unei astfel de adeverințe, entitățile financiare rămân în orice moment pe deplin responsabile pentru impactul testelor menționate la pct. 124.	-	compatibil	Autoritatea competentă este redată prin BNM. Recunoașterea reciprocă a testelor între autoritățile competente din Uniune nu necesită măsuri naționale.
(8) Entitățile financiare contractează entități de testare în scopul efectuării TLPT în conformitate cu articolul 27. Atunci când entitățile financiare utilizează entități interne de testare în scopul efectuării TLPT, acestea contractează entități externe de testare la fiecare trei teste. Instituțiile de credit care sunt clasificate drept semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, utilizează numai entități externe de testare în conformitate cu articolul 27 alineatul (1) literele (a)-(e). Autoritățile competente identifică entitățile financiare care sunt obligate să efectueze TLPT ținând seama de criteriile prevăzute la articolul 4 alineatul (2), pe baza unei evaluări a următoarelor elemente: (a) factorii legați de impact, în special măsura în care serviciile furnizate și activitățile întreprinse de entitatea financiară au impact asupra sectorului financiar;	PF+CN	128. Entitățile financiare contractează entități de testare în scopul efectuării TLPT în conformitate cu pct. 132-134. Atunci când entitățile financiare utilizează entități interne de testare în scopul efectuării TLPT, acestea contractează entități externe de testare la fiecare trei teste. 129. Instituțiile de credit identificate ca societăți de importanță sistemică în sensul Legii nr. 202/2017 privind activitatea băncilor utilizează numai entități externe de testare în conformitate cu pct. 132. 130. BNM identifică entitățile financiare care sunt obligate să efectueze TLPT ținând seama de criteriile principiului proporționalității, pe baza unei evaluări a următoarelor elemente: 130.1. factorii legați de impact, în special măsura în care serviciile furnizate și activitățile întreprinse de entitatea financiară au impact asupra sectorului financiar;	-	compatibil	Instituțiile de credit semnificative în sensul Regulamentului (UE) nr. 1024/2013 sunt redate prin băncile identificate ca societăți de importanță sistemică în sensul Legii nr. 202/2017. Autoritatea competentă este redată prin BNM. Ultimele două alineate ale pct. 130 (TLPT efectuat la nivelul grupului și comunicarea identificării cu cel puțin 12 luni înainte) sunt precizări naționale.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(b) posibile preocupări legate de stabilitatea financiară, inclusiv caracterul sistemic al entității financiare la nivelul Uniunii sau la nivel național, după caz; (c) profilul de risc TIC specific, nivelul de maturitate a entității financiare din perspectiva TIC sau caracteristicile tehnologice implicate.		130.2. posibile preocupări legate de stabilitatea financiară, inclusiv caracterul sistemic al entității financiare la nivel național; 130.3. profilul de risc TIC specific, nivelul de maturitate a entității financiare din perspectiva TIC sau caracteristicile tehnologice implicate. La identificare și la stabilirea frecvenței TLPT, BNM poate lua în considerare TLPT efectuat la nivelul grupului din care face parte entitatea financiară, dacă acesta acoperă funcțiile critice sau importante ale entității financiare, iar documentația prevăzută la pct. 126 este pusă la dispoziția BNM. BNM comunică entității financiare identificarea și termenul primului TLPT cu cel puțin 12 luni înainte de expirarea acestui termen.			
(9) Statele membre pot desemna o autoritate publică unică în sectorul financiar care să fie responsabilă de aspectele legate de TLPT în sectorul financiar la nivel național și îi încredințează acesteia toate competențele și sarcinile în acest sens.	CN	131. BNM este responsabilă de aspectele legate de TLPT în sectorul financiar la nivel național pentru entitățile financiare menționate la pct. 2 și îi sunt încredințate toate competențele și sarcinile în acest sens.	-	compatibil	BNM este desemnată autoritatea responsabilă de aspectele legate de TLPT.
(10) În absența unei desemnări în conformitate cu alineatul (9) de la prezentul articol și fără a aduce atingere competenței de a identifica entitățile financiare care trebuie să efectueze TLPT, o autoritate competentă poate delega exercitarea unora sau a tuturor sarcinilor menționate la prezentul articol și la articolul 27 unei alte autorități naționale din sectorul financiar.	N/A	-	-	prevederi UE neaplicabile	Prevedere aplicabilă în lipsa desemnării de la alin. (9), care a fost făcută (pct. 131).
(11) AES elaborează, în acord cu BCE, proiecte comune de standarde tehnice de reglementare în conformitate cu cadrul TIBER–EU pentru a aduce precizări suplimentare privind: (a) criteriile utilizate în scopul aplicării alineatului (8) al doilea paragraf; (b) cerințele și standardele care reglementează utilizarea entităților interne de testare; (c) cerințele privind: (i) sfera de aplicare a TLPT menționată la alineatul (2); (ii) metodologia de testare și abordarea de urmat pentru fiecare fază specifică a procesului de testare;	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(iii) rezultatele, încheierea și etapele procesului de remediere aferente testării; (d) tipul de cooperare în materie de supraveghere și alt tip de cooperare relevant care sunt necesare pentru punerea în aplicare a TLPT și pentru facilitarea recunoașterii reciproce a testării respective, în contextul entităților financiare care operează în mai multe state membre, pentru a permite un nivel adecvat de implicare din perspectiva supravegherii și o aplicare flexibilă, astfel încât să se țină seama de specificitățile subsectoarelor financiare sau ale piețelor financiare locale. Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES țin seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Articolul 27. Cerințe pentru entitățile de testare în ceea ce privește efectuarea TLPT (1) Entitățile financiare utilizează, în scopul efectuării TLPT, numai entități de testare care: (a) sunt cele mai adecvate și de cea mai înaltă reputație; (b) dețin capacități tehnice și organizatorice și demonstrează expertiză specifică în ceea ce privește datele operative privind amenințările, testele de penetrare și testarea de tipul „echipa roșie”; (c) sunt certificate de un organism de acreditare dintr-un stat membru sau aderă la coduri de conduită sau cadre etice formale; (d) oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu efectuarea TLPT, inclusiv protecția corespunzătoare a informațiilor confidențiale ale entității financiare și măsurile	PF	132. Entitățile financiare utilizează, în scopul efectuării TLPT, numai entități de testare care: 132.1. sunt cele mai adecvate și de cea mai înaltă reputație; 132.2. dețin capacități tehnice și organizatorice și demonstrează expertiză specifică în ceea ce privește datele operative privind amenințările, testele de penetrare și testarea de tipul „echipa roșie”; 132.3. sunt certificate sau aderă la coduri de conduită ori la cadre etice formale; 132.4. oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu efectuarea TLPT, inclusiv protecția corespunzătoare a informațiilor confidențiale ale entității financiare și măsurile reparatorii pentru riscurile legate de activitățile entității financiare;	-	compatibil	Subpct. 132.6 este o prevedere cu specific național, preluată din Regulamentul BNM nr. 29/2025 (pct. 33.4).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
reparatorii pentru riscurile legate de activitățile entității financiare; (e) sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență.		132.5. sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență; 132.6. dispun de testeri care dețin cel puțin una dintre următoarele certificări: CEPT, CPT, CEH, OSCP, OPST, CPENT, GPEN, GWAPT, LPT, PTC sau alte certificări recunoscute la nivel internațional.			
(2) În cazul utilizării entităților interne de testare, entitățile financiare se asigură că, în plus față de cerințele de la alineatul (1), se respectă toate condițiile următoare: (a) utilizarea a fost aprobată de autoritatea competentă relevantă sau de autoritatea publică unică desemnată în conformitate cu articolul 26 alineatele (9) și (10); (b) autoritatea competentă relevantă a verificat că entitatea financiară are suficiente resurse alocate și s-a asigurat că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului; și (c) furnizorul de date operative privind amenințările este extern entității financiare.	PF+CN	133. În cazul utilizării entităților interne de testare, entitățile financiare se asigură că, în plus față de cerințele de la pct. 132, se respectă toate condițiile următoare: 133.1. utilizarea a fost aprobată de BNM; 133.2. BNM a verificat că entitatea financiară are suficiente resurse alocate și s-a asigurat că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului; 133.3. furnizorul de date operative privind amenințările este extern entității financiare.	-	compatibil	Autoritatea competentă este redată prin BNM.
(3) Entitățile financiare se asigură că contractele încheiate cu entități externe de testare impun o gestionare solidă a rezultatelor TLPT și că orice prelucrare de date de către acestea, inclusiv orice generare, stocare, agregare, elaborare, raportare, comunicare sau distrugere, nu creează riscuri pentru entitatea financiară.	PF	134. Entitățile financiare se asigură că contractele încheiate cu entități externe de testare impun o gestionare solidă a rezultatelor TLPT și că orice prelucrare de date de către acestea, inclusiv orice generare, stocare, agregare, elaborare, raportare, comunicare sau distrugere, nu creează riscuri pentru entitatea financiară.	-	compatibil	-
CAPITOLUL V Gestionarea riscurilor TIC generate de părți terțe **Secțiunea I Principii-cheie pentru o gestionare solidă a riscurilor TIC generate de părți terțe** **Articolul 28. Principii generale** (1) Entitățile financiare gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC astfel cum este menționat la articolul 6 alineatul (1) și în conformitate cu următoarele principii: (a) entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment	PF	136. Entitățile financiare gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC și în conformitate cu următoarele principii: 136.1. entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor care decurg din prezentul regulament și din dreptul aplicabil în domeniul serviciilor financiare; 136.2. gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor care decurg din prezentul regulament și din dreptul aplicabil în domeniul serviciilor financiare; (b) gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare: (i) natura, amploarea, complexitatea și importanța dependențelor legate de TIC; (ii) riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.		aplicare din perspectiva principiului proporționalității, luând în considerare: a) natura, amploarea, complexitatea și importanța dependențelor legate de TIC; b) riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.			
(2) Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori menționată la articolul 6 alineatul (9), după caz. Această strategie privind riscurile TIC generate de părți terțe include o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Pe baza unei evaluări a profilului general de risc al entității financiare și a amplorii și complexității serviciilor comerciale, organul de conducere examinează periodic riscurile identificate în ceea ce privește acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante.	PF	137. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare, altele decât microîntreprinderile, adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori menționată la pct. 21, după caz. Această strategie privind riscurile TIC generate de părți terțe include o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Pe baza unei evaluări a profilului general de risc al entității financiare și a amplorii și complexității serviciilor comerciale, organul de conducere examinează periodic riscurile identificate în ceea ce privește acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante.	-	compatibil	Entitățile menționate la art. 16 alin. (1) nu există în legislația națională.
(3) Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC.	PF+CN	138. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC.	-	compatibil	Autoritatea competentă este redată prin BNM. La pct. 140, raportarea se face prin PCSI, în termenul de la pct. 135. La pct. 142, informarea „în timp util” este

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Acordurile contractuale menționate la primul paragraf sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă. Entitățile financiare raportează cel puțin o dată pe an autorităților competente cu privire la numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile TIC care sunt oferite. Entitățile financiare pun la dispoziția autorității competente, la cererea acesteia, registrul complet de informații sau, după caz, secțiuni specifice din acesta, împreună cu orice informații considerate necesare pentru a permite supravegherea eficace a entității financiare. Entitățile financiare informează autoritatea competentă în timp util cu privire la orice acord contractual planificat privind utilizarea unor servicii TIC care sprijină funcții critice sau importante, precum și atunci când o funcție a devenit critică sau importantă.		139. Acordurile contractuale menționate la pct. 138 sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă. 140. Entitățile financiare raportează cel puțin o dată pe an către BNM cu privire la numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile TIC care sunt oferite. Raportarea se efectuează prin PCSI, în termenul prevăzut la pct. 135. 141. Entitățile financiare pun la dispoziția BNM, la cererea acesteia, registrul complet de informații sau, după caz, secțiuni specifice din acesta, împreună cu orice informații considerate necesare pentru a permite supravegherea eficace a entității financiare. 142. Entitățile financiare informează BNM, prin PCSI, cu cel puțin 30 de zile înainte de încheierea oricărui acord contractual planificat privind utilizarea unor servicii TIC care sprijină funcții critice sau importante, precum și fără întârziere atunci când o funcție a devenit critică sau importantă. Informarea nu constituie o procedură de aprobare a acordului. Notificarea acordului efectuată potrivit actelor normative ale BNM privind externalizarea ține loc de informare, dacă indică faptul că serviciul TIC sprijină o funcție critică sau importantă.			precizată prin termenul de 30 de zile, iar notificarea făcută potrivit actelor BNM privind externalizarea ține loc de informare.
(4) Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare: (a) evaluează dacă acordul contractual vizează utilizarea unor servicii TIC care sprijină o funcție critică sau importantă; (b) evaluează dacă sunt îndeplinite condițiile pentru contractare din perspectiva supravegherii; (c) identifică și evaluează toate riscurile relevante legate de acordul contractual, inclusiv posibilitatea ca un astfel de acord contractual să contribuie la consolidarea riscului de concentrare a serviciilor TIC, astfel cum este menționat la articolul 29; (d) efectuează toate diligențele necesare cu privire la potențialii furnizori terți de servicii TIC și se asigură,	PF	143. Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare: 143.1. evaluează dacă acordul contractual vizează utilizarea unor servicii TIC care sprijină o funcție critică sau importantă; 143.2. evaluează dacă sunt îndeplinite condițiile pentru contractare din perspectiva supravegherii; 143.3. identifică și evaluează toate riscurile relevante legate de acordul contractual, inclusiv posibilitatea ca un astfel de acord contractual să contribuie la consolidarea riscului de concentrare a serviciilor TIC; 143.4. efectuează toate diligențele necesare cu privire la potențialii furnizori terți de servicii TIC și se asigură, pe parcursul proceselor de selecție și	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
pe parcursul proceselor de selecție și evaluare, că furnizorul terț de servicii TIC este adecvat; (e) identifică și evaluează conflictele de interese pe care acordul contractual le poate cauza.		evaluare, că furnizorul terț de servicii TIC este adecvat; 143.5. identifică și evaluează conflictele de interese pe care acordul contractual le poate cauza.			
(5) Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.	PF	144. Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.	-	compatibil	-
(6) În exercitarea drepturilor de acces, de inspecție și de audit cu privire la furnizorul terț de servicii TIC, entitățile financiare stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit. În cazul în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată, entitatea financiară verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.	PF	145. În exercitarea drepturilor de acces, de inspecție și de audit cu privire la furnizorul terț de servicii TIC, entitățile financiare stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit. Pentru exercitarea acestor drepturi, entitățile financiare pot utiliza, pe baza evaluării riscurilor, audituri comune organizate împreună cu alte entități financiare care utilizează serviciile aceluiași furnizor terț de servicii TIC, certificări emise de terți și rapoarte de audit puse la dispoziție de furnizor, dacă domeniul acestora acoperă sistemele și controalele relevante, sunt actuale și sunt întocmite cu respectarea standardelor profesionale recunoscute. Utilizarea acestor metode nu limitează drepturile prevăzute la subpct. 161.5 și nu înlocuiește, în timp, auditul propriu sau auditul comun. 146. În cazul în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată, entitatea financiară verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.	-	compatibil	Alineatul al doilea de la pct. 145 (audituri comune, certificări și rapoarte ale furnizorului) ține seama de art. 8 din Regulamentul delegat (UE) 2024/1773.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(7) Entitățile financiare se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe: (a) încălcarea semnificativă de către furnizorul terț de servicii TIC a actelor cu putere de lege, a reglementărilor sau a clauzelor contractuale aplicabile; (b) circumstanțe identificate pe parcursul monitorizării riscurilor TIC generate de părți terțe care sunt considerate capabile să modifice îndeplinirea funcțiilor oferite prin acordul contractual, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC; (c) deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal; (d) în cazul în care autoritatea competentă nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta.	PF+CN	147. Entitățile financiare se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe: 147.1. încălcarea semnificativă de către furnizorul terț de servicii TIC a actelor normative, a reglementărilor sau a clauzelor contractuale aplicabile; 147.2. circumstanțe identificate pe parcursul monitorizării riscurilor TIC generate de părți terțe care sunt considerate capabile să modifice îndeplinirea funcțiilor oferite prin acordul contractual, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC; 147.3. deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal; 147.4. în cazul în care BNM nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta.	-	compatibil	Autoritatea competentă este redată prin BNM.
(8) Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire. Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate la alineatul (7). Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără: (a) perturbarea activităților lor comerciale; (b) limitarea respectării cerințelor în materie de reglementare;	PF	148. Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire. Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate la pct. 147. 149. Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără: 149.1. perturbarea activităților lor comerciale; 149.2. limitarea respectării cerințelor în materie de reglementare;	-	compatibil	-

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) afectarea continuității și calității serviciilor furnizate către clienți. Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu criteriile stabilite la articolul 4 alineatul (2), trebuie să fie testate în mod suficient și revizuite periodic. Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lor către furnizori alternativi sau să le reintegreze în sistemul propriu. Entitățile financiare instituie măsuri adecvate pentru situații neprevăzute astfel încât să păstreze continuitatea activității în cazul apariției situațiilor menționate la primul paragraf.		149.3. afectarea continuității și calității serviciilor furnizate către clienți. 150. Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu criteriile stabilite la pct. 5, trebuie să fie testate în mod suficient și revizuite periodic. 151. Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lor către furnizori alternativi sau să le reintegreze în sistemul propriu. 152. Entitățile financiare instituie măsuri adecvate pentru situații neprevăzute astfel încât să păstreze continuitatea activității în cazul apariției situațiilor menționate la pct. 148.			
(9) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de punere în aplicare pentru a stabili modelele standard pentru registrul de informații menționat la alineatul (3), inclusiv informații care sunt comune tuturor acordurilor contractuale privind utilizarea serviciilor TIC. AES transmit Comisiei aceste proiecte de standarde tehnice de punere în aplicare până la 17 ianuarie 2024. Se conferă Comisiei competența de a adopta standardele tehnice de punere în aplicare menționate la primul paragraf în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.
(10) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind conținutul detaliat al politicii menționate la alineatul (2) în legătură cu acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC. Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
sale. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Articolul 29. Evaluarea preliminară a riscului de concentrare a serviciilor TIC (1) La identificarea și evaluarea riscurilor menționate la articolul 28 alineatul (4) litera (c), entitățile financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații: (a) stabilirea unei relații contractuale cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau (b) instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați. Entitățile financiare evaluează beneficiile și costurile soluțiilor alternative, cum ar fi utilizarea unor furnizori terți de servicii TIC diferiți, luând în considerare dacă și în ce mod soluțiile avute în vedere corespund nevoilor și obiectivelor operaționale stabilite în strategia lor privind reziliența digitală.	PF	153. La identificarea și evaluarea riscurilor menționate la subpct. 143.3, entitățile financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații: 153.1. stabilirea unei relații contractuale cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau 153.2. instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați. 154. Entitățile financiare evaluează beneficiile și costurile soluțiilor alternative, cum ar fi utilizarea unor furnizori terți de servicii TIC diferiți, luând în considerare dacă și în ce mod soluțiile avute în vedere corespund nevoilor și obiectivelor operaționale stabilite în strategia lor privind reziliența operațională digitală.	-	compatibil	-
(2) În cazul în care acordurile contractuale privind utilizarea de servicii TIC care sprijină funcții critice sau importante includ posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare servicii TIC care sprijină o funcție critică sau importantă către alți furnizori terți de servicii TIC, entitățile financiare evaluează beneficiile și riscurile care pot apărea în legătură cu o astfel de subcontractare, în special în cazul unui subcontractant TIC stabilit într-o țară terță. În cazul în care acordurile contractuale privesc servicii TIC care sprijină funcții critice sau importante, entitățile financiare iau în considerare în mod	PF+CN	155. În cazul în care acordurile contractuale privind utilizarea de servicii TIC care sprijină funcții critice sau importante includ posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare servicii TIC care sprijină o funcție critică sau importantă către alți furnizori terți de servicii TIC, entitățile financiare evaluează beneficiile și riscurile care pot apărea în legătură cu o astfel de subcontractare, în special în cazul unui subcontractant TIC stabilit într-un stat terț. 156. În cazul în care acordurile contractuale privesc servicii TIC care sprijină funcții critice sau importante, entitățile financiare iau în considerare în	-	compatibil	„Țară terță” este redată prin „stat terț”, iar normele Uniunii privind protecția datelor prin legislația privind protecția datelor cu caracter personal. Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
corespunzător dispozițiile din legislația privind insolvența care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC, precum și orice constrângere care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante sunt încheiate cu un furnizor terț de servicii TIC stabilit într-o țară terță, entitățile financiare iau în considerare, în afară de aspectele menționate la al doilea paragraf, și conformitatea cu normele Uniunii privind protecția datelor și asigurarea efectivă a respectării legii în respectiva țară terță. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante prevăd subcontractarea, entitățile financiare evaluează dacă și în ce mod lanțurile de subcontractare potențial lungi sau complexe pot avea un impact asupra capacității lor de a monitoriza pe deplin funcțiile contractate și asupra capacității autorității competente de a supraveghea efectiv entitatea financiară din acest punct de vedere.		mod corespunzător dispozițiile din legislația privind insolvența care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC, precum și orice constrângere care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare. 157. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante sunt încheiate cu un furnizor terț de servicii TIC stabilit într-un stat terț, entitățile financiare iau în considerare, pe lângă aspectele menționate la pct. 156, conformitatea cu legislația privind protecția datelor cu caracter personal și asigurarea efectivă a respectării legii în statul terț respectiv. 158. Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante prevăd subcontractarea, entitățile financiare evaluează dacă și în ce mod lanțurile de subcontractare potențial lungi sau complexe pot avea un impact asupra capacității lor de a monitoriza pe deplin funcțiile contractate și asupra capacității BNM de a supraveghea efectiv entitatea financiară din acest punct de vedere.		
Articolul 30. Dispoziții contractuale esențiale (1) Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris. Contractul complet include acordurile privind nivelul serviciilor și este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.	PF	159. Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris. Contractul complet include acordurile privind nivelul serviciilor și este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.	-	compatibil	-
(2) Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente: (a) o descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări; (b) locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC	PF+CN	160. Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente: 160.1. o descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări;	-	compatibil	Subpct. 160.7 și 160.8 trimit la BNM și la autoritățile de rezoluție.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
contractate sau subcontractate și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri; (c) dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal; (d) dispoziții privind asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară în caz de insolvență, de rezoluție sau de încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale; (e) descrieri la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora; (f) obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, atunci când survine un incident TIC care este legat de serviciul TIC furnizat entității financiare; (g) obligația furnizorului terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare, inclusiv cu persoanele numite de acestea; (h) drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție; (i) condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale în conformitate cu articolul 13 alineatul (6).		160.2. locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC contractate sau subcontractate și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri; 160.3. dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal; 160.4. dispoziții privind asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară în caz de insolvență, de rezoluție sau de încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale; 160.5. descrieri la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora; 160.6. obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, atunci când survine un incident legat de TIC care este legat de serviciul TIC furnizat entității financiare; 160.7. obligația furnizorului terț de servicii TIC de a coopera pe deplin cu BNM și cu autoritățile de rezoluție ale entității financiare, inclusiv cu persoanele numite de acestea; 160.8. drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale, în conformitate cu așteptările BNM și ale autorităților de rezoluție; 160.9. condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale în conformitate cu pct. 87.			
(3) Acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante includ, în plus față de elementele menționate la alineatul (2), cel puțin următoarele:	PF+CN	161. Acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante includ, în plus față de elementele menționate la pct. 160, cel puțin următoarele:	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(a) descrieri complete la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora, cu obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite monitorizarea eficace de către entitatea financiară a serviciilor TIC și adoptarea unor măsuri corective adecvate, fără întârzieri nejustificate, atunci când nu sunt asigurate nivelurile convenite ale serviciilor; (b) perioade de preaviz și obligații de raportare către entitatea financiară pentru furnizorul terț de servicii TIC, inclusiv notificarea oricărei evoluții care ar putea avea un impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC în sprijinul funcțiilor critice sau importante, în concordanță cu nivelurile convenite ale serviciului; (c) cerințe ca furnizorul terț de servicii TIC să pună în aplicare și să testeze planuri pentru situații neprevăzute și să dispună de măsuri, instrumente și politici în materie de securitate a TIC care să asigure un nivel adecvat de securitate în ceea ce privește furnizarea serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare; (d) obligația furnizorului terț de servicii TIC de a participa la TLPT ale entității financiare și de a coopera pe deplin în cadrul realizării acestora, astfel cum se menționează la articolele 26 și 27; (e) dreptul de a monitoriza, în permanență, performanța furnizorului terț de servicii TIC, care presupune următoarele: (i) drepturile nerestricționate de acces, de inspecție și de audit de către entitatea financiară sau o parte terță desemnată și de către autoritatea competentă, precum și dreptul de a produce copii ale documentelor relevante la fața locului, dacă acestea sunt esențiale pentru operațiunile furnizorului terț de servicii TIC, drepturi a căror exercitare efectivă nu este împiedicată sau limitată de alte acorduri contractuale sau politici de punere în aplicare; (ii) dreptul de a conveni asupra unor niveluri de asigurare alternative în cazul în care sunt afectate drepturile altor clienți;		161.1. descrieri complete la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora, cu obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite monitorizarea eficace de către entitatea financiară a serviciilor TIC și adoptarea unor măsuri corective adecvate, fără întârzieri nejustificate, atunci când nu sunt asigurate nivelurile convenite ale serviciilor; 161.2. perioade de preaviz și obligații de raportare către entitatea financiară pentru furnizorul terț de servicii TIC, inclusiv notificarea oricărei evoluții care ar putea avea un impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC în sprijinul funcțiilor critice sau importante, în concordanță cu nivelurile convenite ale serviciului; 161.3. cerințe ca furnizorul terț de servicii TIC să pună în aplicare și să testeze planuri pentru situații neprevăzute și să dispună de măsuri, instrumente și politici în materie de securitate a TIC care să asigure un nivel adecvat de securitate în ceea ce privește furnizarea serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare; 161.4. obligația furnizorului terț de servicii TIC de a participa la TLPT ale entității financiare și de a coopera pe deplin în cadrul realizării acestora; 161.5. dreptul de a monitoriza, în permanență, performanța furnizorului terț de servicii TIC, care presupune următoarele: a) drepturile nerestricționate de acces, de inspecție și de audit de către entitatea financiară sau o parte terță desemnată și de către BNM, precum și dreptul de a produce copii ale documentelor relevante la fața locului, dacă acestea sunt esențiale pentru operațiunile furnizorului terț de servicii TIC, drepturi a căror exercitare efectivă nu este împiedicată sau limitată de alte acorduri contractuale sau politici de punere în aplicare; b) dreptul de a conveni asupra unor niveluri de asigurare alternative în cazul în care sunt afectate drepturile altor clienți;			

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(iii) obligația furnizorului terț de servicii TIC de a coopera pe deplin în timpul inspecțiilor și auditurilor la fața locului efectuate de autoritățile competente, de supraveghetorul principal, de entitatea financiară sau de o parte terță desemnată; și (iv) obligația de a transmite detalii privind domeniul de aplicare, procedurile care trebuie urmate și frecvența unor astfel de inspecții și audituri; (f) strategiile de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii: (i) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile TIC respective vizând să reducă riscul de perturbare în cadrul entității financiare sau să asigure rezoluția și restructurarea sa eficace; (ii) care permite entității financiare să migreze către un alt furnizor terț de servicii TIC sau să treacă la soluții dezvoltate de aceasta pe plan intern, în conformitate cu complexitatea serviciului furnizat.		c) obligația furnizorului terț de servicii TIC de a coopera pe deplin în timpul inspecțiilor și auditurilor la fața locului efectuate de BNM, de entitatea financiară sau de o parte terță desemnată; și d) obligația de a transmite detalii privind domeniul de aplicare, procedurile care trebuie urmate și frecvența unor astfel de inspecții și audituri; 161.6. strategiile de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii: a) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile TIC respective vizând să reducă riscul de perturbare în cadrul entității financiare sau să asigure rezoluția și restructurarea sa eficace; b) care permite entității financiare să migreze către un alt furnizor terț de servicii TIC sau să treacă la soluții dezvoltate de aceasta pe plan intern, în conformitate cu complexitatea serviciului furnizat.		
Prin derogare de la litera (e), furnizorul terț de servicii TIC și entitatea financiară care este o microîntreprindere pot conveni ca drepturile de acces, de inspecție și de audit ale entității financiare să poată fi delegate unui terț independent, numit de furnizorul terț de servicii TIC, și ca entitatea financiară să poată solicita în orice moment din partea terțului informații și asigurări cu privire la performanța furnizorului terț de servicii TIC.	PF	162. Prin derogare de la subpct. 161.5, furnizorul terț de servicii TIC și entitatea financiară care este o microîntreprindere pot conveni ca drepturile de acces, de inspecție și de audit ale entității financiare să poată fi delegate unui terț independent, numit de furnizorul terț de servicii TIC, și ca entitatea financiară să poată solicita în orice moment din partea terțului informații și asigurări cu privire la performanța furnizorului terț de servicii TIC.	-	compatibil	-
(4) La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard elaborate de autoritățile publice pentru servicii specifice.	PF	163. La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard elaborate de autoritățile publice pentru servicii specifice.	-	compatibil	-
(5) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare cu privire la elementele menționate la alineatul (2) litera (a), pe care o entitate financiară trebuie să le stabilească și să le evalueze atunci când subcontractează servicii TIC care sprijină funcții critice sau importante. Atunci când elaborează aceste proiecte de standarde tehnice de reglementare, AES țin seama de	N/A	-	-	prevederi UE neaplicabile	Mandat al AES de elaborare a standardelor tehnice. Nu necesită măsuri naționale. Standardele adoptate de Comisia Europeană în temeiul mandatului se analizează separat.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
dimensiunea și de profilul general de risc al entității financiare, precum și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Secțiunea II Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC **Articolul 31. Desemnarea furnizorilor terți esențiali de servicii TIC** (1) AES, prin intermediul Comitetului comun și la recomandarea Forumului de supraveghere instituit în temeiul articolului 32 alineatul (1): (a) desemnează furnizorii terți de servicii TIC care sunt esențiali pentru entitățile financiare, în urma unei evaluări care ține seama de criteriile menționate la alineatul (2); (b) desemnează drept supraveghetor principal pentru fiecare furnizor terț esențial de servicii TIC acea AES care este responsabilă, în conformitate cu Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 sau (UE) nr. 1095/2010, de entitățile financiare care dețin împreună cea mai mare parte a activelor totale din valoarea activelor totale ale tuturor entităților financiare care utilizează serviciile furnizorului terț esențial de servicii TIC relevant, astfel cum reiese din suma bilanțurilor individuale ale entităților financiare respective. (2) Desemnarea prevăzută la alineatul (1) litera (a) se bazează pe toate criteriile următoare în ceea ce privește serviciile TIC furnizate de furnizorul terț de servicii TIC: (a) impactul sistemic asupra stabilității, continuității sau calității furnizării serviciilor financiare în situația în care furnizorul terț de servicii TIC relevant s-ar confrunta cu o defecțiune operațională la scară largă în ceea ce privește furnizarea serviciilor sale, ținând	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
seama de numărul de entități financiare și de valoarea totală a activelor entităților financiare cărora furnizorul terț de servicii TIC relevant le oferă servicii; (b) caracterul sistemic sau importanța entităților financiare care se bazează pe furnizorul terț de servicii TIC relevant, evaluată în conformitate cu următorii parametri: (i) numărul de instituții de importanță sistemică globală (G-SII) sau de alte instituții de importanță sistemică (O-SII) care se bazează pe respectivul furnizor terț de servicii TIC; (ii) interdependența dintre G-SII sau O-SII menționate la punctul (i) și alte entități financiare, inclusiv situațiile în care G-SII sau O-SII furnizează servicii de infrastructură financiară altor entități financiare; (c) dependența entităților financiare de serviciile furnizate de furnizorul terț de servicii TIC relevant în ceea ce privește funcțiile critice sau importante ale entităților financiare care implică, în ultimă instanță, același furnizor terț de servicii TIC, indiferent dacă entitățile financiare se bazează direct sau indirect pe aceste servicii, prin intermediul unor acorduri de subcontractare; (d) gradul de substituibilitate a furnizorului terț de servicii TIC, ținând seama de următorii parametri: (i) lipsa unor alternative reale, chiar și parțiale, având în vedere numărul limitat de furnizori terți de servicii TIC activi pe o anumită piață sau cota de piață deținută de furnizorul terț de servicii TIC relevant sau complexitatea tehnică ori gradul de sofisticare implicat, inclusiv în ceea ce privește orice tehnologie protejată, sau caracteristicile specifice ale modului de organizare sau ale activității furnizorului terț de servicii TIC; (ii) dificultăți în ceea ce privește migrarea parțială sau integrală a datelor și a volumelor de lucru relevante de la furnizorul terț de servicii TIC relevant către un alt furnizor terț de servicii TIC, fie ca urmare a costurilor financiare semnificative, a timpului sau a altor resurse pe care le poate implica procesul de migrare, fie din cauza unor riscuri TIC sporite sau a altor riscuri operaționale la care poate fi expusă entitatea financiară prin intermediul unei astfel de migrări.					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(3) În cazul în care furnizorul terț de servicii TIC face parte dintr-un grup, criteriile menționate la alineatul (2) sunt examinate în raport cu serviciile TIC furnizate de grup în ansamblul său. (4) Furnizorii terți esențiali de servicii TIC care fac parte dintr-un grup desemnează o persoană juridică drept punct de coordonare pentru a asigura în mod adecvat reprezentarea și comunicarea cu supraveghetorul principal. (5) Supraveghetorul principal notifică furnizorului terț de servicii TIC rezultatul evaluării care a dus la desemnarea menționată la alineatul (1) litera (a). În termen de șase săptămâni de la data notificării, furnizorul terț de servicii TIC îi poate transmite supraveghetorului principal o declarație motivată conținând orice informații relevante în scopul evaluării. Supraveghetorul principal analizează declarația motivată și poate solicita să îi fie furnizate informații suplimentare în termen de 30 de zile calendaristice de la primirea unei astfel de declarații. După ce a desemnat un furnizor terț de servicii TIC ca fiind esențial, AES, prin intermediul Comitetului comun, informează furnizorul terț de servicii TIC cu privire la această desemnare și cu privire la data de la care va începe să facă efectiv obiectul activităților de supraveghere. Data respectivă trebuie să fie la cel mult o lună de la momentul notificării. Furnizorul terț de servicii TIC informează entitățile financiare cărora le furnizează servicii cu privire la desemnarea sa drept esențial. (6) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin precizarea mai în detaliu a criteriilor menționate la alineatul (2) de la prezentul articol, până la 17 iulie 2024. (7) Nu se recurge la desemnarea menționată la alineatul (1) litera (a) decât după ce Comisia a adoptat un act delegat în conformitate cu alineatul (6). (8) Desemnarea menționată la alineatul (1) litera (a) nu se aplică în ceea ce privește: (i) entitățile financiare care furnizează servicii TIC altor entități financiare;					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(ii) furnizorii terți de servicii TIC care fac obiectul unor cadre de supraveghere instituite cu scopul de a sprijini misiunile menționate la articolul 127 alineatul (2) din Tratatul privind funcționarea Uniunii Europene; (iii) furnizorii de servicii TIC intragrup; (iv) furnizorii terți de servicii TIC care furnizează servicii TIC numai într-un stat membru unor entități financiare care își desfășoară activitatea numai în statul membru respectiv. (9) AES, prin intermediul Comitetului comun, elaborează, publică și actualizează anual lista furnizorilor terți esențiali de servicii TIC la nivelul Uniunii. (10) În sensul alineatului (1) litera (a), autoritățile competente transmit, anual și agregat, Forumului de supraveghere instituit în temeiul articolului 32 rapoartele menționate la articolul 28 alineatul (3) al treilea paragraf. Forumul de supraveghere evaluează dependențele entităților financiare față de furnizorii terți de servicii TIC pe baza informațiilor primite de la autoritățile competente. (11) Furnizorii terți de servicii TIC care nu sunt incluși în lista menționată la alineatul (9) pot solicita să fie desemnați ca fiind esențiali în conformitate cu alineatul (1) litera (a). În scopul aplicării primului paragraf, furnizorul terț de servicii TIC transmite o cerere motivată către ABE, ESMA sau EIOPA care, prin intermediul Comitetului comun, decide dacă să desemneze respectivul furnizor terț de servicii TIC ca fiind esențial în conformitate cu alineatul (1) litera (a). Decizia menționată la al doilea paragraf se adoptă și se notifică furnizorului terț de servicii TIC în termen de șase luni de la primirea cererii. (12) Entitățile financiare utilizează serviciile unui furnizor terț de servicii TIC stabilit într-o țară terță și care a fost desemnat ca fiind esențial în conformitate cu alineatul (1) litera (a) numai în cazul în care acesta din urmă a înființat o filială în Uniune în termen de 12 luni de la desemnare. (13) Furnizorul terț esențial de servicii TIC menționat la alineatul (12) informează supraveghetorul principal					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
cu privire la orice modificare a structurii conducerii filialei înființate în Uniune.					
Articolul 32. Structura cadrului de supraveghere (1) Comitetul comun, în conformitate cu articolul 57 alineatul (1) din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, instituie Forumul de supraveghere ca subcomitet în scopul sprijinirii activității Comitetului comun și a supraveghetorului principal menționat la articolul 31 alineatul (1) litera (b) în domeniul riscurilor TIC generate de părți terțe în toate sectoarele financiare. Forumul de supraveghere pregătește proiectele de poziții comune și de acte comune ale Comitetului comun în acest domeniu. Forumul de supraveghere discută periodic despre evoluțiile relevante cu privire la riscurile și vulnerabilitățile TIC și promovează o abordare consecventă în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe la nivelul Uniunii. (2) Forumul de supraveghere efectuează anual o evaluare colectivă a rezultatelor și a constatărilor activităților de supraveghere desfășurate pentru toți furnizorii terți esențiali de servicii TIC și promovează măsuri de coordonare pentru a spori reziliența operațională digitală a entităților financiare, a încuraja cele mai bune practici în ceea ce privește abordarea riscurilor de concentrare a serviciilor TIC și a studia factorii de diminuare în cazul transferurilor riscurilor la nivel transsectorial. (3) Forumul de supraveghere prezintă criterii de referință cuprinzătoare pentru furnizorii terți esențiali de servicii TIC, care urmează să fie adoptate de Comitetul comun ca poziții comune ale AES în conformitate cu articolul 56 alineatul (1) din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010. (4) Forumul de supraveghere este compus din: (a) președinții AES; (b) un reprezentant la nivel înalt provenind din personalul actual al autorității competente relevante menționate la articolul 46 din fiecare stat membru;	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) directorii executivi ai fiecărei AES și câte un reprezentant din partea Comisiei, CERS, BCE și ENISA, în calitate de observatori; (d) după caz, un reprezentant suplimentar al unei autorități competente menționate la articolul 46 din fiecare stat membru, în calitate de observator; (e) după caz, un reprezentant al autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, în calitate de observator. Forumul de supraveghere poate, după caz, să solicite avizul unor experți independenți numiți în conformitate cu alineatul (6). (5) Fiecare stat membru desemnează autoritatea competentă relevantă din cadrul personalului căreia este numit reprezentantul la nivel înalt menționat la alineatul (4) primul paragraf litera (b) și informează supraveghetorul principal în acest sens. AES publică pe site-ul lor lista reprezentanților la nivel înalt, provenind din personalul actual al autorității competente relevante, desemnați de statele membre. (6) Experții independenți menționați la alineatul (4) al doilea paragraf sunt numiți de Forumul de supraveghere dintr-un grup de rezervă de experți selectați în urma unui proces de candidatură public și transparent. Experții independenți sunt numiți pe baza cunoștințelor și experienței lor în materie de stabilitate financiară, reziliență operațională digitală și securitate TIC. Aceștia acționează independent și obiectiv în interesul exclusiv al Uniunii în ansamblul său și nu solicită și nu primesc instrucțiuni din partea instituțiilor sau a organelor Uniunii, din partea vreunui guvern al unui stat membru sau din partea vreunui alt organism public sau privat. (7) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES emit, până la 17 iulie 2024, în scopul aplicării prezentei secțiuni, orientări privind cooperarea dintre AES și autoritățile competente cuprinzând procedurile și condițiile detaliate pentru					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
alocarea și executarea sarcinilor între autoritățile competente și AES, precum și detaliile privind schimburile de informații care sunt necesare pentru ca autoritățile competente să se asigure că recomandările adresate furnizorilor terți esențiali de servicii TIC în temeiul articolului 35 alineatul (1) litera (d) sunt urmate. (8) Cerințele prevăzute în prezenta secțiune nu aduc atingere aplicării Directivei (UE) 2022/2555 și a altor norme ale Uniunii privind supravegherea aplicabilă furnizorilor de servicii de cloud computing. (9) AES, prin intermediul Comitetului comun și pe baza lucrărilor pregătitoare desfășurate de Forumul de supraveghere, prezintă anual Parlamentului European, Consiliului și Comisiei un raport privind aplicarea prezentei secțiuni.					
Articolul 33. Sarcinile supraveghetorului principal (1) Supraveghetorul principal, numit în conformitate cu articolul 31 alineatul (1) litera (b), efectuează supravegherea furnizorilor terți esențiali de servicii TIC atribuiți și este, cu privire la toate aspectele legate de supraveghere, punctul de contact principal pentru respectivii furnizori terți esențiali de servicii TIC. (2) În scopul aplicării alineatului (1), supraveghetorul principal evaluează dacă fiecare furnizor terț esențial de servicii TIC a instituit norme, proceduri, mecanisme și măsuri cuprinzătoare, solide și eficace de gestionare a riscurilor TIC pe care le poate genera pentru entitățile financiare. Evaluarea menționată la primul paragraf se axează în principal pe serviciile TIC furnizate de furnizorul terț esențial de servicii TIC care sprijină funcțiile critice sau importante ale entităților financiare. Atunci când este necesar pentru a aborda toate riscurile relevante, evaluarea respectivă se extinde la serviciile TIC care sprijină alte funcții decât cele critice sau importante. (3) Evaluarea prevăzută la alineatul (2) cuprinde: (a) cerințele privind TIC pentru a asigura, în special, securitatea, disponibilitatea, continuitatea, scalabilitatea și calitatea serviciilor pe care furnizorul terț esențial de servicii TIC le furnizează entităților financiare, precum și capacitatea de a menține în permanență standarde înalte de disponibilitate,	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
autenticitate, integritate sau confidențialitate a datelor; (b) securitatea fizică ce contribuie la asigurarea securității TIC, inclusiv securitatea sediilor, a instalațiilor, a centrelor de date; (c) procesele de gestionare a riscurilor, inclusiv politicile de gestionare a riscurilor TIC, politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC; (d) mecanismele de guvernanță, inclusiv o structură organizatorică cu arii de responsabilitate și norme privind răspunderea clare, transparente și coerente, care permit gestionarea eficace a riscurilor TIC; (e) identificarea, monitorizarea și raportarea promptă a incidentelor semnificative legate de TIC către entitățile financiare, gestionarea și soluționarea acestor incidente, în special a atacurilor cibernetice; (f) mecanismele de portabilitate a datelor, de portabilitate a aplicațiilor și de interoperabilitate, care asigură exercitarea efectivă a drepturilor de încetare de către entitățile financiare; (g) testarea sistemelor, a infrastructurii și a controalelor TIC; (h) auditurile privind TIC; (i) utilizarea standardelor naționale și internaționale relevante aplicabile furnizării serviciilor sale TIC către entitățile financiare. (4) Pe baza evaluării prevăzute la alineatul (2) și în coordonare cu Rețeaua de supraveghere comună (RSC) menționată la articolul 34 alineatul (1), supraveghetorul principal adoptă un plan de supraveghere individual clar, detaliat și motivat care descrie obiectivele anuale de supraveghere și principalele acțiuni de supraveghere planificate pentru fiecare furnizor terț esențial de servicii TIC. Planul respectiv este comunicat în fiecare an furnizorului terț esențial de servicii TIC. Înainte de adoptarea planului de supraveghere, supraveghetorul principal comunică proiectul planului de supraveghere furnizorului terț esențial de servicii TIC. La primirea proiectului de plan de supraveghere, furnizorul terț esențial de servicii TIC poate prezenta,					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
în termen de 15 zile calendaristice, o declarație motivată prin care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor. (5) Odată ce planurile de supraveghere anuale menționate la alineatul (4) au fost adoptate și notificate furnizorilor terți esențiali de servicii TIC, autoritățile competente pot lua măsuri privind acești furnizori terți esențiali de servicii TIC numai în acord cu supraveghetorul principal.					
Articolul 34. Coordonarea operațională a supraveghetorilor principali (1) Pentru a asigura o abordare coerentă a activităților de supraveghere și a permite coordonarea strategiilor generale de supraveghere și coeziunea abordărilor operaționale și a metodologiilor de lucru, cei trei supraveghetori principali numiți în conformitate cu articolul 31 alineatul (1) litera (b) instituie o RSC pentru a-și coordona acțiunile în cursul etapelor pregătitoare și al desfășurării activităților de supraveghere a furnizorilor terți esențiali de servicii TIC pe care îi supraveghează fiecare dintre ei, precum și în cursul oricărei acțiuni care ar putea fi necesară în temeiul articolului 42. (2) În scopul aplicării alineatului (1), supraveghetorii principali elaborează un protocol de supraveghere comun în care precizează procedurile detaliate care trebuie urmate pentru realizarea coordonării curente și pentru asigurarea unor schimburi și reacții rapide. Protocolul este revizuit periodic pentru a reflecta nevoile operaționale, în special evoluția modalităților practice de supraveghere. (3) Supraveghetorii principali pot solicita ad-hoc BCE și ENISA să ofere consiliere tehnică, să facă schimb de experiență practică sau să participe la anumite reuniuni de coordonare ale RSC.	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.
Articolul 35. Competențele supraveghetorului principal (1) În scopul îndeplinirii atribuțiilor care îi revin în temeiul prezentei secțiuni, supraveghetorul principal	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES,

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
are următoarele competențe în ceea ce privește furnizorii terți esențiali de servicii TIC: (a) de a solicita toate informațiile și documentele relevante în conformitate cu articolul 37; (b) de a efectua investigații generale și inspecții în conformitate cu articolele 38 și, respectiv, 39; (c) de a solicita, după încheierea activităților de supraveghere, rapoarte în care se specifică acțiunile întreprinse sau măsurile de remediere care au fost puse în aplicare de furnizorii terți esențiali de servicii TIC în legătură cu recomandările menționate la litera (d) de la prezentul alineat; (d) de a emite recomandări privind domeniile menționate la articolul 33 alineatul (3), în special privind: (i) utilizarea unor cerințe sau procese specifice de securitate și calitate în domeniul TIC, în special în ceea ce privește introducerea de corecții, actualizări, criptări și alte măsuri de securitate pe care supraveghetorul principal le consideră relevante pentru asigurarea securității din perspectiva TIC a serviciilor furnizate entităților financiare; (ii) utilizarea termenelor și condițiilor, inclusiv punerea în aplicare tehnică a acestora, potrivit cărora furnizorii terți esențiali de servicii TIC furnizează servicii TIC entităților financiare, pe care supraveghetorul principal le consideră relevante pentru prevenirea generării unor puncte unice de defecțiune sau a amplificării acestora sau pentru reducerea la minimum a impactului sistemic potențial la nivelul sectorului financiar al Uniunii în cazul unor riscuri de concentrare a serviciilor TIC; (iii) orice subcontractare planificată, în cazul în care supraveghetorul principal consideră că subcontractarea în continuare, inclusiv acordurile de subcontractare pe care furnizorii terți esențiali de servicii TIC intenționează să le încheie cu furnizori terți de servicii TIC sau cu subcontractanți de servicii TIC stabiliți într-o țară terță, poate genera riscuri pentru furnizarea de servicii de către entitatea financiară sau riscuri pentru stabilitatea financiară, pe baza examinării informațiilor colectate în conformitate cu articolele 37 și 38;					supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(iv) abținerea de la încheierea unui nou acord de subcontractare, în cazul în care sunt îndeplinite următoarele condiții cumulative: — subcontractantul avut în vedere este un furnizor terț de servicii TIC sau un subcontractant de servicii TIC stabilit într-o țară terță; — subcontractarea vizează funcții critice sau importante ale entității financiare; și — supraveghetorul principal consideră că utilizarea unei astfel de subcontractări prezintă un risc clar și grav pentru stabilitatea financiară a Uniunii sau pentru entitățile financiare, inclusiv pentru capacitatea entităților financiare de a se conforma cerințelor de supraveghere. În scopul aplicării punctului (iv) de la prezenta literă, furnizorii terți de servicii TIC transmit informațiile privind subcontractarea supraveghetorului principal, utilizând modelul prevăzut la articolul 41 alineatul (1) litera (b). (2) Atunci când exercită competențele prevăzute la prezentul articol, supraveghetorul principal: (a) asigură o coordonare regulată în cadrul RSC și, în special, urmărește aplicarea unor abordări coerente, după caz, în ceea ce privește supravegherea furnizorilor terți esențiali de servicii TIC; (b) ține seama în mod corespunzător de cadrul instituit prin Directiva (UE) 2022/2555 și, atunci când este necesar, consultă autoritățile competente relevante desemnate sau instituite în conformitate cu directiva respectivă, pentru a evita suprapunerea măsurilor tehnice și organizatorice care s-ar putea aplica furnizorilor terți esențiali de servicii TIC în temeiul directivei respective; (c) urmărește să reducă la minimum, în măsura posibilului, riscul de perturbare a serviciilor furnizate de furnizori terți esențiali de servicii TIC unor clienți care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament.					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(3) Supraveghetorul principal consultă Forumul de supraveghere înainte de a exercita competențele menționate la alineatul (1). Înainte de a emite recomandări în conformitate cu alineatul (1) litera (d), supraveghetorul principal îi oferă furnizorului terț de servicii TIC posibilitatea de a prezenta, în termen de 30 de zile calendaristice, informații relevante care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor. (4) Supraveghetorul principal informează RSC cu privire la rezultatul exercitării competențelor prevăzute la alineatul (1) literele (a) și (b). Supraveghetorul principal transmite fără întârzieri nejustificate rapoartele menționate la alineatul (1) litera (c) către RSC și către autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC. (5) Furnizorii terți esențiali de servicii TIC cooperează cu bună credință cu supraveghetorul principal și îl asistă pe acesta în îndeplinirea sarcinilor sale. (6) În cazul nerespectării totale sau parțiale a măsurilor care trebuie luate ca urmare a exercitării competențelor prevăzute la alineatul (1) literele (a), (b) și (c) și după expirarea unui termen de cel puțin 30 de zile calendaristice de la data la care furnizorul terț esențial de servicii TIC a fost notificat cu privire la măsurile respective, supraveghetorul principal adoptă o decizie prin care impune o penalitate cu titlu cominatoriu pentru a obliga furnizorul terț esențial de servicii TIC să se conformeze măsurilor respective. (7) Penalitățile cu titlu cominatoriu prevăzute la alineatul (6) se impun pe zi de întârziere până când conformitatea este asigurată și pe o perioadă de maximum șase luni de la data notificării deciziei de impunere a unei penalități cu titlu cominatoriu furnizorului terț esențial de servicii TIC. (8) Cuantumul penalității cu titlu cominatoriu, calculat de la data prevăzută în decizia de impunere a penalității cu titlu cominatoriu, este de până la 1 % din cifra de afaceri zilnică medie globală a furnizorului terț esențial de servicii TIC din exercițiul financiar					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
precedent. La stabilirea cuantumului penalității cu titlu cominatoriu, supraveghetorul principal ține seama de următoarele criterii referitoare la nerespectarea măsurilor prevăzute la alineatul (6): (a) gravitatea și durata neconformității; (b) dacă neconformitatea a fost săvârșită în mod intenționat sau din neglijență; (c) nivelul de cooperare al furnizorului terț de servicii TIC cu supraveghetorul principal. În scopul aplicării primului paragraf, pentru a asigura o abordare coerentă, supraveghetorul principal efectuează consultări în cadrul RSC. (9) Penalitățile cu titlu cominatoriu sunt de natură administrativă și sunt executorii. Executarea este reglementată de normele de procedură civilă în vigoare în statul membru pe teritoriul căruia au loc inspecțiile și este acordat accesul. Plângerile legate de neregulile survenite în cursul executării sunt de competența instanțelor judecătorești ale statului membru în cauză. Sumele aferente penalităților se alocă bugetului general al Uniunii Europene. (10) Supraveghetorul principal face publice toate penalitățile cu titlu cominatoriu aplicate, cu excepția cazurilor în care publicarea lor ar perturba grav pieţele financiare sau ar aduce un prejudiciu disproporționat părților implicate. (11) Înainte de a impune o penalitate cu titlu cominatoriu în temeiul alineatului (6), supraveghetorul principal oferă reprezentanților furnizorului terț esențial de servicii TIC care face obiectul procedurii posibilitatea de a fi audiat cu privire la constatări și își întemeiază deciziile numai pe constatările asupra cărora furnizorul terț esențial de servicii TIC care face obiectul procedurii a avut ocazia să își prezinte observațiile. Dreptul la apărare al persoanelor care fac obiectul procedurii se respectă pe deplin pe durata acesteia. Furnizorul terț esențial de servicii TIC care face obiectul procedurii are dreptul de a avea acces la dosar, sub rezerva interesului legitim al altor persoane de a-și proteja secretele comerciale. Dreptul de acces la dosar nu se extinde și la					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
informațiile confidențiale sau la documentele interne de lucru ale supraveghetorului principal.					
Articolul 36. Exercitarea competențelor supraveghetorului principal în afara Uniunii (1) Atunci când obiectivele de supraveghere nu pot fi atinse prin intermediul interacțiunii cu filiala înființată potrivit dispozițiilor articolului 31 alineatul (12) sau prin exercitarea de activități de supraveghere la sedii situate în Uniune, supraveghetorul principal poate exercita competențele menționate la următoarele dispoziții, cu privire la orice sediu situat într-o țară terță care este deținut sau utilizat în orice mod în scopul furnizării de servicii către entități financiare din Uniune de către un furnizor terț esențial de servicii TIC, în legătură cu operațiunile, funcțiile sau serviciile sale comerciale, inclusiv orice birou, sediu, teren, clădire sau altă proprietate folosită cu scop administrativ, comercial sau operațional: (a) la articolul 35 alineatul (1) litera (a); și (b) la articolul 35 alineatul (1) litera (b), în conformitate cu articolul 38 alineatul (2) literele (a), (b) și (d) și articolul 39 alineatul (1) și alineatul (2) litera (a). Competențele menționate la primul paragraf pot fi exercitate sub rezerva îndeplinirii tuturor condițiilor următoare: (i) supraveghetorul principal consideră că efectuarea unei inspecții într-o țară terță este necesară pentru a-i permite să își îndeplinească pe deplin și în mod eficace sarcinile care îi revin în temeiul prezentului regulament; (ii) inspecția într-o țară terță este direct legată de furnizarea de servicii TIC unor entități financiare din Uniune; (iii) furnizorul terț esențial de servicii TIC în cauză este de acord cu efectuarea unei inspecții într-o țară terță; și (iv) autoritatea relevantă din țara terță în cauză a fost notificată oficial de supraveghetorul principal și nu a formulat nicio obiecție cu privire la aceasta. (2) Fără a aduce atingere competențelor instituțiilor Uniunii și, respectiv, ale statelor membre, în scopul aplicării alineatului (1), ABE, ESMA sau EIOPA încheie	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
acorduri de cooperare administrativă cu autoritatea relevantă din țara terță pentru a permite buna desfășurare a inspecțiilor în țara terță în cauză de către supraveghetorul principal și echipa desemnată de acesta pentru misiunea sa în țara terță respectivă. Aceste acorduri de cooperare nu creează obligații juridice pentru Uniune și statele sale membre și nu împiedică statele membre și autoritățile lor competente să încheie acorduri bilaterale sau multilaterale cu țările terțe respective și cu autoritățile competente ale acestora. Aceste acorduri de cooperare specifică cel puțin următoarele elemente: (a) procedurile privind coordonarea activităților de supraveghere desfășurate în temeiul prezentului regulament și orice monitorizare analoagă a riscurilor TIC generate de părți terțe în sectorul financiar efectuată de autoritatea relevantă din țara terță în cauză, inclusiv detaliile privind transmiterea acordului acesteia din urmă pentru a permite efectuarea, de către supraveghetorul principal și echipa desemnată de acesta, a investigațiilor generale și a inspecțiilor la fața locului menționate la alineatul (1) primul paragraf pe teritoriul aflat sub jurisdicția sa; (b) mecanismul de transmitere a oricăror informații relevante între ABE, ESMA sau EIOPA și autoritatea relevantă din țara terță în cauză, în special în legătură cu informațiile care pot fi solicitate de supraveghetorul principal în temeiul articolului 37; (c) mecanismele prin care se realizează notificarea promptă de către autoritatea relevantă din țara terță în cauză a ABE, ESMA sau EIOPA cu privire la cazurile în care se consideră că un furnizor terț de servicii TIC stabilit într-o țară terță și desemnat ca fiind esențial în conformitate cu articolul 31 alineatul (1) litera (a) a încălcat cerințele pe care este obligat să le respecte în temeiul dreptului aplicabil al țării terțe în cauză atunci când furnizează servicii unor instituții financiare din țara terță respectivă, precum și măsurile corective și sancțiunile aplicate; (d) transmiterea periodică de informații actualizate privind evoluțiile în materie de reglementare sau de supraveghere în ceea ce privește monitorizarea					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
riscurilor TIC generate de părți terțe ale instituțiilor financiare din țara terță în cauză; (e) detaliile pentru a permite, dacă este necesar, participarea unui reprezentant al autorității competente din țara terță la inspecțiile efectuate de supraveghetorul principal și de echipa desemnată. (3) În cazul în care supraveghetorul principal nu este în măsură să desfășoare activitățile de supraveghere în afara Uniunii menționate la alineatele (1) și (2), supraveghetorul principal: (a) își exercită competențele prevăzute la articolul 35 pe baza tuturor faptelor și documentelor de care dispune; (b) documentează și explică orice consecință a imposibilității sale de a desfășura activitățile de supraveghere preconizate la care se referă prezentul articol. Consecințele potențiale menționate la litera (b) de la prezentul alineat sunt luate în considerare în cadrul recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d).					
Articolul 37. Solicitarea de informații (1) Supraveghetorul principal poate, printr-o simplă cerere sau printr-o decizie, să solicite furnizorilor terți esențiali de servicii TIC să furnizeze toate informațiile necesare pentru ca supraveghetorul principal să își îndeplinească sarcinile care îi revin în temeiul prezentului regulament, inclusiv toate documentele comerciale sau operaționale relevante, contractele, documentele de politică, rapoartele de audit privind securitatea TIC, rapoartele privind incidentele legate de TIC, precum și orice informații legate de părțile cărora furnizorul terț esențial de servicii TIC le-a externalizat funcții sau activități operaționale. (2) Atunci când trimite o simplă solicitare de informații în temeiul alineatului (1), supraveghetorul principal: (a) face trimitere la prezentul articol ca temei juridic al solicitării sale; (b) menționează scopul solicitării; (c) specifică informațiile care sunt solicitate; (d) stabilește un termen pentru furnizarea informațiilor;	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(e) informează reprezentantul furnizorului terț esențial de servicii TIC de la care sunt solicitate informațiile cu privire la faptul că acesta nu este obligat să furnizeze informațiile, dar că, în cazul unui răspuns voluntar la solicitare, informațiile furnizate nu trebuie să fie incorecte sau să inducă în eroare. (3) Atunci când solicită printr-o decizie furnizarea de informații în temeiul alineatului (1), supraveghetorul principal: (a) face trimitere la prezentul articol ca temei juridic al solicitării sale; (b) menționează scopul solicitării; (c) specifică informațiile care sunt solicitate; (d) stabilește un termen pentru furnizarea informațiilor; (e) indică penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) în cazul în care informațiile solicitate sunt furnizate incomplet sau dacă aceste informații nu sunt furnizate în termenul menționat la litera (d) de la prezentul alineat; (f) indică dreptul de a contesta decizia în fața comisiei de apel a AES și de a solicita controlul legalității deciziei de către Curtea de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție”), în conformitate cu articolele 60 și 61 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010. (4) Reprezentanții furnizorilor terți esențiali de servicii TIC furnizează informațiile solicitate. Avocații autorizați în mod corespunzător să acționeze pot furniza informațiile în numele clienților lor. Furnizorii terți esențiali de servicii TIC au în continuare întreaga responsabilitate în cazul în care informațiile furnizate sunt incomplete, incorecte sau induc în eroare. (5) Supraveghetorul principal transmite fără întârziere o copie a deciziei prin care se solicită furnizarea de informații autorităților competente ale entităților financiare care folosesc serviciile furnizorilor terți esențiali de servicii TIC relevanți și RSC.					
Articolul 38. Investigații generale (1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipa de examinare comună	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
menționată la articolul 40 alineatul (1), poate, atunci când este necesar, să efectueze investigații cu privire la furnizorii terți esențiali de servicii TIC. (2) Supraveghetorul principal este abilitat: (a) să analizeze evidențele, datele, procedurile și orice alte materiale relevante pentru executarea atribuțiilor sale, indiferent de suportul pe care sunt stocate; (b) să facă sau să obțină copii certificate ale unor astfel de evidențe, date, documente care prevăd proceduri și ale oricăror alte materiale, precum și extrase din acestea; (c) să convoace reprezentanții furnizorului terț esențial de servicii TIC pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și să înregistreze răspunsurile; (d) să pună întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări în scopul colectării de informații referitoare la obiectul unei investigații; (e) să solicite înregistrări ale convorbirilor telefonice și ale traficului de date. (3) Funcționarii și celelalte persoane autorizate de supraveghetorul principal în scopul efectuării investigației menționate la alineatul (1) își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul investigației. Autorizația respectivă indică, de asemenea, penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) aplicabile în cazul în care evidențele, datele, documentele care prevăd proceduri sau orice alte materiale solicitate sau răspunsurile la întrebările adresate reprezentanților furnizorului terț de servicii TIC nu sunt furnizate sau sunt incomplete. (4) Reprezentanții furnizorilor terți esențiali de servicii TIC sunt obligați să se supună investigațiilor pe baza unei decizii a supraveghetorului principal. Decizia specifică obiectul și scopul investigației, penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr.					Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție. (5) În timp util înainte de începerea investigației, supraveghetorul principal informează autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC cu privire la investigația preconizată și la identitatea persoanelor autorizate. Supraveghetorul principal comunică RSC toate informațiile primite în temeiul primului paragraf.					
Articolul 39. Inspecții (1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipele de examinare comună menționate la articolul 40 alineatul (1), poate să aibă acces la orice sediu comercial, teren sau proprietate a furnizorilor terți de servicii TIC, cum ar fi sediile sociale, centrele de operațiuni sau sediile secundare, și poate să efectueze toate inspecțiile la fața locului necesare, precum și să efectueze inspecții la distanță. În scopul exercitării competențelor menționate la primul paragraf, supraveghetorul principal consultă RSC. (2) Funcționarii și celelalte persoane autorizate de supraveghetorul principal să efectueze o inspecție la fața locului sunt abilitați: (a) să intre în orice astfel de sediu comercial, teren sau proprietate; și (b) să sigileze orice astfel de sediu comercial, registre sau evidențe, pe perioada inspecției și în măsura în care acest lucru este necesar pentru inspecție. Funcționarii și celelalte persoane autorizate de supraveghetorul principal își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul inspecției, precum și penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) în cazul în care reprezentanții furnizorilor terți esențiali de servicii TIC în cauză nu se supun inspecției.	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(3) În timp util înainte de începerea inspecției, supraveghetorul principal informează autoritățile competente ale entităților financiare care utilizează respectivul furnizor terț de servicii TIC. (4) Inspecțiile acoperă întreaga gamă de sisteme TIC, rețele, dispozitive, informații și date relevante care sunt utilizate sau contribuie la furnizarea de servicii TIC către entități financiare. (5) Înainte de orice inspecție la fața locului planificată, supraveghetorul principal le dă un preaviz rezonabil furnizorilor terți esențiali de servicii TIC, cu excepția cazului în care un astfel de preaviz nu este posibil din cauza unei situații de urgență sau de criză sau în cazul în care acesta ar conduce la o situație în care inspecția sau auditul nu ar mai fi eficace. (6) Furnizorul terț esențial de servicii TIC se supune inspecțiilor la fața locului dispuse prin decizia supraveghetorului principal. Decizia specifică obiectul și scopul inspecției, stabilește data la care va începe inspecția și indică penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție. (7) În cazul în care funcționarii și celelalte persoane autorizate de supraveghetorul principal constată că un furnizor terț esențial de servicii TIC se opune unei inspecții dispuse în temeiul prezentului articol, supraveghetorul principal informează furnizorul terț esențial de servicii TIC cu privire la consecințele unei astfel de opoziții, inclusiv cu privire la posibilitatea ca autoritățile competente ale entităților financiare relevante să solicite entităților financiare să înceteze acordurile contractuale încheiate cu respectivul furnizor terț esențial de servicii TIC.					
Articolul 40. Supravegherea permanentă (1) Atunci când desfășoară activități de supraveghere, în special investigații generale sau inspecții, supraveghetorul principal este asistat de o echipă de examinare comună, instituită pentru fiecare furnizor terț esențial de servicii TIC. (2) Echipa de examinare comună menționată la alineatul (1) este formată din membri ai personalului:	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(a) AES; (b) autorităților competente relevante care supraveghează entitățile financiare cărora furnizorul terț esențial de servicii TIC le oferă servicii TIC; (c) autorității naționale competente menționate la articolul 32 alineatul (4) litera (e), pe bază de voluntariat; (d) unei autorități naționale competente din statul membru în care este stabilit furnizorul terț esențial de servicii TIC, pe bază de voluntariat. Membrii echipei de examinare comună au cunoștințe de specialitate în domeniul TIC și în ceea ce privește riscurile operaționale. Echipa de examinare comună lucrează sub coordonarea unui membru desemnat al personalului supraveghetorului principal („coordonatorul supraveghetorului principal”). (3) În termen de trei luni de la încheierea unei investigații sau a unei inspecții, supraveghetorul principal, după consultarea Forumului de supraveghere, adoptă recomandări care urmează a fi adresate furnizorului terț esențial de servicii TIC în temeiul competențelor menționate la articolul 35. (4) Recomandările menționate la alineatul (3) se comunică imediat furnizorului terț esențial de servicii TIC și autorităților competente ale entităților financiare cărora acesta le furnizează servicii TIC. În scopul executării activităților de supraveghere, supraveghetorul principal poate lua în considerare certificările relevante ale unei părți terțe și rapoartele de audit TIC intern sau extern ale unei părți terțe puse la dispoziție de furnizorul terț esențial de servicii TIC.					măsuri naționale de punere în aplicare.
Articolul 41. Armonizarea condițiilor care permit desfășurarea activităților de supraveghere (1) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a preciza: (a) informațiile care trebuie furnizate de un furnizor terț de servicii TIC în cererea prin care solicită în mod voluntar să fie desemnați ca fiind esențiali în temeiul articolului 31 alineatul (11); (b) conținutul, structura și formatul informațiilor care trebuie transmise, comunicate sau raportate de furnizorii terți de servicii TIC în temeiul articolului 35	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
alineatul (1), inclusiv modelul pentru furnizarea informațiilor privind acordurile de subcontractare; (c) criteriile privind stabilirea componenței echipei de examinare comune, asigurând o participare echilibrată a membrilor personalului AES și a membrilor personalului autorităților competente relevante, precum și modul de desemnare, sarcinile și acordurile de lucru ale acestora; (d) detaliile evaluării efectuate de autoritățile competente cu privire la măsurile luate de furnizorii terți esențiali de servicii TIC pe baza recomandărilor supraveghetorului principal în conformitate cu articolul 42 alineatul (3). (2) AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024. Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (1), în conformitate cu procedura prevăzută la articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.					
Articolul 42. Acțiunile ulterioare întreprinse de autoritățile competente (1) În termen de 60 de zile calendaristice de la primirea recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d), furnizorii terți esențiali de servicii TIC fie informează supraveghetorul principal cu privire la intenția lor de a urma recomandările, fie oferă o explicație cu privire la motivele pentru care nu vor urma recomandările respective. Supraveghetorul principal transmite imediat aceste informații autorităților competente ale entităților financiare în cauză. (2) Supraveghetorul principal face publice cazurile în care un furnizor terț esențial de servicii TIC nu informează supraveghetorul principal în conformitate cu alineatul (1) sau cazurile în care explicația furnizată de furnizorul terț esențial de servicii TIC nu este considerată suficientă. Informațiile publicate dezvăluie identitatea furnizorului terț esențial de servicii TIC, precum și informații privind tipul și natura neconformității. Aceste informații se limitează la	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
ceea ce este pertinent și proporțional în scopul asigurării informării publicului, cu excepția cazului în care această publicare ar cauza prejudicii disproporționate părților implicate sau ar putea periclita grav buna funcționare și integritatea piețelor financiare sau stabilitatea întregului sistem financiar al Uniunii sau a unei părți a acestuia. Supraveghetorul principal informează furnizorul terț de servicii TIC cu privire la respectiva informare publică. (3) Autoritățile competente informează entitățile financiare relevante cu privire la riscurile identificate în cadrul recomandărilor adresate furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 35 alineatul (1) litera (d). Atunci când gestionează riscuri TIC generate de părți terțe, entitățile financiare țin seama de riscurile menționate la primul paragraf. (4) În cazul în care o autoritate competentă consideră că o entitate financiară, în cadrul activității sale de gestionare a riscurilor TIC generate de părți terțe, nu ține seama de riscurile specifice identificate în cadrul recomandărilor sau nu le contracarează suficient, aceasta notifică entitatea financiară cu privire la posibilitatea adoptării unei decizii, în termen de 60 de zile calendaristice de la primirea unei astfel de notificări, în temeiul alineatului (6), în lipsa unor acorduri contractuale adecvate care să aibă drept scop contracararea acestor riscuri. (5) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c) și înainte de a lua o decizie astfel cum se menționează la alineatul (6) de la prezentul articol, autoritățile competente pot, în mod voluntar, să consulte autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC. (6) Autoritățile competente pot, ca măsură de ultimă instanță, în urma informării și, dacă este cazul, a consultării prevăzute la alineatele (4) și (5) din prezentul articol, în conformitate cu articolul 50, să adopte o decizie prin care să solicite entităților					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
financiare să suspende temporar, parțial sau integral, utilizarea sau implementarea unui serviciu furnizat de furnizorul terț esențial de servicii TIC până la contracararea riscurilor identificate în cadrul recomandărilor adresate furnizorilor terți esențiali de servicii TIC. În cazul în care este necesar, acestea pot solicita entităților financiare să rezilieze parțial sau integral acordurile contractuale relevante încheiate cu furnizorii terți esențiali de servicii TIC. (7) În cazul în care un furnizor terț esențial de servicii TIC refuză să accepte recomandările în baza unei abordări divergente față de cea recomandată de supraveghetorul principal, și o astfel de abordare divergentă ar putea avea un impact negativ asupra unui număr mare de entități financiare sau asupra unei părți semnificative a sectorului financiar, iar avertismentele individuale emise de autoritățile competente nu au avut drept rezultat abordări coerente care să atenueze riscul potențial la adresa stabilității financiare, supraveghetorul principal poate, după consultarea Forumului de supraveghere, să emită avize neobligatorii și fără caracter public adresate autorităților competente, pentru a promova măsuri ulterioare de supraveghere coerente și convergente, după caz. (8) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c), autoritățile competente, atunci când iau o decizie în conformitate cu alineatul (6) de la prezentul articol, țin seama de tipul și de amploarea riscului care nu a fost contracarat de furnizorul terț esențial de servicii TIC, precum și de gravitatea neconformității, având în vedere următoarele criterii: (a) gravitatea și durata neconformității; (b) dacă neconformitatea a evidențiat deficiențe grave în ceea ce privește procedurile, sistemele de gestionare, gestionarea riscurilor și controalele interne ale furnizorului terț esențial de servicii TIC; (c) dacă prin neconformitate a fost facilitată sau ocazionată o infracțiune financiară sau dacă aceasta este imputabilă în alt mod neconformității; (d) dacă neconformitatea a fost intenționată sau este rezultatul unei neglijențe;					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(e) dacă suspendarea sau încetarea acordurilor contractuale dă naștere unui risc la adresa continuității activităților economice ale entității financiare în pofida eforturilor acesteia de a evita perturbarea furnizării serviciilor sale; (f) după caz, avizul autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, aviz solicitat în mod voluntar în conformitate cu alineatul (5) de la prezentul articol. Autoritățile competente le acordă entităților financiare perioada de timp necesară pentru a le permite să adapteze acordurile contractuale cu furnizorii terți esențiali de servicii TIC pentru a evita apariția unor efecte negative asupra rezilienței lor operaționale digitale și pentru a le permite să implementeze strategiile de ieșire și planurile de tranziție, astfel cum sunt menționate la articolul 28. (9) Decizia menționată la alineatul (6) de la prezentul articol se notifică membrilor Forumului de supraveghere menționat la articolul 32 alineatul (4) literele (a), (b) și (c) și RSC. Furnizorii terți esențiali de servicii TIC vizați de deciziile prevăzute la alineatul (6) cooperează pe deplin cu entitățile financiare afectate, în special în contextul procesului de suspendare sau de încetare a acordurilor lor contractuale. (10) Autoritățile competente informează periodic supraveghetorul principal cu privire la abordările urmate și măsurile luate în cadrul atribuțiilor lor de supraveghere în ceea ce privește entitățile financiare, precum și cu privire la acordurile contractuale încheiate de entitățile financiare în cazul în care furnizorii terți esențiali de servicii TIC nu au acceptat, parțial sau în întregime, recomandările adresate de supraveghetorul principal. (11) Supraveghetorul principal poate, la cerere, să furnizeze clarificări suplimentare cu privire la recomandările emise pentru a îndruma autoritățile competente cu privire la măsurile ulterioare.					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Articolul 43. Taxele de supraveghere (1) În conformitate cu actul delegat menționat la alineatul (2) de la prezentul articol, supraveghetorul principal percepe de la furnizorii terți esențiali de servicii TIC taxe care acoperă integral cheltuielile necesare ale supraveghetorului principal în legătură cu îndeplinirea atribuțiilor de supraveghere în temeiul prezentului regulament, inclusiv rambursarea oricăror costuri care ar putea fi suportate ca urmare a activității desfășurate de echipa de examinare comună prevăzută la articolul 40, precum și a costurilor aferente consultanței furnizate de experții independenți menționați la articolul 32 alineatul (4) al doilea paragraf, în legătură cu aspecte care intră în sfera activităților de supraveghere directă. Cuantumul unei taxe percepute de la un furnizor terț esențial de servicii TIC acoperă toate costurile care decurg din efectuarea sarcinilor stabilite în prezenta secțiune și este proporțional cu cifra sa de afaceri. (2) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin stabilirea cuantumului taxelor și a modalității de plată a acestora, până la 17 iulie 2024.	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.
Articolul 44. Cooperarea internațională (1) Fără a aduce atingere articolului 36, ABE, ESMA și EIOPA pot, în conformitate cu articolul 33 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010, să încheie acorduri administrative cu autorități de reglementare și de supraveghere din țări terțe pentru a încuraja cooperarea internațională cu privire la riscurile TIC generate de părți terțe în diferite sectoare financiare, în special prin elaborarea de bune practici pentru revizuirea practicilor de gestionare a riscurilor TIC și a controalelor aferente, a măsurilor de atenuare și a răspunsurilor la incidente. (2) AES transmit, prin intermediul Comitetului comun, o dată la cinci ani, un raport confidențial comun Parlamentului European, Consiliului și Comisiei, în care sintetizează constatările discuțiilor relevante purtate cu autoritățile țărilor terțe menționate la alineatul (1), axându-se pe evoluția riscurilor TIC generate de părți terțe și pe implicațiile pentru	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
stabilitatea financiară, integritatea pieței, protecția investitorilor și funcționarea pieței interne.					
CAPITOLUL VI Acorduri privind schimbul de informații **Articolul 45. Acorduri privind schimbul de informații referitoare la informații și date operative privind amenințările cibernetice** (1) Entitățile financiare pot face schimb reciproc de informații și date operative privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative: (a) vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin creșterea gradului de conștientizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare; (b) au loc în cadrul unor comunități de încredere ale entităților financiare; (c) sunt puse în aplicare prin intermediul unor acorduri privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și orientările privind politica în domeniul concurenței.	PF	164. Entitățile financiare pot face schimb reciproc de informații și date operative privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative: 164.1. vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin creșterea gradului de conștientizare cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare; 164.2. au loc în cadrul unor comunități de încredere ale entităților financiare; 164.3. sunt puse în aplicare prin intermediul unor acorduri privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal și reglementările în domeniul concurenței.	-	compatibil	-
(2) În scopul aplicării alineatului (1) litera (c), acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea autorităților publice și calitatea în care acestea pot fi asociate la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.	PF+CN	165. În scopul aplicării subpct. 164.3, acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea BNM și calitatea în care aceasta poate fi asociată la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.	-	compatibil	Autoritatea competentă este redată prin BNM.
(3) Entitățile financiare informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații menționate la alineatul	PF+CN	166. Entitățile financiare informează BNM cu privire la participarea lor la acordurile privind schimbul de informații menționate la pct. 164, în momentul	-	compatibil	Autoritatea competentă este redată prin BNM.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(1), în momentul validării sau, după caz, al încetării participării lor, odată ce aceasta începe să producă efecte.		validării sau, după caz, al încetării participării lor, odată ce aceasta începe să producă efecte.			
CAPITOLUL VII Autoritățile competente **Articolul 46. Autoritățile competente** Fără a aduce atingere dispozițiilor privind cadrul de supraveghere pentru furnizorii terți esențiali de servicii TIC menționat în capitolul V secțiunea II din prezentul regulament, respectarea prezentului regulament este asigurată de următoarele autorități competente în conformitate cu prerogativele conferite prin actele juridice respective: (a) pentru instituțiile de credit și pentru instituțiile exceptate în temeiul Directivei 2013/36/UE, autoritatea competentă desemnată în conformitate cu articolul 4 din directiva respectivă, iar pentru instituțiile de credit clasificate ca fiind semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, BCE, în conformitate cu competențele și atribuțiile conferite prin regulamentul respectiv; (b) pentru instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366, instituțiile emitente de monedă electronică, inclusiv cele exceptate în temeiul Directivei 2009/110/CE, și prestatorii de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366, autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366; (c) pentru firmele de investiții, autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului; (d) pentru furnizorii de servicii de criptoactive autorizați în temeiul Regulamentului privind piețele criptoactivelor și pentru emitenții de tokenuri raportate la active, autoritatea competentă desemnată în conformitate cu dispozițiile relevante din regulamentul respectiv; (e) pentru depozitarii centrali de titluri de valoare, autoritatea competentă desemnată în conformitate cu articolul 11 din Regulamentul (UE) nr. 909/2014;	CN	-	**Legea nr. 202/2017 privind activitatea băncilor, art. 4 alin. (1):** (1) Banca Națională a Moldovei este autoritatea competentă pentru bănci. În acest sens, Banca Națională a Moldovei exercită atribuțiile de licențiere, reglementare și supraveghere prudențială potrivit prevederilor prezentei legi și Legii nr. 548/1995 cu privire la Banca Națională a Moldovei. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 93 alin. (1), alin. (2):** (1) Autorități publice responsabile de supravegherea respectării prezentei legi și a actelor normative emise în vederea executării legii sînt Banca Națională și Ministerul Finanțelor (în continuare – autorități de supraveghere). (2) Banca Națională, în calitate de autoritate de supraveghere, are următoarele atribuții: a) supraveghează sistemele de plăți din Republica Moldova; b) supraveghează și reglementează, din punct de vedere prudențial, societățile de plată, societățile emitente de monedă electronică, furnizorii de servicii poștale; b¹) supraveghează și reglementează activitatea de prestare a serviciilor de plată și/sau activitatea de emitere a monedei electronice ale	parțial compatibil	BNM este autoritatea competentă pentru bănci, prestatorii de servicii de plată, emitenții de monedă electronică, societățile de asigurare și de reasigurare și intermediarii în asigurări și în reasigurări, potrivit legilor sectoriale. Pentru entitățile care nu se află în supravegherea BNM, autoritatea competentă se stabilește prin actele care vor pune în aplicare regulamentul pentru acestea.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(f) pentru contrapărțile centrale, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012; (g) pentru locurile de tranzacționare și furnizorii de servicii de raportare a datelor, autoritatea competentă desemnată în conformitate cu articolul 67 din Directiva 2014/65/UE și autoritatea competentă definită la articolul 2 alineatul (1) punctul 18 din Regulamentul (UE) nr. 600/2014; (h) pentru registrele centrale de tranzacții, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012; (i) pentru administratorii de fonduri de investiții alternative, autoritatea competentă desemnată în conformitate cu articolul 44 din Directiva 2011/61/UE; (j) pentru societățile de administrare, autoritatea competentă desemnată în conformitate cu articolul 97 din Directiva 2009/65/CE; (k) pentru întreprinderile de asigurare și de reasigurare, autoritatea competentă desemnată în conformitate cu articolul 30 din Directiva 2009/138/CE; (l) pentru intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare, autoritatea competentă desemnată în conformitate cu articolul 12 din Directiva (UE) 2016/97; (m) pentru instituțiile pentru furnizarea de pensii ocupaționale, autoritatea competentă desemnată în conformitate cu articolul 47 din Directiva (UE) 2016/2341; (n) pentru agențiile de rating de credit, autoritatea competentă desemnată în conformitate cu articolul 21 din Regulamentul (CE) nr. 1060/2009; (o) pentru administratorii de indici de referință critici, autoritatea competentă desemnată în conformitate cu articolele 40 și 41 din Regulamentul (UE) 2016/1011; (p) pentru furnizorii de servicii de finanțare participativă, autoritatea competentă desemnată în conformitate cu articolul 29 din Regulamentul (UE) 2020/1503;			societăților de plată, ale societăților emitente de monedă electronică, ale furnizorilor de servicii poștale, ale băncilor; c) coordonează activitatea autorităților de supraveghere în domeniul supravegherii activității de prestare a serviciilor de plată. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 115 alin. (1):** (1) Autoritatea de supraveghere este competentă și responsabilă pentru reglementarea, autorizarea și supravegherea, inclusiv la nivel de grup, a participanților profesioniști pe piața asigurărilor, a sucursalelor societăților de asigurare sau de reasigurare din statele terțe (în ceea ce privește operațiunile desfășurate pe teritoriul Republicii Moldova), precum și a biroului național.		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(q) pentru registrele centrale de securitizări, autoritatea competentă desemnată în conformitate cu articolul 10 și cu articolul 14 alineatul (1) din Regulamentul (UE) 2017/2402.					
Articolul 47. Cooperarea cu structurile și autoritățile înființate prin Directiva (UE) 2022/2555 (1) Pentru a încuraja cooperarea și a permite schimburile de informații în scopuri de supraveghere între autoritățile competente desemnate în temeiul prezentului regulament și Grupul de cooperare instituit prin articolul 14 din Directiva (UE) 2022/2555, AES și autoritățile competente pot participa la activitățile Grupului de cooperare în ceea ce privește chestiuni care privesc activitățile lor de supraveghere în legătură cu entitățile financiare. AES și autoritățile competente pot solicita să fie invitate să participe la activitățile Grupului de cooperare cu privire la chestiuni legate de entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost, de asemenea, desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament. (2) După caz, autoritățile competente se pot consulta și pot face schimb de informații cu punctele unice de contact și cu echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555. (3) După caz, autoritățile competente pot solicita orice tip de consultanță și asistență tehnică relevantă din partea autorităților competente desemnate sau stabilite în conformitate cu Directiva (UE) 2022/2555 și pot stabili acorduri de cooperare pentru a permite crearea unor mecanisme de coordonare eficace și rapide. (4) Acordurile menționate la alineatul (3) de la prezentul articol pot specifica, printre altele, procedurile pentru coordonarea activităților de supraveghere și, respectiv, de control în ceea ce privește entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament, inclusiv pentru efectuarea, în conformitate cu dreptul intern, a investigațiilor și a inspecțiilor la fața locului, precum și pentru mecanismele privind schimbul de	CN	Pct. 105 (transcris la art. 19 alin. (6)). Pct. 167 (transcris la art. 49 alin. (1)).	**Legea nr. 48/2023 privind securitatea cibernetică, art. 7 alin. (2):** (2) Autoritatea competentă exercită inclusiv funcția de echipă de răspuns la incidentele cibernetice la nivel național și cea de punct național unic de contact.	parțial compatibil	Autoritatea competentă potrivit Legii nr. 48/2023 exercită și funcțiile de echipă de răspuns la incidentele cibernetice și de punct unic de contact (art. 7 alin. (2)). Cooperarea este reflectată parțial, prin transmiterea detaliilor despre incidente către ASC (pct. 105) și prin mecanismele comune (pct. 167). Consilierea tehnică și acordurile de cooperare se stabilesc prin acord între BNM și ASC.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
informații dintre autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau stabilite în conformitate cu directiva respectivă, care include accesul la informațiile solicitate de autoritățile din urmă.					
Articolul 48. Cooperarea între autorități (1) Autoritățile competente cooperează îndeaproape între ele și, după caz, cu supraveghetorul principal.	CN	-	**Legea nr. 202/2017 privind activitatea băncilor, art. 5 alin. (5):** (5) Pentru a facilita o supraveghere prudențială eficientă a băncilor licențiate, Banca Națională a Moldovei încheie acorduri scrise de coordonare și cooperare cu alte autorități competente din Republica Moldova.	parțial compatibil	Cooperarea dintre autoritățile naționale este prevăzută de legislația sectorială. Cooperarea cu supraveghetorul principal se exercită la nivelul Uniunii.
(2) Autoritățile competente și supraveghetorul principal își transmit reciproc, în timp util, toate informațiile relevante privind furnizorii terți esențiali de servicii TIC care sunt necesare pentru îndeplinirea sarcinilor care le revin în temeiul prezentului regulament, în special în legătură cu riscurile identificate, cu abordările și cu măsurile adoptate în cadrul sarcinilor de supraveghere ale supraveghetorului principal.	N/A	-	-	prevederi UE neaplicabile	Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC se exercită la nivelul Uniunii (AES, supraveghetorul principal). Nu necesită măsuri naționale de punere în aplicare.
Articolul 49. Exerciții, comunicare și cooperare transsectoriale în domeniul financiar (1) AES, prin intermediul Comitetului comun și în colaborare cu autoritățile competente, cu autoritățile de rezoluție menționate la articolul 3 din Directiva 2014/59/UE, cu BCE, cu Comitetul unic de rezoluție în ceea ce privește informațiile referitoare la entitățile care intră sub incidența Regulamentului (UE) nr. 806/2014, cu CERS și cu ENISA, după caz, pot stabili mecanisme care să permită schimbul de practici eficace între sectoarele financiare în vederea îmbunătățirii gradului de conștientizare a situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor. Acestea pot elabora exerciții de gestionare a crizelor și pentru situații neprevăzute care implică scenarii de atacuri cibernetice, cu scopul de a dezvolta canale de comunicare și de a permite treptat un răspuns coordonat eficace la nivelul UE în cazul unui incident	CN	167. BNM, în colaborare cu ASC, după caz, poate stabili mecanisme care să permită schimbul de practici eficace între subsectoarele financiare în vederea îmbunătățirii gradului de conștientizare a situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor. BNM și ASC pot elabora exerciții de gestionare a crizelor și pentru situații neprevăzute care implică scenarii de atacuri cibernetice, cu scopul de a dezvolta canale de comunicare și de a permite treptat un răspuns coordonat eficace la nivel național în cazul unui incident transfrontalier major legat de TIC sau al unei amenințări conexe cu un impact sistemic asupra sectorului financiar. Exercițiile respective pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.	-	compatibil	Mecanismele și exercițiile stabilite la nivelul Uniunii de AES sunt preluate, la nivel național, de BNM în colaborare cu ASC.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
transfrontalier major legat de TIC sau al unei amenințări conexe cu un impact sistemic asupra sectorului financiar al Uniunii în ansamblu. Exercițiile respective pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.					
(2) Autoritățile competente, AES și BCE cooperează strâns și fac schimb de informații pentru a-și îndeplini atribuțiile prevăzute la articolele 47-54. Acestea își coordonează îndeaproape activitățile de supraveghere pentru a identifica și a remedia cazurile de nerespectare a prezentului regulament, pentru a elabora și a promova bune practici, a facilita colaborarea, a stimula consecvența interpretării și a furniza evaluări interjurisdicționale în cazul oricăror neînțelegeri.	N/A	-	-	prevederi UE neaplicabile	Prevedere privind activitatea autorităților europene de supraveghere (AES), a Comisiei Europene sau a altor instituții ale Uniunii. Nu necesită măsuri naționale de punere în aplicare.
Articolul 50. Sancțiuni administrative și măsuri de remediere (1) Autoritățile competente dispun de toate competențele de supraveghere, de investigare și de sancționare necesare pentru a-și îndeplini atribuțiile în conformitate cu prezentul regulament. (2) Competențele menționate la alineatul (1) includ cel puțin următoarele: (a) competența de a avea acces la orice document sau date deținute sub orice formă pe care autoritatea competentă le consideră relevante pentru îndeplinirea sarcinilor sale și competența de a primi sau de a face o copie a acestora; (b) competența de a efectua inspecții la fața locului sau investigații, incluzând, printre altele, următoarele activități: (i) convocarea reprezentanților entităților financiare pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și înregistrarea răspunsurilor; (ii) punerea de întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări în scopul colectării de informații referitoare la obiectul unei investigații; (c) competența de a solicita măsuri corective și de remediere pentru încălcările cerințelor prezentului regulament.	CN	168. Pentru încălcarea prevederilor prezentului regulament, BNM aplică măsurile de remediere și sancțiunile prevăzute de Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, Legea nr. 202/2017 privind activitatea băncilor, Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică și Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, după caz.	**Legea nr. 202/2017 privind activitatea băncilor, art. 138 alin. (1), alin. (3), alin. (4), alin. (6):** (1) În exercitarea funcțiilor sale, Banca Națională a Moldovei deține competența să dispună, față de o bancă, față de acționarii acesteia, față de membrii organului de conducere al băncii, față de persoanele care dețin funcții-cheie în cadrul băncii, care încalcă dispozițiile prezentei legi, ale actelor normative sau ale altor acte emise în aplicarea acesteia, referitoare la supraveghere sau la condițiile de desfășurare a activității, măsuri potrivit prevederilor art. 139 și/sau să aplice sancțiuni și măsuri sancționatoare potrivit prevederilor art. 141. (3) Banca Națională a Moldovei are competența de a colecta toate informațiile necesare și de a efectua toate cercetările necesare în exercitarea funcțiilor sale.	compatibil	Competențele de supraveghere, de investigare și de sancționare sunt stabilite prin legile sectoriale, la care trimite pct. 168.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			(4) Fără a aduce atingere prevederilor prezentei legi și ale actelor normative emise în aplicarea acesteia, competența prevăzută la alin. (3) include: a) competența de a solicita furnizarea tuturor informațiilor necesare de la orice persoană fizică sau juridică prevăzută la alin. (5), pentru îndeplinirea atribuțiilor care revin Băncii Naționale a Moldovei, inclusiv a informațiilor care trebuie furnizate, în scopuri de supraveghere și în scopuri statistice, la intervale regulate și în formatele specificate; b) competența de a efectua toate cercetările necesare pentru îndeplinirea atribuțiilor care revin Băncii Naționale a Moldovei în legătură cu orice persoană fizică sau juridică prevăzută la alin. (5); c) competența de a efectua toate inspecțiile necesare la sediile persoanelor juridice menționate la alin. (5) și la sediul oricărei alte societăți incluse în supravegherea consolidată pentru care Banca Națională a Moldovei este supraveghetor consolidant, cu condiția acordului prealabil al autorităților competente implicate. (6) Competența prevăzută la alin. (4) lit. b) include dreptul: a) de a solicita prezentarea de documente; b) de a examina evidențele și registrele persoanelor menționate la alin. (5) și de a ridica fotocopii sau extrase ale acestor evidențe și registre;		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			c) de a obține explicații scrise sau verbale de la orice persoană prevăzută la alin. (5) sau de la reprezentanții ori personalul acesteia; d) de a intervieva orice altă persoană, cu consimțământul acesteia, în scopul colectării de informații referitoare la obiectul unei cercetări; e) de a avea acces la sistemele informaționale și de a solicita prezentarea de informații din bazele de date aferente. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 94 alin. (1), alin. (2):** În scopul exercitării atribuției de supraveghere și reglementare prudențiale și a celei de supraveghere și reglementare a activității de prestare a serviciilor de plată și de emitere a monedei electronice, autoritatea de supraveghere este împuternicită: a) să solicite prestatorului de servicii de plată, emitentului de monedă electronică, precum și organelor de conducere, membrilor organelor de conducere, persoanelor care dețin funcții-cheie, angajaților acestora să furnizeze informațiile necesare, conform legislației, indicând scopul solicitării, după caz, și termenul rezonabil pentru furnizarea informațiilor; b) să desfășoare, prin intermediul funcționarilor săi și al altor specialiști numiți, potrivit legii, inspecții la sediul prestatorilor de servicii de plată, emitenților de monedă electronică, filialelor,		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			agenților și furnizorilor funcțiilor externalizate, să examineze conturile, registrele și documentele acestora; c) să adopte acte normative cu privire la modalitatea și condițiile de prestare a serviciilor de plată și de emitere a monedei electronice, la licențierea și activitatea societăților de plată, societăților emitente de monedă electronică, furnizorilor de servicii poștale, la activitatea băncilor în calitate de prestatori de servicii de plată și de emitenți de monedă electronică, la protecția drepturilor utilizatorilor serviciilor de plată și ale deținătorilor de monedă electronică, precum și să adopte acte normative pentru realizarea supravegherii conform prezentei legi și să ia măsurile cuvenite pentru a exercita împuternicirile sale ce decurg din prezenta lege; d) să dispună măsuri de remediere și să aplice sancțiuni prestatorului de servicii de plată și emitentului de monedă electronică dacă aceștia, acționarii/asociații, organele de conducere, membrii organelor de conducere, persoanele care dețin funcții-cheie ori angajații, sucursalele, agenții sau furnizorii funcțiilor externalizate ai acestora au comis încălcări. (2) Prestatorii de servicii de plată și emitenții de monedă electronică, filialele, agenții și furnizorii funcțiilor externalizate ai acestora vor permite personalului împuternicit al autorităților de supraveghere și altor specialiști numiți, potrivit		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			legii, accesul la sediile lor pentru a examina evidențele, conturile și operațiunile, furnizînd în acest scop toate documentele și informațiile cu privire la administrarea, controlul intern și operațiunile prestatorilor de servicii de plată și emitenților de monedă electronică, și vor conlucra cu ei în limitele competenței atribuite prin lege. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 115 alin. (3), alin. (5):** (3) În cadrul supravegherii, autoritatea de supraveghere solicită participanților profesioniști pe piața asigurărilor orice documente și/sau informații pentru îndeplinirea eficientă a atribuțiilor conferite de lege. (5) În vederea exercitării funcțiilor de control și asigurării unei supravegheri eficiente, inclusiv la nivel de grup, participanții profesioniști pe piața asigurărilor, autoritățile administrației publice, organizațiile și întreprinderile sunt obligate să prezinte autorității de supraveghere orice documente și/sau informații solicitate pentru executarea prezentei legi. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 116 alin. (1), alin. (2):** (1) Autoritatea de supraveghere are competența de a lua orice măsuri de supraveghere, necesare în ceea ce privește societățile de asigurare sau de		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			reasigurare, sucursalele societăților de asigurare sau de reasigurare din statele terțe și/sau, după caz, intermediarii în asigurări și/sau în reasigurări, precum și membrii organelor de conducere și persoanele care dețin funcții-cheie ale acestora, inclusiv: a) de a face recomandări și atenționări; b) de a emite prescripții privind înlăturarea încălcărilor; c) de a lua măsuri suplimentare de implementare a managementului riscurilor; d) de a suspenda oricare tranzacții cu activele asigurătorului sau reasigurătorului admise la acoperirea cerinței de capital minim și/sau a obligațiilor aferente contractelor de asigurare și/sau de reasigurare; e) de a prescrie majorarea capitalului social în vederea asigurării stabilității financiare a societății de asigurare sau de reasigurare și a sucursalelor societății de asigurare sau de reasigurare din statele terțe; f) de a institui administrarea specială; g) de a redresa/remedia situația financiară; h) de a aplica măsuri de rezoluție; i) de a aplica sancțiuni; j) de a suspenda sau retrage licența; k) de a iniția proceduri de lichidare silită; l) de a iniția proceduri de insolvabilitate;		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			m) de a lua alte măsuri prevăzute de prezenta lege. (2) Supravegherea societăților de asigurare sau de reasigurare, a sucursalelor societăților de asigurare sau de reasigurare din statele terțe și a intermediarilor în asigurări și/sau în reasigurări se realizează prin următoarele metode: a) monitorizarea, colectarea, verificarea, analiza și evaluarea rapoartelor, informațiilor și notificărilor prezentate în temeiul prezentei legi și al actelor normative ale autorității de supraveghere; b) verificarea operațiunilor realizate în activitatea de asigurare sau de reasigurare; c) efectuarea controalelor la sucursalele și subdiviziunile societății de asigurare sau de reasigurare; d) impunerea măsurilor de supraveghere.		
(3) Fără a aduce atingere dreptului statelor membre de a impune sancțiuni penale în conformitate cu articolul 52, statele membre prevăd norme de stabilire a sancțiunilor administrative și a măsurilor de remediere corespunzătoare pentru încălcările prezentului regulament și asigură punerea lor efectivă în aplicare. Aceste sancțiuni și măsuri sunt eficace, proporționale și disuasive. (4) Statele membre conferă autorităților competente competența de a aplica cel puțin următoarele sancțiuni administrative sau măsuri de remediere în cazul încălcării prezentului regulament: (a) emiterea unei dispoziții prin care i se cere persoanei fizice sau juridice să înceteze comportamentul care încalcă prezentul regulament și	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 202/2017 privind activitatea băncilor, art. 141 alin. (1), alin. (2):** (1) Sancțiunile care pot fi aplicate potrivit prezentei legi sînt: a) avertisment scris; b) avertisment public prin care se indică persoana fizică, persoana juridică, inclusiv banca și natura încălcării; c) aplică și percepe incontestabil amendă băncii pînă la 5% din fondurile proprii ale băncii, calculate la data ultimei raportări, și/sau deținătorilor direcți și indirecți de deținere în capitalul social al băncii pînă la 100% din	parțial compatibil	Sancțiunile și măsurile de remediere sunt stabilite prin legile sectoriale. Declarațiile publice (alin. (4) lit. (e)) sunt prevăzute pentru bănci și pentru prestatorii de servicii de plată. Pentru asigurători, Legea nr. 92/2022 prevede avertismentul în scris, iar sancțiunile aplicate se publică potrivit art. 75³ din Legea nr. 548/1995. Solicitarea înregistrărilor deținute de operatorii de telecomunicații (alin. (4)

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
să se abțină de la repetarea comportamentului respectiv; (b) solicitarea încetării temporare sau permanente a oricărei practici sau a oricărui comportament în legătură cu care autoritatea competentă consideră că contravine dispozițiilor prezentului regulament și prevenirea repetării practicii sau a comportamentului în cauză; (c) adoptarea oricărui tip de măsură, inclusiv de natură pecuniară, pentru a asigura că entitățile financiare respectă în continuare cerințele legale; (d) solicitarea, în măsura în care dreptul intern permite acest lucru, a unor înregistrări existente ale schimburilor de date deținute de un operator de telecomunicații, atunci când există o suspiciune rezonabilă privind o încălcare a prezentului regulament și atunci când aceste înregistrări pot fi relevante pentru o investigație referitoare la încălcări ale prezentului regulament; și (e) emiterea unor anunțuri publice, inclusiv a unor declarații publice care indică identitatea persoanei fizice sau juridice și natura încălcării.			mărimea deținerii în capitalul social al băncii, calculată la valoarea nominală; d) amendă aplicabilă persoanei juridice, de pînă la 10% din valoarea totală netă a cifrei de afaceri realizată în exercițiul financiar precedent, care include venitul brut constînd din dobînzile de încasat și alte venituri similare, venituri din acțiuni și alte titluri cu randament variabil sau fix, precum și comisioanele ori taxele de încasat; în cazul în care persoana juridică are calitatea de filială a unei întreprinderi-mamă, venitul brut relevant este cel rezultat din situațiile financiare consolidate ale întreprinderii-mamă de cel mai înalt rang, din exercițiul financiar precedent; e) amendă aplicabilă membrului organului de conducere sau persoanei care deține funcții-cheie, de la 1 la 100 de salarii medii ale persoanei fizice sancționate, pentru ultimele 12 luni, care includ toate beneficiile (suplimente, prime și alte adaosuri la salariul de funcție); f) amendă aplicabilă persoanei fizice, alta decît cea menționată la lit. e), de la 5000 de lei pînă la 100 de milioane de lei; g) retragerea aprobării acordate persoanelor prevăzute la art. 43; h) amendă egală cu pînă la valoarea dublă a beneficiului obținut ca urmare a încălcării, dacă acesta poate fi determinat. (2) Măsurile sancționatoare care pot fi aplicate potrivit prezentei legi sînt:		lit. (d)) nu are corespondent în legislația sectorială.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			a) ordin de încetare a conduitei ilicite a persoanei și de abținere de la repetarea acesteia; b) interzicerea temporară a exercitării unor funcții într-o bancă de către persoanele prevăzute la art. 43 responsabile de săvîrșirea încălcării; c) retragerea licenței acordate băncii, potrivit prevederilor art. 22; d) suspendarea exercitării drepturilor de vot ale acționarului sau acționarilor responsabili. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 99 alin. (1), alin. (3):** (1) În cazul constatării încălcărilor în activitatea prestatorului de servicii de plată sau a emitentului de monedă electronică, autoritatea de supraveghere are dreptul să dispună următoarele măsuri de remediere: a) să emită prescripții privind încetarea și lichidarea încălcărilor; b) să prescrie modificarea mecanismelor, a politicilor și a procedurilor interne; c) să interzică sau să restricționeze desfășurarea activității de prestare a unor sau a tuturor serviciilor de plată/de emitere a monedei electronice pînă la lichidarea încălcărilor constatate. (3) În cazul constatării încălcărilor, autoritatea de supraveghere are dreptul să aplice prestatorului de servicii de		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			plată și emitentului de monedă electronică următoarele sancțiuni: 1) emiterea unui avertisment în scris; 2) emiterea unui avertisment public, prin care se indică persoana fizică, persoana juridică, inclusiv prestatorul de servicii de plată și emitentul de monedă electronică, precum și natura încălcării; 3) aplicarea și perceperea incontestabilă a amenzii de la societatea de plată, de la furnizorul de servicii poștale și de la societatea emitentă de monedă electronică în mărime de până la 10% din capitalul reglementat necesar a fi menținut în conformitate cu prevederile art. 13 alin. (1) sau art. 83 alin. (1); 3¹) aplicarea și perceperea incontestabilă a amenzii de la bancă în conformitate cu prevederile art. 141 alin. (1) lit. c) din Legea nr. 202/2017 privind activitatea băncilor; 4) aplicarea amenzii față de organul de conducere, membrul organelor de conducere, persoana care deține o funcție-cheie în mărime de la unu la 100 de salarii medii ale persoanei fizice sancționate, care includ toate beneficiile (suplimente, prime și alte adaosuri la salariul de funcție), fiind luat în calcul salariul mediu pentru: a) ultimele 12 luni lucrate în cadrul prestatorului de servicii de plată sau în cadrul emitentului de		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			monedă electronică, precedente datei la care s-a constatat fapta; b) perioada totală lucrată în cadrul prestatorului de servicii de plată sau în cadrul emitentului de monedă electronică, precedentă datei la care s-a constatat fapta, dacă perioada respectivă este mai mică de 12 luni; c) ultimele 12 luni lucrate în cadrul prestatorului de servicii de plată sau în cadrul emitentului de monedă electronică, în cazul în care raporturile de muncă au încetat înainte de data la care s-a constatat fapta; d) perioada totală lucrată în cadrul prestatorului de servicii de plată sau în cadrul emitentului de monedă electronică, în cazul în care perioada respectivă este mai mică de 12 luni și raporturile de muncă au încetat înainte de data la care s-a constatat fapta; 5) amendă în mărime de până la valoarea dublă a beneficiului obținut ca urmare a încălcării, dacă acesta poate fi determinat; 6) suspendarea licenței (activității) societății de plată, furnizorului de servicii poștale și societății emitente de monedă electronică pe un termen de la o lună până la 6 luni; 7) retragerea licenței societății de plată, furnizorului de servicii poștale și societății emitente de monedă electronică. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 122 alin. (2):** (2) În caz de constatare a încălcărilor menționate la alin.(1), autoritatea de supraveghere		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			poate aplica următoarele sancțiuni: 1) avertisment în scris; 2) suspendarea sau retragerea certificatelor de calificare eliberate de aceasta; 3) amendă aplicată persoanei cu funcție de conducere sau persoanei care deține funcție-cheie, din cadrul societății de asigurare sau de reasigurare, din cadrul sucursalei societăților de asigurare sau reasigurare din statele terțe sau din cadrul intermediarului în asigurări și/sau în reasigurări, în mărime de la 1 la 100 de salarii medii ale persoanei fizice sancționate, care includ toate beneficiile (suplimente, prime și alte adaosuri la salariul de funcție), fiind luat în calcul salariul mediu pentru: a) ultimele 12 luni lucrate în cadrul entității supravegheate respective, precedente datei la care s-a constatat fapta; b) perioada totală lucrată în cadrul entității supravegheate respective, precedentă datei la care s-a constatat fapta, dacă perioada respectivă este mai mică de 12 luni; c) ultimele 12 luni lucrate în cadrul entității supravegheate respective, în cazul în care raporturile de muncă au încetat înainte de data la care s-a constatat fapta; d) perioada totală lucrată în cadrul entității supravegheate respective, în cazul în care perioada respectivă este mai mică de 12 luni și raporturile de		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			muncă au încetat înainte de data la care s-a constatat fapta; 4) amendă aplicată persoanei fizice care exercită atribuțiile funcției actuariale în mărime de la 10 000 de lei la 1 milion de lei; 5) amendă aplicată intermediarului în asigurări persoană fizică în mărime de la 5 000 de lei până la 1 milion de lei; 6) amendă aplicată persoanei fizice, alta decât cele menționate la pct. 3)–5), în mărime de la 5 000 de lei la 1 milion de lei; 7) amendă de până la 15% din cerința de capital minim aplicată societății de asigurare sau de reasigurare ori sucursalelor societăților de asigurare sau reasigurare din statele terțe conform categoriei de asigurări sau activității de reasigurări în care s-a constatat încălcarea; 8) amendă de până la 15% din capitalul social aplicată intermediarului în asigurări și/sau în reasigurări. În cazul agenților bancassurance, amenda se aplică în limita capitalului de 100 000 de lei; 9) limitarea operațiunilor prin interzicerea subscrierii unor noi contracte de asigurare și/sau de reasigurare și a încasării primelor aferente acestora pentru toate clasele de asigurare sau activitățile de reasigurare ori pentru anumite tipuri/clase sau activități; 10) amendă aplicată deținătorilor direcți și indirecți de acțiuni în capitalul social al societății de asigurare sau de reasigurare și/sau beneficiarului efectiv –		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			până la 100% din mărimea deținerii în capitalul social al societății de asigurare sau de reasigurare, calculată la valoarea nominală; 11) amendă de până la valoarea dublă a beneficiului obținut ca urmare a încălcării, dacă acesta poate fi determinat; 12) suspendarea sau retragerea calității de persoană cu funcție de conducere și care deține funcție-cheie, aprobată în prealabil de către autoritatea de supraveghere; 13) suspendarea sau retragerea parțială ori totală a licenței; 14) suspendarea exercitării drepturilor de vot ale acționarului sau acționarilor responsabili; 15) interzicerea dispunerii libere de activele societății de asigurare sau de reasigurare ori ale sucursalelor societăților de asigurare sau reasigurare din statele terțe; 16) alte sancțiuni prevăzute de prezenta lege.		
(5) Atunci când alineatul (2) litera (c) și alineatul (4) se aplică unor persoane juridice, statele membre conferă autorităților competente competența de a aplica sancțiunile administrative și măsurile de remediere, sub rezerva condițiilor prevăzute în dreptul intern, membrilor organului de conducere, precum și altor persoane care, în temeiul dreptului intern, sunt responsabile de încălcare.	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 202/2017 privind activitatea băncilor, art. 141 alin. (5):** (5) Sancțiunile prevăzute la alin. (1) lit. a), b) și d)–g) și măsura sancționatorie prevăzută la alin. (2) lit. a) se aplică persoanelor cărora le poate fi imputată fapta, întrucît aceasta nu s-ar fi produs dacă persoanele respective și-ar fi exercitat în mod corespunzător responsabilitățile care decurg din îndatoririle funcției lor stabilite conform legislației, actelor normative emise în aplicarea prezentei legi și cadrului intern de	compatibil	Sancțiunile aplicabile membrilor organelor de conducere și persoanelor responsabile sunt prevăzute de legile sectoriale. Pentru prestatorii de servicii de plată, art. 99 alin. (3) pct. 4) din Legea nr. 114/2012 este transcris la art. 50 alin. (3) și (4).

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			administrare, ori, după caz, persoanelor în privința cărora Banca Națională a Moldovei constată că acestea nu acționează în conformitate cu regulile unei practici bancare prudente și sănătoase și/sau că nu mai corespund cerințelor de reputație și competență adecvată naturii, extinderii și complexității activității băncii și responsabilităților încredințate. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 122 alin. (3¹):** (3¹) Sancțiunile prevăzute la alin. (2) pct. 1), 3)–6) și 12) se aplică persoanelor cărora le poate fi imputată fapta, întrucât aceasta nu s-ar fi produs dacă persoanele respective și-ar fi exercitat în mod corespunzător responsabilitățile care decurg din îndatoririle funcției lor, stabilite conform legislației, actelor normative emise în aplicarea prezentei legi și cadrului intern de administrare, ori, după caz, persoanelor în privința cărora Banca Națională a Moldovei constată că acestea nu acționează în conformitate cu regulile unei practici prudente și sănătoase și/sau că nu mai corespund cerințelor de reputație și competență adecvată naturii, extinderii și complexității activității participanților profesioniști pe piața asigurărilor și responsabilităților încredințate.		
(6) Statele membre se asigură că orice decizie de impunere a unor sancțiuni administrative sau a unor măsuri de remediere prevăzute la alineatul (2) litera	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 11 alin. (4), alin. (5¹), alin. (6):**	compatibil	Actele BNM, inclusiv cele emise față de asigurători, pot fi contestate potrivit art. 11 alin. (4)-(6) din Legea

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) este justificată în mod corespunzător și face obiectul unei căi de atac.			(4) Actele Băncii Naţionale sunt supuse controlului de legalitate în instanţele de contencios administrativ conform procedurii stabilite de Codul administrativ, în măsura în care aceasta nu contravine prezentei legi. Dispoziţiile altor legi pot fi aplicate în cazurile privind contestarea actelor Băncii Naţionale doar în măsura în care nu contravin normelor stabilite de prezenta lege. (5 1) Actele Băncii Naţionale pot fi contestate la Comitetul executiv al Băncii Naţionale prin depunerea unei cereri prealabile în termen de 30 de zile de la data comunicării actului. Termenul de 30 de zile nu se extinde asupra actelor cu caracter normativ. (6) Acţiunile de contencios administrativ privind actele Băncii Naţionale sau privind nesoluţionarea de către aceasta în termen legal a unei cereri se înaintează la Curtea de Apel Chișinău, cu condiţia respectării obligatorii a procedurii prealabile prevăzute la alineatele (5 1)–(5 3). Contestarea sau acţiunea în justiţie nu suspendă executarea actelor emise de Banca Naţională. **Legea nr. 202/2017 privind activitatea băncilor, art. 144 alin. (1):** (1) Actele Băncii Naționale a Moldovei prin care sînt dispuse măsuri sau sînt aplicate sancțiuni ori măsuri sancționatoare potrivit prezentei legi pot fi atacate în instanța de contencios administrativ competentă, cu		nr. 548/1995 (cerere prealabilă la Comitetul executiv, apoi acțiune în contencios administrativ), precum și potrivit art. 144 din Legea nr. 202/2017 și art. 101 din Legea nr. 114/2012.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			respectarea prezentului articol și a art. 11 și 11¹ din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 101:** Actele adoptate de autoritatea de supraveghere corespunzător dispozițiilor prezentei legi pot fi contestate în conformitate cu prevederile Codului administrativ.		
Articolul 51. Exercitarea competenței de a impune sancțiuni administrative și măsuri de remediere (1) Autoritățile competente își exercită competențele de a impune sancțiunile administrative și măsurile de remediere menționate la articolul 50 în conformitate cu cadrele lor juridice naționale, dacă este cazul, după cum urmează: (a) în mod direct; (b) în colaborare cu alte autorități; (c) sub responsabilitate proprie prin delegare către alte autorități; sau (d) prin sesizarea autorităților judiciare competente.	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 202/2017 privind activitatea băncilor, art. 138 alin. (2):** (2) Banca Națională a Moldovei își exercită competențele de supraveghere și de aplicare a măsurilor, sancțiunilor și măsurilor sancționatoare, potrivit prevederilor prezentei legi, în oricare dintre următoarele modalități: a) în mod direct; b) în colaborare cu alte autorități; c) prin sesizarea autorităților judiciare competente.	compatibil	Modalitățile de exercitare sunt prevăzute la art. 138 alin. (2) din Legea nr. 202/2017. Delegarea către alte autorități nu este prevăzută.
(2) La stabilirea tipului și a nivelului unei sancțiuni administrative sau al unei măsuri de remediere care urmează să fie impuse în temeiul articolului 50, autoritățile competente iau în considerare măsura în care încălcarea este intenționată sau rezultă din neglijență și toate celelalte circumstanțe relevante, inclusiv, după caz, următoarele elemente: (a) importanța semnificativă, gravitatea și durata încălcării; (b) gradul de responsabilitate al persoanei fizice sau juridice responsabile de încălcare; (c) soliditatea financiară a persoanei fizice sau juridice responsabile; (d) importanța profiturilor obținute sau a pierderilor evitate de către persoana fizică sau juridică	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 202/2017 privind activitatea băncilor, art. 142 alin. (2):** (2) La stabilirea tipului sancțiunii sau a măsurii sancționatoare și a cuantumului amenzii, Banca Națională a Moldovei are în vedere toate circumstanțele relevante ale săvîrșirii faptei, inclusiv următoarele aspecte, după caz: a) gravitatea și durata faptei; b) gradul de vinovăție a persoanei fizice sau juridice responsabile; c) capacitatea financiară a persoanei fizice sau juridice	compatibil	Criteriile de stabilire a tipului și a nivelului sancțiunilor sunt prevăzute de legile sectoriale.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
responsabilă, în măsura în care acestea pot fi determinate; (e) pierderile suferite de terți în urma respectivei încălcări, în măsura în care acestea pot fi determinate; (f) nivelul de cooperare cu autoritatea competentă a persoanei fizice sau juridice responsabile, fără a aduce atingere necesității de a asigura confiscarea profiturilor obținute sau a pierderilor evitate de persoana fizică sau juridică respectivă; (g) încălcările anterioare comise de persoana fizică sau juridică responsabilă.			responsabile de încălcare, astfel cum rezultă, de exemplu, din venitul anual al persoanei fizice responsabile sau din cifra de afaceri totală a persoanei juridice responsabile; d) importanța profiturilor realizate sau a pierderilor evitate de către persoana fizică sau juridică responsabilă, în beneficiul acesteia, în măsura în care acestea pot fi determinate; e) prejudiciile cauzate terților, în măsura în care pot fi determinate; f) gradul de cooperare a persoanei fizice sau juridice responsabile cu Banca Națională a Moldovei; g) încălcările săvîrșite anterior de persoana fizică sau juridică responsabilă; h) orice posibile consecințe sistemice ale faptei săvîrșite. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 100 alin. (1¹):** (1¹) La stabilirea tipului sancțiunii sau a măsurii de remediere și a cuantumului amenzii față de prestatorii de servicii de plată și față de emitenții de monedă electronică, Banca Națională are în vedere criteriile stabilite prin actele normative ale Băncii Naționale. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 122 alin. (9):** (9) La stabilirea tipului sancțiunii și a cuantumului amenzii, autoritatea de supraveghere examinează toate circumstanțele		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			relevante ale săvârșirii faptei, inclusiv următoarele aspecte, după caz: a) gravitatea și durata faptei; b) gradul de vinovăție a persoanei responsabile; c) capacitatea financiară a persoanei responsabile de încălcare, astfel cum rezultă, de exemplu, din venitul anual al persoanei fizice responsabile sau din cifra de afaceri totală a persoanei juridice responsabile; d) importanța profiturilor realizate sau a pierderilor evitate de către persoana responsabilă, în beneficiul acesteia, în măsura în care acestea pot fi determinate; e) prejudiciile cauzate contractanților, asiguraților, reasiguraților, beneficiarilor asigurării, terților păgubiți și altor persoane ale căror drepturi pot fi lezate, în măsura în care pot fi determinate; f) gradul de cooperare cu autoritatea de supraveghere; g) încălcările săvârșite anterior; h) orice posibile consecințe sistematice ale faptei săvârșite.		
Articolul 52. Sancțiuni penale (1) Statele membre pot decide să nu stabilească norme privind sancțiunile administrative sau măsurile de remediere în cazul încălcărilor care fac obiectul sancțiunilor penale în dreptul lor intern. (2) În cazul în care statele membre au ales să prevadă sancțiuni penale pentru încălcările prezentului regulament, acestea se asigură că sunt instituite măsuri adecvate astfel încât autoritățile competente să dispună de toate competențele necesare pentru a asigura legătura cu autoritățile judiciare, de urmărire penală sau autoritățile judiciare	N/A	-	-	prevederi UE neaplicabile	Opțiune a statelor membre, fără corespondent în legislația națională. Aplicarea sancțiunilor potrivit legilor sectoriale nu înlătură răspunderea penală.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
penale din jurisdicția lor pentru a primi informații specifice referitoare la anchete sau proceduri penale inițiate pentru încălcarea prezentului regulament, precum și pentru a furniza aceleași informații altor autorități competente, precum și ABE, ESMA sau EIOPA astfel încât să își îndeplinească obligațiile de cooperare în scopul aplicării prezentului regulament.					
Articolul 53. Obligații de notificare Statele membre notifică actele cu putere de lege și actele administrative de punere în aplicare a prezentului capitol, inclusiv orice dispoziții relevante de drept penal, Comisiei, ESMA, ABE și EIOPA până la 17 ianuarie 2025. Statele membre înștiințează fără întârzieri nejustificate Comisia, ESMA, ABE și EIOPA cu privire la orice modificare ulterioară a acestor acte.	N/A	-	-	prevederi UE neaplicabile	Obligație de notificare a Comisiei Europene și a AES, care nu necesită măsuri naționale de punere în aplicare.
Articolul 54. Publicarea sancțiunilor administrative (1) Autoritățile competente publică pe site-urile lor internet oficiale, fără întârzieri nejustificate, orice decizie de impunere a unei sancțiuni administrative care nu face obiectul niciunei căi de atac după notificarea destinatarului sancțiunii cu privire la decizia respectivă. (2) Publicarea menționată la alineatul (1) include informații privind tipul și natura încălcării, identitatea persoanelor responsabile și sancțiunile impuse. (3) În cazul în care autoritatea competentă, în urma unei evaluări de la caz la caz, consideră că publicarea identității, în cazul persoanelor juridice, sau a identității și a datelor cu caracter personal, în cazul persoanelor fizice, ar fi disproporționată, comportând riscuri cu privire la protecția datelor cu caracter personal, ar pune în pericol stabilitatea piețelor financiare sau desfășurarea unei anchete penale în curs sau ar cauza, în măsura în care acestea pot fi determinate, prejudicii disproporționate persoanei implicate, aceasta adoptă una dintre următoarele soluții în ceea ce privește decizia de impunere a unei sancțiuni administrative: (a) amână publicarea sa până când toate motivele pentru nepublicare încetează; (b) publică decizia menținând anonimatul persoanei în cauză, în conformitate cu dreptul intern; sau	CN	Pct. 168 (transcris la art. 50 alin. (1) și (2)).	**Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 75³ alin. (1), alin. (2), alin. (3), alin. (4):** (1) Banca Națională publică, fără întârziere, pe pagina sa web oficială sancțiunile aplicate, precum și informațiile privind tipul și natura încălcării comise și privind identitatea persoanei fizice sau juridice sancționate, după notificarea acesteia cu privire la aplicarea sancțiunii. În cazul în care sancțiunea aplicată a fost contestată în condițiile legii, Banca Națională publică, fără întârziere, informațiile privind etapa la care se află contestarea și rezultatul acesteia. (2) Banca Națională publică sancțiunile, fără a indica identitatea persoanelor fizice sau juridice sancționate, în oricare dintre următoarele situații: a) sancțiunea este aplicată unei persoane fizice și, în urma unei evaluări anterioare obligatorii, s-a constatat că publicarea datelor	compatibil	Publicarea sancțiunilor aplicate de BNM, inclusiv a informațiilor privind contestarea, publicarea fără indicarea identității și amânarea publicării, este prevăzută de art. 75³ din Legea nr. 548/1995, pentru toate entitățile supravegheate, precum și de art. 146 din Legea nr. 202/2017 și art. 100 alin. (7) din Legea nr. 114/2012.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(c) se abține de la publicarea acesteia, în cazul în care opțiunile prevăzute la literele (a) și (b) sunt considerate insuficiente pentru a garanta lipsa oricărui pericol pentru stabilitatea piețelor financiare sau în cazul în care o astfel de publicare nu ar fi proporțională cu clemența sancțiunii impuse. (4) În cazul unei decizii de a publica sancțiunea administrativă menținând anonimatul persoanei în cauză în conformitate cu alineatul (3) litera (b), publicarea datelor relevante poate fi amânată. (5) Dacă o autoritate competentă publică o decizie de impunere a unei sancțiuni administrative care face obiectul unei căi de atac în fața autorităților judiciare relevante, autoritățile competente includ imediat pe site-ul lor internet oficial această informație și, ulterior, orice informații conexe ulterioare cu privire la rezultatul căii de atac. Se publică, de asemenea, hotărârile judecătorești care anulează deciziile de impunere a unei sancțiuni administrative. (6) Autoritățile competente se asigură că orice publicare menționată la alineatele (1)-(4) rămâne pe site-ul lor internet oficial numai pe perioada care este necesară pentru ca prezentul articol să își producă efectele. Această perioadă nu poate depăși cinci ani de la data publicării.			cu caracter personal este disproporționată; b) publicarea ar pune în pericol stabilitatea piețelor financiare sau urmărirea penală în curs de desfășurare; c) publicarea ar cauza, în măsura în care se poate stabili acest lucru, un prejudiciu disproporționat persoanelor fizice sancționate. (3) În cazul în care Banca Națională consideră că situațiile prevăzute la alin. (2) pot înceta într-un termen rezonabil, aceasta poate amâna publicarea sancțiunilor conform alin. (1) pentru un astfel de termen. (4) Informațiile publicate potrivit alin. (1) sau (2) din prezentul articol rămân pe pagina web oficială a Băncii Naționale pentru o perioadă de cel puțin 5 ani. Datele cu caracter personal sunt păstrate pe pagina web oficială a Băncii Naționale doar atât timp cât este necesar, cu respectarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal. **Legea nr. 202/2017 privind activitatea băncilor, art. 146:** Publicarea sancțiunilor se efectuează în conformitate cu prevederile art. 75³ din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 100 alin. (7):** (7) În cazul cînd consideră că este necesar, Banca Națională are dreptul să facă publică informația despre aplicarea		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			măsurilor de remediere și a sancțiunilor.		
Articolul 55. Secretul profesional (1) Informațiile confidențiale primite, schimbate sau transmise în temeiul prezentului regulament fac obiectul condițiilor privind respectarea secretului profesional prevăzute la alineatul (2).	PF+CN	169. Informațiile confidențiale primite, schimbate sau transmise în temeiul prezentului regulament fac obiectul condițiilor privind respectarea secretului profesional prevăzute de Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, Legea nr. 202/2017 privind activitatea băncilor, Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică și Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, după caz.	-	compatibil	Regimul secretului profesional este stabilit prin art. 36 din Legea nr. 548/1995, art. 126-129 din Legea nr. 202/2017, art. 103 din Legea nr. 114/2012 și art. 120 din Legea nr. 92/2022, la care trimite pct. 169.
(2) Obligația de păstrare a secretului profesional se aplică tuturor persoanelor care lucrează sau care au lucrat pentru autoritățile competente în temeiul prezentului regulament sau pentru orice autoritate, întreprindere de pe piață sau persoană fizică ori juridică căreia respectivele autorități competente i-au delegat competențele lor, inclusiv auditorilor și experților contractați de acestea.	CN	Pct. 169 (transcris la art. 55 alin. (1)).	**Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 36 alin. (1):** (1) Membrii organelor de conducere, salariaţii Băncii Naţionale, experţii contabili, contabilii autorizaţi şi alţi specialişti numiţi, potrivit legii, de aceasta să efectueze controlul, precum şi auditorii sunt obligaţi să păstreze secretul profesional asupra oricărei informaţii ce reprezintă secret bancar, comercial, fiscal şi alt secret ocrotit de lege, de care iau cunoştinţă în cursul executării obligaţiilor lor. Aceste persoane sunt obligate să păstreze secretul profesional şi după încetarea activităţii la Banca Naţională sau după încetarea raporturilor de altă natură cu aceasta. **Legea nr. 202/2017 privind activitatea băncilor, art. 126 alin. (1):** (1) Membrii organelor de conducere și salariații Băncii Naționale a Moldovei, precum și salariații entităților de audit sau experții numiți de Banca Națională a Moldovei pentru efectuarea de verificări, potrivit	compatibil	Obligația de păstrare a secretului profesional se aplică membrilor organelor de conducere, salariaților BNM, experților și auditorilor numiți de aceasta.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			prevederilor art. 106 alin. (5), sînt obligaţi să păstreze secretul profesional asupra oricărei informaţii confidenţiale de care iau cunoştinţă în cursul exercitării atribuţiilor lor în aplicarea prezentei legi. Membrii organelor de conducere şi salariaţii Băncii Naţionale a Moldovei sînt obligaţi să păstreze secretul profesional şi după încetarea activităţii în cadrul băncii. **Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, art. 103 alin. (1):** (1) Membrii organelor de conducere și angajații autorității de supraveghere, experții contabili, contabilii și specialiștii desemnați de autoritatea de supraveghere, conform legii, pentru efectuarea controlului, precum și auditorii au obligația să păstreze secretul profesional privind toate informațiile confidențiale de care iau cunoștință în exercitarea atribuțiilor. Persoanele respective sunt obligate să păstreze secretul profesional și după încetarea activității în cadrul autorității de supraveghere sau după încetarea raporturilor de altă natură cu aceasta. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 120 alin. (1):** (1) Membrii consiliului de administrație și angajații autorității de supraveghere, precum și experții desemnați de aceasta, auditorii, administratorii speciali și lichidatorii sunt obligaţi să protejeze		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			confidențialitatea tuturor informațiilor obținute atât pe parcursul exercitării atribuțiilor de supraveghere, cât și după ce nu mai îndeplinesc funcţii, nu mai sunt angajați, nu mai sunt autorizați sau nu mai există în niciun alt raport juridic în baza căruia aceste persoane au avut acces la informațiile confidențiale.		
(3) Informaţiile care fac obiectul secretului profesional, inclusiv schimbul de informaţii între autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555, nu se comunică niciunei alte persoane sau autorităţi, cu excepția cazului în care acest lucru este prevăzut de dreptul Uniunii sau de dreptul intern.	CN	Pct. 169 (transcris la art. 55 alin. (1)).	**Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 36 alin. (4):** (4) Informaţiile ce constituie secret profesional pot fi divulgate sau furnizate în următoarele situaţii: a) când există consimţământul expres al persoanei la care se referă informaţiile; b) când aceste informaţii urmează a fi publicate conform legislaţiei; c) în cazul furnizării acestor informaţii în formă sumară sau agregată, astfel încât nu poate fi identificată banca sau persoana la care acestea se referă; d) în cazurile prevăzute la art. 97 din Legea nr. 202/2017 privind activitatea băncilor și la art. 103 din Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică, care se aplică în mod corespunzător; e) în cadrul acordurilor de cooperare cu alte autorităţi publice sau din iniţiativa Băncii Naţionale, în scopul exercitării atribuţiilor specifice de supraveghere şi control asupra respectării prevederilor legale;	compatibil	Informațiile pot fi comunicate doar în cazurile prevăzute de lege.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			f) în cazul furnizării acestor informaţii Fondului de garantare a depozitelor în sistemul bancar, necesare exercitării atribuţiilor acestuia; g) în cadrul procedurilor legate de lichidarea silită a unei bănci, cu excepţia informaţiilor referitoare la terţii implicaţi în acţiuni legate de lichidarea băncii respective; h) când interesele Băncii Naţionale necesită dezvăluirea acestor informaţii în cadrul unor proceduri judiciare; i) la cererea băncilor centrale, organelor de supraveghere a pieţei financiare şi a sistemelor de plăţi din alte state, în condițiile alin. (6). **Legea nr. 202/2017 privind activitatea băncilor, art. 126 alin. (2), alin. (5):** (2) Persoanele prevăzute la alin.(1) nu pot divulga informații confidențiale niciunei persoane sau autorități, cu excepția furnizării acestor informații în formă sumară sau agregată, astfel încît banca sau altă persoană la care se referă informațiile confidențiale să nu poată fi identificată. (5) Dispozițiile alin. (1)–(3) nu aduc în niciun fel atingere prevederilor legislației potrivit cărora se poate impune divulgarea de informații confidențiale în anumite situații. **Legea nr. 92/2022 privind activitatea de asigurare sau de reasigurare, art. 120 alin. (2), alin. (3):** (2) Persoanele menționate la alin. (1) nu pot divulga informațiile		

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
			confidențiale persoanelor fizice sau persoanelor juridice, cu excepția cazului în care aceste informații sunt prezentate într-o formă sintetică sau agregată care nu permite recunoașterea societății de asigurare sau de reasigurare la care se face referire sau a altor cazuri stabilite de legislație. (3) Interdicția menționată la alin. (2) nu se aplică în cazul: a) verificării îndeplinirii condițiilor de licențiere/înregistrare în Registrul agenților de asigurare și agenților bancassurance de către societățile de asigurare sau de reasigurare sau intermediarii în asigurări și/sau în reasigurări; b) aplicării sancțiunilor; c) contestării actelor normative ale autorității de supraveghere; d) furnizării informațiilor pentru desfășurarea procedurilor penale; e) insolvabilității sau lichidării obligatorii a unei societăți de asigurare sau de reasigurare pentru executarea creanțelor creditorilor împotriva acesteia.		
(4) Toate informațiile care fac obiectul unor schimburi între autoritățile competente în temeiul prezentului regulament și care privesc condițiile comerciale sau operaționale și alte chestiuni economice sau personale sunt considerate confidențiale și intră sub incidența obligației referitoare la secretul profesional, cu excepția cazului în care autoritatea competentă precizează, la momentul comunicării, că informațiile respective pot fi divulgate sau a cazului în care divulgarea acestora este necesară pentru desfășurarea unei proceduri judiciare.	CN	Pct. 169 (transcris la art. 55 alin. (1)).	**Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, art. 36 alin. (2):** (2) Obligaţia de păstrare a secretului profesional se extinde şi asupra informaţiilor confidenţiale create de Banca Naţională în scopul ori în legătură cu exercitarea atribuţiilor ei, a căror divulgare ar putea afecta exercitarea atribuțiilor de bază ale Băncii Naționale ori ar putea dăuna interesului sau prestigiului persoanei la care se referă.	parțial compatibil	Informațiile confidențiale sunt protejate prin lege. Legile naționale nu prevăd posibilitatea ca autoritatea să precizeze, la comunicare, că informațiile pot fi divulgate.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Articolul 56. Protecția datelor (1) AES și autoritățile competente sunt autorizate să prelucreze date cu caracter personal numai în cazul în care acest lucru este necesar în scopul îndeplinirii obligațiilor și sarcinilor care le revin în temeiul prezentului regulament, în special în ceea ce privește investigarea, realizarea de inspecții, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, evaluarea și elaborarea de planuri de supraveghere. Datele cu caracter personal se prelucrează în conformitate cu Regulamentul (UE) 2016/679 sau cu Regulamentul (UE) 2018/1725, în funcție de care dintre acestea este aplicabil.	PF+CN	170. BNM este autorizată să prelucreze date cu caracter personal numai în cazul în care acest lucru este necesar în scopul îndeplinirii obligațiilor și sarcinilor care îi revin în temeiul prezentului regulament, în special în ceea ce privește investigarea, realizarea de inspecții, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, aprecierea și elaborarea de planuri de supraveghere. Datele cu caracter personal se prelucrează în conformitate cu legislația privind protecția datelor cu caracter personal.	-	compatibil	Regulamentele (UE) 2016/679 și (UE) 2018/1725 sunt redate prin legislația națională privind protecția datelor cu caracter personal.
(2) Cu excepția cazului în care se prevede altfel în alte acte sectoriale, datele cu caracter personal menționate la alineatul (1) se păstrează până la îndeplinirea atribuțiilor de supraveghere aplicabile și, în orice caz, pentru o perioadă maximă de 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită păstrarea acestor date pentru o perioadă mai lungă.	PF	171. Cu excepția cazului în care se prevede altfel în alte acte sectoriale, datele cu caracter personal menționate la pct. 170 se păstrează până la îndeplinirea atribuțiilor de supraveghere aplicabile și, în orice caz, pentru o perioadă maximă de 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită păstrarea acestor date pentru o perioadă mai lungă.	-	compatibil	-
CAPITOLUL VIII Acte delegate **Articolul 57. Exercitarea delegării de competențe** (1) Se conferă Comisiei competența de a adopta acte delegate, cu respectarea condițiilor stabilite la prezentul articol. (2) Competența de a adopta acte delegate menționată la articolul 31 alineatul (6) și la articolul 43 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la 17 ianuarie 2024. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade. (3) Delegarea de competențe menționată la articolul 31 alineatul (6) și la articolul 43 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării competenței specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de	N/A	-	-	prevederi UE neaplicabile	Exercitarea delegării de competențe de către Comisia Europeană.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare. (4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare. (5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului. (6) Un act delegat adoptat în temeiul articolului 31 alineatul (6) și al articolului 43 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de trei luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.					
CAPITOLUL IX Dispoziții tranzitorii și finale **Secțiunea I** **Articolul 58. Clauza de reexaminare** (1) Până la 17 ianuarie 2028, după ce se consultă cu AES și CERS, după caz, Comisia efectuează o reexaminare și prezintă un raport Parlamentului European și Consiliului, însoțit, dacă este cazul, de o propunere legislativă. Reexaminarea include cel puțin următoarele aspecte: (a) criteriile pentru desemnarea furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 31 alineatul (2); (b) caracterul voluntar al notificării amenințărilor cibernetice semnificative menționat la articolul 19; (c) regimul menționat la articolul 31 alineatul (12) și competențele supraveghetorului principal prevăzute la articolul 35 alineatul (1) litera (d) punctul (iv) prima liniuță, în vederea evaluării eficacității dispozițiilor respective în ceea ce privește asigurarea unei supravegheri eficace a furnizorilor terți esențiali de	N/A	-	-	prevederi UE neaplicabile	Clauză de reexaminare de către Comisia Europeană.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
servicii TIC stabiliți într-o țară terță și necesitatea de a înființa o filială în Uniune. În scopul aplicării primului paragraf de la prezenta literă, reexaminarea include o analiză a regimului menționat la articolul 31 alineatul (12), inclusiv a condițiilor de acces al entităților financiare din Uniune la servicii din țări terțe și a disponibilității unor astfel de servicii pe piața Uniunii, și ține seama de evoluția pieței serviciilor care fac obiectul prezentului regulament, de experiența practică a entităților financiare și a supraveghetorilor financiari în ceea ce privește aplicarea și, respectiv, supravegherea regimului respectiv, precum și de orice evoluții relevante în materie de reglementare și de supraveghere care au loc la nivel internațional; (d) oportunitatea includerii în domeniul de aplicare al prezentului regulament a entităților financiare menționate la articolul 2 alineatul (3) litera (e) care recurg la sisteme de vânzări automatizate, ținând seama de evoluțiile viitoare ale pieței în ceea ce privește utilizarea unor astfel de sisteme; (e) funcționarea și eficacitatea RSC în ceea ce privește sprijinirea coerenței supravegherii și a eficienței schimbului de informații în interiorul cadrului de supraveghere. (2) În contextul reexaminării Directivei (UE) 2015/2366, Comisia evaluează necesitatea unei mai mari rezilienețe cibernetice a sistemelor de plăți și a activităților de prelucrare a plăților, precum și oportunitatea extinderii domeniului de aplicare al prezentului regulament la operatorii sistemelor de plată și la entitățile implicate în activitățile de prelucrare a plăților. În lumina acestei evaluări, Comisia prezintă Parlamentului European și Consiliului, în cadrul reexaminării Directivei (UE) 2015/2366, un raport până cel târziu la 17 iulie 2023. Pe baza respectivului raport de reexaminare și după consultarea AES, BCE și CERS, Comisia poate prezenta, dacă este cazul și ca parte a propunerii legislative pe care o poate adopta în temeiul articolului 108 al doilea paragraf din Directiva (UE) 2015/2366, o propunere urmărind să asigure faptul că toți operatorii sistemelor de plată și entitățile implicate în activitățile de prelucrare a plăților fac					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
obiectul unei supravegheri adecvate, ținând seama în același timp de supravegherea existentă din partea băncilor centrale. (3) Până la 17 ianuarie 2026, după consultarea AES și a Comitetului Organismelor Europene de Supraveghere a Auditului, Comisia efectuează o reexaminare și prezintă Parlamentului European și Consiliului un raport, însoțit, după caz, de o propunere legislativă, cu privire la oportunitatea unor cerințe mai stricte pentru auditorii statutari și firmele de audit în ceea ce privește reziliența operațională digitală, prin includerea auditorilor statutari și a firmelor de audit în domeniul de aplicare al prezentului regulament sau prin intermediul unor modificări ale Directivei 2006/43/CE a Parlamentului European și a Consiliului.					
Secțiunea II Modificări **Articolul 59. Modificarea Regulamentului (CE) nr. 1060/2009** Regulamentul (CE) nr. 1060/2009 se modifică după cum urmează: 1. În anexa I secțiunea A punctul 4, primul paragraf se înlocuiește cu următorul text: „Agenția de rating de credit dispune de proceduri contabile și administrative sigure, de mecanisme de control intern, de tehnici eficiente de evaluare a riscurilor și de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului. Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).” " 2. În anexa III, punctul 12 se înlocuiește cu următorul text: „12. Agenția de rating de credit încalcă articolul 6 alineatul (2), coroborat cu punctul 4 din anexa I secțiunea A,	N/A	-	-	prevederi UE neaplicabile	Modificarea altor acte ale Uniunii.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
prin faptul că nu dispune de proceduri contabile sau administrative sigure, de mecanisme de control intern, de proceduri eficiente de evaluare a riscurilor sau de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 sau prin faptul că nu pune în aplicare sau nu menține proceduri decizionale ori structuri organizaționale în conformitate cu punctul respectiv.”					
Articolul 60. Modificarea Regulamentului (UE) nr. 648/2012 Regulamentul (UE) nr. 648/2012 se modifică după cum urmează: 1. Articolul 26 se modifică după cum urmează: (a) alineatul (3) se înlocuiește cu următorul text: „(3) CPC mențin și utilizează o structură organizatorică adecvată pentru a le asigura continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților. Ele utilizează sisteme, resurse și proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului. Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”;" (b) alineatul (6) se elimină. 2. Articolul 34 se modifică după cum urmează: (a) alineatul (1) se înlocuiește cu următorul text: „(1) CPC prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite și puse în aplicare în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor.”;	N/A	-	-	prevederi UE neaplicabile	Modificarea altor acte ale Uniunii.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
(b) la alineatul (3), primul paragraf se înlocuiește cu următorul text: „(3) Pentru a asigura aplicarea consecventă a prezentului articol, ESMA, după consultarea membrilor SEBC, elaborează proiecte de standarde tehnice de reglementare în care precizează conținutul și cerințele minime ale politicii de continuitate a activității și ale planului de recuperare în caz de dezastru, excluzând politica de continuitate a activității TIC și planurile de recuperare în caz de dezastru în domeniul TIC.” 3. La articolul 56 alineatul (3), primul paragraf se înlocuiește cu următorul text: „(3) Pentru a asigura aplicarea consecventă a prezentului articol, ESMA elaborează proiecte de standarde tehnice de reglementare în care precizează detaliile, altele decât cele pentru cerințele legate de gestionarea riscurilor TIC, ale cererii de înregistrare menționate la alineatul (1).” 4. La articolul 79, alineatele (1) și (2) se înlocuiesc cu următorul text: „(1) Registrele centrale de tranzacții identifică sursele de risc operațional și le reduc la minimum și prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554. (2) Registrele centrale de tranzacții prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor.” 5. La articolul 80, alineatul (1) se elimină. 6. În anexa I, secțiunea II se modifică după cum urmează: (a) literele (a) și (b) se înlocuiesc cu următorul text: „(a) un registru central de tranzacții încalcă articolul 79 alineatul (1) dacă nu identifică sursele de risc operațional și nu reduce la minimum riscurile					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
respective prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554; (b) un registru central de tranzacții încalcă articolul 79 alineatul (2) dacă nu prevede, nu aplică sau nu menține o politică adecvată de continuitate a activității și un plan adecvat de redresare în caz de dezastru instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor sale, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor;"; (b) litera (c) se elimină. 7. Anexa III se modifică după cum urmează: (a) secțiunea II se modifică după cum urmează: (i) litera (c) se înlocuiește cu următorul text: „(c) CPC de nivel 2 încalcă articolul 26 alineatul (3) dacă nu mențin sau nu utilizează o structură organizatorică care să asigure continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților lor sau dacă nu utilizează sisteme, resurse sau proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554"; (ii) litera (f) se elimină; (b) în secțiunea III, litera (a) se înlocuiește cu următorul text: „(a) CPC de nivel 2 încalcă articolul 34 alineatul (1) dacă nu prevăd, aplică sau mențin o politică adecvată de continuitate a activității și un plan adecvat de răspuns și de recuperare instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CPC, care să permită cel puțin reluarea tuturor tranzacțiilor aflate în curs în momentul întreruperii, astfel încât CPC să poată continua să funcționeze în condiții de certitudine și să efectueze decontarea la data stabilită;".					
Articolul 61. Modificarea Regulamentului (UE) nr. 909/2014	N/A	-	-	prevederi UE neaplicabile	Modificarea altor acte ale Uniunii.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Articolul 45 din Regulamentul (UE) nr. 909/2014 se modifică după cum urmează: 1. Alineatul (1) se înlocuiește cu următorul text: „(1) CSD-urile identifică sursele de riscuri operaționale, atât interne, cât și externe, și reduc la minimum impactul acestora și prin implementarea unor instrumente, procese și politici TIC adecvate, instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului, precum și prin orice alte instrumente, mecanisme de control și proceduri adecvate relevante pentru alte tipuri de riscuri operaționale, inclusiv pentru toate sistemele de decontare a titlurilor de valoare pe care le exploatează. Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).” " 2. Alineatul (2) se elimină. 3. Alineatele (3) și (4) se înlocuiesc cu următorul text: „(3) Pentru serviciile pe care le prestează, precum și pentru fiecare sistem de decontare a titlurilor de valoare pe care îl exploatează, CSD-urile prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura continuitatea serviciilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CSD-urilor în cazul unor evenimente care prezintă un risc semnificativ de perturbare a operațiunilor. (4) Planul menționat la alineatul (3) prevede reluarea tuturor tranzacțiilor și pozițiilor participanților în momentul perturbării, pentru a permite participanților la un CSD să continue să funcționeze în condiții de siguranță și să efectueze decontarea la data stabilită, inclusiv prin garantarea faptului că sistemele IT					

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
esențiale pot relua operațiunile aflate în curs în momentul perturbării, astfel cum se prevede la articolul 12 alineatele (5) și (7) din Regulamentul (UE) 2022/2554.” 4. Alineatul (6) se înlocuiește cu următorul text: „(6) CSD-urile identifică, monitorizează și gestionează riscurile pe care le pot prezenta pentru operațiunile lor participanții principali la sistemele de decontare a titlurilor de valoare pe care le exploatează, precum și furnizorii de servicii și utilități, dar și alte CSD-uri sau alte infrastructuri ale piețelor. La cerere, CSD-urile furnizează autorităților competente și relevante informații cu privire la orice astfel de riscuri identificate. De asemenea, acestea informează autoritatea competentă și autoritățile relevante, fără întârziere, cu privire la orice incident operațional, altul decât cele legate de riscurile TIC, care rezultă din astfel de riscuri.” 5. La alineatul (7), primul paragraf se înlocuiește cu următorul text: „(7) ESMA elaborează, în strânsă cooperare cu membrii SEBC, proiecte de standarde tehnice de reglementare care să precizeze riscurile operaționale menționate la alineatele (1) și (6), altele decât riscurile TIC, metodele de testare, abordare și reducere la minimum a riscurilor respective, inclusiv politicile de continuitate a activității și planurile de recuperare în caz de dezastru menționate la alineatele (3) și (4), precum și modalitățile de evaluare a acestora.”					
Articolul 62. Modificarea Regulamentului (UE) nr. 600/2014 Regulamentul (UE) nr. 600/2014 se modifică după cum urmează: 1. Articolul 27g se modifică după cum urmează: (a) alineatul (4) se înlocuiește cu următorul text: „(4) APA respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului. Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022	N/A	-	-	prevederi UE neaplicabile	Modificarea altor acte ale Uniunii.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).";" (b) la alineatul (8), litera (c) se înlocuiește cu următorul text: „(c) cerințele organizatorice concrete prevăzute la alineatele (3) și (5).” 2. Articolul 27h se modifică după cum urmează: (a) alineatul (5) se înlocuiește cu următorul text: „(5) CTP respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.”; (b) la alineatul (8), litera (e) se înlocuiește cu următorul text: „(e) cerințele organizatorice concrete prevăzute la alineatul (4).” 3. Articolul 27i se modifică după cum urmează: (a) alineatul (3) se înlocuiește cu următorul text: „(3) ARM respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.”; (b) la alineatul (5), litera (b) se înlocuiește cu următorul text: „(b) cerințele organizatorice concrete prevăzute la alineatele (2) și (4).”					
Articolul 63. Modificarea Regulamentului (UE) 2016/1011 La articolul 6 din Regulamentul (UE) 2016/1011 se adaugă următorul alineat: „(6) Pentru indicii de referință critici, administratorul dispune de proceduri administrative și contabile sigure, de mecanisme de control intern, de proceduri eficace de evaluare a riscurilor și de mecanisme eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu	N/A	-	-	prevederi UE neaplicabile	Modificarea altor acte ale Uniunii.

6. Prevederile Regulamentului/Deciziei UE	7. Tehnica aplicată (cod)	8. Prevederile proiectului	9. Prevederile actului/actelor normativ(e) național(e)	10. Calificativul de compatibilitate	11. Observații/justificări
Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului.					
Articolul 64. Intrarea în vigoare și aplicarea Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene. Se aplică de la 17 ianuarie 2025.	N/A	-	-	prevederi UE neaplicabile	Intrarea în vigoare a regulamentului. Intrarea în vigoare a proiectului se stabilește prin hotărârea Comitetului executiv al BNM.